

Version 8.2

# Layer 7 Policy Manager User Manual



1.800.681.9377  
info@layer7tech.com  
www.layer7tech.com



Copyright © 2014 CA. All rights reserved.

This documentation and any related computer software help programs (hereinafter referred to as the "Documentation") are for your informational purposes only and are subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW OR AS AGREED BY CA IN ITS APPLICABLE LICENSE AGREEMENT, CA PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO THE END USER OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

# Contents

|   |           |
|---|-----------|
| <b>Chapter 1: Getting Started</b>       | <b>1</b>  |
| <b>Overview</b>                         | <b>1</b>  |
| Supported Standards                     | 1         |
| CA API Gateway                          | 2         |
| CA API Gateway - Policy Manager         | 3         |
| Securespan XML VPN Client               | 3         |
|   | 4         |
| <b>Chapter 2: The Policy Manager</b>    | <b>5</b>  |
| <b>Starting the Policy Manager</b>      | <b>5</b>  |
| Running the Desktop Client              | 5         |
| Running the Browser Client              | 6         |
| <b>Connecting to the Gateway</b>        | <b>8</b>  |
| <b>Policy Manager Browser Client</b>    | <b>11</b> |
| <b>Learning the Interface</b>           | <b>12</b> |
| Interfaces                              | 13        |
| Main Menu                               | 15        |
| Main Tool Bar                           | 22        |
| Assertions Tool Bar                     | 23        |
| Policy Tool Bar                         | 24        |
| [Identity Providers] Tab                | 25        |
| [Assertions] Tab                        | 25        |
| Services and Policies                   | 25        |
| Home Page                               | 27        |
| Policy Development Window               | 28        |
| Policy Validation Messages Window       | 28        |
| Status Bar                              | 28        |
| Assertion Numbering                     | 30        |
| Policy Search Bar                       | 31        |
| Viewing Assertion Information           | 32        |
| My Account                              | 34        |
| <b>General Workflow</b>                 | <b>36</b> |
| <b>Managing Gateway Licenses</b>        | <b>37</b> |
| Installing a License File               | 38        |
| Removing a License File                 | 39        |
| <b>Managing Cluster-Wide Properties</b> | <b>40</b> |
| <b>Managing Stored Passwords</b>        | <b>42</b> |
| Changing a Password                     | 44        |
| Stored Password Properties              | 45        |
| Managing Password Policy                | 48        |
| Force Administrative Password Reset     | 53        |
| <b>Managing Listen Ports</b>            | <b>54</b> |
| Listen Port Properties                  | 57        |
| Managing Interfaces                     | 76        |
| Managing Firewall Rules                 | 78        |
| Firewall Rule Properties                | 81        |
| <b>Managing JDBC Connections</b>        | <b>82</b> |
| JDBC Connection Properties              | 83        |

|  |            |
|--|------------|
| <b>Managing JMS Destinations</b>           | <b>89</b>  |
| Context Variables Created by JMS Requests  | 91         |
| Resolving Requests in JMS Destinations     | 91         |
| Understanding JMS Message Size             | 92         |
| Working with JMS Destinations              | 92         |
| Troubleshooting Connection Issues with EMS | 93         |
| Running the Manage JMS Destinations Task   | 94         |
| JMS Destination Properties                 | 96         |
| <b>Managing MQ Native Queues</b>           | <b>110</b> |
| Understanding MQ Native Message Size       | 110        |
| Working with MQ Native Queues              | 111        |
| MQ Native Queue Properties                 | 114        |
| Customizing MQ Messages                    | 122        |
| <b>Managing Email Listeners</b>            | <b>126</b> |
| Email Listener Properties                  | 127        |
| <b>Managing Roles</b>                      | <b>130</b> |
| Predefined Roles and Permissions           | 132        |
| Understanding Role Permissions             | 137        |
| Add Permissions to Role Wizard             | 142        |
| Creating a Custom Role                     | 149        |
| Editing a Custom Role                      | 150        |
| Deleting a Custom Role                     | 151        |
| Adding a User or Group to a Role           | 152        |
| Removing a User or Group from a Role       | 152        |
| <b>Managing Security Zones</b>             | <b>153</b> |
| Working with the Security Zones Area       | 155        |
| About the [Properties] Tab                 | 155        |
| About the [Entities] Tab                   | 156        |
| Understanding Security Zones               | 156        |
| Security Zone Properties                   | 159        |
| Assigning Security Zones                   | 160        |
| <b>Managing Log Sinks</b>                  | <b>164</b> |
| Logged Information                         | 165        |
| Creating a Log Sink                        | 166        |
| Log Sink Properties                        | 167        |
| Managing the Audit Sink                    | 175        |
| Configure External Audit Store Wizard      | 177        |
| Working with the Audit Sink Policy         | 178        |
| Working with the Audit Lookup Policy       | 182        |
| Working with Log Sinks and Debug Logs      | 185        |
| <b>Managing ESM User Mappings</b>          | <b>186</b> |
| <b>Managing HTTP Options</b>               | <b>188</b> |
| Adding an HTTP Option                      | 190        |
| Selecting Cipher Suites                    | 194        |
| <b>Managing Service Resolution</b>         | <b>196</b> |
| <b>Managing SFTP Polling Listeners</b>     | <b>199</b> |
| SFTP Polling Listener Properties           | 201        |
| Working with SCP/SFTP Messages             | 206        |
| <b>Managing Keystore</b>                   | <b>208</b> |
| <b>Configuring Preferences</b>             | <b>210</b> |
| <b>Working with JSON</b>                   | <b>213</b> |

|   |                |
|---|----------------|
| Transforming Messages Between XML and JSON .....                            | 213            |
| <b>Working With Dynamic Routing .....</b>                                   | <b>214</b>     |
| <b>Working with CA SiteMinder .....</b>                                     | <b>216</b>     |
| Creating a SiteMinder Configuration .....                                   | 216            |
| Basic User Authentication using SiteMinder Assertions .....                 | 217            |
| Basic User Authentication via HTTP Cookie using SiteMinder Assertions ..... | 217            |
| Advanced SiteMinder Authorization with Status Check of Session .....        | 218            |
| Troubleshooting SiteMinder .....  | 219            |
| Managing SiteMinder Configurations .....                                    | 220            |
| SiteMinder Configuration Properties .....                                   | 222            |
| <b>How to Establish Outbound Secure Conversation .....</b>                  | <b>227</b>     |
| <b>How to Integrate the Gateway with WCF .....</b>                          | <b>228</b>     |
| Scenario 1: Gateway as WCF Client .....                                     | 228            |
| Scenario 2: Gateway as WCF Service .....                                    | 229            |
| Scenario 3: Gateway as a "Secure Conversation pass-through" .....           | 229            |
| <b>How to Configure Listeners for the Enterprise Service Manager .....</b>  | <b>230</b>     |
| <b>How to Use the Gateway as an HTTP Proxy .....</b>                        | <b>232</b>     |
| <b>Troubleshooting Mode .....</b>   | <b>233</b>     |
| <b>Wildcard Matching of Hostnames .....</b>                                 | <b>234</b>     |
| <b>Configuring Encryption Settings .....</b>                                | <b>235</b>     |
| <br><b>Chapter 3: Managing Certificates .....</b>                           | <br><b>237</b> |
| <b>Certificate Expiration Notification .....</b>                            | <b>237</b>     |
| <b>Adding a New Certificate .....</b>                                       | <b>239</b>     |
| <b>Add Certificate Wizard .....</b>   | <b>240</b>     |
| Step 1: Enter Certificate Info .....  | 240            |
| Step 2: View Certificate Details .....                                      | 241            |
| Step 3: Specify Certificate Options .....                                   | 242            |
| Step 4: Configure Validation .....  | 244            |
| <b>Certificate Properties .....</b>   | <b>246</b>     |
| <b>Editing a Certificate .....</b>  | <b>247</b>     |
| <b>Deleting a Certificate .....</b>   | <b>247</b>     |
| <b>Exporting a Certificate .....</b>  | <b>248</b>     |
| <b>Importing Certificates .....</b>   | <b>248</b>     |
| <b>Configure Recipient Certificate Wizard .....</b>                         | <b>250</b>     |
| <b>Managing Certificate Validation .....</b>                                | <b>251</b>     |
| Trust Anchors .....   | 252            |
| Editing a Revocation Checking Policy .....                                  | 254            |
| Certificate Revocation Checking Properties .....                            | 257            |
| Searching Trusted Certificates .....  | 259            |
| <b>Managing Private Keys .....</b>  | <b>260</b>     |
| Creating a Private Key .....  | 262            |
| Importing a Private Key .....   | 265            |
| Exporting a Private Key .....   | 266            |
| Deleting a Private Key .....  | 266            |
| Generating a Certificate Signing Request (CSR) .....                        | 267            |
| Signing a Certificate .....   | 268            |
| Private Key Properties .....  | 271            |
| Private Key Locations .....   | 274            |
| Setting a Default SSL or CA Private Key .....                               | 274            |
| Selecting a Custom Private Key .....  | 275            |

|   |            |
|---|------------|
| <b>Chapter 4: Working with Identity Providers</b> | <b>279</b> |
| Impact of Security Zones                          | 280        |
| Searching Identity Providers                      | 280        |
| Working with Policy-Backed Identity Providers     | 282        |
| Identity Tags                                     | 283        |
| Revoking User Certificates                        | 285        |
| Internal Identity Provider Users and Groups       | 286        |
| Creating an Internal User                         | 286        |
| Internal User Properties                          | 288        |
| Creating an Internal Group                        | 294        |
| Group Properties                                  | 295        |
| Editing or Deleting a User or Group               | 299        |
| Internal Identity Provider Wizard                 | 300        |
| Managing Administrative User Account Policy       | 301        |
| LDAP Identity Providers                           | 303        |
| Simple LDAP Identity Providers                    | 304        |
| LDAP Identity Provider Users and Groups           | 304        |
| Creating an LDAP or Simple LDAP Identity Provider | 304        |
| Cloning an LDAP or Simple LDAP Identity Provider  | 305        |
| Editing an LDAP or Simple LDAP Identity Provider  | 305        |
| Deleting an LDAP or Simple LDAP Identity Provider | 306        |
| LDAP Identity Provider Wizard                     | 306        |
| Simple LDAP Identity Provider Wizard              | 319        |
| LDAP User Properties                              | 321        |
| Policy-Backed Identity Providers                  | 325        |
| Backing Policy                                    | 325        |
| Hints and Tips                                    | 325        |
| Creating a Policy-Backed Identity Provider        | 326        |
| Editing a Policy-Backed Identity Provider         | 327        |
| Deleting a Policy-Backed Identity Provider        | 327        |
| Policy-Backed Identity Provider Wizard            | 327        |
| <b>Chapter 5: Working with Services</b>           | <b>331</b> |
| Working with SOAP Web Services                    | 331        |
| Publish SOAP Web Service Wizard                   | 333        |
| Create WSDL Wizard                                | 337        |
| Publishing a Non-SOAP Application                 | 346        |
| Publish Web API Wizard                            | 346        |
| Working with RESTful Web Services                 | 349        |
| Securing a RESTful Web Service                    | 350        |
| Publish REST Service Proxy Wizard                 | 352        |
| Managing Published Services                       | 356        |
| Service Properties                                | 357        |
| Disabling a Service                               | 367        |
| Enabling a Service                                | 368        |
| Renaming a Service                                | 368        |
| Deleting a Published Service                      | 369        |
| Viewing the WSDL for a Service                    | 369        |
| Resetting the WSDL for a Service                  | 370        |
| Changing the Resolution Path for a Service        | 371        |

|  |            |
|--|------------|
| <b>Working with Internal Services</b>                          | <b>371</b> |
| Specifying a Resource for an WSDM Service                      | 373        |
| Publishing an Internal Service                                 | 374        |
| Publish Internal Service Wizard                                | 375        |
| Working with the Security Token Service                        | 377        |
| Working with the Generic Identity Management Service           | 382        |
| <b>Sample Messages</b>   | <b>386</b> |
| Adding a Sample Message  | 386        |
| Editing a Sample Message                                       | 388        |
| Deleting a Sample Message                                      | 388        |
| <b>Working with FTP Requests</b>                               | <b>389</b> |
| Setting Up the FTP Server                                      | 390        |
| Configuring a Policy for FTP                                   | 390        |
| Context Variables Used   | 391        |
| Limitations and Considerations                                 | 391        |
| <b>Configuring a Reverse Web Proxy</b>                         | <b>392</b> |
| Using the Publish Reverse Web Proxy Wizard                     | 392        |
| Using a Global Policy to Proxy Multiple Web Applications       | 393        |
| Using Multiple Listen Ports to Proxy Multiple Web Applications | 394        |
| Publish Reverse Web Proxy Wizard                               | 395        |
| <b>Chapter 6: Analyzing Gateway Performance</b>                | <b>401</b> |
| <b>Dashboard - Service Metrics</b>                             | <b>402</b> |
| Filters  | 403        |
| Response Times   | 404        |
| Notification Bar   | 404        |
| Message Rates  | 404        |
| Interval Summary   | 405        |
| Zooming Time Intervals   | 406        |
| <b>Dashboard - Cluster Status</b>                              | <b>406</b> |
| Gateway Status Table   | 407        |
| Service Statistics Table                                       | 409        |
| <b>Viewing Logs</b>  | <b>409</b> |
| Saving the Log   | 412        |
| <b>FTP Audit Archiver</b>                                      | <b>413</b> |
| <b>Gateway Audit Events</b>                                    | <b>415</b> |
| Showing/Hiding Panels  | 417        |
| Source Panel   | 417        |
| Time Range Panel   | 418        |
| Audit Record Search Parameters                                 | 418        |
| Entity Search Parameters                                       | 420        |
| Associated Logs Search Parameter                               | 420        |
| Message Operation Search Parameter                             | 420        |
| Validate Signatures  | 420        |
| Audit Events Panel   | 421        |
| Event Details Panel  | 422        |
| Invoking the Audit Viewer Policy                               | 424        |
| Gateway Audit Event Actions                                    | 424        |
| <b>Saved Events</b>  | <b>426</b> |
| <b>Overriding the Audit Level</b>                              | <b>427</b> |

|  |            |
|--|------------|
| <b>Chapter 7: Identity Bridging</b>  | <b>429</b> |
| <b>The Identity Silo Problem</b>   | <b>429</b> |
| <b>Identity Bridging for Cross-Domain Application Integration</b>                  | <b>429</b> |
| Identity Bridging Using the SAML Credential SourceCA Technologies                  | 430        |
| Identity Bridging Using the X.509 Certificate Credential Source                    | 431        |
| <b>Identity Bridging with CA Products</b>  | <b>431</b> |
| SecureSpan Gateway   | 431        |
| Securespan XML VPN Client  | 432        |
| CA API Gateway Policy Manager  | 432        |
| <b>Identity Bridging Requirements</b>  | <b>433</b> |
| Web Service Requestor-Side Requirements  | 433        |
| Trusted Authority (Authentication Domain) Requirements                             | 433        |
| Federated Gateway (Authorization Domain) Requirements                              | 434        |
| <b>Verifying Hostnames for Outbound SSL Connections</b>                            | <b>434</b> |
| <b>Workflow Using SAML</b>   | <b>436</b> |
| <b>Workflow Using an X.509 Certificate</b>   | <b>437</b> |
| Certificate Usage Scenarios  | 438        |
| <b>Federated Identity Providers</b>  | <b>440</b> |
| Creating a Federated Identity Provider   | 441        |
| Cloning a Federated Identity Provider  | 441        |
| Editing a Federated Identity Provider  | 441        |
| Deleting a Federated Identity Provider   | 442        |
| Federated Identity Provider Wizard   | 442        |
| <b>Federated Identity Provider Users and Groups</b>                                | <b>445</b> |
| Creating a Federated User  | 446        |
| Federated User Properties  | 448        |
| Creating a Federated Group   | 451        |
| Creating a Federated Virtual Group   | 452        |
| Group Properties   | 454        |
| Editing or Deleting a User or Group  | 458        |
| <b>Searching Identity Providers</b>  | <b>459</b> |
| Working with Policy-Backed Identity Providers                                      | 461        |
| <b>Configuring SAML Policies for Identity Bridging</b>                             | <b>462</b> |
| <b>Using the Securespan XML VPN Client for Identity Bridging</b>                   | <b>466</b> |
| <b>Chapter 8: Tutorials</b>  | <b>467</b> |
| <b>Tutorial #1: How to Configure Your System to Work with the Demo Environment</b> | <b>468</b> |
| Step 1: Locate the hosts file  | 468        |
| Step 2: Edit the hosts file  | 469        |
| Next Steps   | 470        |
| <b>Tutorial #2: How to Access a Test Service Using soapUI</b>                      | <b>471</b> |
| Step 1: Load WSDL in soapUI  | 471        |
| Step 2: Send a request and view the response                                       | 472        |
| Next Steps   | 474        |
| <b>Tutorial #3: How to Access a Test Service via the Gateway</b>                   | <b>475</b> |
| Step 1: Publish and configure the service  | 475        |
| Step 2: Send a test message through the CA API Gateway                             | 479        |
| Next Steps   | 480        |
| <b>Tutorial #4: How to Manage Identity Providers</b>                               | <b>481</b> |
| Using the Internal Identity Provider   | 481        |



|  |            |
|--|------------|
| Configuring an LDAP Connection .....                                   | 485        |
| Next Steps .....   | 489        |
| <b>Tutorial #5: How to Add SSL and HTTP Basic Authentication</b> ..... | <b>490</b> |
| Step 1: Add SSL constraint and send a test message .....               | 490        |
| Step 2: Add HTTP Basic Authentication .....                            | 493        |
| Next Steps .....   | 495        |
| <b>Tutorial #6: How to Use the SecureSpan Policy Language</b> .....    | <b>496</b> |
| Basic Concepts .....   | 496        |
| Editing a Policy .....   | 497        |
| Policy Branching .....   | 499        |
| Hints and Tips .....   | 500        |
| Exercises .....  | 501        |
| Client vs. Server View of Policy .....                                 | 502        |
| Next Steps .....   | 502        |
| <b>Chapter 9: Solution Kits</b> .....                                  | <b>503</b> |
| <b>Salesforce Integration Solution Kit</b> .....                       | <b>503</b> |
| Managing Salesforce Operation Service Connections .....                | 503        |
| Salesforce Connection Properties .....                                 | 504        |
| <b>Appendix A: Contacting CA Technologies</b> .....                    | <b>507</b> |
| <b>Technical Support</b> .....   | <b>507</b> |
| <b>Contact Information</b> .....                                       | <b>507</b> |
| <b>Appendix B: Features by Product</b> .....                           | <b>509</b> |
| <b>Appendix C: Context Variables</b> .....                             | <b>517</b> |
| Multivalued Context Variables .....                                    | 518        |
| Where Context Variables are Defined .....                              | 518        |
| Context Variable Naming Rules .....                                    | 518        |
| Context Variable Data Types .....                                      | 519        |
| Context Variable Validation .....                                      | 520        |
| Checking for Existence of Context Variables .....                      | 520        |
| Predefined Context Variables .....                                     | 521        |
| General Context Variables .....  | 522        |
| Audit Variables .....  | 524        |
| Audit Lookup Variables .....   | 524        |
| Audit Sink Variables .....   | 528        |
| Authentication Variables .....   | 531        |
| Certificate Attributes Variables .....                                 | 533        |
| Credential Certificates Variables .....                                | 537        |
| Date and Time Variables .....  | 539        |
| Kerberos Ticket Authorization Info Variables .....                     | 540        |
| Message Layer Variables .....  | 544        |
| Message Routing Variables .....  | 547        |
| Service/Policy Variables .....   | 549        |
| System Variables .....   | 549        |
| Transport Layer Variables .....  | 550        |
| Working with Multivalued Context Variables .....                       | 558        |
| Context Variables for XPath's .....                                    | 560        |
| Context Variables for CA SiteMinder .....                              | 562        |

|  |            |
|--|------------|
| <b>Appendix D: Gateway Cluster Properties</b>              | <b>567</b> |
| Time Units   | 567        |
| Administrative Account Cluster Properties                  | 567        |
| Audit Archiver Cluster Properties                          | 568        |
| Audit Cluster Properties                                   | 569        |
| Certificate Validation Cluster Properties                  | 574        |
| Credential Caching Cluster Properties                      | 577        |
| Email Cluster Properties                                   | 580        |
| Enterprise Service Manager Cluster Properties              | 580        |
| Fault Level Cluster Properties                             | 581        |
| FTP Cluster Properties                                     | 582        |
| Global Cluster Properties                                  | 583        |
| Input/Output Cluster Properties                            | 584        |
| JDBC Cluster Properties                                    | 595        |
| Kerberos Cluster Properties                                | 597        |
| LDAP Cluster Properties                                    | 598        |
| Message Validation Cluster Properties                      | 599        |
| Rate Limit Cluster Properties                              | 602        |
| SAML Cluster Properties                                    | 602        |
| Service Cluster Properties                                 | 603        |
| Traffic Logger Cluster Properties                          | 605        |
| UDDI Cluster Properties                                    | 606        |
| WS-Security Cluster Properties                             | 607        |
| XML Security Cluster Properties                            | 610        |
| Miscellaneous Cluster Properties                           | 613        |
| <b>Appendix E: Assertion Status Codes</b>                  | <b>625</b> |
| <b>Appendix F: Audit Message Codes</b>                     | <b>627</b> |
| Customizing the Audit Format for Logging                   | 651        |
| <b>Appendix G: Key Usage Enforcement Policy</b>            | <b>653</b> |
| Recognized Action Names                                    | 653        |
| Sample Enforcement Policy Template                         | 654        |
| <b>Appendix H: Actional Integration</b>                    | <b>657</b> |
| Configuring the Actional Integration                       | 657        |
| Configuring the Routing Assertion                          | 659        |
| Enabling Debugging   | 660        |
| <b>Appendix I: Stylesheet for Transforming XML to JSON</b> | <b>661</b> |
| <b>Appendix J: SiteMinder Failure Reasons</b>              | <b>665</b> |
| <b>Index</b>   | <b>667</b> |

## List of Figures

|   |     |
|---|-----|
| Figure 1: CA API Gateway Deployment Architecture .....  | 2   |
| Figure 2: Login dialog .....  | 9   |
| Figure 3: General Interface: Identity Provider and Home Page .....                              | 13  |
| Figure 4: General Interface: Assertions and Policy Tree .....                                   | 14  |
| Figure 5: Audit Alert dialog .....  | 29  |
| Figure 6: Assertion numbering example .....   | 30  |
| Figure 7: Context variables listed in a tooltip .....   | 32  |
| Figure 8: The Assertion Information dialog .....  | 33  |
| Figure 9: My Account - [Properties] tab .....   | 35  |
| Figure 10: Manage Gateway Licenses dialog .....   | 37  |
| Figure 11: Manage Cluster-Wide Properties (with sample values) .....                            | 41  |
| Figure 12: Manage Stored Passwords dialog .....   | 43  |
| Figure 13: Change Password dialog .....   | 45  |
| Figure 14: Stored Password Properties - Adding a password .....                                 | 46  |
| Figure 15: Stored Password Properties - Adding a PEM private key .....                          | 46  |
| Figure 16: Stored Password Properties - Editing a password .....                                | 47  |
| Figure 17: Internal Identity Provider Password Policy dialog .....                              | 50  |
| Figure 18: Force Administrative Passwords Reset dialog .....                                    | 54  |
| Figure 19: Manage Listen Ports dialog .....   | 55  |
| Figure 20: Listen Port Properties - [Basic Settings] tab .....                                  | 59  |
| Figure 21: Listen Port Properties - [SSL/TLS Settings] tab .....                                | 62  |
| Figure 22: Listen Port Properties - [Pool Settings] tab .....                                   | 63  |
| Figure 23: Listen Port Properties - [FTP Settings] tab .....                                    | 64  |
| Figure 24: Listen Port Properties - [Other Settings] tab .....                                  | 71  |
| Figure 25: Listen Port Properties - [Advanced] tab .....  | 74  |
| Figure 26: Managing Interfaces dialog .....   | 77  |
| Figure 27: Manage Firewall Rules dialog .....   | 79  |
| Figure 28: Simple Firewall Rule Properties .....  | 81  |
| Figure 30: Manage JDBC Connection dialog .....  | 82  |
| Figure 31: JDBC Connection Properties dialog .....  | 87  |
| Figure 32: Manage JMS Destinations dialog .....   | 94  |
| Figure 33: JMS Destination Properties - [Basics] tab .....                                      | 97  |
| Figure 34: JMS Destination Properties - [JNDI] tab (based on Provider Type "TIBCO EMS") .....   | 99  |
| Figure 35: JMS Destination Properties - [Destination] tab (for provider type 'TIBCO EMS') ..... | 101 |
| Figure 36: JMS Destination Properties - [Inbound Options] tab .....                             | 104 |
| Figure 37: JMS Destination Properties - [Outbound Options] tab .....                            | 108 |
| Figure 38: Manage MQ Native Queues dialog .....   | 112 |
| Figure 39: MQ Native Queue Properties - [MQ Connection Properties] tab .....                    | 115 |
| Figure 40: MQ Native Queue Properties - [Inbound Options] tab .....                             | 118 |
| Figure 41: MQ Native Queue Properties - [Outbound Options] tab .....                            | 121 |
| Figure 42: MQ Message sequence diagram .....  | 123 |
| Figure 43: Customize message descriptors .....  | 124 |
| Figure 44: Adding a customized message descriptor .....   | 125 |
| Figure 45: Manage Email Listeners form .....  | 126 |
| Figure 46: Email Listener Properties dialog .....   | 128 |
| Figure 47: Manage Roles dialog .....  | 131 |
| Figure 48: Permissions for a role .....   | 138 |
| Figure 49: Add Permissions to Role Wizard - Step 1 .....  | 143 |
| Figure 50: Add Permissions to Role Wizard - Step 2 (selection by condition example) .....       | 144 |
| Figure 51: Add Permissions to Role Wizard - Step 3 .....  | 148 |
| Figure 52: Create Role dialog .....   | 149 |
| Figure 53: Permission Group Properties: example of "<complex scope>" .....                      | 150 |

|  |     |
|--|-----|
| Figure 54: Remove Role confirmation dialog .....                             | 151 |
| Figure 55: Manage Security Zones dialog .....                                | 154 |
| Figure 56: Security zone unavailable message .....                           | 158 |
| Figure 57: Security Zone Properties dialog .....                             | 159 |
| Figure 58: Set security zone via right-click .....                           | 161 |
| Figure 59: Selecting a security zone .....                                   | 161 |
| Figure 60: The Security Zone setting in a properties dialog .....            | 162 |
| Figure 61: Assign Security Zones dialog .....                                | 163 |
| Figure 62: Manage Log Sinks dialog .....                                     | 164 |
| Figure 63: Log Sink Properties - [Base Settings] tab .....                   | 168 |
| Figure 64: Log Sink Properties - [File Settings] tab .....                   | 171 |
| Figure 65: Log Sink Properties - [Syslog Settings] tab .....                 | 173 |
| Figure 66: Audit Sink Properties .....                                       | 175 |
| Figure 67: Configure External Audit Store Wizard .....                       | 177 |
| Figure 68: Audit Sink Policy on the interface .....                          | 178 |
| Figure 69: Audit sink default policy - custom .....                          | 180 |
| Figure 70: Audit sink default policy - JDBC .....                            | 181 |
| Figure 71: Audit Lookup Policy on the interface .....                        | 182 |
| Figure 72: Sample custom audit lookup policy .....                           | 183 |
| Figure 73: Default JDBC audit sink lookup policy .....                       | 184 |
| Figure 74: Manage ESM User Mappings dialog .....                             | 187 |
| Figure 75: Manage HTTP Options dialog .....                                  | 188 |
| Figure 76: Edit HTTP Options - [General] tab .....                           | 191 |
| Figure 77: Edit HTTP Options - [Proxy] tab .....                             | 193 |
| Figure 78: Enabled Cipher Suites .....                                       | 196 |
| Figure 79: Service Resolution Settings dialog .....                          | 197 |
| Figure 80: Manage Email Listeners dialog .....                               | 200 |
| Figure 81: SFTP Polling Listener Properties - [Connection] tab .....         | 201 |
| Figure 82: SFTP Polling Listener Properties - [Message Processing] tab ..... | 203 |
| Figure 83: SFTP Polling Listener Properties - [Advanced] tab .....           | 205 |
| Figure 84: Manage Keystore dialog .....                                      | 209 |
| Figure 85: Preferences dialog (desktop client) .....                         | 211 |
| Figure 86: Sample policy for dynamic routing .....                           | 215 |
| Figure 87: Basic user authentication using SiteMinder .....                  | 217 |
| Figure 88: Basic authentication via HTTP cookie using SiteMinder .....       | 218 |
| Figure 89: Advanced SiteMinder authorization policy example .....            | 219 |
| Figure 90: Manage SiteMinder Configurations dialog .....                     | 221 |
| Figure 91: SiteMinder Configuration Properties dialog .....                  | 223 |
| Figure 92: SiteMinder Registration Properties dialog .....                   | 224 |
| Figure 93: Configuring encryption settings - General .....                   | 235 |
| Figure 94: Configuring encryption settings - Advanced .....                  | 235 |
| Figure 95: Manage Certificates dialog .....                                  | 238 |
| Figure 96: Add Certificate Wizard - Step 1 .....                             | 240 |
| Figure 97: Add Certificate Wizard - Step 2 .....                             | 242 |
| Figure 98: Add Certificate Wizard - Step 3 .....                             | 243 |
| Figure 99: Add Certificate Wizard - Step 4 .....                             | 245 |
| Figure 100: Certificate Properties .....                                     | 246 |
| Figure 101: Import Certificates dialog .....                                 | 249 |
| Figure 102: Configure Recipient Certificate wizard .....                     | 250 |
| Figure 103: Manage Certificate Validation dialog .....                       | 253 |
| Figure 104: Edit Revocation Checking Policy dialog .....                     | 255 |
| Figure 105: Edit Certificate Revocation Checking Properties dialog .....     | 257 |
| Figure 106: Search Trusted Certificates dialog .....                         | 259 |
| Figure 107: Manage Private Keys dialog .....                                 | 261 |

|   |     |
|---|-----|
| Figure 108: Create Private Key dialog - [Basic] tab .....   | 263 |
| Figure 109: Create Private Key dialog - [Advanced] tab .....  | 264 |
| Figure 110: Special private key deletion confirmation .....   | 267 |
| Figure 111: Signing Certificate Properties .....  | 269 |
| Figure 112: Private Key Properties .....  | 271 |
| Figure 113: Private Key Alias dialog .....  | 276 |
| Figure 114: Search Identity Provider dialog, with sample search results .....                         | 281 |
| Figure 115: Creating a template user .....  | 283 |
| Figure 116: Adding or changing an identity tag .....  | 285 |
| Figure 117: Create Internal User dialog .....   | 287 |
| Figure 118: Create Internal Group dialog .....  | 295 |
| Figure 119: Internal Identity Provider Wizard .....   | 301 |
| Figure 120: Administrative User Account Properties .....  | 302 |
| Figure 121: LDAP Identity Provider Wizard - Step 1 .....  | 307 |
| Figure 122: LDAP Identity Provider Wizard - Step 2 .....  | 309 |
| Figure 123: LDAP Identity Provider Wizard - Step 3 .....  | 310 |
| Figure 124: LDAP Identity Provider Wizard - Step 4 .....  | 312 |
| Figure 125: LDAP Identity Provider Wizard - Step 5 .....  | 314 |
| Figure 126: LDAP Identity Provider Wizard - Step 6 .....  | 315 |
| Figure 127: Simple LDAP Identity Provider Wizard .....  | 319 |
| Figure 128: Policy-Backed Identity Provider wizard .....  | 328 |
| Figure 129: Publish SOAP Web Service Wizard .....   | 333 |
| Figure 130: Create WSDL Wizard, Step 1 .....  | 338 |
| Figure 131: Create WSDL Wizard, Step 2 .....  | 339 |
| Figure 132: Create WSDL Wizard, Step 3 .....  | 340 |
| Figure 133: Create WSDL Wizard, Step 4 .....  | 342 |
| Figure 134: Create WSDL Wizard, Step 5 .....  | 343 |
| Figure 135: Create WSDL Wizard, Step 6 .....  | 344 |
| Figure 136: Create WSDL Wizard, Step 7 .....  | 345 |
| Figure 137: Publish Web API Wizard .....  | 347 |
| Figure 138: Publish REST Service Proxy Wizard - Step 1 .....  | 353 |
| Figure 139: Publish REST Service Proxy Wizard - Step 2 (manual entry) .....                           | 354 |
| Figure 140: Publish REST Service Proxy Wizard - Step 2 (load from WADL) .....                         | 354 |
| Figure 141: Publish REST Service Proxy Wizard - Step 3 .....  | 355 |
| Figure 142: Published Service Properties - [General] tab .....  | 358 |
| Figure 143: Published Service Properties - [HTTP/FTP] tab .....                                       | 360 |
| Figure 144: Published Service Properties - [WSDL] tab .....   | 362 |
| Figure 145: Published Service Properties - [UDDI] tab .....   | 364 |
| Figure 146: Publish Internal Service Wizard .....   | 376 |
| Figure 147: Sample Message dialog .....   | 387 |
| Figure 148: Configuring a listen port to proxy multiple web applications - [Basic Settings] tab ..... | 394 |
| Figure 149: Configuring a listen port to proxy multiple web applications - [Advanced] tab .....       | 395 |
| Figure 150: Publish Reverse Web Proxy Wizard - Step 1 .....   | 397 |
| Figure 151: Publish Reverse Web Proxy Wizard - Step 2 .....   | 399 |
| Figure 152: Dashboard - Service Metrics .....   | 402 |
| Figure 153: Dashboard - Cluster Status .....  | 407 |
| Figure 154: Select Log dialog .....   | 410 |
| Figure 155: Log Viewer dialog .....   | 411 |
| Figure 156: FTP(S) Audit Archiver Properties dialog .....   | 414 |
| Figure 157: Gateway Audit Events window .....   | 416 |
| Figure 158: An Identity Bridging Configuration Using a SAML Token .....                               | 430 |
| Figure 159: An Identity Bridging Configuration Using an X.509 Certificate .....                       | 431 |
| Figure 160: How the Gateway determines when to verify hostnames .....                                 | 435 |
| Figure 161: Create Federated Identity Provider Wizard - Step 1 .....                                  | 442 |

|  |     |
|--|-----|
| Figure 162: Create Federated Identity Provider Wizard - Step 2 .....                   | 443 |
| Figure 163: Create Federated Identity Provider Wizard - Step 3 .....                   | 444 |
| Figure 164: Create Federated User dialog .....   | 447 |
| Figure 165: Create Federated Group dialog .....  | 451 |
| Figure 166: Create Virtual Group dialog .....  | 453 |
| Figure 167: Search Identity Provider dialog, with sample search results .....          | 460 |
| Figure 168: Creating a template user .....   | 462 |
| Figure 169: Sample hosts file in Windows .....   | 470 |
| Figure 170: New soapUI Project with sample ACME Warehouse .....                        | 472 |
| Figure 171: Sample ACME Warehouse project .....  | 472 |
| Figure 172: Opening the Request window .....   | 472 |
| Figure 173: Sending a request .....  | 473 |
| Figure 174: Receiving the expected response .....                                      | 473 |
| Figure 175: The Policy Manager main interface .....                                    | 476 |
| Figure 176: Publish SOAP Web Service Wizard - step 1 .....                             | 477 |
| Figure 177: Publish SOAP Web Service Wizard - step 2 .....                             | 477 |
| Figure 178: Newly published SOAP Web service .....                                     | 478 |
| Figure 179: Adding a new endpoint in soapUI .....                                      | 479 |
| Figure 180: Add new endpoint dialog .....  | 479 |
| Figure 181: Expected response after routing request through Gateway .....              | 480 |
| Figure 182: The [Identity Providers] tab .....   | 481 |
| Figure 183: Create Internal User dialog .....  | 482 |
| Figure 184: Create Internal Group dialog .....   | 483 |
| Figure 185: Search Identity Provider dialog .....                                      | 484 |
| Figure 186: Authenticating any user in the IIP .....                                   | 485 |
| Figure 187: Authenticating a specific user in the IIP .....                            | 485 |
| Figure 188: Authenticating multiple users in the IIP .....                             | 485 |
| Figure 189: Create LDAP Identity Provider Wizard - Step 1 .....                        | 487 |
| Figure 190: LDAP test success .....  | 487 |
| Figure 191: Create LDAP Identity Provider Wizard - Step 4 .....                        | 488 |
| Figure 192: New LDAP identity provider added to the Policy Manager .....               | 488 |
| Figure 193: Accessing the Require SSL or TLS Transport assertion .....                 | 491 |
| Figure 194: Positioning the Require SSL or TLS Transport assertion in the policy ..... | 491 |
| Figure 195: SOAP Fault caused by missing SSL in message .....                          | 492 |
| Figure 196: Creating an HTTPS endpoint in soapUI .....                                 | 492 |
| Figure 197: Policy updated with HTTP Basic Authentication .....                        | 493 |
| Figure 198: Entering credentials of authenticated user in soapUI .....                 | 494 |
| Figure 199: The expected response is displayed after credentials are entered .....     | 494 |
| Figure 200: Simple policy example .....  | 497 |
| Figure 201: Assertions palette in the Policy Manager .....                             | 498 |
| Figure 202: Folder assertions policy example .....                                     | 499 |
| Figure 203: Manage Salesforce Operation Service Connections dialog .....               | 503 |
| Figure 204: Salesforce Operation Service Connection Properties dialog box .....        | 505 |

## List of Tables

|  |    |
|--|----|
| Table 1: Login dialog .....                              | 9  |
| Table 2: Managing client certificates .....              | 10 |
| Table 3: Policy Manager browser client differences ..... | 11 |
| Table 4: Using a wizard .....                            | 14 |
| Table 5: Audit Alert options .....                       | 29 |

|  |     |
|--|-----|
| Table 6: Using the Policy Search Bar .....   | 31  |
| Table 7: Manage Gateway License tasks .....  | 37  |
| Table 8: Editing cluster-wide properties .....                                     | 41  |
| Table 9: Manage Stored Passwords tasks .....                                       | 43  |
| Table 10: Changing a password .....  | 45  |
| Table 11: Stored password settings .....   | 47  |
| Table 12: Managing password policy .....   | 50  |
| Table 13: Listen Ports columns .....   | 55  |
| Table 14: Manage Listen Ports tasks .....  | 56  |
| Table 15: Listen Port Basic Settings .....   | 59  |
| Table 16: Listen Port SSL/TLS Settings .....                                       | 62  |
| Table 17: Listen Port Pool Settings .....  | 64  |
| Table 18: Listen Port FTP Settings .....   | 65  |
| Table 19: Commands that can be proxied in the extended FTP command set .....       | 66  |
| Table 20: Accepted FTP commands that are not processed as messages .....           | 67  |
| Table 21: Unsupported FTP commands .....   | 68  |
| Table 22: Listen Port - Other Settings .....                                       | 72  |
| Table 23: Listen Port - Advanced Settings .....                                    | 74  |
| Table 24: Manage Interfaces tasks .....  | 77  |
| Table 25: Manage Firewall columns .....  | 79  |
| Table 26: Manage Listen Ports tasks .....  | 80  |
| Table 27: Simple Firewall Rule settings .....                                      | 81  |
| Table 29: Managing JDBC connections tasks .....                                    | 83  |
| Table 30: JDBC driver classes .....  | 84  |
| Table 31: JDBC connection settings .....   | 87  |
| Table 32: Context variables created when the Gateway receives a JMS message .....  | 91  |
| Table 33: Working with JMS Destinations .....                                      | 94  |
| Table 34: JMS Destination Properties - [JNDI] tab .....                            | 99  |
| Table 35: JMS Destination Properties - [Destination] tab .....                     | 102 |
| Table 36: JMS Destination Properties - [Inbound Options] tab .....                 | 105 |
| Table 37: JMS Destination Properties - [Outbound Options] tab .....                | 108 |
| Table 38: Working with MQ Native Queues .....                                      | 112 |
| Table 39: MQ Native Queue Properties - [MQ Connection Properties] tab .....        | 115 |
| Table 40: MQ Native Queue Properties - [Inbound Options] tab .....                 | 118 |
| Table 41: MQ Native Queue Properties - [Outbound Options] tab .....                | 121 |
| Table 42: Customize message descriptors settings .....                             | 124 |
| Table 43: Managing email listener tasks .....                                      | 126 |
| Table 44: Email listener settings .....  | 128 |
| Table 45: Manage Roles dialog .....  | 131 |
| Table 46: Predefined roles and permissions .....                                   | 132 |
| Table 47: Columns in the Permissions table .....                                   | 139 |
| Table 48: Add Permissions to Role Wizard - Step 2 (specifying by conditions) ..... | 145 |
| Table 49: Create Role settings .....   | 149 |
| Table 50: Manage Security Zones tasks .....  | 155 |
| Table 51: Security zone tasks .....  | 158 |
| Table 52: Security zone settings .....   | 160 |
| Table 53: Manage Log Sinks tasks .....   | 164 |
| Table 54: Log/audit severity levels .....  | 166 |
| Table 55: Log Sink Properties - [Base Settings] tab .....                          | 168 |
| Table 56: Log Sink Properties - Filter types .....                                 | 169 |
| Table 57: Log Sink Properties - [File Settings] tab .....                          | 171 |
| Table 58: Log Sink Properties - [Syslog Settings] tab .....                        | 173 |
| Table 59: Using the Configure External Audit Store Wizard .....                    | 177 |
| Table 60: HTTP Options - [General] tab .....                                       | 191 |

|  |     |
|--|-----|
| Table 61: Service Resolution settings .....                                | 197 |
| Table 62: Managing SFTP polling listener tasks .....                       | 200 |
| Table 63: SFTP Polling Listening settings - [Connection] tab .....         | 202 |
| Table 64: SFTP Polling Listening settings - [Message Processing] tab ..... | 203 |
| Table 65: SFTP Polling Listening settings - [Advanced] tab .....           | 205 |
| Table 66: Information about your keystore .....                            | 209 |
| Table 67: Preferences settings .....                                       | 211 |
| Table 68: Manage SiteMinder Configuration columns .....                    | 221 |
| Table 69: Manage SiteMinder Configurations tasks .....                     | 221 |
| Table 70: SiteMinder Registration settings .....                           | 224 |
| Table 71: SiteMinder Configuration settings .....                          | 225 |
| Table 72: Configuring encryption settings .....                            | 236 |
| Table 73: Manage Certificates tasks .....                                  | 238 |
| Table 74: Certificate Properties tabs .....                                | 246 |
| Table 75: Managing certificate validation .....                            | 253 |
| Table 76: Revocation Checking Policy settings .....                        | 255 |
| Table 77: Certificate Revocation Checking settings .....                   | 258 |
| Table 78: Search Trusted Certificates settings .....                       | 260 |
| Table 79: Manage private keys tasks .....                                  | 262 |
| Table 80: Basic private key properties .....                               | 263 |
| Table 81: Signing Certificate Properties .....                             | 269 |
| Table 82: Private key properties settings .....                            | 271 |
| Table 83: Private key locations .....                                      | 274 |
| Table 84: Private Key Alias dialog .....                                   | 276 |
| Table 85: Search Identity Provider settings .....                          | 281 |
| Table 86: Internal user basic properties .....                             | 287 |
| Table 87: User Properties - [General] tab .....                            | 289 |
| Table 88: Editing a User or Group actions .....                            | 299 |
| Table 89: Administrative user account settings .....                       | 302 |
| Table 90: Member Strategies .....  | 317 |
| Table 91: Troubleshooting LDAP configuration problems .....                | 318 |
| Table 92: Configuring the Simple LDAP Identity Provider Wizard .....       | 319 |
| Table 93: Troubleshooting Simple LDAP configuration problems .....         | 320 |
| Table 94: Policy-Backed Identity Provider settings .....                   | 328 |
| Table 95: SOAP web service tasks .....                                     | 332 |
| Table 96: Publish Web API Wizard settings .....                            | 347 |
| Table 97: Steps to secure a RESTful web service .....                      | 350 |
| Table 98: Service Properties - [General] tab .....                         | 358 |
| Table 99: Service Properties - [HTTP/FTP] tab .....                        | 360 |
| Table 100: Service Properties - [WSDL] tab .....                           | 362 |
| Table 101: Service Properties - [UDDI] tab .....                           | 365 |
| Table 102: Internal service tasks .....                                    | 375 |
| Table 103: Using the Publish Internal Service Wizard .....                 | 376 |
| Table 104: Security Token Service default policy .....                     | 378 |
| Table 105: Action URLs for request type 'issue SAML token' .....           | 382 |
| Table 106: Action URLs for request type 'issue SCT' .....                  | 382 |
| Table 107: Actions URLs for request type 'cancel token' .....              | 382 |
| Table 108: Parameters for GIMS user authentication .....                   | 383 |
| Table 109: Attributes for returned authentication information .....        | 384 |
| Table 110: Error cases for GIMS .....                                      | 385 |
| Table 111: Configuring a sample message .....                              | 387 |
| Table 112: Reverse proxy service tasks .....                               | 392 |
| Table 113: Dashboard - Service Metrics mouse actions .....                 | 403 |
| Table 114: Gateway Status table .....                                      | 407 |



|  |     |
|--|-----|
| Table 115: Node operations .....   | 408 |
| Table 116: Cluster Status Service Statistics .....   | 409 |
| Table 117: Log Viewer settings .....   | 411 |
| Table 118: FTP(S) Audit Archiver settings .....  | 414 |
| Table 119: Gateway Audit Events: Time Range .....  | 418 |
| Table 120: Gateway Audit Events - Search Parameters .....  | 418 |
| Table 121: Gateway Audit Events - Audit events .....   | 421 |
| Table 122: Gateway Audit Events - Event details .....  | 422 |
| Table 123: Verifying hostnames flowchart explanation .....   | 435 |
| Table 124: Identity Bridging workflow using SAML .....   | 436 |
| Table 125: Identity Bridging workflow using an X.509 .....   | 437 |
| Table 126: Federated user basic properties .....   | 447 |
| Table 127: Federated group additional properties .....   | 452 |
| Table 128: Federated Virtual Group properties .....  | 453 |
| Table 129: Editing a User or Group actions .....   | 458 |
| Table 130: Search Identity Provider settings .....   | 460 |
| Table 131: Configuring the SAML Token Profile Wizard for identity .....  | 463 |
| Table 132: Adding a shared federated user .....  | 465 |
| Table 133: Location of Hosts file .....  | 468 |
| Table 134: LDAP Provider Configuration for Demo Environment .....  | 486 |
| Table 135: Managing Salesforce connections tasks .....   | 504 |
| Table 136: Salesforce connection settings .....  | 505 |
| Table 137: Features available in each version of the Gateway .....   | 509 |
| Table 138: Context variable validation messages .....  | 520 |
| Table 139: General context variables .....   | 522 |
| Table 140: Context variables for auditing .....  | 524 |
| Table 141: Context variables used to reconstruct audits from an audit lookup policy .....                          | 525 |
| Table 142: Context variables used to retrieve an entire audit record .....   | 526 |
| Table 143: Context variables used for searching audits .....   | 527 |
| Table 144: Context variables for audit sink policy .....   | 528 |
| Table 145: Context variables for message audit records in an audit sink policy .....                               | 529 |
| Table 146: Context variables for authentication .....  | 531 |
| Table 147: Context variables for certificate attributes .....  | 534 |
| Table 148: Context variables for Subject/Issuer DN attributes .....  | 536 |
| Table 149: Context variables for credential certificates .....   | 537 |
| Table 150: Built-in context variables for date and time .....  | 539 |
| Table 151: Suffixes for date and time variables .....  | 539 |
| Table 152: Context variables for Kerberos Ticket Authorization Info .....  | 540 |
| Table 153: Context variables for message layer .....   | 544 |
| Table 154: Context variables for message routing .....   | 547 |
| Table 155: Variables for services and policies .....   | 549 |
| Table 156: Variables for the system .....  | 550 |
| Table 157: Context variables for transport layer .....   | 550 |
| Table 158: Context variables in XPath expressions .....  | 561 |
| Table 159: Context variables for CA SiteMinder .....   | 562 |
| Table 160: SiteMinder attributes .....   | 564 |
| Table 161: Context variables created by the Authenticate with SiteMinder R12 Protected Resource<br>assertion ..... | 565 |
| Table 162: Gateway Cluster Properties - Time .....   | 567 |
| Table 163: Gateway Cluster Properties - Password .....   | 567 |
| Table 164: Gateway Cluster Properties - Audit Archiver .....   | 568 |
| Table 165: Gateway Cluster Properties - Audit settings .....   | 569 |
| Table 166: Gateway Cluster Properties - Certificate Validation .....   | 574 |
| Table 167: Gateway Cluster Properties - Credential Caching .....   | 577 |

|   |     |
|---|-----|
| Table 168: Gateway Cluster Properties - Email .....                         | 580 |
| Table 169: Gateway Cluster Properties - ESM .....                           | 580 |
| Table 170: Gateway Cluster Properties - Fault level .....                   | 581 |
| Table 171: Gateway Cluster Properties - FTP .....                           | 582 |
| Table 172: Gateway Cluster Properties - Global .....                        | 583 |
| Table 173: Gateway Cluster Properties - I/O .....                           | 584 |
| Table 174: Gateway Cluster Properties - JDBC .....                          | 595 |
| Table 175: Gateway Cluster Properties - Kerberos .....                      | 597 |
| Table 176: Gateway Cluster Properties - LDAP .....                          | 598 |
| Table 177: Gateway Cluster Properties - Message validation .....            | 599 |
| Table 178: Gateway Cluster Properties - Rate Limit .....                    | 602 |
| Table 179: Gateway Cluster Properties - Miscellaneous .....                 | 602 |
| Table 180: Gateway Cluster Properties - Services .....                      | 603 |
| Table 181: Gateway Cluster Properties - Traffic logger .....                | 605 |
| Table 182: Gateway Cluster Properties - UDDI .....                          | 606 |
| Table 183: Gateway Cluster Properties - WS-Security .....                   | 607 |
| Table 184: Gateway Cluster Properties - XML Security .....                  | 610 |
| Table 185: Gateway Cluster Properties - Miscellaneous .....                 | 613 |
| Table 186: Assertion status codes .....                                     | 625 |
| Table 187: Audit message groupings .....                                    | 627 |
| Table 188: Audit message codes .....  | 627 |
| Table 189: Cluster properties to customize audit format .....               | 651 |
| Table 190: Validity of variables for audit format cluster properties .....  | 652 |
| Table 191: Recognized key usage actions .....                               | 653 |
| Table 192: Actional Integration cluster properties .....                    | 658 |
| Table 193: CA SiteMinder authentication/authorization failure reasons ..... | 665 |

# Chapter 1: Getting Started

Welcome to CA Technologies' Policy Manager version 8.2. This manual provides extensive information and user instructions for the Policy Manager, including:

- Instructions for [connecting](#) to one or more Gateways
- Instructions for [installing](#) and [viewing](#) a Gateway license
- Instructions for setting up [identity providers](#) and for configuring users and groups
- Instructions for publishing and managing SOAP Web [services](#) and XML (non-SOAP) applications
- Policy assertion and policy configuration information and instructions
- Instructions for monitoring and [analyzing Gateway performance](#)
- Instructions for configuring [identity bridging](#) in the Policy Manager and Securespan XML VPN Client
- [Technical support](#) contact information.

For information about the new features and changes in this version, please refer to the Release Notes that accompany this release.

---

**Note:** Depending on which version of the Gateway you have installed, not all features described in this manual may be available. See "Appendix B: Features by Product" on page 509 for a list of which features are available for each product.

---

## Overview

The CA API Gateway product line is composed of three interoperable products—the Gateway, the Securespan XML VPN Client, and the Policy Manager—that protect applications exposed as web services, connect applications across security and identity domains, and validate policy compliance end-to-end across a transaction.

## Supported Standards

Please refer to [www.layer7tech.com](http://www.layer7tech.com) for a list of the standards supported by the CA API Gateway product suite.

Additional supported standards and tool kits are referenced with their applicable feature or function.

---

**Internationalization Note:** The Policy Manager and the Gateway supports a variety of encoding, including single and multi-byte characters. However note that certain industry standards may have specific encoding requirements (for example, the HTTP specifications require that HTML headers and values be restricted to the ISO-8859-1 character set). Field lengths specified in this documentation apply equally to single and multi-byte character sets (for example, a field with a maximum length of 32 characters can accept 32 English or Korean characters.)

---

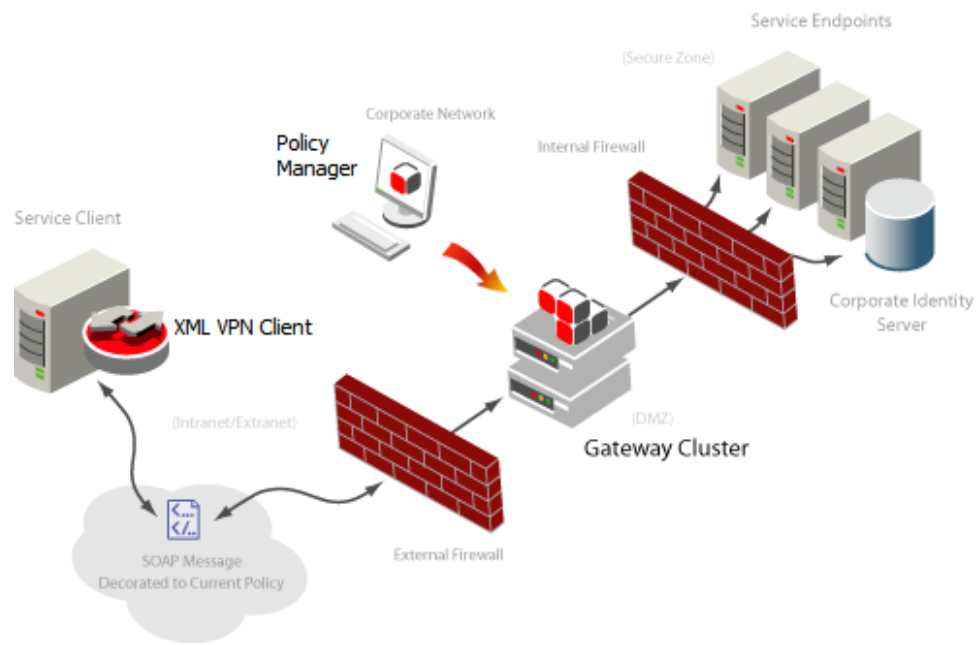


Figure 1: CA API Gateway Deployment Architecture

## CA API Gateway

The CA API Gateway is a policy-optimized and ASIC-accelerated XML Firewall and Web services Gateway that protects and controls how shared web services are accessed by and exposed to external applications. In accordance with customer needs, the Gateway is delivered in one of the following form factors:

- As a software package running on general application servers or corporate-mandated hardware
- As an ASIC-accelerated DMZ appliance, or
- As a 64-bit ASIC-accelerated appliance for EAI or ESB implementations.

As the administrative application for the Gateway, the Policy Manager documentation contains in-depth information for almost all Gateway features and functions. Gateway procedures not performed through the Policy Manager are described in the *Layer 7 Installation and Maintenance Manual*. These procedures include: installing, configuring, troubleshooting, and maintaining the Gateway.

Instructions for installing and configuring the custom assertion on the Gateway are provided in the *CA API Gateway Custom Assertion Installation Manual*.

In this Help System, the term "Gateway" includes all of the Gateway products. For information about the features available in each Gateway product, see "Appendix B: Features by Product" on page 509.

For information about monitoring and auditing the Gateway from the Policy Manager, see "Chapter 6: Analyzing Gateway Performance" on page 401.

## **CA API Gateway - Policy Manager**

The Policy Manager is a GUI-based application that allows administrators to centrally define, provision, verify, and audit fine-grained security and connectivity policies for cross-domain web services and XML integrations. The Policy Manager is available as software for Red Hat Enterprise Linux, Sun Microsystems Solaris, and Microsoft Windows operating systems. It is also available through a SOAP API. The Policy Manager is available as either a standard desktop client or a browser-based client running on a compliant Web browser.

The Policy Manager documentation includes installation instructions in the *Layer 7 Installation and Maintenance Manual*, user instructions in a program-based Help System and an electronic (PDF) User Manual based on the Help System content.

## **Securespan XML VPN Client**

The Securespan XML VPN Client is a cross-domain enablement product designed to speed and secure web services integrations spanning identity and security domains. The Securespan XML VPN Client is available in three form factors:

- As class libraries
- As a software executable
- Integrated inside a Gateway for drop-in partner connectivity and web services federation.

The Securespan XML VPN Client documentation includes installation instructions in the *Layer 7 Installation and Maintenance Manual*, user instructions in a program-based Help System, and an electronic (PDF) User Manual based on the Help System content.

## Chapter 2: The Policy Manager

The Policy Manager is the user interface for the CA API Gateway. Located on the internal local area network, the Policy Manager communicates with the Gateway over default ports. Use the Policy Manager to construct web service and XML application policies, manage policy users, configure identity bridging, and configure, audit, and monitor the Gateway.

The Policy Manager offers two different operating modes:

- Normal GUI for all configuration and management tasks
- [Troubleshooting Mode](#) for Network Administrators to gather additional information about system errors (available in Windows version only).

For information on the general Policy Manager workflow, see "General Workflow" on page 36.

---

**Note:** Depending on which Gateway product you have installed, not all features described in this help system may be available. See "Appendix B: Features by Product" on page 509 for a list of which features are available for each product.

---

### Starting the Policy Manager

There are two ways to start the Policy Manager:

- **Desktop client:** The standard desktop client provides maximum functionality and best performance, but it requires the Policy Manager application to be installed on the client computer. For more information, see the Layer 7 Policy Manager User Manual, v8.2.
- **Browser client:** The browser-based client provides the greatest flexibility—you can run the Policy Manager from virtually any computer with an Internet connection and a compatible web browser with a Java Runtime Environment (JRE) installed. However, not all features are available.

For more information, see "Policy Manager Browser Client" on page 11.

### Running the Desktop Client

Do the following to start the Policy Manager as a standard client:

- *Linux*: Navigate to the directory where the Policy Manager is installed and then either run **./Manager.sh** or double click the **.sh** icon.
- *Windows*: Click **[Start] > All Programs > Layer 7 Policy Manager > Layer 7 Policy Manager**

Once the Policy Manager is started, you can connect to the Gateway. For more information, see "Connecting to the Gateway" on page 8.

## Running the Browser Client

---

**Note:** Browser client access can be disabled by clearing the **Enable web-based administration** check box in the [Listen Port Properties](#) ([Endpoints] tab) for the SSL endpoint.

---

### *Prerequisites:*

- For a list of the supported browsers and Java environment, see the *Readme.txt* file which accompanies the Policy Manager (**Note:** Other browsers may work but their performance is not guaranteed by CA Technologies.)
- Browser should have any JavaScript blockers disabled
- Operator running the browser client must have least one assigned [role](#) in the Policy Manager

### ➤ *To run the Policy Manager from a browser:*

1. Start the browser and type the following URL in the address bar:

**`https://<gatewayHostName>:9443/ssg/webadmin`**

2. When presented with security or authentication prompts, accept the certificates after verifying the certificate information and thumbprint in accordance with your organization's security policy. Note that the Java plugin must be running the applet in "trusted" mode for the browser client to perform operations that require access to your local drives.

### **Special note for Internet Explorer users**

The security built into Internet Explorer may require special handling to eliminate warning messages if your Gateway's SSL certificate is not signed by a certificate authority that your browser is configured to trust.

1. You will see a browser tab with the words: **There is a problem with this website's security certificate**. Disregard the warning and click **[Continue to this website]**. You are then prompted to log into the Gateway.



2. Enter your **User name** and **Password**, just as if you were logging into the Policy Manager standard client.
3. Next to the address bar, there will be a [**Certificate Error**] button. Click this button and then select **View Certificates**.
4. Click [**Install Certificate**]. The *Certificate Import Wizard* appears.
5. Click [**Next**] to proceed to the **Certificate Store** step of the wizard.
6. Select **Automatically select the certificate store based on the type of certificate** and then click [**Next**]. The successful completion screen should now appear.
7. Click [**Finish**]. A confirmation dialog tells you that the SSL certificate was imported successfully.
8. Click [**OK**] to dismiss the confirmation.
9. Next, import the CA root certificate by selecting the [**Certification Path**] tab on the Certificates dialog.
10. Select the root certificate on the tree of the Certificate Path and then click [**View Certificate**]. The certificate information is displayed.
11. Click [**Install Certificate**] and run the *Certificate Import Wizard*. At the security warning, carefully verify the certificate according to your organization's security policies. Contact your network administrator if unsure.
12. If the certificate is satisfactory, click [**Yes**] to proceed with the installation.
13. Click [**OK**] to dismiss the Certificate dialog. (**Note:** The browser will continue to display [**Certificate Error**] until it is restarted, at which point it becomes a padlock icon. To confirm that the certificates are correctly installed: click the error button, select [**View certificates**], and then select the [Certificate Path] tab. The certificate status should show: "*This certificate is OK.*").

#### Special note for Firefox users

The security built into Firefox may require special handling to eliminate warning messages if your Gateway's SSL certificate is not signed by a certificate authority that your browser is configured to trust.

- a. You will see a browser tab with the words: **Secure Connection Failed**. Disregard the warning and click "**Or you can add an exception...**" at the

bottom. Two new buttons will appear.

- b. Click the button labelled **Add Exception...** The Add Security Exception dialog appears.
  - c. Verify that the Gateway URL is correct and then click **Get Certificate**.
  - d. Select the **Permanently store this exception** check box and then click **Confirm Security Exception**. The Policy Manager login screen appears.
3. Enter your **User name** and **Password** when prompted, then click **[Login]**.

Once the connection to the Gateway is established, the Policy Manager checks your user permissions as defined by your [role](#), and then enables the appropriate features within the system.

---

**Note:** If you encounter any problems relating to field focus in the browser client (in other words, you cannot get the cursor to enter a text field), disable any third party tool bars that may be installed in your browser. Note that some browsers require a mouse click to switch focus to the browser applet first, before subsequent mouse clicks are interpreted by the Policy Manager.

---

## Connecting to the Gateway

*This topic applies only to the desktop client version of the Policy Manager. In the browser client version, you are connected to the Gateway when Policy Manager interface appears.*

Each time you [start](#) the Policy Manager, the **Login** dialog automatically appears. Use this dialog to:

- Connect to an existing Gateway or cluster by selecting its URL from the drop-down list on the Login dialog, or
- Connect to a new Gateway or cluster by typing its URL in the Login dialog.

You can also display the Login dialog from within the Policy Manager by doing either of the following:

- Click **[Connect]** on the [Main Tool Bar](#) (if currently connected, you must first **Disconnect** before connecting to a different Gateway)
- Select **[File] > Connect** from the [Main Menu](#)

Once the connection to the Gateway is established, the Policy Manager checks your user permissions as defined by your [role](#), and then enables the appropriate features within the system.

**Tip:** CA recommends using separate account for administrative access (i.e., connecting to the Gateway) and for message processing (i.e., adding a user to a service policy). To simplify using separate user accounts, you may consider using different identity providers for administration/message traffic. For more information, see [Identity Providers](#) in the *Layer 7 Policy Manager User Manual*.



The image shows a 'Login' dialog box titled 'Connecting to the Gateway'. It has a blue title bar with a close button. The dialog contains two radio buttons: 'User Name / Password' (selected) and 'Client certificate'. Under 'User Name / Password', there are text boxes for 'User Name' (containing 'admin') and 'Password' (masked with dots). Under 'Client certificate', there is a 'Certificate' dropdown menu and a 'Manage' button. At the bottom, there is a 'Gateway' dropdown menu showing 'ssg.acmecorp.com'. 'OK' and 'Cancel' buttons are at the bottom right.

Figure 2: Login dialog

Complete the login dialog as follows:

Table 1: Login dialog

| Option                    | Description   |
|---------------------------|---|
| <b>User Name/Password</b> | To log in using a password, enter your <b>User Name</b> and <b>Password</b> . Your account may be configured to <a href="#">remember</a> your user name.<br><b>Note:</b> For security, the administrative user account will be locked for 20 minutes after five unsuccessful login attempts. No further login attempts may be made during the lockout period. The settings can be changed using the <a href="#">Manage Administrative User Account Policy</a> dialog. |
| <b>Client certificate</b> | To log in using a client certificate, select from the <b>Certificate</b> drop-down list. To add or remove certificates from the list, click <b>Manage</b> and choose a task from Table 2.<br><b>Notes:</b> (1) Users with client certificates are required to use their certificates during login. (2) The 'CN' value in the certificate must match the username.   |
| <b>Gateway</b>            | Select the Gateway to connect to from the drop-down list. If the correct Gateway is not listed, type the URL in the <b>Gateway</b> field, in the format <i>machinename.domain.com</i> . The URL is saved to the list.   |

| Option | Description   |
|--------|---|
|        | <p>After connecting to a new Gateway, you will need to <a href="#">install the license file</a>.</p> <p><b>Connecting to a non-default port</b></p> <p>To connect to a port other than the default 8443, you must append the SSL Endpoint port number to the Gateway name; for example: <i>mygateway.domain.com:8445</i>. Contact your system administrator if you are unsure of the port number to use.</p> <p><b>IPv6 Support</b></p> <p>The Gateway field supports IPv6 literals for the Gateway host. The following formats are supported:</p> <p style="text-align: center;">[2222::7]<br/>[2222::7]:8443</p> <p>Note that IPv6 literals must be enclosed within square brackets ("[]") to be interpreted correctly.</p> |

To edit the list of client certificates:

Table 2: Managing client certificates

| To...  | Do this...   |
|--|--|
| <b>Add a client certificate to the list</b>      | <ol style="list-style-type: none"> <li>1. Click <b>Manage</b> under the Client Certificate option. The Certificate Manager dialog appears.</li> <li>2. Click <b>Import</b> and then navigate to the PKCS#12 keystore to load.</li> <li>3. Enter the <b>Keystore Password</b> when prompted. The details of the selected certificate are displayed.</li> <li>4. Verify that the details are correct and then click <b>[OK]</b>. The imported certificate is added to the list.</li> </ol>                                 |
| <b>Remove a client certificate from the list</b> | <ol style="list-style-type: none"> <li>1. Click <b>Manage</b> under the Client Certificate option. The Certificate Manager dialog appears.</li> <li>2. Select the certificate to be deleted from the <b>Certificate List</b>. The details of the certificate are displayed.</li> <li>3. Click <b>Delete</b> and then click <b>Yes</b> to confirm. The certificate is removed from the <b>Certificate List</b>.</li> <li>4. Click <b>[OK]</b> to close the Certificate Manager and return to the Login dialog.</li> </ol> |

## Policy Manager Browser Client

The browser client version of the Policy Manager allows you to manage the Gateway using a standard web browser.

The browser client version is very similar to the standard client in both functionality and look and feel. Table 3 summarizes the differences between the two versions.

---

**Tips:** (1) Browser client access can be disabled by clearing the **Enable web-based administration** check box in the [Listen Port Properties](#) (Endpoints tab) for the SSL endpoint. (2) If you experience problems starting the browser client, access the Java Control Panel for your operating system, clear the temporary Java files, and then try starting the browser client again.

---

### Trusted Mode

Note that the Java applet in the Policy Manager browser client must be in *trusted mode* to run certain features. Trusted mode is enabled if you had answered **[Yes]** to the browser and Java plug-in security dialogs on first use of the browser client version of the Policy Manager.

For more information on running the browser client, see "Starting the Policy Manager" on page 5.

Table 3: Policy Manager browser client differences

| Feature   | Browser client difference   |
|---|---|
| <b>Main Menu</b>  | Instead of a Main Menu, the browser client has an enhanced <a href="#">Main Tool Bar</a> .  |
| <b>[File] &gt; Exit</b>   | The Exit command has been removed. To exit the browser client, first click <a href="#">[Save]</a> and then either click <a href="#">[Disconnect]</a> or close the browser.                |
| <b>[File] &gt; Preferences</b><br><b>Main Tool Bar &gt; Preferences</b> | <a href="#">Preferences</a> in the browser client do not include the following settings:<br><i>Inactivity Timeout</i><br><i>Remember Last Login ID</i><br><i>Gateway URL History Size</i> |
| <b>[View] &gt; Status Bar</b>   | The <a href="#">Status Bar</a> is not included in the browser client.   |
| <b>Policy Templates</b>   | There is no Policy Templates category in the <a href="#">[Assertion] tab</a> , but you can still import and export template files.  |
| <b>Exporting/Importing Policies</b>                                     | Exporting a policy to a file or importing a policy from a file is supported in the browser client only if the Java applet is running in the trusted mode.                                 |
| <b>UDDI Registry</b>  | Importing a policy from a UDDI Registry is supported only when the Java   |

| Feature   | Browser client difference   |
|-----------|---|
|           | applet is in trusted mode.  |
| Log files | <p>The browser client does not write to the local log files. To view local log information, show the Java console as follows:</p> <ul style="list-style-type: none"> <li>• Select <b>Sun Java Console</b> in your browser's Tools menu if available, or</li> <li>• Open the Java control panel. Select the [Advanced] tab &gt; <b>Java console</b> &gt; <b>Show console</b>. Restart the browser if necessary.</li> </ul> <p>For more information about log files, see the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <p><b>Note:</b> The local logs in the Java console only contain information about the internal activities of the browser client. These logs may be useful in helping to diagnose applet-specific problems, such as unresponsive buttons or drag-and-drop operations that do not complete.</p> <p>The local logs are unrelated to the Gateway's logs and audit records, which continue to be available through the <a href="#">Gateway Audit Events</a> and <a href="#">Dashboard - Cluster Status</a> windows.</p> |

## Learning the Interface

The Policy Manager interface is made up of the following areas:

|   |    |
|---|----|
| Interfaces .....                        | 13 |
| Main Menu .....                         | 15 |
| Main Tool Bar .....                     | 22 |
| Assertions Tool Bar .....               | 23 |
| Policy Tool Bar .....                   | 24 |
| [Identity Providers] Tab .....          | 25 |
| [Assertions] Tab .....                  | 25 |
| Services and Policies .....             | 25 |
| Home Page .....                         | 27 |
| Policy Development Window .....         | 28 |
| Policy Validation Messages Window ..... | 28 |
| Status Bar .....                        | 28 |
| Assertion Numbering .....               | 30 |
| Policy Search Bar .....                 | 31 |
| Viewing Assertion Information .....     | 32 |
| My Account .....                        | 34 |

## Interfaces

This topic describes the Policy Manager interface as seen by those with the Administrator role. Some elements may not be visible or editable if you have a more restrictive role. For more information, see "Managing Roles" on page 130.

### General Interface: Identity Providers & Home Page

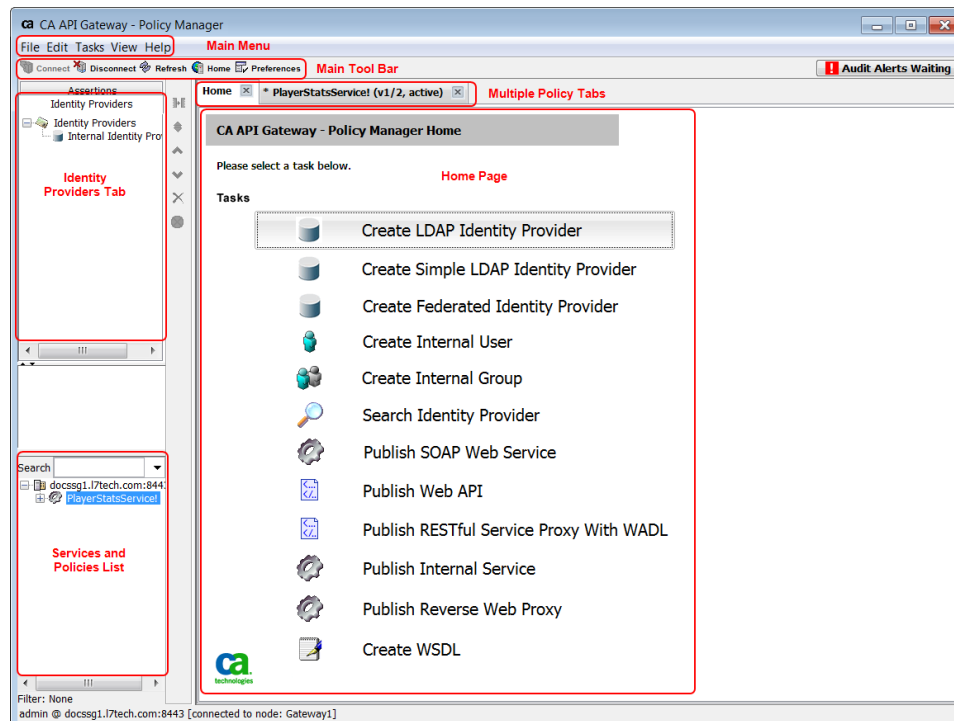


Figure 3: General Interface: Identity Provider and Home Page

## General Interface: Assertions & Policy Tree

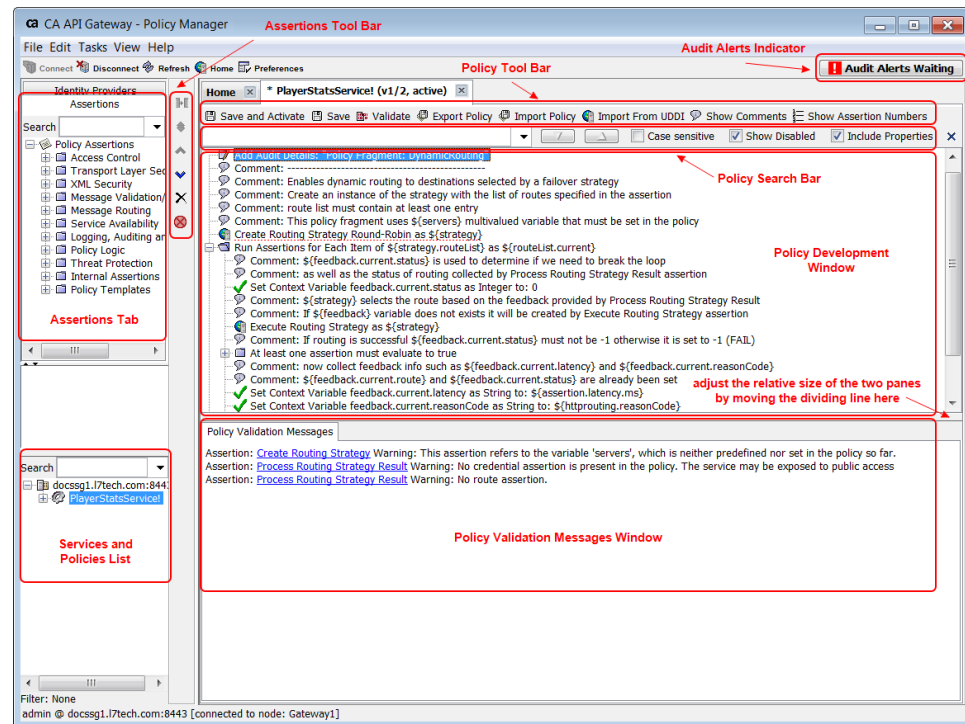


Figure 4: General Interface: Assertions and Policy Tree

## Wizards

Policy Manager uses wizards to help you configure complex processes. Simply advance through the steps and answer the questions. The configuration is complete when the wizard finishes.

The following table summarizes the controls available on a wizard:

Table 4: Using a wizard

| Button        | Description  |
|---------------|--|
| <b>Back</b>   | Return to the previous step to verify a setting or to make a correction.<br><br>Information entered on a current wizard page is preserved when you go back to a previous page. |
| <b>Next</b>   | Move to the next step of the wizard when you have finished entering information in the current step.   |
| <b>Finish</b> | Close the wizard and complete the configuration (for example, adding a Require SAML Token Profile assertion)   |



| Button        | Description  |
|---------------|--|
|               | to the policy window).<br>The <b>[Finish]</b> button is available only on the last step of the wizard. |
| <b>Cancel</b> | Close the wizard and discard all entries.  |
| <b>Help</b>   | Display the online help.   |

Most wizards also display a brief tip when you select a control or field on the wizard.

## Main Menu

---

**Note:** As the Main Menu is not present in the [browser client](#) version of the Policy Manager; use the alternate methods to access each menu item.

---

The Main Menu organizes features into the following menus:

### File menu

- **Save and Activate:** Saves the current policy or policy fragment as a new revision and makes it the active revision. This is indicated in the tab title for the revision. Also available on the [Policy Tool Bar](#). *Keyboard shortcut:* **[Ctrl]+[Alt]+S**
- **Save:** Saves the current policy or policy fragment as a new revision, without changing its active state. Also available on the [Policy Tool Bar](#). *Keyboard shortcut:* **[Alt]+S**
- **Export Policy:** Exports the policy to a file. Also available on the [Policy Tool Bar](#). *Keyboard shortcut:* **[Alt]+R**
- **Import Policy:** Imports a policy from an external file. Also available on the [Policy Tool Bar](#). *Keyboard shortcut:* **[Alt]+I**
- **Validate:** Validates a policy. Also available on the [Policy Tool Bar](#). *Keyboard shortcut:* **[Alt]+V**
- **Active Policy Assertions:** *(Visible only when a policy is open in the policy development window)* Loads the active revision into the policy development window. This shortcut removes the need to first display the revision history, then manually loading the active revision into the editor. Also available by right-clicking on the name of the service in the [Services and Policies](#) list. **Tip:** An even faster method to load the active revision is to double-click on the name of the service.
- **Service Properties:** Displays the [properties](#) for the service. Also available by right-clicking on the name of the service in the [Services and Policies](#) list.

- **Publish to UDDI:** Publishes information to a UDDI registry. Also available by right-clicking on the name of the service in the [Services and Policies](#) list .
- **Delete Service:** Deletes a published service. Also available by right-clicking on the name of the service in the [Services and Policies](#) list.
- **Compare Policy:** Compares any two policies and displays the results in a color-coded list. Can display differences between two assertions, including showing the properties or raw XML.
- **Connect:** [Connects](#) to a Gateway. Also available on the [Main Tool Bar](#). *Keyboard shortcut: [Alt]+C*
- **Disconnect:** [Disconnects](#) from a Gateway and logs you out. Also available on the [Main Tool Bar](#). *Keyboard shortcut: [Alt]+D*

When using the browser client, you should close your browser after disconnecting to securely log out. This clears your user name and password from the browser cache.

- **My Account:** Displays the [My Account](#) dialog, where you can view basic information about your account (including [role](#) information) and change your password. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#). *Keyboard shortcut: [Alt]+space*
- **Preferences:** Configures [preferences](#) for the Policy Manager. Also available on the [Main Tool Bar](#). *Keyboard shortcut: [Alt]+P*
- **Exit:** Closes the Policy Manager. You will be prompted to save if there are unsaved changes. In the browser client, close the browser after disconnecting to exit. *Keyboard shortcut: [Alt]+X*

### Edit menu

- **Copy:** Copies the selected item to the clipboard, ready to be pasted elsewhere. Useful for quickly replicating an assertion within a policy, replicating an include-policy fragment, [service](#), or alias, copying the underlying XML code of an assertion, or copying validation messages. When copying a composite assertion, all child assertions are copied as well.

---

**Notes:** (1) When copying a service, the information on the [\[UDDI\] tab](#) of the [Published Service Properties](#) is not carried over. This must be manually reentered upon pasting. (2) Internal and Global policies cannot be copied. (3) Avoid copying a service that has been converted to be a "portal managed" API. Doing so will cause the new service to be mapped to the original API. From the API Portal's perspective, it would appear that the original API has been replaced by the new one.

---

In the browser client, use either the alternative or keyboard shortcut methods to perform a Copy. **Note:** If the browser client is running in the untrusted mode, the Copy option is disabled in the right-click context menu for added security and you must use the keyboard shortcut instead.

*Alternative:* Right-click an assertion or selected text and select **Copy**

*Keyboard shortcut:* **[Ctrl]+C**

- **Copy All:** Copies all the assertions in the [policy development window](#). The XML code for all the assertions is placed in the clipboard, ready to be pasted back into the same policy or another external application.

In the browser client, use either the alternative or keyboard shortcut methods to perform a Copy All.

*Alternative:* Right-click anywhere within the policy development window and select **Copy All**.

*Keyboard shortcut:* **[Ctrl]+[Shift]+C**

- **Paste:** Pastes the items that were [copied](#) to the clipboard.
  - When pasting an include policy fragment, [service](#), or alias, select the destination folder before pasting. The properties for that policy or [service](#) are automatically displayed upon pasting, allowing you to make modifications to the copied settings before saving. Pasted policies start their own revision sequence (i.e., the version number is not related to the source item).
  - When pasting an assertion, the clipboard must contain valid policy XML code before Paste will work. The pasted assertion is inserted after the selected assertion in the policy development window or after the last assertion if no assertion is selected

In the browser client, use either the alternative or keyboard shortcut methods to perform a Paste.

*Alternative:* Right-click an assertion and select **Paste**.

*Keyboard shortcut:* **[Ctrl]+V**

Note the following about the Paste operation:

- When **Copy All** was used, Paste will group the pasted assertions within an "All Assertions" folder beneath the currently selected assertion. You can then use the [Assertions Tool Bar](#) to reposition if necessary.
- Source XML code for the Paste operation can come from an external application.
- If a pasted assertion requires immediate configuration, its properties will be displayed, just as if you had added it to the policy.

- If a pasted assertion refers to unknown entities (for example, unknown users or identity providers), a policy validation error will be displayed.
- Nothing will happen if you attempt to paste non XML or invalid policy XML code. However, this operation will be noted in the Policy Manager logs as a FINE event.
- **Go to Assertion:** Displays the assertion with the given [number](#). **Tip:** To see assertion numbers, click **[Show Assertion Numbers]** on the [Policy Tool Bar](#) or select this option under the View menu. *Keyboard shortcut: [Ctrl]+G*
- **Find:** Locates assertions in the policy that contain a specific search string. For more information, see "Policy Search Bar" on page 31. *Keyboard shortcut: [Ctrl]+F*
- **Find Next:** Finds the next matching item. *Keyboard shortcut: [F3]*
- **Find Previous:** Finds the previous matching item. *Keyboard shortcut: [Shift]+[F3]*
- **Migrate Namespaces:** Updates all XPath assertions from one namespace to another. For more information, see Migrating Namespaces in the *Layer 7 Policy Authoring User Manual*.

## Tasks menu

---

**Note:** In the [browser client](#), many of the items below are accessed from the "Manage" menu.

---

- **Create Identity Provider:** Creates an [LDAP](#) or [Federated](#) Identity Provider. Also available on the [Home](#) page.
- **Create Internal User:** Creates an Internal Identity Provider [user](#). Also available on the [Home](#) page.
- **Create Internal Group:** Creates an Internal Identity Provider [group](#). Also available on the [Home](#) page.
- **Manage Account Policies:** Displays the following options: [Manage Administrative User Account Policy](#), [Force Administrative Passwords Reset](#), and [Manage Password Policy](#). In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Search Identity Provider:** [Searches](#) for an identity provider (internal, Federated, or LDAP). Also available on the [Home](#) page.
- **Publish SOAP Web Service:** [Publishes](#) a SOAP web service. Also available on the [Home](#) page.
- **Create WSDL:** [Publishes](#) a Web service when a WSDL document is not available. Also available on the [Home](#) page.

- **Create Policy:** Creates a new policy fragment or internal use policy. Also available by right-clicking the root node within the [Services and Policies](#) list.
- **Publish Web API:** [Publishes](#) a Web API or non-SOAP application. Also available on the [Home](#) page.
- **Publish RESTful Service Proxy with WADL:** [Publishes](#) a REST proxy from a WADL file. Also available on the [Home](#) page.
- **Publish Internal Service:** [Publishes](#) an internal service. Also available on the [Home](#) page.
- **Publish Reverse Web Proxy:** [Publishes](#) a policy that enables the Gateway to function as a reverse web proxy.
- **Manage Certificates:** Displays the [Manage Certificates](#) dialog, where you can [add](#), [edit](#), [delete](#), or [export](#) a certificate. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Private Keys:** Displays the [Manage Private Keys](#) dialog, where you can configure custom private keys for outbound SSL communication, outbound message signing, and inbound message decryption. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Stored Passwords:** Displays the [Manage Stored Passwords](#) dialog, which you can use to store and select passwords and plain text PEM private keys in the Gateway database.
- **Revoke User Certificates:** [Revokes](#) all user certificates issued by the Gateway certificate authority. In the browser client, this is accessed by right-clicking an [Identity Provider](#).
- **Manage Global Resources:** Displays the Manage Global Resources dialog, where you can add, edit, or delete global schemas. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Cluster-Wide Properties:** Displays the [Manage Cluster-Wide Properties](#) dialog, where you can configure settings for the Gateway node. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Listen Ports:** Displays the [Manage Listen Ports](#) dialog, where you can configure additional listeners on the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage JDBC Connections:** Displays the [Manage JDBC Connections](#) dialog, where you can configure JDBC connections on the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).

- **Manage JMS Destinations:** Displays the [Manage JMS Destinations](#) dialog, where you can configure the destinations that will be used in the Route via JMS assertion. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Kerberos Configuration:** Displays the state of your Kerberos configuration. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Roles:** Displays the [Manage Roles](#) dialog, where you can add roles for a user. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Security Zones:** Displays the [Manage Security Zones](#) dialog, where you can configure security zones to control access to various elements in the Policy Manager. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Configure Audit Alert Options:** Displays the [Configure Audit Alert Options](#) dialog, where you can specify how often to check for new audits, the audit notification threshold, and enable/disable the audit alert feature. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Log/Audit Sinks:** Displays the [Manage Log Sinks](#) dialog, where you can configure additional message sinks on the Gateway. You also use this task to [Manage Audit Sinks](#). In the browser client, this task is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Email Listeners:** Displays the [Manage Email Listener](#) dialog, where you can configure email listeners on the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Configure FTP Audit Archiver:** Displays the [FTP\(S\) Audit Archiver Properties](#) dialog, where you specify the FTP host to use for archiving audit records. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage ESM User Mappings:** Displays the [Manage ESM User Mappings](#) dialog, which lists the Enterprise Service Managers currently being trusted by this Gateway and the user mappings. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage UDDI Registries:** Displays the Manage UDDI Registries dialog, which lists the UDDI registries recognized by the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).

- **Manage HTTP Options:** Displays the [Manage HTTP Options](#) dialog, which is used to edit the default HTTP proxy settings. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Service Resolution:** Displays the [Service Resolution Settings](#) dialog, which is used to configure how the CA API Gateway resolves services. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage Encapsulated Assertions:** Displays the Manage Encapsulated Assertions dialog, where you can perform various actions on your encapsulated assertions. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Manage MQ Native Queues:** (under "**Additional Actions**") Displays the [Manage MQ Native Queues](#) dialog, where you can configure SFTP polling listeners on the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **Install OAuth Toolkit:** (under "**Additional Actions**") Launches the installer for the Layer 7 OAuth Toolkit. For detailed instructions on installing and using this toolkit, see the *Layer 7 OAuth Toolkit User Manual*. For information on obtaining this OAuth Toolkit, please [contact](#) CA Technologies.
- **Manage SFTP Polling Listeners:** (under "**Additional Actions**") Displays the [Manage SFTP Polling Listeners](#) dialog, where you can configure SFTP polling listeners on the Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).

#### View menu

- **Policy Messages:** Shows/hides the [Policy Validation Messages](#) window. This window should normally be displayed, so that you can see validation messages. In the browser client, this is available under the Help tool on the [Main Tool Bar](#).
- **Status Bar:** Shows/hides the [Status Bar](#) at the bottom of the Policy Manager interface. The Status Bar is not used in the browser client version.
- **Show Assertion Numbers/Hide Assertion Numbers:** Shows or hides assertion numbers in the policy development window. Also available on the [Policy Tool Bar](#).  
*Keyboard shortcut: [Alt]+N*
- **Refresh:** Updates all tabs in the policy development window. Useful if multiple users are updating a policy simultaneously. Also available on the [Main Tool Bar](#).  
*Keyboard shortcut: [F5]*
- **Dashboard:** Displays [Service Metrics](#) and [Cluster Status](#) information. In the browser client, this is available under the Monitor tool on the [Main Tool Bar](#).

- **Gateway Audit Events:** Displays the [Gateway Audit Events](#) window. In the browser client, this is available under the Monitor tool on the [Main Tool Bar](#).
- **View Logs:** Used to [view the logs](#) in the system. In the browser client, this is available under the Monitor tool on the [Main Tool Bar](#).
- **Saved Events:** Used to view log or audit events that have been [saved](#). In the browser client, this is available under the Monitor tool on the [Main Tool Bar](#).
- **Filter Service and Policy Tree:** In the [policy tree](#), display only Services, Policy Fragments, or All. (**Note:** Filtering the display affects what is returned by Search box—only displayed entities are searched.) In the browser client, this is available by right-clicking the root folder in [the policy tree](#).
- **Sort Service and Policy Tree By:** Sort the [policy tree](#) by Name or Type, in ascending or descending order. In the browser client, this is available by right-clicking the root folder in [the policy tree](#).

#### Help menu

- **Help System:** Displays the online help for Policy Manager. *Keyboard shortcut: [F1]*
- **Manage Gateway License:** Displays the [Manage Gateway Licenses](#) dialog, where you can install, view, and remove the licenses for your Gateway. In the browser client, this is available under the Manage tool on the [Main Tool Bar](#).
- **About:** Displays information about the version of the Policy Manager.

## Main Tool Bar

The Main Tool Bar contains shortcuts to commonly used program features:

- **Connect:** [Connects](#) to a Gateway.
- **Disconnect:** [Disconnects](#) from a Gateway and logs you out.  
  
When using the browser client, you should close all browser windows after disconnecting to securely log out. This clears your user name and password from the browser.
- **Refresh:** Updates the policy development window by retrieving information from the Gateway again.
- **Home:** Displays the Home page. (To return to policy view, double-click the name of the service.)
- **Preferences:** Configures [preferences](#) for the standard version of the Policy Manager. **Note:** Preferences are not available in the browser client version of the Policy Manager.




In the [browser client](#) version of Policy Manager, the Main Tool Bar also contains these tools:

- **Manage:** Contains the "manage" tasks from the [Tasks](#) menu.
- **Monitor:** Contains items found in the [View](#) menu.
- **Help:** Contains options to access the online Help, toggle the [Policy Validation Messages](#) window, and view information about your version of the Policy Manager.







## Assertions Tool Bar


The Assertions Tool Bar contains shortcut buttons used to add and organize assertions in the [policy development window](#). Many of these actions are also available by right-clicking the assertion in the policy development window.

---

**Tip:** All operations (except for the  button) can be performed on more than one assertion at a time. To select multiple assertions, hold down the **[Ctrl]** or **[Shift]** key while selecting assertions in the policy. The **[Shift]** key selects blocks of assertions, while **[Ctrl]** key allows for discontinuous selection.

---

| Button  | Description   |
|---|---|
|  | <p>Adds the selected assertion to the policy.</p> <p><i>Alternative:</i> Drag the assertion from the [Assertions] tab and drop it into the policy development window.</p>   |
|  | <p>Expands and collapses the selected composite assertion(s) or included policy fragment assertion(s) in the policy development window. If no assertions are selected, then all assertions in the policy are expanded or collapsed.</p> <p>These buttons are not active if you select a branch with nothing to expand or collapse (in other words, it does not show the  or  icon).</p> <p><i>Alternative:</i> Right-click the assertion and select <b>Expand Assertion</b> or <b>Collapse Assertion</b>.</p> |
|  | <p>Moves the selected assertion(s) in the policy up or down one line.</p> <p><i>Alternatives:</i> (1) Drag and drop the assertion. (2) Right-click the assertion and select <b>Move Assertion Up</b> or <b>Move Assertion Down</b>.</p>   |
|  | <p>Deletes the selected assertion(s) from the policy.</p> <p><i>Alternative:</i> Right-click the assertion and then select</p>  |

| Button  | Description  |
|---|--|
|   | <b>Delete Assertion.</b>   |
|  | Disables the selected assertion(s) in the policy.<br><i>Alternative:</i> Right-click the assertion and then select <b>Disable Assertion.</b> |

For more information, see Configuring a Policy in the *Layer 7 Policy Authoring User Manual*.

## Policy Tool Bar

The Policy Tool Bar contains shortcuts to commonly used policy features:

- **Save and Activate:** Saves the policy or policy fragment in the [policy development window](#) and makes it the active revision. This button is available only if you have opened a non-active version for editing and changes have been made in the policy editor.
- **Save:** Saves the policy or policy fragment in the [policy development window](#) as a new revision but does not change the active version. **Tip:** To activate an inactive version, either use **[Save and Activate]** or the **[Set Active]** button in the Policy Revisions dialog.

---

**Note:** The **[Save]** and **[Save and Activate]** buttons will be unavailable if you have a role that permits read access to policies but not write access (for example, the "Operator" role). Should this happen, policy changes can be preserved by exporting the policy. For more information, see "Predefined Roles and Permissions" on page 132.

---

- **Validate:** Validates the policy.
- **Export Policy:** Exports the policy to a file.
- **Import Policy:** Imports a policy from a file.
- **Import from UDDI:** Imports a file via a UDDI registry. Similar to **Import Policy**, except instead of importing from a file, the source is XML resolved from an HTTP URL published in a UDDI registry.
- **Show Comments/Hide Comments:** Toggles the display of comments in the policy development window.
- **Show Assertion Numbers/Hide Assertion Numbers:** [Toggles the display of line numbers](#) next to each assertion in the policy development window.


## [Identity Providers] Tab

Contains the [identity providers](#) that have been set up in the Policy Manager. Right-click on a provider name to see the available actions.

## [Assertions] Tab

Contains a categorized list of the policy assertions used to construct a policy for a service. Expand a category to see the assertions within it.

## Services and Policies

The Services and Policies list in the lower left corner of the interface lists all published services and policies under a single root folder  bearing the hostname. You can right-click this root folder to perform any of the following actions:

- [Publish SOAP Web Service](#)

- [Create WSDL](#)

- [Publish Web API](#)

- [Publish RESTful Service Proxy](#)

- [Publish Internal Service](#)

- Create Policy




- Create New Folder

- Refresh:** Refreshes the list of services; used to reflect changes made by other concurrent users

- Paste

- Filter:** Choose to display only Services, Policy Fragments, or both in the tree. (**Note:** Filtering the display affects what is returned by Search box—only displayed entities are searched.)

- Sort by:** Choose to sort the tree by Name or Type (service or policy), in ascending or descending order

When you right-click on any published service (including [SOAP web services](#) , [XML applications](#) , and [internal services](#) ) , the following actions are available:

- Active Policy Assertions:** Loads the active version of the policy into the policy development window (see Policy Revisions)

- [Service Properties](#)

- Publish to UDDI

- [Delete Service](#)

- Copy as Alias

- [Create Log Sink](#)

- Revision History




- Service Debugger

Compare Policy

**Refresh:** Refreshes the list; used to reflect changes made by other concurrent users

Cut

Copy

When you right-click on any policy (including policy fragments  or internal use policies  or global policies ) the following actions are available:

**Active Policy Assertions:** Loads the active version of the policy into the policy development window (see Policy Revisions); **Tip:** You can select this option for a policy fragment currently visible in the policy development window to open the fragment for editing. This applies only if you have edit permission for the fragment.

Policy Properties

Delete Policy

Copy as Alias

Create Log Sink

Revision History


Service Debugger

Compare Policy

**Refresh:** Refreshes the list; used to reflect changes made by other concurrent users

Cut

Copy

When you right-click a folder , the following actions are available:

Publish SOAP Web Service

Create WSDL

Publish Web API

Publish RESTful Service Policy

Publish Internal Service

Create Log Sink

Create Policy

Rename Folder

Create New Folder

Delete Folder


Cut

Paste

---

**Note:** This applies only applies to folders created to group services and policies. It does not apply to the "Bindings" and "Services" items under a SOAP web service. For more information, see Organizing Services and Policies into Folders in the *Layer 7 Policy Authoring User Manual*.

---

A service is enabled by default when it is published, but it can be disabled through the [service's properties](#). Disabled services show this icon: .

## Quick Search

➤ *To quickly locate a service or policy in the Services and Policies list:*

1. Type the first few characters of the name in the **Search** box at the top of the Services and Policies list. A pop-up list displays items that match the characters typed. If you type a '/' at the beginning of the search string, only the routing URIs are searched. For example, typing "/ware" would display a list of services with custom URIs beginning with "/ware", such as "/warehouse".
2. Select the appropriate item from the list and then press **[Enter]**. The tree view expands to open the folder containing the selected search item.

---

**Note:** If the display has been filtered to show only services or policy fragments, only the filtered items are searched.

---

## Multiple Delete

You can delete multiple items (such as folders and policies) at once. You can also delete non-empty folders, provided that they do not contain policies (or fragments) used by the policy outside of the folder.

➤ *To delete more than one item in the Services and Policies list:*

1. Hold down the [Ctrl] or [Shift] key to select the items to delete.
2. Right-click and select **Delete Targets**, or press the [Delete] key. A two-step confirmation box is displayed.
3. Verify the deletion by selecting the check box. This enables the **[OK]** button.
4. Click **[OK]** to delete. Any folder and its contents will be removed, unless its content is still being used elsewhere outside of the folder.

## Home Page

The Home Page is displayed upon startup or when **[Home]** is clicked on the [Main Tool Bar](#). The Home Page contains shortcuts to commonly used wizards and dialogs:

- [Create LDAP Identity Provider](#)
- [Create Simple LDAP Identity Provider](#)

- [Create Federated Identity Provider](#)
- [Create Internal User](#)
- [Create Internal Group](#)
- [Search Identity Provider](#)
- [Publish SOAP Web Service](#)
- [Publish Web API](#)
- [Publish RESTful Service Policy](#)
- [Publish Internal Service](#)
- [Create WSDL](#)

## Policy Development Window

Used to view or edit a policy revision for the selected published service. Each policy or revision is displayed in a separate tab. The tab name indicates whether the revision is active or inactive.

## Policy Validation Messages Window

This window displays confirmation, warning, and error messages about the policy. You can show/hide this window using the **[View] > Policy Messages** menu option (in [browser client](#), from the **Help** menu). Unless you need the screen space for the [policy development window](#), you should always have the validation window open. For more information, see *Validating a Policy* in the *Layer 7 Policy Manager User Manual*.

## Status Bar

---

**Note:** The Status Bar is not present in the [browser client](#) version of the Policy Manager.

---

The Status Bar displays user, Gateway, and port information. This bar may be toggled on and off by using **[View] > Status Bar**.

To learn more about obtaining system information, see "Chapter 6: Analyzing Gateway Performance" on page 401.

## Audit Alerts

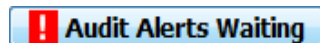
The Policy Manager can alert you to important audit events that require your attention. These events could have occurred while you were logged off or while you are using the Policy Manager.

---

**Note:** In order to receive audit alerts, your [role](#) must allow you to view the [Gateway Audit Events](#) window.

---

When an audit event occurs that meets a preset threshold, the following alert indicator will appear in the top right corner of the [user interface](#):



Click this indicator to open the following dialog:

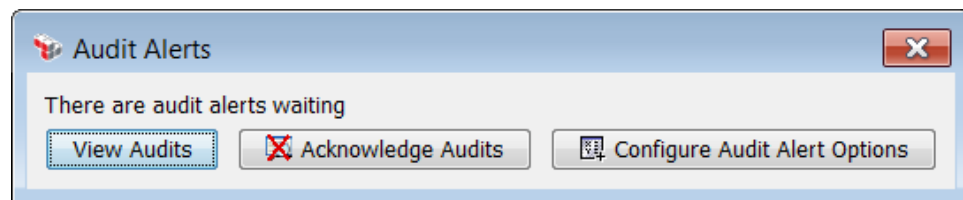


Figure 5: Audit Alert dialog

Your options are as follows:

Table 5: Audit Alert options

| Option                               | Description  |
|--------------------------------------|--|
| <b>View Audits</b>                   | <p>Launches the <a href="#">Gateway Audit Events</a> window, where you can see more information about the audit items.</p> <p>When [View Audits] is clicked, the audit alert indicator will not appear again until there are new audits requiring your attention.</p>  |
| <b>Acknowledge Audits</b>            | <p>Acknowledges the alert and closes the dialog without displaying the Gateway Audit Events window.</p>  |
| <b>Configure Audit Alert Options</b> | <p>Opens the Configure Audit Alerts dialog to allow you to configure the following settings:</p> <ul style="list-style-type: none"> <li>• <b>Enable Audit Alerts:</b> Use this check box to enable or disable the Audit Alert feature.</li> <li>• <b>Check for new audits every:</b> Specify how often the Policy Manager should check for new audit events. The default is every 30 seconds.</li> <li>• <b>Check for audits at or above level:</b> Select the <a href="#">severity</a> of the audit event before the audit alert appears. At the default WARNING level, only events rated WARNING or SEVERE will be brought to your attention. Be aware that choosing a threshold below WARNING will result in a large number of audit alerts (the</li> </ul> |

| Option | Description  |
|--------|--|
|        | <p>Gateway generates many INFO alerts).</p> <p><b>Tip:</b> To configure audit alerts when the Audit Alerts Waiting indicator is not present, select <b>Configure Audit Alert Options</b> from the <a href="#">Task</a> menu (in the browser client version, this is accessed from the Manage tool on the Main Tool Bar).</p> |

## Assertion Numbering

To assist you during policy editing, you can display assertion numbers in the policy development window. These numbers are especially useful when dealing with complex policies. They are also used during policy debug tracing.

➤ To display or hide assertion numbers:

- Do one of the following:
  - In the [policy tool bar](#), click [**Show Assertion Numbers**] or [**Hide Assertion Numbers**].
  - Under the [View menu](#), select **Show Assertion Numbers** or **Hide Assertion Numbers**.
  - Press [**Alt**]+**N** to toggle assertions numbers on/off (only valid for the [desktop client](#))

The following numbering system is used:

- The first assertion in the policy is always number "2". This is because there is an implicit "All assertions must evaluate to true" assertion at the root of every policy that occupies the number "1" position. For simplicity, this assertion is hidden in the Policy Manager interface but is visible in the underlying XML code for the service.
- The same rule applies when a policy fragment is added to a service policy: the first assertion within that fragment is number "2":



Figure 6: Assertion numbering example

- Included policy fragments will cause an increase to the numbering hierarchy. Using the example shown in Figure 6, the first "Include" increases the numbering by one decimal place (6 > 6.2), while the nested "Include" increases the hierarchy again



(6.4 > 6.4.2).

- Assertions within composite assertions such as "All assertions..." and "At least one assertion..." are numbered contiguously and do not cause an increase to the numbering hierarchy.

## Policy Search Bar

The Policy Search Bar in the policy development window helps you quickly locate an assertion based on text visible in the policy editor, or in the underlying XML code.





---


**Tip:** You can hide the Policy Search Bar by pressing the [Esc] key or by clicking the "x" in the upper right corner. Press [Ctrl]+F or select **Edit > Find** to re-enable the search bar.

---

The following table describes the controls in the Policy Search Bar:

Table 6: Using the Policy Search Bar

| Element   | Description  |
|---|--|
|    | Type the text in this search box. As you type, any assertions that contain the matching text are displayed.<br><br><b>Tip:</b> If <b>[Include Properties]</b> is selected, the match may not be obvious: the match may occur in the underlying XML code for the assertion.                             |
|  | Click this to see a drop-down list showing the matching assertions again.  |
|  | Click this button to jump to the next matching assertion. This is the same as selecting <b>Find Next</b> from the <b>Edit menu</b> (keyboard shortcut <b>[F3]</b> ).   |
|  | Click this button to jump to the previous matching assertion. This is the same as selecting <b>Find Previous</b> from the <b>Edit menu</b> (keyboard shortcut <b>[Shift]+[F3]</b> ).   |
| <b>Case sensitive</b>   | Select this check box to match the case of the search string.<br><br>Clear this check box to ignore case during searches. This setting is the default.   |
| <b>Show Disabled</b>  | Select this check box to include disabled assertions in the searches. This setting is the default.<br><br>Clear this check box to show only active assertions.   |
| <b>Include Properties</b>   | Select this check box to include the assertion properties in the searches. This setting is the default.<br><br>Clear this check box to search only the assertion name.<br><br><b>Note:</b> When including properties, the underlying XML code is also searched. This may result in unexpected matches. |

| Element   | Description  |
|---|--|
|   | <b>Tip:</b> To see the underlying XML code, <a href="#">copy</a> the assertion and then paste the contents into a text editor. Note that only text viewable in the underlying XML is searchable. |
|  | Click this button to close the Policy Search Bar.  |

During the search, feedback messages similar to the following may appear:

No more results. Press F3 to search from the top.

These messages are for informational purposes only and will disappear when you click on them or perform another search task.

## Viewing Assertion Information

The Assertion Information dialog can be displayed for any assertion in the policy window. This dialog summarizes context variable usage for that assertion: the variables set by the assertion (if any) and the variables used by the assertion (if any). This can help you during policy authoring and troubleshooting.

There are two ways to view context variable information for an assertion:

- **via tooltip:** Assertions that *set* context variables will display a tooltip (visible when you hover the mouse pointer over the assertion) that lists the variables set by that assertion:

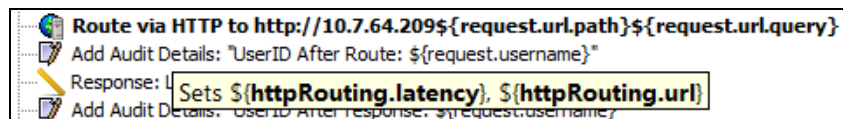


Figure 7: Context variables listed in a tooltip

**Note:** The tooltip only lists the context variables that are set by the assertion. To see which variables are used by the assertion, you must use the second method below.

- **via Assertion Information dialog:** For a more comprehensive display, right-click the assertion within the policy and select **View Info**. This displays the Assertion Information dialog:

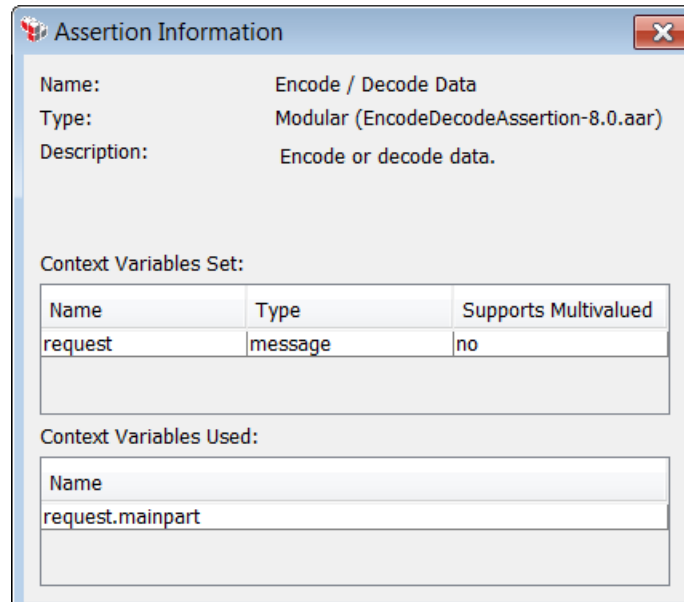


Figure 8: The Assertion Information dialog

The upper part of the dialog displays basic information about the assertion:

- **Name:** The name of the assertion as it appears on the assertion palette.
- **Type:** The type of the assertion. There are four different types of assertions:
  - **Core:** These assertions are shipped with the Gateway.
  - **Custom:** These are extra cost assertions purchased from CA Technologies to do a specific task. They can also be customer-created assertions, created using the Layer 7 Custom Assertion SDK. The file name of the custom assertion is shown within parenthesis.
  - **Encapsulated:** These are encapsulated assertions created by the customer. For more information, see Working with Encapsulated Assertions in the *Layer 7 Policy Authoring User Manual*.
  - **Modular:** These are assertions created by CA Technologies and designed to be easily installed on any Gateway. The file name for the modular assertion is shown within parenthesis.
- **Description:** The assertion description, as shown on the interface of the Policy Manager.

The "Context Variables Set" table lists the context variables that are set by the assertion—in other words, the assertion will populate values into these variables:

- **Name:** The name of the [context variable](#) that will be populated. In most instances, this is a predefined context variable that is shipped with the system.

However it can also be a custom context variable that is created by the assertion.

- **Type:** The data type of the context variable. For more information, see "[Context Variable Data Types](#)" under "Appendix C: Context Variables" on page 517
- **Supports Multivalued:** Indicates whether the context variable is multivalued. For more information, see "Working with Multivalued Context Variables" on page 558.

The "Context Variables Used" table lists the context variables that are used by the assertion—in other words, the assertion requires the values within these variables during its execution.

## My Account

The My Account dialog provides a quick way to show you (as the logged-in user) the roles in which you are a member. This will give you an idea as to what is available to you in the Policy Manager.

With the exception of changing your password, no information can be modified through the My Account dialog.

---

**Tip:** The information shown under My Account is a subset of the User Properties dialog, which may or may not be available to you depending on the security permissions.

---

➤ *To view my account information:*

1. In the Policy Manager, select [**File**] > **My Account** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The My Account dialog appears.
2. The [Properties] tab shows basic information about your account, including when your account will expire (if one has been set).
  - If you need to change your password, click [**Change Password**] and follow the prompts. For more information, see "Changing a Password" on page 44.

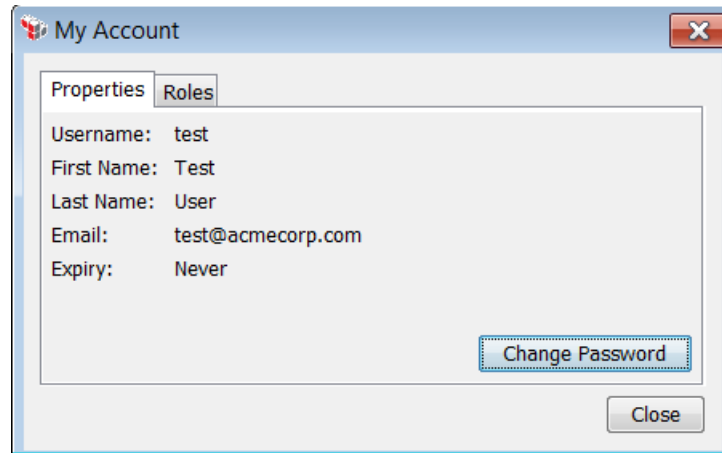
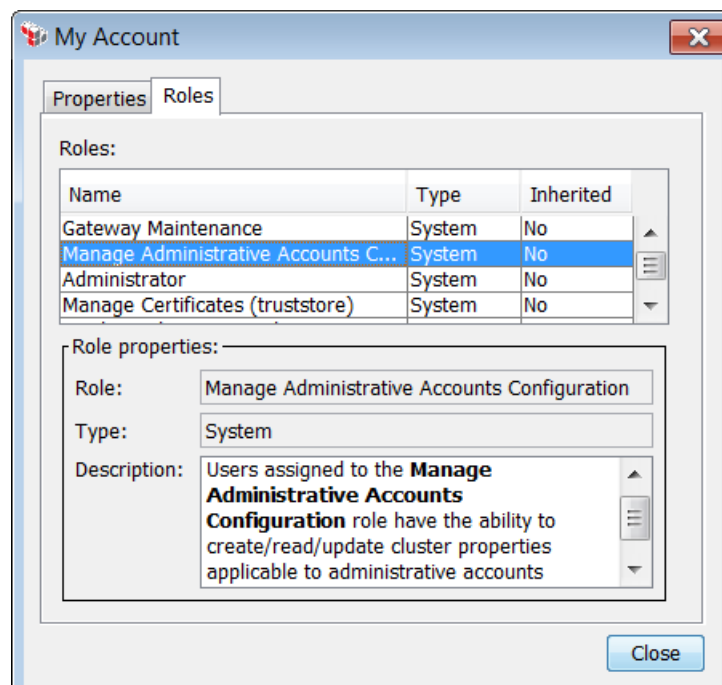


Figure 9: My Account - [Properties] tab

3. The [Roles] tab shows the roles in which you are a member:



The Roles table lists the roles in which you are assigned, either directly or indirectly:

- **Name:** The name of the role.
- **Type:** "System" indicates a role that is either predefined or automatically generated (see ""Predefined Roles and Permissions" on page 132"). "Custom" indicates a role that has been defined at your organization (see ""Managing Roles" on page 130").

- **Inherited:** "No" means have been assigned to the role directly; "Yes" means you are a member of a group that has been assigned to that role.

The Role properties section at the bottom displays the complete description for the selected role.

4. Click **[Close]** when done.

## General Workflow

Several Policy Manager tasks are required before you can leverage the Gateway's functionality. Since every organization will use the Policy Manager differently, the following list includes only the key tasks for configuring and using the Policy Manager. If you require assistance in the configuration process, [contact](#) CA Technical Support.

The following workflow assumes the user has the Administrator [role](#). For information on the steps required to configure identity bridging in the Policy Manager and Securespan XML VPN Client, see [Identity Bridging](#).

1. [Connect](#) to the Gateway.
2. Upon first connection to a Gateway, you need to [install](#) the license file.
3. Each Gateway Internal Identity Provider (IIP) is pre-configured with a single default administrative user ("admin") and a set of predefined [roles](#). Optionally configure additional [users and groups](#) for the IIP.
4. Configure [LDAP Identity Providers](#).
5. Publish a new [SOAP web service](#), [Web API service](#), or a [RESTful service proxy](#).
6. Construct a valid policy for a published service.
7. [Analyze](#) the performance of the Gateway and refine if necessary.

## Managing Gateway Licenses

CA Technologies provides a signed XML license file with every Gateway. This license file unlocks specific Gateway features for a predetermined period. In license-enabled mode, the Gateway processes incoming service messages, provides ancillary services such as WSDL and policy discovery, and provides full administrative services to any connected Policy Manager. If a license is not installed or is expired, then most Policy Manager features will be disabled until a valid license is installed.

A Primary license is required for any functionality to be enabled. You will be prompted to install a Primary license the first time the Policy Manager is used to [connect](#) to a Gateway or cluster. Once the Primary license is installed, you can [install](#) additional license files to activate new functionality at any time.

The Gateway is able to maintain multiple licenses. Use the Manage Gateway Licenses dialog box to install, remove, or view details of a license.

---

**Tip:** New Gateways may have had their licenses auto-provisioned already. This means you will not need to install the license using the Manage Gateway Licenses dialog box. To confirm the details of your auto-provisioned license, see "View Details" below. For more information, see "Auto-Provisioning a License" in the *Layer 7 Installation and Maintenance Manual*.

---

➤ To manage Gateway licenses:

1. Ensure that you are [connected](#) to a Gateway.
2. In the Policy Manager, select **[Help] > Manage Gateway Licenses**. The table of licenses appear on the Manage Gateway Licenses dialog.

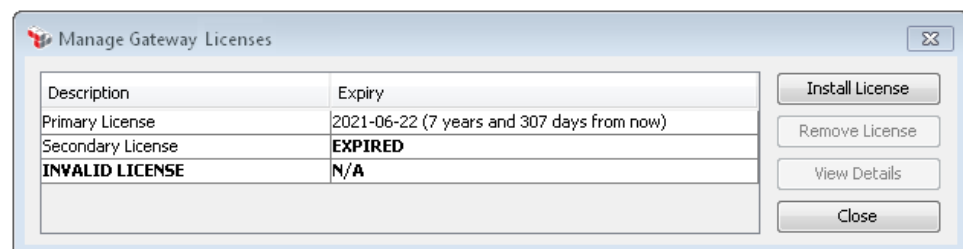


Figure 10: Manage Gateway Licenses dialog

3. Select a task to perform:

Table 7: Manage Gateway License tasks

| To...             | Do this...                    |
|-------------------|-------------------------------|
| Install a license | See Installing a License File |

Table 7: Manage Gateway License tasks

| To...                   | Do this...   |
|-------------------------|--|
| <b>Remove a license</b> | See "Removing a License File" on page 39   |
| <b>View Details</b>     | <ol style="list-style-type: none"> <li>1. Select a license to view.</li> <li>2. Click [<b>View Details</b>] to see more information about the license. If you need to review the contents of the License Agreement, click [<b>View EULA</b>].</li> </ol> |

4. Click [**Close**] when done.

## Installing a License File

You must install a [license file](#) in order to unlock the CA API Gateway.

There are two types of licenses:

1. **Primary:** Unlocks the base functionality of the Gateway. This license was supplied when the product suite was first purchased.
2. **Feature:** Unlocks additional features that are purchased at a later date.

You are automatically prompted for a license file the first time the Policy Manager is connected to a Gateway or cluster. You can also update this license file at any time (for example, to replace an expired license or install a new license that unlocks different features).

These are common scenarios of installing a license.

---

**Notes:** (1) If the Gateway Primary license was auto-provisioned, you do not need to install the license file as described below. For more information, see "Auto-Provisioning a License" in the *Layer 7 Installation and Maintenance Manual*. (2) To avoid possible data loss, save any policy changes prior to installing or removing a license.

---

➤ *To install a Primary license for the first time:*

1. [Connect](#) to the Gateway.
2. The Gateway License warning dialog appears automatically when no license is present.
3. Click [**Install License**] in the Manage Gateway Licenses dialog. The file selection dialog appears.
4. Select a valid license file from the file selection dialog and click [**Open**].
5. Click [**I Agree**] to accept the license agreement.



➤ *To install an additional license:*

1. [Connect](#) to the Gateway.
2. From the [Main Menu](#), select **[Help] > Manage Gateway Licenses**. The Manage Gateway License dialog appears.
3. Click **[Install License]** in the Manage Gateway Licenses dialog. The file selection dialog appears.
4. Click **[I Agree]** to accept the license agreement.

➤ *To replace a license that has expired:*

1. From the [Main Menu](#), select **[Help] > Manage Gateway Licenses**. The Manage Gateway License dialog appears.
2. Select the expired license from the list of installed licenses.
3. Click **[Remove License]**.
4. Click **[Yes]** in the Gateway License warning dialog to view the license manager.
5. Click **[Install License]** in the Manage Gateway Licenses dialog. The file selection dialog appears.
6. Select a valid license file and click **[Open]**.
7. Click **[I Agree]** to accept the license agreement.

When a license is about to expire, you only need to install the newer version.

### Enforcing FIPS Compliancy

If you are installing a license that enforces the use of FIPS-compliant cryptographic algorithms, you must restart the Gateway after installing the license for the enforcement to take effect.

---

**Note:** When a FIPS-compliant license is installed, it will override the [security.fips.enabled](#) cluster property.

---

### Removing a License File

You can remove a license by using the Manage Gateway License task.

## W A R N I N G

Removing a license file is irreversible. It will disable all functionality that the license file allows. Be sure that you have a suitable replacement license prior to removing the license file.

➤ To remove a license:

1. [Connect](#) to the Gateway or cluster using Administrator credentials.
2. From the [Main Menu](#), select **[Help] > Manage Gateway Licenses**. The Manage Gateway License dialog appears.
3. Select a license from the list of installed licenses.
4. Click **[Remove License]**.
5. Select the check box and then click **[OK]**. Due to the irrevocable nature of this action, you must select the check box first to enable the **[OK]** button.
6. Once you remove a license and close the Manage Gateway Licenses dialog, the Policy Manager will automatically disconnect from the Gateway.

If you have any unsaved policy changes, you will be prompted to export your policies. Click **[Save Policy]** to export to a file, or click **[Discard Policy]** to continue without exporting.

---

**Tip:** If you export to a file, you can import the policy back into the Policy Manager after re-licensing. For more information, see *Importing a Policy from a File* in the *Layer 7 Policy Authoring User Manual*.

---

## Managing Cluster-Wide Properties

The *Manage Cluster-Wide Properties* task is used to configure settings for your Gateway node. If your node is part of a cluster, all other nodes in the cluster inherit the new settings as well.

Assertions that can use context variables can also indirectly read cluster-wide properties through the `${gateway.<clusterProperty>}` variable. For more information, see "Appendix C: Context Variables" on page 517.

For a list of all the properties that can be configured, see "Appendix D: Gateway Cluster Properties" on page 567.

➤ To manage cluster-wide properties:

1. In the Policy Manager, select **[Tasks] > Manage Cluster-Wide Properties** from the **Main Menu** (on the **browser client**, from the **Manage** menu). The Manage Cluster-Wide Properties appear.

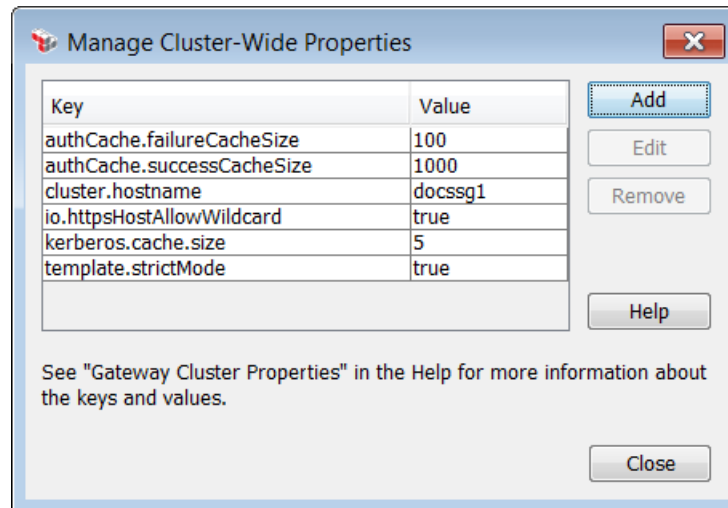


Figure 11: Manage Cluster-Wide Properties (with sample values)

Select one of the following actions:

Table 8: Editing cluster-wide properties

| Action                         | Description  |
|--------------------------------|--|
| <b>Add a cluster property</b>  | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>.</li> <li>2. Enter the <b>cluster property name</b> in the <b>Key</b> field or choose a property from the drop-down list.</li> <li>3. Enter a value for the property in the <b>Value</b> field. The value must be a valid value listed in the property's description. Note that this only applies to cluster properties with clearly defined values; properties with freeform values (e.g., <i>log.levels</i>) are not validated.<br/><br/>For a description of the format of expected values, see <i>"Time Units"</i> in "Appendix D: Gateway Cluster Properties" on page 567.</li> <li>4. Click <b>[OK]</b>. This value is now used by all nodes in the cluster.</li> </ol> |
| <b>Modify a property value</b> | <ol style="list-style-type: none"> <li>1. Select the key to modify.</li> <li>2. Click <b>[Edit]</b>. The Edit Cluster Property dialog appears.<br/><br/><b>Note:</b> If the property you are editing has a description, that description is displayed above the Key. If not, the description box is blank.</li> <li>3. Enter a new valid value for the property.</li> </ol>  |

| Action                   | Description  |
|--------------------------|--|
|                          | 4. Click <b>[OK]</b> . The value for the key is updated.   |
| <b>Remove a property</b> | 1. Select the key to delete.<br>2. Click <b>[Remove]</b> . The key is deleted immediately. The property value reverts to the default listed in "Appendix D: Gateway Cluster Properties" on page 567. |

2. Click **[Close]** when done.

## Managing Stored Passwords

The *Manage Stored Passwords* task is used to securely store passwords and plain text PEM private keys in the Gateway database, where they will be safeguarded in database backups, and can be easily selected in situations where a password is required.

---

**Note:** Only plain text PEM private keys are stored in the *Manage Stored Passwords* task. Asymmetric private keys with certificate chains are stored using the [Manage Private Keys](#) task

---

Stored passwords also have the added security of allowing you to reference them via context variables. This lets you avoid explicitly stating the password in certain situations. For example, you may have a *Return Template Response to Requestor* assertion that sends back a password:

```
<p>Your password is: thisisthepassword </p>
```

With stored passwords, you can replace it with this:

```
<p>Your password is: ${secpass.salesgroup.plaintext}</p>
```

In the first example, the password is stored in the database in plain text, and will be included in any exported policy XML files. In the second example, the password is not visible as plain text and is not included in the policy, preventing it from being leaked during a policy export.

---

**Tips:** (1) For added security, referencing passwords via context variables is an optional setting that must be explicitly enabled for each password. Once enabled, there is no further security to control its use, so use this feature with care. (2) To set permissions for stored passwords, select the "Secure Passwords" entity type in the [Add Permissions to Role Wizard](#).

---

➤ To manage stored passwords:

1. In the Policy Manager, select **[Tasks] > Manage Stored Passwords** from the [Main Menu](#). The Manage Stored Passwords dialog appears.

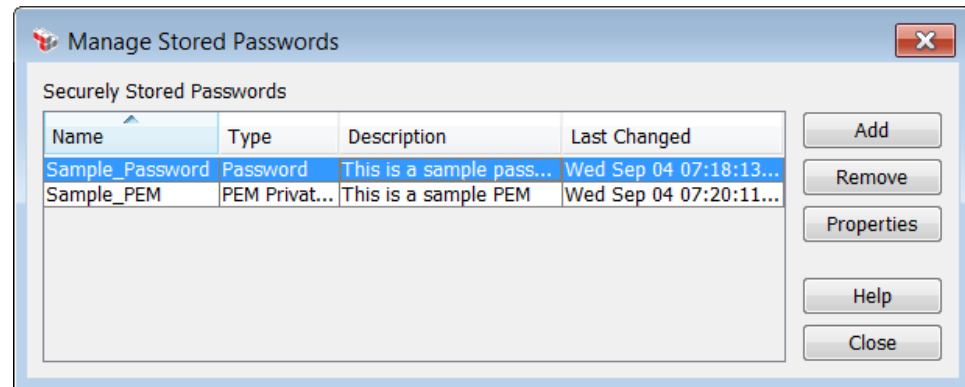


Figure 12: Manage Stored Passwords dialog

The dialog displays details about the passwords being stored, but it will never display the passwords themselves.

Select a task to perform:

Table 9: Manage Stored Passwords tasks

| To...  | Do this...   |
|--|--|
| <b>Add a new password</b>                                      | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>.</li> <li>2. Complete the details for the new password. For details, see "Stored Password Properties" on page 45.</li> </ol>  |
| <b>Remove a password</b>                                       | <ol style="list-style-type: none"> <li>1. Select the password to remove.</li> <li>2. Click <b>[Remove]</b>.</li> <li>3. Click <b>[OK]</b> to confirm. The system will attempt to remove the stored password.</li> </ol> <p><b>Note:</b> A password cannot be removed if it is being referenced by <a href="#">HTTP options</a>.</p>  |
| <b>Edit an existing password/<br/>View password properties</b> | <ol style="list-style-type: none"> <li>1. Select the password to edit or view.</li> <li>2. Click <b>[Properties]</b>.</li> <li>3. Modify the password details if required. For details, see "Stored Password Properties" on page 45.</li> </ol> <p><b>Notes:</b> (1) Editing password details allows you to change the password, but you cannot see the actual password. (2) Users with Read-only access to the "secure passwords" <a href="#">entity type</a> can only view (but not modify) password properties.</p> |

2. Click **[Close]** when done.

## Changing a Password

There are two ways to change the password used to [connect](#) to the Gateway:

- Users who have the [roles](#) "Administrator" or a custom role ("Read" Identity Provider; "Read" and "Update" Users) can change the password for any [internal user](#) in the system. Simply use the **[Change Password]** button on the [General] tab of the user's Properties dialog. For more information, see "Editing or Deleting a User or Group" on page 458.
- Any user in the system (regardless of role) can change his or her password at any time using the Change Password dialog, which is accessed from the My Account dialog.

---

**Note:** LDAP users must use the LDAP administrative program to change passwords. They cannot change their passwords using the Policy Manager.

---

### Background: Authentication Caching

When a password is changed, there is a short period of time before the new credentials are recognized and the old credentials are discarded. The following is some background information on how the Gateway uses cached credentials:

- Credentials that are successfully authenticated against an identity provider are cached for a period of 60 seconds by default. Credentials that fail authorization are cached for 30 seconds by default.
- During the cache period, the Gateway will not re-authenticate the same credentials; it will return the cached result instead (either success or failure).
- While beneficial for performance, cached credentials may cause valid credentials to be rejected or invalid credentials to be accepted for a short period of time.

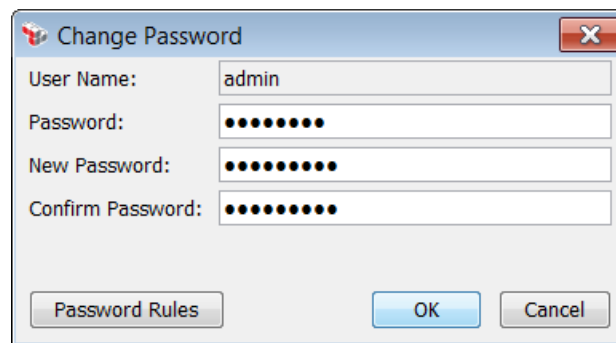
*Example:* Bob's password is changed from *widget* to *gizmo*. Within 60 seconds of the change, the password *widget* is still accepted. The new password *gizmo* will not be accepted for at least 30 seconds after the change.

If the Gateway is part of a cluster, an extra 15 seconds may be required for the changes to propagate through the nodes.

➤ *To change your own password:*

1. In the Policy Manager, select **[File] > My Account** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The My Account dialog appears
2. Click **[Change Password]** in the [Properties] tab.

The Change Password dialog appears.



The image shows a 'Change Password' dialog box with a title bar containing a red 'X' button. It has four input fields: 'User Name' (containing 'admin'), 'Password' (masked with dots), 'New Password' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom, there are three buttons: 'Password Rules', 'OK', and 'Cancel'.

Figure 13: Change Password dialog

2. Configure the dialog as follows:

Table 10: Changing a password

| Field                   | Description  |
|-------------------------|--|
| <b>User Name</b>        | Your user name is displayed for reference; it cannot be edited.  |
| <b>Password</b>         | Type your current password.  |
| <b>New Password</b>     | Type your new password, between 8 and 32 characters long. Be sure it conforms to the password rules.                                   |
| <b>Confirm Password</b> | Retype your new password to confirm.   |
| <b>Password Rules</b>   | Displays a reminder of the password rules. For more information on how these rules are set, see "Managing Password Policy" on page 48. |

3. Click **[OK]**. Your password is changed immediately. **Tip:** If the **[OK]** button is not available, click **[Password Rules]** to ensure that your new password conforms to all the rules listed.

## Stored Password Properties

When adding or editing a stored password, the Stored Passwords Properties appear. This dialog records details about a new password and it lets you modify details for an existing password.

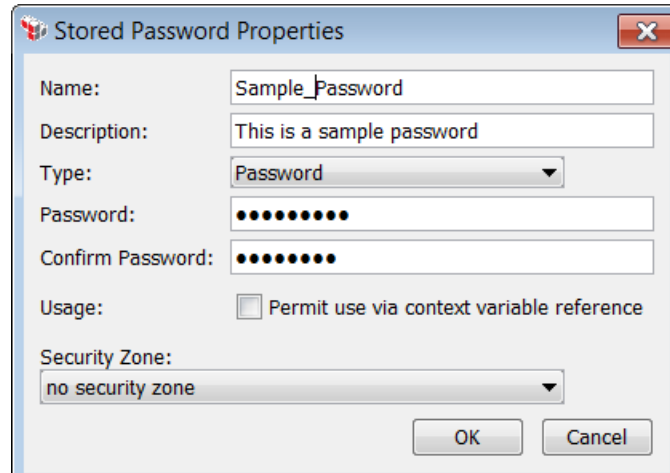
---

**Note:** A "password" can be either a plain text password or a plain text PEM private key. All other private keys are stored using the [Manage Private Keys](#) task.

---

➤ To access the properties for a stored password:

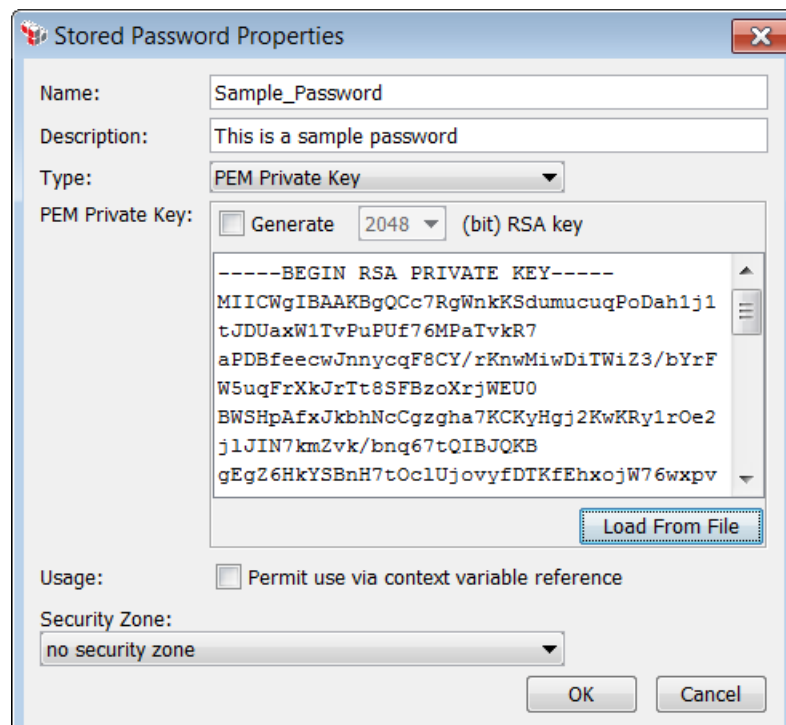
1. Run the [Manage Stored Passwords](#) task.
2. Select a password from the list and then click **[Edit]**. You can also click **[Add]** to enter a new password. Slightly different versions of the Stored Password Properties appear, depending on whether you are adding or editing a password.



The 'Stored Password Properties' dialog box is shown with the following fields and options:

- Name:** Sample\_Password
- Description:** This is a sample password
- Type:** Password (selected from a dropdown menu)
- Password:** A text field containing 10 black dots.
- Confirm Password:** A text field containing 10 black dots.
- Usage:** ☐ Permit use via context variable reference
- Security Zone:** no security zone (selected from a dropdown menu)
- Buttons:** OK and Cancel

Figure 14: Stored Password Properties - Adding a password



The 'Stored Password Properties' dialog box is shown with the following fields and options:

- Name:** Sample\_Password
- Description:** This is a sample password
- Type:** PEM Private Key (selected from a dropdown menu)
- PEM Private Key:**
  - ☐ Generate 2048 (bit) RSA key
  - A text area containing a sample PEM private key:

```
-----BEGIN RSA PRIVATE KEY-----
MIICWgIBAAKBgQCc7RgWnkKSdumucugPoDah1j1
tJDUaxW1TvPuPUf76MPaTvR7
aPDBfeecwJnnycqF8CY/rKnwMiwDiTWiZ3/bYrF
W5uqFrXkjrTt8SFBzoXrjWEU0
BWSHpAfxJkbhNcCgzgha7KCKyHgJ2KwKRy1rOe2
j1JIN7kmZvk/bnq67tQIBJQKB
gEgZ6HkYSBnH7tOclUjovyfDTKfEhxojW76wxpv
-----
```
  - Load From File:** A button to load a key from a file.
- Usage:** ☐ Permit use via context variable reference
- Security Zone:** no security zone (selected from a dropdown menu)
- Buttons:** OK and Cancel

Figure 15: Stored Password Properties - Adding a PEM private key



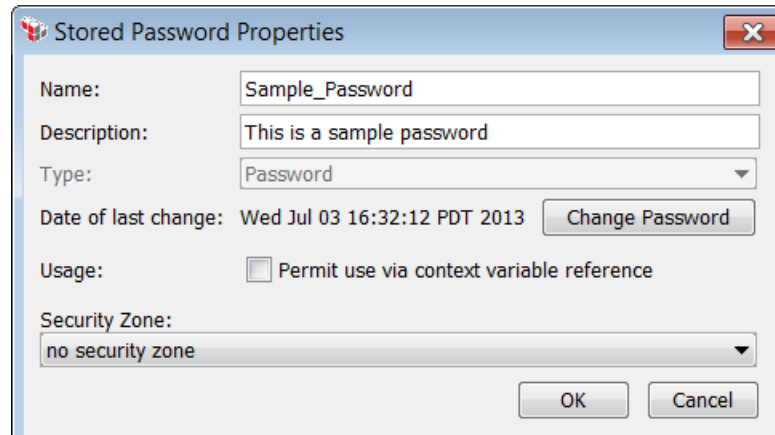


Figure 16: Stored Password Properties - Editing a password

3. Configure the properties as follows:

Table 11: Stored password settings

| Setting  | Description  |
|--|--|
| <b>Name</b>  | Identify the password being stored. You may use letters, numbers, dashes, and underscores.<br><br><b>Note:</b> Names that contain spaces or periods are valid, but the resulting stored password cannot be referenced via context variable.  |
| <b>Description</b>                                       | Optionally enter a description of the password.  |
| <b>Type</b>  | When adding a stored password, choose its type from the drop-down list: <b>Password</b> or <b>PEM Private Key</b> .<br><br>When editing a stored password, the type is display only and cannot be changed.   |
| <b>Password/<br/>Confirm Password</b><br>(Password only) | Enter a password and then retype it to confirm. The <b>[OK]</b> button will become active only when both passwords match.<br><br>When editing a password, the <b>Password/Confirm Password</b> fields appear after you click <b>[Change Password]</b> .  |
| <b>PEM Private Key</b><br>(PEM Private Key only)         | Enter the PEM private key using any of these methods: <ul style="list-style-type: none"> <li>• <b>Automatically generate:</b> Select the <b>Generate</b> check box to have the Policy Manager automatically generate an RSA key and then choose a key size to use. The default key size is <b>2048</b> bits.<br/><br/><b>Note:</b> Certain clients have a minimum size for the server's host key. CA recommends against using RSA key sizes below 1024 bits.<br/><br/><b>Tip:</b> To view the public key, click <b>[View Public Key]</b> when editing this key.</li> </ul> |

| Setting  | Description   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• <b>Paste from another source:</b> Paste the private key directly into the text box.</li> <li>• <b>Load from file:</b> Click <b>[Load From File]</b> to upload a PEM private key.</li> </ul>  |
| <b>Date of last change</b><br>(editing only)     | This displays the date and time when the password was last changed. You can use it to help keep track of password changes.  |
| <b>Change Password</b><br>(editing only)         | Click this to change the password. You will be prompted to enter a new password.  |
| <b>Permit use via context variable reference</b> | <p>Select this check box to allow the password details to be referenced by the <code>\${secpass.*}</code> <a href="#">context variables</a>.</p> <p>Clear this check box to prevent password details from being revealed by the <code>\${secpass.*}</code> context variables.</p> <p><b>Notes:</b> (1) Enable this feature with care, as there is no way to restrict the use of such passwords. (2) This feature is unavailable if the stored password name contains spaces or periods.</p>   |
| <b>View Public Key</b>                           | Click this to view the public key in PEM format, where it can be copied and pasted elsewhere.   |
| <b>Security Zone</b>                             | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> |

4. Click **[OK]** when done.

---

**Note:** If you click **[Cancel]** instead, all changes will be discarded, including any pending password changes.

---

## Managing Password Policy

A password policy defines the rules for password use in the Policy Manager, such as the length of a password, characters that must be included, when the password expires, how often passwords can be reset, etc. The password policy applies to all areas where user passwords are specified, such as when a user account is [created](#), when a password is reset or [changed](#), or when users are asked to reset their passwords at login.

The password policy applies to internal users of the Internal Identity Provider regardless of whether their accounts will be used to authenticate message traffic or for gateway administration.

An administrative user is a person with an account in the Policy Manager that allows them access to the Gateway. Changes to the password policy do not apply to existing administrative users until they change their password. A password reset can be forced using the [Force Administrative Password Reset](#) feature.

In order to manage passwords, you must be assigned either the "Administrator" or the "Manage Password Policies" [role](#). For more information about roles, see "Predefined Roles and Permissions" on page 132.

---

**Note:** If you are not assigned to one of these roles, the menu item to access this feature is unavailable.

---

➤ *To manage password policy:*

1. In the Policy Manager, do *one* of the following:
  - Right click **Internal Identity Provider** in the [\[Identity Providers\] tab](#), and select **Manage Password Policy**.
  - On the Main Menu, select **[Tasks] > Manage Account Policies > Manage Password Policy** (on the [browser client](#), from the **Manage** menu).

The Internal Identity Provider Password Policy dialog displays.

Figure 17: Internal Identity Provider Password Policy dialog

2. Configure this dialog as follows:

Table 12: Managing password policy

| Setting   | Description   |
|---|---|
| <b>Force password change for new user and reset</b> | <p>Select this check box to force a password change upon next login for the following users:</p> <ul style="list-style-type: none"> <li>Administrative user accounts logging on for the first time</li> <li>Administrative user accounts that have had their <a href="#">passwords reset</a> by an administrator</li> </ul> <p>This does not apply when users <a href="#">change their own passwords</a>.</p> <p>When a password is <a href="#">reset</a> by an administrator, or when a <a href="#">new account is created</a>, some password rules are temporarily relaxed. The password itself must satisfy the password requirements; however, the following rules will be temporarily ignored:</p> <ul style="list-style-type: none"> <li>Character difference</li> <li>Password Repeat Frequency</li> </ul> |

| Setting                                       | Description  |
|---|--|
|   | <ul style="list-style-type: none"> <li>Allow One Password Change Per 24 Hours</li> </ul> <p>Selecting the <b>Force password change for new user and reset</b> check box ensures that all password rules are met before users can access the Gateway for administrative purposes.</p> <p>The forced password change will not apply to users who log in with certificates. However, if a certificate is revoked, a password change will be required at the user's next login.</p> <p><b>Tip:</b> To force <i>all</i> administrative users on an Internal Identity provider to reset their passwords, see "Force Administrative Password Reset" on page 53.</p> |
| <b>Minimum Password Length</b>                | <p>Enter the minimum number of characters, between 3 and 128, required for the password.</p> <p><b>Default:</b> 8</p>  |
| <b>Maximum Password Length</b>                | <p>Enter the maximum allowable number of characters for the password. This number must be between 3 and 128.</p> <p><b>Default:</b> 32</p>   |
| <b>Password Repeat Frequency</b>              | <p>Enter the number of times, between 1 and 50, that a new password must be different from the current password. For example, if 10 is selected, the next 10 passwords must be different from the current password.</p> <p><b>Default:</b> 10</p>  |
| <b>Password Expiry</b>                        | <p>Enter the number of days, between 1 and 1825, before the active password expires.</p> <p><b>Default:</b> 90 days</p>  |
| <b>Allow One Password Change Per 24 Hours</b> | <p>Select this check box to limit the number of password changes a user can make to one every 24 hours.</p> <p>Clear this check box to allow a user unlimited password changes within a 24 hour period.</p> <p><b>Note:</b> Users assigned to the Administrator role are exempt from this password rule, so that they can change their password as frequently as they want.</p>  |
| <b>Required Password Characters</b>           | <p>This section lets you specify what characters are allowed in a password and the minimum occurrence of these characters.</p> <p>Select each check box to enforce the rule. When a check box is selected, the minimum value is 1, and the combined maximum of all minimum character requirements is the current value for "Minimum Password Length" to ensure a valid password can be created.</p> <ul style="list-style-type: none"> <li><b>uppercase A-Z:</b> Select this check box to set the number of uppercase letters (A-Z) required for the password. When this check box is selected, the default value of 1 is automatically</li> </ul>           |

| Setting | Description   |
|---------|---|
|         | <p>applied.</p> <p>Clear this check box to not enforce the use of uppercase letters in the password.</p> <ul style="list-style-type: none"> <li>• <b>lowercase a-z:</b> Select this check box to set the number of lowercase letters (a-z) required for the password. When this check box is selected, the default value of 1 is automatically applied.</li> </ul> <p>Clear this check box to not enforce the use of lowercase letters in the password.</p> <ul style="list-style-type: none"> <li>• <b>numbers 0-9:</b> Select this check box to set how many numbers (0-9) are required for the password. When this check box is selected, the default value of 1 is automatically applied.</li> </ul> <p>Clear this check box to not enforce the use of numbers in the password.</p> <ul style="list-style-type: none"> <li>• <b>symbol:</b> Select this check box to set how many symbol characters (!@#\$%^&amp;*-) are required for the password. When this check box is selected, the default value of 1 is automatically applied.</li> </ul> <p>Clear this check box to not enforce the use of symbols in the password.</p> <ul style="list-style-type: none"> <li>• <b>non-numeric:</b> Select this check box to set the minimum number of non-numeric characters (not 0-9). Letters and symbols count. When this check box is selected, the default value of 1 is automatically applied.</li> </ul> <p>Clear this check box to not enforce the use of non-numeric characters in the password.</p> <ul style="list-style-type: none"> <li>• <b>character difference:</b> Select this check box to set the number of physical characters that must be different from the last password. When this check box is selected, the Gateway will reject any new password that does not contain the set number of new characters. For example, if this value is set to "2" and the previous password is "7layer", the Gateway will reject the new password "layer7" but will accept "8player" because it contains a difference of more than two characters.</li> </ul> <p>Clear this check box to not enforce the use of character difference in the password.</p> <ul style="list-style-type: none"> <li>• <b>no repeating characters:</b> Select this check box to disallow repeating characters in a password to prevent a password like 'aaa' being accepted.</li> </ul> <p>Clear this check box to allow the use of repeating characters in the password.</p> <p><b>Note:</b> Default values for these fields come from the STIG minimum settings. For more information, see the Reset to STIG Minimum button.</p> |

| Setting                         | Description  |
|---------------------------------|--|
|                                 | <b>Tip:</b> The total number of required password characters should be less than or equal to the specified minimum password length so that the minimum password can still comply with all the requirements.  |
| <b>Reset to PCI-DSS Minimum</b> | Click this button to quickly reset the password policy to the minimum Payment Card Industry Data Security Standard (PCI DSS) settings as defined by the Payment Card Industry Security Standards Council.  |
| <b>Reset to STIG Minimum</b>    | Click this button to quickly reset the password policy to the minimum Secure Technical Implementation Guide (STIG) settings, as defined by the Defense Information Systems Agency (DISA), a support agency to the United States Department of Defense. |

- Click **[OK]** when done.

## Force Administrative Password Reset

The Force Administrative Passwords Reset feature allows any user assigned the 'Administrator' or 'Manage Internal Users and Groups' [role](#) to force a password reset for all internal administrative users. Internal users created for message traffic authentication will not be affected. For more information on internal users, see "Creating an Internal User" on page 286.

This feature allows you to enforce a new password policy or forces administrative users to adopt changes in the existing password policy. For more information, see "Managing Password Policy" on page 48.

---

**Note:** The forced password change will not impact users who log in with certificates. However, if a user certificate is revoked, a password change will be required at next login.

---

➤ *To force a password reset:*

- In the Policy Manager, do *one* of the following:
  - Right click **Internal Identity Provider** in the [\[Identity Providers\] tab](#), and select **Force Administrative Passwords Reset**.
  - On the Main Menu, select **[Tasks] > Manage Account Policies > Force Administrative Passwords Reset** (on the [browser client](#), from the **Manage** menu).

The Force Administrative Passwords Reset dialog displays.

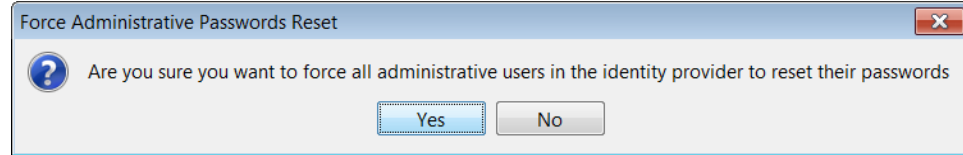


Figure 18: Force Administrative Passwords Reset dialog

2. Click **[Yes]** to confirm the password reset.

## Managing Listen Ports

A *listen port* is a TCP port that "listens" for incoming messages that are then passed to the Gateway message processor. The Manage Listen Ports task lets you define passive listeners, including HTTP(S) and FTP(S). (JMS message polling is handled by the [JMS queuing](#) capabilities of the Gateway, while email listeners are configured using the [Manage Email Listeners](#) task.)

At least one administrative listen port is configured when the Gateway is first set up (see *Gateway Configuration Wizard* in the *Layer 7 Installation and Maintenance Manual*). After this, you use the Manage Listen Ports task to add, modify, or delete ports.

Changes to the listen ports will propagate through a gateway cluster within 30 seconds—new ports will be effective within 30 seconds, while deleted ports should be unavailable after 30 seconds or when the last "keep-alive" connection closes, whichever is later.

### Policy Manager Port Requirements

A listen port for the Policy Manager was defined when the Gateway was configured. If you need to create a new listen port, it must conform to the following characteristics:

- must be above port 1024
- must be SSL
- must not require a client certificate
- must have one of the following options enabled: **[Policy Manager access]** for the standard client, or **[Browser-based administration]** for the [browser client](#); these are set in the [Basic Settings] tab of the [listen port properties](#)

---

**Note:** Configuring listen ports is intended for advanced technical users. The predefined ports should be adequate in most cases. Do not modify these ports unless instructed by CA Technical Support.

---



➤ To manage listen ports:

1. In the Policy Manager, select **[Tasks] > Manage Listen Ports** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Listen Ports dialog appears.

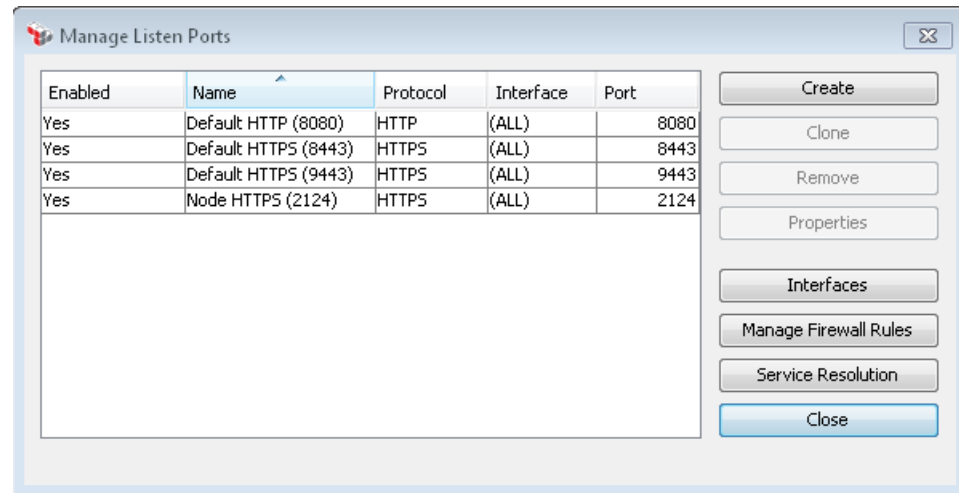


Figure 19: Manage Listen Ports dialog

**Tips:** 1) Listen ports shown in red text indicate a possible conflict with another port. 2) Though the Manage Listen Ports dialog allows you to delete the predefined listen ports, you must ensure that the features are enabled in some other listener to ensure correct Gateway functionality.

2. The following table describes each column (these are set in the listening port's [properties](#)):

Table 13: Listen Ports columns

| Column          | Description   |
|-----------------|---|
| <b>Enabled</b>  | Indicates whether the port is enabled for listening. If disabled, the Gateway will treat the port as if it was removed from the system.<br><br>The listen port is enabled or disabled in the [Basic Settings] tab of the "Listen Port Properties" on page 57.           |
| <b>Name</b>     | The "friendly" name given to the port. This name is used only for logging and display purposes. The name is defined in the [Basic Settings] tab of the "Listen Port Properties" on page 57.   |
| <b>Protocol</b> | Indicates the transport protocol used by the listener. The following protocols are available: <ul style="list-style-type: none"> <li>• <b>HTTP:</b> This is the standard HTTP interface to the Gateway. All available IP addresses are used, over port 8080.</li> </ul> |

| Column           | Description   |
|------------------|---|
|                  | <ul style="list-style-type: none"> <li>• <b>HTTPS:</b> This is the SSL interface to the Gateway, used during mutual authentication. All available IP addresses are used, over port 8443.</li> <li>• <b>HTTPS (no client authentication):</b> This endpoint is the same as the SSL Endpoint without client certificate challenges. All available IP addresses are used, over port 9443.</li> <li>• <b>FTP:</b> This endpoint provides unsecured transport, similar to HTTP.</li> <li>• <b>FTPS:</b> This endpoint provides secured transport, similar to HTTPS.</li> <li>• <b>SSH2:</b> This endpoint provides secured transport via the SSH2 protocol.</li> </ul> <p>The protocols are defined in the [Basic Settings] tab of the "Listen Port Properties" on page 57.</p>                        |
| <b>Interface</b> | Lists the interfaces used by the listen port. This is configured in the [Basic Settings] tab of the "Listen Port Properties" on page 57.  |
| <b>Port</b>      | <p>The port number being monitored. Ports 1 to 1024 are reserved by the Gateway. The port number is specified in the [Basic Settings] tab of the "Listen Port Properties" on page 57.</p> <p><b>Firewall Adjustments on Software Gateways</b></p> <p>If the Policy Manager is connected to a software version of the Gateway (i.e., not an appliance), you must ensure that the firewall protecting the Gateway host machine permits traffic through the ports specified here.</p> <p>For a list of the ports required, consult the file <code>&lt;Gateway_home&gt;/var/firewall_rules</code> on the Gateway machine. This file is a standard Linux firewall configuration file that can be used to automatically adjust the firewall if you are using the Linux RHEL version of the Gateway.</p> |

**Note:** If the Policy Manager will be connecting to the Gateway using a port other than the default 8443, the port number must be appended to the Gateway name. For more information, see "Connecting to the Gateway" on page 8.

3. Select a task to perform:

Table 14: Manage Listen Ports tasks

| To...                                | Do this...   |
|--------------------------------------|--|
| <b>Add a new listen port</b>         | <ol style="list-style-type: none"> <li>1. Click <b>[Create]</b>.</li> <li>2. Complete the <a href="#">Listen Port Properties</a>.</li> </ol> |
| <b>Clone an existing listen port</b> | <ol style="list-style-type: none"> <li>1. Select the port to clone.</li> </ol>   |

| To...   | Do this...  |
|---|---|
|   | <ol style="list-style-type: none"> <li>Click <b>[Clone]</b>.</li> <li>Edit the <a href="#">Listen Port Properties</a> as required.</li> </ol>                       |
| <b>Remove a listen port</b>                         | <ol style="list-style-type: none"> <li>Select the port to remove.</li> <li>Click <b>[Remove]</b>.</li> </ol>  |
| <b>View or edit the properties of a listen port</b> | <ol style="list-style-type: none"> <li>Select the port to view.</li> <li>Click <b>[Properties]</b>. See "Listen Port Properties" on page 57 for details.</li> </ol> |
| <b>Manage interfaces</b>                            | <ul style="list-style-type: none"> <li>Click <b>[Interfaces]</b>. See "Managing Interfaces" on page 76 for details.</li> </ul>                                      |
| <b>Manage Firewall Rules</b>                        | <ul style="list-style-type: none"> <li>Click <b>[Manage Firewall Rules]</b>. See "Managing Interfaces" on page 76 for details.</li> </ul>                           |
| <b>Configure how services are resolved</b>          | <ul style="list-style-type: none"> <li>Click <b>[Service Resolution]</b>. See "Managing Service Resolution" on page 196 for details.</li> </ul>                     |

- Click **[Close]** when done.

---

**Note:** You cannot remove or modify the port currently used to administer the Gateway. To move the admin listener to another port: (1) Create a new admin listener on the new port. (2) Reconnect the Gateway on the new port. (3) Remove the old admin listener.

---

## Listen Port Properties

When creating or viewing details about a [listen port](#), the Listen Port Properties appear. The port properties are organized across these tabs:

- Basic Settings
- SSL/TLS Settings
- Pool Settings
- FTP Settings
- Other Settings
- Advanced

For more information about listen ports, see "Managing Listen Ports" on page 54.

---

**Note:** A listen port will automatically restart when its properties are edited.

---

## Defining FTP Ports

The following are some important details about FTP(S) support in the Gateway:

- Common FTP clients such as FileZilla, FireFTP, WinFTP and WinSCP are supported.
- FTP support is available only in the SOA Gateway. FTP endpoints are not supported in the XML Data Screen, XML Firewall, or XML Accelerator products.
- Only passive FTP is supported.
- The FTP(S) server uses the specified private key for its SSL listener (client certificates not supported); files may only be transferred in binary mode (ASCII/EBCDIC not supported).
- For upload-only FTP requests, the Content-Type is assumed to be "text/xml", while the SOAPAction header is assumed to be empty. For the extended mode, the content type is "application/octet-stream".

➤ *To access the properties for a listen port:*

1. Run the [Manage Listen Ports](#) task.
2. Select a port and then click [**Properties**]. You can also click [**Create**] to enter the properties for a new port. The Listen Port Properties appear.
3. Configure each tab within the properties as necessary. Refer to the appropriate section below for a complete description of each tab.
4. Click [**OK**] when done.

## Configuring the [Basic Settings] Tab

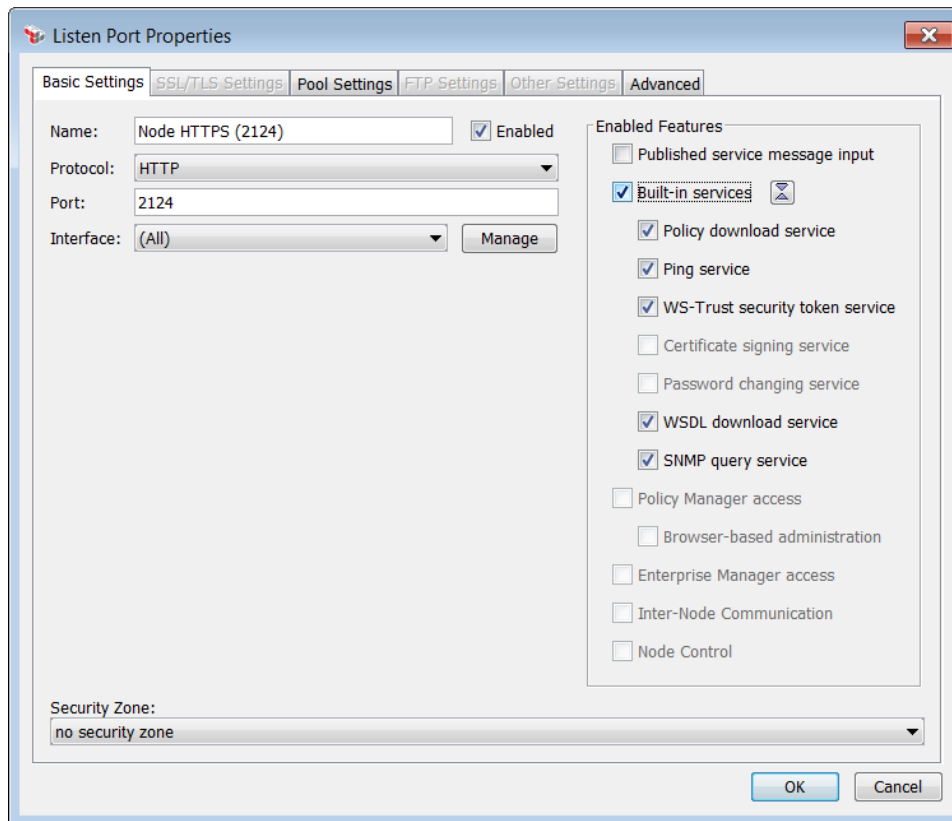




Figure 20: Listen Port Properties - [Basic Settings] tab

This tab configures basic information relevant to all listen ports, regardless of type.

Table 15: Listen Port Basic Settings

| Setting         | Description   |
|-----------------|---|
| <b>Name</b>     | Describe the purpose of the listen port. This "friendly" description is displayed on the <a href="#">Manage Listen Ports</a> dialog.  |
| <b>Enabled</b>  | <p>Select this check box to listen for traffic on the specified port. If the listener is disabled for a port, the Gateway will behave as if no listener had been configured for the port.</p> <p><i>Example:</i> If you disable the listener on port 8080, the system will behave as if there was no listener configured for port 8080. Attempts to connect to that port will result in a "connection refused" error.</p> |
| <b>Protocol</b> | From the drop-down list, select the protocol to be used: <b>HTTP</b> , <b>HTTPS</b> , <b>FTP</b> , <b>FTPS</b> , or <b>SSH2</b> . If custom transport protocols have been added, they are listed here. There is one predefined custom transport protocol <b>I7.raw.tcp</b> .  |

| Setting  | Description   |
|--|---|
| <b>Port</b>  | <p>Enter the TCP port number. For FTP and FTPS, this will be the port number used to open the control connection. The passive data connections will use ports allocated from the FTP passive range configured on the <b>[FTP Settings]</b> tab.</p> <p><b>Note:</b> If the listen port is using the SSH2 protocol, avoid using port 22, as it may conflict with the default SSH port 22 on Linux or Unix systems.</p>   |
| <b>Interface</b>   | <p>From the drop-down list, select an interface or IP address to monitor. The list displays all available IP addresses on the Gateway and interfaces configured using the <b>[Manage]</b> button.</p> <p>To listen on all available addresses, select <b>All</b>.</p>   |
| <b>Manage</b>  | <p>Click <b>[Manage]</b> to add or remove interfaces from the list. For more information, see "Managing Interfaces" on page 76.</p>   |
| <p><i>Enabled Features: This section determines which Gateway services can be accessed through this listen port.</i></p> |   |
| <b>Published service message input</b>   | <p>Allow requests to be submitted to the message processor, where they are resolved to a service and processed by a policy. To learn more about how a request is resolved, see <i>Understanding the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>   |
| <b>Built-in services</b>   | <p>Allows requests to be made to the following built-in services. Use  and  to expand and collapse the list of built-in services.</p> <p>Select the <b>Built-in services</b> check box to enable all applicable services. Clear the check box to disable all the built-in services. <b>Note:</b> A cleared check box may also indicate one or more services has been disabled.</p> <p>You can also enable or disable specific services:</p> <ul style="list-style-type: none"> <li>• <i>Policy download service:</i> used by the Securespan XML VPN Client</li> <li>• <i>Ping service:</i> Used to test Gateway availability. For more information, see <i>Ping URL Test</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</li> <li>• <i>WS-Trust security token service:</i> used by the Securespan XML VPN Client for getting SAML assertions and establishing WS-SecureConversation sessions</li> <li>• <i>Certificate signing (CA) service:</i> used by the Securespan XML VPN Client (only available when the 'Protocol' for the port is set to HTTPS)</li> <li>• <i>Password changing service:</i> used by the Securespan XML VPN Client (only available when the 'Protocol' for the port is set to HTTPS)</li> <li>• <i>WSDL download service:</i> used by the Securespan XML VPN Client and end user programs</li> </ul> |

| Setting                             | Description   |
|-------------------------------------|---|
|                                     | <ul style="list-style-type: none"> <li><i>SNMP query service</i>: HTTP-based SNMP query service that uses localhost as host</li> </ul> <p><b>Note:</b> This option can be suppressed by changing the <a href="#">builtinService.snmpQuery.enabled</a> cluster property.</p>   |
| <b>Policy Manager access</b>        | Allows the desktop client version of the Policy Manager to access the Gateway.  |
| <b>Browser-based administration</b> | <p>Allows the <a href="#">browser client</a> version of the Policy Manager to access the Gateway. This option is available only when <b>[Policy Manager access]</b> is enabled.</p> <p>Enabling browser-based administration also enables the following features:</p> <ul style="list-style-type: none"> <li>ability to back up the Gateway (for more information, see <i>Backing Up the Gateway</i> in the <i>Layer 7 Installation and Maintenance Manual</i>)</li> <li>ability to ping the Gateway (for more information, see <i>Ping URL Test</i> in the <i>Layer 7 Installation and Maintenance Manual</i>)</li> </ul>                      |
| <b>Enterprise Manager access</b>    | <p>Allows the Enterprise Service Manager to access the Gateway.</p> <p>The associated port number must be set in the <i>admin.esmPort</i> cluster property so that the Enterprise Service Manager can communicate with the Gateway cluster. For more information, see "Appendix D: Gateway Cluster Properties" on page 567.</p> <p><b>Note:</b> The <b>Enterprise Manager access</b> check box is available only when the listener uses HTTPS ("Protocol" field in the [Basic Settings] tab) and permits client authentication (The "Client Authentication" field in the [SSL/TLS Settings] tab is set to either "Optional" or "Required").</p> |
| <b>Inter-Node Communication</b>     | Allows communication between nodes and is required for certain administrative functionality, such as <a href="#">viewing logs</a> . If disabled, logs for other nodes in the cluster cannot be viewed.  |
| <b>Node Control</b>                 | <p>Allows each Gateway node in a cluster to be individually stopped/started. If disabled, the Gateway status cannot be retrieved. Node control must be enabled for correct operation of a Gateway appliance.</p> <p><b>Note:</b> The Node Control feature is available only when listening on "(All)" or a loopback/localhost address (for example, "<b>127.0.0.1</b>" or "<b>:::1</b>").</p>   |
| <b>Security Zone</b>                | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "<b>No security zone</b>".</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>   |

## Configuring the [SSL/TLS Settings] Tab

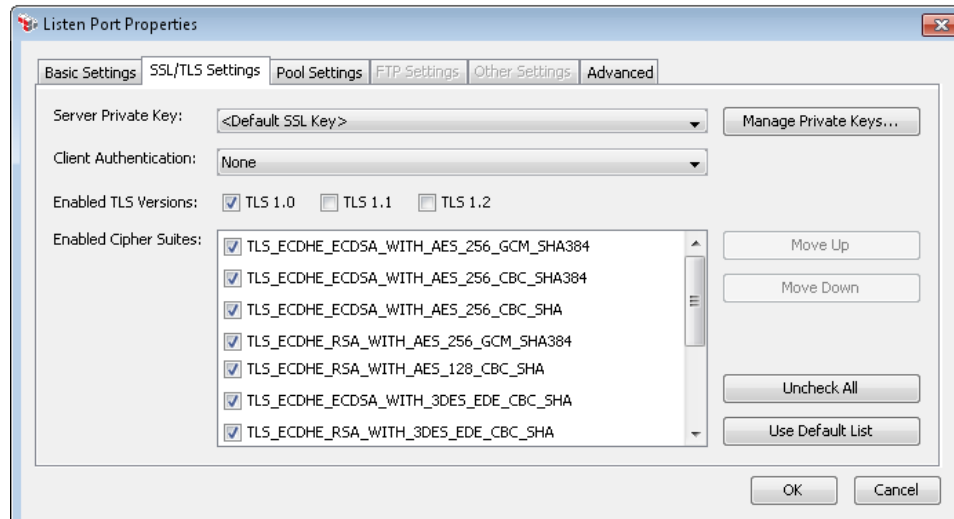


Figure 21: Listen Port Properties - [SSL/TLS Settings] tab

If the listener protocol is HTTPS or FTPS, complete the settings in this tab.

Table 16: Listen Port SSL/TLS Settings

| Setting                      | Description   |
|------------------------------|---|
| <b>Server Private Key</b>    | <p>From the drop-down list, select the server private key to be used for the listen port. An SSL listener can use any private key in the system, from any keystore. If you do not see the appropriate private key, click <b>[Manage Private Keys]</b> to add it. For more information, see "Managing Private Keys" on page 260.</p> <p><b>Note:</b> If the Server Private Key is set to anything other than the default SSL key, then the <b>[Policy Manager access]</b> and <b>[Browser-based administration]</b> options are disabled on the [Basic Settings] tab.</p>  |
| <b>Client Authentication</b> | <p>Specify whether the client must present a certificate to authenticate:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> The client never needs to present a certificate. This setting will not permit login via client certificate when <a href="#">connecting</a> to the Gateway using the desktop client. However this setting will result in fewer security prompts when connecting to the Gateway using the browser client version of the Policy Manager.</li> <li>• <b>Optional:</b> The client can optionally present a certificate. This setting permits login via client certificate when <a href="#">connecting</a> to the Gateway.</li> <li>• <b>Required:</b> The client must always present a certificate to authenticate. With this setting, the <b>[Policy Manager access]</b> and <b>[Browser-based administration]</b> options are disabled on the [Basic Settings] tab.</li> </ul> |



| Setting                      | Description   |
|------------------------------|---|
|                              | The Gateway will accept any client certificate during the SSL handshake, provided that the client holds the corresponding private key.  |
| <b>Enabled TLS Versions</b>  | <p>Select the check box next to the TLS versions to be enabled for the listen port.</p> <p><b>Note:</b> TLS 1.1 and TLS 1.2 are not supported if the Gateway uses either the SafeNet Luna or Sun SCA 6000 as its keystore.</p>  |
| <b>Enabled Cipher Suites</b> | <p>Select the cipher suites that will be enabled on the SSL listen port. During the SSL handshake, both sides negotiate a cipher suite based on what is available on each side and the preference order.</p> <p>If you disable a cipher suite on a listener, the Gateway will never allow it to be selected for use during an SSL handshake using that listener. If the client and server have no other cipher suites in common, the SSL handshake will fail.</p> <p>You can use the <b>[Move Up]</b> and <b>[Move Down]</b> buttons to change a cipher suite's preference by the Gateway if the client and server have more than one cipher suite in common. Cipher suites closer to the top of the list are preferred over those closer to the bottom.</p> <p>The list of ciphers presented may vary, depending on the security configuration of the Gateway. For a list of all the supported cipher suites, see "Selecting Cipher Suites" on page 194.</p> |
| <b>Use Default List</b>      | Click this button to restore the cipher list to the system default preference order and enable state.   |

## Configuring the [Pool Settings] Tab

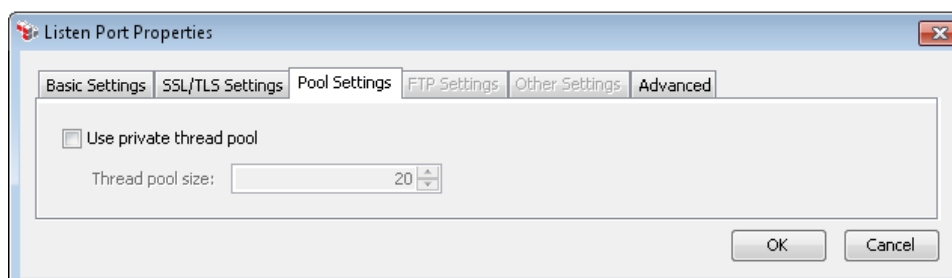


Figure 22: Listen Port Properties - [Pool Settings] tab

This tab allows configuration of the thread pool used by the listener and is enabled only for these protocols: HTTP, HTTPS, or a custom transport protocol. By default, all new listeners use a shared thread pool. You may configure a listener to use a private thread pool if necessary. Private thread pools allow you to separate Gateway resources and

dedicate them to a particular listener. Message processing traffic should use the shared pool, but you could use private pools if you wanted to dedicate resources to particular listeners (perhaps for different users of your services) or for listen ports with high message traffic.

Restrictions caused by using private thread pools include:

- Private threads cannot be used by other listeners, so this is a less flexible approach.
- The Gateway cannot support an unlimited number of threads, so using private pools will require other configuration changes to support this (for example, reduce the shared thread pool size, increase the number of available DB connections, reduce the maximum message size, etc.).

The default node configuration and control listen port 2124 ("Node Control") for the Gateway uses a private thread pool for maximum performance.

Table 17: Listen Port Pool Settings

| Setting                        | Description   |
|--------------------------------|---|
| <b>Use private thread pool</b> | Enable the listener to use a private thread pool.   |
| <b>Thread pool size</b>        | Specify how many threads to allocate to this private pool. The minimum is <b>1</b> and the maximum is <b>10,000</b> (not recommended).<br><br><b>IMPORTANT:</b> If you intend to use a large value for thread pool size, please contact CA Technical Support for additional Gateway configuration changes that may be required. |

## Configuring the [FTP Settings] Tab

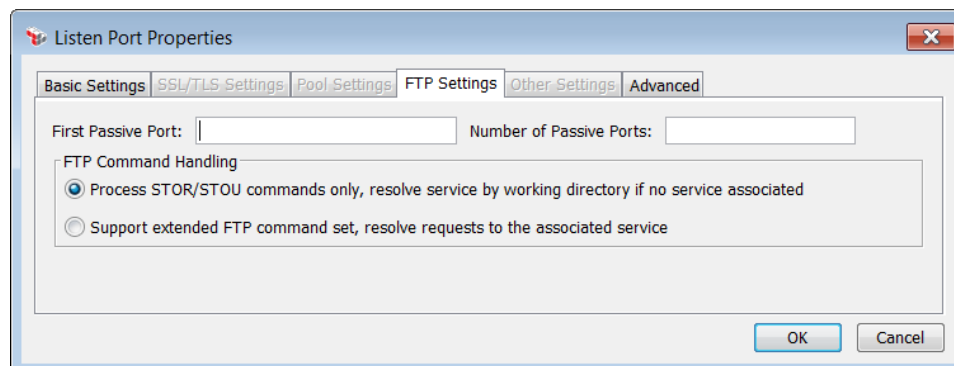


Figure 23: Listen Port Properties - [FTP Settings] tab

If the listener protocol is FTP or FTPS, complete the settings in this tab.

Table 18: Listen Port FTP Settings

| Setting                        | Description  |
|--------------------------------|--|
| <b>First Passive Port</b>      | Specify the first port in the range to use for passive data connections.   |
| <b>Number of Passive Ports</b> | Specify the number of ports in the range to use for passive connections.   |
| <b>FTP Command Handling</b>    | <p>Choose an FTP command handling mode to use. For a detailed description of each mode, see "<a href="#">Understand the FTP Command Handling Modes</a>" below.</p> <p><b>Tip:</b> The default mode is "Process STOR/STOU commands only...", which replicates FTP command handling capability prior to version 8.2.0.</p> |

### Understanding the FTP Command Handling Modes

#### Process STOR/STOU commands only, resolve service by working directory if no service associated

Choose this option if your needs are limited to upload-only FTP command set and handling. This option is best suited to non-interactive upload scenarios. In this mode:

- When a STOR or STOU command is sent, the file will be transferred from the client by the Gateway and is used to create a Request message to a published service.
- PORT, PASS, TYPE, and most other standard connection-related commands will behave as expected.
- Directory navigation commands (such as CWD, CDUP) will always succeed. The Gateway does not confirm the existence of the directory. The client will assume all requested directories exist and that they are empty.
- Other commands may produce unexpected or erroneous results. Because of this, it is recommended that you choose the "Support extended FTP command set..." option if you need to route more than STOR/STOU commands.

#### Support extended FTP command set, resolve requests to the associated service

Choose this option to use the extended FTP command set. This option is intended for use with the Route via FTP(S) Assertion in a FTP proxy scenario. Ensure that a published service is associated with the listen port (defined in the [\[Advanced\] tab](#)).

In this mode, all commands that can be proxied (see Table 19) are processed as requests to the specified service.

Table 19: Commands that can be proxied in the extended FTP command set

| Command | Description  |
|---------|--|
| APPE    | Append a file  |
| CDUP    | Change working directory to parent   |
| CWD     | Change working directory   |
| DELE    | Delete the specified file  |
| LIST    | List the specified file or contents of the specified directory                       |
| MDTM    | Return the last modified time of a specified file over the control connection        |
| MKD     | Make directory   |
| MLSD    | List the details of the files in the specified directory in a standardized format    |
| MLST    | Returns info on the specified file over the control connection                       |
| NLST    | List the names of files in the specified directory                                   |
| NOOP    | No operation   |
| PWD     | Return the working directory over the control connection                             |
| RETR    | Retrieve (i.e., download/get) the specified file                                     |
| RMD     | Remove directory   |
| SIZE    | Returns the size of the file in bytes over the control connection                    |
| STOR    | Store (i.e., upload/put) the specified file in the remote working directory          |
| STOU    | Store (i.e., upload/put) the specified file uniquely in the remote working directory |

**Notes:** (1) The STOU (Store Unique) is not selectable from within the Route via FTP(S) Assertion and will be routed as a STOR command if encountered (for example, in a context variable). (2) A NOOP (No operation) command will be routed if specified in a context variable (for example, the `${request.ftp.command}` variable set by the listen port), but it is not selectable from within the Route via FTP(S) Assertion.

The following commands are accepted by the FTP listen port, but will not be processed as messages by the associated policy:

Table 20: Accepted FTP commands that are not processed as messages

| Command | Description                                      | RFC  | Notes   |
|---------|--|------|---|
| ABOR    | Abort an active file transfer                    | 959  |   |
| AUTH    | Establish authentication/security mechanism      | 2228 |   |
| EPRT    | Specifies extended address & port for connection | 2428 |   |
| EPSV    | Enter extended passive mode                      | 2428 |   |
| FEAT    | List the supported extended features             | 2389 | Content of lists depends on "FTP command handling" mode of listen port  |
| HELP    | Help   | 959  |   |
| LANG    | Language negotiation                             | 2640 | Only English currently supported.   |
| MODE    | Specify transfer mode                            | 959  | 'Streaming' and 'Compressed' only   |
| OPTS    | Select options for a feature                     | 2228 | As 'UTF8' is the listen port server default, the setting 'OPTS UTF8' has no effect.<br>"OPTS MLSD" commands will not affect the format of MLSD results because they are dependent on the settings of the remote FTP server. |
| PASS    | Specify user password                            | 959  | User name and password are not authenticated by the listen port server, but are part of the request made to the associated service, so they may be authenticated there.   |
| PASV    | Enter passive mode                               | 959  |   |
| PBSZ    | Protection buffer size                           | 2228 | Supports PBSZ 0 only.   |
| PORT    | Specify address and port to connect to           | 959  |   |
| PROT    | Set Data Channel Protection Level                | 2228 | Supports 'Clear' and 'Private'.   |
| QUIT    | Disconnect                                       | 959  |   |
| REIN    | Reinitialize user connection                     | 959  |   |
| STAT    | Returns the current status                       | 959  | Listen port server only; does not reflect the status of the remote FTP server   |

Table 20: Accepted FTP commands that are not processed as messages

| Command | Description                 | RFC | Notes   |
|---------|-----------------------------|-----|---|
| STRU    | Set file transfer structure | 959 | File structure only   |
| SYST    | Return system type          | 959 | Corresponds to "os.name" Java system property of the Gateway.   |
| TYPE    | Set the transfer mode       | 959 | Will accept Binary and ASCII options, but routed transfer commands will fail if not set to Binary.  |
| USER    | Authentication username     | 959 | User name and password are not authenticated by the listen port server, but are part of the request made to the associated service, so they may be authenticated there. |

## Unsupported FTP Commands

The following commands are currently not supported:

Table 21: Unsupported FTP commands

| Command | Description                        | RFC  |
|---------|------------------------------------|------|
| ACCT    | Account information                | 959  |
| ALLO    | Allocate disk space                | 959  |
| CCC     | Clear command channel              | 2228 |
| ADAT    | Authentication/Security mechanism  | 2228 |
| CONF    | Confidentiality protection command | 2228 |
| ENC     | Privacy protected command          | 2228 |
| MIC     | Integrity protected command        | 2228 |
| LPRT    | Specify long address & port        | 1639 |
| LPSV    | Enter long passive mode            | 1639 |
| REST    | Restart file transfer              | 3659 |
| RNFR    | Rename from                        | 959  |
| RNTO    | Rename to                          | 959  |
| SITE    | Issue site-specific commands       | 959  |
| SMNT    | Mount file structure               | 959  |

Table 21: Unsupported FTP commands

| Command | Description                          | RFC |
|---------|--------------------------------------|-----|
| X***    | All <a href="#">RFC 775</a> commands | 775 |

### Example: How to Configure an Extended FTP Command Support Proxy

The following example shows how to use the extended FTP commands along with the listen ports and Route via FTP(S) Assertion. This configuration is compatible with FileZilla, FireFTP, WinFTP and WinSCP clients.

#### Precondition:

- A configured remote FTP server
- A service policy that includes the Route via FTP(S) Assertion configured to route to the remote FTP server with the relevant host, security and port settings.

#### ➤ To configure an extended FTP command support proxy:

1. Complete the [Basic Settings] tab of the Listen Port Properties.
2. Complete the [FTP Settings] tab of the Listen Port Properties. Be sure to choose the "Support extended FTP..." option.
3. Complete the [Advanced] tab of the Listen Port Properties as follows:
  - a. If you need to support large uploads (>2GB), select the "Override maximum message size" check box and specify a new limit or allow unlimited message size.
  - b. Associate the port with a published service. This is required in order to support the extended FTP command set.
  - c. Configure the Advanced Properties if you wish to override any of the cluster properties for this listen port. The following are the available FTP-related advanced properties, shown with their default values:

```
ftp.sessionIdleTimeout=60
ftp.maxRequestProcessingThreads=10
ftp.anonymousLoginsEnabled=true
ftp.maxAnonymousLogins=10
ftp.maxConcurrentLogins=10
ftp.userMaxConcurrentLogins=10
ftp.userMaxConcurrentLoginsPerIp=10
```

For a description of these properties, see "FTP Cluster Properties" on page 582.

4. Construct a service policy. The following example shows how to use the extended FTP commands along with the listen ports and the Route via FTP(S) Assertion. In this example, the credentials supplied by the FTP client will be used for authenticating the connection to the remote FTP server:

*Require FTP Credentials*

*Request: Configure Message Streaming: enable streaming*

*Route via FTPS Server*

---

**Note:** The Configure Message Streaming Assertion allows the transparent uploading of files and more accurate progress monitors in FTP clients. Omitting this assertion will slow down the routing of most (non-trivial) uploads and introduce the potential for timeouts.

---

5. Configure these settings in the [Connection] tab of the FTP(s) Routing Properties as follows:
  - a. Choose "**From Variable**" for the command and then enter **request.ftp.command** for the command variable.
  - b. Enter **\${request.ftp.path}** as the directory.
  - c. Enter **\${request.ftp.argument}** as the argument.
  - d. Choose the assertion outcome "**Never fail as long as target replies**". This setting permits the FTP clients to receive useful responses from the remote FTP server that will (in most cases) indicate reasons for failure (for example, insufficient privileges, incorrectly-formatted arguments).
6. Configure all the remaining settings in the assertion properties as appropriate for your environment. For a description of each setting, see the Route via FTP(S) assertion in the *Layer 7 Policy Authoring User Manual*.

The following is a high level overview of FTP request proxying using the LIST command as an example:

1. The FTP client connects to the Gateway on the designated listen port.
2. The FTP client sends a request to the Gateway to list the contents of the working directory using the FTP command "LIST".
3. The Gateway processes this command and opens a data connection to the FTP client. The FTP request variables are populated.



4. After the user's credentials are extracted by the Require FTP Credentials assertion (if using the credentials from the FTP client for authentication), the Route via FTP (S) assertion reads the values of the FTP request variables to find the command, working directory, and argument. It then connects to the remote server using the extracted credentials.
5. The Route via FTP(S) Assertion issues the LIST command to the remote server and receives the listing, which it uses to create a response message. The FTP response variables are populated.
6. The response message body is transferred to the FTP client over the data connection, which is closed when the transfer is complete. The reply code and text from the remote FTP server is sent to the FTP client over the control connection.

### Configuring the [Other Settings] Tab

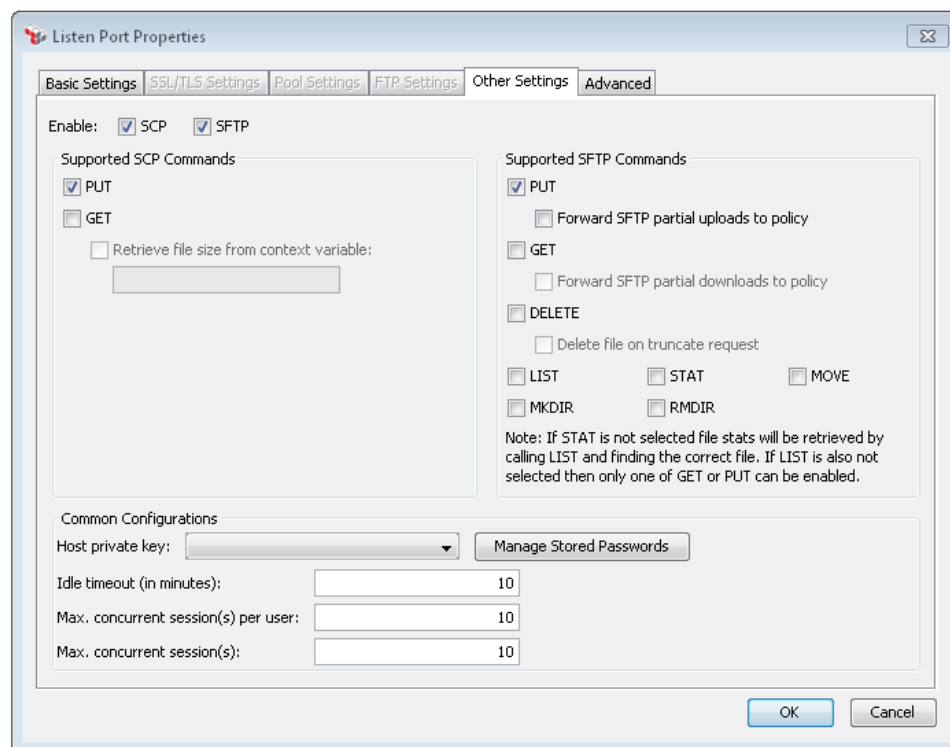



Figure 24: Listen Port Properties - [Other Settings] tab

This tab is available when either SSH2 or a custom transport protocol has been selected on the [Basic Settings] tab. If SSH2 was selected, the following fields display.

Table 22: Listen Port - Other Settings

| Setting                        | Description   |
|--------------------------------|---|
| <b>Enable</b>                  | Select the network protocol(s) to support on the SSH2 server. Both SCP and SFTP are enabled by default..  |
| <i>Supported SCP Commands</i>  |   |
| <b>PUT</b>                     | Select this option to allow SCP clients to upload files.  |
| <b>GET</b>                     | <p>Select this option to allow the file to be sent back to the SCP client.</p> <ul style="list-style-type: none"> <li><i>Retrieve file size from context variable:</i> Select this option to retrieve the file size from the specified <a href="#">context variable</a>. Clear this check box to not retrieve the file size from a context variable. In this case, the entire message stream will need to be read in order to detect the file size. </li> </ul> |
| <i>Supported SFTP Commands</i> |   |
| <b>PUT</b>                     | <p>Select this option to allow SFTP clients to upload files.</p> <ul style="list-style-type: none"> <li><i>Forward SFTP partial uploads to policy:</i> Select this option to allow uploading files in parts. This will execute policy once for every file partially uploaded. Clear this check box to not allow partial uploads.</li> </ul>   |
| <b>GET</b>                     | <p>Select this option to allow SFTP clients to download files.</p> <ul style="list-style-type: none"> <li><i>Forward SFTP partial downloads to policy:</i> Select this option to allow downloading files in parts. This will execute policy once for every file partially downloaded. Clear this check box to not allow partial downloads.</li> </ul>   |
| <b>LIST</b>                    | Select this option to allow SFTP clients to list files. When the SFTP client sends the LIST command, the policy will be called with the LIST set as the request.command.type.   |
| <b>STAT</b>                    | <p>Select this option to retrieve the file attributes for the file specified. When the SFTP client sends the STAT command, the policy will be called with the STAT set as the request.command.type.</p> <p><b>Note:</b> You must enable STAT or LIST to be able to upload and download files. If both are disabled, only one of GET or PUT can be enabled. In this case dummy file statistics will be returned to the SFTP client.</p>  |
| <b>DELETE</b>                  | <p>Select this option to retrieve the file attributes for the file specified.</p> <ul style="list-style-type: none"> <li><i>Delete file on truncate request:</i> Select this optional check box if you have selected "Forward SFTP partial uploads" under <b>PUT</b>. In most cases the files are automatically truncated before they are overwritten. Clear this check box to retain the file on truncated requests.</li> </ul>  |
| <b>MOVE</b>                    | Select this option to allow SFTP clients to move or rename the files.   |

| Setting                                     | Description   |
|---|---|
| <b>MKDIR</b>                                | Select this option to allow SFTP clients to create directories.   |
| <b>RMDIR</b>                                | Select this option to allow SFTP clients to remove directories.   |
| <i>Common Configurations</i>                |   |
| <b>Host private key type</b>                | Click <b>[Manage Stored Passwords]</b> to enter a private key for the SSH2 server. For more information, see "Managing Stored Passwords" on page 42. This field is required.  |
| <b>Idle timeout (in minutes)</b>            | Enter the number of minutes for the idle timeout. This field is required.<br>The default is <b>10</b> minutes.  |
| <b>Max. concurrent session(s) per user:</b> | Enter how many concurrent sessions are permitted for a user. A value of <b>"0"</b> (zero) means unlimited. The default is <b>10</b> .<br><b>Note:</b> The concurrent sessions allowed for a user is limited by the maximum number of concurrent sessions permitted (see the following setting). |
| <b>Max. concurrent session(s):</b>          | Enter the total maximum number of concurrent sessions permitted. A value of <b>"0"</b> (zero) means unlimited. The default is <b>10</b> .   |

If a custom transport protocol was selected, the contents of this tab will depend on the protocol. For the "l7.raw.tcp" transport protocol, the following field is shown:

- **Socket timeout:** Enter the period of time before the socket times out, in milliseconds.

## Configuring the [Advanced] Tab

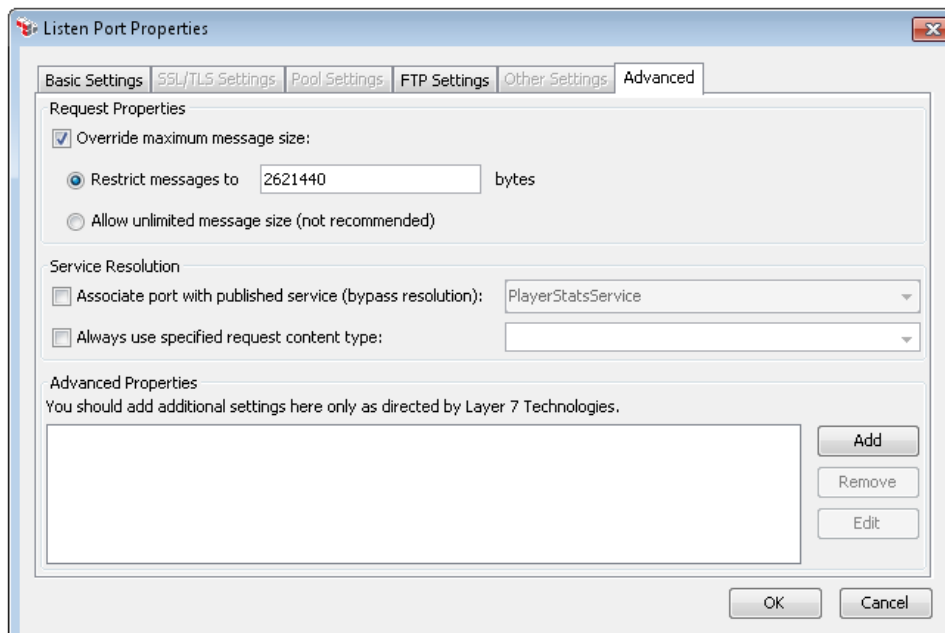



Figure 25: Listen Port Properties - [Advanced] tab

This tab is used to define advanced settings for the listen port. In particular, it is recommended that only advanced technical users modify the Advanced Properties table.

Table 23: Listen Port - Advanced Settings

| Setting   | Description  |
|---|--|
| <i>Request Properties</i>   |  |
| <b>Override maximum message size</b>  | <p>Select this check box to override the permitted maximum size of the routing message. Clear this check box to use the value set in the <a href="#">io.xmlPartMaxBytes</a> cluster property.</p> <ul style="list-style-type: none"> <li><i>Restrict messages to:</i> Enter the maximum permitted size of the request message, in bytes. You may reference context variables. </li> <li><i>Allow unlimited message size (not recommended):</i> Select this option to allow response messages of unlimited size. This is not recommended and should be used only under the direction of CA Technical Support.</li> </ul> |
| <p><i>Service Resolution:</i> The settings under "Service Resolution" are available for all types of transport, predefined or custom. These two settings are designed for transports that do not communicate information that are necessary for correct operation of the listen port.</p> |  |

| Setting   | Description  |
|---|--|
| <b>Associate port with single published service</b> | Select this option to pre-select a published service for the listen port. Any message arriving via this listen port will be routed immediately to the specified published service. Choose the service to use from the drop-down list. For more information about published services, see "Working with SOAP Web Services" on page 331. |
| <b>Always use specified request content type</b>    | Select this option to pre-select a Content-Type for the listen port. Choose the Content-Type to use from the drop-down list or type a valid Content-Type.  |

### Advanced Properties

This section is used to define additional settings for the listen port. You will be directed by CA Technical Support when such properties are required.

The following are some examples for advanced properties:

- The Advanced Properties can be used to obfuscate the default server for the Gateway's HTTP listener. For example, the response returns "Apache-Coyote/1.1", which is the Tomcat default server. To minimize information disclosure, add the advanced property **server** = <value>. For example, adding the property **server** with the value **foobar** will replace "Apache-Coyote/1.1" with "foobar" in the "Server" heading in the response.
- If you need to allow renegotiations, add the advanced property *allowUnsafeLegacyRenegotiation* = *true*. This suppresses the application-level disablement of renegotiation and allows the underlying JSSE provider to handle it. **Tip:** Setting this advanced property will not introduce any security vulnerabilities with current JDK versions.
- By default, the Gateway truncates any space between the Content-Type and the charset in the response header. To prevent this, add the advanced property *trimContentType* = *false*. **Note:** This does not affect the outbound request headers, where truncation does not occur.
- You can override the default FTP(S) listen port behavior for a specific listen port, by using the following advanced properties

```
ftp.sessionIdleTimeout
ftp.maxRequestProcessingThreads
ftp.anonymousLoginsEnabled
ftp.maxAnonymousLogins
ftp.maxConcurrentLogins
ftp.userMaxConcurrentLogins
ftp.userMaxConcurrentLoginsPerIp
```

These properties match their corresponding FTP cluster property counterparts. For more information about these properties, see "FTP Cluster Properties" on page 582.

- By default, the maximum number of headers that can be retrieved in a single GET call is 100. If you need to retrieve a greater number, add the advanced property *maxHeaderCount* = <new maximum value>.

---

**Note:** If *ftp.maxRequestProcessingThreads* is set to '0' (zero) and *ftp.maxConcurrentLogins* is set to unlimited, the Gateway will use the default thread number of 10. However, if *ftp.maxRequestProcessingThreads* is zero and *ftp.maxConcurrentLogins* has a fixed value, then the maximum number of threads created will be equal to the value of *ftp.maxConcurrentLogins*.

---

## Managing Interfaces

The *Managing Interfaces* task is used to configure interfaces that can be monitored by a [listen port](#). Defining an interface gives you greater control over the IP addresses that will be monitored—you can specify multiple IP address patterns—and you can name an interface to make it easier to identify. For example, you can define that:

- listen ports tagged with "external" will monitor the IP address 192.168.1.77
- listen ports tagged with "internal" will monitor the IP range 10.48.20, 192.168/16, 208
- listen ports tagged with "loopback" will monitor 127.0.0.1

If you do not create interfaces, then you can still choose any single IP address or choose to monitor all addresses for a given protocol in a [listen port's properties](#).

---

**Note:** Configuring interfaces is an advanced feature. Please consult your system administrator or CA Technical Support on the need to change existing interfaces or create new ones.

---

➤ *To manage interfaces:*

1. Do one of the following:
  - Run the [Manage Listen Ports](#) task and then click **[Interfaces]** on the Manage Listen Ports dialog.
  - Open the [Listen Port Properties](#) for a specific port and then click **[Manage]** on the **[Basic Settings]** tab.

The Manage Interfaces dialog is displayed.

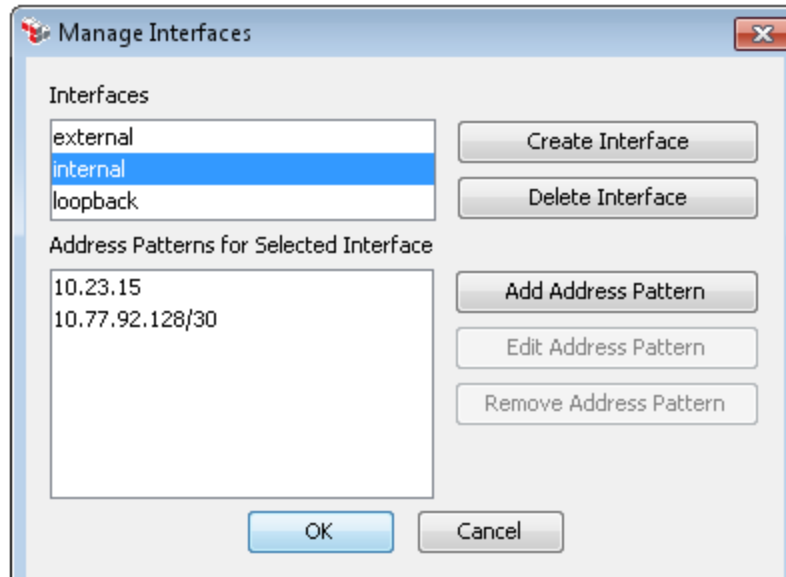


Figure 26: Managing Interfaces dialog

2. Select an action from the following table.

Table 24: Manage Interfaces tasks

| To...  | Do this...   |
|--|--|
| <b>Create a new interface</b>                    | <ol style="list-style-type: none"> <li>1. Click <b>[Create Interface]</b>.</li> <li>2. Type a name for the interface. The name must begin with either a letter or an underscore "_" character.</li> <li>3. Click <b>[OK]</b> to add the tag.</li> <li>4. Add one or more IP address patterns. An interface must have at least one IP address or address range associated with it.</li> </ol>   |
| <b>Delete an interface</b>                       | <ol style="list-style-type: none"> <li>1. From the <b>Interfaces</b> list, select the interface to delete. This interface must not currently be used by any listen port.</li> <li>2. Click <b>[Delete Interface]</b>. The interface and its address patterns are removed from the list.</li> </ol>   |
| <b>Add an IP address pattern to an interface</b> | <ol style="list-style-type: none"> <li>1. From the <b>Interfaces</b> list, select the interface to edit.</li> <li>2. Click <b>[Add Address Pattern]</b>.</li> <li>3. Enter the IP address pattern. <ul style="list-style-type: none"> <li>• The pattern is an IP address followed by an optional netmask specifier.</li> <li>• The netmask specifier is indicated with a forward slash followed by a number between 0 and 32 (inclusive).<br/><i>Example:</i> 10.77.92.128/30</li> <li>• Both IPv4 and IPv6 addresses are accepted.</li> </ul> </li> <li>4. Click <b>[OK]</b> to add the pattern.</li> </ol> |

| To...   | Do this...  |
|---|---|
|   | <p>Repeat steps 2 to 4 to enter additional address patterns for the interface.</p> <p><b>Note:</b> The Policy Manager will allow you to enter any address pattern. If a nonexistent address is entered and then associated with a listen port, the listen port will not be opened. If the address pattern matches multiple IP addresses, the listen port will be opened only for the numerically lowest matching address on each host. In both cases, the appropriate error or warning messages will be logged.</p> |
| <b>Edit an IP address pattern for an interface</b>    | <ol style="list-style-type: none"> <li>1. From the <b>Interfaces</b> list, select the interface.</li> <li>2. From the list of addresses, select the pattern to edit.</li> <li>3. Click <b>[Edit Address Pattern]</b>.</li> <li>4. Modify the IP address pattern.</li> <li>5. Click <b>[OK]</b> to save the changes.</li> </ol>  |
| <b>Remove an IP address pattern from an interface</b> | <ol style="list-style-type: none"> <li>1. From the <b>Interfaces</b> list, select the interface to edit.</li> <li>2. From the list of addresses, select the pattern to remove.</li> <li>3. Click <b>[Remove Address Pattern]</b>.</li> </ol>  |

3. Click **[OK]** when done.

---

**Note:** Any changes to an interface will cause all affected listeners to restart. This is the same as editing a listener's [properties](#).

---

## Managing Firewall Rules

The *Manage Firewall Rules* task lets you manage the list of existing firewall rules as well as create, clone, edit, and remove them.

➤ *To manage firewall rules:*

1. In the Policy Manager, select **[Tasks] > Manage Listen Ports** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). Select **Manage Firewall Rules** button. The Manage Firewall Rules dialog appears.



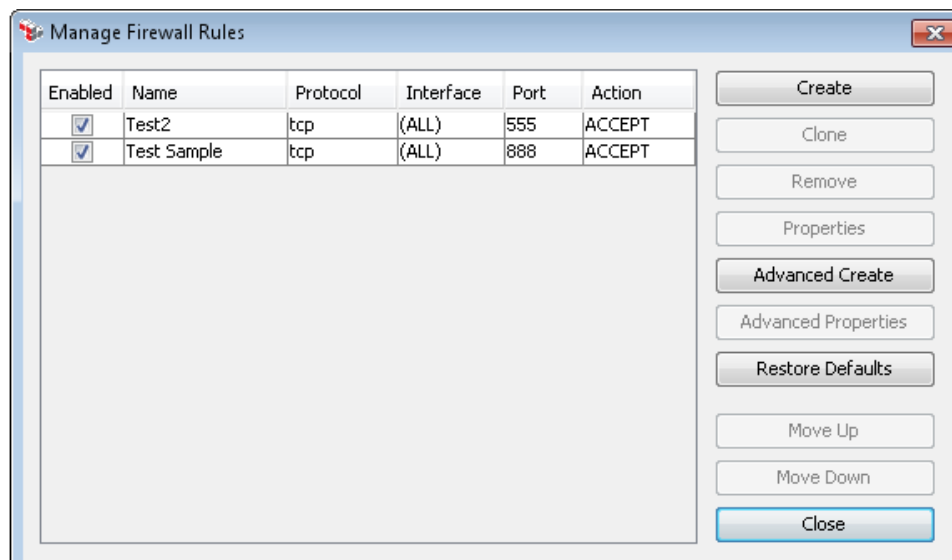


Figure 27: Manage Firewall Rules dialog

2. The following table describes each column (these are set in the firewall rule's [properties](#)):

Table 25: Manage Firewall columns

| Column           | Description  |
|------------------|--|
| <b>Enabled</b>   | Indicates whether the rule is enabled or not.  |
| <b>Name</b>      | The "friendly" name given to the rule. This name is used only for logging and display purposes.  |
| <b>Protocol</b>  | <p>Select the transport protocol associated with the rule from the drop-down menu. The following protocols are available:</p> <ul style="list-style-type: none"> <li>• <b>TCP</b></li> <li>• <b>UDP</b></li> <li>• <b>ICMP</b> (This protocol is only available via the "Advanced Properties" on page 80 settings.)</li> </ul>   |
| <b>Interface</b> | Lists the interfaces bound by the rule.  |
| <b>Port</b>      | <p>The port number associated with the rule. The port number must be between 1 and 65535 (inclusive).</p> <p><b>Firewall Adjustments on Software Gateways</b></p> <p>If the Policy Manager is connected to a software version of the Gateway (i.e., not an appliance), you must ensure that the firewall protecting the Gateway host machine permits traffic through the ports specified here.</p> <p>For a list of the ports required, consult the file <code>&lt;Gateway_home&gt;/var/firewall_rules</code> on the Gateway machine. This file is a</p> |

| Column | Description  |
|--------|--|
|        | standard Linux firewall configuration file that can be used to automatically adjust the firewall if you are using the Linux RHEL version of the Gateway. |
| Action | This is the rule action. See "Managing Interfaces" on page 76 for details.   |

### 3. Select a task to perform:

Table 26: Manage Listen Ports tasks

| To...   | Do this...   |
|---|--|
| <b>Add a new firewall rule</b>                        | <ol style="list-style-type: none"> <li>1. Click <b>[Create]</b>.</li> <li>2. Complete the "Firewall Rule Properties" on page 81.</li> </ol>  |
| <b>Clone an existing firewall rule</b>                | <ol style="list-style-type: none"> <li>1. Select the rule to clone.</li> <li>2. Click <b>[Clone]</b>.</li> <li>3. Edit the "Firewall Rule Properties" on page 81 as required.</li> </ol>   |
| <b>Remove a firewall rule</b>                         | <ol style="list-style-type: none"> <li>1. Select the rule to remove.</li> <li>2. Click <b>[Remove]</b>.</li> <li>3. Click <b>[Yes]</b> to confirm removal of the rule.</li> </ol>  |
| <b>View or edit the properties of a firewall rule</b> | <ol style="list-style-type: none"> <li>1. Select the rule to view.</li> <li>2. Click <b>[Properties]</b>.</li> <li>3. Edit the "Firewall Rule Properties" on page 81 as required.</li> </ol>   |
| <b>Create an advanced firewall rule</b>               | <ol style="list-style-type: none"> <li>1. Click <b>[Advanced Create]</b>.</li> <li>2. Click <b>[OK]</b>. View "Firewall Rule Properties" on page 81 for details.</li> </ol>  |
| <b>Advanced Properties</b>                            | <ol style="list-style-type: none"> <li>1. Select the rule to view.</li> <li>2. Click <b>[Advanced Properties]</b>. View "Firewall Rule Properties" on page 81 for details.</li> </ol>  |
| <b>Restore Defaults</b>                               | <p>Click <b>[Restore Defaults]</b> to restore to the default firewall rules of the Gateway appliance.</p> <p><b>Note:</b> This option only clears the custom added rules.</p>  |
| <b>Reorder the list of rules</b>                      | <p>Select a firewall rule and then click <b>[Move Up]</b> or <b>[Move Down]</b> to reorder the list of rules. The rules within each action type (Accept/Redirect/Drop) will be applied sequentially, in a top-to-bottom order. Moving the rule to the top will execute it first in the action group. Moving the rule down will make it apply later in that action group.</p> |

### 4. Click **[Close]** to exit the dialog box.

## Firewall Rule Properties

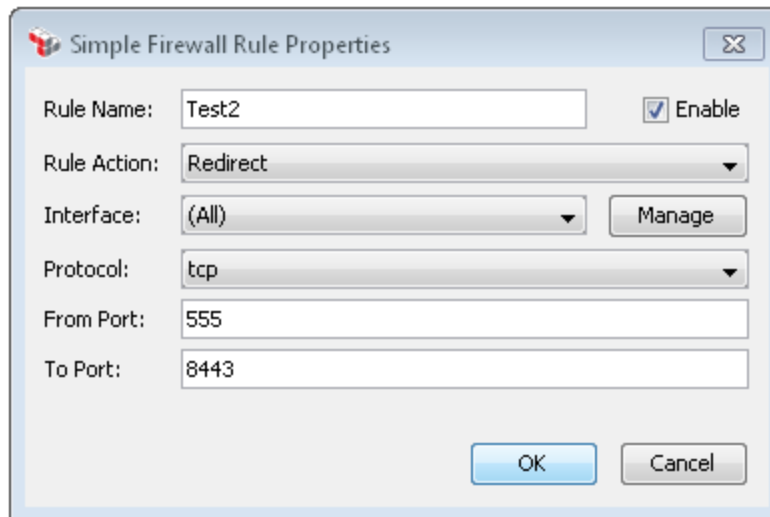
*Firewall Rule Properties* allows you to configure specific properties in handling inbound and outbound traffic. Ports can be configured as a firewall entry to allow inbound traffic as well as redirecting traffic from one port to another.

For more information about firewall rules, see "Managing Firewall Rules" on page 78.

➤ To access the properties for a firewall rule:

1. Run the [Manage Listen Ports](#) task.
2. Click **[Manage Firewall Rules]**.
3. Click **[Create]**. The Simple Firewall Rule Properties appear.
4. Click **[OK]** when done.

## Configuring the Simple Firewall Rule Properties



The dialog box titled "Simple Firewall Rule Properties" contains the following fields and controls:

- Rule Name:** Text input field containing "Test2".
- Enable:** Checkmark icon.
- Rule Action:** Drop-down menu showing "Redirect".
- Interface:** Drop-down menu showing "(All)".
- Manage:** Button next to the Interface drop-down.
- Protocol:** Drop-down menu showing "tcp".
- From Port:** Text input field containing "555".
- To Port:** Text input field containing "8443".
- OK:** Button at the bottom right.
- Cancel:** Button at the bottom right.

Figure 28: Simple Firewall Rule Properties

You can create a firewall rule by using the Simple Firewall Rule Properties dialog.

Table 27: Simple Firewall Rule settings

| Setting            | Description   |
|--------------------|---|
| <b>Rule Name</b>   | Enter a name for the firewall rule. This "friendly" description is displayed on the <a href="#">Manage Listen Ports</a> dialog.   |
| <b>Rule Action</b> | Select the action for the rule from the drop-down menu: <ul style="list-style-type: none"> <li><b>Accept:</b> Choose this option to allow the traffic through.</li> </ul> |

| Setting          | Description   |
|------------------|---|
|                  | <ul style="list-style-type: none"> <li><b>Redirect:</b> Choose this option to redirect the traffic from a destination port to a different port.</li> </ul>  |
| <b>Interface</b> | <p>From the drop-down list, select an interface or IP address to monitor. The list displays all available IP addresses on the Gateway and interfaces configured using the <b>[Manage]</b> button.</p> <p>To listen on all available addresses, select <b>All</b>.</p> |
| <b>Protocol</b>  | Select the protocol from the drop-down list.  |
| <b>From Port</b> | The port number associated with the rule. The port number must be between 1 and 65535 (inclusive).  |
| <b>To Port</b>   | This field is only enabled when "Redirect" is selected in the "Rule Action" drop-down menu. The port number must be between 1 and 65535 (inclusive).  |

## Configuring the Advanced Firewall Rule Properties

You can add more specific definitions to the firewall rules through the Advanced Firewall Rule Properties.

## Managing JDBC Connections

JDBC connections allow the Gateway to query external databases and then use the query results during policy consumption. Use the *Manage JDBC Connections* task to create, edit, remove, or test a JDBC connection.

➤ *To manage JDBC connections:*

1. In the Policy Manager, select **[Tasks] > Manage JDBC Connection** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage JDBC Connection dialog appears.

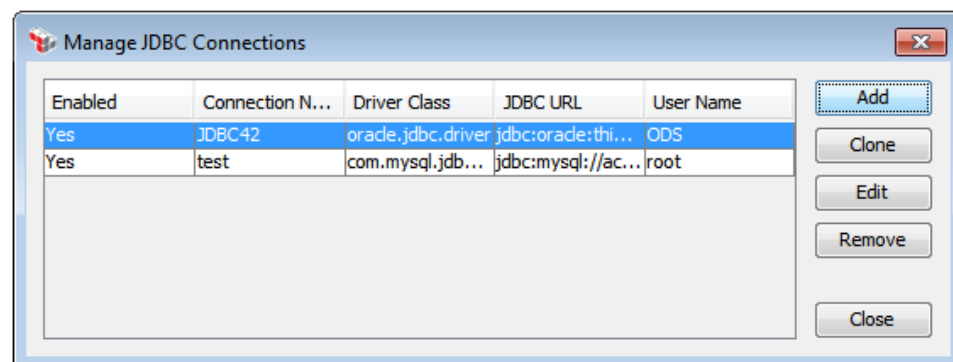


Figure 30: Manage JDBC Connection dialog

- The JDBC connections that have been configured are displayed. Choose an action to perform:

Table 29: Managing JDBC connections tasks

| To...                                    | Do this...   |
|--|--|
| <b>Create a new JDBC connection</b>      | <ol style="list-style-type: none"> <li>Click <b>[Add]</b>. The JDBC Connection Properties appear.</li> <li>Complete the properties for the connection. For a description of each property, see "JDBC Connection Properties" on page 83.</li> </ol> |
| <b>Clone an existing JDBC connection</b> | <ol style="list-style-type: none"> <li>Select the connection to copy.</li> <li>Click <b>[Clone]</b>.</li> <li>Edit the properties as required. For a description of each property, see "JDBC Connection Properties" on page 83.</li> </ol>         |
| <b>Edit a JDBC connection</b>            | <ol style="list-style-type: none"> <li>Select the connection to view or edit.</li> <li>Click <b>Properties</b>. The <b>JDBC Connection Properties</b> are displayed.</li> <li>Edit the properties as required.</li> </ol>                          |
| <b>Remove a JDBC connection</b>          | <ol style="list-style-type: none"> <li>Select the connection to remove.</li> <li>Click <b>Remove</b>. The JDBC connection is removed from the list.</li> </ol>   |

- Click **[Close]** when done.

## JDBC Connection Properties

When creating or viewing details about a [JDBC connection](#), the JDBC Connection Properties appear.

---

**Note:** Failover protection will be in effect only if there are two or more database servers on the JDBC connection set to switch upon failure, and if the JDBC driver provides failover capabilities.

---

## Understanding the Driver Classes

By default, the following driver classes are white-listed for support by the CA API Gateway.

---

**Tip:** For more details on the databases supported by each driver class, refer to the Progress DataDirect data sheet at this location:

<http://www.datadirect.com/~media/DataDirect/Documents/JDBC/DataSheets/dd-for-jdbc.pdf>.

---

Table 30: JDBC driver classes

| <b>DB2</b>              |   |
|-------------------------|---|
| <b>Description</b>      | Supports IBM DB2 DB   |
| <b>Driver class</b>     | com.l7tech.jdbc.db2.DB2Driver   |
| <b>URL</b>              | jdbc:l7tech:db2://hostname:port;DatabaseName=value[:property=value[:...]]   |
| <b>Examples</b>         | jdbc:l7tech:db2://10.0.0.1:50000;DatabaseName=SAMPLE<br>jdbc:l7tech:db2://10.0.0.1:50000;Database=SAMPLE;User=test;Password=secret  |
| <b>MySQL Enterprise</b> |   |
| <b>Description</b>      | Supports MySQL Enterprise Edition   |
| <b>Driver class</b>     | com.l7tech.jdbc.mysql.MySQLDriver   |
| <b>URL</b>              | jdbc:l7tech:mysql://hostname:[port];DatabaseName=value[:property=value[:...]]   |
| <b>Examples</b>         | jdbc:l7tech:mysql://localhost:3306;DatabaseName=test<br>jdbc:l7tech:mysql://10.0.0.1:3306;Database=test;User=test;Password=secret   |
| <b>MS SQL Server</b>    |   |
| <b>Description</b>      | Supports Microsoft SQL Server   |
| <b>Driver class</b>     | com.l7tech.jdbc.sqlserver.SQLServerDriver   |
| <b>URL</b>              | jdbc:l7tech:sqlserver://hostname:port;DatabaseName=value[:property=value[:...]]   |
| <b>Examples</b>         | jdbc:l7tech:sqlserver://10.0.0.1:1433;DatabaseName=test<br>jdbc:l7tech:sqlserver://10.0.0.1:1433;Database=test;User=test;Password=secret  |
| <b>Special note</b>     | For Microsoft MS SQL server, the JDBC driver requires "Bouncy Castle" to be the JCE provider. To use this, set the following system property:<br><b>com.l7tech.common.security.jceProviderEngineName=bc</b><br>A Gateway restart is required. For more information, see "System Properties" in the <i>Layer 7 Installation and Maintenance Manual</i> . |
| <b>MySQL Community</b>  |   |
| <b>Description</b>      | Supports MySQL Community Edition  |
| <b>Driver class</b>     | com.mysql.jdbc.Driver   |
| <b>URL</b>              | jdbc:mysql://hostname:[port];<database name>  |

Table 30: JDBC driver classes

|   |   |
|---|---|
| <b>Example</b>  | jdbc:mysql://localhost:3306/test  |
| <b>Oracle</b>   |   |
| <b>Description</b>  | Supports Oracle Database  |
| <b>Driver class</b>   | com.l7tech.jdbc.oracle.OracleDriver   |
| <b>URL</b>  | jdbc:l7tech:oracle://hostname:port;DatabaseName=value[:property=value[:...]]  |
| <b>Example</b>  | jdbc:l7tech:oracle://10.0.0.1:1521;DatabaseName=XE<br>jdbc:l7tech:oracle://10.0.0.1:1521;ServiceName=XE;<br>jdbc:l7tech:oracle://10.0.0.1:1521;SID=XE;User=test;Password=secret |
| <b>Custom JDBC</b>  |   |
| <p>To configure a custom JDBC driver, do the following:</p> <ol style="list-style-type: none"> <li>1. Install the JDBC driver into the <i>lib/ext</i> directory on the Gateway.</li> <li>2. Add the driver to the white list the driver (see below).</li> <li>3. Optionally configure the driver class in the <a href="#">jdbcConnection.driverClass.defaultList</a> cluster property so that it is available in the drop down list of JDBC drivers.</li> </ol> <p>For assistance, please <a href="#">contact</a> CA Technical Support.</p> |   |

## Updating the White List

By default, the following driver classes are white-listed:

```
com.mysql.jdbc.Driver
com.l7tech.jdbc.mysql.MySQLDriver
com.l7tech.jdbc.db2.DB2Driver
com.l7tech.jdbc.oracle.OracleDriver
com.l7tech.jdbc.sqlserver.SQLServerDriver
```

To modify the list of white-listed driver classes, add this system property to *system.properties* with a list of all drivers to be enabled:

```
com.l7tech.server.jdbcDriver = <driver class A>\n<driver class B>\n...<driver class N>
```

All the drivers must be listed in a single line, delimited with "\n".

For more information on setting system properties, see "System Properties" in the *Layer 7 Installation and Maintenance Manual*. Note that a Gateway restart is required for changes to take effect.

---

**Note:** When `com.l7tech.server.jdbcDriver` has not been defined, the system falls back to recognizing the default driver classes listed above.

---

To control which drivers are available in the Driver Class drop-down list in Figure 31, add them to this cluster property:

[jdbcConnection.driverClass.defaultList](#)

---

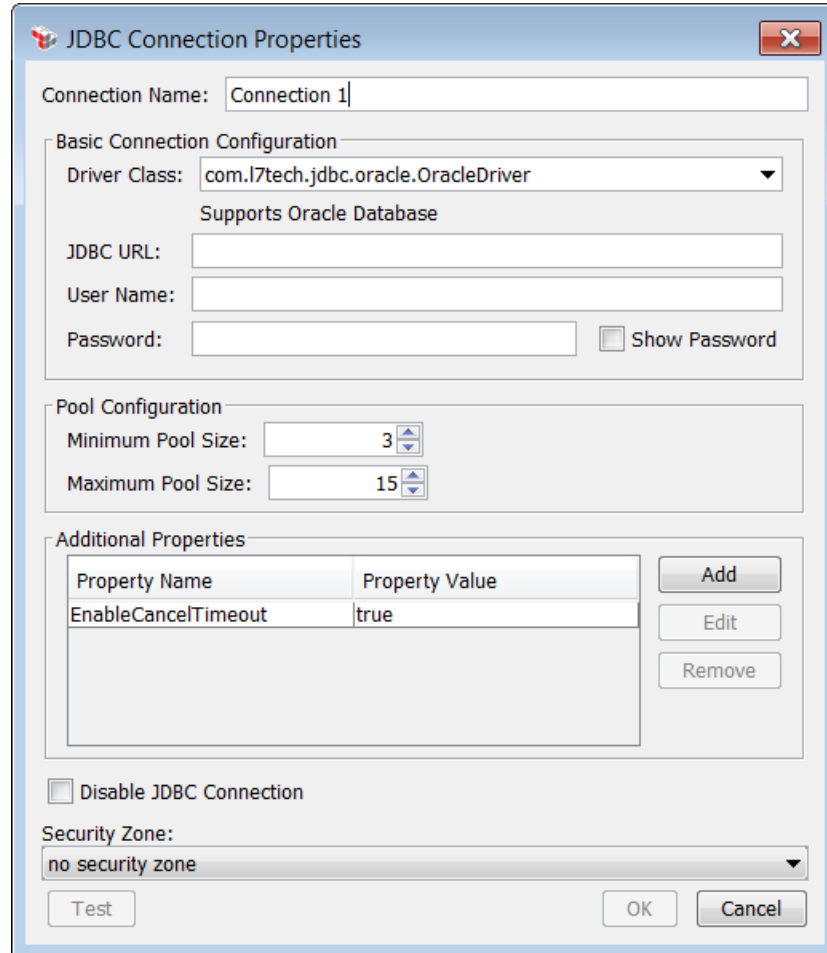
**Tip:** Driver classes added to `com.l7tech.server.jdbcDriver` but not to the cluster property will not appear in the drop-down list, but can still be used by typing in the driver class name manually. However, driver classes added to the cluster property but not to `com.l7tech.server.jdbcDriver` will not be available for use.

---

➤ *To access the properties for JDBC connection:*

1. Run the [Manage JDBC Connection](#) task.
2. Select a connection from the list and then click [**Properties**]. You can also click [**Add**] to define a new connection. The JDBC Connection Properties appear.





The dialog box is titled "JDBC Connection Properties" and contains the following sections:

- Connection Name:** A text field containing "Connection 1".
- Basic Connection Configuration:**
  - Driver Class:** A dropdown menu showing "com.l7tech.jdbc.oracle.OracleDriver".
  - Supports Oracle Database:** A checkbox that is checked.
  - JDBC URL:** An empty text field.
  - User Name:** An empty text field.
  - Password:** An empty text field with a "Show Password" checkbox to its right.
- Pool Configuration:**
  - Minimum Pool Size:** A spinner box set to "3".
  - Maximum Pool Size:** A spinner box set to "15".
- Additional Properties:**
  - A table with two columns: "Property Name" and "Property Value". It contains one row: "EnableCancelTimeout" with value "true".
  - Buttons: "Add", "Edit", and "Remove".
- Disable JDBC Connection:** An unchecked checkbox.
- Security Zone:** A dropdown menu showing "no security zone".
- Buttons:** "Test", "OK", and "Cancel" at the bottom.

Figure 31: JDBC Connection Properties dialog

3. Configure the properties as follows:

Table 31: JDBC connection settings

| Setting                | Description   |
|------------------------|---|
| <b>Connection Name</b> | <p>Enter a unique name to describe the JDBC connection.</p> <p>This name is used to select a connection in the Perform JDBC Query assertion.</p>  |
| <b>Driver Class</b>    | <p>Choose the appropriate JDBC driver class from the drop-down menu. If the driver class you need is not listed, you may be able to enter it manually (depending on whether that class has been white-listed).</p> <p>For more information about the driver classes, see "<a href="#">Understanding the Driver Classes</a>" above.</p> <p><b>Note:</b> It is possible that depending on the JDBC drivers installed on the Gateway that the driver class found for a JDBC URL does not match the configured Driver Class. This may cause the connection to fail as</p> |

| Setting                        | Description   |
|--------------------------------|---|
|                                | the Driver Class must be validated against the white list. If this happens, it is likely that the incorrect driver class was configured. Ensure that you are not referencing a deprecated driver class.   |
| <b>JDBC URL</b>                | Enter the URL for the JDBC connection. The URL format will differ depending on the driver type. The URLs for the default white-listed drivers are listed under " <a href="#">Understanding the Driver Classes</a> " above.<br><b>Note:</b> IPv6 literals are currently not supported for the JDBC URL.  |
| <b>User Name / Password</b>    | Enter the login information for the connection, if required.<br><b>Note:</b> Although you may enter the actual password here, it is recommended that you use a secure password reference instead. To do this, define your password using the <a href="#">Manage Stored Passwords</a> task and then reference it here using the <code>\${secpass.&lt;name&gt;.plaintext}</code> context variable.  |
| <b>C3P0 Pool Configuration</b> | Modify the pool sizes if necessary. The default sizes should work well in most instances. <ul style="list-style-type: none"> <li><b>Minimum Pool Size:</b> Minimum number of JDBC connections a pool will maintain at any given time. The default is <b>3</b>.</li> <li><b>Maximum Pool Size:</b> Maximum number of JDBC connections a pool will maintain at any given time. The default is <b>15</b>.</li> </ul> <b>Tip:</b> The pool size defaults are stored in the <a href="#">cluster properties</a> : <code>jdbcConnection.pooling.minPoolSize.defaultValue</code> and <code>jdbcConnection.pooling.maxPoolSize.defaultValue</code> , respectively. Additional C3P0 configuration may be made in the <b>Additional Properties</b> section.  |
| <b>Additional Properties</b>   | Configure additional properties as required by the JDBC connection.<br><b>Tip:</b> By default, the property <code>EnableCancelTimeout = true</code> has been added. This property ensures that requests to cancel a query are handled correctly. It is recommended that you do not remove or change this property for DataDirect driver unless you are certain of the consequences.<br><i>To add a new property:</i> <ol style="list-style-type: none"> <li>Click <b>[Add]</b>.</li> <li>Enter the <b>Property Name</b> and <b>Property Value</b>.</li> <li>Select the <b>To set a C3P0 pooling property</b> check box if this property applies to C3P0 pooling. The Policy Manager will automatically add the prefix "c3p0" to the property name to avoid naming collisions.</li> <li>Click <b>[OK]</b>.</li> </ol> <i>To modify a property:</i> <ol style="list-style-type: none"> <li>Select the property to change and then click <b>[Edit]</b>.</li> </ol> |

| Setting                        | Description   |
|--------------------------------|---|
|                                | <ol style="list-style-type: none"> <li>2. Make the necessary modifications.</li> <li>3. Click <b>[OK]</b>.</li> </ol> <p><i>To remove a property:</i></p> <ul style="list-style-type: none"> <li>• Select the property and then click <b>[Remove]</b>.</li> </ul>   |
| <b>Disable JDBC Connection</b> | <p>By default, the Policy Manager will immediately attempt to establish a JDBC connection after the properties dialog is closed. Select this check box if you want to keep the connection disabled.</p> <p>When a new connection is started, any old connection is stopped automatically.</p>   |
| <b>Test</b>                    | <p>Click <b>[Test]</b> to validate the settings as configured for the JDBC connection. If the test is not successful, the Policy Manager will display error messages to help you correct the problem.</p> <p><b>Note:</b> The <b>[Test]</b> button will not operate if you used context variables in any of the settings.</p>   |
| <b>Security Zone</b>           | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> |

---

**Note:** Context variables cannot be used in the JDBC Connection Properties, since the variables cannot be evaluated until runtime. Use of context variables will cause the JDBC connection to fail.

---

4. Click **[OK]** when done.

## Managing JMS Destinations

In the CA API Gateway, a JMS destination is either a *queue* or a topic. One or more JMS destinations must be configured in the Policy Manager before the Gateway can use JMS (Java Message Service) to communicate with service requestors and published services. A JMS destination can be used for receiving messages from requestors (inbound) or for sending messages to a web service or XML application (outbound).

The Gateway automatically monitors all inbound destinations configured in the Policy Manager. When the Gateway receives a message from an inbound destination, it determines which service the message is destined for and executes the applicable policy.

Policies could contain a Route via HTTP(S) or Route via JMS assertion that specifies message forwarding using either HTTP(S) or JMS, respectively. In the Gateway, there are three possible HTTP(S) and JMS routing scenarios:

- **JMS-to-JMS Configuration**

In a JMS-to-JMS configuration scenario, the Gateway receives messages from a monitored inbound JMS destination (iJMS), and then uses a Route via JMS assertion to transmit the messages to an outbound JMS destination (oJMS):

*Requestor* ← *iJMS* → *Gateway* ← *oJMS* → *Service*

Both the iJMS and oJMS destinations can be configured for a variety of reply behavior. This determines how the Gateway will respond. For details, see the [\[Inbound Options\]](#) and [\[Outbound Options\]](#) tabs on the JMS destination Properties dialog.

- **JMS-to-HTTP Configuration**

In the JMS-to-HTTP configuration scenario, the Gateway receives messages from a monitored inbound JMS destination (iJMS), and then transmits the messages to the service using HTTP:

*Requestor* ← *iJMS* → *Gateway* ← *HTTP* → *Service*

Once again, the Gateway monitors the inbound JMS destination (iJMS) configured in the Policy Manager. When the Gateway picks up a message from the destination, it routes the message to the service URL specified in the Route via HTTP(S) assertion in the service's policy. The Gateway responds to the inbound message based on the inbound JMS destination configuration (for details, see the [\[Inbound Options\]](#) tab of the "JMS Destination Properties" on page 96).

---

**Note:** When you publish a service, the Policy Manager automatically adds the service URL specified during the publication process as a Route via HTTP(S) assertion in the policy.

---

- **HTTP-to-JMS Configuration**

In the HTTP-to-JMS configuration scenario, the Gateway receives messages via HTTP, and then transmits the messages to an outbound JMS destination (oJMS):

*Requestor* ← *HTTP* → *Gateway* ← *oJMS* → *Service*

The Gateway receives a message over HTTP or HTTP(S), allowing the use of the Require HTTP Basic Credentials and Require SSL or TLS Transport with Client Authentication assertions in the policy. The Gateway responds to the oJMS response based on the outbound JMS destination configuration (for details, see the [\[Outbound Options\] tab](#) of the [JMS Destination Properties](#)). The Gateway then routes the reply message back to the requesting HTTP or HTTP(S) requestor, unless the "no replies" option was set.

## Context Variables Created by JMS Requests

When the Managing JMS Destination assertion is run, it populates the context variables in [Table 1](#) with the header information.

Table 32: Context variables created when the Gateway receives a JMS message

| Variable   | Description  |
|--|--|
| <code>\${request.jms.header.&lt;name&gt;}</code> | Returns the value of the JMS header, where <i>&lt;name&gt;</i> is the header name.   |
| <code>\${request.jms.headernames}</code>         | This is a multivalued context variable that returns the names of all headers that are present.   |
| <code>\${request.jms.allheadervalue}</code>      | <p>This is a multivalued context variable that returns all the header names and values that are present, in the format <i>headername:headervalue</i>.</p> <p>The following are the possible headers:</p> <p><i>JMSDestination</i><br/> <i>JMSDeliveryMode</i><br/> <i>JMSExpiration</i><br/> <i>JMSPriority</i><br/> <i>JMSMessageID</i><br/> <i>JMSTimestamp</i><br/> <i>JMSCorrelationID</i><br/> <i>JMSReplyTo</i><br/> <i>JMSType</i><br/> <i>JMSRedelivered</i></p> |

---

**Tip:** For a list of the context variables created by a JMS response, see the *Route Via JMS* in the *Layer 7 Policy Authoring User Manual*.

---

## Resolving Requests in JMS Destinations

Requests received via a JMS destination can either be sent to a specific published service (bypassing the resolution process), or they can undergo the standard resolution rules. You can optionally augment the service resolution using SOAPAction values retrieved from a specified JMS message property.

If SOAPAction message properties are configured on inbound destinations, the combination of SOAPAction values and payload namespace URI(s) should be distinct for every service that is expected to receive requests over JMS. If SOAPAction message attributes are not configured, every service that is expected to receive requests over JMS must have payload namespace URI(s) that are not shared by any other service on the Gateway.

For more information on how the Gateway resolves requests, see *Understanding the Service Resolution Process* in the *Layer 7 Installation and Maintenance Manual*. The resolver used for JMS requests is described in Step 4 of that section.

## Understanding JMS Message Size

The maximum size of a JMS message is governed by the following two global [cluster properties](#):

- **io.xmlPartMaxBytes:** This controls the maximum size of any XML message, including JMS messages. By default, this is 2621440 bytes (2.5MB).
- **io.jmsMessageMaxBytes:** This controls the maximum size of JMS messages, including the XML and all MIME parts. By default, this is the same as *io.xmlPartMaxBytes* (2.5MB).

Normally, these two properties would have the same limit. If you have a need to further restrict the size of JMS messages globally, set *io.jmsMessageMaxBytes* to a lower value than *io.xmlPartMaxBytes*.

## Working with JMS Destinations

An inbound destination allows the Gateway to receive messages from a JMS destination, whereas an outbound destination allows the Gateway to route messages to a service that is listening on a JMS destination. Destinations must be created in the JMS system's management application before they can be configured in the Policy Manager. A JMS destination can be edited or deleted at any time, and the Gateway will enable such changes within a few seconds.

---

**Note:** The configuration of a new destination requires the JNDI directory settings specified during the JMS configuration process. Consult your Administrator for the required values.

---

## Outbound JMS Connection Management

The Gateway will close an outbound JMS connection under any of the following conditions:

- the connection has been idle for too long (controlled by [io.jms.ConnectionCacheMaxIdleTime](#) cluster property)
- the connection is too old (controlled by [io.jms.ConnectionCacheMaxAge](#) cluster property)
- there are too many open connections (controlled by [io.jms.ConnectionCacheMaxSize](#) cluster property)

---

**Tip:** If many outbound destinations are in use, you can improve performance by reducing the idle time and increasing the cache size.

---

## Template Outbound Destinations

A template outbound destination is a special type of destination that allows certain properties to be omitted when the destination is created, to be filled in later during policy construction:

*Initial Context Factory class name* ([JNDI tab](#))

*JNDI URL* ([JNDI tab](#))

*JNDI User Name, Password* ([JNDI tab](#))

*Connection Factory Name* ([Destination tab](#))

*Destination Name* ([Destination tab](#))

*Destination User Name, Password* ([Destination tab](#))

*Reply-to queue name* ([Outbound Options tab](#))

When you omit any of these properties during the destination definition, the policy author can enter the values during policy design in the Route via JMS assertion. However if any of the above properties are set in the template destination, they cannot be changed when the template is used in the Route via JMS assertion.

## Troubleshooting Connection Issues with EMS

If you find that your JMS destinations do not reconnect after the TIBCO EMS server is shut down and restarted, do the following:

1. Locate the *tibemsd.conf* file on the EMS server and open it for editing.

---

**Tip:** There are two *tibemsd.conf* files with the same name: one is a sample file, while the functional one resides in the TIBCO home folder, which may differ in each installation. For example, a search for "tibemsd.conf" may bring up these results:

```
/opt/tibco/ems/6.1/samples/config/tibemsd.conf
/root/TIBCO_HOME/tibco/cfgmgmt/ems/data/tibemsd.conf
```

---

2. Add the following parameters:

**server\_heartbeat\_client = 5**

**client\_timeout\_server\_connection = 25**

The unit is seconds, so the parameters above are 5 and 25 seconds. **Tip:** Ensure that *client\_timeout\_server\_connection* is at least five times the value of *server\_heartbeat\_client*.

This should resolve the reconnection issues. For more information about these parameters, refer to the *TIBCO Enterprise Messaging Service User Guide*.

## Running the Manage JMS Destinations Task

➤ To manage JMS destinations:

1. In the Policy Manager, select **[Tasks] > Manage JMS Destinations** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage JMS Destinations dialog appears.

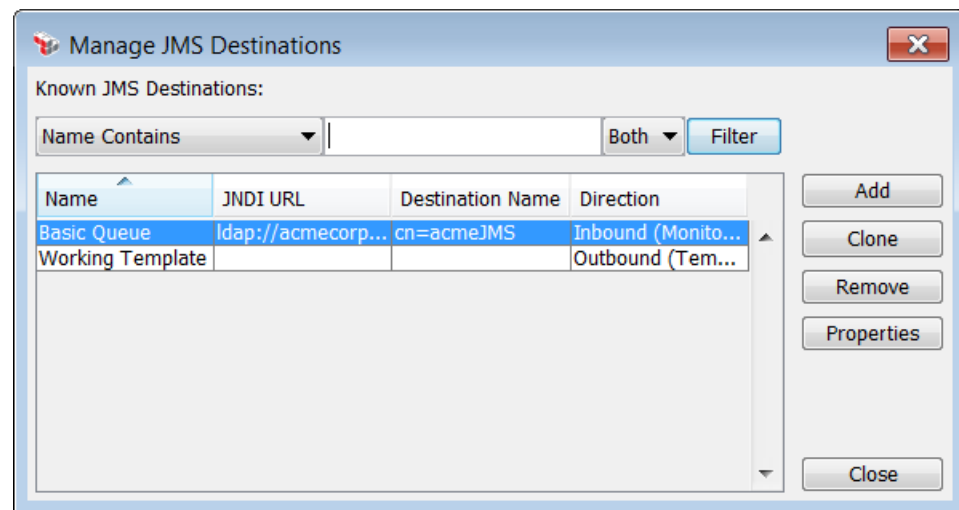


Figure 32: Manage JMS Destinations dialog

Choose one of the following actions:

Table 33: Working with JMS Destinations

| Action   | Description  |
|--|--|
| <b>Filter list of destinations</b><br>(optional) | <p>When there are a large number of JMS destinations, you can filter the list to more easily locate the destination you want:</p> <ol style="list-style-type: none"> <li>From the drop-down list, select the destination property to filter on:<br/><b>Name</b> (from [Basics] tab)</li> </ol> |



| Action                                       | Description   |
|--|---|
|  | <p><b>JNDI URL</b> (from [JNDI] tab)</p> <p><b>Destination Name</b> (from [Destination] tab)</p> <p>These are all in the "JMS Destination Properties" on page 96.</p> <ol style="list-style-type: none"> <li>Type a few characters to search on. This text will be matched anywhere within the chosen destination property and is not case sensitive. <b>Tip:</b> For more powerful filtering, you can use regular expressions.</li> <li>Indicate whether to include only <b>Inbound</b>, <b>Outbound</b>, or <b>Both</b> types of destinations.</li> <li>Click [<b>Filter</b>]. The list is filtered to display only those destinations matching the filter criteria.</li> </ol> |
| <b>Sort destination list based on column</b> | <p>By default, the list of destinations is sorted in ascending order by Name.</p> <p>Click on any column heading to re-sort the table based on that column. The following markers indicate the sorting column:</p> <ul style="list-style-type: none"> <li>▲ = The table is sorted in <i>ascending</i> alphabetical order based on the indicated column.</li> <li>▼ = The table is sorted in <i>descending</i> alphabetical order based on the indicated column.</li> </ul>  |
| <b>Add a new JMS destination</b>             | <p>Click [<b>Add</b>] and then configure the properties for the new destination. See "JMS Destination Properties" on page 96 for details.</p> <p>You can also create a new JMS destination by clicking [<b>New Destination</b>] on the JMS Routing Properties dialog.</p> <p><b>Note:</b> The same Outbound destination may be defined multiple times, as long as each resolves to a different web service.</p>   |
| <b>Clone an existing JMS destination</b>     | <p>Select the destination to clone, then click [<b>Clone</b>]. Edit the destination properties as required. See "JMS Destination Properties" on page 96 for details.</p>  |
| <b>Modify an existing JMS destination</b>    | <p>Select the destination to modify, then click [<b>Properties</b>]. Edit the destination properties as necessary. See "JMS Destination Properties" on page 96 for details.</p> <p><b>Note:</b> Be sure to test your new settings to ensure the connection is valid.</p>  |
| <b>Remove a JMS destination</b>              | <p>Select the destination to remove and then click [<b>Remove</b>]. Click [<b>OK</b>] to confirm the deletion.</p> <p><b>Note:</b> Removing a destination only unregisters it from the Gateway. The destination still exists in the JMS system's management application.</p>  |

2. Click **[Test Settings]** to test the connection between the Gateway and JMS destination. A test is considered successful if the Gateway can:
  - Read from an inbound destination
  - Write to an outbound destination
  - Contact any additional destinations specified in the configuration (for example, a Reply-to queue, Failure queue, Wait-for-reply queue)

If a connection cannot be established, make a note of the diagnostic information that is displayed, double-check the destination and Gateway settings, and then try again. If you are unsuccessful, [contact](#) CA Technical Support for assistance.

3. Click **[Save]** to close the JMS Destination Properties. When adding a destination, the new destination is registered in the Gateway and added to the **Known JMS Destinations** table in the Manage JMS Destinations dialog.

The **[Save]** button is unavailable if there is information missing in any of the tabs.

4. Click **[Close]** when done.

## JMS Destination Properties

When creating or viewing details about [JMS destinations](#), the JMS Destination Properties appear. The properties are organized across these tabs:

- Basics
- JNDI
- Destination
- Inbound Options
- Outbound Options

For more information about JMS destinations, see "Managing JMS Destinations" on page 89.

---

**Note:** If you are configuring Websphere as a JMS Destination, refer to the Appendix "WebSphere JMS Provider" in the *Layer 7 Installation and Maintenance Manual* for configuration steps that must be completed first.

---

➤ *To access the properties for an MQ native queue:*

1. Run the [Manage JMS Destinations](#) task.
2. Select a destination and then click **[Properties]**. You can also click **[Add]** to create a new queue. The JMS Destination Properties appear.

3. Configure each tab within the properties as necessary. Refer to the appropriate section below for a complete description of each tab.
4. Click **[Save]** when done.

### Configuring the [Basics] Tab

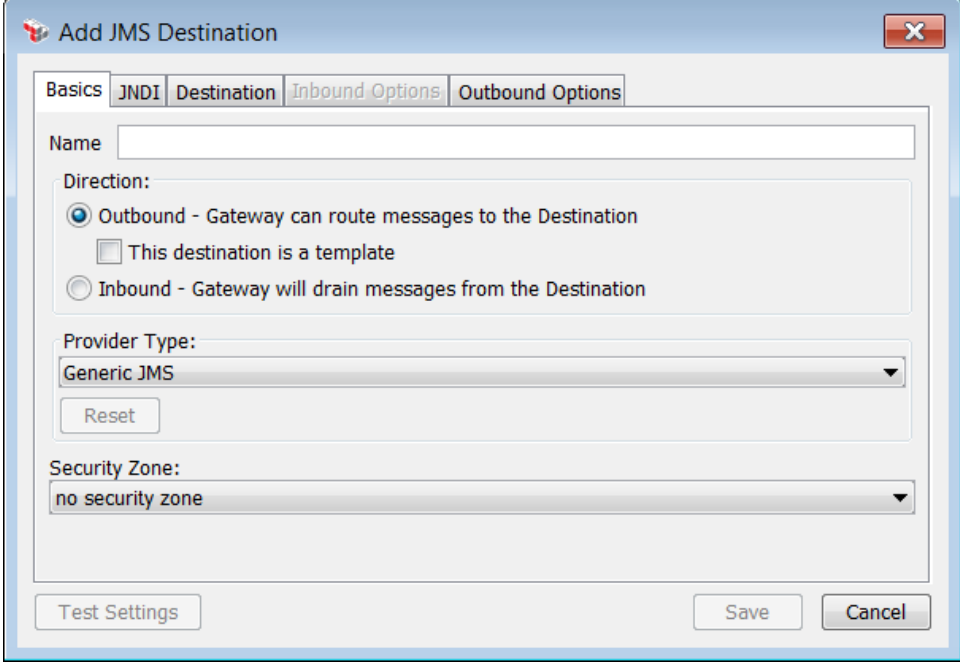


Figure 33: JMS Destination Properties - [Basics] tab

The **[Basics]** tab is used to set the destination direction and provider type.

1. Enter a name for the JMS destination. This name will be displayed in the policy window; it can be the same as the **Destination Name** in the **[Destination]** tab or it can be a descriptive label to help users more easily identify the destination. This name is required.
2. Specify the **Direction** of the destination being configured:
  - Select **Outbound** to configure an outbound destination.
    - Select the **This destination is a template** check box to configure a template outbound destination that allows certain details to be entered later, using the Route via JMS assertion. For more information, see ["Template Outbound Destinations"](#) in "Managing JMS Destinations" on page 89.
  - Select **[Inbound]** to configure an inbound destination.

---

**Note:** Selecting a direction is possible only when adding or modifying a destination using the [Manage JMS Destinations](#) task. When creating a new destination from the Route via JMS assertion, the outbound option is always used.

---

3. Select the JMS provider type from the drop-down list.

- Choose **Generic JMS** to connect to a JMS provider not listed.

The "Generic JMS" option can be used to configure the JMS destination to work with other JMS providers not listed in the drop-down list.

For example, to connect to **webMethods Broker**: enter the following Context Factory class name in the [\[JNDI\]](#) tab:

*com.webmethods.jms.naming.WmJmsNamingCtxFactory*

- Choose **TIBCO EMS** if connecting to a TIBCO Enterprise Message Service (EMS) server.
- Choose **WebSphere MQ over LDAP** if connecting to an IBM WebSphere MQ server using the LDAP protocol.

---

**Note:** If you are configuring an MQSeries destination with a backout destination configured, this destination will hold the messages that cannot be processed.

---

- Choose **WebLogic JMS** if connecting to a WebLogic JMS server.

---

**Note:** When connecting to a WebLogic JMS provider, you should set the [io.jmsConnectionCacheMaxSize](#) cluster property to "0" (zero) and also set the system property *com.l7tech.server.transport.jms.detectJmsTypes* to **true**. This property must be set on each node in a cluster and the Gateway must be restarted for the new setting to take effect.

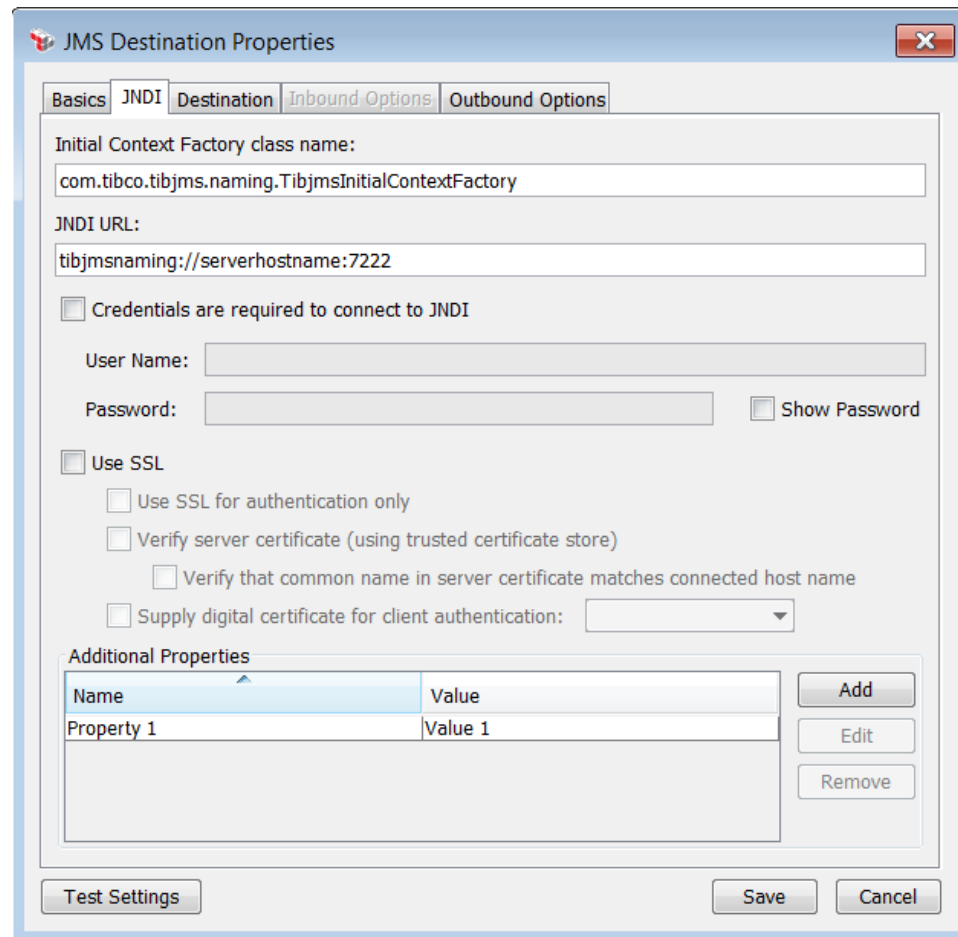
---

Please [contact](#) CA Technical Support if you require assistance configuring the destination for other JMS providers.

The **[Reset]** button allows you to quickly set destination properties for the current provider using the predefined defaults. You will be warned if existing configuration will be overwritten. The **[Reset]** button is not available for Generic JMS destinations.

4. Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "**No security zone**". For more information about security zones, see [Understanding Security Zones](#) in the *Layer 7 Policy Manager User Manual*. **Note:** This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).

## Configuring the [JNDI] Tab



**JMS Destination Properties**

Initial Context Factory class name:  
com.tibco.tibjms.naming.TibjmsInitialContextFactory

JNDI URL:  
tibjmsnaming://serverhostname:7222

☐ Credentials are required to connect to JNDI

User Name:

Password:  ☐ Show Password

☐ Use SSL

☐ Use SSL for authentication only

☐ Verify server certificate (using trusted certificate store)

☐ Verify that common name in server certificate matches connected host name

☐ Supply digital certificate for client authentication:

Additional Properties

| Name       | Value   |
|------------|---------|
| Property 1 | Value 1 |

Figure 34: JMS Destination Properties - [JNDI] tab (based on Provider Type "TIBCO EMS")

The **[JNDI]** tab is used to configure the JNDI connection properties. Note that the settings described below may not be available for all provider types.

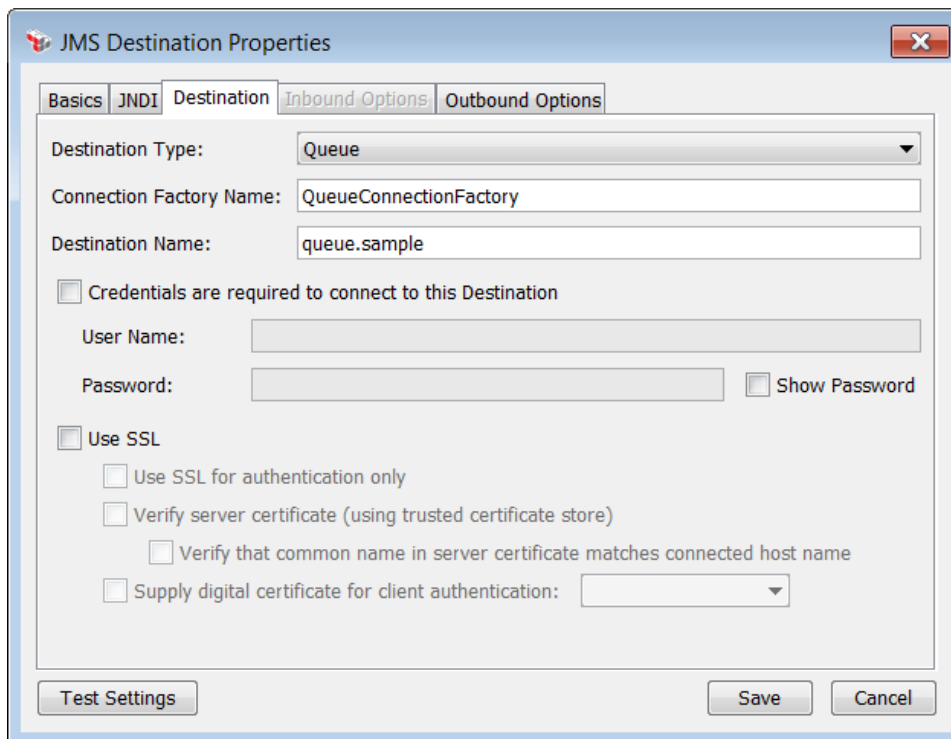
Table 34: JMS Destination Properties - [JNDI] tab

| Setting                                   | Description   |
|---|---|
| <b>Initial Context Factory class name</b> | <p>Enter the name of the initial context class.</p> <p>For <a href="#">outbound template destinations</a>, you may leave this field blank to be filled in later using the Route via JMS assertion.</p> <p><i>Examples:</i></p> <p><b>WebSphere MQ:</b> <code>com.sun.jndi.Ldap.LdapCtxFactory</code></p> <p><b>TIBCO EMS:</b><br/><code>com.tibco.tibjms.naming.TibjmsInitialContextFactory</code></p> <p><b>WebLogic JMS:</b> <code>weblogic.jndi.WLInitialContextFactory</code></p> |

| Setting   | Description   |
|---|---|
|   | <b>WebSphere:</b><br><i>com.ibm.websphere.naming.WsnInitialContextFactory</i>   |
| <b>JNDI URL</b>   | <p>Enter the address of the JNDI (Java Naming and Directory Interface) server, followed by a port number (if required).</p> <p>For <a href="#">outbound template destinations</a>, you may leave this field blank to be filled in later using the Route via JMS assertion.</p> <p><i>Examples:</i></p> <p><b>WebSphere MQ:</b><br/> <i>ldap://servername.company.com/dc=companydomain,dc=com</i></p> <p><b>TIBCO EMS:</b> <i>tibjmsnaming://machinename:7222</i><br/> <b>(Important:</b> Enter only the machine name, not the full host name—i.e., <i>machine.company.com</i>.)</p>   |
| <b>Credentials are required to connect to JNDI</b>                      | <p>If login information is required, select this check box and then enter the <b>User Name</b> and <b>Password</b>.</p> <p>For <a href="#">outbound template destinations</a>, you may select the check box and leave the credential fields blank to be filled in later using the Route via JMS assertion.</p>  |
| <b>Use SSL</b><br><i>(only available for Provider Type "TIBCO EMS")</i> | <p>Select this check box if you want to use an SSL connection for the JMS destination.</p> <ul style="list-style-type: none"> <li>For Provider Type <b>TIBCO EMS</b>, additional SSL settings become available once the <b>Use SSL</b> check box is selected.</li> </ul> <p>The following options are available once this check box is selected for Provider Type <b>TIBCO EMS</b>:</p> <ul style="list-style-type: none"> <li><b>Use SSL for authentication only:</b> Select this check box to use SSL only when authenticating. Clear this check box to use SSL for all communication (for both authentication and subsequent messages).</li> <li><b>Verify server certificate (using trusted certificate store):</b> Select this check box to verify the server certificate. Clear this check box to not verify the server certificate. <ul style="list-style-type: none"> <li><b>Verify that common name in server certificate matches connected host name:</b> Select this check box to verify the server certificate with the host name. Clear this check box if you know that the common name in the server certificate will not match the connected EMS server host.</li> </ul> <p>This option is available only when the <b>Verify server certificate</b> check box is selected.</p> <p><b>Tip:</b> Normally you should verify the certificate name with the host name. You may disable this option for testing purposes, when a temporary non-production certificate is installed on the EMS server.</p> </li> <li><b>Supply digital certificate for client authentication:</b> Select</li> </ul> |

| Setting                      | Description   |
|------------------------------|---|
|                              | <p>this check box if you are supplying a certificate and private key for client authentication. This is required if the EMS server is configured with <code>"ssl_require_client_cert = enabled"</code>. From the drop-down list, select the digital certificate to be used.</p> <p><b>Note:</b> Private keys stored in an internal Hardware Security Module (HSM) on the Gateway cannot be used for client certificate authentication with the TIBCO EMS server, and will not appear in the drop-down list.</p>   |
| <b>Additional Properties</b> | <p>Optionally define additional properties required by the JNDI connection.</p> <p><b>Note:</b> Please consult with your administrator or CA Technical Support to determine the need for additional properties.</p> <ul style="list-style-type: none"> <li>To add an additional property, click <b>[Add]</b> and then enter the <b>Name</b> and <b>Value</b>.</li> <li>To modify a property in the list, select the row and then click <b>[Edit]</b>. Edit the <b>Value</b> as required.</li> <li>To remove a property from the list, select the row and then click <b>[Remove]</b>.</li> </ul> |

## Configuring the [Destination] Tab



**JMS Destination Properties**

Basics JNDI **Destination** Inbound Options Outbound Options

Destination Type: Queue

Connection Factory Name: QueueConnectionFactory

Destination Name: queue.sample

☐ Credentials are required to connect to this Destination

User Name:

Password: ☐ Show Password

☐ Use SSL

☐ Use SSL for authentication only

☐ Verify server certificate (using trusted certificate store)

☐ Verify that common name in server certificate matches connected host name

☐ Supply digital certificate for client authentication:

Test Settings Save Cancel

Figure 35: JMS Destination Properties - [Destination] tab (for provider type 'TIBCO EMS')

The **[Destination]** tab is used to configure the JMS destination details.

Table 35: JMS Destination Properties - [Destination] tab

| Setting  | Description   |
|--|---|
| <b>Destination Type</b>  | <p>From the drop-down list, select the destination type:</p> <ul style="list-style-type: none"> <li><b>Queue:</b> The destination is a JMS Queue, where the message will be received by exactly one consumer. If no consumers are available, then the message will be held until a consumer is available. If a consumer receives a message and does not acknowledge it before closing then the message will be redelivered to another consumer.</li> <li><b>Topic:</b> The destination is a JMS Topic. It will be received by all consumers who have subscribed to this topic. Only subscribers with an active subscription will get a copy of the message.</li> </ul>  |
| <b>Connection Factory Name</b>   | <p>Enter the JNDI Connection Factory reference name.</p> <p>For <a href="#">outbound template destinations</a>, you may leave this field blank to be filled in later using the Route via JMS assertion.</p> <p>The Connection Factory Name should be displayed if WebSphere has been correctly configured as a JMS destination.</p> <p><b>Tip:</b> If the system property <code>com.17tech.server.transport.jms.detectJmsTypes</code> is set to "true" (default), the Gateway will try to detect the connection type (either Queue or Topic) automatically. For more information, see "System Properties" in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>  |
| <b>Destination Name</b>  | <p>Enter the destination reference name.</p> <p>For <a href="#">outbound template destinations</a>, you may leave this field blank to be filled in later using the Route via JMS assertion.</p>   |
| <b>Credentials are required to connect to this Destination</b>                             | <p>If this JMS destination requires login information, select this check box and then enter the <b>User Name</b> and <b>Password</b>.</p> <p>For <a href="#">outbound template destinations</a>, you may select the check box and leave the credential fields blank to be filled in later using the Route via JMS assertion.</p>  |
| <b>Use SSL</b><br><i>(only available for Provider Types = 'TIBCO EMS' and 'WebSphere')</i> | <p>When the Provider Type is <b>TIBCO EMS</b>:</p> <ul style="list-style-type: none"> <li>See "Use SSL" in Table 34 for details.</li> </ul> <p>When the Provider Type is <b>WebSphere MQ over LDAP</b>:</p> <ul style="list-style-type: none"> <li>Select this check box to have the Gateway connect to the MQ Queue Manager using SSL. The Gateway will <i>always</i> use its primary SSL keypair as a client certificate on the MQ connection. Additionally, the Gateway will <i>always</i> perform hostname and server certificate validation using the Gateway's standard trusted certificate store.</li> </ul> <p>Clear this check box if you are certain that the MQ Queue Manager does not require SSL.</p> <ul style="list-style-type: none"> <li><b>Use Client Authentication:</b> When connecting using SSL,</li> </ul> |



| Setting | Description  |
|---------|--|
|         | <p>select this check box to present a certificate to the server during the SSL handshake, if one is requested. Clear this check box to never present a certificate, even if one is requested. Note that access may be denied in this case.</p> <ul style="list-style-type: none"><li>• <b>Keystore:</b> From the drop-down list, select the keystore from which to retrieve the certificate.</li></ul> <p>The [<b>Use SSL</b>] check box assumes that the MQ Queue Manager has been correctly configured to use SSL.</p> |

## Configuring the [Inbound Options] Tab

**Add JMS Destination**

Basics | JNDI | Destination | **Inbound Options** | Outbound Options

Acknowledgement Behavior: **On Take**

**Inbound Reply Behavior**

- ☒ Automatic (send reply if specified in inbound message)
- ☐ Do not send replies (one-way)
- ☐ Send Reply to specified queue:

**Request/Response Correlation**

- ☒ Copy CorrelationID from Request to Response
- ☐ Set Response CorrelationID from Request's MessageID

**Service Resolution**

- ☐ Associate destination with published service (bypass resolution)
  - Service name:
- ☐ Get SOAPAction values from the specified JMS message property for service resolution:
  - Property name:
- ☐ Specify Content Type
  - ☒ Use Content Type
  - ☐ Get Content Type from JMS Property
- ☐ Send failed requests to the specified queue:
  - Failure queue name:
- ☐ Stop listening on this destination

Consumer Connections:

☐ Override maximum message size:

- ☒ Restrict messages to  bytes
- ☐ Allow unlimited message size (not recommended)

Test Settings Save Cancel

Figure 36: JMS Destination Properties - [Inbound Options] tab


The **[Inbound Options]** tab is used to configure details for inbound JMS destinations.

**Note:** Inbound JMS destinations are used by published JMS services and do not require an assertion. The JMS service publication process is the same as the publication process for a regular [service](#). If you are publishing a service that will accept incoming messages from a JMS queue, ensure that the appropriate inbound JMS queue is monitored for the messages. JMS messages will be processed according to the assertions defined in the policy.

Table 36: JMS Destination Properties - [Inbound Options] tab

| Setting                         | Description   |
|---------------------------------|---|
| <b>Acknowledgement Behavior</b> | <p>From the drop-down list, select how the Gateway should acknowledge incoming JMS messages:</p> <ul style="list-style-type: none"> <li>• <b>On Take:</b> Automatically acknowledge each message as it is read from the destination.</li> <li>• <b>On Completion:</b> Delay acknowledging the incoming message until the services policy execution completes.</li> </ul> <p>Using "On Completion" acknowledgement increases the reliability of message processing. If a Gateway fails during the processing of a message, that message will remain in the JMS destination and can be processed by another node. (This assumes that a cluster of nodes has been configured. For more information, see <i>Configure a Gateway Cluster</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.)</p> <p><b>Note:</b> If you have not configured a failure destination or a backout destination, then messages that consistently fail (for example, a backend service is non-functional) will remain in the queue indefinitely. The Gateway will continually try to process these messages and may get stuck in a loop, unless one of the above destinations are configured.</p> <p><b>Note:</b> The Protect Against Message Replay assertion should not be used in any policy that will process messages from JMS destinations that are configured with the "On completion" acknowledgment mode without a specified failure destination.</p> |
| <b>Inbound Reply Behavior</b>   | <p>Select a JMS reply behavior for the inbound destination:</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> Choose this option to have the Gateway send response messages on the destination named in the corresponding request message's <i>JMSReplyTo</i> attribute. If the attribute is not present, no response messages will be sent.</li> <li>• <b>Do not send replies:</b> Choose this option to never send replies to requests received on this inbound destination. This will ignore any <i>JMSReplyTo</i> attribute in inbound messages.</li> <li>• <b>Send reply to specified queue:</b> Choose this option to send all replies to requests received on this inbound destination to the specified queue. This will override any <i>JMSReplyTo</i> attribute in inbound messages. Enter the name of the queue in the adjacent box.</li> </ul>  |

| Setting  | Description  |
|--|--|
| <b>Request/Response Correlation</b>                | <p>The inbound Request/Response correlation behavior can be specified if either the "Automatic" or "Send reply to specified queue" option was selected:</p> <ul style="list-style-type: none"> <li>• <b>Copy CorrelationID from Request to Response:</b> Choose this option to have the Gateway copy the <i>JMSCorrelationID</i> value from the inbound request message to the <i>JMSCorrelationID</i> attribute on the outbound response.</li> <li>• <b>Set Response CorrelationID from Request's MessageID:</b> Choose this option to have the Gateway copy the <i>MessageID</i> from the inbound request message to the <i>JMSCorrelationID</i> attribute on the outbound response.</li> </ul>  |
| <b>Service Resolution</b>                          | <p>Select how the service should be resolved:</p> <ul style="list-style-type: none"> <li>• <b>Associate destination with published service (bypass resolution):</b> <ul style="list-style-type: none"> <li>• Select this check box to associate the inbound JMS destination with a published service. This overrides the Gateway's built-in service resolution logic. This is useful if you need to publish the same WSDL multiple times and have the same target namespace, yet still be consumed through JMS. Choose the service from the <b>Service name</b> drop-down list.</li> <li>• Clear this check box to have the Gateway determine the applicable policy for each message. This is done based on message-level inspection. For example, a SOAP payload will be resolved against a set of published services and associated WSDL documents to find a match.</li> </ul> </li> <li>• <b>Get SOAPAction values from the specified JMS message property for service resolution:</b> Select this check box to use a specific JMS message property as the "SOAPAction" for service resolution purposes. Enter the name of the property to use.</li> <li>• <b>Specify content type:</b> Select this check box to specify the Content-Type to be associated with the inbound destination. Choose from one of the following: <ul style="list-style-type: none"> <li>• Select the Content-Type to use from the <b>Use Content Type</b> drop-down list. If the Content-Type you need isn't listed, type it directly into the drop-down list.</li> <li>• Select <b>Get Content Type from JMS Property</b> and then specify a JMS message property to retrieve from.</li> </ul> <p>If a Content-Type is not specified, the Gateway will assume type "text/xml".</p> </li> </ul> |
| <b>Send failed requests to the specified queue</b> | <p>Select this check box to route the message to a special queue if the service policy does not successfully complete.</p>   |

| Setting                                   | Description   |
|---|---|
|   | <p>The messages sent to the failure queue are not due to a Gateway failure, but rather from other causes such as routing failure, message content, etc.</p> <p>If this check box is not selected, then the JMS provider configuration will be expected to ensure that messages that could not be processed do not remain in the queue indefinitely.</p> <p>This option is available only when <b>Acknowledgement Behavior</b> is set to "On Completion".</p>  |
| <b>Failure queue name</b>                 | <p>If sending requests to a failure queue, enter the name of the queue (topics are not supported) that will receive messages that were not successfully processed.</p>  |
| <b>Stop listening on this destination</b> | <p>Select this check box to instruct the Gateway to stop listening for messages on this JMS destination. During this stoppage, incoming client requests will accumulate in the destination until the Gateway resumes listening. When listening restarts, the Gateway will process the queued messages and send a response.</p>  |
| <b>Consumer Connections</b>               | <p>Enter the number of JMS consumer connections permitted for a particular JMS destination, between 1 and 10000. Default: <b>1</b></p> <p><b>Notes:</b> (1) This setting only applies to JMS Queues, not to JMS Topics. (2) The default can be changed using the <a href="#">io.jmsConsumerConnections</a> cluster property. (3) Consumer connections stay open until the "Stop listening on this destination" check box is selected.</p>   |
| <b>Override maximum message size</b>      | <p>Select this check box to override the permitted maximum size of the routing message. Clear this check box to use the value set in the <a href="#">io.xmlPartMaxBytes</a> cluster property.</p> <ul style="list-style-type: none"> <li>• <i>Restrict messages to:</i> Enter the maximum permitted size of the response message, in bytes. You may reference context variables. </li> <li>• <i>Allow unlimited message size (not recommended):</i> Select this option to allow response messages of unlimited size. This is not recommended and should be used only under the direction of CA Technical Support.</li> </ul> |

## Configuring the [Outbound Options] Tab

The screenshot shows the 'JMS Destination Properties' dialog box with the 'Outbound Options' tab selected. The dialog has five tabs: Basics, JNDI, Destination, Inbound Options, and Outbound Options. The 'Outbound Options' tab contains the following settings:

- Outbound Reply Behavior:**
  - ☒ Always use temporary queue
  - ☐ No replies (one-way)
  - ☐ Wait for Reply on specified queue: [text field]
- Request/Response Correlation:**
  - ☒ Generate New CorrelationID for Request
  - ☐ Expect Receiver to copy Request MessageID to Response CorrelationID
- Outbound Message Format:**
  - ☒ Automatic
  - ☐ BytesMessage
  - ☐ TextMessage
- Session Pooling Setting:**
  - Session Pool Size: [8]
  - Max Session Idle: [8]
  - Max Wait (ms): [5000]

At the bottom of the dialog are three buttons: 'Test Settings', 'Save', and 'Cancel'.

Figure 37: JMS Destination Properties - [Outbound Options] tab

The **[Outbound Options]** tab is used to configure details for outbound JMS destinations. For more information on using an outbound destination in a service with JMS routing, see Route via JMS assertion in the *Layer 7 Policy Authoring User Manual*.

Table 37: JMS Destination Properties - [Outbound Options] tab

| Setting                        | Description   |
|--------------------------------|---|
| <b>Outbound Reply Behavior</b> | <p>Specify a JMS reply behavior for the outbound destination:</p> <ul style="list-style-type: none"> <li> <b>Always use temporary queue:</b> Choose this to have the Gateway create a temporary queue, set it as the <i>JMSReplyTo</i> attribute on outbound requests, then listen on that temporary queue for a response. </li> </ul> <p><b>Tip:</b> For a topic destination type, it is recommended that you choose the <b>"No replies (one way)"</b> option for an outbound topic. This will prevent errors when the Route via JMS assertion</p> |

| Setting                             | Description  |
|-------------------------------------|--|
|                                     | <p>is processed.</p> <ul style="list-style-type: none"> <li>• <b>No replies (one way):</b> Choose this to have the Gateway send the request and then return immediately without waiting for a reply. The response to the requestor will be empty, unless some other assertion fills it in.</li> <li>• <b>Wait for reply on specified queue:</b> Choose this to have the Gateway look up the specified queue, set it as the <i>JMSReplyTo</i> attribute on the outbound request, and then wait on that queue for the response. Enter the name of the queue in the adjacent box.</li> </ul> <p>For <a href="#">outbound template destinations</a>, you may leave this field blank to be filled in later using the Route via JMS assertion.</p>               |
| <b>Request/Response Correlation</b> | <p>If waiting for a reply on a specific destination, select a Request/Response Correlation option:</p> <ul style="list-style-type: none"> <li>• <b>Generate New CorrelationID for Request:</b> Choose this to have the Gateway generate a unique ID, set it as the <i>JMSCorrelationID</i> attribute on the outbound request, and then select only messages with the matching <i>JMSCorrelationID</i> value from the response destination.</li> <li>• <b>Expect Receiver to Copy Request MessageID to Response CorrelationID:</b> Choose this to send the request message as-is, then select only messages with the <i>JMSCorrelationID</i> attribute matching the outbound request's <i>MessageID</i> attribute from the response destination.</li> </ul> |
| <b>Outbound Message Format</b>      | <p>Select the desired output Content-Type:</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> Requests arriving over JMS as <i>TextMessage</i> will be forwarded as <i>TextMessage</i>, otherwise it will be forwarded as <i>BytesMessage</i>. This setting is the default.</li> <li>• <b>BytesMessage:</b> Always forward requests as <i>BytesMessage</i>, regardless of incoming format.</li> <li>• <b>TextMessage:</b> Always forward requests as <i>TextMessage</i>, regardless of incoming format.</li> </ul>   |
| <b>Session Pooling Setting</b>      | <p>Specify the JMS session pooling settings:</p> <ul style="list-style-type: none"> <li>• <b>Session Pool Size:</b> Specify the maximum number of sessions that can be allocated by the session pool (maximum 10000). Enter <b>-1</b> to indicate no limit. Enter <b>0</b> to create a new connection each time the Route via JMS assertion sends a message to the queue.<br/>Default: <b>8</b>.</li> <li>• <b>Max Session Idle:</b> Specify the maximum number of sessions that can sit idle in the session pool (maximum 10000). Enter <b>-1</b> to indicate no limit.</li> </ul>  |

| Setting | Description   |
|---------|---|
|         | <p>Default: <b>8</b>.</p> <p><b>Note:</b> When this setting is too low on a heavily loaded system, you may see sessions (producers) being destroyed and new sessions being created almost immediately.</p> <ul style="list-style-type: none"> <li>• <b>Max Wait:</b> Specify the maximum period of time to wait for an idle session when the pool is exhausted (maximum 999999999).</li> </ul> <p>Default: <b>5000</b> (milliseconds)</p> |

## Managing MQ Native Queues

The *Manage MQ Native Queues* task is used to configure the CA API Gateway to natively communicate with IBM WebSphere MQ to exchange both inbound and outbound messages.

IBM WebSphere MQ is a widely-deployed message-oriented middleware (MOM) solution that is commonly used in enterprises to integrate disparate systems and enable asynchronous transaction models. Most integrations typically use standards-based protocols such as JMS. However, there may be instances where integration using proprietary channels is preferred. For example, instead of using JMS and JNDI to exchange messages with MQ Native, you can use the native CA integration.

---

**Note:** For information on installing the MQ Native .JAR files, refer to the "Installing the JMS Interface" appendix in the *Layer 7 Installation and Maintenance Manual* for your Gateway form factor.

---

## Understanding MQ Native Message Size

The maximum size of an MQ Native message is governed by the following two global cluster properties:

- **io.xmlPartMaxBytes:** This controls the maximum size of any XML message, including MQ messages. By default, this is 2621440 bytes (2.5MB).
- **io.mqMessageMaxBytes:** This controls the maximum size of MQ Native messages, including the XML and all MIME parts. By default, this is the same as *io.xmlPartMaxBytes* (2.5MB).

Normally, these two properties would have the same limit. If you need to further restrict the size of MQ Native messages globally, set *io.mqMessageMaxBytes* to a lower value than *io.xmlPartMaxBytes*.

These global limits can be overridden for both inbound MQ native messages and outbound MQ native messages (via the Route via MQ Native assertion).



## Working with MQ Native Queues

An inbound queue allows the Gateway to consume messages from an MQ connection, whereas an outbound queue allows the Gateway to send/route messages to that connection. Queues must be created in the WebSphere MQ management application before they can be configured in the Policy Manager.

Once the queues are created in the WebSphere MQ management application, you can add, edit, or remove customized message descriptors, properties, and additional headers.

For inbound and outbound MQ Native messages, you can modify the Message Descriptor, Message Properties, and Additional Headers. To customize Message Descriptors, use the Manage Transport Properties/Headers assertion. An MQ Native queue can be edited or deleted at any time. The Gateway will enable such changes within a few seconds.

Header type conversions such as MQRFH to MQRFH2 and vice-versa are supported for configuring the Additional Header and Message Property.

---

**Tip:** When the Route via MQ Native assertion is configured to “Get from queue”, it will be able to consume a message from an outbound queue.

---

## Outbound MQ Connection Management

The Gateway will close an outbound MQ connection under any of the following conditions:

- the connection has been idle for too long (controlled by [io.mqConnectionCacheMaxIdleTime](#) cluster property)
- the connection is too old (controlled by [io.mqConnectionCacheMaxAge](#) cluster property)
- there are too many open connections (controlled by [io.mqConnectionCacheSize](#) cluster property)

---

**Tip:** If many outbound queues are in use, you can improve performance by reducing the idle time and increasing the cache size.

---

## Template Outbound Queues

A template outbound queue is a special type of queue that allows the following properties to be omitted when the queue is created, to be filled in later during policy construction:

*Queue name* ([MQ Connections Properties tab](#))

Wait for Reply reply on specified queue name ([Outbound Options tab](#))

When you omit either of these properties during the queue definition, the policy author can enter the values during policy design in the Route via MQ Native assertion. However if any of the above properties are set in the template queue, they cannot be changed when the template is used in the Route via MQ Native assertion.

➤ To manage MQ Native Queues:

1. In the Policy Manager, select **[Tasks] > Additional Actions > Manage MQ Native Queues** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage MQ Native Queues dialog appears.

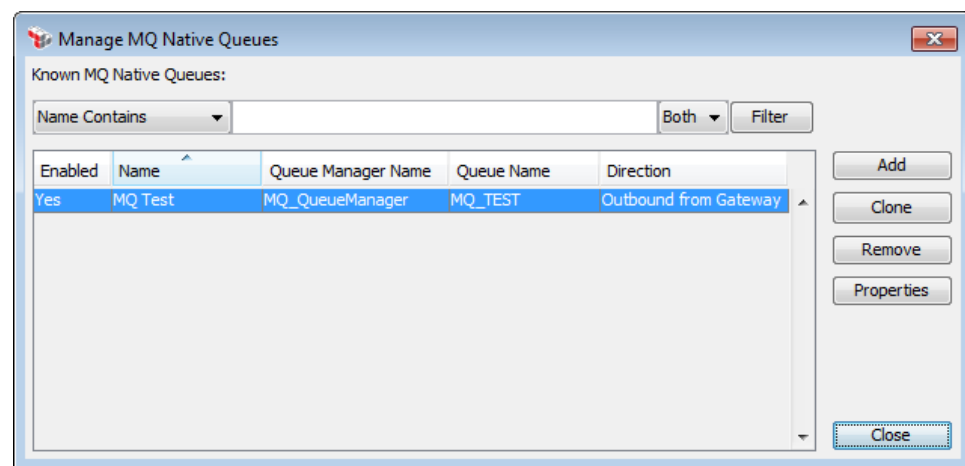


Figure 38: Manage MQ Native Queues dialog

2. Choose one of the following actions:

Table 38: Working with MQ Native Queues

| Action                                     | Description  |
|--|--|
| <b>Filter list of queues</b><br>(optional) | <p>When there are a large number of MQ Native queues, you can filter the list to more easily locate the queue you want:</p> <ol style="list-style-type: none"> <li>1. From the drop-down list, select the queue property to filter.</li> <li>2. Type a few characters to search on. This text will be matched anywhere within the chosen queue property and is not case sensitive. <b>Tip:</b> For more powerful filtering, you can use regular expressions.</li> <li>3. Indicate whether to include only <b>Inbound</b>, <b>Outbound</b>, or <b>Both</b> types of queues.</li> <li>4. Click <b>[Filter]</b>. The list is filtered to display only those queues matching the filter criteria.</li> </ol> |
| <b>Sort queue list</b>                     | By default, the list of queues is sorted in ascending order by Name.   |

| Action                                    | Description  |
|---|--|
| <b>based on column</b>                    | <p>Click on any column heading to re-sort the table based on that column. The following markers indicate the sorting column:</p> <ul style="list-style-type: none"> <li>▲ = The table is sorted in <i>ascending</i> alphabetical order based on the indicated column.</li> <li>▼ = The table is sorted in <i>descending</i> alphabetical order based on the indicated column.</li> </ul> |
| <b>Add a new MQ Native queue</b>          | <p>Click <b>[Add]</b> and then configure the properties for the new queue. See "MQ Native Queue Properties" on page 114 for details.</p> <p>You can also create a new MQ Native queue by clicking <b>[New Queue]</b> on the Native MQ Routing Properties dialog.</p>   |
| <b>Clone an existing MQ Native queue</b>  | <p>Select the queue to clone, then click <b>[Clone]</b>. Edit the queue properties as required. See "MQ Native Queue Properties" on page 114 for details.</p>  |
| <b>Modify an existing MQ Native queue</b> | <p>Select the queue to modify, then click <b>[Properties]</b>. Edit the queue properties as necessary. See "MQ Native Queue Properties" on page 114 for details.</p> <p><b>Note:</b> Be sure to test your new settings to ensure the connection is valid.</p>  |
| <b>Remove an MQ Native queue</b>          | <p>Select the queue to remove and then click <b>[Remove]</b>. Click <b>[OK]</b> to confirm the deletion.</p> <p><b>Note:</b> Removing a queue will unregister it from the Gateway. The queue still exists in the WebSphere MQ queue management application.</p>  |

- Click **[Test Settings]** to test the connection between the Gateway and MQ Native queue. A test is considered successful if the Gateway can:

- Read from an inbound queue
- Write to an outbound queue
- Contact any additional queue specified in the configuration (for example, a Reply-to queue, Failure queue, Wait-for-reply queue)

If a connection cannot be established, make a note of the diagnostic information that is displayed, double-check the queue and Gateway settings, and then try again. Occasionally, the queue may enter an unstable state and restarting the MQ Queue Manager and its listener could resolve the issue. If you are unsuccessful in making a successful connection, please [contact](#) CA Technical Support for assistance.

- Click **[Save]** to close the MQ Native Queue Properties. When adding a queue, the new queue is registered in the Gateway and added to the **Known MQ Native**

**Queues** table in the Manage MQ Native Queues dialog.

The **[Save]** button is unavailable if there is information missing in any of the tabs.

5. Click **[Close]** when done.

## MQ Native Queue Properties

When creating or viewing details about [MQ native queues](#), the MQ Native Queue Properties appear. The queue properties are organized across these tabs:

- MQ Connection Properties
- Inbound Options
- Outbound Options

For more information about MQ native queues, see "Managing MQ Native Queues" on page 110.

➤ *To access the properties for an MQ native queue:*

1. Run the [Manage MQ Native Queues](#) task.
2. Select a queue and then click **[Properties]**. You can also click **[Create]** to enter the properties for a new queue. The MQ Native Queue Properties appear.
3. Configure each tab within the properties as necessary. Refer to the appropriate section below for a complete description of each tab.
4. Click **[OK]** when done.

## Configuring the [MQ Connection Properties] Tab

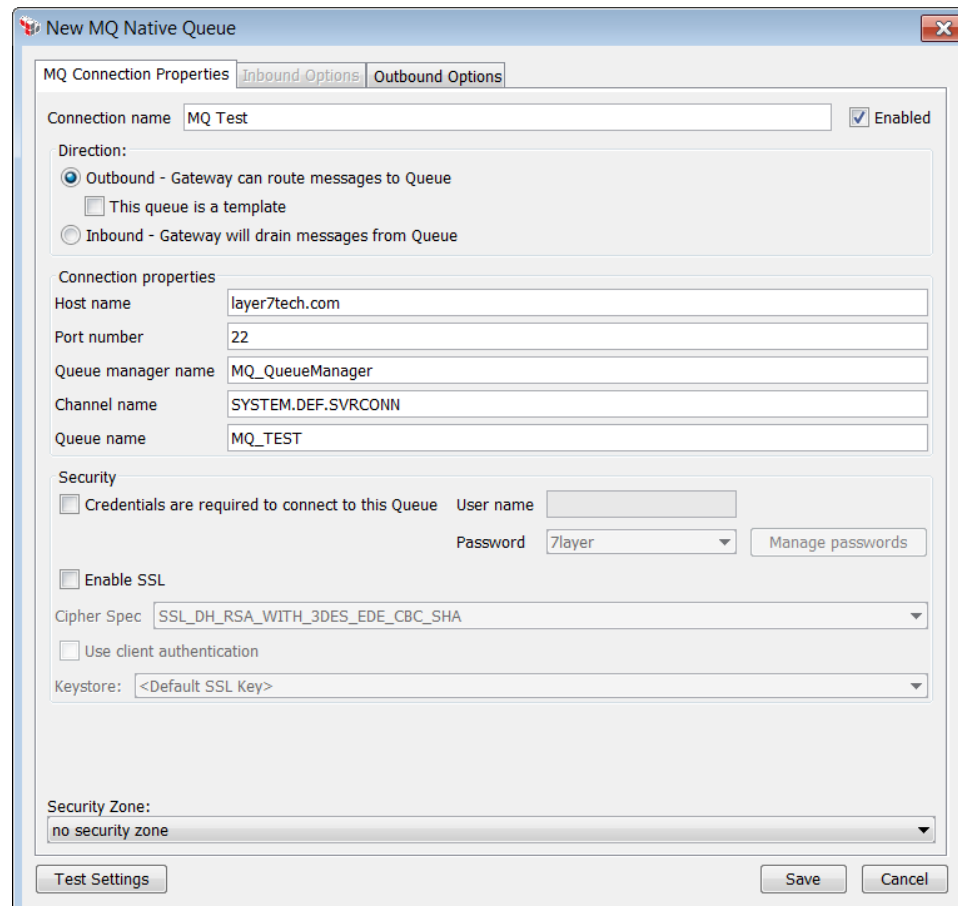


Figure 39: MQ Native Queue Properties - [MQ Connection Properties] tab

The [MQ Connection Properties] tab is used to set connection properties common to both inbound and outbound queues. Configure this tab as follows:

Table 39: MQ Native Queue Properties - [MQ Connection Properties] tab

| Setting                | Description  |
|------------------------|--|
| <b>Connection name</b> | Enter a name to identify the MQ Native connection. This name will be displayed in the policy window when the queue is selected for routing. The connection name is also displayed in the <a href="#">Managing MQ Native Queues</a> dialog box.   |
| <b>Enabled</b>         | Select this check box to enable the queue. Clear this check box to disable the queue as follows: <ul style="list-style-type: none"> <li><i>Inbound queue:</i> The listener will stop listening for messages.</li> <li><i>Outbound queue:</i> Any Route via MQ Native assertion that</li> </ul> |

| Setting                      | Description   |
|------------------------------|---|
|                              | uses this queue will stop working.  |
| <b>Direction</b>             | <p>Select the direction of the queue:</p> <ul style="list-style-type: none"> <li>• <b>Outbound:</b> The Gateway can send/route messages to the connection. Queues registered as outbound can be referenced in a CA policy workflow inside a Route via MQ Native assertion. <ul style="list-style-type: none"> <li>• Select the <b>This queue is a template</b> check box to configure a template outbound queue that allows the queue name and reply queue name to be specified later, when the Route via MQ Native assertion is configured in a policy.</li> </ul> </li> <li>• <b>Inbound:</b> The Gateway will consume messages from the connection. Queues registered as inbound will be monitored by the CA API Gateway.</li> </ul>   |
| <b>Connection properties</b> | <p>Configure the properties for the connection:</p> <ul style="list-style-type: none"> <li>• <b>Host name:</b> Enter the MQ queue end point.</li> <li>• <b>Port number:</b> Enter the MQ queue end point port number. This value must be between 1 and 65535.</li> <li>• <b>Queue manager name:</b> Enter the name of the queue manager. This name is displayed on the <a href="#">Manage MQ Native Queues</a> dialog.</li> <li>• <b>Channel name:</b> Enter the MQ queue channel name. <b>Tip:</b> If you are using an SSL connection for the MQ Native queue, be sure to specify an SSL channel name.</li> <li>• <b>Queue name:</b> Enter a name for the queue. This name is displayed on the <a href="#">Manage MQ Native Queues</a> dialog.</li> </ul>  |
| <b>Security</b>              | <p>Specify any security required to access the queue:</p> <ul style="list-style-type: none"> <li>• <b>[Credentials are required to...]:</b> Select this check box if the target MQ server requires login credentials. Clear this check box if authentication is not required.</li> <li>• <b>User name:</b> If credentials are required, enter the user name.</li> <li>• <b>Password:</b> If credentials are required, select the stored password to use from the drop-down list. <b>Note:</b> Only stored passwords may be used here—you cannot type in a password. To define a stored password, click <b>[Manage passwords]</b>. For more information, see "Managing Stored Passwords" on page 42.</li> <li>• <b>[Enable SSL]:</b> Select this check box to use an SSL connection for the MQ Native connection.</li> </ul> |

| Setting              | Description  |
|----------------------|--|
|                      | <p><b>Note:</b> Enabling SSL requires a matching Cipher Spec for the SSL channel defined on the MQ server. It also requires an SSL channel name in the "<a href="#">Channel Name</a>" field; the default channel name SYSTEM.DEF.SVRCONN cannot be used for SSL connections.</p> <ul style="list-style-type: none"> <li>• <b>Cipher Spec:</b> When connecting using SSL, choose the cipher specification to use for the SSL channel. <b>Tip:</b> If you are unsure of the cipher to use, try the default cipher first.</li> <li>• <b>[Use client authentication]:</b> When connecting using SSL, select this check box to present a certificate to the server, if one is requested. Clear this check box to never present a certificate, even if one is requested. Note that access may be denied in this case.</li> <li>• <b>Keystore:</b> From the drop-down list, choose the keystore from which to retrieve the certificate. Used only if client certificates are used.</li> </ul> |
| <b>Test Settings</b> | Click this button to test the connection settings. This button is unavailable when any required information is missing on this tab.  |
| <b>Security Zone</b> | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "<b>No security zone</b>".</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>  |

## Configuring the [Inbound Options] Tab

Figure 40: MQ Native Queue Properties - [Inbound Options] tab

The [Inbound Options] tab is used to configure inbound queues that will be monitored by the CA API Gateway. Configure this tab as follows

Table 40: MQ Native Queue Properties - [Inbound Options] tab

| Setting                     | Description  |
|-----------------------------|--|
| <b>Acknowledge Behavior</b> | <p>From the drop-down list, select how the Gateway should acknowledge incoming MQ Native messages:</p> <ul style="list-style-type: none"> <li><b>On Take:</b> The Gateway will send a reply based on the chosen "Inbound Reply Behavior" when it reads the message from the queue being monitored (this is the "Queue name" from the [MQ Connection Properties] tab).</li> <li><b>On Completion:</b> The Gateway will send a reply only after successful execution of the associated service (defined under</li> </ul> |



| Setting                             | Description   |
|-------------------------------------|---|
|                                     | <p>"Service Resolution" on this tab).</p> <p>Using "On Completion" acknowledgment increases the reliability of message processing. If a Gateway fails during the processing of a message, that message will remain in the queue and can be processed by another node. (This assumes that a cluster of nodes has been configured. For more information, see "Configure a Gateway Cluster" in the <i>Layer 7 Installation and Maintenance Manual</i>.)</p> <p><b>Notes:</b> (1) If you have not configured a failure queue, then messages that consistently fail (for example, a backend service is non-functional) will remain in the queue indefinitely. The Gateway will continually try to process these messages and may get stuck in a loop, unless a failure queue is configured. (2) The Protect Against Message Replay assertion should not be used in any policy that will process messages from queues that are configured with the "On completion" acknowledgment mode without a specified failure destination.</p> |
| <b>Inbound Reply Behavior</b>       | <p>Select a reply behavior for the inbound queue:</p> <ul style="list-style-type: none"> <li>• <b>Automatic:</b> Choose this option to have the Gateway send a reply if the <i>MQReplyTo</i> queue name is specified in the message/header attribute.</li> <li>• <b>Do not send replies:</b> Choose this option to never send a reply to any queue.</li> <li>• <b>Send reply to specified queue:</b> Choose this option to send replies to a specific queue, overriding any <i>replyToQueueName</i> attribute in the MQ message descriptor (MQMD) attribute in inbound messages. Enter the name of the queue in the adjacent box.</li> </ul>  |
| <b>Request/Response Correlation</b> | <p>The inbound Request/Response correlation behavior can be specified if either the "Automatic" or "Send reply to specified queue" option was selected:</p> <ul style="list-style-type: none"> <li>• <b>Copy CorrelationID from Request to Response:</b> Choose this option to copy the Correlation ID from the request to the response.</li> <li>• <b>Set Response CorrelationID from Request's MessageID:</b> Choose this option to use the Message ID from the request as the Correlation ID in the response.</li> </ul>   |
| <b>Service Resolution</b>           | <p>Select how the service should be resolved:</p> <ul style="list-style-type: none"> <li>• <b>Associate queue with published service (bypass resolution):</b><br/>Select this check box to associate the inbound MQ Native queue with a specific published service, bypassing the normal service resolution logic. <ul style="list-style-type: none"> <li>• <b>Service name:</b> If associating with a service, choose the</li> </ul> </li> </ul>   |

| Setting  | Description  |
|--|--|
|  | <p>service from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Specify content type:</b> Select this check box to override the content type.</li> <li>• <b>Use Content Type:</b> If overriding the content type, choose the content type to use from the drop-down list. If the content type you need isn't listed, type it directly into the drop-down list.</li> </ul>  |
| <b>Send failed requests to the specified queue</b> | <p>Select this check box to route the message to a special queue if the service policy does not successfully complete.</p> <p>The messages sent to the failure queue are not due to a Gateway failure, but rather from other causes such as routing failure, message content, etc.</p> <p>If this check box is not selected, then the MQ Native configuration will be expected to ensure that messages that could not be processed do not remain in the queue indefinitely.</p> <p>This option is available only when <b>Acknowledgment Behavior</b> is set to "On Completion".</p> <ul style="list-style-type: none"> <li>• <b>Failure queue name:</b> If sending requests to a failure queue, enter the name of the queue that will receive messages that were not successfully processed</li> </ul> |
| <b>Specify multiple inbound connections</b>        | <p>Select this check box to set the maximum number of concurrent inbound connections permitted. The default is <b>20</b>.</p> <p>Clear this check box restrict concurrency to a single inbound connection with this queue configuration .</p> <p><b>Note:</b> The <i>mq.listenerMaxConcurrentConnections</i> property specifies the absolute maximum concurrency and will override any larger value entered here.</p>  |
| <b>Override maximum message size</b>               | <p>Select this check box to override the permitted maximum size of the message.</p> <p>Clear this check box to use the value set in the <a href="#">io.mqMessageMaxBytes</a> cluster property.</p> <ul style="list-style-type: none"> <li>• <b>Restrict messages to:</b> Enter the maximum permitted size of the message, in bytes.</li> <li>• <b>Allow unlimited message size (not recommended):</b> Select this option to allow response messages of unlimited size. This is not recommended and should be used only under the direction of CA Technical Support.</li> </ul>   |

## Configuring the [Outbound Options] Tab

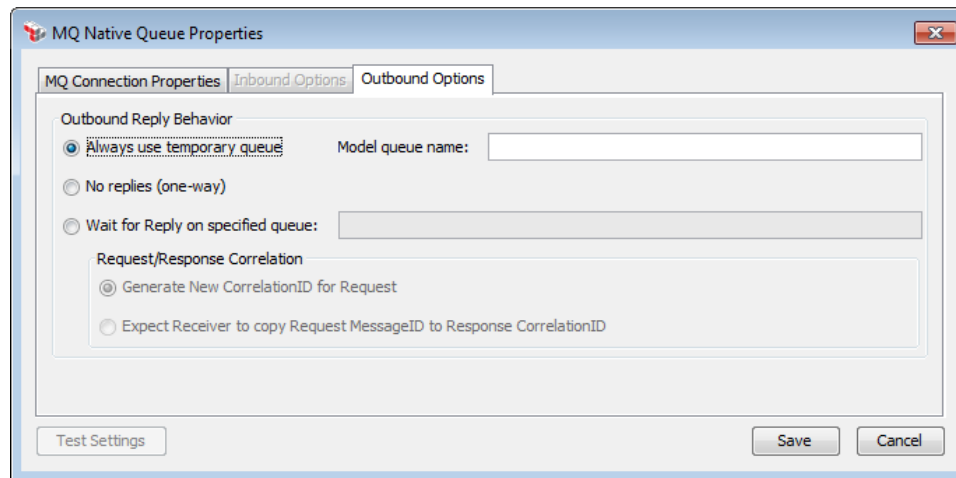


Figure 41: MQ Native Queue Properties - [Outbound Options] tab

The [Outbound Options] tab is used to configure outbound queues that can be referenced in a Route via MQ Native assertion. Configure this tab as follows

Table 41: MQ Native Queue Properties - [Outbound Options] tab

| Setting                        | Description  |
|--------------------------------|--|
| <b>Outbound Reply Behavior</b> | <p>Specify an outbound reply behavior for the queue:</p> <ul style="list-style-type: none"> <li> <b>Always use temporary queue:</b> Choose this to always create a temporary dynamic queue for each request. Use this temporary queue as the reply queue for outbound requests and listen for a response on this queue. <ul style="list-style-type: none"> <li> <b>Model queue name:</b> Enter an input mask for the temporary dynamic queue name. For example, the model name, <code>SYSTEM.DEFAULT.MODEL.QUEUE</code> might create a temporary dynamic queue named: <code>SYSTEM.DEFAULT.MODEL.QUEUE.4F14B2E020012504</code>.<br/><br/>The model queue must be a permanent queue created by the MQ administrator (for example, <code>MQQDT_PREDEFINED</code>). </li> </ul> </li> <li> <b>No replies (one way):</b> Choose this to not send a reply or wait for a request on the queue. The response to the requestor will be empty, unless some other assertion fills it in. </li> <li> <b>Wait for Reply on specified queue:</b> Choose this to have the Gateway look up the specified queue and then wait on that queue for the response. Enter the name of the queue in the adjacent box. <p><b>Tip:</b> If this queue is to be a <a href="#">template</a>, the dynamic properties setting for "Wait for Reply on specified queue" will be available only if this</p> </li> </ul> |

| Setting                             | Description   |
|-------------------------------------|---|
|                                     | outbound reply behavior is set here, and the queue name box is left blank.  |
| <b>Request/Response Correlation</b> | <p>If the <b>Outbound Reply Behavior</b> is "Wait for a Reply on a specified queue", select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Generate New CorrelationID for Request:</b> Choose this to have the Gateway generate a unique ID, set it as the <i>CorrelationID</i> attribute on the outbound request, and then select only messages with the matching CorrelationID value from the reply queue.</li> <li>• <b>Expect Receiver to Copy Request MessageID to Response CorrelationID:</b> Choose this to send the request message as-is, then select only messages with the <i>CorrelationID</i> attribute matching the outbound request's <i>MessageID</i> attribute from the reply queue.</li> </ul> |

## Customizing MQ Messages

You can customize MQ Message by adding values to existing messages. You must have a valid MQ Native Queue configured before proceeding. See the "Managing MQ Native Queues" on page 110 for more information.

The diagram below illustrates the process of configured messages passing through the descriptor, message properties, and headers.

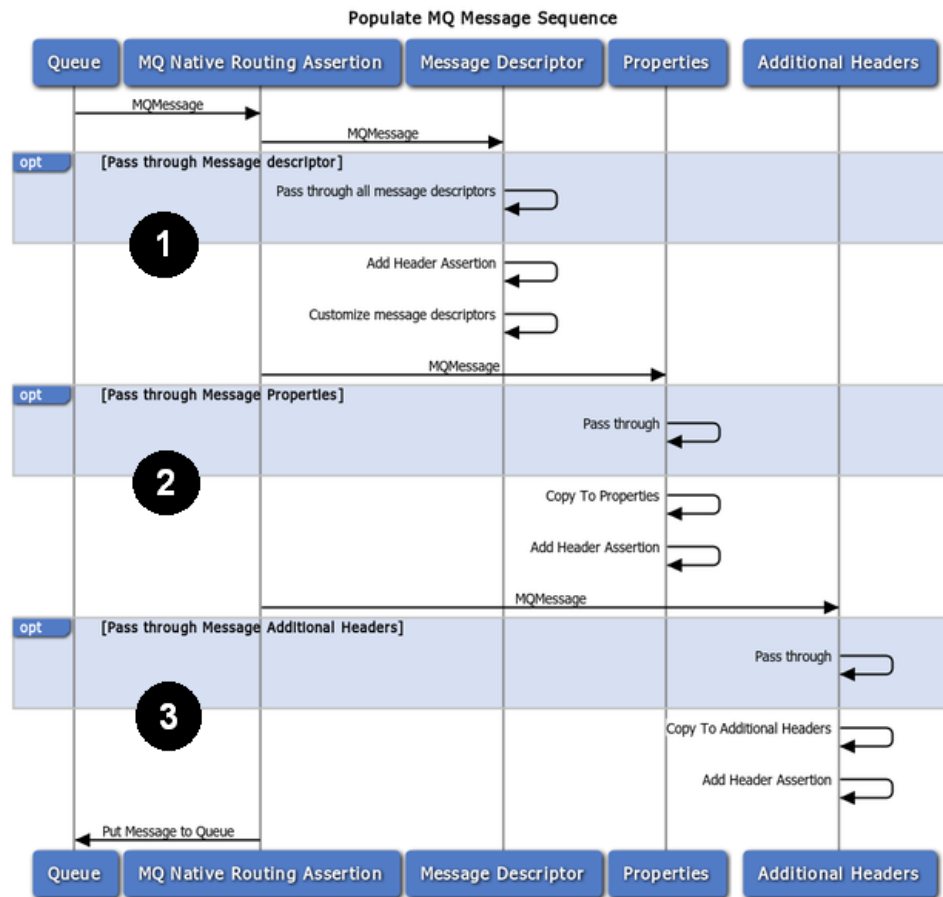


Figure 42: MQ Message sequence diagram

The sequence of applying the values is important. Below is a general sequence for each section.

- ❶ Message Descriptors
  1. Passes through all message descriptors
  2. Manage Transport Properties/Headers assertion
  3. Customized message descriptors in the Route via MQ Native assertion
- ❷ Message Properties
  1. Pass through
  2. Copy to Properties
  3. Manage Transport Properties/Headers assertion
- ❸ Message Additional Headers
  1. Pass through
  2. Copy to Additional Headers
  3. Manage Transport Properties/Headers assertion

## Customizing MQ Message Descriptors

**Note:** The following procedures to be used for only policies that existed prior to version 8.0.

➤ To access the message descriptors:

1. Add the Route via MQ Native assertion in the policy window and select **MQ Native Routing Properties** or double-click the assertion in the policy window.
2. In the [Request] and [Response] tabs, select the **Pass through all MQ message headers** check box. The value of the descriptor from the original MQ message will be passed to the message result.
3. Go to either the [Request] or [Response] tabs and view the "Customize message descriptors" section, as shown in Figure 43.

| Name         | Value  |
|--------------|--------|
| format       | sample |
| characterSet | w      |

Add Edit Remove

Figure 43: Customize message descriptors

4. Configure the message descriptors as follows.

Table 42: Customize message descriptors settings

| To...                                  | Do this...   |
|--|--|
| <b>Add a new message descriptor</b>    | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>.</li> <li>2. See "<a href="#">Adding a New Message Descriptor</a>" below for more information.</li> <li>3. Click <b>[OK]</b> when done</li> </ol> |
| <b>Edit a new message descriptor</b>   | <ol style="list-style-type: none"> <li>1. Select the item to edit.</li> <li>2. Click <b>[Edit]</b> and then modify the values as required.</li> <li>3. Click <b>[OK]</b> when done</li> </ol>                  |
| <b>Remove a new message descriptor</b> | <ol style="list-style-type: none"> <li>1. Select the item to remove.</li> <li>2. Click <b>[Remove]</b>.</li> <li>3. Click <b>[OK]</b> to confirm the deletion..</li> </ol>                                     |

### Adding a New Message Descriptor

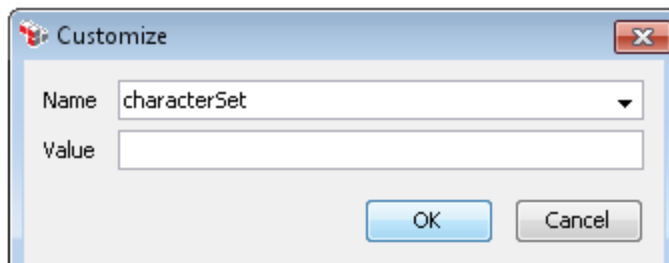


Figure 44: Adding a customized message descriptor

1. Choose the name of the message descriptor from the "Name" drop-down list. By default, only the descriptors visible in the list can be used.

---

**Tip:** If you wish to use MQ message descriptors not shown in the list, set the cluster property [io.mqRoutingSetAllContext](#) to "true". This will allow you to specify message descriptors not visible in the list. To do this, type in the descriptor name in the "Name" field.

---

Note that the following message descriptors cannot be set, even when the cluster property is set to "true":

*backoutCount*  
*messageSequenceNumber*  
*originalLength*

2. Enter the value of the message descriptor in the "Value" field. You may reference a [context variable](#).
3. Click **[OK]**.

Alternatively, you can use the Manage Transport Properties/Headers assertion to customize the message descriptor.

## Managing Email Listeners

You can configure the Gateway to periodically poll an email server for SOAP messages to process. If a new message is found, it is retrieved from the server and processed.

An email listener can receive emails from either a POP3 server or an IMAP 4/IMAP4rev1 server and supports SSL encryption. Multiple email listeners may be configured at once. While the Gateway can process SOAP messages from email traffic, it cannot return a response.

Email listeners can use the internal trust store for trusting email server certificates when using SSL. If the certificate is signed by a root signing authority, then it is trusted. If not, then you must import the certificate into the trust store and specify that the certificate is trusted for outbound SSL connections. For more information, see "Add Certificate Wizard" on page 240; in step 3, select the "Outbound SSL Connection" option.

➤ To manage email listeners:

1. In the Policy Manager, select **[Tasks] > Manage Email Listeners** from the **Main Menu** (on the **browser client**, from the **Manage** menu). The Manage Email Listeners dialog appears.

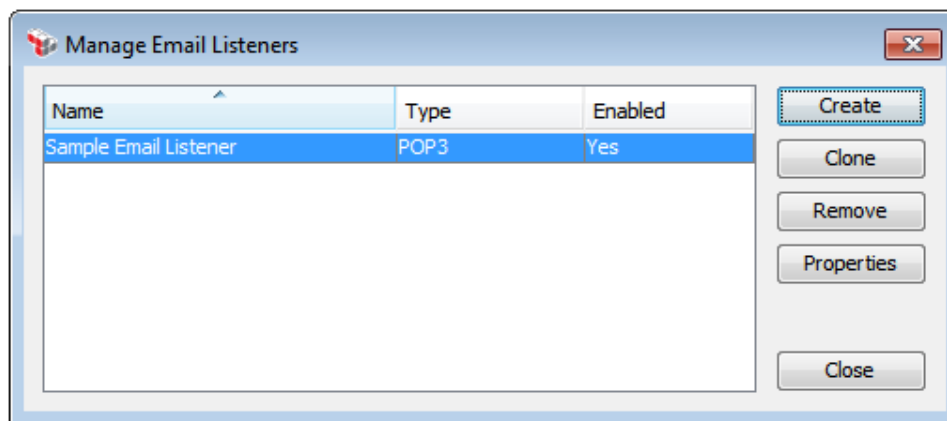


Figure 45: Manage Email Listeners form

2. The email listeners configured are displayed. Choose an action to perform:

Table 43: Managing email listener tasks

| To...                              | Do this...  |
|------------------------------------|---|
| <b>Create a new email listener</b> | <ol style="list-style-type: none"> <li>1. Click <b>[Create]</b>. The Add Email Listener dialog appears.</li> <li>2. Configure the new listener. For a description of each property, see "Email Listener Properties" on page 127.</li> </ol> |



| To...  | Do this...   |
|--|--|
| <b>Clone an existing email listener</b>                  | <ol style="list-style-type: none"> <li>1. Select the listener to clone.</li> <li>2. Click <b>[Clone]</b>.</li> <li>3. Edit the "Email Listener Properties" on page 127 as required.</li> </ol>   |
| <b>Remove an email listener</b>                          | <ol style="list-style-type: none"> <li>1. Select the listener to remove.</li> <li>2. Click <b>[Remove]</b>. The listener is removed from the list.</li> </ol> <p><b>Tip:</b> As an alternative to remove the listener, you can disable it instead. To disable a listener, view its properties and clear the <b>Active</b> check box.</p> |
| <b>View or edit the properties for an email listener</b> | <ol style="list-style-type: none"> <li>1. Select the listener to view or edit.</li> <li>2. Click <b>[Properties]</b>. The <a href="#">Email Listener Properties</a> dialog is displayed.</li> <li>3. Edit the properties as required.</li> </ol>   |

3. Click **[Close]** when done.

## Email Listener Properties

When creating or viewing details about an [email listener](#), the Email Listener Properties appear. This dialog lets you retrieve SOAP messages from a POP or IMAP mail server for processing by the Gateway.

➤ *To access the properties for an email listener:*


1. Run the [Manage Email Listeners](#) task.
2. Select an email listener from the list and then click **[Properties]**. You can also click **[Create]** to enter the properties for a new listener. The Email Listener Properties appear.

Figure 46: Email Listener Properties dialog

3. Configure the properties as follows:

Table 44: Email listener settings

| Setting            | Description   |
|--------------------|---|
| <b>Name</b>        | Enter the name of the email listener. If you are creating several listeners, make sure the name is descriptive.   |
| <b>Active</b>      | Select this check box to make the listener active. Clear this check box to deactivate the listener. Deactivating a listener is an alternative to removing it. |
| <b>Hostname</b>    | Enter the hostname of the email server. This name is verified against the X.509 certificate.  |
| <b>Port</b>        | Enter the port number to monitor.   |
| <b>Server Type</b> | From the drop-down list, select the type of email server (POP3 or IMAP).  |
| <b>Use SSL</b>     | Select this check box to use a secure connection (POP3S or IMAPS). Clear the check box to use a standard connection.  |

| Setting  | Description  |
|--|--|
| <b>Delete on Receive</b>                               | Select this check box to delete the messages on the mail server after retrieving. Clear this check box to keep the messages on the server.   |
| <b>Username</b>  | Enter the email account name.  |
| <b>Password</b>  | Enter the email account password.  |
| <b>Folder</b> (only for IMAP)                          | Select the folder name to check for emails. In most cases, this will be the "Inbox" folder. To change the folder, click <b>[Browse]</b> and select another folder.<br><br>This setting is valid only for IMAP mail servers.  |
| <b>Interval</b>  | Indicate the polling interval, in seconds. The listener will check for email after the specified number of seconds.  |
| <b>Associate email listener with published service</b> | Select this check box to associate the email listener with a published service, bypassing the resolution process normally used to determine the service.<br><br>Clear this check box to use the normal service resolution process. To learn more about how the Gateway determines the service, see <i>Understanding the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i> .   |
| <b>Service name</b>                                    | If associating an email listener with a specific service, select the service from the drop-down list. If the service you want is not in the list, you must <a href="#">publish</a> it first.   |
| <b>Override maximum message size</b>                   | Select this check box to override the permitted maximum size of the message. Clear this check box to use the value set in the <a href="#">io.EmailListenerMessageMaxBytes</a> cluster property. <ul style="list-style-type: none"> <li>• <i>Restrict messages to:</i> Enter the maximum permitted size of the message, in bytes. You may reference context variables. </li> <li>• <i>Allow unlimited message size (not recommended):</i> Select this option to allow response messages of unlimited size. This is not recommended and should be used only under the direction of CA Technical Support.</li> </ul> |
| <b>Security Zone</b>                                   | Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b> .<br><br>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i> .<br><br><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).   |

4. Click **[OK]** when done.

## Managing Roles

The Policy Manager uses security roles that control user permissions. A user must be assigned to at least one of these roles in order to [connect to the Gateway](#) and perform administrative tasks in the Policy Manager. The Policy Manager has a number of factory-defined roles, plus you can create your own custom roles to tailor permissions specifically. In addition, performing certain tasks automatically create accompanying security roles. These auto-created roles are the "Manage [name]..." and "View [name]..." roles in "Predefined Roles and Permissions" on page 132. **Tip:** The auto-creation of these roles can be turned off by using the `rbac.autoRole.manage<name>.autoAssign` [cluster properties](#), where "<name>" is "Policy", "Provider", or "Service".

---

**IMPORTANT:** Creating custom roles is an advanced feature that requires careful planning and forethought. The system will not check the validity of custom roles, so it is possible to create roles that either have no effect or which produce unexpected results.

---

A user added to a role automatically inherits all the permissions defined for that role. If a user is added to multiple roles, the user receives permissions from *all* the roles. For example, user Bob is a member of the *Operators* role. He can view (but not update) anything in the system. Sue is a member of the *Operators* and *Publish Web Services* roles. She can view anything in the system and also publish web services.

Users may be added to roles either directly or indirectly when a group to which a user belongs is added to a role.

Role-based permissions provide a fast and flexible way to control user operations and maintain the integrity of your data.

For a description of all the predefined roles in Policy Manager, see "Predefined Roles and Permissions" on page 132.

---

**Note:** If a user has the same username and password in both the internal identity provider and in a LDAP identity provider, the Policy Manager will use the roles associated with the internal identity provider first. If multiple users share a login ID, they are differentiated by their passwords.

---



---

**Tip:** If a user is denied permission to perform a task and you are certain that permission has been granted, check whether the number of group memberships for that user exceeds the `principalSessionCache.maxPrincipalGroups` [cluster property](#).

---

➤ *To manage roles:*

1. In the Policy Manager, select **[Tasks] > Manage Roles** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Roles dialog appears.

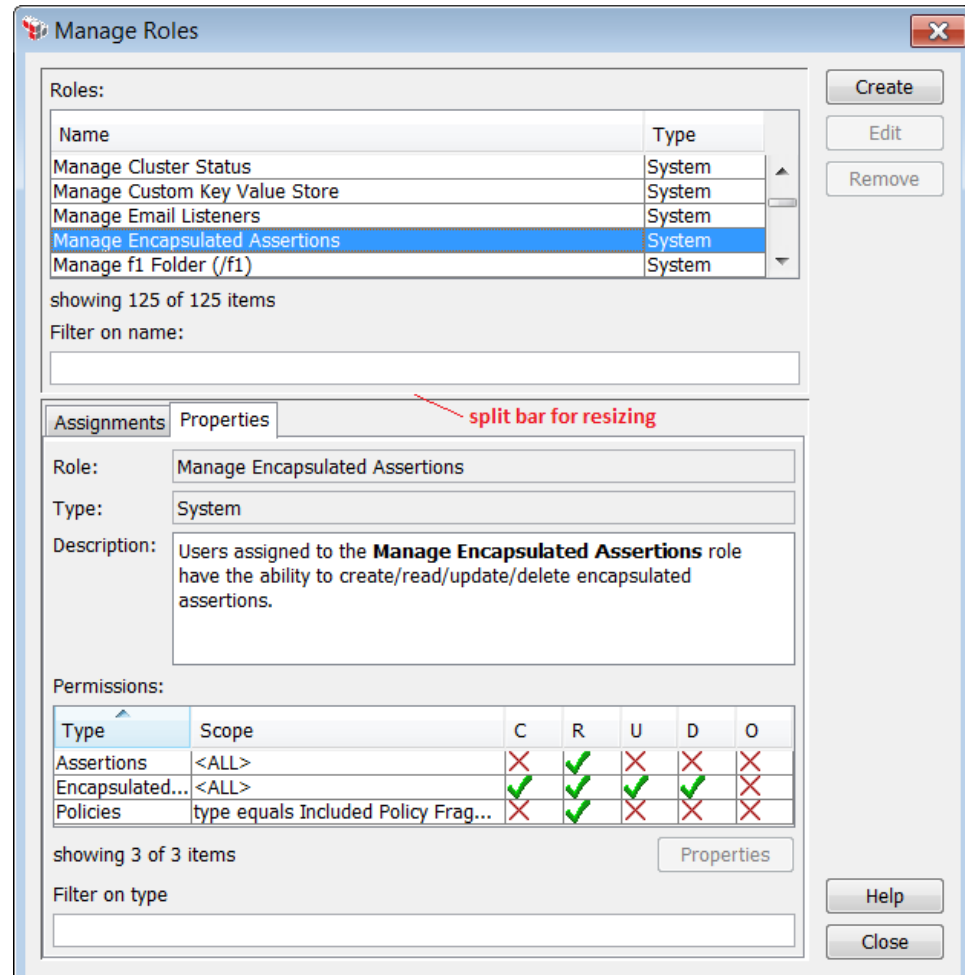


Figure 47: Manage Roles dialog

The following table describes the various elements in the dialog:

Table 45: Manage Roles dialog

| Element              | Description   |
|----------------------|---|
| <b>Roles table</b>   | Displays all the roles in the system. "System" indicates roles that are factory-predefined and auto-created roles. "Custom" indicates roles created by end users. |
| <b>Create button</b> | Click this to create a new custom role. For more information, see "Creating a Custom Role" on page 149.   |
| <b>Edit button</b>   | Click this to modify an existing custom role. For more information, see "Editing a Custom Role" on page 150   |
| <b>Remove button</b> | Click this to delete a custom role. For more information, see "Deleting a Custom Role" on page 151.   |

Table 45: Manage Roles dialog

| Element                | Description  |
|------------------------|--|
| <b>Filter on name</b>  | This filters the roles list to display only those roles containing the filter text. Delete the filter text to restore the full list of roles.  |
| <b>Assignments tab</b> | Lists the users and/or groups that have been assigned to the role. Use this tab to add or remove users and group from the role. For more information, see "Adding a User or Group to a Role" on page 152 and "Removing a User or Group from a Role" on page 152. |
| <b>Properties tab</b>  | Displays information about the role (Name, Type, Description). It also provides detailed information about the permissions granted by that role. For more information, see "Understanding Role Permissions" on page 137  |

**Tip:** The split bar may be used to adjust the spacing allocated to the Roles list vs. the Assignment/Properties tabs.

2. Click **[Close]** when done.

## Predefined Roles and Permissions

There are a number of roles and permissions predefined in Policy Manager. Any user added to a [role](#) automatically inherits the permissions for that role. If a user is added to multiple roles, that user is granted permissions from all the roles.

**Note:** The Policy Manager currently does not support creating new roles or modifying the permissions of existing roles.

Table 46: Predefined roles and permissions

| Role                       | Permissions   | For more information, see...   |
|----------------------------|---|--|
| <b>Administrator</b>       | Create, read, update, and delete any object in the system.  | This role provides unrestricted access to the Gateway.<br><br>The Policy Manager describes the features from an Administrator perspective. |
| <b>Gateway Maintenance</b> | Create, read, and update configuration for the FTP Audit Archiver. Delete any audit record.<br><br><b>Note:</b> The hidden cluster property <i>audit.archiver.ftp.config</i> stores the configuration of the FTP Audit Archiver that is visible on the interface. Contact CA Technical Support if you need to modify this property. | "FTP Audit Archiver" on page 413   |

| Role  | Permissions  | For more information, see...   |
|---|--|--|
| <b>Invoke Audit Viewer Policy</b>                   | Users with this role will be permitted to invoke the Audit Viewer Policy.  | <p>"Invoking the <a href="#">Audit Viewer Policy</a>" in "Gateway Audit Events" on page 415</p> <p>Working with Internal Use Policies in the <i>Layer 7 Policy Authoring User Manual</i></p> |
| <b>Manage Administrative Accounts Configuration</b> | <p>Create, read, and update cluster properties applicable to administrative account configuration: <i>logon.maxAllowableAttempts</i>, <i>logon.lockoutTime</i>, <i>logon.sessionExpiry</i>, and <i>logon.inactivityPeriod</i>.</p> <p><b>Tip:</b> These cluster properties can also be set using the <a href="#">Manage Administrative Users</a> task.</p> | <p>"Managing Administrative User Account Policy" on page 301</p> <p>"Appendix D: Gateway Cluster Properties" on page 567</p>   |
| <b>Manage Certificates (truststore)</b>             | Create, read, update, and delete trusted certificates and policies for revocation checking.  | <p>"Chapter 3: Managing Certificates" on page 237</p> <p>"Managing Certificate Validation" on page 251</p>   |
| <b>Manage Cluster Properties</b>                    | Create, read, update, and delete any cluster property.   | <p>"Managing Cluster-Wide Properties" on page 40</p> <p>"Appendix D: Gateway Cluster Properties" on page 567</p>   |
| <b>Manage Cluster Status</b>                        | Create, read, update, and delete cluster status information.   | "Dashboard - Cluster Status" on page 406   |
| <b>Manage Custom Key Value Store</b>                | Create, read, update, and delete key values from custom key value store.   | Custom Assertions API  |
| <b>Manage Email Listeners</b>                       | Create, read, update, and delete email listeners.  | "Managing Email Listeners" on page 126   |
| <b>Manage Encapsulated Assertions</b>               | Create, read, update, and delete encapsulated assertions. Read any policy fragment. Read all assertions.   | <p>Managing Encapsulated Assertions in the <i>Layer 7 Policy Authoring User Manual</i></p> <p>Working with Policy Fragments in the <i>Layer 7 Policy Authoring User Manual</i></p>           |
| <b>Manage Firewall Rules</b>                        | Create, read, update, and delete firewall rules.   | "Managing Firewall Rules" on page 78   |
| <b>Manage JDBC</b>                                  | Create, read, update, and delete JDBC  | "Managing JDBC   |

| Role                               | Permissions  | For more information, see...  |
|------------------------------------|--|---|
| <b>Connections</b>                 | connections.   | Connections" on page 82.  |
| <b>Manage Listen Ports</b>         | Create, read, update, and delete Gateway listen ports (both HTTP(S) and FTP(S)) and to list published services.  | "Managing Listen Ports" on page 54  |
| <b>Manage Log Sinks</b>            | Create, read, update, and delete log sinks. Read access to the following entities:<br><i>Email listeners</i><br><i>Folders</i><br><i>Identity Providers</i><br><i>JMS Destinations</i><br><i>Listen ports</i><br><i>Log files</i><br><i>Policies</i><br><i>Services</i><br><i>Users</i>  | "Managing Email Listeners" on page 126<br>Organizing Services and Policies into Folders in the <i>Layer 7 Policy Authoring User Manual</i><br>"Chapter 4: Working with Identity Providers" on page 279<br>"Managing JMS Destinations" on page 89<br>"Managing Listen Ports" on page 54<br>"Managing Log Sinks" on page 164<br>"Viewing Logs" on page 409<br>Policies in the <i>Layer 7 Policy Authoring User Manual</i><br>"Chapter 5: Working with Services" on page 331 |
| <b>Manage Message Destinations</b> | Create, read, update, and delete message destinations. This includes: <ul style="list-style-type: none"> <li>Create, read, update, and delete JMS Connections</li> <li>Create, read, update, and delete JMS Endpoints</li> <li>Create, read, update, and delete Polling Listeners</li> <li>Read Private Keys</li> <li>Read Private Key Stores</li> <li>Read Published Services</li> <li>Read Secure Passwords</li> </ul> | "Managing JMS Destinations" on page 89<br>"Managing Listen Ports" on page 54<br>"Managing Private Keys" on page 260<br>"Managing Published Services" on page 356<br>"Managing Stored Passwords" on page 42  |
| <b>Manage Password Policies</b>    | Read and update the password policy.   | "Managing Password Policy" on page 48   |



| Role                                   | Permissions  | For more information, see...   |
|--|--|--|
|  |  |  |
| <b>Manage Private Keys</b>             | Create, read, update, and delete private keys, as well as ability to change the default SSL key and default CA key.  | "Managing Private Keys" on page 260<br>"Private Key Properties" on page 271  |
| <b>Manage Secure Passwords</b>         | Read, create, update, and delete any stored password.  | "Managing Stored Passwords" on page 42   |
| <b>Manage SiteMinder Configuration</b> | Read, create, update, and delete SiteMinder configurations. This includes the Read all secure passwords.   | "Managing SiteMinder Configurations" on page 220<br>"Managing Stored Passwords" on page 42   |
| <b>Manage UDDI Registries</b>          | Create, read, update, and delete any UDDI registry connection.   | Managing UDDI Registries in the <i>Layer 7 Policy Authoring User Manual</i><br>Publish to UDDI Settings in the <i>Layer 7 Policy Authoring User Manual</i><br>"Service Properties" on page 357   |
| <b>Manage Web Services</b>             | Publish any new web service and edit existing users. Edit a global policy fragment.<br><br>Create, read, update any policy. Delete any policy, excluding global policy fragments, internal policies, and policy fragments.<br><br>Read any encapsulated assertion.                                       | "Working with SOAP Web Services" on page 331<br><br>Working with Global Policy Fragments in the <i>Layer 7 Policy Authoring User Manual</i><br>"Service Properties" on page 357<br><br>Working with Internal Use Policies in the <i>Layer 7 Policy Authoring User Manual</i> .<br><br>Working with Policy Fragments in the <i>Layer 7 Policy Authoring User Manual</i> . |
| <b>Manage [name]Folder</b>             | Create, read, update, and delete the contents, including aliases*, of the named folder. If there are nested sub folders, these privileges extend to the sub folder and its contents as well.<br><br>* Only if user also has a role granting access to the original service or policy. The type of folder | Organizing Services and Policies into Folders in the <i>Layer 7 Policy Authoring User Manual</i><br><br>Working with Aliases in the <i>Layer 7 Policy Authoring User</i>   |

| Role                                       | Permissions  | For more information, see...   |
|--|--|--|
|  | <i>role ('Manage' or 'View') does not affect what can be done to an alias.</i>   | <i>Manual</i>  |
| <b>Manage [name] Identity Provider</b>     | Read, update, and delete the named identity provider. Also create, search, update, and delete its users and groups.                                    | "Federated Identity Providers" on page 440<br>"LDAP Identity Providers" on page 303<br>"Federated Identity Provider Users and Groups" on page 445  |
| <b>Manage [name] Policy</b>                | Read, update, and delete the named policy (either included fragment, global fragment, or internal use policy).<br><br>Read any encapsulated assertion. | Creating a Policy in the <i>Layer 7 Policy Authoring User Manual</i><br><br>Working with Encapsulated Assertions in the <i>Layer 7 Policy Authoring User Manual</i>  |
| <b>Manage [name] Service</b>               | Read, update, and delete the named service.  | "Chapter 5: Working with Services" on page 331<br><a href="#">Service Properties</a><br>Working with Encapsulated Assertions in the <i>Layer 7 Policy Authoring User Manual</i>  |
| <b>Manage [name] Zone</b>                  | Create, read, update, and delete entities in the named security zone.<br><br>View the root node folder.  | <a href="#">Understanding Security Zones</a><br><a href="#">Managing Security Zones</a>  |
| <b>Operator</b>                            | Read-only access to the Gateway.   | Similar to the <i>Administrator</i> role, except permissions are read only. To allow other permissions, assign other roles.<br><br>Policy changes made with an Operator role cannot be saved (both <b>[Save]</b> and <b>[Save and Activate]</b> buttons are disabled). However, policy changes can be preserved by exporting the policy. |
| <b>Publish External Identity Providers</b> | Create any external (LDAP or Federated) Identity Provider.   | "Federated Identity Providers" on page 440<br>"LDAP Identity Providers" on page 303  |

| Role                           | Permissions   | For more information, see...   |
|--------------------------------|---|--|
| <b>Publish Web Services</b>    | Publish any new web service.<br>Read any encapsulated assertion.  | "Publish SOAP Web Service Wizard" on page 333<br>"Searching Identity Providers" on page 459<br>Working with Encapsulated Assertions in the <i>Layer 7 Policy Authoring User Manual</i> |
| <b>Search Users and Groups</b> | Search and view users and groups in all identity providers.   | "Searching Identity Providers" on page 459   |
| <b>View [name] Folder</b>      | View the contents of the named folder, including the contents of any nested folders. Does not imply permission to view aliases, unless user also holds a role granting access to the original service or policy. The type of folder role ('Manage' or 'View') does not affect what can be done to an alias.<br><br><b>Note:</b> If a folder is nested within another folder, this role can see the parent folder(s) but not the contents of the parent folders. | Organizing Services and Policies into Folders in the <i>Layer 7 Policy Authoring User Manual</i><br><br>Working with Aliases in the <i>Layer 7 Policy Authoring User Manual</i>        |
| <b>View Audit Records</b>      | View audits in the Policy Manager.  | "Gateway Audit Events" on page 415<br>"Viewing Logs" on page 409   |
| <b>View Service Metrics</b>    | View any cluster node information, published service, service metrics bin, and service usage record.  | "Dashboard - Cluster Status" on page 406   |
| <b>View [name] Log Sink</b>    | View the contents of the named log sink, including any log files associated with the sink.  | "Viewing Logs" on page 409<br>"Managing Log Sinks" on page 164   |
| <b>View [name] Zone</b>        | View the entities within the named security zone.<br>View the root node folder.   | "Understanding Security Zones" on page 156   |

## Understanding Role Permissions

When you view a role in the [Manage Roles](#) dialog, the permissions for that role are displayed in the [Properties] tab. These permissions describe precisely what access is permitted to specific entities in the system when a user is assigned to that role.

Note that the "Add Permissions to Role Wizard" on page 142 may result in the construction of multiple permission entries.

*Example:*

You make the following selections in the wizard:

*All objects*  
*Read, Update*  
*Include Folder A*  
*Include Zones A & B*  
*All entities with name starting with "A"*  
*ID starts with 12*

This will result in these permission groups:

*RU on All Entities in folder "Folder A", in security zone "Zone A", Name starts with A, ID starts with 12*  
*RU on All Entities in folder "Folder A", in security zone "Zone B", Name starts with A, ID starts with 12*

You can deduce whether a permission will result in a single or multiple permission group by the logic involved in the permission:

- If it is technically possible for an object to meet *all* the conditions, a single permission group is created ("AND" logic applies).
- If it is *not* possible for an object to meet all the conditions, multiple permission groups are created ("OR" logic applies).

In our example, objects can only exist in a single zone (Zone A OR Zone B), so the permission is split into two groups. By comparison, it is possible for an object to have a name that starts with "A" and an ID that starts with "12", so they remain in the same permission group.

Figure 48 shows an example of the Permissions table in the [Properties] tab:

Permissions:

| Type            | Scope                              | C | R | U | D | O |
|-----------------|------------------------------------|---|---|---|---|---|
| Assertions      | <ALL>                              | ✗ | ✓ | ✗ | ✗ | ✗ |
| Encapsulated... | <ALL>                              | ✗ | ✓ | ✗ | ✗ | ✗ |
| Folders         | ancestors of folder "admin-f1 / /a | ✗ | ✓ | ✗ | ✗ | ✗ |

showing 17 of 17 items

Properties

Figure 48: Permissions for a role

When there are many entries in the Permissions table, you can type a few characters in the "Filter on type" box to filter the list by Type.

The following is a description of each column:

Table 47: Columns in the Permissions table

| Column       | Description  |
|--------------|--|
| <b>Type</b>  | This is the entity type—for example, Folders, Policies, Private Key, etc. When Type = "<ALL>", it means the privileges are applied to all entity types.  |
| <b>Scope</b> | <p>This dictates the scope of the permission for the entity type: "&lt;ALL&gt;" means all entities of that entity type are included, otherwise the scope is given in a straightforward description. The scope may be any of the following:</p> <ul style="list-style-type: none"> <li>• The specific entity affected by the permission.</li> <li>• Any entities that meet the specified comparison shown (for example, "ID equals 1234" or "name starts with 'A'").</li> <li>• A security zone name when privileges are restricted to entities in a specific security zone.</li> <li>• A path and folder name when privileges are restricted to entities in a specific folder.</li> </ul> <p>Keep in mind the following:</p> <ul style="list-style-type: none"> <li>• If there is not enough space to show the full scope in the table, you can click [Properties] to see the complete text in a dialog box.</li> <li>• Simpler scopes are shown in the table (possibly truncated), however more complex scopes involving multiple conditions are shown as "&lt;complex scope&gt;". In this case you must use the Properties button to see the scope.</li> <li>• If the entity is located in the folder tree and privileges apply to its parents folders higher up in the tree, the text "ancestors of" is added before the text.</li> </ul> |
| <b>C</b>     | Role has permission to create entities of this type.   |
| <b>R</b>     | <p>Role has permission to read (view) entities of this type in the Policy Manager interface. The entity will be visible in the GUI.</p> <p><b>Tip:</b> Read permission is required in order to Update or Delete an entity. It is also highly recommended if Create permission is granted. (This only applies when performing these actions via the Policy Manager; does not apply when using the CA API Gateway Management Interface.)</p>   |
| <b>U</b>     | Role has permission to update entities of this type.   |
| <b>D</b>     | Role has permission to delete entities of this type.   |
| <b>O</b>     | <p>Role has another permission not listed above. This will be displayed in a tooltip.</p> <p><b>Tip:</b> Only system roles can have other permissions. Currently, the "other" permission only applies to: "log-viewer" and "audit-viewer-policy".</p>  |

Note the following permission type information that may not be immediately obvious for some entities:

- **Assertions:** Read access allows users to see assertions in the palette and use the assertion in a policy; Update access allows the security zone to be changed.
- **Service Templates:** Read access allows users to view the service template in the Publish Internal Service Wizard and to publish an internal service using the service template.
- **Audit Records:** Read access allows users to view audit messages within the [audit viewer](#). **Note:** The user must also have Read access to the source entity for the given audit message, if applicable.
- **UDDI Service Controls/UDDI Proxied Service Infos:** Create access allows users to publish a service to or from a UDDI registry. Read access allows users to view the UDDI details of a service published to or from a UDDI registry. Update access allows users to update the UDDI details of a service published to or from a UDDI registry. Delete access allows users to remove a service's connection to or from a UDDI registry.
- **Service Metrics Bins:** Read access allows users to view the Dashboard. This is the only permission available. For more information, see "Dashboard - Cluster Status" on page 406 and "Dashboard - Service Metrics" on page 402.

## Hints and Tips for Role Permissions

- When creating your custom permissions, be aware that services, policies, and assertions are interdependent. If you grant access to one entity type, you should probably grant at least some level of access to the other entity types where dependencies exist; otherwise, unexpected results may occur.

### *Examples:*

- Keep in mind that creating a service also creates a policy.
- All policies are wrapped within an implicit "All assertions must evaluate to true" assertion (though this does not show in the Policy Manager). This means that a role that can create a service must also have permissions to create a policy and have (at the very least) Read access to the "All assertions..." composite assertion.
- When you publish a SOAP service, the default policy created has a Route via HTTP(S) assertion. So this means that a publish service role must have the ability to read this assertion.
- Roles giving access to any of the [internal services](#) must also have permissions to read all the assertions that are included in the policies associated with these services.

- A user must have Read permission for every assertion that they wish to use in a policy. This either means granting a blanket "all assertions" permission, or creating a role that specifically includes the necessary assertions.
- A role with permissions to Read service templates should also include permissions to Create services and policies, and Read all assertions in the template. This is necessary in order to publish an internal service (which is the primary purpose of service templates).
- A role with permissions to Read, Create, or Update [private keys](#) must also have Read/Update permission on the [keystore](#) as well.
- A role that includes [revocation checking policies](#) must be able to Read at least one [trusted certificate](#). This is because revocation checking policies are accessed from the [Manage Certificates](#) dialog.)
- Encapsulated assertions require specific role permissions. These are described under "Making Encapsulated Assertions Available in a Role" in Working with Encapsulated Assertions in the *Layer 7 Policy Authoring User Manual*.
- Debug trace policies require specific role permissions. These are described under "Security Permissions" in Working with the Debug Trace Policy in the *Layer 7 Policy Authoring User Manual*.
- When creating permissions for [sample messages](#), note that sample message are only accessible via the XPath assertions or the encrypt/decrypt XML assertions (for a complete list, see "Sample Messages" on page 386). This means that for a role with any permissions for sample message also requires permission to Read and/or Update a policy and have Read permission to the assertions listed under "Sample Messages" on page 386.
- A role that includes [firewall rules](#) must be able to Read at least one [listen port](#). This is because firewall rules are accessed from the [Manage Listen Ports](#) dialog.  
**Note:** Firewall rules only apply to appliance (including virtual appliance) Gateways.
- A role that includes service usage records (viewable in the [Dashboard](#), [Cluster Status] tab, under "Service Statistics") also requires permissions to these entities: Read Service Metrics Bins; Read Published Services; Read Cluster Node Info Records. **Note:** It is not possible to view service usage records for services that have been deleted, as these no longer appear in the Dashboard.
- A role that includes audit records (at least Read permission for any of the audit types) must also have Read permissions for cluster node information.

- When creating a role that includes access to a JMS Endpoint, the system will automatically grant access to the corresponding [JMS Connection](#). Together, these two entities make up a [JMS Destination](#) (there is no single entity type called "JMS Destination"). **Note:** This will result in multiple permission groups—one for the endpoint and one for every associated connection.
- When including the [Trusted ESM](#) or Trusted ESM User entity types, only the Read and Delete permissions are available. This is because it is not possible to Create or Update these entities in the Policy Manager.
- A role that includes Policy Aliases should also have permissions to the original service or policy.
- A role that includes full permissions (Create, Read, Update, Delete) on all objects with name starting with "custom" also needs the following permissions to work:
  - full permissions for cluster properties with "name starting with 'interfaceTags'"
  - Read permission to at least one [listen port](#)

**Note:** This is relevant only for users who need to be able to modify Interfaces, either through the Policy Manager or the Gateway Management Interface (refer to the *CA API Gateway Management Interface* document for more details).
- A role that includes permissions for [secure passwords](#) requires Update permission in order to create a secure password.

## Add Permissions to Role Wizard

The *Add Permissions to Role Wizard* guides you through the process of defining [permissions](#) for specific entities to be added to a [custom role](#).

This wizard appears when you add permissions to a role when it is [created](#) or [edited](#).

For more information on using wizards, see "[Wizards](#)" under "Interfaces" on page 13.

---

**Tip:** It is important to approach your permissions with a clear goal in mind. There are many possible object permutations using this wizard. This can result in fairly complex permission groups being created. See "Understanding Role Permissions" on page 137 for examples on how your permissions from this wizard are translated into permission groups that appear in the [Manage Roles](#) dialog and for useful hints and tips.

---

### Step 1: Permission Options

This step of the wizard lets you choose the options for the permissions.



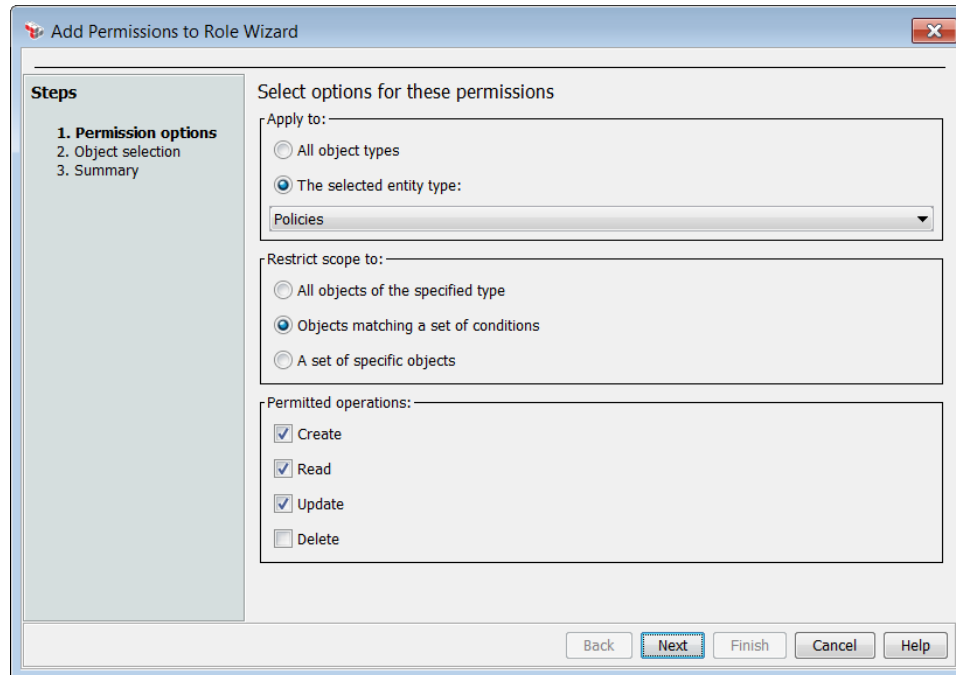


Figure 49: Add Permissions to Role Wizard - Step 1

Complete this step as follows:

1. Choose the entity types to which the permission applies:
  - **All entity types:** Permission will apply to all entity types in the system.
  - **The selected entity type:** Permission will apply only to the entity type that you select from the drop-down list (for example, "Assertions").

---

**Tip:** Be sure to read "Hints and Tips for Role Permissions" under "Understanding Role Permissions" on page 137 for information about various entity types that may not be immediately obvious.

---

2. Specify the scope of the entity type to include:
  - **All objects of the specified type:** All objects of the specified entity type will be included (for example, if "Assertions" was chosen, then all assertions in the system are included). With this option, Step 2 of the wizard is disabled and clicking **[Next]** proceeds to Step 3.

**Tip:** Choosing the "All objects..." scope will permit the selected operations on the entity regardless of the state of the entity (for example, regardless of the zone or folder that the object may be in).

- **Objects matching a set of conditions:** Create a set of conditions in Step 2 to choose the objects to include. Depending on the entity type selected, the available scope options will change.
  - **A set of specific objects:** Choose the individual objects yourself in Step 2.
3. Select at least one permitted operation:

**Create**  
**Read**  
**Update**  
**Delete**

For a description of each operation, see "Understanding Role Permissions" on page 137.

---

**Tip:** It is highly recommended to always include the "Read" permission in conjunction with the other permissions.

---

## Step 2: Object Selection

This step is used to select the objects to include in the permission. **Note:** This step is skipped if "All objects of the specified type" was chosen for the "Restrict scope to" option.

**Add Permissions to Role Wizard**

**Steps**

1. Permission options
- 2. Object selection**
3. Summary

Select options for these permissions

Permissions will only apply to objects that match the specified conditions.

Attributes Folders Zones

| Attribute | Comparison | Value |
|-----------|------------|-------|
| id        | sw         | 555   |

Remove

Criteria specification

Attribute: id

Comparison: starts with

Value: 555

Add

Back Next Finish Cancel Help

Figure 50: Add Permissions to Role Wizard - Step 2 (selection by condition example)

This step is used to specify the conditions for choosing the objects or to choose specific objects directly, depending on what was selected in Step 1.

## Specifying by Conditions

The conditions are arranged in a series of tabs. Configure each tab as necessary to construct a rule that precisely targets the objects you are seeking.

Table 48: Add Permissions to Role Wizard - Step 2 (specifying by conditions)

| Tab               | Descriptions   |
|-------------------|--|
| <b>Types</b>      | <p>If your chosen entity type can be further classified into specific types, this tab will be displayed to let you choose the type.</p> <p>The [Types] tab is most commonly used for audit records, where permissions can be set individually for each of the three audit record types (described in detail under Message Auditing in the <i>Layer 7 Policy Authoring User Manual</i>). <b>Note:</b> Only "Message" audit records can exist in security zones. This could have an impact on the functionality on the [Zones] tab.</p>  |
| <b>Attributes</b> | <p>This tab lets you specify the objects by name, ID, or other attributes specific to your chosen entity type to be included in the permission group (the attributes available depend on the entity type). At the top is a list of criteria that have been defined. You may remove any entry by selecting it and clicking <b>[Remove]</b>.</p> <p>The "Criteria specification" section at the bottom is where you construct your criteria list:</p> <ol style="list-style-type: none"> <li>1. Choose the <b>Attribute</b> that you wish to search by.</li> <li>2. Specify the <b>Comparison</b> operator: <b>starts with</b> means any attribute beginning with the specified value is matched; <b>equals</b> requires an exact match of the value.</li> <li>3. Enter the <b>Value</b> to match against.</li> <li>4. Click <b>[Add]</b> to add the criteria set to the table at the top.</li> </ol> <p><b>Note:</b> Selecting objects by attributes is designed for advanced users or for use under the direction of CA Technical Support. The following tips are not immediately obvious:</p> <ul style="list-style-type: none"> <li>• When selecting by assertion name, use the <i>full class name</i> for the assertion. For example, to grant Read access to all assertions in the Policy Manager using a name attribute, select "Assertions" for the entity type and then add the attribute: <code>name = com.l7tech.policy.assertion.composite.AllAssertion</code>. CA recommends specifying by <a href="#">manual selection</a> wherever possible to reduce the possibility of error. (For example, using the above example you would choose "Assertions" as the entity type and "A set of specific objects" as the scope. Then in Step 2, click "select all" to include all the assertions.)</li> <li>• The entity type "Policies" can be further refined by setting operations for each specific type of policies: Global Policy Fragment, Included Policy Fragment, and Internal Use Policy.</li> </ul> <p><b>Tips:</b> (1) Use the comparison operation "starts with" and then enter the value "Global", "Included", etc., to avoid having to type out the entire label. (2) The values are case sensitive, so "Global" works, but "global" does not. (3) To reference the standard service policy, use "Private Service Policy".</p> <ul style="list-style-type: none"> <li>• When selecting objects using the Attribute "type", each row in the permissions table corresponds to an "OR" logic, while each scope (comma separated)</li> </ul> |

Table 48: Add Permissions to Role Wizard - Step 2 (specifying by conditions)

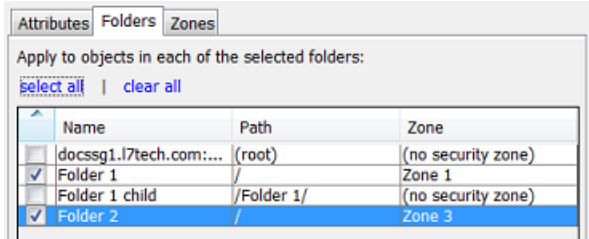
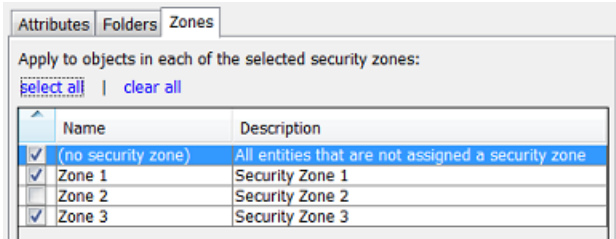
| Tab            | Descriptions   |
|----------------|--|
|                | <p>item corresponds to an "AND" logic. Be careful to not create a list of comma-separated items that are impossible to meet. For more information, see "Understanding Role Permissions" on page 137.</p>   |
| <b>Folders</b> | <p>This tab lets you narrow down the access to objects within specific folders. All the folders to which you currently have read access are displayed. Select the folder(s) that should be part of the permission group. Folders at the root are denoted by "/". The root folder itself is denoted by "(root)" as the path. You may select folders alone or in conjunction with security zones.</p>  <p>Only entities that can reside in folders are affected by this condition; these include: folders, services, service aliases, policies, and policy aliases. The [Folders] tab is visible only if you are dealing with all entities or an entity type that can exist in folders.</p> <p><b>Tips:</b> (1) Be aware that this tab is only used to target objects <i>within</i> the selected folder. It is not meant to apply the permitted operation <i>to the selected folder itself</i>. To do this, select the "Grant access to all necessary folder" check box. (2) If there are many items in a table, you can type a few characters in the "Filter on..." box to filter the by the condition.</p> <p>You can further refine folder access with these options:</p> <ul style="list-style-type: none"> <li>• <b>Apply to objects in all subfolders:</b> Select this check box to include all objects residing in subfolders of the designated folder. Clear this check box to include only the objects residing in the designated folder.</li> <li>• <b>Grant read access to all necessary folders:</b> Select this check box to automatically grant access read access to the selected folder and all ancestor folders of the designated folder, if the user does not have access already. If "Apply to objects in all subfolders" is also selected, read access to all subfolders below the designated folder is also granted. Clear this check box to not have the system grant this implicit access—you are then responsible for ensuring that users can access the folder tree.</li> </ul> <p><i>Example:</i> Consider this folder hierarchy: <i>root &gt; Folder A &gt; Folder B &gt; Folder C</i>. You create a permission group for "Folder C" and Sue is added to the resulting role. When the "Grant..." option is selected, Sue will be able to access the objects within Folder C regardless of her current access to the parent folders. But if the "Grant..." option is <i>not</i> selected, then you must ensure that Sue has access to the root folder as well as to Folders A, B, and C, otherwise she will not be able to access Folder C regardless of the permission group.</p> |

Table 48: Add Permissions to Role Wizard - Step 2 (specifying by conditions)

| Tab          | Descriptions   |
|--------------|--|
| <b>Zones</b> | <p>This tab lets you specify the <a href="#">security zone(s)</a> as a condition. Only objects belonging to the zone(s) selected here will be included in the permission.</p>  <p>Keep in mind the following:</p> <ul style="list-style-type: none"> <li>• The selection "&lt;no security zone&gt;" allows the permission group to access all entities that are <i>not</i> currently assigned to a security zone. If this selection is not chosen, then entities that do not have a security zone cannot be accessed by this permission group.</li> <li>• The [Zones] tab is unavailable for objects that cannot be placed in a zone.</li> </ul> |

### Specifying by Manual Selection

A list of the objects belonging to the specified entity type is shown. Select the check box next to each object to include in the permission. **Tip:** To quickly locate an object in the list, enter the first few characters of its name in the "Filter on name" box.

Keep in mind the following:

- Only the objects to which you have Read access are displayed. Because of this, it is recommended that only administrators (who have full permissions) create new permissions. This ensures that all objects are available for selection.
- When selecting objects of type "Cluster Property", all the predefined cluster properties (that is, the properties visible in the drop-down list) will always be visible, regardless of any permissions. However, custom cluster properties (that is, properties that are set by typing in their names) may or may not be visible, depending on the your permissions.
- When selecting objects of type "Trusted ESM User", first choose the Trusted ESM from the drop-down list. The users associated with that Trusted ESM are then displayed for your selection.

- When selecting objects of type "UDDI Proxied Service Infos", the wizard will by default also grant additional access to the UDDI services referenced by each selected UDDI proxied service info. This is necessary because UDDI entities cannot be viewed unless the user can also read the relevant service for any selected UDDI Proxied Service. **Note:** This only grants access to the service itself; it does not grant folder ancestry.

Clear this check box to not grant this additional access. This is not recommended and should be selected only under the guidance of CA Technical Support.

- The same as above applies for objects of type "UDDI Service Controls". The wizard will by default also grant access to the UDDI services referenced by each UDDI service control.

### Step 3: Summary

This step summarizes the selections from the first two steps.

| Type     | Scope                                    | C | R | U | D | O |
|----------|--|---|---|---|---|---|
| Folders  | ancestors of folder "Folder 1 (/Fold...  | X | ✓ | X | X | X |
| Folders  | ancestors of folder "Folder 2 (/Fold...  | X | ✓ | X | X | X |
| Folders  | Folder "Folder 1 (/Folder 1)"            | X | ✓ | X | X | X |
| Folders  | Folder "Folder 2 (/Folder 2)"            | X | ✓ | X | X | X |
| Folders  | in folder "Folder 1 (/Folder 1)" and ... | X | ✓ | X | X | X |
| Folders  | in folder "Folder 2 (/Folder 2)" and ... | X | ✓ | X | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |
| Policies | <complex scope>                          | ✓ | ✓ | ✓ | X | X |

Figure 51: Add Permissions to Role Wizard - Step 3

Review the summary carefully to ensure that this particular set of permissions is correct and then click **[Finish]** to close the wizard. If corrections are necessary, click **[Back]** to return to the appropriate step. To view full Scope details for a permission group, select it and then click **[Properties]**.

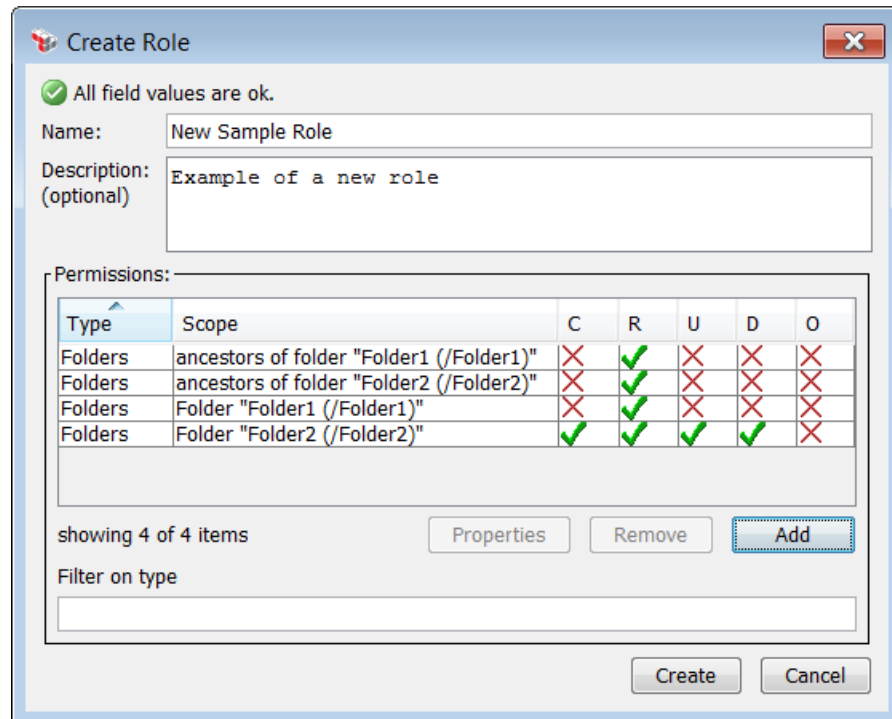
## Creating a Custom Role

The Policy Manager has a variety of predefined and automatically [roles and permissions](#) that can be assigned to users to control their access to the system. If none of these roles meet your needs, you can create your own custom roles to precisely control the permissions for various entities.

Only administrators can create custom roles.

➤ To create a custom role:

1. In the Policy Manager, select **[Tasks] > Manage Roles** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The [Manage Roles](#) dialog appears.
2. Click **[Create]**. The Create Role dialog appears.



The 'Create Role' dialog box is shown. It has a title bar with a close button. Inside, there's a status bar that says 'All field values are ok.' with a green checkmark. Below this are two text input fields: 'Name:' with the value 'New Sample Role' and 'Description: (optional)' with the value 'Example of a new role'. Below these is a 'Permissions:' section containing a table with 5 columns: 'Type', 'Scope', 'C', 'R', 'U', 'D', and 'O'. The table has 4 rows of data. Below the table, it says 'showing 4 of 4 items'. There are three buttons: 'Properties', 'Remove', and 'Add'. At the bottom right are 'Create' and 'Cancel' buttons. There is also a 'Filter on type' input field.

| Type    | Scope                                    | C | R | U | D | O |
|---------|--|---|---|---|---|---|
| Folders | ancestors of folder "Folder1 (/Folder1)" | ✗ | ✓ | ✗ | ✗ | ✗ |
| Folders | ancestors of folder "Folder2 (/Folder2)" | ✗ | ✓ | ✗ | ✗ | ✗ |
| Folders | Folder "Folder1 (/Folder1)"              | ✗ | ✓ | ✗ | ✗ | ✗ |
| Folders | Folder "Folder2 (/Folder2)"              | ✓ | ✓ | ✓ | ✓ | ✗ |

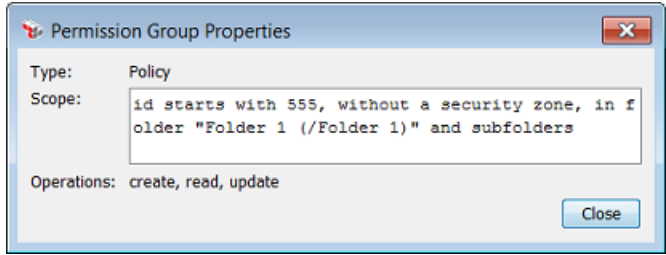
Figure 52: Create Role dialog

3. Complete the dialog as follows:

Table 49: Create Role settings

| Setting            | Description   |
|--------------------|---|
| <b>Name</b>        | Enter a name for the custom role.                                       |
| <b>Description</b> | Optionally enter a description to describe the role's intended use, the |

Table 49: Create Role settings

| Setting                  | Description  |
|--------------------------|--|
|                          | <p>permissions granted, etc.</p> <p><b>Tip:</b> At this point, you may click <b>[Create]</b> to save the role or proceed to define permissions for the role. If you exit now, you can add permissions later by <a href="#">editing</a> the role.</p>   |
| <b>Permissions table</b> | <p>This table describes the permissions that have been defined for the role. For details about the Permissions table, see "Understanding Role Permissions" on page 137.</p> <ul style="list-style-type: none"> <li>To add a new permission, click <b>[Add]</b> and then complete the "Add Permissions to Role Wizard" on page 142.</li> <li>To remove a permission, select it and then click <b>[Remove]</b>. The permission is removed immediately.</li> <li>To view the complete permission information, select a row and then click <b>[Properties]</b> to display the Permission Group Properties. This dialog is helpful when the Scope details are truncated in the table or when the scope is too complex to show in the table.</li> </ul>  <p><i>Figure 53: Permission Group Properties: example of "&lt;complex scope&gt;"</i></p> |
| <b>Filter on type</b>    | <p>When there are many entries in the Permissions table, you can type a few characters into this box and the table is filtered to display only the entity types that match your filter string.</p>   |

- Click **[Create]** to save the role and return to the Manage Roles dialog.

## Editing a Custom Role

Administrators can modify the permission set of any custom role. **Note:** Predefined and automatically generated [roles](#) in the Policy Manager cannot be edited.

➤ To edit a custom role:

- In the Policy Manager, select **[Tasks] > Manage Roles** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The [Manage Roles](#) dialog appears.
- Select the role to modify and then click **[Edit]**. The Edit Role dialog appears.



3. Modify the settings as necessary. For a description of each setting, see "Creating a Custom Role" on page 149.

---

**Tip:** When you add a new permission, a check mark appears in the "New" column and the entry is shown in yellow to indicate that the permission group is newly added during the editing session. This check mark and yellow background are cleared when you close the dialog.

---

5. Click **[Edit]** to save the changes and return to the Manage Roles dialog.

## Deleting a Custom Role

Administrators can delete any custom role. **Note:** Predefined and automatically generated [roles](#) in the Policy Manager cannot be deleted.

➤ *To delete a custom role:*

1. In the Policy Manager, select **[Tasks] > Manage Roles** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The [Manage Roles](#) dialog appears.
2. Select the role to delete and then click **[Remove]**. The Remove Role confirmation dialog displays to warn you whether there are any users or groups currently assigned to this role. **Tip:** Though it is possible to remove a role that still in use, it is best practice to first remove all users and groups from a role prior to deletion.

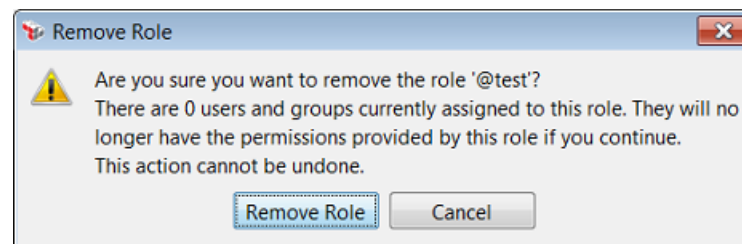


Figure 54: Remove Role confirmation dialog

3. Click **[Remove Role]** to proceed with the deletion.

---

**Tip:** To see exactly which users and groups are still assigned to the role, click **[Cancel]** to dismiss the dialog and then review the [\[Assignments\]](#) tab in the Manage Roles dialog.

---

## Adding a User or Group to a Role

You can add users or groups to the roles in the Policy Manager.

➤ *To add a user or group to a role:*

1. Start the [Manage Roles](#) task and then select the role to which you are adding the user or group.
2. In the [Assignments] tab, click [**Add**]. The [Search Identity Provider](#) dialog appears.

Optionally filter the search by using the **Name** drop-down list and field. You can use the asterisk (\*) wildcard to match any number of characters. Note that only [Internal Identity Provider](#) and [LDAP Identity Provider](#) users and groups can be added to a role.

---

**Tip:** If adding LDAP users, ensure that the **Allow assignment to administrative roles** check box has been selected in the [LDAP Identity Provider](#) properties.

---

3. Click [**Search**]. The list of users and groups is displayed.

If the user or group you want isn't found, you can add it by following the instructions under "Creating an Internal User" on page 286 or "Creating an Internal Group" on page 294.

4. Select the user or group to add, then click [**Select**]. The user or group is added to the role.
5. Click [**OK**] when done.

---

**Note:** All role changes are effective immediately on the Gateway, however changes may not be reflected on the Policy Manager interface until the Manager is restarted or the current user logs out and in again.

---

## Removing a User or Group from a Role

There are several ways to remove users or groups from a role.

➤ *Option 1: Remove using the Manage Roles dialog:*

1. Start the [Manage Roles](#) task and then select the role for which you are removing from the user or group.
2. In the [Assignments] tab, select the user or group to remove.

3. Click **[Remove]**. The user or group is removed from the role.
4. Click **[OK]** when done.

➤ *Option 2: Remove using the properties dialog:*

1. Open the properties dialog for the user or group. For more information, see:
  - "Internal User Properties" on page 288
  - "LDAP User Properties" on page 321
  - "Group Properties" on page 454
2. Select the [Roles] tab.
3. Select the role to remove for that user or group and then click **[Remove]**.

---

**Note:** All role changes are effective immediately on the Gateway, however changes may not be reflected on the interface until the Policy Manager is restarted or the current user logs out and in again.

---

## Managing Security Zones

The *Manage Security Zones* task is used to manage all facets of your [security zones](#). Use this task to:

- create, edit, or remove security zones
- see the types of entities permitted within a zone
- see a list of the actual entities assigned to a zone
- bulk assign eligible entities to a zone

---

**Tips:** (1) Changes to security zones may not fully take effect until the next session for a user. For example, if you add new entity types to the Test zone, users currently logged in with the "Manage Test Zone" role will not have these entity types available until they log off and back on. (2) The Policy Manager will not prevent simultaneous editing of zones. CA recommends that you develop a process for maintaining security zones, to avoid potential collisions caused by simultaneous editing of the same zone.

---

The Manage Security Zones dialog box (Figure 55) is divided into these main areas:

- The **Security Zones** area is where you add, modify, and delete security zones. If eligible, you can also bulk assign entities into and out of security zones.
- The **[Properties]** tab displays the complete description of the security zone and

lists the entities types that can be added to that zone.

- The **[Entities]** tab displays the entities that have been added to the zone.

Each area is described in greater detail below.

➤ To manage security zones:

- In the Policy Manager, select **[Tasks] > Manage Security Zones** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Security Zones dialog appears.

| Name   | Description                |
|--------|----------------------------|
| Zone 1 | allow folders only         |
| Zone 2 | allow assertions + folders |
| Zone 3 | allow all entity types     |

| Type                   | Permitted |
|------------------------|-----------|
| Assertion              | X         |
| Email Listener         | X         |
| Encapsulated Assertion | X         |
| Folder                 | ✓         |
| Global Resource        | X         |
| HTTP Options           | X         |

Figure 55: Manage Security Zones dialog

## Working with the Security Zones Area

The Security Zones area displays a table showing the security zones that have been defined, with action buttons for each task. Select a task to perform:

Table 50: Manage Security Zones tasks

| To...   | Do this...  |
|---|---|
| <b>Add a new security zone</b>                    | <ol style="list-style-type: none"> <li>1. Click <b>[Create]</b>. The Create Security Zone dialog appears.</li> <li>2. Complete the "Security Zone Properties" on page 159.</li> <li>3. Click <b>[Create]</b> to save the zone. The new zone appears in the list.</li> </ol>   |
| <b>Modify an existing security zone</b>           | <ol style="list-style-type: none"> <li>1. Select the security zone to edit from the list and then click <b>[Edit]</b>.</li> <li>2. Modify the "Security Zone Properties" on page 159 as required.</li> <li>3. Click <b>[Update]</b>. The zone is updated.</li> </ol>  |
| <b>Delete a security zone</b>                     | <ol style="list-style-type: none"> <li>1. Select the security zone to delete from the list.</li> <li>2. Click <b>[Remove]</b>. You are prompted to confirm.</li> <li>3. Confirm the deletion. All entities in that zone revert to a "no security zone" state and are now eligible to be added to another zone.</li> </ol>   |
| <b>Assign entities to or from a security zone</b> | <p>To quickly assign entities in bulk to a security zone, use the <b>[Manage Assignments]</b> button if it is available. This button is visible to any user who:</p> <ul style="list-style-type: none"> <li>• have the Administrator <a href="#">role</a>, or</li> <li>• have two or more "Manage X Zone" roles that both permit at least one shared entity type (a custom role may be created to permit a user to manage at least two security zones)</li> </ul> <p>For detailed information on the different ways you can assign entities to a security zone, including using the Assign Security Zones button, see "Assigning Security Zones" on page 160.</p> |

## About the [Properties] Tab

The [Properties] tab displays more information about the selected security zone. All information here is view only; any changes must be made through the [Security Zone properties](#) dialog, accessed through the [Edit] button.

- **Name:** Name of the security zone.
- **Description:** Full description of the security zone.
- **Entity types permitted in this zone:** Lists all the entity types in the system, with a check mark next to the permitted entities. **Tip:** If a security zone accepts all entities, you will see "Any entity type is permitted in this zone" instead of a list.

## About the [Entities] Tab

The [Entities] tab lists the actual entities that have been assigned to the zone.

- **Show entities of type:** This drop-down lists the permitted entity types from the [Properties] tab.
- **Name:** This list shows the entities of the selected type in the zone. For example, if "Assertions" was selected, then all the assertions that have been added to the security zone are listed, along with their paths (assertion palettes). To learn about the different ways to add entities to a zone, see "Assigning Security Zones" on page 160.
- **Filter on name:** If the list contains many entities, you can filter the list by typing a few characters. The list updates as you type to display only the entities with a matching character string in their names. This will help you quickly locate a specific entity.

## Understanding Security Zones

*Security zones* is a feature on the Gateway that allows the Administrator to partition portions of the Gateway to be managed by other administrators. A security zone is a collection of related entities (for example: services, policies, folders, trusted certificates).

Security zones extend the built-in [roles](#) to help you more precisely control who has access to what on the Gateway. Keep in mind that the Gateway uses the "permissive" model of security access. This basically means if a user has one role that does not provide access to a certain feature but has another that role does, then access is granted.

When a security zone is created, two new roles are automatically added:

*View X Zone*  
*Manage X Zone*

where "X" is the name of the security zone. You can use these roles in conjunction with the existing roles to control access.

*Examples:*

You define a zone named "Widget A" and then add some assertions and folders into that zone. The roles "View Widget A Zone" and "Manage Widget A Zone" become available.

- Bob has the "Operator" role, which allows him to view any entity, regardless of security zone. Bob will be able to view the items in the Widget A zone, even without the security zone roles.

- Sue has the custom role "View any Folder where Security Zone = Widget B". This allows Sue to view any folder which has been given the Security Zone of Widget B. This does not necessarily give Sue access to the *contents* of the folders however—only to the folders themselves.
- Fred has a role that allows him to view assertions that were placed in the "Widget A" zone. This means Fred will be able to work with those assertions, even without having the "View Widget A Zone" role.
- Sally is assigned the role "Manage Widget A Zone". She now has permission to create, view, update, and delete any of the entities added to the Widget A zone. It is not necessary to explicitly grant access to these entities using any other roles.

Security zones are especially useful in controlling access to specific assertions. By placing the appropriate assertions into specific zones, you can delegate management as follows:

- Network administrators can edit policy fragments to check things like source IP addresses.
- Security administrators can edit policy fragments dealing with TLS and message-level encryption.
- Application administrators can write XSL transformations and other policy logic.

---

**Tips:** (1) Read (view) access to a security zone will make the assertion visible in the assertion palette on the interface. However Create access (to the zone) is required to save a policy containing assertions in a security zone. (2) When security zones have been implemented, you must have a "Manage X Zone" role that includes the "All assertions must..." composite assertion as well as every assertion currently in the policy (or will be added to the policy) in order to create or edit that policy.

---

Most entities can be placed into a security zone. Notable exceptions include the following:

- Users
- Groups
- Keystore
- Cluster properties & cluster information
- Service usage
- Metrics bin
- Roles
- Audit records for Admin and System events
- Password policy
- Security zones

Note the following restrictions for security zones:

- An entity can only be in one zone at a time.
- A security zone cannot be placed within another security zone.

The following table summarizes the security zone tasks:

Table 51: Security zone tasks

| To...   | See...   |
|---|--|
| Add, edit, or remove a security zone              | "Managing Security Zones" on page 153                |
| Add or remove entities from a security zone       | "Assigning Security Zones" on page 160               |
| View a list of all entities within an entity type | "Managing Security Zones" on page 153 (Entities tab) |
| Learn about the security zone roles               | "Predefined Roles and Permissions" on page 132       |

## When Security Zone Details are Unavailable

Security zones are designed to restrict access to only similarly zoned entities for a user. However due to the Policy Manager's "cumulative" nature of security [roles](#), a user may still have access to entities outside of their security zone if that user has other roles that permit this. When this occurs, the Policy Manager will display "*Current zone (zone details are unavailable)*" when you attempt to view security zone information.

*Example:*

When you publish a service, you are assigned to the "Manage <service>" role. Among its permissions is the ability to read *all* identity providers in the system, regardless of security zone. Bob has a role that permits access to "Zone A" entities and there is an LDAP Identity Provider "Alpha" that is in "Zone B". Bob publishes a service and now has the "Manage <service>" role.

Prior to publishing the service, Bob is not able to see the "Alpha" entity because it is in a different zone. After publishing the service, Bob can now view the "Alpha" identity provider, however when he checks its security zone, this is displayed:

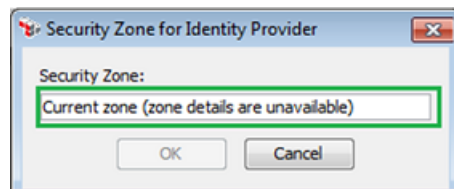


Figure 56: Security zone unavailable message



This indicates to Bob that the identity provider is in a different security zone, but that he can view it because of permissions granted by other roles.

---

**Tip:** The "Current zone (zone details are unavailable)" message will also be displayed in rare instances where you have access to the entities inside the zone, but for whatever reason you do not have Read access to zone attributes themselves (for example, name of the zone). Contact your administrator for more information. If this behavior is not intentional, [contact CA Technical Support](#) for assistance.

---

## Security Zone Properties

When creating or modifying a [security zone](#), the Security Zone Properties appear. This dialog is used to add or modify the name and description of the security zone, plus the entity types that are permitted within the zone.

➤ To access the properties for a security zone:

1. Run the [Manage Security Zones](#) task.
2. Create or edit a security zone. The Security Zone Properties appear.

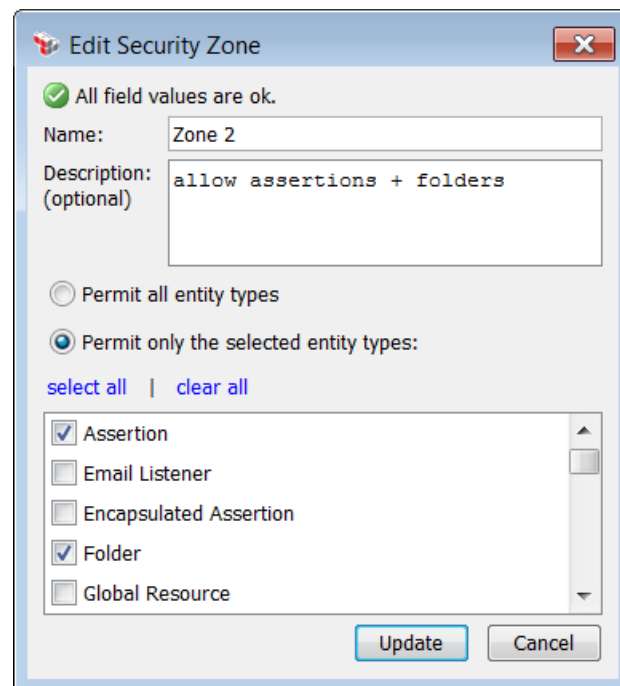


Figure 57: Security Zone Properties dialog

3. Configure the properties as follows:

Table 52: Security zone settings

| Setting            | Description  |
|--------------------|--|
| <b>Name</b>        | Enter the name of the security zone.   |
| <b>Description</b> | Optionally, enter a description of the security zone.<br>This description may display truncated on the Manage Security Zones dialog, but the complete description is visible in the [Properties] tab of that dialog box.   |
| <entity types>     | Choose which types of entities may be placed in the security zone: <ul style="list-style-type: none"> <li>• <b>Permit All Entity Types:</b> All available entity types are acceptable. In this instance, the entity list becomes display-only.</li> <li>• <b>Permit Only the Specified Entity Types:</b> Only the entity types selected in the list below are acceptable.</li> </ul> |
| <entity list>      | If only specific entity types are acceptable, select them here. At least one entity type must be selected.<br>This list is unavailable if all entity types are permitted.  |

- Click [**Create**] or [**Update**] when done.

## Assigning Security Zones

There are several ways to assign a [security zone](#) to an entity:

- **Assign individually:** Select an assignable entity and then either right-click or access its properties to set or change the security zone.
- **Assign in bulk:** Select [**Assign Security Zones**] from the [Manage Security Zones](#) dialog to quickly assign entities to a zone.

Each method is described in more detail below.

---

**Note:** In order to add or change security zones, your security [role](#) must allow update privileges to the entities being changed.

---



---

**Tip:** If a security zone accepts the entity "Published Services" it should also accept "Policy", otherwise you will only be able to edit the service properties but not view or edit the policy of the published service.

---

## Assigning Zones Individually

Two different methods are used to assign individual entities to zones.

### Method 1: Assertions, Internal Identity Provider, aliases, and root node

1. Right-click the item and then select **Security Zone**.

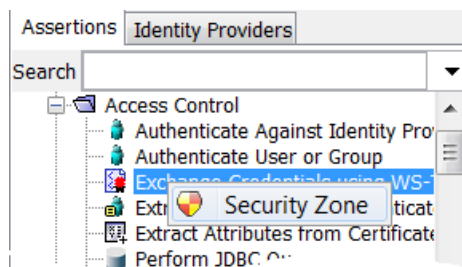


Figure 58: Set security zone via right-click

2. Choose the security zone from the drop-down list. If your permissions allow it, you can remove the item from a security zone by choosing **"No security zone"**.

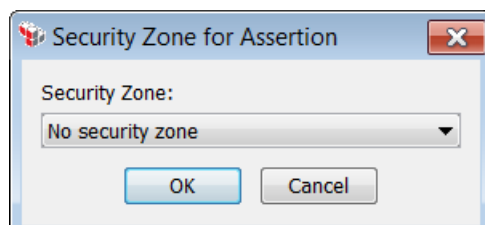


Figure 59: Selecting a security zone

---

**Tip:** To remove an entity from a security zone, your security role must allow update privileges to that entity. For example, if your only role is "Manage Test Zone" you can modify entities within the Test zone, but you cannot remove entities from the Test zone. If you also had an additional role such as "Manage Widget Service", then you will be able to select "No security zone" for the Widget service because then you have full update privileges on that particular entity, regardless of its zone.

---

3. Click **[OK]**. The item is added to the selected security zone (or removed from the zone).

### Method 2: Set via properties

This method is used for all other entities that do not display a "Security Zone" right-click option (or where right-clicking is not possible, for example: [log sinks](#) or [listen ports](#)).

Access the properties dialog for the entity. The security zone setting is visible at the bottom of the dialogs. If there are multiple tabs within the properties, this setting is usually on the first tab (for example "General" or "Base Settings" tabs).

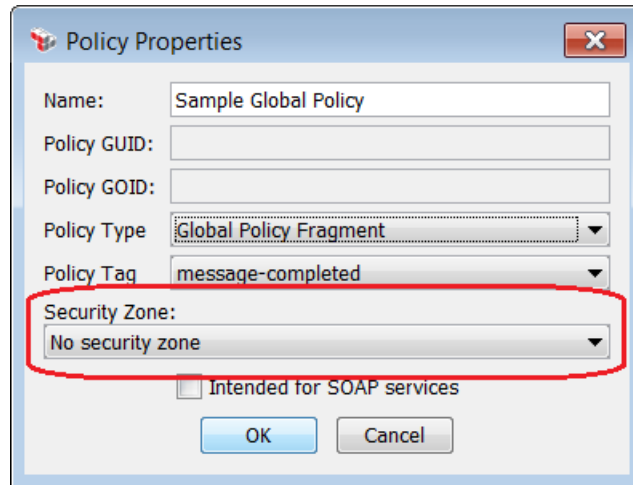


Figure 60: The Security Zone setting in a properties dialog

Choose the security zone from the drop-down list. The security zone is changed when you close the properties.

---

**Tip:** The Security Zone drop-down is visible only when at least one security zone is defined, otherwise it is hidden.

---

## Assigning Entities in Bulk

To quickly assign a large number of entities to a security zone, use the Assign Security Zones dialog.

---

**Note:** The bulk entry method is only available to Administrators or users who have two or more "Manage X Zone" roles that both permit at least one shared entity type (for example "Zone A" and "Zone B" roles that both include assertions). It is also available via custom roles.

---

➤ *To assign entities in bulk:*

1. Run the [Manage Security Zones](#) task. The Manage Security Zones dialog box appears.
2. Click **[Assign Security Zones]**. The Assign Security Zone dialog appears.

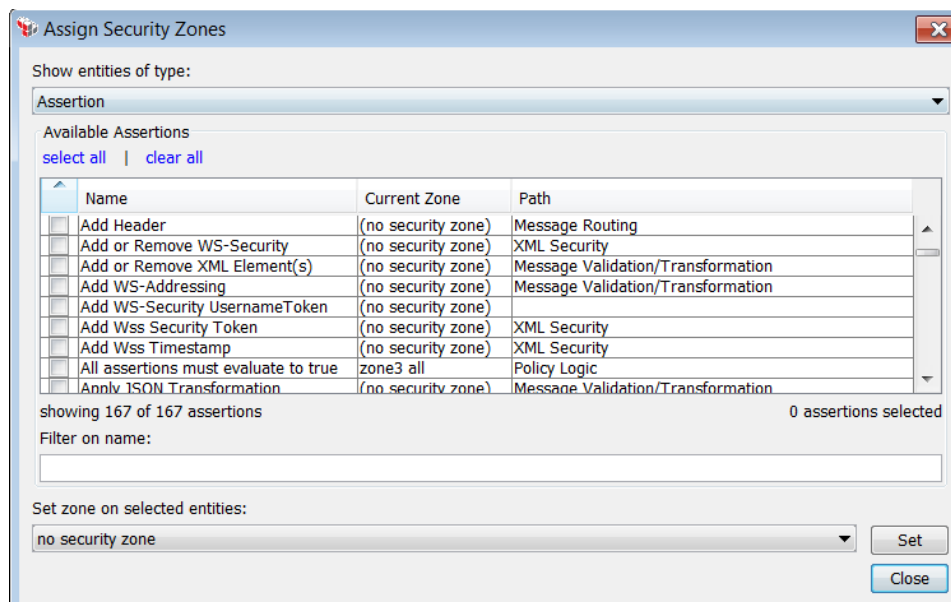


Figure 61: Assign Security Zones dialog

- From the drop-down list, choose the entity type you wish to added to a security zone (for example "Folder"). If the entity type you want is not listed, then it cannot be controlled via a security zone.
- The list updates to show all the entities of that type available to be added to a zone. The name of the entity, its current zone, and path (location of entity) are displayed.
- Select the check box next to the entities to be added to a zone. You can use the **"select all"** and **"clear all"** links to quickly select or clear all the check boxes.

**Tip:** If the list is long, enter a search string in the "Filter on name" field to help you find the appropriate entities to add. The list is updated as you type based on your search string. The string is matched anywhere within the entity name.

- Choose the security zone to be applied to your selected entries. If you choose **"No security zone"** then the selected entries will be removed from whatever security zone they happen to be in.
- Click **[Set]** to add the selected entities to the zone.
- Repeat steps 3 to 7 if you need to add different entities to security zones.
- Click **[Close]** when finished.

## Managing Log Sinks

The Gateway supports any number of administrator-defined sinks for logging. Use the *Manage Log Sinks* task to create, modify or remove a log sink.

You can also use this task to manage where audit records should be sent: either to the Gateway database and/or to a special audit sink policy that defines what happens to the audit event. For more information, see "Managing the Audit Sink" on page 175

*Prerequisite:* If logging to a Syslog log sink, ensure that a Syslog daemon that supports either UDP or plain TCP from remote systems has been configured.

---

**Note:** Creating additional log sinks does not affect the built-in [auditing](#) features of the Gateway. Audit information can still be logged to the Gateway database and/or to an audit sink, even if information is also written to one or more log sinks.

---

➤ *To manage log sinks:*

1. In the Policy Manager, select **[Tasks] > Manage Log/Audit Sinks** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Log Sinks dialog appears.

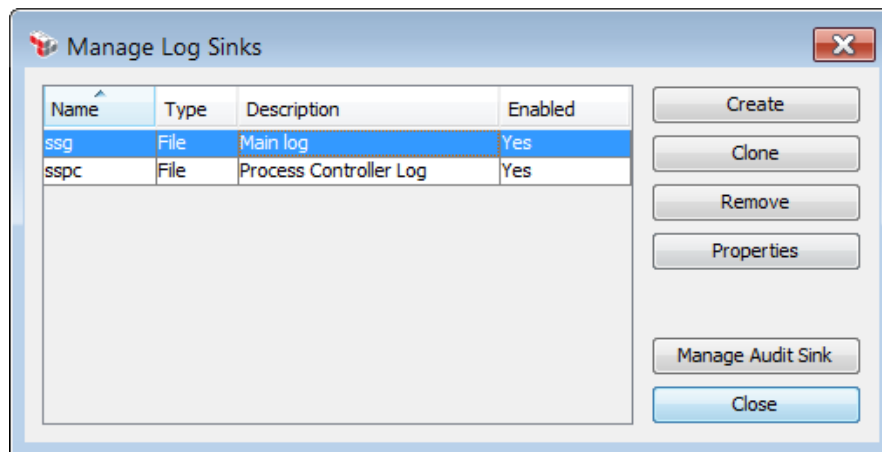


Figure 62: Manage Log Sinks dialog

2. Select a task to perform:

Table 53: Manage Log Sinks tasks

| To...                 | Do this...  |
|-----------------------|---|
| Create a new log sink | <ol style="list-style-type: none"> <li>1. Click <b>[Create]</b>.</li> <li>2. Complete the "Log Sink Properties" on page 167.</li> </ol> |

| To...  | Do this...  |
|--|---|
| <b>Clone an existing log sink</b>                | <ol style="list-style-type: none"> <li>1. Select the log to clone.</li> <li>2. Click <b>[Clone]</b>.</li> <li>3. Edit the "Log Sink Properties" on page 167 as required.</li> </ol> |
| <b>Remove a log sink</b>                         | <ol style="list-style-type: none"> <li>1. Select the log to remove.</li> <li>2. Click <b>[Remove]</b>.</li> </ol>   |
| <b>View or edit the properties of a log sink</b> | <ol style="list-style-type: none"> <li>1. Select the log to view.</li> <li>2. Click <b>[Properties]</b>. See "Log Sink Properties" on page 167 for details.</li> </ol>              |
| <b>Control how audit records are handled</b>     | <ul style="list-style-type: none"> <li>• Click <b>[Manage Audit Sink]</b>. See "Managing the Audit Sink" on page 175 for details.</li> </ul>  |

3. Click **[Close]** when done.

## Logged Information

How information is logged depends on whether the log sink outputs to a file or a Syslog server:

- If a file, log/audit information will be written in the 'Standard' format. For more information, see "Log Sink Properties" on page 167, **[File Settings]** tab, **Format** field.
- If Syslog, log/audit information will be mapped to the Syslog items as follows:
  - **Facility:** As configured
  - **Severity:** Mapped from the log/audit level (see Table 54 below)
  - **Timestamp:** As per the log/audit event
  - **Hostname:** The hostname of the Gateway
  - **Message**
    - **Tag:** Identifier for the process, which is the Gateway plus "default\_" and thread (for example: *Gateway1-default\_[17282]*)
    - **Content:** As per the log/audit event, truncated to size limit (line feeds are replaced with a single space if TCP)

These items are a standard part of the Syslog protocol as defined in *RFC 3164 - The BSD Syslog Protocol*. For more information, see <http://www.faqs.org/rfcs/rfc3164.html>.

Table 54: Log/audit severity levels

| Code | Severity                                  | Levels  |
|------|---|---|
| 0    | Emergency: system is unusable             |   |
| 1    | Alert: action must be taken immediately   |   |
| 2    | Critical: critical conditions             |   |
| 3    | Error: error conditions                   | SEVERE  |
| 4    | Warning: warning conditions               | WARNING   |
| 5    | Notice: normal but significant conditions |   |
| 6    | Informational: informational messages     | INFO  |
| 7    | Debug: debug-level messages               | CONFIG, FINE, FINER, FINEST<br><b>Note:</b> Debug message may not be saved in default configurations. |

## Creating a Log Sink

You can create a log sink using either the Manage Log/Audit Sinks task (normal method) or by right-clicking a service, folder, or policy (shortcut method).

➤ *To create a log sink (normal method):*

The "normal" method creates a new log sink with all settings empty.

1. In the Policy Manager, select **[Tasks] > Manage Log/Audit Sinks** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The [Manage Log Sinks](#) dialog appears.
2. Click **[Create]**.
3. Complete the properties for the log sink. For more information, see "Log Sink Properties" on page 167.

➤ *To create a log sink (shortcut method):*

The "shortcut" method lets you quickly create a new log sink without needing to invoke the Manage Log/Audit Sinks task. It creates a new log sink prepopulated with filter information based on the item that was right-clicked.



1. In the [services and policies list](#), right-click a service, folder, or policy.
2. Select **Create Log Sink** from the context menu. This creates a new log sink with the **Name**, **Description**, and **Filters** fields prepopulated with information based on the service, folder, or policy.
3. Complete the remaining [Log Sink Properties](#) as required.

## Log Sink Properties

When creating or viewing details about a [log sink](#), the Log Sink Properties appear. Information about the sink is organized across these tabs:

- Basic Settings
- File Settings
- Syslog Settings

For more information, see "Managing Log Sinks" on page 164.

➤ *To access the properties for a log sink:*

1. Run the [Manage Log Sinks/Audit Sinks](#) task.
2. Select a log sink and then click [**Properties**]. You can also click [**Create**] to enter the properties for a new log sink. The Log Sink Properties appear.
3. Configure each tab in the dialog as necessary. See below for a complete description of each tab.
4. Click [**OK**] when done.

## Configuring the [Base Settings] tab

The screenshot shows the 'Log Sink Properties' dialog box with the 'Base Settings' tab selected. The 'Name' field is 'ssg' and the 'Enabled' checkbox is checked. The 'Description' is 'Main log'. The 'Type' is set to 'File'. The 'Severity Threshold' is 'Info'. The 'Filters' list contains 'Category=Audits' and 'Category=Gateway Log'. The 'Security Zone' is 'no security zone'. There are 'Add' and 'Remove' buttons next to the filters, and 'OK' and 'Cancel' buttons at the bottom right.

Figure 63: Log Sink Properties - [Base Settings] tab

The [Base Settings] tab defines properties common to both File and Syslog sinks. Complete this tab as follows:

Table 55: Log Sink Properties - [Base Settings] tab

| Field                     | Description   |
|---------------------------|---|
| <b>Name</b>               | If creating a new log sink, enter a name for the log sink here. If editing a log sink, the existing name is displayed here and cannot be changed.<br><br><b>Note:</b> The log sink name is restricted to ASCII letters and numbers, underscores, and hyphens. Non-English single byte and multi-byte characters are not supported.                                    |
| <b>Enabled</b>            | Select this check box to enable the log sink.<br>Clear this check box to disable the log sink.  |
| <b>Description</b>        | Optionally enter or modify the description of the log sink.   |
| <b>Type</b>               | Choose the type of log sink from the drop-down list: <ul style="list-style-type: none"> <li><b>File:</b> The logged messages will be stored in a file, defined in the <a href="#">[File Settings] tab</a>.</li> <li><b>Syslog:</b> The logged messages will be forwarded to a central repository, as defined in the <a href="#">[Syslog Settings] tab</a>.</li> </ul> |
| <b>Severity Threshold</b> | Choose the severity threshold for information to be recorded by this sink. Only information at this level or higher will be processed. Choose   |

| Field                | Description   |
|----------------------|---|
|                      | <p><b>All</b> to include events from every severity threshold.</p> <p>To learn more about how the severity threshold in log sinks work, see <i>Understanding Logging Thresholds</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>  |
| <b>Filters</b>       | <p>Configure the filters for the log sink to control which messages are output to the sink. By combining several filters, you can indicate with precision which events will be logged.</p> <ul style="list-style-type: none"> <li>To define a new filter, click <b>[Add]</b> and then complete the filter details. See <a href="#">"Configuring Log Sink Filters"</a> below for details on each of the different filter types.</li> <li>To delete a filter from the list, select it and then click <b>[Remove]</b>.<br/> <b>Tip:</b> You may remove multiples filters at once by holding down the [Ctrl] key to select the filters.</li> </ul> <p><b>Note:</b> If an item in the filter list has been deleted or is inaccessible (that is, the user does not have permission to access the entity), "Not Found/Inaccessible" will be shown next to the entity name; for example:</p> <p style="text-align: center;"><i>Folder=Not Found/Inaccessible '-2:12345678'</i></p> <p>where "-2" is an internal code for the entity type and "12345678" is an internal identifier for the entity.</p> |
| <b>Security Zone</b> | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>   |

## Configuring Log Sink Filters

You can configure the following filter types for a log sink:

Table 56: Log Sink Properties - Filter types

| Filter Type     | Description   |
|-----------------|---|
| <b>Category</b> | <p>Select the category(ies) of Gateway log information to be output by the log sink. <b>Tip:</b> Hold down the [Ctrl] key to select more than one category.</p> <ul style="list-style-type: none"> <li><b>Audits:</b> This is information gathered from the Gateway auditing subsystem. For more information, see <i>Message Auditing</i> in the <i>Layer 7 Policy Authoring User Manual</i>.</li> <li><b>Gateway Log:</b> This is information gathered from the Gateway</li> </ul> |

| Filter Type      | Description   |
|------------------|---|
|                  | <p>logging subsystem.</p> <ul style="list-style-type: none"> <li>• <b>Traffic Log:</b> This is information for each request/response that is processed by the Gateway.</li> </ul> <p><b>IMPORTANT:</b> At least one Category filter must be created in order for the log sink to work correctly.</p>  |
| <b>Client IP</b> | Enter the IP address of the client to be output by the log sink.  |
| <b>Folder</b>    | <p>Select the folder(s) to be output by the log sink. All items within that folder (including any subfolders) will be included in the related log sink (as if you had manually selected all the services and policies).</p> <p>Any logging events that are not generated in relation to an item (service or policy) within the selected folder(s) will not be included in the related log sink.</p> <p><b>Tip:</b> Selecting the root folder will include log events from <i>all</i> your services and policy fragments, including the contents of all subfolders. For more information, see Organizing Services and Policies into Folders in the <i>Layer 7 Policy Authoring User Manual</i></p> |
| <b>Package</b>   | <p>Enter the name of the package to be output by the log sink. CA Technical Support will typically provide you with specific package names.</p> <p><b>Tip:</b> The package can be the name entered in the Add Audit Detail assertion.</p>   |
| <b>Policy</b>    | <p>Select the policies to be output by the log sink.</p> <p><b>Tip:</b> At least one policy (fragment, global, or internal) must exist before this filter can be used. For more information, see <i>Working with Service Policies</i> in the <i>Layer 7 Policy Authoring User Manual</i>.</p>   |
| <b>Service</b>   | <p>Select the services to be output by the log sink. Only log messages associated with that service will be included in the log sink.</p> <p>For more information, see "Services and Policies" on page 25.</p>  |
| <b>Transport</b> | <ol style="list-style-type: none"> <li>1. From the drop-down list, choose which transport <b>Type</b> should be output to the log sink: <a href="#">Email Listener</a>, <a href="#">JMS Connection</a> (Inbound only), or <a href="#">Listen Port</a>. The items that have been defined for the type are listed.</li> <li>2. In the <b>Name</b> box, select the items to include.<br/><b>Tip:</b> Hold down the [Ctrl] key to select more than one item.</li> </ol>   |
| <b>User</b>      | <ol style="list-style-type: none"> <li>1. Search for the users to be output by the log sink. For information on using the search interface, see "Searching Identity Providers" on page 459.</li> <li>2. In the <b>Search Results</b> box, select the users to include.<br/><b>Tip:</b> Hold down the [Ctrl] key to select more than one user.</li> </ol>  |

## Configuring the [File Settings] tab

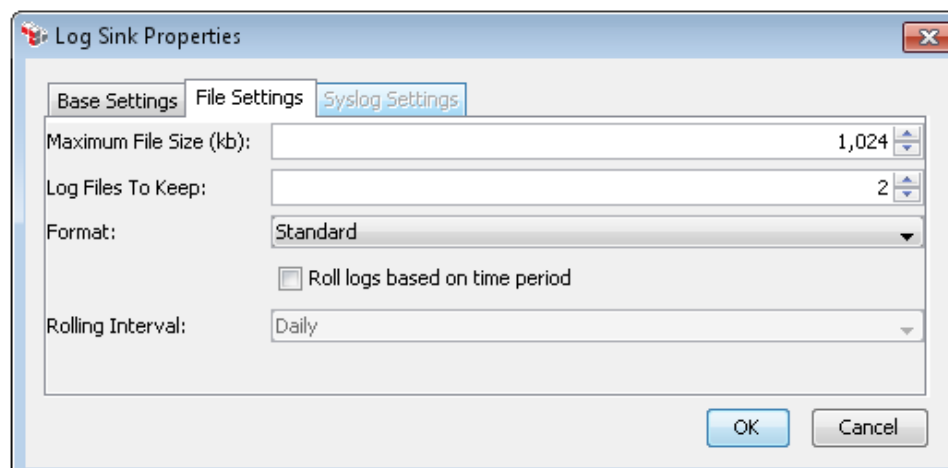


Figure 64: Log Sink Properties - [File Settings] tab

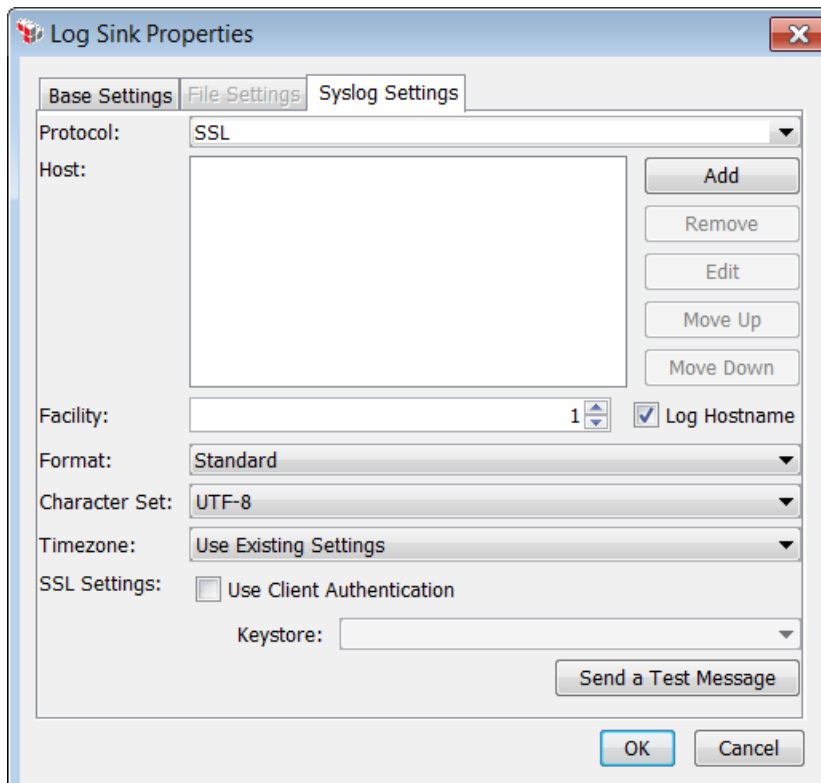
The following configuration options are available for logs of type "File":

Table 57: Log Sink Properties - [File Settings] tab

| Tab                      | Description  |
|--------------------------|--|
| <b>Maximum File Size</b> | Enter the maximum size per log file, in KB. Once the maximum is reached, the system rotates to the next log file. The minimum file size is 1KB, while the maximum is 1GB (1048576KB). The default is <b>1024</b> .   |
| <b>Log Files to Keep</b> | Enter the number of log files to keep, from 1 to 100. The default is <b>2</b> .<br><br><b>Notes:</b> (1) The combined maximum file for all logs is 5GB. ( <i>Maximum File Size</i> x <i>Log Files to Keep</i> ). (2) If you keep only one log file, it will be purged when its maximum size is reached.  |
| <b>Format</b>            | Choose the format to write log messages: <ul style="list-style-type: none"> <li>• <b>Raw:</b> Contains only the logged message; this is most suitable for traffic logging. Example of a Raw message:<br/><br/><code>Boot process complete.</code></li> <li>• <b>Standard:</b> The default format, recommended for general use. Example of a Standard message:<br/><br/><code>Dec 5, 2007 3:49:27 PM 10<br/>com.17tech.server.BootProcess<br/>INFO: Boot process complete.</code></li> <li>• <b>Verbose:</b> A verbose format, useful for debugging but not recommended for production environments due to potential performance impact. Example of a Verbose message:<br/><br/><code>Dec 5, 2007 3:49:27 PM 10<br/>com.17tech.server.BootProcess start</code></li> </ul> |

| Tab                                   | Description   |
|---------------------------------------|---|
|                                       | INFO: Boot process complete   |
| <b>Roll logs based on time period</b> | <p>Select this check box to roll the log files based on time interval. The file size settings are disabled when this is selected.</p> <p>Clear this check box to roll the log files based on file size.</p>   |
| <b>Rolling Interval</b>               | <p>When rolling logs are based on time interval, choose the frequency from the drop-down list.</p> <ul style="list-style-type: none"> <li>• <b>Hourly:</b> Select this to rotate the log file on an hourly basis. The rotation occurs at the top of each hour.</li> <li>• <b>Daily:</b> Select this to rotate the log file on a daily basis. The rotation occurs at midnight.</li> </ul> <p>The date format for each type of rotation is as follows:</p> <ul style="list-style-type: none"> <li>• <b>Daily:</b> yyyy-MM-dd</li> <li>• <b>Hourly:</b> yyyy-MM-dd-HH</li> </ul> <p>For example, a sink named "TEST" will have a file named "TEST.2012-10-23.log" for a daily rotation.</p> <p><b>Note:</b> Time-based rotation may create very large log files, especially if the sink is configured to log a large amount of information. It is best to keep the amount of data being logged to a minimum.</p> |

## Configuring the [Syslog Settings] tab



The screenshot shows the 'Log Sink Properties' dialog box with the 'Syslog Settings' tab selected. The 'Protocol' is set to 'SSL'. The 'Host' field is an empty list with buttons for 'Add', 'Remove', 'Edit', 'Move Up', and 'Move Down'. The 'Facility' is set to '1' and 'Log Hostname' is checked. The 'Format' is 'Standard', 'Character Set' is 'UTF-8', and 'Timezone' is 'Use Existing Settings'. Under 'SSL Settings', 'Use Client Authentication' is unchecked and the 'Keystore' is empty. A 'Send a Test Message' button is at the bottom right, along with 'OK' and 'Cancel' buttons.

Figure 65: Log Sink Properties - [Syslog Settings] tab

The following configuration options are available for logs of type "Syslog":

Table 58: Log Sink Properties - [Syslog Settings] tab

| Tab             | Description  |
|-----------------|--|
| <b>Protocol</b> | Select the protocol to use: <b>TCP (plain)</b> , <b>UDP</b> , or <b>SSL</b> . The default is <b>TCP</b> .  |
| <b>Host</b>     | <p>Define the hosts to receive the log file. You can enter multiple hosts to support Syslog failover. The Gateway uses a "round robin" failover strategy, beginning with the first host, then moving to subsequent hosts upon failure. If the Gateway is restarted, the first host on the list is used.</p> <ul style="list-style-type: none"> <li>To add a host, click <b>[Add]</b> and then enter the hostname or IP address for the Syslog server, followed by the port number: <code>&lt;host&gt;:&lt;port&gt;</code>.</li> <li>To remove a host from the list, select it and then click <b>[Remove]</b>.</li> <li>To modify host details, select it and then click <b>[Edit]</b>.</li> <li>To reposition the host in the list, select it and then click either <b>[Move Up]</b> or <b>[Move Down]</b>.</li> </ul> |
| <b>Facility</b> | Enter the facility number to log as, from 0 to 23. The default is 1. For assistance on the facility number, contact your Syslog administrator.   |

| Tab                        | Description  |
|----------------------------|--|
| <b>Format</b>              | <p>Choose the format to write log messages:</p> <ul style="list-style-type: none"> <li> <b>Raw:</b> Contains only the logged message; this is most suitable for traffic logging. Examples of Raw messages: <pre>Sep 14 10:44:05 localhost SSG[101]: Authenticated on Internal Identity Provider</pre> <pre>Sep 14 10:44:05 localhost SSG[101]: User 'admin' logged in from IP '127.0.0.1'.</pre> </li> <li> <b>Standard:</b> The default format, recommended for general use. Example of a Standard message: <pre>Sep 14 10:44:56 localhost SSG[117]: INFO com.l7tech.server.admin.AdminSessionManager: Authenticated on Internal Identity Provider</pre> <pre>Sep 14 10:44:56 localhost SSG[117]: INFO com.l7tech.server.admin.AdminLoginImpl: User 'admin' logged in from IP '127.0.0.1'.</pre> </li> <li> <b>Verbose:</b> A verbose format, useful for debugging but not recommended for production environments due to potential performance impact. Example of a Verbose message: <pre>Sep 14 10:45:56 localhost SSG[129]: [SyslogLogSink] INFO com.l7tech.server.admin.AdminSessionManager authenticate: Authenticated on Internal Identity Provider</pre> <pre>Sep 14 10:45:56 localhost SSG[129]: [SyslogLogSink] INFO com.l7tech.server.admin.AdminLoginImpl login: User 'admin' logged in from IP '127.0.0.1'.</pre> </li> </ul> |
| <b>Log Hostname</b>        | <p>Select this check box to include the Gateway hostname in the logged information. This setting is turned on by default, but you may need to clear the check box to avoid duplication with certain Syslog servers.</p>  |
| <b>Character Set</b>       | <p>Select the character set to log in from the drop-down list: <b>UTF-8, LATIN-1, ASCII</b>. The default is <b>UTF-8</b>.</p>  |
| <b>Timezone</b>            | <p>Select the time zone for logging. The default is to use the existing system settings.</p>   |
| <b>SSL Settings</b>        | <p>This section is available only if the selected Protocol is "SSL".</p> <ul style="list-style-type: none"> <li> <b>Use Client Authentication:</b> When connecting using SSL, select this check box to present a certificate to the server during the SSL handshake, if one is requested. Clear this check box to never present a certificate, even if one is requested. Note that access may be denied in this case. </li> <li> <b>Keystore:</b> From the drop-down list, select the keystore from which to retrieve the certificate. Used only if client certificates are used. </li> </ul>  |
| <b>Send a Test Message</b> | <p>Click this button to send a test message to the Syslog sink. Use this to verify the settings.</p>   |



## Managing the Audit Sink

The Policy Manager can be configured to send audit messages to one or both of the following locations:

- **Gateway database.** You can view and manage the audit events using the "Gateway Audit Events" on page 415
- **An audit sink policy.** Every audit event is run through a special audit sink policy that performs a specific action on the event, for example:
  - Branch based on the information being audited.
  - Post information via HTTP, JMS, FTP, email, SNMP, or JDBC.
  - Transform messages before auditing them to remove passwords, etc.

An audit sink policy lets you send messages to an external database, message queue, or other location. For more information on this policy, see "Working with the Audit Sink Policy" on page 178.

---

**Tip:** When using an audit sink, consider changing the auditing threshold in the cluster property [audit.messageThreshold](#) from WARNING to INFO. This will generate more events, but it will ensure that the audit sink policy is invoked for all "bad request" issues that might otherwise be omitted.

---

➤ *To manage the audit sink:*

1. In the Policy Manager, select [Tasks] > **Manage Log/Audit Sinks** from the [Main Menu](#). The Manage Log Sinks dialog is displayed (see "Managing Log Sinks" on page 164).
2. On the Manage Log Sinks dialog, click [**Manage Audit Sink**]. The Audit Sink Properties appear.

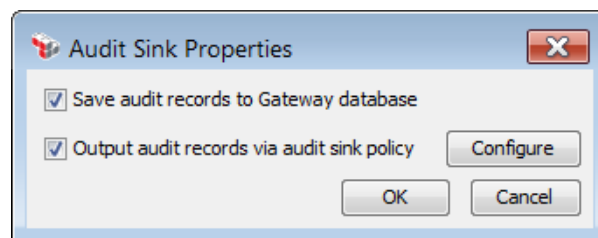


Figure 66: Audit Sink Properties

3. By default, the **Save audit records to Gateway database** check box is selected. This will send the audit events to the Gateway database, where you can examine them using the "Gateway Audit Events" on page 415 If you wish to disable the

internal auditing, clear this check box.

4. Select the **Output audit records via audit sink policy** check box to send records to the audit sink. An audit sink policy must already be configured. To configure or reconfigure an audit sink policy, click **[Configure]** and then complete the "Configure External Audit Store Wizard" on page 177.

Clear this check box if you do not want the audit events processed by the audit sink policy. Clearing the check box does not remove the audit sink policy.

5. Click **[OK]** when done. You return to the Manage Log Sinks dialog.

Do the following next:

- If you enabled a custom audit sink policy, you should edit the audit sink lookup policy now. This policy appears as "[Internal Audit Sink Policy]" in the [Services and Policies](#) list on the interface (see Figure 68). For more information, see "Working with the Audit Sink Policy" on page 178.

---

**Note:** The template audit sink policy created by the "custom" option is for illustrative purposes only and is designed to always fail, which causes auditing to fall back to the Gateway database.

---

- If you created an external JDBC audit sink, the lookup policy also appears as "[Internal Audit Sink Policy]" in the Services and Policies list. Modify the policy as required by inserting assertions at the end, but do not modify the system-generated portion of the policy.

## Configure External Audit Store Wizard

The *Configure External Audit Store Wizard* is used to configure an external audit store to output audit records via the audit sink policy. It can be used to create an external JDBC audit sink (and its associated) lookup policy or it can create a custom audit sink and lookup policy. When creating a custom audit sink, you are free to configure the lookup policy as necessary. By comparison, you must not modify the system-generated policy for JDBC audit stores.

The Configure External Audit Store Wizard starts when you click **[Configure]** on the Audit Sink Properties dialog. For more information, see "Managing the Audit Sink" on page 175.

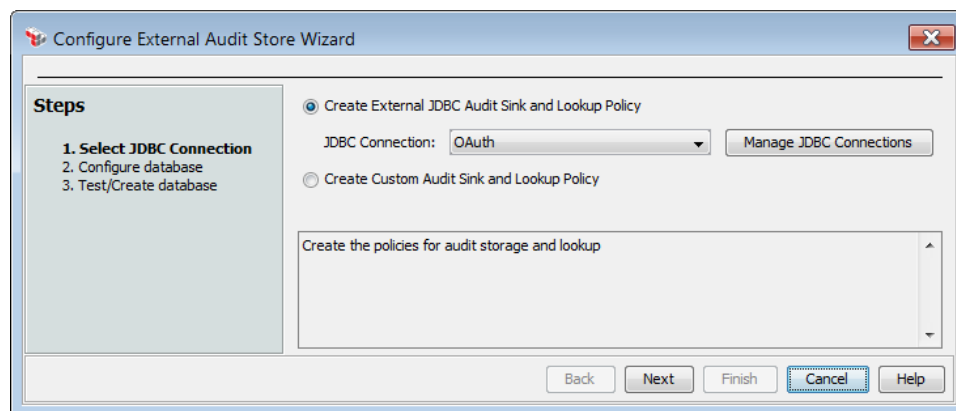


Figure 67: Configure External Audit Store Wizard

For more information about wizards, see "[Wizard](#)" under [Interfaces](#) in the *Layer 7 Policy Manager User Manual*.

Table 59: Using the Configure External Audit Store Wizard

| Wizard Step                           | Description  |
|---------------------------------------|--|
| <b>Step 1: Select JDBC Connection</b> | <p>Choose the type of external audit store to create:</p> <ul style="list-style-type: none"> <li>Select <b>Create External JDBC Audit Sink and Lookup Policy</b> to create an audit store based on a JDBC connection. <ul style="list-style-type: none"> <li>Select the connection to use from the drop-down list. If the connection you need is not displayed, click <b>[Manage JDBC Connections]</b> to create it. For more information, see "Managing JDBC Connections" on page 82.</li> </ul> </li> <li>Select <b>Custom Audit Sink and Lookup Policy</b> to create an audit sink and lookup policy that you can customize later.</li> </ul> <p>If choosing this type of policy, the wizard is now complete. Click <b>[Finish]</b> to create or overwrite any existing audit sink and lookup</p> |

| Wizard Step   | Description  |
|---|--|
|   | policies.  |
| <b>Step 2: Configure database</b><br><i>(JDBC audit store only)</i>   | Enter names for the following tables: <ul style="list-style-type: none"> <li>Audit Record Table (Default: <b>audit_main</b>)</li> <li>Audit Detail Table (Default: <b>audit_detail</b>)</li> </ul> <p>These tables are used in the database that will be created for the external audit store in Step 3 of the wizard.</p>   |
| <b>Step 3: Test/Create database</b><br><i>(JDBC audit store only)</i> | <p>In this step, the database schema is displayed. You may examine the schema as shown in the scrolling list or you may copy the schema to the Clipboard and paste it into another application. At this point you can:</p> <ul style="list-style-type: none"> <li>Click <b>[Create Tables]</b> to create the database tables required for logging into the database, using the displayed schema and table names from Step 2. Enter the <b>Username</b> and <b>Password</b> when prompted. <b>Note:</b> This assumes that you have permission to create databases.</li> <li>Click <b>[Check Tables Exist]</b> to verify that the database tables have been set up correctly.</li> <li>Click <b>[Finish]</b> to close the wizard. This will create or overwrite the audit sink and lookup properties.</li> </ul> |

## Working with the Audit Sink Policy

A special audit sink policy can be configured to direct audit messages to an external database, or message queue, or other location. This policy is created when the [audit sink is first enabled](#) and can be reconfigured later if necessary.

The audit sink policy is found in the [Services and Policies](#) list on the Policy Manager interface:

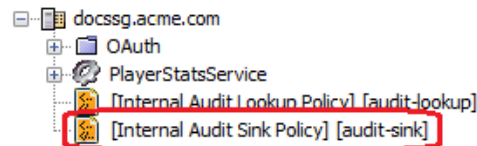


Figure 68: Audit Sink Policy on the interface

The following characteristics are unique to the audit sink policy:

- Only one audit sink policy is created per Gateway cluster.
- Disabling the audit sink does not remove the audit sink policy—it simply redirects audit messages to the Gateway database.

---

**Note:** It is possible to configure the audit messages to be sent simultaneously to the database and audit sink. See "Managing the Audit Sink" on page 175 for more details.

---

- An audit sink policy can be deleted only when first disabled in the [Audit Sink Properties](#).
- An audit sink policy is the only place where the Convert Audit Record to XML assertion can be used.
- Unlike normal policies, which require a valid XML request message (which may have a blank message body, but HTTP headers are present), the audit sink policy can work with a "blank" request—that is, a request that is initially completely uninitialized. You can use the Convert Audit Record to XML assertion to populate the sink policy's request with some XML.
- An audit sink policy can access a large number of auditing-specific context variables that are not available elsewhere in the system. See "Audit Sink Variables" on page 528 for details.
- The properties for an audit sink policy cannot be modified.
- Similar to the [audit lookup policy](#), there is no request XML coming into the policy.

Aside from the above exceptions, the audit sink policy is configured and edited in similar fashion to an ordinary policy. Multiple policy revisions may be created and you may export or import the audit sink policy.

## Troubleshooting an Audit Sink Policy

Detecting and correcting problems in an audit sink policy require slightly different techniques from troubleshooting normal policies, since auditing is disabled while an audit sink policy is being evaluated. The following tips may help:

1. Develop the audit sink policy functionality (excluding the Convert Audit Record to XML assertion, if applicable) within a policy fragment.
2. Publish an XML service to act as a test harness. This should invoke the audit sink policy with the relevant `${audit.*}` [context variables](#) prepopulated and the request already set to an example audit record. The actual audit sink policy would consist of just:

*Convert Audit Record to XML Assertion*

*Include Policy Fragment Assertion: Actual audit sink policy*

3. Audits will just be logged (for example, the Add Audit Detail assertion will just output as log).

For assistance in troubleshooting an audit sink policy, [contact](#) CA Technical Support.

## Deleting the Audit Sink Policy

When the audit sink policy is no longer required, you can delete it by right-clicking it in the [Services and Policies list](#) and selecting **Delete Policy**.

---

**Tip:** If you delete the audit sink policy, it will be recreated the next time the audit sink is [enabled](#).

---

## Understanding the Audit Sink Default Policy

When the audit sink is enabled, it can be [configured](#) as a custom audit sink or an external JDBC audit sink. Each produces a default policy that you can use as a starting point in your customization.

### Custom Audit Sink

The following policy is created when a custom audit sink is selected:

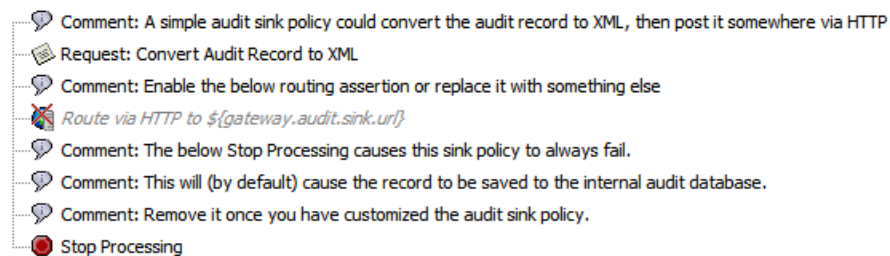


Figure 69: Audit sink default policy - custom

This default policy is for illustrative purposes only and must be configured. If used in its unmodified form, it is designed to always fail, reverting auditing back to the Gateway database.

Excluding the comments, the default policy contains these three assertions:

- **Convert Audit Record to XML:** This assertion takes the incoming audit records and converts them into an XML request, to mimic a standard incoming request in a service policy. To learn more about this assertion, see [Convert Audit Record to XML Assertion](#) in the *Layer 7 Policy Authoring User Manual*.

---

**Tip:** This assertion is technically not necessary in an audit sink policy. If you only need to retrieve a few specific values from the audit event, use a context variable from [Table 144](#) and [Table 145](#) under "[Context Variables](#)" instead.

---

- **Route via HTTP:** This assertion routes the request (i.e, audit record) to a specific endpoint. Edit this assertion as necessary or replace it with another routing assertion. Alternatively, replace this routing assertion with other policy logic. This assertion is disabled by default. To learn more about this assertion, see *Route via HTTP(S) Assertion* in the *Layer 7 Policy Authoring User Manual*.
- **Stop Processing:** This assertion causes the sample policy to fail and revert to auditing to the internal database. Be sure to delete this assertion once you have finished customizing the audit sink policy. To learn more about this assertion, see *Stop Processing Assertion* in the *Layer 7 Policy Authoring User Manual*.

### JDBC Audit Sink

The following policy is created when a JDBC audit sink is selected:

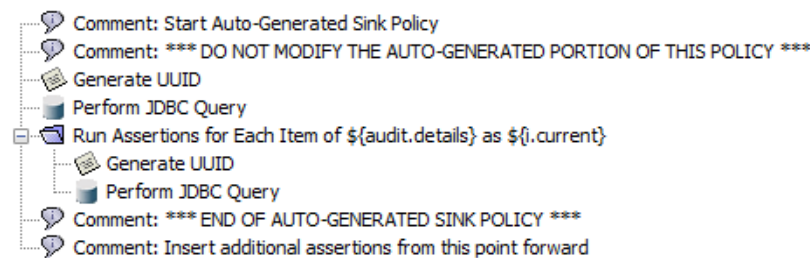


Figure 70: Audit sink default policy - JDBC

The JDBC audit sink policy has an auto-generated portion that must not be modified. The assertions in the auto-generated portion query the JDBC database. Add your customizations after the final comment shown above.

### Failure of the Audit Sink Policy

When the audit sink policy fails, the audit system will (by default) fall back to auditing to the internal database. This can be disabled by setting the cluster property `audit.sink.fallbackToInternal` to **"false"**. If fallback is disabled and the audit sink policy cannot be completed, an error is logged and the audit record is discarded.

---

**Tip:** As in a standard policy, an audit sink policy can have multiple branches to take some failover action in a backup branch should the primary branch fail. This way, you can avoid failing the entire audit sink policy because (for example) one particular sink endpoint is down.

---

### Context Variables in an Audit Sink Policy

For a list of the context variables specific to an audit sink policy, see ["Audit Sink Variables"](#) in "Appendix C: Context Variables" on page 517

---

**Tip:** For additional auditing-related context variables, see "[Audit Variables](#)" in "Appendix C: Context Variables" on page 517.

---

## Working with the Audit Lookup Policy

A special audit lookup policy can be configured to look up audit records in an external audit store. This policy is created automatically when the [audit sink is first enabled](#) and is overwritten when the external audit store is changed .

The audit lookup policy can be found in the [Services and Policies](#) list on the Policy Manager interface:

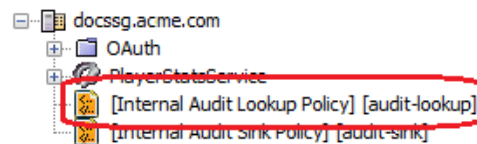


Figure 71: Audit Lookup Policy on the interface

The following characteristics are unique to the audit sink policy:

- Only one audit lookup policy is created per Gateway cluster.
- Disabling the audit sink does not remove the audit lookup policy.
- An audit lookup policy can be deleted only when the audit sink is disabled in the [Audit Sink Properties](#).
- After the audit lookup policy is deleted, re-enabling the audit sink does not recreate the policy—you must run the [Configure External Audit Store Wizard](#) again.
- An audit lookup policy can access a large number of auditing-specific context variables that are not available elsewhere in the system. See "[Context Variables for the Audit Lookup Policy](#)" below for details.
- The properties for an audit lookup policy cannot be modified.
- Similar to the [audit sink policy](#), there is no request XML coming into the policy.

Aside from the above exceptions, the audit lookup policy is configured and edited in similar fashion to an ordinary policy. Multiple policy revisions may be created and you may export or import the audit lookup policy.



## Deleting the Audit Lookup Policy

When the audit lookup policy is no longer required (that is, the audit sink has been disabled), you can delete it by right-clicking it in the [Services and Policies list](#) and selecting **Delete Policy**.

## Understanding the Default Audit Lookup Policies

Different default audit lookup policies are displayed in the Policy Manager depending on the type of audit store that was configured in the [Configure External Audit Store Wizard](#).

### Custom Audit Sink

If "Create Custom Audit Sink and Lookup Policy" was selected in the wizard, the default audit lookup policy consists of a single Add Audit Details assertion. You will then customize this policy as necessary to meet your needs.

---

**Tip:** To view the retrieved audits in the Gateway Audit Events window, ensure that your customized audit lookup policy populates the context variables listed under "[Context Variables for the Audit Lookup Policy](#)" below.

---

The following is one example of an audit lookup policy:

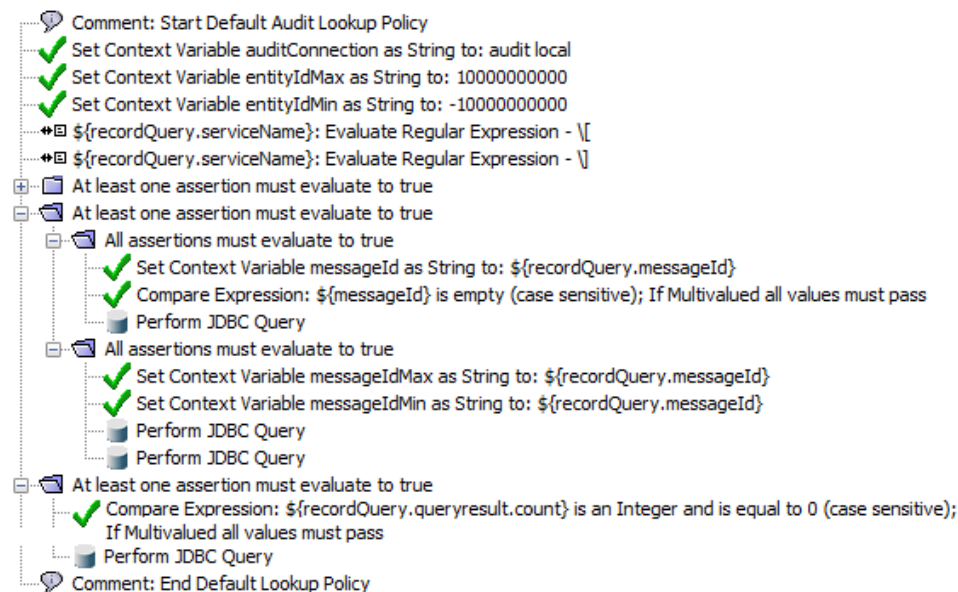


Figure 72: Sample custom audit lookup policy

## External JDBC Audit Sink

**Tip:** To view the retrieved audits in the Gateway Audit Events window, ensure that your JDBC audit lookup policy contains logic to populate the context variables listed under "[Context Variables for the Audit Lookup Policy](#)" below.

If "Create External JDBC Audit Sink and Lookup Policy" was selected in the wizard, the following default lookup policy is created:

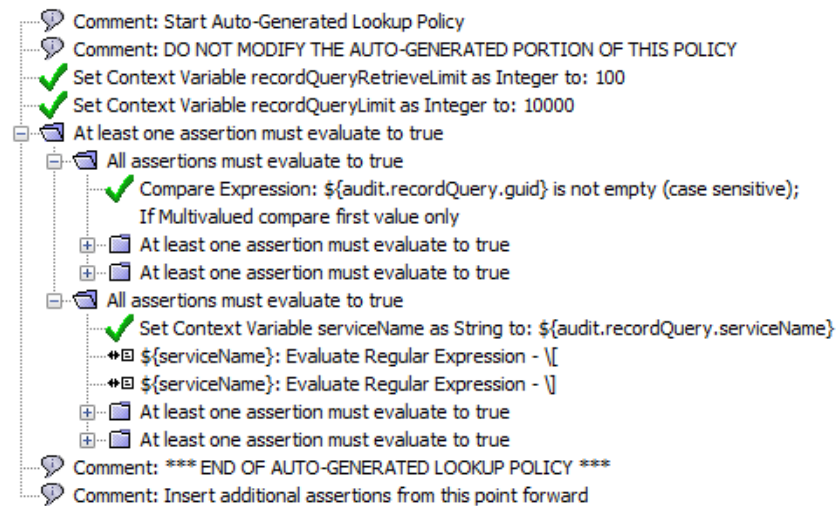


Figure 73: Default JDBC audit sink lookup policy

For JDBC audit sinks, the Policy Manager auto-generates the beginning of the lookup policy and you will customize it by adding assertions at the end.

**Note:** It is important that you do not modify the assertions contained in the auto-generated portion, otherwise the policy may not work properly. You may insert additional assertions at the end.

## Context Variables for the Audit Lookup Policy

For a list of the context variables specific to an audit lookup policy, "[Audit Lookup Variables](#)" in "Appendix C: Context Variables" on page 517

**Tip:** For additional auditing-related context variables, see "[Audit Variables](#)" in "Appendix C: Context Variables" on page 517.

## Working with Log Sinks and Debug Logs

The following procedures describe common scenarios involving log sinks and debug logs.

### Creating Log Sink for Custom Logger

➤ *To create a log sink for all messages from a custom logger:*

1. Use the [Manage Log Sink](#) task to create a new log sink for the [package com.l7tech.log.custom.<customLoggerName>](#).
2. Configure an Add Audit Detail assertion with the "<customLoggerName>" in the **Custom logger name** field.

During policy execution, audit details are sent only to the sink for the specified custom logger.

### Creating Log Sink for Service(s)

➤ *To create a log sink for all messages from a service:*

- Use the [Manage Log Sink](#) task to create a new log sink that filters by one or more [services](#).

During policy execution, only messages related to the selected services are sent to the log sink.

### Debugging a Client IP

➤ *To create a log sink for all messages from a client IP:*

1. Use the [Manage Log Sink](#) task to create a new log sink that filters by a specific [client IP address](#).
2. In the [Log Sink Properties](#), set the [severity threshold](#) to **FINE**.
3. Set the severity level for the appropriate package to **FINE** in the [log.levels](#) cluster property for the appropriate loggers—for example, "<packageName>.level=FINE". Please contact CA Technical Support for assistance with the package names.

During policy execution, only messages related to the specified client IP address are sent to the log sink.

## Debugging SSL/TLS

➤ To enable SSL/TLS debug for an HTTPS listen port:

1. Set the `io.debugSsl` cluster property to "true" to enable SSL/TLS debugging globally.
2. Set the `log.stdoutLevel` cluster property to **FINE**.
3. Update the `log.levels` cluster property to include the line **STDOUT.level=FINE**.
4. Use the [Manage Log Sink](#) task to create a new log sink that filters for the [category Gateway Log](#) and the [package STDOUT](#).
5. Use the [Manage Listen Ports](#) task to create a new HTTPS listen port.

During policy execution, the SSL/TLS output related to the consumption will be sent only to the configured log sink. (This assumes that no other log sinks are currently configured to allow "FINE" messages.)

---

**Note:** If debug trace logging has been enabled for HTTP(S), be aware that this can log passwords, including passwords used to log in to the Policy Manager. Use this capability with caution. For assistance on enabling debug trace logging in HTTP(S), please contact CA Technical Support.

---

## Managing ESM User Mappings

The *Manage ESM User Mappings* task shows whether your Gateway cluster is being remotely managed by the Enterprise Service Manager (ESM). Use this task to:

- View identification information about the Enterprise Service Manager and break the link if necessary.
- See which Gateway user has been mapped to an Enterprise Service Manager user and remove the mapping if necessary.

---

**Tip:** The *Managing ESM User Mappings* assertion is available only when your Gateway is currently being remotely managed by the Enterprise Service Manager.

---

You cannot *initiate* a link between your Gateway cluster and an Enterprise Service Manager using the *Manage ESM User Mappings* task. This involves enabling Remote Node Management from within the Gateway and then adding the cluster in the ESM. For complete details, see *Configuring the Enterprise Service Manager* in the Enterprise Service Manager documentation.

➤ To manage ESM user mappings:

1. In the Policy Manager, select **[Tasks] > Manage ESM User Mappings** from the **Main Menu** (on the **browser client**, from the **Manage** menu). The Manage ESM User Mappings dialog appears.

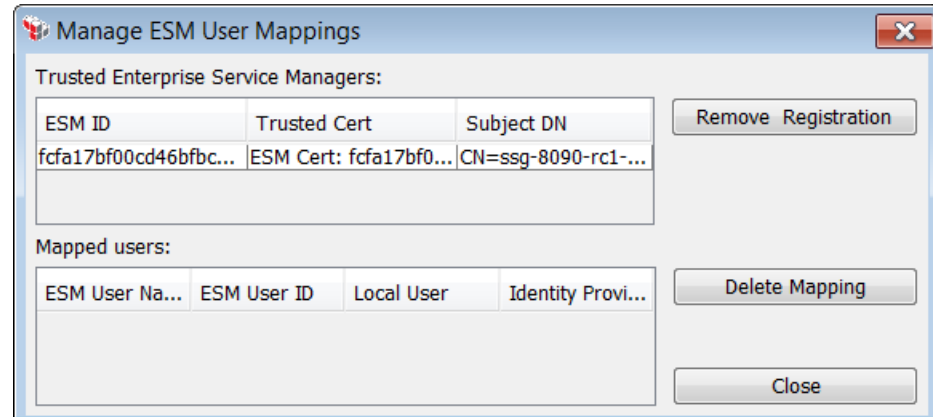


Figure 74: Manage ESM User Mappings dialog

2. The upper list shows which Enterprise Service Manager has been trusted to manage this Gateway cluster.
  - To sever the link between the Gateway cluster and the ESM system, select the ESM row from the list and then click **[Remove Registration]**. Click **[OK]** to acknowledge the confirmation. The ESM registration is removed.

---

**Note:** Removing the registration also removes all mapped users from that Enterprise Service Manager system. These users will no longer be able to perform any task involving the Gateway cluster (such as monitoring system properties, migrating services/policies, or generating reports).

---
3. The lower list shows which ESM user has been mapped to which Gateway user.
  - To remove a mapping between an ESM user and a Gateway user, select the appropriate row from the list and then click **[Delete Mapping]**. Click **[OK]** to acknowledge the confirmation. The ESM user is now considered untrusted and will have limited access to the Gateway cluster, regardless of his or her role within the Enterprise Service Manager. For more information, see *Mapping an ESM User to a Cluster* in the Enterprise Service Manager documentation.
4. Click **[Close]** when done.

## Managing HTTP Options

The *Manage HTTP Options* task is used to configure various options to be used by the Gateway for HTTP/HTTPS connections. For example, you can configure the login credentials for an HTTPS host, define a proxy for the host, or specify a private key to be used for authentication. This task is also used to edit the default HTTP proxy settings.

Only users with the [role](#) of 'Administrator' can create, edit, or remove HTTP options. Users in the following roles are able to view HTTP options:

*Manage Web Services*  
*Manage <name> Policy*  
*Manage <name> Service*  
*Operator*  
*Publish Web Services*

For more information, see "Predefined Roles and Permissions" on page 132.

---

**Note:** The HTTP options do not apply to HTTP routing, only to other HTTP(S) connections.

---

➤ *To manage HTTP options:*

1. In the Policy Manager, select [Tasks] > **Manage HTTP Options** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage HTTP Options dialog appears.

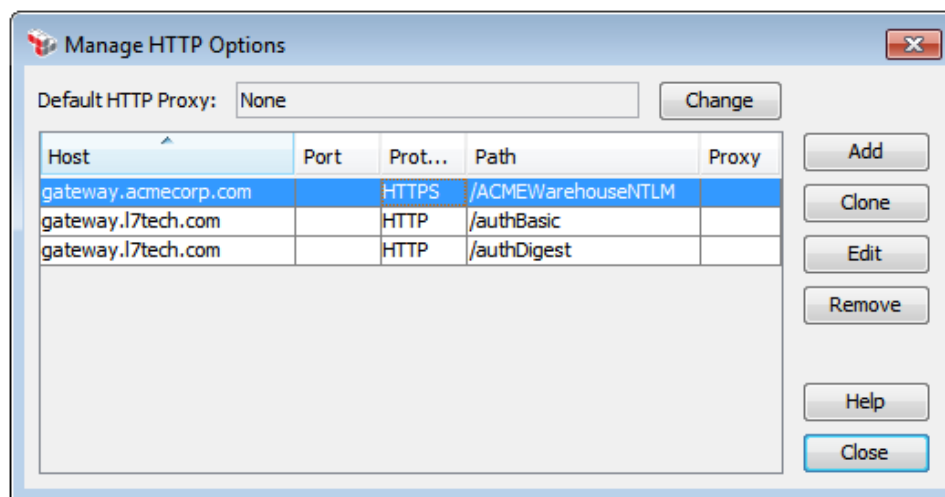


Figure 75: Manage HTTP Options dialog

The current default HTTP Proxy is shown (if one has been set). The list shows the HTTP options that have been defined.

## 2. Configure the dialog as follows:

| Setting                   | Description  |
|---------------------------|--|
| <b>Default HTTP Proxy</b> | <p>Displays the current default HTTP proxy host and port number (e.g., <i>myproxy:8888</i>).</p> <p>To change the default proxy, click <b>[Change]</b> and then complete the following fields in the Edit Default HTTP Proxy dialog:</p> <ol style="list-style-type: none"> <li>1. Enter the <b>Host</b> name of the new default proxy.</li> <li>2. Enter the <b>Port</b> number for the proxy.</li> <li>3. Enter the <b>Username</b> to log into the host.</li> <li>4. From the drop-down list, select the Password to use to log in. If the password you require is not listed, click <b>[Manage Stored Passwords]</b> to add it to the list of stored passwords. For more information, see "Managing Stored Passwords" on page 42.</li> </ol> <p><b>Tip:</b> You cannot type the password directly here; it must be defined in the Gateway's <a href="#">secure password storage</a>.</p> |
| <options list>            | <p>The list of HTTP options that have been defined. The following information is shown for each item:</p> <ul style="list-style-type: none"> <li>• <b>Host:</b> Hostname or IP address of the HTTP server.</li> <li>• <b>Port:</b> Port number of the HTTP server.</li> <li>• <b>Protocol:</b> Protocol used by the HTTP server: <b>HTTP</b>, <b>HTTPS</b>, or <b>&lt;Any&gt;</b>.</li> <li>• <b>Path:</b> The URL path prefix to match, which may include a query string.</li> <li>• <b>Proxy:</b> The proxy host and port number.</li> </ul>   |
| <b>[Add]</b>              | Use this to add a new item to the list. For more information, see "Adding an HTTP Option" on page 190.   |
| <b>[Clone]</b>            | Use this to create a new HTTP option by copying an existing one. Select the item to be cloned and then click <b>[Clone]</b> . Edit the fields as required. For more information about the fields, see "Adding an HTTP Option" on page 190.   |
| <b>[Edit]</b>             | Use this to modify the selected item. For information about the fields, see "Adding an HTTP Option" on page 190.   |
| <b>[Remove]</b>           | Use this to remove the selected item from the list. Click <b>[OK]</b> to confirm.  |

3. Click **[Close]** when done.

## Adding an HTTP Option

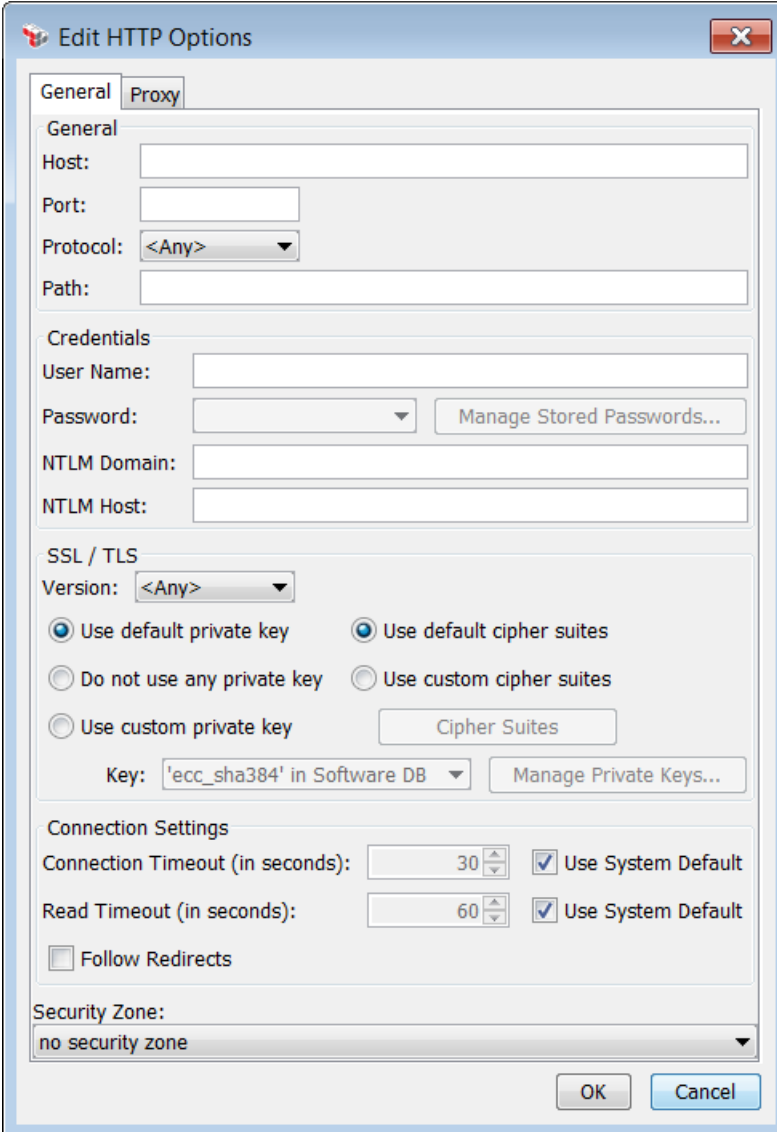
In the [Manage HTTP Options](#) task, you can add as many HTTP options as required. These options let you configure all aspects of an HTTP connection, including credentials, SSL/TLS settings, connection timeouts, and proxy settings.

➤ *To add a new HTTP option:*

1. In the Policy Manager, choose [**Tasks**] > **Manage HTTP Options** from the [Main Menu](#). The Manage Global Resources dialog appears.
2. Click [**Add**]. The Edit HTTP Options dialog appears.
3. Configure each tab as necessary.
4. Click [**OK**] when done.



## Configuring the [General] tab



**Edit HTTP Options**

**General** | Proxy

**General**

Host:

Port:

Protocol:

Path:

**Credentials**

User Name:

Password:

NTLM Domain:

NTLM Host:

**SSL / TLS**

Version:

☒ Use default private key    ☒ Use default cipher suites  
☐ Do not use any private key    ☐ Use custom cipher suites  
☐ Use custom private key   

Key:

**Connection Settings**

Connection Timeout (in seconds):  ☒ Use System Default

Read Timeout (in seconds):  ☒ Use System Default

☐ Follow Redirects

**Security Zone:**

Figure 76: Edit HTTP Options - [General] tab

The **[General]** tab is used to configure general information for the options.

Table 60: HTTP Options - [General] tab

| Section        | Description  |
|----------------|--|
| <b>General</b> | <p>Each HTTP option must have a unique combination of HTTP host, port, protocol, and path.</p> <ul style="list-style-type: none"> <li><b>Host:</b> Enter a valid hostname or IP address of the HTTP host.</li> </ul> |

| Section                    | Description   |
|----------------------------|---|
|                            | <p>This is required.</p> <ul style="list-style-type: none"> <li>• <b>Port:</b> Enter the port number to match. This is optional.</li> <li>• <b>Protocol:</b> Choose the protocol(s) to match from the drop-down list: <b>&lt;Any&gt;</b>, <b>HTTP</b>, <b>HTTPS</b>.</li> <li>• <b>Path:</b> Enter a well-formed URI.</li> </ul>  |
| <b>Credentials</b>         | <p>This section records HTTP authentication information. Enter the appropriate HTTP credentials: <b>User Name</b>, <b>Password</b>, <b>NTLM Domain</b>, and <b>NTLM Host</b> (assuming NTLM has been enabled).</p> <p>Note that the <b>Password</b> requires that you choose it from the drop-down list. If the password you need is not shown, click <b>[Manage Stored Passwords]</b> to define it first. For more information, see "Managing Stored Passwords" on page 42.</p>  |
| <b>SSL/TLS</b>             | <p>This section is enabled when the protocol selected is either <b>&lt;Any&gt;</b> or <b>HTTPS</b>.</p> <ul style="list-style-type: none"> <li>• <b>Version:</b> Choose the version of SSL/TLS to use or choose <b>&lt;Any&gt;</b> to allow all supported versions.</li> <li>• <b>Private key:</b> Indicate the private key requirements: choose either <b>default</b>, <b>none</b>, or a <b>custom</b> key from the keystore that you specify. You can click <b>[Manage Private Keys]</b> to examine your private keys more closely. For more information, see "Managing Private Keys" on page 260.</li> <li>• <b>Cipher suite:</b> Indicate the cipher requirements: choose either a <b>default</b> or <b>custom</b> suite to use. The default suite consists of those ciphers that will offer the greatest compatibility when the Gateway connects to a server via HTTPS. Alternatively, you can click <b>[Cipher Suites]</b> to choose which ciphers to use and in which order. For more information, see "Selecting Cipher Suites" on page 194.</li> </ul> |
| <b>Connection Settings</b> | <ul style="list-style-type: none"> <li>• <b>Connection Timeout:</b> This defines the maximum time to wait for a connection to be established. If exceeded, the connection will fail.<br/><br/>To override the system default, clear the <b>Use System Default</b> check box and then enter a different value. The system default for this timeout is defined by the <a href="#">io.outConnectTimeout</a> cluster property. The default value is 30 seconds.</li> <li>• <b>Read Timeout:</b> This defines the maximum time allowed for response data to be read. If exceeded, the request will fail.<br/><br/>To override the system default, clear the <b>Use System Default</b> check box and enter a value. The system default for this timeout is defined by the <a href="#">io.outTimeout</a> cluster property. The default value is 60 seconds.</li> </ul>   |

| Section              | Description   |
|----------------------|---|
|                      | <ul style="list-style-type: none"> <li>• <b>Follow Redirects:</b> Select this check box to follow HTTP redirect responses.</li> </ul>   |
| <b>Security Zone</b> | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "<b>No security zone</b>".</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> |

## Configuring the [Proxy] tab

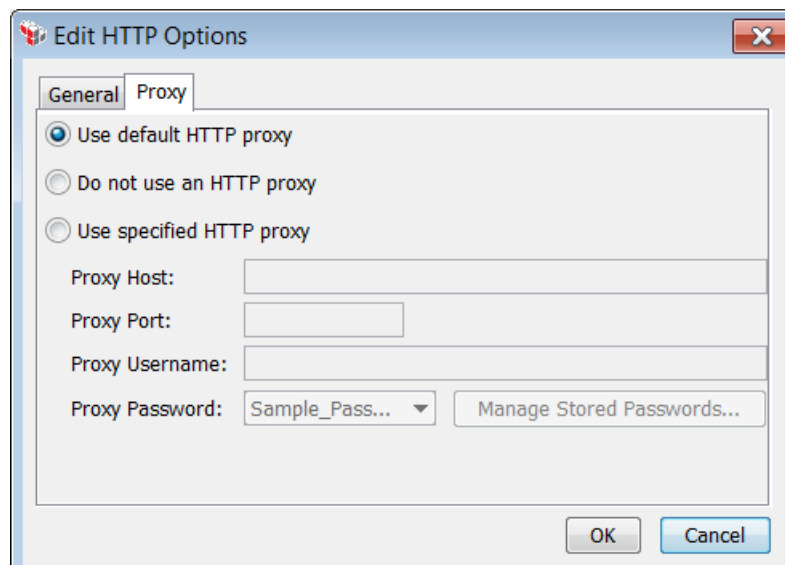


Figure 77: Edit HTTP Options - [Proxy] tab

The **[Proxy]** tab lets you specify proxy options. By default, the shared proxy settings will be used. You can specify to not use an HTTP proxy or to use a specific HTTP proxy with the settings indicated here.

- **Proxy Host:** Enter a valid hostname or IP address for the host.
- **Proxy Port:** Enter a value port number.
- **Proxy Username:** Enter the user name to log onto the proxy host.
- **Proxy Password:** Choose the proxy password from the drop-down list. If the password you need is not shown, click **[Manage Stored Passwords]** to define it first. For more information, see "Managing Stored Passwords" on page 42.

## Selecting Cipher Suites

The Cipher Suite Configuration dialog is used to specify which outbound TLS cipher suites you want to enable on the CA API Gateway for a specific target host.

### Supported Cipher Suites

The following is a list of the cipher suites supported by the CA API Gateway. These are the suites that are available when the Policy Manager is connected to a Gateway using the default configuration with the Software DB keystore. If your Gateway uses a different security configuration, not all suites will be functional.

```

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_RC4_128_MD5
SSL_DHE_RSA_WITH_DES_CBC_SHA
SSL_RSA_WITH_DES_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
TLS_ECDH_ECDSA_WITH_RC4_128_SHA
TLS_ECDH_RSA_WITH_RC4_128_SHA
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

```

TLS\_DH\_RSA\_WITH\_AES\_256\_GCM\_SHA384  
TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA256  
TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA  
TLS\_DH\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA256  
TLS\_DH\_RSA\_WITH\_AES\_128\_CBC\_SHA  
SSL\_DH\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA  
SSL\_DH\_RSA\_WITH\_DES\_CBC\_SHA

➤ To select cipher suites to use:

1. Do one of the following:
  - Click [**Cipher Suites**] on the Edit HTTP Options dialog. For more information, see "Adding an HTTP Option" on page 190.
  - Click [**Cipher Suites**] on the [Security] tab of the HTTP(S) Routing Properties. For more information, see Route via HTTP(S) assertion in the *Layer 7 Policy Authoring User Manual*.
  - Select the [SSL/TLS Settings] tab of the "Listen Port Properties" on page 57.

---

**Tip:** In the Listen Port Properties, the cipher suites are selected directly in the [SSL/TLS Settings] tab; there is no separate "Enable Cipher Suites" dialog (Figure 78).

---

The Enabled Cipher Suites dialog is displayed. This dialog lists the suites that are recognized by the Gateway. Note that list of ciphers suites visible depends on the security configuration of your Gateway. See "[Supported Cipher Suites](#)" above for a complete list.

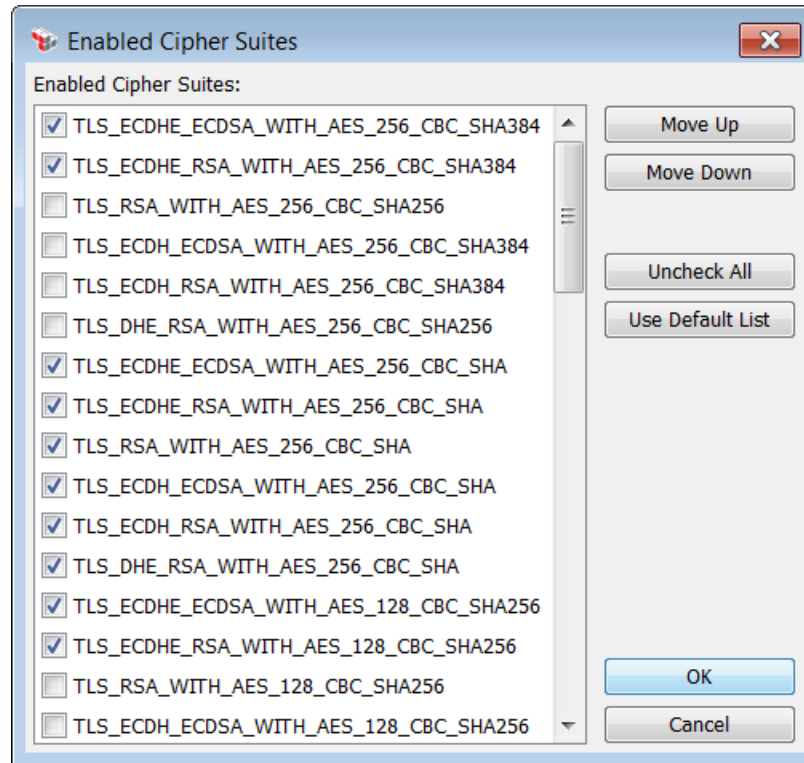


Figure 78: Enabled Cipher Suites

2. Specify the order of the cipher suites to use:
  - Select one or more lines and use **[Move Up]** and **[Move Down]** to reorder the cipher suites.
  - Select **[Uncheck All]** to quickly remove all selections so that you can specify the suite(s) you want to use.
  - Select **[Use Default List]** to reset the list to the default set of cipher suites. The default suites are those that are least likely to cause compatibility issues with target servers.
3. Click **[OK]** when done.

## Managing Service Resolution

When a message is received by the CA API Gateway, it is necessary to determine the target service—this process is known as *service resolution*. The Service Resolution Settings dialog allows you to configure resolution behavior.

To learn more about the Gateway's service resolution logic, see *Understanding the Service Resolution Process* in the *Layer 7 Installation and Maintenance Manual*.

Before you change any of the resolution settings, be aware of the following ramifications:

- Changing service resolution settings may cause services that previously resolved to no longer resolve. For example, you have two services that share the same custom resolution path but are capitalized differently. If you change the resolution to be case insensitive, those services will conflict.
- The default resolution settings are compatible with the SecureSpan XML VPN Client.

➤ To configure service resolution:

1. In the Policy Manager, select **[Tasks] > Manage Service Resolution** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Service Resolution Settings dialog appears. You can also access this dialog from the [Manage Listen Ports](#) task.

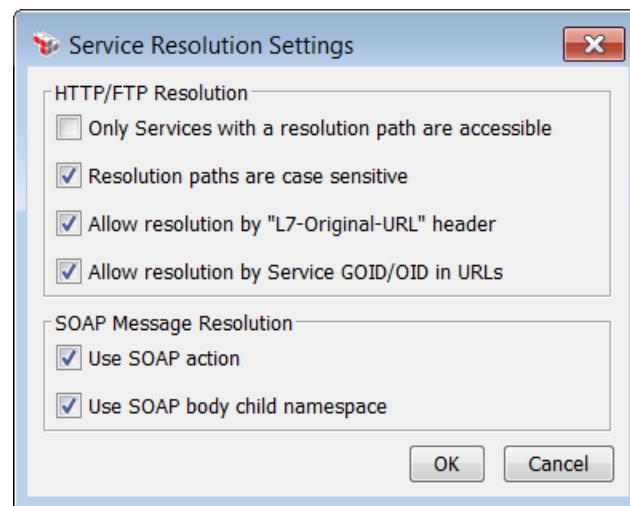


Figure 79: Service Resolution Settings dialog

3. Configure the dialog as follows:

Table 61: Service Resolution settings

| Setting  | Description   |
|--|---|
| <i>HTTP/FTP Resolution</i>                                 |   |
| <b>Only Services with a resolution path are accessible</b> | <p>Select this check box to prevent access to any service that was not assigned a resolution path via HTTP/FTP listeners. This is useful when you have services associated with a JMS or Email listener and you wish to prevent any other access.</p> <p>Clear this check box to allow all services to be resolved as described under <i>Understanding the Service Resolution Process</i> in the <i>Layer 7</i></p> |

| Setting   | Description   |
|---|---|
|   | <i>Installation and Maintenance Manual</i> . This setting is the default.   |
| <b>Resolution paths are case sensitive</b>          | <p>Select this box to enforce case sensitivity of resolution paths. This setting is the default.</p> <p>Clear this check box to ignore case when comparing a request to a services custom resolution path. Relaxing the case will allow services to be more readily matched.</p> <p><b>IMPORTANT:</b> Switching to case insensitive comparisons may cause services that previously resolved to no longer resolve. For example, there are two services that have the same custom resolution path differentiated only by case. In the default behavior, these two paths are unique, but when case sensitivity is removed, those resolution paths are now the same and the services will conflict.</p> <p><b>Other Areas Affected by Case Sensitivity Changes</b></p> <p>Changing the case sensitivity for resolution paths also affects how other areas of the Gateway resolve services:</p> <ul style="list-style-type: none"> <li>• <b>WSDL Proxy:</b> A path can be used in the WSDL proxy to identify from which service the WSDL should be download. When case sensitivity is disabled, the WSDL proxy will match services accordingly.</li> </ul> <p>For more information, see "Downloading a WSDL" in the <i>WSDL Proxy &amp; Policy Downloads</i> appendix in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <ul style="list-style-type: none"> <li>• <b>WSDM Services:</b> A path can be used to identify a WSDM service. When case sensitivity is disabled, the WSDM services will match services accordingly.</li> </ul> <p>For more information, see "Working with Internal Services" on page 371.</p> |
| <b>Allow resolution by "L7-Original-URL" header</b> | <p>Select this check box to allow a service to be resolved using a path supplied in an HTTP header. This setting is the default.</p> <p><b>Tip:</b> If your deployment does not use the SecureSpan XML VPN Client, you may disable this functionality.</p> <p>For more information, see "Step 2: Determine service based on URI" under <i>Understand the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>  |
| <b>Allow resolution by Service GOID/OID in URLs</b> | <p>Select this check box to permit services to be resolved by URLs that contain the service GOID (i.e., entity ID) or OID. This setting is the default.</p> <p>Clear this check box to not permit resolution by service GOID or OID.</p> <p><b>Note:</b> Any service URLs published to UDDI by the Gateway will not resolve if consumed.</p> <p>For more information, see "Step 1: Determine service based on service entity ID" under <i>Understand the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>  |



| Setting                              | Description   |
|--------------------------------------|---|
| <i>SOAP Message Resolution</i>       |   |
| <b>Use SOAP action</b>               | <p>Select this check box to permit services to be resolved based on the SOAP action in the incoming message. This setting is the default.</p> <p>Clear this check box to not consider the SOAP action when resolving the service.</p> <p>For more information, see "Step 3: Determine service based on SOAPAction" under <i>Understand the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>                                      |
| <b>Use SOAP body child namespace</b> | <p>Select this check box to permit services to be resolved based on the SOAP payload namespace of the message body. This setting is the default.</p> <p>Clear this check box to not consider the namespace in the SOAP payload when resolving the service.</p> <p>For more information, see "Step 4: Determine service based on SOAP payload namespace" under <i>Understand the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> |

- Click **[OK]** when done.

## Managing SFTP Polling Listeners

You can configure the Gateway to periodically poll a directory on an external SFTP server for messages to process. If a new message is found, it is retrieved from the server and processed.

➤ *To manage SFTP polling listeners:*

- In the Policy Manager, select **[Tasks] > Additional Actions > Manage SFTP Polling Listeners** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage SFTP Polling Listeners dialog appears.

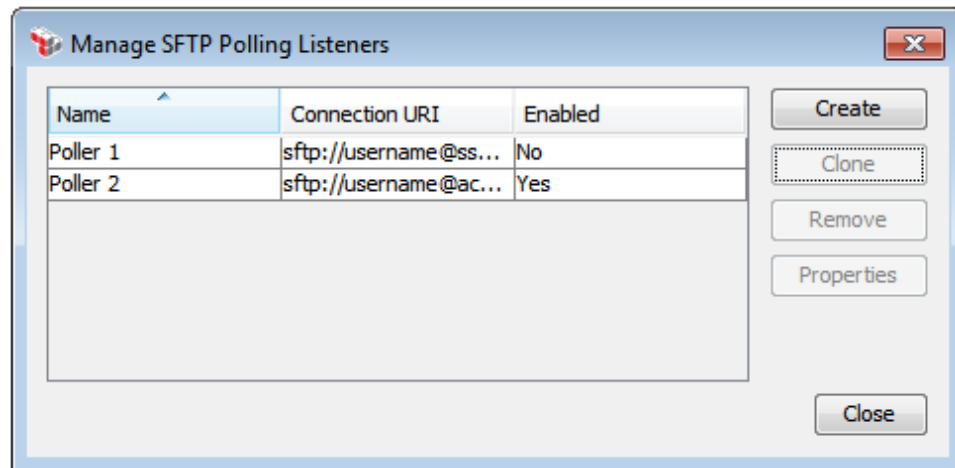


Figure 80: Manage Email Listeners dialog

- The SFTP polling listeners configured are displayed. Choose an action to perform:

Table 62: Managing SFTP polling listener tasks

| To...   | Do this...  |
|---|---|
| <b>Create a new SFTP polling listener</b>                       | <ol style="list-style-type: none"> <li>Click <b>[Create]</b>.</li> <li>Configure the new listener. For a description of each property, see "SFTP Polling Listener Properties" on page 201.</li> </ol>   |
| <b>Clone an existing SFTP polling listener</b>                  | <ol style="list-style-type: none"> <li>Select the listener to clone.</li> <li>Click <b>[Clone]</b>.</li> <li>Edit the <a href="#">SFTP Polling Listener Properties</a> as required.</li> </ol>  |
| <b>Remove an SFTP polling listener</b>                          | <ol style="list-style-type: none"> <li>Select the listener to remove.</li> <li>Click <b>[Remove]</b>. The listener is removed from the list.</li> </ol> <p><b>Tip:</b> As an alternative to remove the listener, you can disable it instead. To disable a listener, view its properties and clear the <b>Enabled</b> check box.</p> |
| <b>View or edit the properties for an SFTP polling listener</b> | <ol style="list-style-type: none"> <li>Select the listener to view or edit.</li> <li>Click <b>[Properties]</b>.</li> <li>Edit the <a href="#">SFTP Polling Listener Properties</a> as required.</li> </ol>  |

- Click **[Close]** when done.

## SFTP Polling Listener Properties

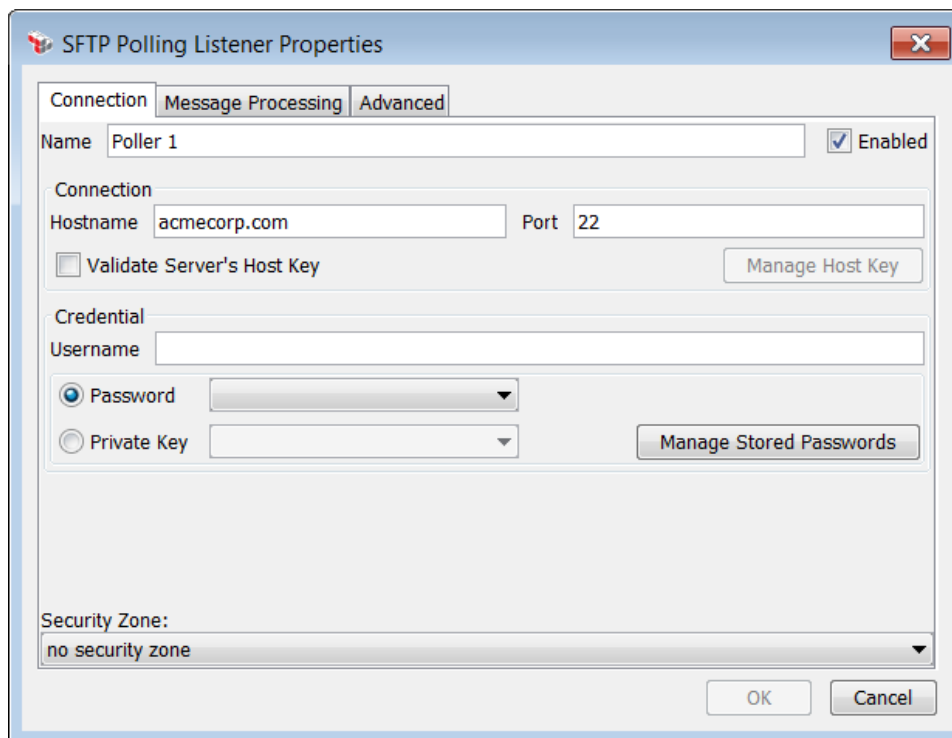
When creating or viewing details about an [SFTP Polling Listener](#), the SFTP Polling Listener Properties appear. This dialog lets you retrieve messages from an external SFTP server for processing on the Gateway.

➤ To access the properties for an SFTP polling listener:

1. Run the [Manage SFTP Polling Listeners](#) task.
2. Select an SFTP polling listener from the list and then click **[Properties]**. You can also click **[Create]** to enter the properties for a new listener.

The SFTP Polling Listener Properties appear. This dialog organizes the service properties across these tabs: **Connection**, **Message Processing**, and **Advanced**.

### Configuring the [Connection] Tab



The screenshot shows the 'SFTP Polling Listener Properties' dialog box with the 'Connection' tab selected. The dialog has three tabs: 'Connection', 'Message Processing', and 'Advanced'. The 'Name' field is 'Poller 1' and the 'Enabled' checkbox is checked. Under the 'Connection' section, the 'Hostname' is 'acmecorp.com' and the 'Port' is '22'. There is a 'Validate Server's Host Key' checkbox and a 'Manage Host Key' button. Under the 'Credential' section, the 'Username' field is empty. The 'Password' radio button is selected, and there is a 'Manage Stored Passwords' button. The 'Private Key' radio button is unselected. At the bottom, the 'Security Zone' dropdown menu is set to 'no security zone'. 'OK' and 'Cancel' buttons are at the bottom right.

Figure 81: SFTP Polling Listener Properties - [Connection] tab

Configure the **[Connection]** tab as follows:

Table 63: SFTP Polling Listening settings - [Connection] tab

| Setting                         | Description   |
|---------------------------------|---|
| <b>Name</b>                     | Enter the name of the SFTP polling listener. If you are creating several listeners, make sure the name is descriptive.  |
| <b>Enabled</b>                  | Select this check box to enable the listener. Clear this check box to deactivate or disable the listener. Deactivating a listener is an alternative to removing it.   |
| <b>Hostname</b>                 | Enter the hostname of the remote SFTP server.   |
| <b>Port</b>                     | Enter the port number to monitor. The default is <b>22</b> .  |
| <b>Validate Server Host Key</b> | Select this check box to validate the server's SSH public key against a fingerprint that you will specify using the <b>[Manage Host Key]</b> button.<br><br>Clear this check box to not validate the server's host key. This setting is the default.  |
| <b>Manage Host Key</b>          | This button is available only when you are validating the server's host key. It is used to enter the fingerprint against which the host key is validated. Complete the following: <ul style="list-style-type: none"> <li>• <b>SSH Public Key Fingerprint:</b> Paste the SSH public key fingerprint as retrieved from the remote server's public key location.</li> <li>• <b>[Load from File]:</b> Click this to load the fingerprint from a text file.</li> </ul> |
| <b>Username</b>                 | Enter the account name to access the SFTP server.<br><br><b>IMPORTANT:</b> Specify a user with limited access rights (for example, create a new listener called "ssgpoll"). Do not use the root user. The polling listener appends the suffix ".processed" to each file that is processed. Using the root user could cause system files to be renamed, rendering the Gateway and the host machine inoperable.   |
| <b>Password</b>                 | If authenticating via password, choose the password from the drop-down list.<br><br>If the password you require is not listed, click <b>[Manage Stored Passwords]</b> to add it to the Gateway's password storage. For more information, see "Managing Stored Passwords" on page 42.<br><br><b>Tip:</b> You cannot type the password directly here; it must be defined in the Gateway's <a href="#">secure password storage</a> .                                 |
| <b>Private Key</b>              | If authenticating via private key, choose the key to use.<br><br>If the key you require is not listed, click <b>[Manage Stored Passwords]</b> to add it to the Gateway's password storage. For more information, see "Managing Stored Passwords" on page 42.  |
| <b>Security Zone</b>            | Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b> .  |

| Setting | Description  |
|---------|--|
|         | <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> |

## Configuring the [Message Processing] Tab

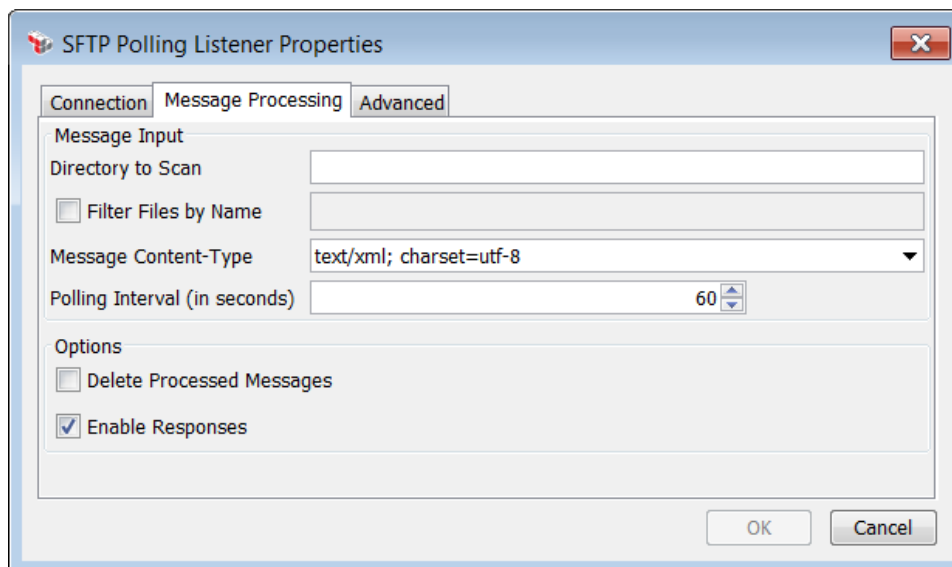


Figure 82: SFTP Polling Listener Properties - [Message Processing] tab

Configure the [Message Processing] tab as follows:

Table 64: SFTP Polling Listening settings - [Message Processing] tab

| Setting                    | Description   |
|----------------------------|---|
| <i>Message Input</i>       |   |
| <b>Directory to Scan</b>   | <p>Specify the directory to poll. It is recommended that a directory be created specifically for polling purposes. This directory must already exist.</p> <p><b>Notes:</b> (1) The user specified in the [Connection] tab must have read and write access for this directory. (2) Specifying the root directory ("/") is not recommended and a warning will be displayed when you save the SFTP polling listener.</p> |
| <b>Filter File by Name</b> | <p>Select this check box to filter files to be processed by name. Clear this check box to process all files.</p>  |

| Setting                              | Description  |
|--------------------------------------|--|
|                                      | Enter the file name in the adjacent text box. You may use regular expressions such as "test\d+\.xml".  |
| <b>Message Content-Type</b>          | Choose the Content-Type to use from the drop-down list. If the Content-Type you need isn't listed, type it directly into the drop-down list.   |
| <b>Polling Interval (in seconds)</b> | Indicate the polling interval, in seconds. The listener will check for messages after the specified number of seconds.   |
| <i>Options</i>                       |  |
| <b>Delete Processed Messages</b>     | <p>Select this check box to delete the request file from the SFTP server once the message is processed.</p> <p>Clear this check box to leave the processed messages on the SFTP server. These messages will have the suffix ".processed".</p>  |
| <b>Enable Responses</b>              | <p>Select this check box to configure the listener to return Gateway responses. A response message will be saved to the SFTP server with the same name as the file that was processed with a suffix of ".response".</p> <p>Clear this check box to not create response files.</p> <p><b>Note:</b> If there is a file of the same name already, the Gateway will try to overwrite the contents of that files. If the Gateway is unable to write the response message, it will log an audit message.</p> |

## Configuring the [Advanced] Tab

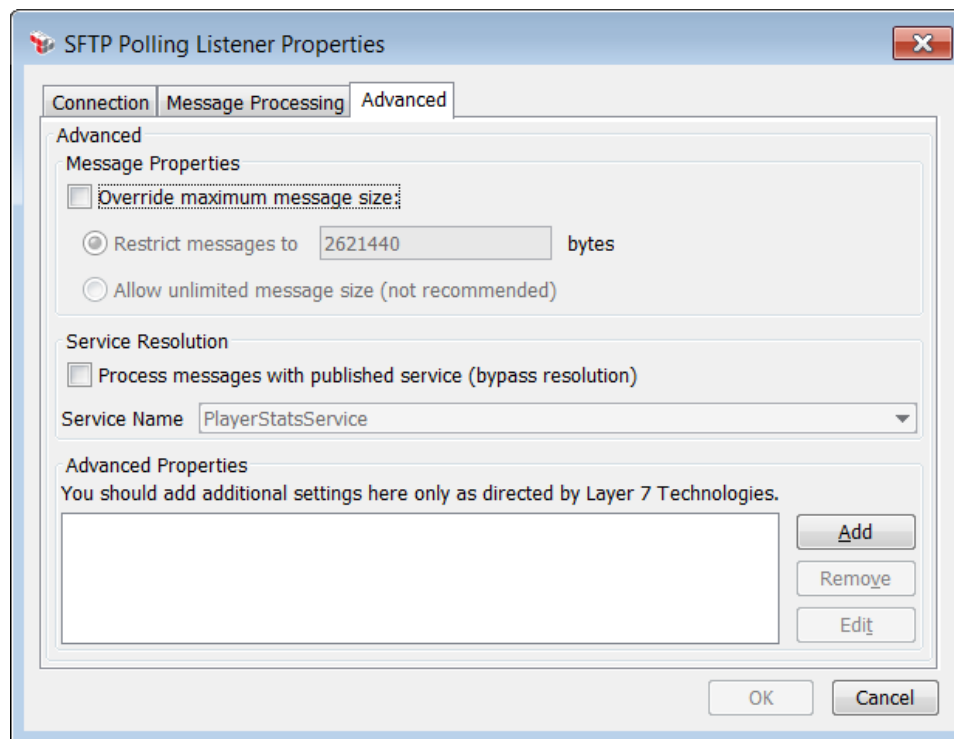


Figure 83: SFTP Polling Listener Properties - [Advanced] tab

Configure the **[Advanced]** tab as follows:

Table 65: SFTP Polling Listening settings - [Advanced] tab

| Setting  | Description   |
|--|---|
| <b>Override maximum message size</b>           | <p>Select this check box to override the permitted maximum size of the message. Clear this check box to use the value set in the <a href="#">io.xmlPartMaxBytes</a> cluster property.</p> <ul style="list-style-type: none"> <li><i>Restrict messages to:</i> Enter the maximum permitted size of the message, in bytes.</li> <li><i>Allow unlimited message size (not recommended):</i> Select this option to allow response messages of unlimited size. This is not recommended and should be used only under the direction of CA Technical Support.</li> </ul> |
| <b>Process messages with published service</b> | <p>Select this check box to resolve messages to a specified published service that you indicate in the <b>Service Name</b> field below. This bypasses the Gateway's normal service resolution process.</p> <p>Clear this check box to process messages using the Gateway's service resolution logic. For more information, see <i>Understanding the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>   |

| Setting                    | Description  |
|----------------------------|--|
| <b>Service name</b>        | If associating an SFTP polling listener with a specific service, choose the service from the drop-down list. If the service you want is not in the list, you must <a href="#">publish</a> it first.  |
| <b>Advanced Properties</b> | This section is used to add, edit, or remove any additional settings required to configure the SFTP Polling Listener Properties. This section is intended for advanced users and should be configured only as directed by <a href="#">CA Technical Support</a> . |

## Working with SCP/SFTP Messages

The CA API Gateway supports SCP (Secure Copy Protocol) and SFTP (SSH File Transfer Protocol) messages, both inbound and outbound. This allows the Gateway to work with backend services which rely on these protocols. These messages are secured using the SSH2 protocol (SSH1 is not supported).

### Using Inbound SSH

➤ *To handle inbound SCP/SFTP messages:*

- Configure an internal SSH server running on a Gateway listen port. This is done by creating a new listen port using the "SSH2" protocol. The SSH listener supports inbound SCP upload and inbound SFTP "PUT" commands to the Gateway. This listener automatically opens and closes the SSH port on start and stop.

For more information, see "Managing Listen Ports" on page 54.

➤ *To resolve the service for SCP/SFTP messages:*

- SOAP-based messages are resolved using the Gateway's service resolution logic. For a detailed explanation, see *Understanding the Gateway Service Process* in the *Layer 7 Installation and Maintenance Manual*.
- Path-based resolution depends on the protocol:
  - **SCP:** You can specify a directory on the SCP server. When a file is uploaded, the full path is used to resolve the service.

The following example uploads an XML/SOAP file to a service with the URI `/xmlservice`:

```
$> scp -P 2222 message.xml user@gateway.17tech.com:/xmlservice
user@gateway.17tech.com's password:
message.xml
```

**Tip:** Enter the password carefully, as there is no feedback at this point if authentication fails due to an incorrect password being entered here.



- **SFTP:** Use the "cd" command to change to a directory on the SFTP server. When a file is uploaded, the full path is used to resolve the service.

This is the same example as above, for SFTP:

```
$> sftp -oPort=2222 anonymous@gateway.17tech.com
anonymous@gateway.17tech.com's password:
Connected to gateway.17tech.com.
sftp> cd xmlservice
sftp> put message.xml
Uploading message.xml to /xmlservice/message.xml
...
sftp> bye
```

➤ *To authenticate users for SCP/SFTP messages:*

- **Method 1: Password authentication:** The user's password from the [Internal Identity Provider](#) is used during SSH processing. The inbound SSH server configured on the Gateway will attempt to validate the user's password during the authentication process.
- **Method 2: Public key authentication:** This requires a one-time setup by copying the user's public key to his or her user record in the Internal Identity Provider. During SSH processing, the inbound SSH server configured on the Gateway will attempt to validate the user's public key during the authentication process. For more information see the [\[SSH\]](#) tab in "Creating an Internal User" on page 286.

### Context Variables

SSH processing populates the following context variables:

```
request.tcp.localPort
request.tcp.remoteAddress
request.tcp.remoteip
request.tcp.remoteHost
request.ssh.path
request.ssh.file
```

For more information about these variables, see "Transport Layer Variables" on page 550.

### Inbound SFTP Polling Listener

The CA API Gateway has a polling feature that will retrieve ("GET") and process messages from a directory on an external SFTP server. In this configuration, the Gateway will act as an SFTP client and periodically check for new messages to process.

For more information, see "Managing SFTP Polling Listeners" on page 199.

### Using Outbound SSH

The CA API Gateway provides the following outbound support for SSH sessions:

- outbound SCP upload and download with an external SCP server
- outbound SFTP "PUT" and "GET" with an external SFTP server

These are handled using the Route via SSH2 assertion in the *Layer 7 Policy Authoring User Manual*.

## Managing Keystore

The Gateway can use either of the following keystores:

- *Software DB*: This is a software keystore that is built into every Gateway database, as a PKCS#12 keystore. The software keystore is always available and will be used unless a hardware keystore is installed. Private keys stored in the software keystore may be exported as PKCS#12 files and then imported into the SafeNet Luna HSM if necessary.
- *Hardware, SafeNet Luna SA*: This is an optional network-attached HSM that can be accessed by the CA API Gateway.

The Manage Keystore task is used to enable, disable, or view the status of the SafeNet Luna HSM.

*Prerequisite*: The SafeNet Luna HSM must be correctly installed and configured, including the JSP on all cluster nodes. Please refer to the setup instructions provided by SafeNet.

### W A R N I N G

Switching from one keystore to another will cause the Gateway to lose access to any private keys stored in the previous keystore. This may cause policies or listen ports to fail. To ensure that you can start the Policy Manager, make sure there is at least one listen port that uses the "Default SSL key".

### Fallback to System Default Keystore

If the SafeNet HSM is enabled but the Gateway is unable to connect to it on startup, the Gateway will fall back to the software keystore.

If fallback occurs, you may need to re-enter the Partition Client PIN with the Policy Manager. For details, see Table 66 below.

➤ *To manage keystores:*

1. In the Policy Manager, select [Tasks] > **Manage Private Keys** from the [Main Menu](#). The [Manage Private Keys](#) dialog appears.

- Click **[Manage Keystore]** and then enter the Gateway partition password if prompted. The Manage Keystore dialog is displayed and will show different messages depending on your current configuration. Figure 84 shows one example:

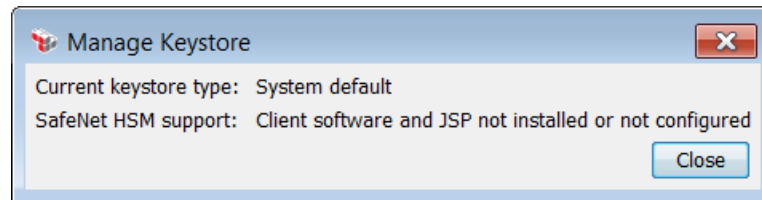


Figure 84: Manage Keystore dialog

This dialog provides details about the current status of your keystore:

Table 66: Information about your keystore

| Label                        | Description   |
|------------------------------|---|
| <b>Current keystore type</b> | <p>Displays the keystore currently being used:</p> <ul style="list-style-type: none"> <li>• <i>SafeNet HSM</i></li> <li>• <i>System default</i></li> <li>• <i>Configured for system default, but using SafeNet HSM:</i> The SafeNet HSM has been disabled but the current Gateway node has not yet restarted for the system default to take effect.</li> <li>• <i>Configured for SafeNet HSM, but using system default:</i> This can indicate one of two things: <ul style="list-style-type: none"> <li>• The SafeNet HSM has been enabled but the current Gateway node has not yet restarted for the SafeNet HSM to take effect.</li> <li>• The Gateway is configured to use the SafeNet HSM but had to fall back to the system default keystore in order to start the node successfully.</li> </ul> </li> </ul> <p>The system default is the software database.</p> |
| <b>SafeNet HSM support</b>   | <p>Displays the current status of the SafeNet HSM:</p> <ul style="list-style-type: none"> <li>• <i>Ready to use:</i> The SafeNet HSM is correctly configured.</li> <li>• <i>Client software and JSP not installed or not configured:</i> The SafeNet HSM client software and Java Service Provider (JSP) is either not present or incorrectly configured. For information on configuring the SafeNet HSM for use with the Gateway, consult the <i>Layer 7 Installation and Maintenance Manual</i>.</li> </ul>   |
| <b>Disable SafeNet HSM</b>   | <p>Available only if a SafeNet HSM is configured and enabled.</p> <p>Disable the SafeNet HSM and revert to using the system default keystore upon Gateway restart.</p>  |
| <b>Enable SafeNet HSM</b>    | <p>Available only if a SafeNet HSM is configured but not enabled.</p>   |

| Label | Description   |
|-------|---|
|       | <p>Enable the SafeNet HSM upon Gateway restart. This button is available even when SafeNet HSM is configured and ready to use, but is not currently the active keystore. The Connect to SafeNet HSM dialog is displayed.</p> <p>Enter the following information and then click <b>[Connect]</b>:</p> <ul style="list-style-type: none"> <li>• <b>Partition Client PIN:</b> Enter the client PIN for the Gateway's intended Luna partition. This is required.</li> <li>• <b>Override slot number:</b> Optionally select this check box to choose a specific slot number to connect to. This is normally not required, but it may be useful for a Software Gateway that is running on a machine that has been configured with access to more than one Luna partition. Consult with your SafeNet Luna administrator for details; if unsure, leave the slot number unchanged.</li> </ul> <p>Restart all Gateway cluster nodes for the configuration changes to take effect.</p> |

3. Click **[Close]** when done.

## Configuring Preferences

The Preferences dialog allows you to configure the following program preferences:

- Inactivity timeout period
- Save login user name
- Disable policy validation
- Control how many Gateway URLs are remembered

You can configure preferences at any time, regardless of whether you are [connected](#) to a Gateway.

➤ *To configure preferences:*

1. Do one of the following:
  - Select **[File]** > **Preferences** from the [Main Menu](#), or
  - Click **[Preferences]** on the [Main Tool Bar](#), or
  - Select **[Manage]** > **Preferences** in the [browser client](#)

The Preferences dialog appears. Note that the fewer preference settings are available when accessed from the browser client.

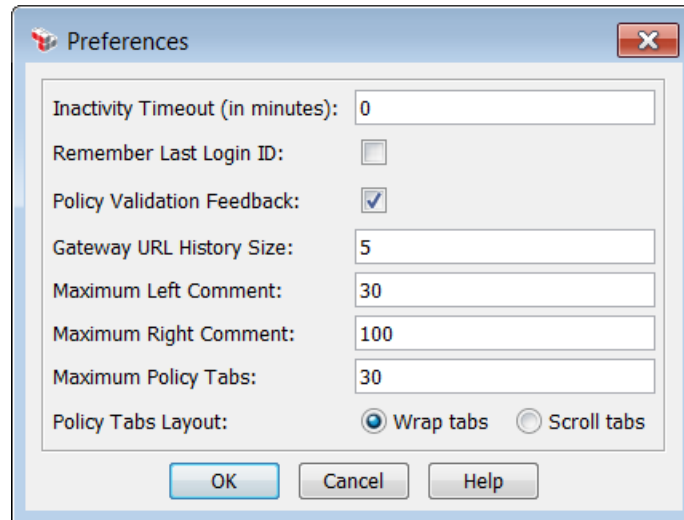


Figure 85: Preferences dialog (desktop client)

2. Configure the dialog as follows:

Table 67: Preferences settings

| Setting   | Description  |
|---|--|
| <b>Inactivity Timeout</b><br><i>(Desktop client only)</i>     | <p>Enter a timeout period, between 1 and 60 minutes. For security purposes, the Policy Manager will automatically disconnect from the Gateway after this many minutes of inactivity (i.e., keyboard presses or mouse activity when the Policy Manager is in the foreground). The default is <b>30</b>. To disable the timeout, enter <b>0</b> (zero).</p> <p><b>Tip:</b> This inactivity timeout applies to the Policy Manager. To configure timeout values for the Gateway, see "Managing Administrative User Account Policy" on page 301.</p>  |
| <b>Remember Last Login ID</b><br><i>(Desktop client only)</i> | <p>Select this check box to have the Policy Manager remember the last user ID used to connect to the Gateway. This is displayed on the <a href="#">Login</a> dialog.</p> <p>This setting is convenient if the same user usually signs into the Policy Manager. If this check box is cleared, the user ID must be typed each time on the Login dialog.</p>  |
| <b>Policy Validation Feedback</b>                             | <p>This check box should normally be selected to enable policy validation. When constructing large and complex policies, you may wish to temporarily disable the validation to prevent the system from slowing down.</p> <p>When disabling/enabling feedback, the change occurs the next time an action is performed that requires validation (i.e., changing assertions in the policy, clicking <b>[Validate]</b>).</p> <p><b>Note:</b> Turning off policy validation disables both the instant feedback messages and the final checks that occur when you click <b>[Save]</b> or</p> |

| Setting  | Description  |
|--|--|
|  | [Validate].  |
| <b>Gateway URL History Size</b><br>(Desktop client only) | Enter the number of Gateway URLs to be remembered on the <a href="#">Login</a> dialog. The maximum history size is 50. The default is 5. To disable the Gateway URL history, enter 0 (zero). This will also clear all URLs currently being remembered.   |
| <b>Maximum Left Comment</b>                              | <p>Enter the number of characters to display in the policy development window for a left comment. Comments longer than this will be truncated but will be visible in a tooltip when mousing over the comment. The default is 30 characters.</p> <p>For more information, see <i>Adding a Comment</i> in the <i>Layer 7 Policy Authoring User Manual</i>.</p> <p><b>Note:</b> This does not affect the maximum left comment size, which remains at 100 characters.</p>  |
| <b>Maximum Right Comment</b>                             | <p>Enter the number of characters to display in the policy development window for a right comment. Comments longer than this will be truncated but will be visible in a tooltip when hovering the mouse pointer over the comment. The default is 100 characters.</p> <p>For more information, see <i>Adding a Comment</i> in the <i>Layer 7 Policy Authoring User Manual</i>.</p> <p><b>Note:</b> This does not affect the maximum right comment size, which remains at 4000 characters.</p>   |
| <b>Maximum Policy Tabs</b>                               | <p>Enter the maximum number of tabs that can be open at once in the policy editor workspace. Once this maximum has been reached, the Policy Manager will automatically close the oldest (least recently used) tab that has no unsaved changes. If there are no tabs that meet these criteria, then you will be prompted to either manually close some tabs or increase the maximum number of tabs. Enter a value from 1 to 100. The default is 30 tabs.</p> <p><b>Tips:</b> (1) This setting is intended to meet your personal workflow. There are no performance implications on the Gateway when opening more tabs. (2) If you change this setting to be less than the number of currently open tabs, no tab closure will be enforced until you attempt to open another tab.</p> |
| <b>Policy Tabs Layout</b>                                | <p>Choose how tabs should be displayed if the number of open tabs exceed the width of the Policy Manager window:</p> <ul style="list-style-type: none"> <li>• <b>Wrap tabs:</b> Multiple rows of tabs will be created.<br/>With this setting, the full tab titles are always visible, however it will occupy more space in the Policy Manager. This setting is the default.</li> <li>• <b>Scroll tabs:</b> Tabs are always displayed in a single row, possibly with truncated titles. Left and right scroll buttons access tabs scrolled out of view.</li> </ul>   |

| Setting | Description   |
|---------|---|
|         | With this setting, less space is used on the interface, but tab titles may be truncated and scroll buttons may be required to access some tabs. |

3. Click **[OK]**. The changes take effect immediately.

## Working with JSON

The CA API Gateway can work with messages in the JSON (JavaScript Object Notation) format. You can use the Gateway to process incoming JSON payloads, validate incoming JSON payloads, output to JSON, or transform messages from JSON to other Content-Types (for example, text/XML).

By default, the CA API Gateway will accept any incoming Content-Type, unless the entry point is associated with a SOAP-based service. When a request containing a JSON payload arrives at the Gateway, the `${request.*}` context variables will contain all aspects of the JSON message. In a service policy, you can validate the JSON structure in a message by using the Validate JSON Schema assertion. You can also validate a JSON-specific pattern or extract parts of a JSON structure by using the Evaluate Regular Expression assertion. The extracted segments can be used as input to other assertions in the service policy that may require a subset of the JSON structure.

If a policy contains a Route via HTTP(S) assertion that returns a JSON output, the standard response message (as contained in the `${response.*}` context variables) will contain the JSON structure. This will be returned to the original requestor of the transaction, unless the response is being transformed.

---

**Tip:** You can create your own Message variables containing JSON by using the Set Context Variable assertion.

---

## Transforming Messages Between XML and JSON

There are two assertions that you can use to transform between XML and JSON:

- **Apply JSON Transformation:** This assertion transforms messages from JSON to XML. For basic messages, it can also transform from XML to JSON. For more information, see Apply JSON Transformation assertion in the *Layer 7 Policy Authoring User Manual*.

- **Apply XSL Transformation:** This assertion offers the greatest flexibility in transforming XML to JSON. For an example of an XSL stylesheet that transforms XML to JSON, see "Appendix I: Stylesheet for Transforming XML to JSON" on page 661. For more information, see Apply XSL Transformation assertion in the *Layer 7 Policy Authoring User Manual*.

---

**Tip:** You can detect whether an XML-to-JSON transformation is necessary by using a Compare Expression assertion to examine the contents of an incoming "Accept" HTTP header to determine whether the requestor expects the response to be formatted as JSON. If so, you can use either the Apply JSON Transformation or Apply XSL Transformation assertions to transform the XML response to JSON.

---

## Working With Dynamic Routing

The CA API Gateway has the ability to route a message to multiple back-end servers, using common failover strategies to route to a dynamic list of IP addresses (which are stored in a context variable).

During dynamic routing, feedback is received for all the routes that were attempted, including both successful and unsuccessful routes. This feedback is stored in context variables that are available to the rest of the policy execution.

In a policy, always use these assertions in the following order:

- Create Routing Strategy configures the routing strategies that will be used by the other assertions.
- Execute Routing Strategy sets the route destination to one of the strategies defined by the Create Routing Strategy assertion.
- Route via HTTP(S) routes the message to the selected destination URL. Alternatively, you can use Route via Raw TCP.
- Process Routing Strategy Result collects the feedback for the selected route and sends the results back to the Execute Routing Strategy assertion.

The following illustration shows how dynamic routing can be used in a policy.



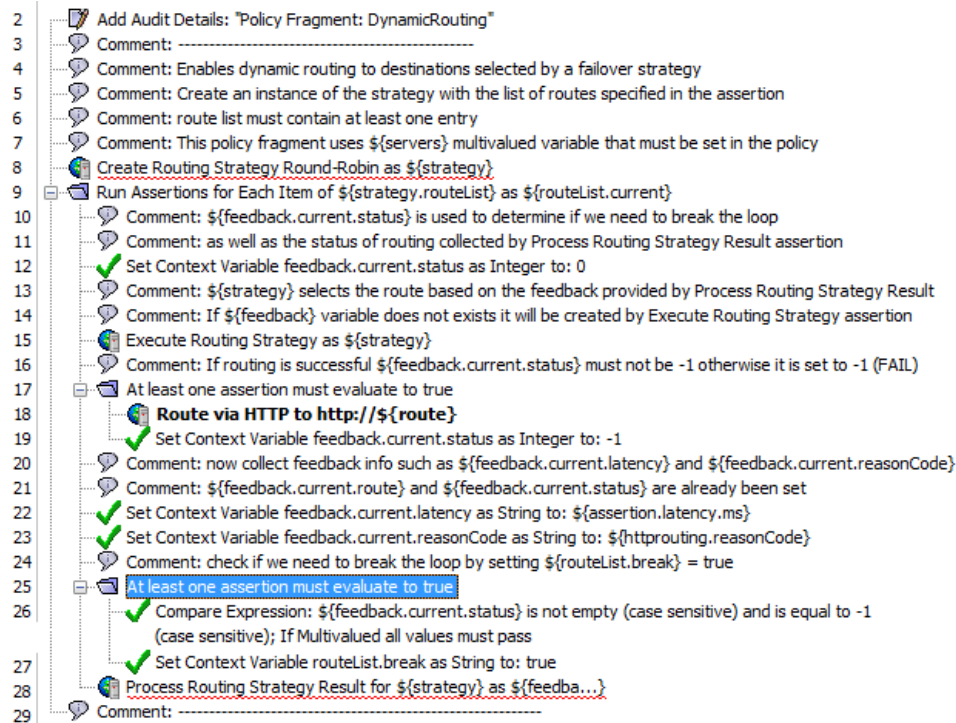


Figure 86: Sample policy for dynamic routing

The following are highlights of the workflow in Figure 86.

1. The Create Routing Strategy assertion is used to get input for executing the strategy (started by the Run Assertions for Each Item assertion, line 9). Route List and their properties are entered through the Create Routing Strategy Properties fields.

---

**IMPORTANT:** The Create Routing Strategy assertion must always precede Execute Routing Strategy and Process Routing Strategy Result assertions.

---

2. Once the Execute Routing Strategy policy is added (line 15), it enters a loop. The Execute Routing Strategy assertion exercises the `${strategy}` by automatically populating the Routing Strategy Prefix field. The method in which the route is selected depends on the type of strategy set in the Create Routing Strategy.
3. The Route Variable Name is then passed to the Route via HTTP(S) assertion (line 18). The URL field in the [Target] tab of the HTTP(S) Routing Properties is automatically populated with the Route Variable Name. The Execute Routing Strategy sets the `${feedbackList.current.route}` for the Process Routing Strategy to collect other feedback (for example, a **reasonCode**) on that particular current.route.

4. The Process Routing Strategy Result assertion (line 28) collects other feedback about the route, whether it has passed or failed.

From this step, there are two outcomes:

- If the HTTP(S) Routing fails, the current.route is replaced with next route on the list (selected by the Execute Routing Strategy), and the process loops back to the Execute Routing Strategy. The looping continues until the Execute Routing Strategy exhausts the routeList or the route succeeds.
- If the HTTP(S) Routing succeeds, the policy exits the loop with the working route `${<route>}` and its collected feedbacks from the Process Route Strategy.

## Working with CA SiteMinder

The Policy Manager provides the following functionality to allow you to authenticate and authorize against a CA SiteMinder Policy Server:

- [Manage SiteMinder Configurations](#) task
- Check Protected Resource Against SiteMinder assertion
- Authenticate Against SiteMinder assertion
- Authorize via SiteMinder assertion

This topic describes how to use this functionality to perform common tasks with CA SiteMinder.

---

**Note:** The SiteMinder feature requires the CA SiteMinder Agent SDK v12.51, which comes pre-installed in the hardware and virtual appliance versions of the CA API Gateway. If you are running the software Gateway, please contact CA Technical Support for assistance in installing the SDK.

---

### Creating a SiteMinder Configuration

You should create a SiteMinder configuration first before performing any other SiteMinder-related tasks.

➤ *To create a SiteMinder configuration:*

1. Access the [Manage SiteMinder Configuration](#) dialog.
2. Click **[Add]** to open the [SiteMinder Configuration Properties](#).
3. Click **[Register]** and complete the [SiteMinder Registration Properties](#).

4. When the registration properties are entered, complete the SiteMinder Configuration Properties by entering a **Configuration Name**.
5. Click **[Test]** to check whether your configuration is valid.

For more information, see "Managing SiteMinder Configurations" on page 220

## Basic User Authentication using SiteMinder Assertions

The steps below provide an overview on how to use the SiteMinder assertions to perform basic user authentications.

1. Ensure an end point has been created on the CA API Gateway.
2. Add the Check Protected Resource Against SiteMinder assertion to your policy.
  - Configure the assertion to use a valid SiteMinder configuration, agent name, protected resource, and action. Keep the default SiteMinder variable prefix ("siteminder").
2. Add the Require HTTP Basic Credentials assertion to the policy.
3. Add the Authenticate Against SiteMinder assertion to the policy. Use the default settings.
4. Add the Authorize via SiteMinder Assertion assertion to the policy, ensuring that it comes after the Authenticate Against SiteMinder assertion.
5. Complete your policy by adding other assertions as required.

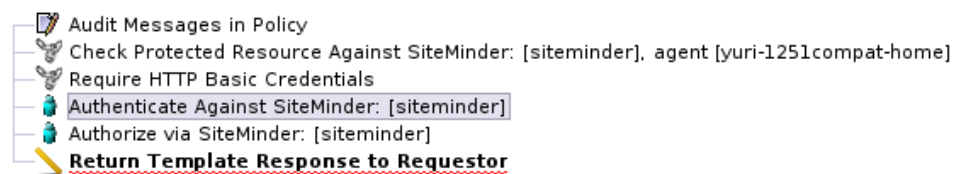


Figure 87: Basic user authentication using SiteMinder

## Basic User Authentication via HTTP Cookie using SiteMinder Assertions

The steps below provide an overview on how to use the SiteMinder assertions to perform basic user authentication using an HTTP cookie.

1. Ensure an end point has been created on the CA API Gateway.
2. Add the Check Protected Resource Against SiteMinder assertion to your policy.

- Configure the assertion to use a valid SiteMinder configuration, agent name, protected resource, and action. Keep the default SiteMinder variable prefix ("siteminder").
3. Add the At least one assertion must evaluate to true composite assertion to the policy. Into this folder add the following assertions:
    - Add the Require HTTP Cookie assertion and configure it as follows:  
Cookie name: **SMSESSION**  
Variable prefix: **cookie** (default)
    - Add the Require HTTP Basic Credentials assertion
  4. Add the Authenticate Against SiteMinder assertion to the policy.
    - Select the **Use SSO Token from Context Variable** check box and then enter the name of the cookie variable from the Require HTTP Cookie assertion (for example, "cookie.SMSESSION").
  5. Add the Authorize via SiteMinder Assertion assertion to the policy, ensuring that it comes after the Authenticate Against SiteMinder assertion.
    - Select the **Set SiteMinder Cookie** check box.
  6. Complete your policy by adding other assertions as required.

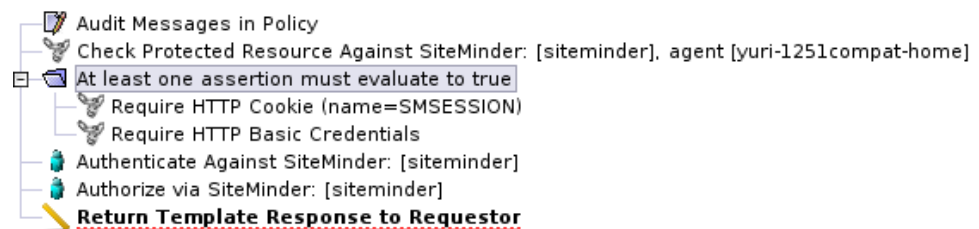


Figure 88: Basic authentication via HTTP cookie using SiteMinder

## Advanced SiteMinder Authorization with Status Check of Session

The SiteMinder assertions can be used in advanced SiteMinder authentication/authorization scenarios, such as collecting user credentials based on the information returned from the assertions, and responding to error conditions.

The following policy is an example of advanced SiteMinder authorization with status checking of the session.

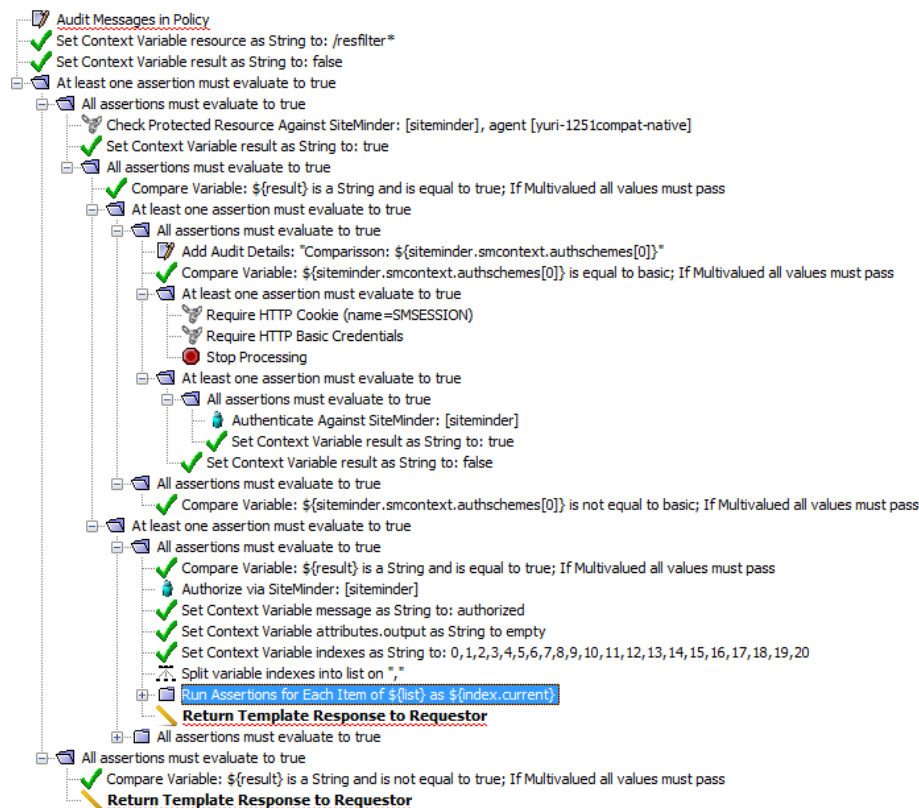


Figure 89: Advanced SiteMinder authorization policy example

## Troubleshooting SiteMinder

This section describes some of the error conditions you may encounter while using the SiteMinder assertions.

### Check Protected Resource Errors

When the Check Protected Resource Against SiteMinder assertion is configured to use a resource that is not protected by SiteMinder, the assertion will fail and the following [audit message](#) is logged:

```
WARNING 10102 SiteMinder Check Protected Resource Against SiteMinder assertion:
The resource <resource> is not protected!
```

### Unsupported Actions

An unsupported or invalid action entered in the Check Protected Resource Against SiteMinder assertion will not trigger a failure of this assertion. Instead, the Authorize via SiteMinder assertion will be declared falsified, with the error message "SM Sessions null is not authorized!" (see "Appendix E: Assertion Status Codes" on page 625). The following

[audit message](#) is also logged:

*"WARNING 10102 SiteMinder Authorize via SiteMinder assertion: SM Sessions null is not authorized!"*

## Authentication Failure

When the Authenticate Against SiteMinder assertion fails, the following audit message is logged:

```
WARNING 10102 SiteMinder Authenticate Against SiteMinder assertion: SiteMinder
Authenticate Against SiteMinder assertion: Unable to authenticate user using SSO
Token:<token sent>
```

## Authentication/Authorization Errors

When there is a SiteMinder authentication or authorization failure, consult the following context variables to help you troubleshoot:

- `${<prefix>.smcontext.attributes.SESS_DEF_REASON}` returns the reason code from the CA SiteMinder Policy Server
- `${<prefix>.smcontext.attributes.ATTR_STATUS_MESSAGE}` returns error of authentication or authorization

For more information about the above context variables, see "Context Variables for CA SiteMinder" on page 562.

For more information about the failure reason codes, see "Appendix J: SiteMinder Failure Reasons" on page 665.

## Managing SiteMinder Configurations

The Manage SiteMinder Configuration task is used to create, modify, and delete CA SiteMinder configurations.

The Gateway supports CA SiteMinder Policy Servers versions 12.5 and 12SP3.

➤ *To manage SiteMinder configurations:*

1. In the Policy Manager, select **[Tasks] > Manage SiteMinder Configurations** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage SiteMinder Configurations dialog appears.

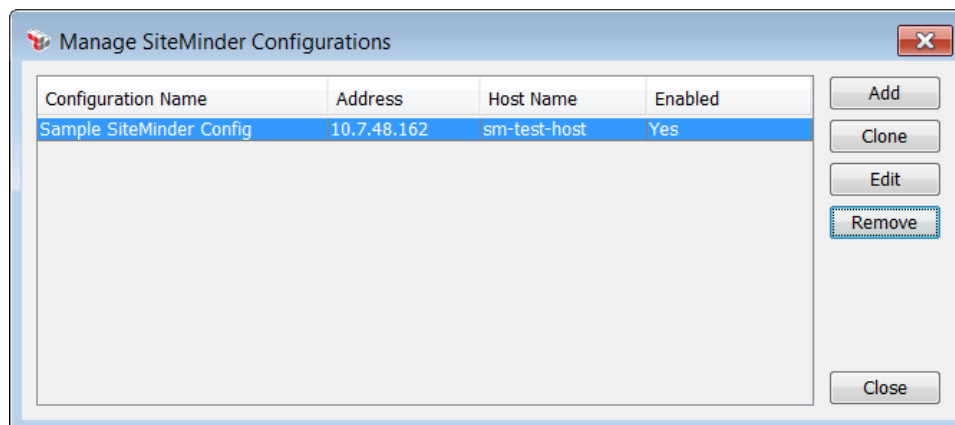


Figure 90: Manage SiteMinder Configurations dialog

2. The following table describes each column (these are set in the SiteMinder configuration [properties](#)):

Table 68: Manage SiteMinder Configuration columns

| Column                    | Description   |
|---------------------------|---|
| <b>Configuration Name</b> | Name of the SiteMinder configuration, as used in the Check Protected Resource Against SiteMinder assertion in the <i>Layer 7 Policy Authoring User Manual</i> . |
| <b>Address</b>            | SiteMinder client IP address.   |
| <b>Host Name</b>          | Name of the host registered with the CA SiteMinder Policy Server.   |
| <b>Enabled</b>            | Indicates whether the specified configuration is currently enabled or disabled.   |

3. Select a task to perform:

Table 69: Manage SiteMinder Configurations tasks

| To...   | Do this...  |
|---|---|
| <b>Add a new SiteMinder Configuration</b>                             | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>.</li> <li>2. Complete the "SiteMinder Configuration Properties" on page 222.</li> </ol>  |
| <b>Create a new SiteMinder Configuration based on an existing one</b> | <ol style="list-style-type: none"> <li>1. Select a SiteMinder configuration to copy.</li> <li>2. Click <b>[Clone]</b>. A new SiteMinder Configuration is created, populated with information from the original source. This new configuration has the default name "<b>Copy of &lt;original name&gt;</b>".</li> <li>3. Edit the <a href="#">SiteMinder Configuration Properties</a> as required.</li> </ol> |
| <b>Modify a SiteMinder Configuration</b>                              | <ol style="list-style-type: none"> <li>1. Select the SiteMinder configuration to modify.</li> <li>2. Click <b>[Edit]</b>.</li> </ol>  |

| To...                                    | Do this...  |
|--|---|
|  | 3. Edit the <a href="#">SiteMinder Configuration Properties</a> as required.  |
| <b>Remove a SiteMinder Configuration</b> | <ol style="list-style-type: none"> <li>1. Select the SiteMinder configuration to remove.</li> <li>2. Click <b>[Remove]</b>.</li> <li>3. Click <b>[OK]</b> to confirm the deletion.</li> </ol> |

4. Click **[Close]** when done.

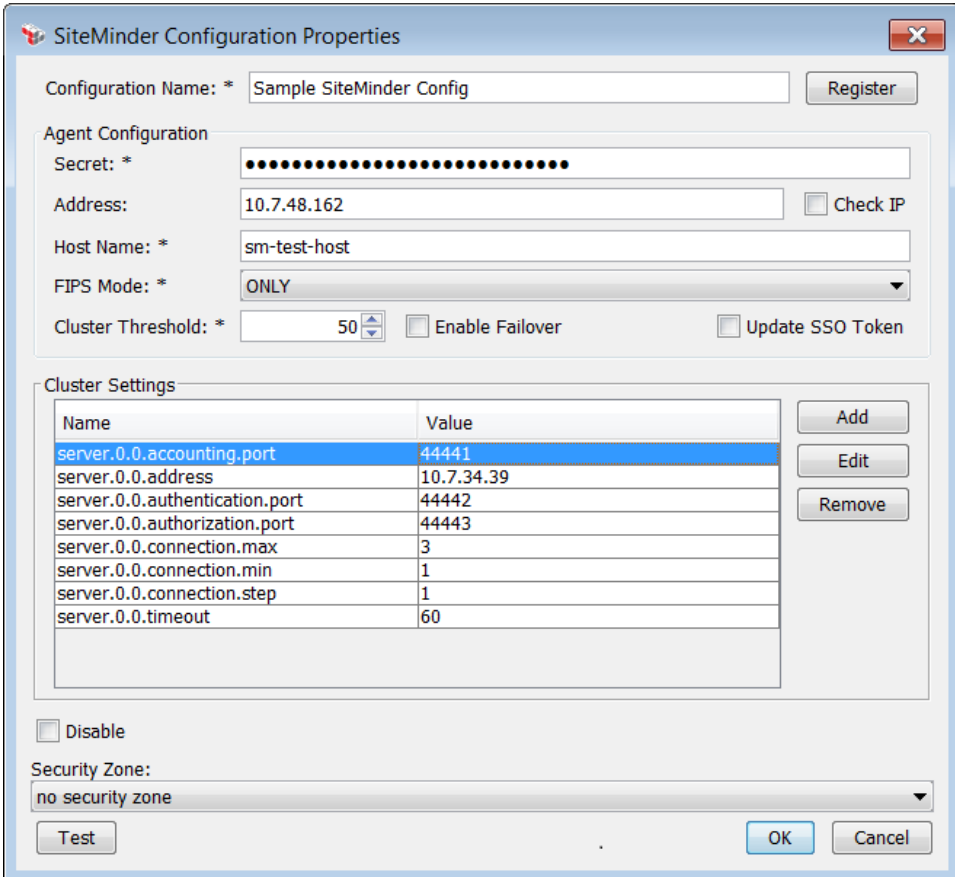
## SiteMinder Configuration Properties

When creating or editing a [SiteMinder configuration](#), the SiteMinder Configuration Properties dialog is displayed. This dialog is used to manage the SiteMinder Agent configuration settings, to enable the CA API Gateway to communicate with a CA SiteMinder Policy Server.

➤ *To access the properties for a SiteMinder configuration:*

1. Run the [Manage SiteMinder Configurations](#) task.
2. Add or edit a SiteMinder configuration. The SiteMinder Configuration Properties appear (Figure 91).





The dialog box is titled "SiteMinder Configuration Properties". It contains the following fields and controls:

- Configuration Name:** \* Sample SiteMinder Config (with a **Register** button)
- Agent Configuration** section:
  - Secret:** \* (masked with dots)
  - Address:** 10.7.48.162 (with a **Check IP** checkbox)
  - Host Name:** \* sm-test-host
  - FIPS Mode:** \* ONLY (dropdown menu)
  - Cluster Threshold:** \* 50 (spin box) (with **Enable Failover** and **Update SSO Token** checkboxes)
- Cluster Settings** section:
 

| Name                           | Value      |
|--------------------------------|------------|
| server.0.0.accounting.port     | 44441      |
| server.0.0.address             | 10.7.34.39 |
| server.0.0.authentication.port | 44442      |
| server.0.0.authorization.port  | 44443      |
| server.0.0.connection.max      | 3          |
| server.0.0.connection.min      | 1          |
| server.0.0.connection.step     | 1          |
| server.0.0.timeout             | 60         |

 (with **Add**, **Edit**, and **Remove** buttons)
- Disable** checkbox
- Security Zone:** no security zone (dropdown menu)
- Test**, **OK**, and **Cancel** buttons

Figure 91: SiteMinder Configuration Properties dialog

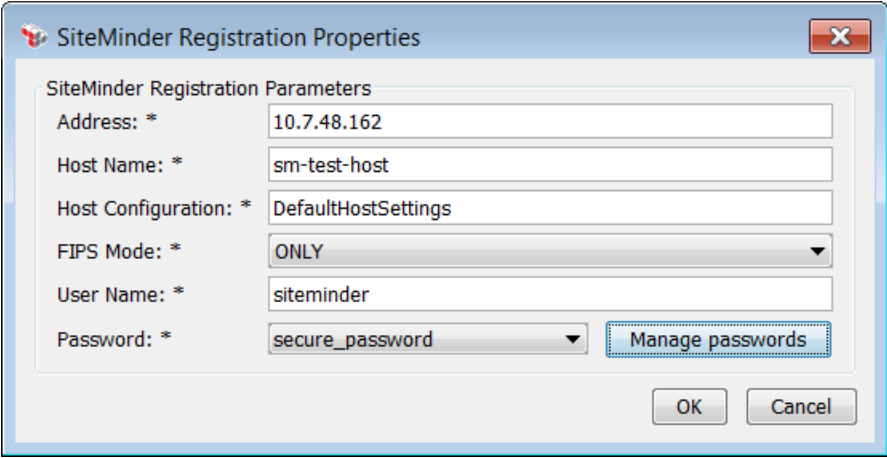
- When *adding* a new SiteMinder configuration, it is recommended that you click **[Register]** and complete the parameters in the SiteMinder Registration Properties (Figure 92).

---

**Tip:** Registration populates most of the Agent Configuration fields for you. If you do not use the Register button, you can manually enter the Agent Configuration, including the shared secret.

---

When *editing* an existing SiteMinder configuration, using **[Register]** will re-register the SiteMinder Agent with the Policy Server. This may invalidate previous registrations, so use this option carefully. A safe alternative is to manually edit the fields in the SiteMinder Configuration Properties.



The image shows a Windows-style dialog box titled "SiteMinder Registration Properties". It contains several input fields and a button. The fields are: "Address: \*" with the value "10.7.48.162", "Host Name: \*" with the value "sm-test-host", "Host Configuration: \*" with the value "DefaultHostSettings", "FIPS Mode: \*" with a dropdown menu showing "ONLY", "User Name: \*" with the value "siteminder", and "Password: \*" with a dropdown menu showing "secure\_password". There is a "Manage passwords" button next to the password field. At the bottom right are "OK" and "Cancel" buttons.

Figure 92: SiteMinder Registration Properties dialog

Complete the fields in the dialog box as shown below. All fields are required.

Table 70: SiteMinder Registration settings

| Setting                   | Description   |
|---------------------------|---|
| <b>Address</b>            | Enter the address of the SiteMinder Policy Service, either as an IP address or hostname.  |
| <b>Host Name</b>          | Enter the name of the registered host. This can be the Gateway name or any other symbolic name used to distinguish the host.  |
| <b>Host Configuration</b> | Enter the CA SiteMinder Policy Server host configuration used by the agent.   |
| <b>FIPS Mode</b>          | Choose the FIPS mode supported by the CA SiteMinder Policy Server. The available values are:<br><br><b>COMPAT</b> (default)<br><b>MIGRATE</b><br><b>ONLY</b>  |
| <b>User Name</b>          | Enter the user name of the SiteMinder administrator.  |
| <b>Password</b>           | Choose the stored password to use from the drop-down list. <b>Note:</b> Only stored passwords may be specified here—you cannot type in a password. To define a stored password, click <b>[Manage Passwords]</b> . For more information, see "Managing Stored Passwords" on page 42. |

- Click **[OK]** to register the trusted host once all the required fields are filled. Upon successful registration, the agent configuration and server settings are populated in the SiteMinder Configuration Properties dialog. **Note:** If registration is unsuccessful, an error message will be displayed.
- Enter or modify the remaining SiteMinder properties as follows:

Table 71: SiteMinder Configuration settings

| Setting                    | Description  |
|----------------------------|--|
| <b>Configuration Name</b>  | Specify the SiteMinder configuration name. This name will be used in the Check Protected Resource Against SiteMinder assertion. This field is required.  |
| <b>Register</b>            | Click this button to enter or update the SiteMinder registration parameters (see Figure 92).   |
| <i>Agent Configuration</i> |  |
| <b>Secret</b>              | <p>This is the SiteMinder shared secret used by the agent to establish communication with the Policy Server. This secret can be generated by clicking <b>[Register]</b> or you can paste it from another source. This field is required.</p> <p><b>Note:</b> The shared secret cannot be copied nor will it be imported during a policy import or exported during a policy export/import.</p>  |
| <b>Address</b>             | <p>Enter the IP address of the SiteMinder agent. This field is required if the <b>Check IP</b> check box is selected, otherwise it may be left blank.</p> <p>This address is used only when the client application does not supply the IP address.</p>   |
| <b>Check IP</b>            | <p>Select this check box to have the CA SiteMinder Policy Server compare the client IP against the address stored in the SiteMinder SSO Token. If they do not match, an error is recorded and the assertion(s) will be considered "falsified".</p> <p><b>Note:</b> The CA SiteMinder Policy Server may be configured to restrict certain IP addresses. This will be enforced if IP Check is enabled.</p> <p>Clear this check box to not check the client IP address against the SSO Token. Requests from a different IP address (but with a valid SSO Token) will result in successful authentication/authorization.</p> |
| <b>Host Name</b>           | Enter the name of the host registered with the CA SiteMinder Policy Server (for example, the name of the CA API Gateway). This field is required.  |
| <b>FIPS Mode</b>           | <p>Choose the FIPS mode supported by the CA SiteMinder Policy Server. The available values are:</p> <p><b>COMPAT</b> (default)<br/> <b>MIGRATE</b><br/> <b>ONLY</b></p> <p><b>Tip:</b> If the Policy Server does not support FIPS mode (for example, CA SiteMinder Policy Server version 6), choose <b>COMPAT</b>.</p> <p>This field is required</p>   |
| <b>Cluster Threshold</b>   | Specify the percentage of servers within a cluster that must be available for Policy Server requests. When the number of available servers in a cluster falls below this percentage, failover to the next  |

| Setting                 | Description   |
|-------------------------|---|
|                         | <p>cluster occurs. This field is required.</p> <p><i>Example:</i> If the failover percentage is "60" and a cluster has five servers, failover occurs when the number of available servers in the cluster falls below three.</p>   |
| <b>EnableFailover</b>   | <p>Select this check box to enable failover. In this mode, SiteMinder continually uses one server until it becomes unavailable, at which time it switches to another server.</p> <p>Clear this check box to enable round-robin. In this mode, SiteMinder dynamically distributes requests across all the servers based on the performance capabilities of each server.</p> <p><b>Note:</b> This setting is meaningful only if the Policy Server has more than one node.</p>   |
| <b>Update SSO Token</b> | <p>Select this check box to update the SSO Token after successful authentication/authorization (provided that the "Use SSO Token from Context Variable" option was selected in the assertions).</p> <p>Clear this check box to not update the SSO Token after authentication/authorization.</p>   |
| <b>Cluster Settings</b> | <p>In this section, you define the additional settings required in order to connect a client application to the Policy Server. You will need to define at least one set of properties.</p> <p><b>Note:</b> All settings begin with "server.x.y.&lt;setting&gt;" where "x" represents the cluster sequence (as there can be more than one cluster) and "y" represents the server sequence in the cluster.</p> <p>The following settings can be defined:</p> <ul style="list-style-type: none"> <li>• <b>accounting.port:</b> Server accounting port</li> <li>• <b>address:</b> Server IP address; required</li> <li>• <b>authentication.port:</b> Server authentication port</li> <li>• <b>authorization.port:</b> Server authorization port (<b>Tip:</b> Ports <b>44441 - 44443</b> are accepted, even when the actual authorization port number is 44443; required)</li> <li>• <b>connection.max:</b> Maximum number of connections</li> <li>• <b>connection.min:</b> Number of initial connections</li> <li>• <b>connection.step:</b> Number of connections to allocate when out of connections</li> <li>• <b>timeout:</b> Connection timeout (in seconds)</li> </ul> <p><b>To add a cluster setting:</b></p> <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>.</li> <li>2. Enter the Name and Value of the setting.</li> <li>3. Click <b>[OK]</b>.</li> </ol> <p><b>To modify a cluster setting:</b></p> |

| Setting              | Description   |
|----------------------|---|
|                      | <ol style="list-style-type: none"> <li>1. Select the setting to edit.</li> <li>2. Click <b>[Edit]</b>.</li> <li>3. Modify the <b>Name</b> or <b>Value</b> as necessary.</li> <li>4. Click <b>[OK]</b>.</li> </ol> <p><b>To remove a cluster setting:</b></p> <ol style="list-style-type: none"> <li>1. Select the setting.</li> <li>2. Click <b>[Remove]</b>.</li> <li>3. Click <b>[Remove]</b> to confirm.</li> </ol>  |
| <b>Disable</b>       | <p>Select this check box to disable the SiteMinder configuration. This will make the configuration unavailable for use, while preserving all settings.</p> <p>Clear this check box to re-enable the configuration.</p>  |
| <b>Security Zone</b> | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> |
| <b>Test</b>          | <p>Click this button to test the SiteMinder configuration. You will see a "Validation passed" message if the configuration is correct.</p>  |

6. Click **[OK]** when done.

## How to Establish Outbound Secure Conversation

The following are the steps to establish outbound secure conversation between a CA API Gateway and some STS (Security Token Service) or back-end service:

1. Check if there is a secure conversation session mapping to the authenticated user and the back-end service. Use the Look Up Outbound Secure Conversation Session Assertion in the *Layer 7 Policy Authoring User Manual* to do this.
2. Generate a new RST SOAP message to request a security token (either a Security Context Token or a SAML Token). Use the Build RST SOAP Request Assertion in the *Layer 7 Policy Authoring User Manual* to do this.

3. Apply the necessary decoration requirements to the RST SOAP message, such as adding WS-Addressing, adding UsernameToken, or configuring WS-Security decoration.
4. Send the RST Request to a back-end service or an STS using the Route via HTTP(S) Assertion.
5. Process the RSTR Response SOAP message to extract the security token (either a Security Context Token or a SAML Token). Use the Process RSTR Response Assertion in the *Layer 7 Policy Authoring User Manual* to do this.
6. Establish a secure connection and save (or cache) the secure conversation session by using the Establish Outbound Secure Conversation Assertion in the *Layer 7 Policy Authoring User Manual*.
7. If the session is no longer used, you may cancel the session using the Cancel Security Context Assertion in the *Layer 7 Policy Authoring User Manual*.

## How to Integrate the Gateway with WCF

The CA API Gateway can operate in WCF (Windows Communication Foundation) environments by configuring it for any of the following scenarios:

- The Gateway functions as a WCF Client
- The Gateway functions as a WCF Service
- The Gateway functions as a "pass through" for secure conversation sessions, interacting with the actual WCF Client and Service.

The following scenarios are just one example of how you can use the Policy Manager assertions to configure the Gateway for WCF.

### Scenario 1: Gateway as WCF Client

In this scenario, the Gateway acts as a WCF Client, which establishes a secure conversation with the WCF service.

The following is a high level overview of the flow of information under this scenario:

1. The Gateway sends an RST (Request Security Token) request to the STS (Security Token Service) to request a SAML Token, which will be used later to authenticate the Gateway in the back-end service.
2. The Gateway receives an RSTR (Request Security Token Response) response with a SAML Token from the STS.

3. The Gateway builds an RST request with the SAML Token and sends the request to the back-end service to request a Security Context Token (SCT).
4. The Gateway receives an RSTR response with an SCT from the back-end service and establishes an outbound secure conversation.
5. The Gateway sends a service request protected by the shared secret to the back-end service.
6. The Gateway receives a service response request from the back-end service.
7. The Gateway undecorates the response to get an undecorated response message.

## **Scenario 2: Gateway as WCF Service**

In this scenario, the Gateway acts as a WCF Service, which establishes a secure conversation for a WCF client.

The following is a high level overview of the flow of information under this scenario:

1. The Gateway receives an RST request with a SAML Token from the client, which is attempting to establish a secure conversation with the Gateway.
2. The Gateway sends the client an RSTR response with an SCT and server entropy.
3. The Gateway receives a service request from the client.
4. The Gateway undecorates the request message by using the shared secret and processes the service request.
5. The Gateway sends the client a service response protected by the shared secret.

## **Scenario 3: Gateway as a "Secure Conversation pass-through"**

In this scenario, the Gateway is positioned in between the client and the back-end service. The secure conversation is established for the Gateway and the back-end service, but the session is also shared by the client and the Gateway.

The following is a high level overview of the flow of information under this scenario:

1. The Gateway receives an RST request from the client to establish a secure conversation with the back-end service.
2. The Gateway forwards the request to the back-end service.
3. The Gateway receives an RSTR response with an SCT from the back-end service.

4. The Gateway establishes an outbound secure conversation session by using the SCT.
5. The Gateway forwards the RSTR response (without any mediation) to the client.
6. The Gateway receives a service request (i.e., business request) from the client to request an actual service.
7. The Gateway mediates the service request, redecorates the request, and then sends it to the back-end service.
8. The Gateway receives a service response from the back-end service.
  - a. If mediating the response is not required, then the Gateway forwards the response to the client.
  - b. If mediating the response is required, then the Gateway undecorates the response message, modifies the response message, redecorates the response message, and then sends it back to the client.

## How to Configure Listeners for the Enterprise Service Manager

By default, the Gateway listens on the following ports for Enterprise Service Manager traffic:

- **8443**: for configuring a cluster in the Enterprise Tree
- **8765**: for configuring remote management

If these default ports are acceptable in your environment, then no further configuration is required beyond reviewing the settings under *Configuring the Gateway for Remote Access* in the *Layer 7 Installation and Maintenance Manual*.

If you wish to use interfaces and ports other than the defaults, follow the appropriate steps below.

---

**Tip:** For more information about the various ports used by the Enterprise Service Manager, please see *Ports Used by the ESM* in the Enterprise Service Manager documentation.

---

➤ *To configure the listen port for configuring a cluster in the Enterprise Tree:*

1. Run the [Manage Listen Ports](#) task, and click **[Interfaces]** to access the **Manage Interfaces** dialog.



2. *Perform this step only if your listen port will be listening specific IP addresses, otherwise skip if it will be listening to all addresses.*

Click **[Create Interface]** and complete the following:

- **Interface Name:** Can be any combination of letters, numbers, or underscores. Do not use spaces.  
Make a note of this name, as it will be used later in this procedure.
- **Address Pattern:** Enter the address pattern for the interface. For more details, see "Managing Interfaces" on page 76. Make note of the address pattern as it will be used later in the procedure.

3. Return to the **Manage Listen Ports** dialog and create a new listen port with the following settings:

- **Name:** Enter the ESM port name.
- **Protocol:** Select **HTTPS**.
- **Port:** Enter any number between 1025 and 65535. Make note of the port number, as it will be used later in the procedure. The default is **8443**.
- **Interface:** Select the interface created in step 2 or accept the default (**All**).

On the [SSL/TLS Settings] tab:

- **Client Authentication:** Select either **Optional** or **Required**.

4. Return to the [Basic Settings] tab and, under Enabled Features, select the **Enterprise Manager access** check box and click **[OK]**.

5. Add the following [cluster properties](#):

- *admin.esmInterfaceTag:* If you created a new interface in step 2, enter it here; otherwise, ignore this cluster property.
- *admin.esmPort:* Use the port number entered in step 3.

For more information see "Managing Cluster-Wide Properties" on page 40.

➤ *To configure the listen port for remote management:*

---

**Note:** This procedure requires access to the Gateway configuration interface. For more information, see *Accessing the Gateway Configuration Interface in the Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

---

1. On the Gateway main menu, select option **5** ("Display Remote Management configuration menu"), then complete the submenu options as follows:

- **(1) Listener IP Address:** Enter the IP address of the Internal Management LAN or enter \* (asterisk) to listen to all IP addresses.
- **(2) Listener Port:** Enter any unused port number between 1025 and 65535. The default is **8765**.
- **(3) Remote node management enabled:** Enter **yes**.
- **(4) Trust certificate:** Enter either the full qualified domain name of the ESM, or enter the thumbprint of the SSL certificate from the ESM.

For more information on each submenu option, see *Configuring the Gateway for Remote Access* in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

2. Restart the Gateway on each node.

For more information, see the topic *Configuring the Gateway Application* (option 7 - Manage CA API Gateway Status) in the *Layer 7 Installation and Maintenance Manual*.

## How to Use the Gateway as an HTTP Proxy

The following procedure describes how to configure the CA API Gateway to behave as an HTTP proxy.

➤ *To configure Gateway as an HTTP proxy:*

1. Publish a new XML service by completing the "Publish Web API Wizard" on page 346. Be sure to enter the following in Step 1 of the wizard:
  - **Target URL:** Enter "`http://<yourHostName>${request.http.uri}${request.url.query}`" (without the quotes); for example:  
`http://www.acmecorp.com${request.http.uri}${request.url.query}`
  - **Gateway URL:** Enter "\*" (asterisk, without the quotes)
2. Open the properties of the newly published service. For more information, see "Service Properties" on page 357.
  - In the [\[HTTP/FTP\]](#) tab select the **HEAD** check box.
3. In your policy, add the Add Audit Detail assertion with these settings:
  - **Message:** Enter a message that includes the context variable `${request.url}`.
  - **Level:** Select **WARNING** from the drop-down list.

This assertion will show the messages being processed successfully and will help you troubleshoot any issues.
4. Locate the HOSTS file on the client machine and add a line for:

<Gateway\_IP> <hostname>

Where:

- <Gateway\_IP> is the IP address of the Gateway
- <hostname> is the site to be browsed (i.e., "www.acmecorp.com")

---

**IMPORTANT:** Only edit the HOSTS file on the client (web browsing) machine, not on the Gateway machine.

---

5. Using your web browser, you can request the service using either the IP address of the Gateway or the hostname of the site to be browsed. Be sure to include the port number to properly process the requests—for example:

*http://192.168.1.5:8080* (where '192.168.1.5' represents the IP of the Gateway)

*http://www.acmecorp.com:8080* (where 'acmecorp' is the site mapped in step 4)

## Troubleshooting Mode

The Microsoft Windows desktop client version of the Policy Manager contains two modes:

- A normal graphical mode for day-to-day use, and
- A Troubleshooting Mode used by Network Administrators to gather additional information about system errors.

---

**Note:** The Linux version of the Policy Manager does not include a separate Troubleshooting Mode. However, log information is available when the "Manager.sh" file is run.

---

The Policy Manager user interface automatically opens when you initiate Troubleshooting Mode. You must log into the Gateway to troubleshoot in order to populate the command window. If the Policy Manager was already open, then another instance of the program will launch when you initiate Troubleshooting Mode. The new instance is tied to the command window and will automatically close when the MS-DOS window is closed.

➤ *To access the Troubleshooting Mode:*

1. Click **[Start] > All Programs > Layer 7 Policy Manager > Policy Manager in Troubleshooting Mode**.
2. A command window appears, the Policy Manager GUI launches, and the Login dialog appears.

- Enter your **User Name** and **Password**.
- Select the target Gateway from the **Gateway URL** drop-down list and click **[OK]**. A pop-up status message appears and then automatically disappears when the Gateway connection is established.

The command window may become minimized after logging in. If so, select it to restore it.

3. The command window is populated with Gateway-specific diagnostic information. If you require troubleshooting assistance, copy and paste the information into an email and [send](#) it to CA Technologies.
4. Click the **[X]** in the top right corner to close the command window. The instance of the Policy Manager GUI that was launched by the Troubleshooting Mode will automatically close when you close the command window.

## Troubleshooting with the Browser Client

To view troubleshooting information in the browser client version of the Policy Manager, you need to display the Java console:

- For Windows browsers, right-click the Java icon in the system tray and select **Open <version> Console**.
- For non-Windows browsers, navigate to `$JAVA_HOME/jre/bin` and then run `javacpl`.

## Wildcard Matching of Hostnames

The Gateway supports wildcard matching of hostnames with HTTPS as defined in [RFC 2818](#) (HTTP Over TLS). Wildcards can be of the form:

```
*.domain.com
*.sub.domain.com
*.sub2.sub1.domain.com
```

Where the '\*' character matches a domain component or part of the domain component, but not a subdomain.

---

**Note:** Wildcard matching is disabled by default. To enable it, set the [io.httpsHostAllowWildcard](#) cluster property to "true".

---

Examples:

**\*.domain.com** will match **host.domain.com** because '\*' can represent *host*  
**h\*.domain.com** will match **host.domain.com** because '\*' can represent *ost*

**\*t.domain.com** will match **host.domain.com** because '\*' can represent *hos*

**host.\*.domain.com** will match **host.sub.domain.com** because '\*' can represent *sub*

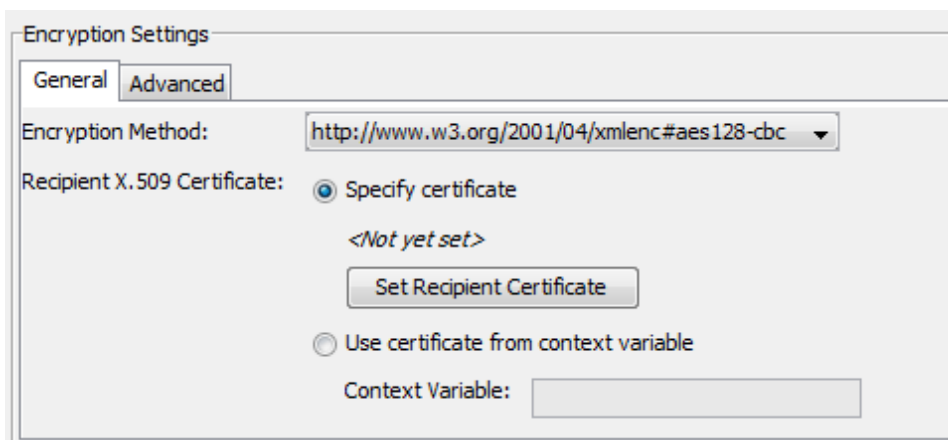
**\*.domain.com** will not match **host.sub.domain.com** because '\*' cannot represent *host.sub*

For LDAPS, POP3S, IMAPS, and SMTPS, the wildcard can only match the hostname, not any other component of the name, so for LDAPS:

**host.\*.domain.com** will not match **host.sub.domain.com** because '\*' cannot represent *sub*

## Configuring Encryption Settings

Certain assertions or wizards may require you to configure the encryption settings, where you can specify the encryption method to use, choose the recipient X.509 certificate, or specify other advanced settings (Figure 93 and Figure 94).



The figure shows a dialog box titled "Encryption Settings" with two tabs: "General" and "Advanced". The "General" tab is selected. It contains the following fields and controls:

- Encryption Method:** A dropdown menu showing "http://www.w3.org/2001/04/xmlenc#aes128-cbc".
- Recipient X.509 Certificate:** A section with two radio buttons:
  - ☒ **Specify certificate**: Below this is the text "<Not yet set>" and a button labeled "Set Recipient Certificate".
  - ☐ **Use certificate from context variable**: Below this is a text field labeled "Context Variable:".

Figure 93: Configuring encryption settings - General





The figure shows the same "Encryption Settings" dialog box, but with the "Advanced" tab selected. It contains the following fields and controls:

- ☐ **Add EncryptedData Type Attribute:** A dropdown menu showing "http://www.w3.org/2001/04/xmlenc#Element".
- ☐ **Add Recipient Attribute:** An empty text field.
- ☐ **Encrypt Only Element Contents**
- ☒ **Use OAEP**

Figure 94: Configuring encryption settings - Advanced

Configure the settings as follows:

Table 72: Configuring encryption settings

| Setting   | Description  |
|---|--|
| <b>[General] tab</b>  |  |
| <b>Encryption Method</b>  | Choose the encryption method to use from the drop-down list. If unsure, use the default method shown.  |
| <b>Recipient X.509 Certificate</b>  | <p>Indicate how the <b>Recipient X.509 Certificate</b> should be obtained:</p> <ul style="list-style-type: none"> <li>• <b>Specify certificate:</b> Select this option to manually configure a recipient X.509 certificate and then click <b>[Set Recipient Certificate]</b> to set the recipient X.509 certificate.<br/>For information on completing this wizard, see "Configure Recipient Certificate Wizard" on page 250.</li> <li>• <b>Use certificate from context variable:</b> Select this option to use an X.509 certificate stored in a context variable. Enter the name of the variable in the adjacent box.</li> </ul> |
| <b>[Advanced] tab</b>   |  |
| <b>Add EncryptedData Type Attribute</b><br> | <p>Select this check box to specify a Type attribute to be included in the <i>xenc:EncryptedData</i> element. Enter a valid URI for the Type attribute. You may specify a context variable. The default is <a href="http://www.w3.org/2001/04/xmlenc#Element">http://www.w3.org/2001/04/xmlenc#Element</a>.</p> <p><b>Note:</b> The assertion will fail if the value at runtime fails to resolve to a valid URI.</p>   |
| <b>Add Recipient Attribute</b><br>         | <p>Select this check box to enter a Recipient attribute that will be included in the <i>xenc:EncryptedKey</i> element. You may specify a context variable.</p> <p><b>Note:</b> If the value resolves to an empty value during runtime, this will result in an attribute with an empty value.</p>   |
| <b>Encrypt Only Element Contents</b><br><i>(available only from the (Non-SOAP) Encrypt XML Element assertion)</i>             | <p>Select this check box to encrypt only the contents of matching elements. The open and close tags, as well as any attributes, are left unencrypted.</p> <p>Clear this check box to encrypt matching elements, tags, and attributes.</p>  |
| <b>Use OAEP</b>   | <p>Select this check box to instruct the assertion to use the RSA-OAEP algorithm to sign the SAML token. For more information, see <a href="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p</a>.</p> <p>Clear this check box to use the RSA 1.5 algorithm, which was used in pre-v8.0 Gateways. This setting is the default for policies created in versions prior to version 8.0.</p>  |

## Chapter 3: Managing Certificates

The *Manage Certificates* task is used to manage both HTTPS and LDAPS certificates. In an [identity bridging](#) configuration, certificates are imported into the Federated Gateway B trust store. The trust store is the repository for four types of policies that may be required by the Federated Identity Provider in an identity bridging configuration:

- CA policies used for signing client policies
- SSL server policies
- CA policies used for signing SSL server policies
- Certificates used for signing SAML assertions.

The combination and purpose of certificates in the trust store are determined by the chosen credential source and optional configuration elements defined in "Workflow Using an X.509 Certificate" on page 437 or "Workflow Using SAML" on page 436. In accordance with the workflow instructions, certificates belonging to the Trusted Gateway A authentication domain will typically be imported into the Federated Gateway B authorization domain using the "Add Certificate Wizard" on page 240.

---

**Tip:** Wildcards can be used in hostnames during verification (for example, certificates with wildcard Subject DN). For more information, see "Wildcard Matching of Hostnames" on page 234.

---

### Certificate Expiration Notification

In addition to the Expiration Date shown on the Manage Certificates dialog, the Gateway can alert if you a trusted certificate has expired or will expire imminently. When the Gateway is started and every 12 hours (default setting) subsequently, it will check for impending certificate expiration:

- If a certificate has expired or will expire within the configured WARNING period (by default, 2 days), a WARNING audit event is logged.
- If a certificate will expire within the configured INFO period (by default, 7 days), an INFO audit event is logged.
- If a certificate will expire within the configured FINE period (by default, 30 days), a FINE audit event is logged.

To set the configured warning periods, see the 'trustedCert' properties under "Certificate Validation Cluster Properties" on page 574 in the [Gateway Cluster Properties](#). To view audit events, see "Gateway Audit Events" on page 415.

Expired certificates are highlighted in red on the Manage Certificates dialog.

---

**Note:** If your Gateway is a cluster, multiple audit events warning you of the same certificate expiration may be logged.

---

➤ To manage certificates:

- In the Policy Manager, select **[Tasks] > Manage Certificates** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Certificates dialog appears.

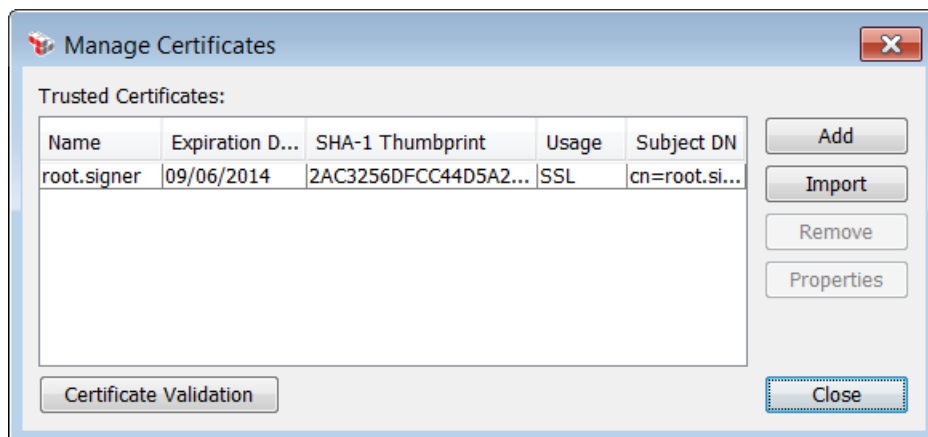


Figure 95: Manage Certificates dialog

Certificates that have expired are shown in red. If there are expired certificates currently scrolled out of view, the Manage Certificates dialog will warn you with the message: *Caution! Some certificate(s) have expired.*

---

**Tip:** It is possible to have multiple trusted certificates with the same DN, provided that the SHA-1 thumbprints differ. This allows you to trust a renewed version of a given certificate (that is, a certificate with the same DN, typically the same key, but a new certificate with a later expiry date) while still trusting the older version of the certificate up until its expiry date. This is useful when dealing with peers that do not yet have the latest version of the certificate.

---

Select a task to perform:

Table 73: Manage Certificates tasks

| To...                                      | See                                  |
|--|--------------------------------------|
| Add a new trusted certificate to the trust | "Add Certificate Wizard" on page 240 |



| To...  | See   |
|--|---|
| <b>store</b>                                     |   |
| <b>Import certificates from a keystore</b>       | "Importing Certificates" on page 248          |
| <b>Remove a certificate from the trust store</b> | "Deleting a Certificate" on page 247          |
| <b>View or edit certificate properties</b>       | "Editing a Certificate" on page 247           |
| <b>Delete a certificate from the trust store</b> | "Deleting a Certificate" on page 247          |
| <b>Export the certificate to a file</b>          | "Exporting a Certificate" on page 248         |
| <b>Configure how certificates are validated</b>  | "Managing Certificate Validation" on page 251 |
| <b>Configure custom private keys</b>             | "Managing Private Keys" on page 260           |

For information on the certificates required in each security domain in an identity bridging configuration, see "Identity Bridging Requirements" on page 433.

## Adding a New Certificate

➤ *To add a new certificate to the federated gateway trust store:*

1. In the Policy Manager, select **[Tasks] > Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Click **[Add]**. The [Add Certificate Wizard](#) appears.
3. Follow the steps in the wizard to complete it.
4. Repeat steps 2 and 3 to add more certificates or click **[Close]** to close the Manage Certificates dialog.

---

**Tip:** Individual client certificates can also be imported into the trust store for specific federated users from the Create Federated User dialog. For more information, see "Creating a Federated User" on page 446. When adding a new trust store certificate, follow the credential source-specific workflow instructions outlined in "Workflow Using an X.509 Certificate" on page 437 or "Workflow Using SAML" on page 436.

---

## Add Certificate Wizard

The *Add Certificate Wizard* assists you in [adding](#) a new certificate to the trust store. The wizard can accept certificates using any of the following methods:

- Retrieved from an HTTPS or LDAPS URL
- Imported from a file
- Pasted directly into the wizard

This wizard starts when you click **[Add]** on the [Manage Certificates](#) dialog.

For more information about wizards, see "[Wizards](#)" under "Interfaces" on page 13.

### Step 1: Enter Certificate Info

This step lets you specify the source of the new HTTPS or LDAPS certificate.

Figure 96: Add Certificate Wizard - Step 1

This step lets you specify the source of the new HTTPS or LDAPS certificate.

Specify how to obtain the certificate:

- **Retrieve via SSL Connection:** Select this option to get the certificate from an HTTPS or LDAPS URL.

- **Import from a File:** Select this option to get the certificate from a local file. Either enter the file path in the field, or use **[Browse]** to locate the file.
- **Import from Known Trusted Certificate:** Choose this option to use a known trusted certificate from the Gateway's trust store, then select the certificate from the drop-down list. For more information about trusted certificates, see "Chapter 3: Managing Certificates" on page 237.
- **Import from Private Key's Certificate Chain:** Choose this option to retrieve the certificate from the certificate chain of the private key, then select the private key from the drop-down list. For more information about private keys, see "Managing Private Keys" on page 260.
- **Copy and Paste:** Choose this option to copy and paste the entire certificate from the originating file into the code window. Specify the format of the certificate being pasted:
  - **Base64 PEM:** The certificate must be surrounded by the PEM markers ('-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----'), with formatting that conforms to RFC3548. This setting is the default.
  - **Base64:** The certificate can be imported regardless of formatting and does not require PEM markers.
- **Security Zone:** Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "**No security zone**". For more information about security zones, see [Understanding Security Zones](#) in the *Layer 7 Policy Manager User Manual*. **Note:** This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).

If you encounter an error moving to the next step of the wizard, verify that the certificate information entered is correct and then try again. If you require assistance, [contact](#) CA Technical Support.

## Step 2: View Certificate Details

This step appears if the Policy Manager was able to obtain the certificate successfully.

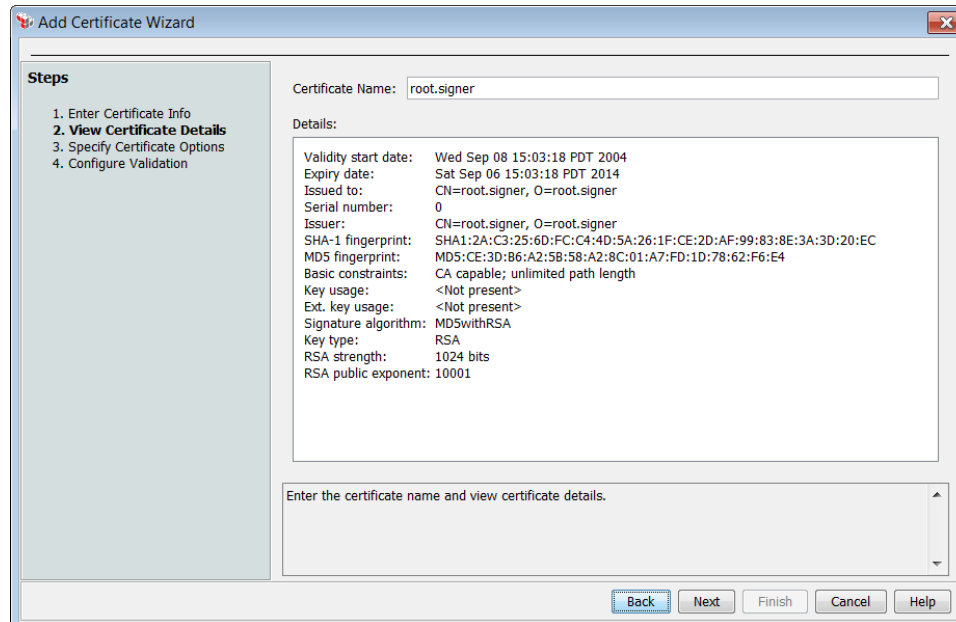


Figure 97: Add Certificate Wizard - Step 2

How to use this step:

- **Certificate Name:** Optionally enter a descriptive name for the certificate.
- **Details:** Examine the certificate details.

When creating a new [Federated Identity Provider user](#) who has a client certificate signed by the CA root certificate, the "Issued to" value of the certificate must match the user's "X509 Subject DN" value. If not, you are prompted whether to replace the original DN with the certificate DN.

### Step 3: Specify Certificate Options

This step allows you to select one or more certificate usage options.

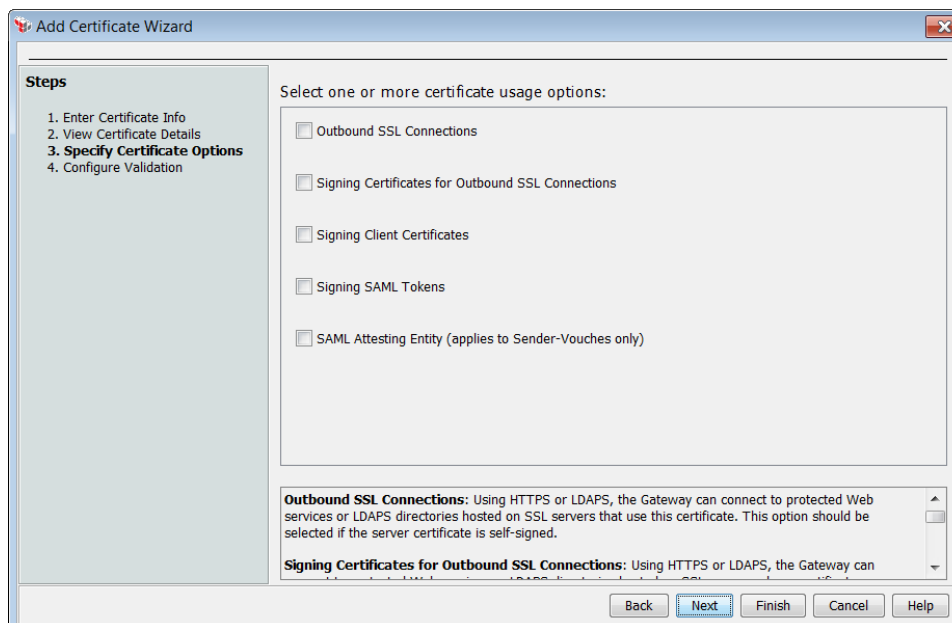


Figure 98: Add Certificate Wizard - Step 3

Specify how the certificate will be used:

#### **Outbound SSL Connections**

Select this option when the imported certificate belongs to an SSL server hosting the protected web services.

Be sure to select this option when importing an SSL certificate of an LDAP server into the trust store.

---

**IMPORTANT:** The Route via HTTP(S) assertion in the web service policy will not be able to connect using SSL if the host server uses a self-signed SSL certificate or an SSL certificate that is signed by an untrusted CA (certificate authority) unless the server's certificate is imported with this certificate usage option. See the *Signing Client Certificates* usage option below for more information

---

#### **Signing Certificates for Outbound SSL Connections**

Select this check box when the imported certificate is the signing certificate of a CA (certificate authority) that signs SSL policies for servers hosting protected web services.

Be sure to select this option when importing the CA certificate of an LDAP server into the trust store.

---

**IMPORTANT:** The Route via HTTP(S) assertion in the web service policy will not be able to connect using SSL if the host server uses a self-signed SSL certificate or an SSL certificate that is signed by an untrusted CA (certificate authority) unless the CA certificate that was used to sign the server's certificate is imported with this certificate usage option. See the *Signing Client Certificates* usage option below for more information.

---

#### **Signing Client Certificates**

Select this check box when the imported certificate is the signing certificate of a CA that signs client policies. The client policies can be used for a variety of purposes, including SSL client authentication and XML signing and encryption. For more information, see XML Security Assertions in the *Layer 7 Policy Authoring User Manual*. Certificates imported with this option enabled can be used in [Federated Identity Providers](#).

#### **Signing SAML Tokens**

Select this check box when the imported certificate is the signing certificate of a SAML issuing authority, such as in the [SAML credential source workflow](#). Certificates imported with this option enabled can be used in [Federated Identity Providers](#).

#### **SAML Attesting Entity**

Select this check box to configure a Federated Identity Provider to authorize identities that attest SAML tokens. The SAML Attesting Entity certificate usage option requires the presence of a Require SAML Token Profile assertion configured with the "Sender Vouches" subject confirmation method (as described in step 6 of the SAML Token Profile Wizard).

To learn how to configure the Securespan XML VPN Client to vouch for a requestor's identity using SAML, see *Configuring SAML Sender Vouches* in the Securespan XML VPN Client documentation.

---

**Tip:** You can complete the wizard without specifying a usage option in Step 3. However, at least one usage option must be specified at a later date before the certificate can be used. To specify an option later, see "Editing a Certificate" on page 247.

---

## **Step 4: Configure Validation**

This step allows you to specify validation options for the certificate.

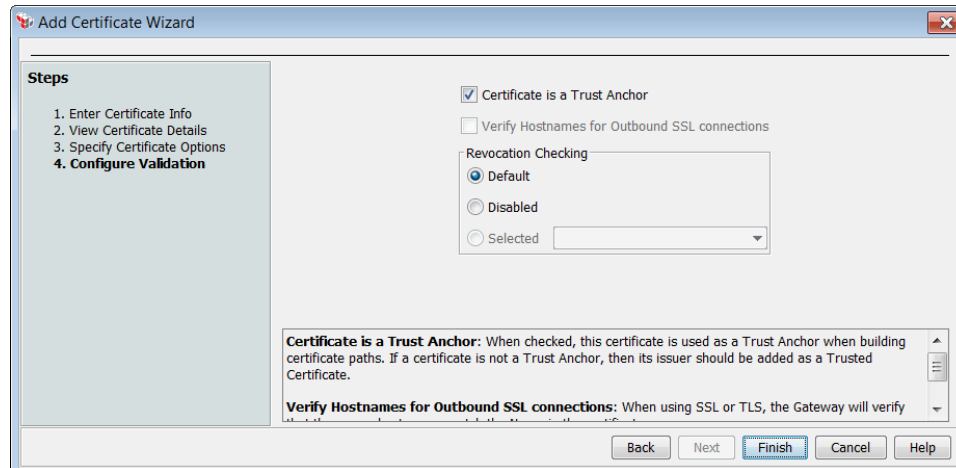


Figure 99: Add Certificate Wizard - Step 4

Specify the following validation options for the certificate:

#### **Certificate is a Trust Anchor**

Specify whether the certificate should be a trust anchor—a starting point from which trust is established. By default, all certificates added to the Gateway trust store are trust anchors.

For more information about trust anchors, see "Managing Certificate Validation" on page 251.

#### **Verify Hostnames for Outbound SSL Connections**

This setting lets you specify whether the Gateway should verify the hostname in a trusted certificate against the hostname in the URL of the request. If this option is enabled and the hostnames do not match, then the request is disallowed. If this option is disabled, then no attempt will be made to verify that the hostnames match.

This setting works in conjunction with the [io.httpsHostVerify](#) cluster property, which also specifies when a server hostname name is verified against a certificate. For more information about this setting, see "Verifying Hostnames for Outbound SSL Connections" on page 434.

#### **Revocation Checking**

Specify how this certificate should be checked for revocation:

- **Default:** Use the default revocation checking policy, as defined in the [Manage Certificate Validation](#) dialog.
- **Disabled:** Do not check this certificate for revocation.
- **Selected:** Use another revocation checking policy from the drop-down list.

For more information on revocation checking, see "Managing Certificate Validation" on page 251.

## Certificate Properties

A certificate's properties are initially set when you [add a new certificate](#) to the Gateway's trust store. You can then [view or edit](#) the properties later.

➤ To access the properties of a certificate:

1. In the Policy Manager, select **[Tasks] > Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Select the certificate you want to edit and then click **[Properties]**. The Certificate Properties dialog appears.

The screenshot shows the 'Certificate Properties' dialog box with the 'General' tab active. The fields are as follows:

- Certificate Name: root.signer
- Issued To: CN=root.signer, O=root.signer
- Issued By: CN=root.signer, O=root.signer
- Expired On: 09/06/2014
- Security Zone: no security zone

Buttons at the bottom: Export, Save, Cancel.

Figure 100: Certificate Properties

3. For information on each tab, see the corresponding steps in the "Add Certificate Wizard" on page 240.

Table 74: Certificate Properties tabs

| Tab     | Corresponds to...  |
|---------|--|
| General | <a href="#">Step 2: View Certificate Details</a> , <i>Certificate Name</i> field<br>The Security Zone is described in <a href="#">Step 1: Enter Certificate Info</a> . |
| Details | <a href="#">Step 2: View Certificate Details</a> , <i>Certificate Details</i> field  |



| Tab        | Corresponds to...                                   |
|------------|---|
| Options    | <a href="#">Step 3: Specify Certificate Options</a> |
| Validation | <a href="#">Step 4: Configure Validation</a>        |

4. If you need to export a certificate to a file, click [**Export**]. For more information, see "Exporting a Certificate" on page 248.
5. Click [**Save**] when done.

## Editing a Certificate

➤ To edit an existing [certificate](#) in the federated gateway trust store:

1. In the Policy Manager, select [**Tasks**] > **Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Select the certificate you want to edit and then click [**Properties**]. The [Certificate Properties](#) dialog appears.
3. Edit the certificate details as required. For more information, see "Certificate Properties" on page 246.
4. If you need to export the certificate to a file, click [**Export**]. For more information, see "Exporting a Certificate" on page 248.
5. Click [**Save**]. The modified certificate is updated in the trust store and Manage Certificates dialog.
6. Click [**Close**] to close the Manage Certificates dialog.

## Deleting a Certificate

➤ To delete an existing certificate from the federated gateway trust store:

1. In the Policy Manager, select [**Tasks**] > **Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Under **Trusted Certificates**, select the certificate want to delete, and then click [**Remove**].
3. Click [**Remove**] when prompted to confirm. The certificate is removed from the trust store and Manage Certificates dialog.
4. Click [**Close**] to close the Manage Certificates dialog.

## Exporting a Certificate

➤ To export a [certificate](#) from the federated gateway trust store:

1. In the Policy Manager, select **[Tasks] > Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Select the certificate to export and then click **[Properties]**. The [Certificate Properties](#) dialog appears.
3. Click **[Export]** and then specify a file name and location for the exported certificate.
4. Click **[Save]**. The certificate is exported.
5. Click **[Cancel]** to close the Certificate Properties dialog, then click **[Close]** to close the Manage Certificates dialog.

## Importing Certificates

You can import certificates from a PKCS#12 keystore into the internal trust store of the Gateway. Certificates can be imported as trust anchors and you can optionally import the entire certificate chain.

➤ To import certificates:

1. In the Policy Manager, select **[Tasks] > Manage Certificates** from the [Main Menu](#). The [Manage Certificates](#) dialog appears.
2. Click **[Import]**.
3. Navigate to the PKCS#12 keystore file (\*.p12 or \*.pfx) and then click **[Load]**.
4. Enter the keystore password when prompted and then click **[OK]**. The Import Certificates dialog appears, displaying all the certificates in the keystore.

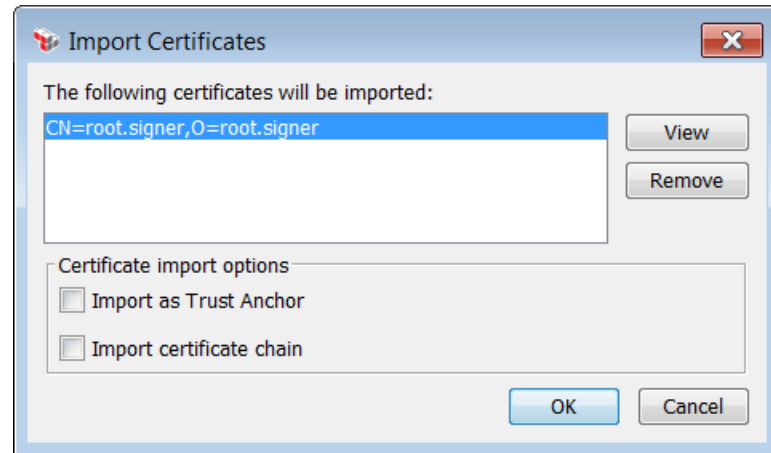


Figure 101: Import Certificates dialog

5. Review the certificates to be imported. Remove the ones that you do not wish to import.
  - To examine a certificate's details before importing, click **[View]** when only one certificate is selected.
  - To exclude a certificate from being imported, select it and then click **[Remove]**. You can select multiple certificates for removal by holding down the **[Shift]** or **[Ctrl]** keys. **Note:** The certificate is only removed from the import list—it is not removed from the keystore.
6. Choose the following import options as necessary:
  - **[Import as Trust Anchor]**: Select this check box to import the certificates as trust anchors—a starting point from which trust is established. For more information about trust anchors, see "Trust Anchors" under [Managing Certificate Validation](#).
  - **[Import certificate chain]**: Select this check box to import the full certificate chain (if any) along with the certificate. If both **[Import as Trust Anchor]** and **[Import certificate chain]** are selected, only the last entry in the chain (i.e., the highest level CA in the chain) is imported as the trust anchor. For more information about certificate chains, see "Private Key Properties" on page 271.
7. Click **[OK]** to import the certificates. Depending on the number of certificates selected and the speed of the network, it may take a moment for the import to complete.

If a certificate could not be imported for whatever reason (already exists, keystore is corrupt, etc.), this will be listed in an error message.

**Tip:** After importing a certificate, you should review its properties to ensure everything is in order. In particular, you may need to specify a certificate usage option. For more information, see the [Options] tab under "Editing a Certificate" on page 247.

## Configure Recipient Certificate Wizard

The *Configure Recipient Certificate* wizard is displayed when [Set Recipient Certificate] is selected in a dialog. This indicates that you wish to configure your own recipient certificate, rather than using a certificate stored in a context variable.

Figure 102: Configure Recipient Certificate wizard

1. Specify how to obtain the certificate:
  - **Retrieve via SSL Connection:** Choose this option if the certificate resides at a secure URL, either HTTPS or LDAPS. Enter the URL in the adjacent box.
  - **Import from a File:** Choose this option if the certificate resides in a text file. Enter the file location in the adjacent box.
  - **Import from Known Trusted Certificate:** Choose this option to use an existing trusted certificate. Select the certificate from the adjacent drop-down list.
  - **Import from Private Key's Certificate Chain:** Choose this option to import the details from the certificate chain for a specific private key. Choose the private key from the adjacent drop-down list.

- **Copy and Paste:** Choose this option to paste the certificate code from the clipboard into the code window. Indicate whether the certificate is in **Base64 PEM** or **Base64** format.
2. Click **[Next]** to view the certificate details.
  3. Examine the certificate details to ensure everything is in order. If you need to select another certificate, click **[Back]** to return or click **[Finish]** to accept the certificate and return to the assertion properties.

## Managing Certificate Validation

The Gateway will verify whether certificates used for authentication and/or authorization are valid; the Gateway can also perform revocation checking for certificates. To enable revocation checking, use the Manage Certificate Validation dialog to define one or more *revocation checking policies*. These policies describe the strategies employed by Gateway to determine the revocation status of a certificate:

- by checking Certificate Revocation List (CRL)
- using Online Certificate Status Protocol (OCSP)

In either case, the URL for the CRL data or OCSP responder can be extracted from the certificate's URL or it can be a predefined URL.

Every certificate in the trust store can have its own revocation checking policy, or more simply, you can designate a default revocation checking policy that will be used for all trusted certificates.

### Technical note

The Gateway will cache Certificate Revocation Lists for improved performance. It will try to fetch a fresh CRL one minute before the old one expires. The *pkix.\* cluster properties* can be used to configure the caching behavior. The cache is configured to use a stale CRL indefinitely while trying to get a new one. The initial attempt to load a CRL that has not yet been cached will block the caller. Subsequent attempts will use the cached value, even if it is stale. If a new CRL needs to be downloaded, one of the request threads will be used to do this, possibly increasing latency. The other threads will continue to use the old value without waiting. It is not possible to configure a local copy of the CRL or to manually repopulate the download cache.

The Manage Certificate Validation dialog also lets you select the validation option for the following types of certificate usage:

- **Identity Providers:** For validation of users' certificates during authentication using the identity provider
- **Routing:** For validation of certificates presented by a server during request routing (i.e., HTTPS, FTPS)
- **Other:** For validating any other certificates (for example, LDAPS or non-routing assertions)

There are three validation options available (see Table 75).

---

**Note:** If mutual certificate security is required between the Gateway and the CRL host, you need to ensure that the Gateway's SSL certificate is trusted by the CRL host.

---

## Trust Anchors

In order for the Gateway to validate certificate paths and check for revocation, it is necessary to have a starting point from which trust is established. This starting point is known as a *trust anchor*. The Gateway recognizes the following as trust anchors:

- Trusted certificates that have the [**Certificate is a trust anchor**] setting selected. This is located in the [Validation] tab of the certificate's properties. For more information on certificate properties, see "Editing a Certificate" on page 247. A certificate can also be flagged as a trust anchor when it is [imported](#).
- The CA certificate belonging to the Gateway.
- Certificates located in the JDK trust store.

➤ *To manage certificate validation:*

1. In the Policy Manager, select [**Tasks**] > **Manage Certificates** from the [Main Menu](#). The Manage Certificates dialog appears.
2. Click [**Certificate Validation**]. The Manage Certificate Validation dialog appears.

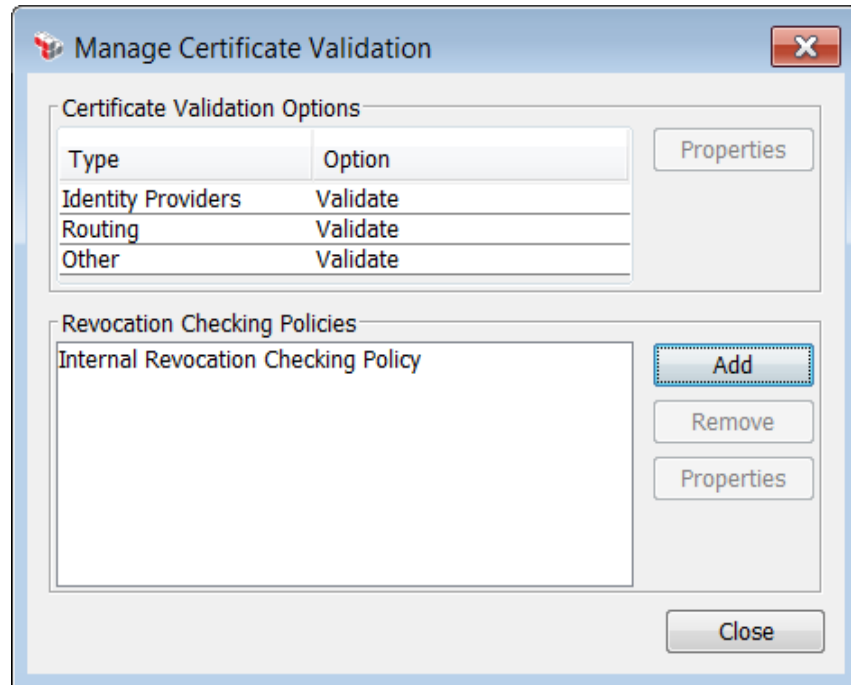


Figure 103: Manage Certificate Validation dialog

3. Configure the dialog as follows:

Table 75: Managing certificate validation

| Setting                               | Description   |
|---------------------------------------|---|
| <b>Certificate Validation Options</b> | <p>Define how the Gateway will perform validation for different types of certificate usage.</p> <ol style="list-style-type: none"> <li>1. Select a certificate type. <b>Note:</b> For Identity Providers, the option specified here will be used only if the Identity Provider properties is set to "Use Default" for certificate validation.</li> <li>2. Click <b>[Properties]</b>.</li> <li>3. Choose how that certificate type should be validated: <ul style="list-style-type: none"> <li>• <b>Validate:</b> Ensure that the certificate is valid and trusted.</li> <li>• <b>Validate Certificate Path:</b> Ensure that the certificate path is valid to a <a href="#">trust anchor</a>.</li> <li>• <b>Revocation Checking:</b> Validate the certificate path <i>and</i> perform revocation checking according to the revocation checking policies.</li> </ul> </li> </ol> <p><b>Tip:</b> The validation options can also be accessed or set using these <a href="#">cluster properties</a>: <code>pkix.validation.identityProvider</code>, <code>pkix.validation.routing</code>, <code>pkix.validation.other</code>.</p> |
| <b>Revocation Checking Policies</b>   | <p>Define the policies that can be attached to trusted certificates to describe how a certificate will be checked for revocation.</p>   |

| Setting | Description   |
|---------|---|
|         | <ul style="list-style-type: none"> <li>To add a new policy, click <b>[Add]</b> and then complete the Edit Revocation Checking Policy dialog. For more information, see "Editing a Revocation Checking Policy" on page 254.</li> <li>To remove a policy from the list, select it and then click <b>[Remove]</b>. You cannot delete a policy if any trusted certificate is using that policy.</li> <li>To view or edit a policy, select it and then click <b>[Properties]</b>. For more information, see "Editing a Revocation Checking Policy" on page 254.</li> </ul> |

- Click **[Close]** when done.

## Editing a Revocation Checking Policy

A revocation checking policy defines the strategies used by the Gateway to determine whether a certificate has been revoked. A policy can contain any combination of the following strategies:

- Check the certificate's revocation status by consulting a Certificate Revocation List (CRL) at a URL extracted from the certificate.
- Check the certificate's revocation status by consulting a CRL at a fixed URL.
- Check the certificate's revocation status by using Online Certificate Status Protocol (OCSP), using a URL extracted from the certificate.
- Check the certificate's revocation status by using OCSP against an OCSP responder at a fixed URL.

You can create any number of revocation checking policies using the [Manage Certificate Validation](#) dialog. The appropriate policy is then associated with a certificate via the [certificate's properties](#).

➤ *To add or edit a revocation checking policy:*

- Open the [Manage Certificate Validation](#) dialog.
- Do one of the following:
  - Click **[Add]** to create a new policy, or
  - Select an existing revocation checking policy and click **[Properties]** to modify it.

The Edit Revocation Checking Policy dialog appears.



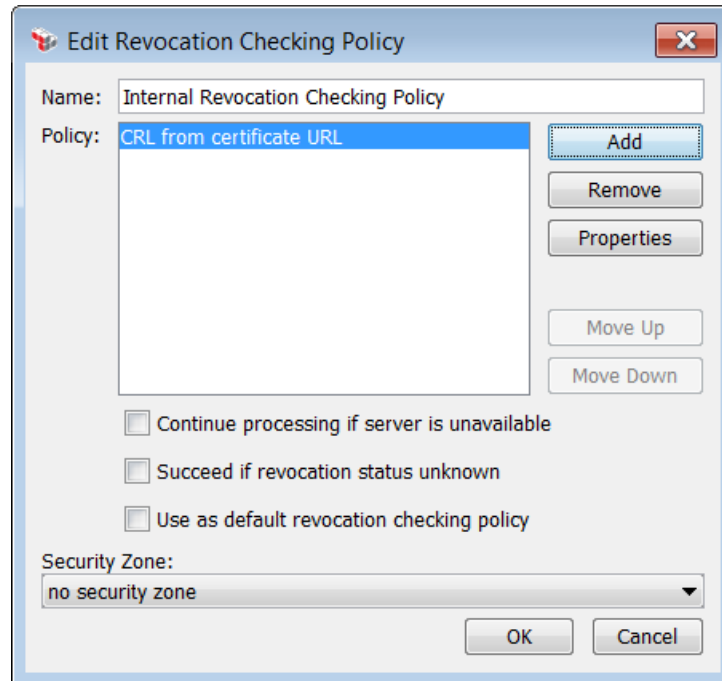


Figure 104: Edit Revocation Checking Policy dialog

3. Configure the dialog as follows:

Table 76: Revocation Checking Policy settings

| Setting       | Description   |
|---------------|---|
| <b>Name</b>   | <p>Enter a name that describes the revocation checking policy.</p> <p><b>Tip:</b> It is not necessary to include the word "default" in the name if you are creating a default policy. Setting the <b>Use as default revocation checking policy</b> check box will do this for you.</p>  |
| <b>Policy</b> | <p>Construct the policy using the following controls. At least one step must be created.</p> <ul style="list-style-type: none"> <li>To add a new step to the policy, click <b>[Add]</b> and then enter the details in the <a href="#">Edit Certificate Revocation Checking Properties</a> dialog.</li> <li>To remove a step from the list, select it and then click <b>[Remove]</b>.</li> <li>To edit a step, select it and then click <b>[Properties]</b>. Edit the details in the <a href="#">Edit Certificate Revocation Checking Properties</a> dialog.</li> <li>To change the order of the steps, select a step and click either <b>[Move Up]</b> or <b>[Move Down]</b>.</li> </ul> <p>The Gateway will go through each step in the order shown until an authoritative response is obtained.</p> |

| Setting   | Description   |
|---|---|
| <b>Continue processing if server is unavailable</b> | <p>This check box lets you control how the Gateway should respond if the CRL or OCSP responder is not available.</p> <ul style="list-style-type: none"> <li>Select this check box to check the cache for the CRL or OCSP response. <ul style="list-style-type: none"> <li>If a cached value is found, that value is used.</li> <li>If a cached value is not found, then the certificate is permitted only if the <b>Succeed if revocation status unknown</b> check box is selected, otherwise it is revoked.</li> </ul> </li> <li>Clear the check box to always revoke a certificate if the server is unavailable.</li> </ul>   |
| <b>Succeed if revocation status unknown</b>         | <p>This check box determines what will happen if all the steps in the policy are exhausted and the status is still undetermined:</p> <ul style="list-style-type: none"> <li>Select this check box to permit use of the certificate even if its revocation status could not be determined.</li> <li>Clear this check box to prevent use of the certificate if its revocation status could not be determined.</li> </ul> <p>A certificate's revocation status is undetermined if the CRL does not cover the certificate in question, or if the OCSP responder is not authoritative for the certificate. A certificate's revocation status is also undetermined if the policy is configured to use the URL in a certificate but the certificate has no URL, or if the URL does not match the configured pattern.</p> |
| <b>Use as default revocation checking policy</b>    | <p>This check box is used to designate a policy as the default revocation checking policy. This default policy is used for all certificates except for trusted certificates that specify a policy disable policy checking. Policies designated as the default will have "[Default]" appended to the policy name.</p> <ul style="list-style-type: none"> <li>Select this check box to make the current policy the default.</li> <li>Clear the check box to remove the default status from the current policy. <b>IMPORTANT:</b> If you do not designate another policy as the default, then all certificates that rely on the 'Default' policy will always fail the revocation check.</li> </ul>   |
| <b>Security Zone</b>                                | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>   |

4. Click **[OK]** when done.

## Certificate Revocation Checking Properties

The Certificate Revocation Checking Properties dialog is used to define the individual steps in the revocation checking policy. A [revocation checking policy](#) describes how the Gateway determines whether a certificate is revoked. These policies are maintained using the "Managing Certificate Validation" on page 251.

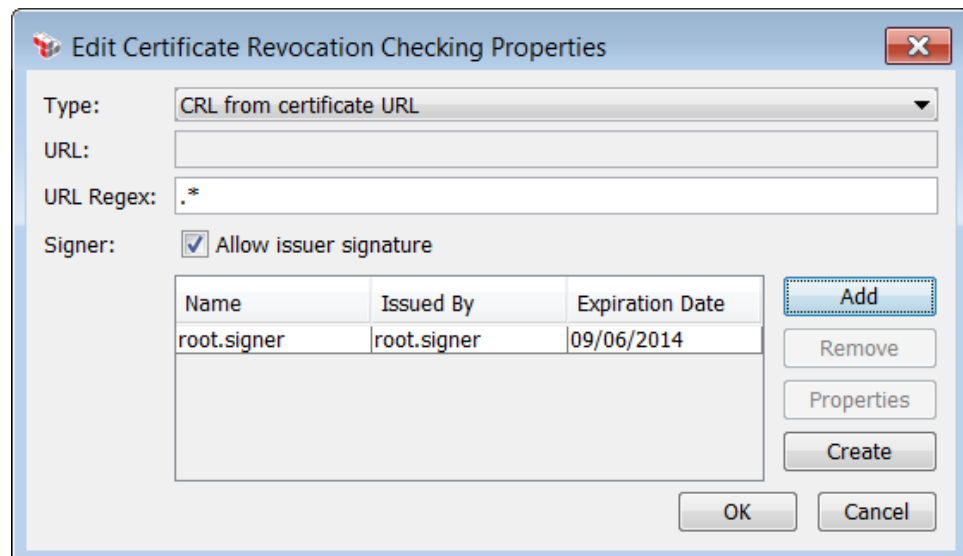
Define the following for each step:

- Select the revocation checking method to be used (either CRL or OCSP)
- Specify the URL or URI to use during checking (either a fixed URL or a variable URL parsed using a regex expression)
- Indicate which certificates are permitted to sign the CRL or OCSP response

➤ To edit the certificate revocation checking properties:

1. Open the [Edit Revocation Checking Policy](#) dialog.
2. Do one of the following:
  - Click **[Add]** to add a new step to the policy, or
  - Select an existing step and click **[Properties]** to modify it.

The Edit Certificate Revocation Checking Properties dialog appears.



| Name        | Issued By   | Expiration Date |
|-------------|-------------|-----------------|
| root.signer | root.signer | 09/06/2014      |

Figure 105: Edit Certificate Revocation Checking Properties dialog

3. Configure the properties as follows:

Table 77: Certificate Revocation Checking settings

| Setting          | Description  |
|------------------|--|
| <b>Type</b>      | <p>From the drop-down list, select how the certificate revocation status should be determined:</p> <ul style="list-style-type: none"> <li>• <b>CRL from certificate URL:</b> Use the Certificate Revocation List (CRL) located at a URL that is extracted from the certificate. Use the <b>URL Regex</b> field to restrict the URL to a particular type or host.</li> <li>• <b>CRL from URL:</b> Use the CRL located in the <b>URL</b> field.</li> <li>• <b>OCSP from certificate URL:</b> Use the Online Certificate Status Protocol (OCSP) responder located at a URL that is extracted from the certificate. Use the <b>URL Regex</b> field to restrict the URL (perhaps to a particular host).</li> <li>• <b>OCSP from URL:</b> Use the OCSP responder located at the <b>URL</b>.</li> </ul>   |
| <b>URL</b>       | <p>If the <b>CRL from URL</b> or <b>OCSP from URL</b> option was selected, enter the URL.</p> <p><b>Note:</b> If HTTP options have been defined for this URL, they will apply here. For more information, see "Managing HTTP Options" on page 188.</p>   |
| <b>URL Regex</b> | <p>If the <b>CRL from certificate URL</b> or <b>OCSP from certificate URL</b> option was selected, enter a regular expression that will restrict the URL.</p>  |
| <b>Signer</b>    | <p>In this section, define the certificates that are permitted to sign the CRL or OCSP response:</p> <ul style="list-style-type: none"> <li>• <b>Allow issuer signature:</b> Select this check box if you will be permitting the entity that issued the certificate. If you do not wish to give to give blanket permission this way, leave this check box unselected and manually add the permitted certificates to the table below.</li> </ul> <p>In the table, optionally define a list of permitted certificates. You can use this table regardless of the <b>Allow issuer signatur</b> check box setting. For example:</p> <ul style="list-style-type: none"> <li>• You elect not to automatically allow all issuer's signatures. Define the permitted certificates in the table.</li> <li>• You wish to permit certificates where the signing entity differs from the issuing entity. In this case, you will select both the <b>Allow issuer signature</b> check box <i>and</i> define a list of permitted certificates.</li> </ul> <p>Define the list of permitted certificates by using the following controls:</p> <ul style="list-style-type: none"> <li>• To add a certificate, click <b>[Add]</b> and then use the <a href="#">Search Trusted Certificates</a> dialog to locate the certificate. If you cannot find the certificate you want, use the <b>[Create]</b> option to add it.</li> <li>• To remove a certificate from the list, select it and then click <b>[Remove]</b>.</li> <li>• To view details about a certificate, select it and then click <b>[Properties]</b>. The certificate properties are displayed. For more information, see "Editing a Certificate" on page 247.</li> </ul> |

| Setting | Description  |
|---------|--|
|         | <ul style="list-style-type: none"> <li>To add a new certificate to the trust store, click <b>[Create]</b> and then complete the wizard. For more information, see "Add Certificate Wizard" on page 240.</li> </ul> |

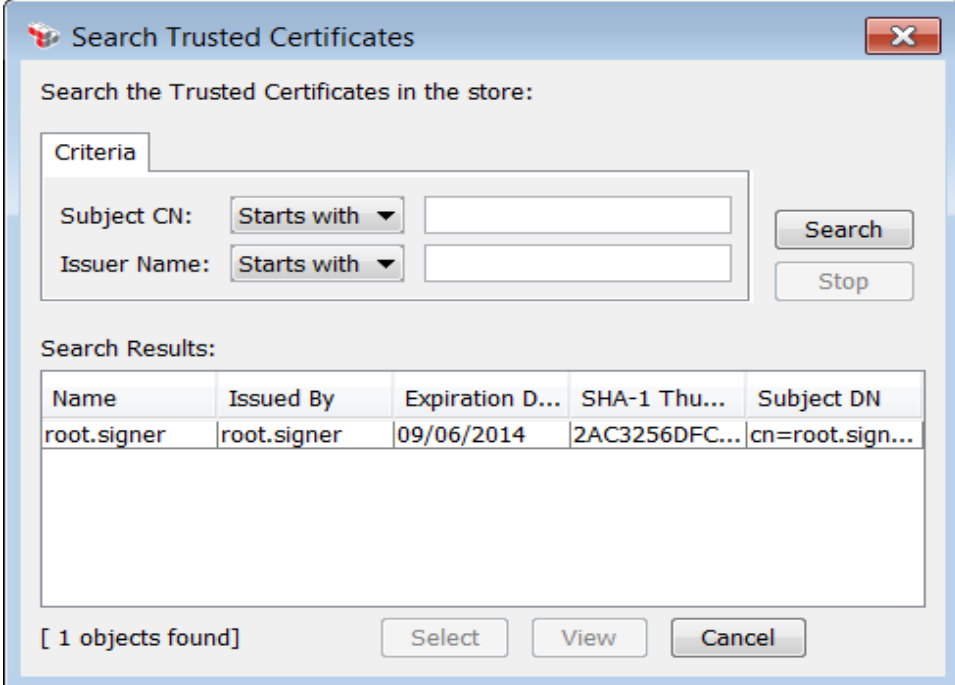
## Searching Trusted Certificates

You can search the list of trusted certificates in the Gateway trust store using the Search Trusted Certificates dialog. When a certificate is found, you can either select it for insertion into the dialog that opened the Search Trusted Certificates dialog, or you can view the certificate details.

➤ To search trusted certificates:

1. Click **[Add]** on the [Edit Certificate Revocation Checking Properties](#) dialog.

The Search Trusted Certificates dialog appears.



| Name        | Issued By   | Expiration D... | SHA-1 Thu...  | Subject DN      |
|-------------|-------------|-----------------|---------------|-----------------|
| root.signer | root.signer | 09/06/2014      | 2AC3256DFC... | cn=root.sign... |

Figure 106: Search Trusted Certificates dialog

2. Configure the search settings as follows:

Table 78: Search Trusted Certificates settings

| Setting            | Description  |
|--------------------|--|
| <b>Subject DN</b>  | To refine your search, you can optionally specify that the Subject DN <b>Equals</b> or <b>Starts with</b> the string of characters that you specify. You can use the asterisk (*) wildcard to match any number of characters.<br><br><b>Tip:</b> In the certificate properties, the Subject DN is shown in the "Issued To:" field under the [General] tab. |
| <b>Issuer Name</b> | To refine your search, you can optionally specify that the Issuer Name <b>Equals</b> or <b>Starts with</b> the string of characters that you specify. You can use the asterisk (*) wildcard to match any number of characters.   |
| <b>Search</b>      | This starts the search. Any certificates found are displayed in the <b>Search Results</b> box.   |
| <b>Stop</b>        | This halts the search before it is completed. You may wish to stop the search if the certificate you are seeking is already displayed or if the search is too broad and too many results are displayed.  |
| <b>Select</b>      | This closes the Search Trusted Certificate dialog and adds the selected certificate to the previous dialog.  |
| <b>View</b>        | This displays the properties for the selected certificate. For more information about the properties, see "Editing a Certificate" on page 247.   |

## Managing Private Keys

The Gateway can be configured to use customized private keys. These customized private keys can be used for SSL communication, outbound message signing, and inbound message decryption.

Private keys are stored in the Gateway as PKCS#12 files or in an external SafeNet HSM network-attached Hardware Security Module.

Once the keystore has been defined, the private keys are managed in the Policy Manager through the Manage Private Keys task.

The Manage Private Keys task lists all certificates installed on the Gateway cluster for which the Gateway possesses a copy of the private key. You can use this dialog to:

- Create a new private key
- Import a private key from another source
- Sign a certificate
- View the properties of an existing private key
- Display information about the configured keystore

---

**Note:** If you need to store plain text PEM private keys, use the [Manage Stored Passwords](#) task instead. The Manage Private Keys task is only used for asymmetric private keys with certificate chains.

---

## Advanced User Tip

### *Creating a Private Key Signed by Another Local Private Key*

You can use the Manage Private Keys task to create a private key with a certificate chain that is signed by a different local private key. If you need to do this:

1. Create two private keys, one CA-capable and the other not.
2. View the [properties](#) of the non-CA key and click **[Generate CSR]**. Save the CSR to a .pem file.
3. Returning to the Manage Private Keys dialog, select the CA key and click **[Sign Cert]**.
4. Locate and open the .PEM file created in step 2.
5. Save the resulting certificate chain to a different .PEM file.
6. View the properties of the non-CA key again and this time click **[Replace Certificate Chain]**.
7. Locate and open the .PEM file created in step 5.

You now have a CA-capable private key with a self-signed certificate and a non-CA key with a certificate that has been signed by the CA key.





➤ *To manage private keys:*

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Private Keys dialog appears.



Figure 107: Manage Private Keys dialog

The following icons are used in the Manage Private Keys dialog:

-  indicates a key with a CA-capable certificate chain
-  indicates a key with a certificate chain that is not CA-capable
-  indicates the default CA key (default is set in the [Private Key Properties](#))
-  indicates the default SSL key (default is set in the [Private Key Properties](#))

2. Select a task to perform:

Table 79: Manage private keys tasks

| To...                              | See  |
|------------------------------------|--|
| <b>Create a new private key</b>    | "Creating a Private Key" on page 262   |
| <b>Import a private key</b>        | "Importing a Private Key" on page 265  |
| <b>Sign a certificate</b>          | "Signing a Certificate" on page 268  |
| <b>View private key properties</b> | "Private Key Properties" on page 271<br>This allows you to access less frequently-used actions such as generating a CSR, replacing the certificate chain, setting the key as the default SSL or CA key, or destroying the key. |
| <b>Manage Keystore</b>             | "Managing Keystore" on page 208<br>This is used to enable or disable the SafeNet Luna keystore (if installed).   |

3. Click **[Close]** when done.

## Creating a Private Key

Private keys are used for SSL communication, outbound message signing, and inbound message decryption. You can create new private keys using the Policy Manager or import existing keys from a PKCS#12 file. For more information on private keys, see "Managing Private Keys" on page 260.

---

**Note:** If you create a new private key in a Gateway cluster configured with an internal Hardware Security Module (HSM), you must restart all nodes in the cluster in order for the new private key to be recognized.

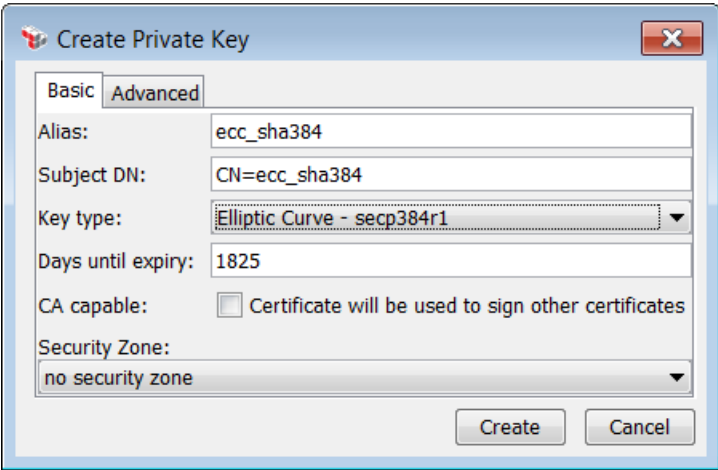
---

➤ To create a new private key:

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The [Manage Private Keys](#) dialog appears.
2. Click **[Create]**.

The Create Private Key dialog appears, with the **[Basic]** tab displayed.





The image shows a 'Create Private Key' dialog box with a 'Basic' tab selected. The fields are as follows:


- Alias: ecc\_sha384
- Subject DN: CN=ecc\_sha384
- Key type: Elliptic Curve - secp384r1
- Days until expiry: 1825
- CA capable: ☐ Certificate will be used to sign other certificates
- Security Zone: no security zone

Buttons: Create, Cancel

Figure 108: Create Private Key dialog - [Basic] tab

- Configure the properties on the **[Basic]** tab as follows:

Table 80: Basic private key properties

| Field                    | Description  |
|--------------------------|--|
| <b>Alias</b>             | Enter an <b>Alias</b> for the key.   |
| <b>Subject DN</b>        | <p>Enter the <b>Subject DN</b> for the initial self-signed certificate for the new private key. This specifies the owner of the initial self-signed certificate and should be in the form of an X.509 subject. For example:</p> <p><i>CN=ssl.layer7tech.com, O="CA Technologies, Inc", L=Vancouver, ST=British Columbia, C=CA</i></p> <p>Note that fields containing commas should be enclosed in quotes.</p>  |
| <b>Key type</b>          | Select the <b>Key type</b> from the drop-down list.  |
| <b>Days until expiry</b> | Enter the number of days before the initial self-signed certificate expires. The default is <b>1825</b> days (5 years).  |
| <b>CA capable</b>        | <p>Select the <b>Certificate will be used to sign other certificates</b> check box if the private key is to be CA-capable. The Policy Manager flags CA-capable keys with a  icon to remind you.</p> <p><b>Note:</b> Keys with self-signed certificates created by the Gateway as CA-capable cannot be used for any other purpose.</p> <p><b>Advanced Tip:</b> It is possible to replace the entire certificate chain with a different one (for example, from an internal or public PKI provider) that certifies the public key for other key usages, even if the initial self-signed certificate was created using the <b>[Certificate will be used to sign other certificates]</b> option.</p> |
| <b>Security Zone</b>     | Optionally choose a security zone. To remove this entity from a  |

| Field | Description  |
|-------|--|
|       | <p>security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p> <p><b>Tip:</b> Security zones apply to private keys but not to the keystore itself. This means (for example) if you only have the "Manage Test Zone" role and you need to manage private keys in the Test zone, you must also have an additional role that grants read permission to the Gateway keystore.</p> |

4. In the **[Advanced]** tab, select a specific signature hash to use when signing a certificate. The default setting of **Auto** means the Gateway will automatically determine the signature hash. This default should work well in most instances.

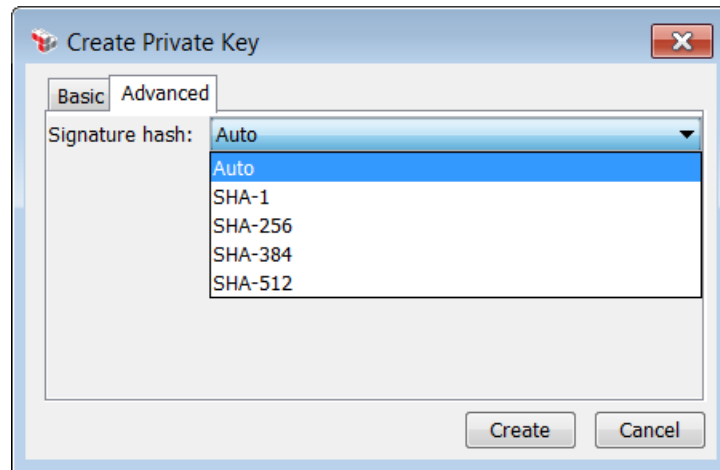


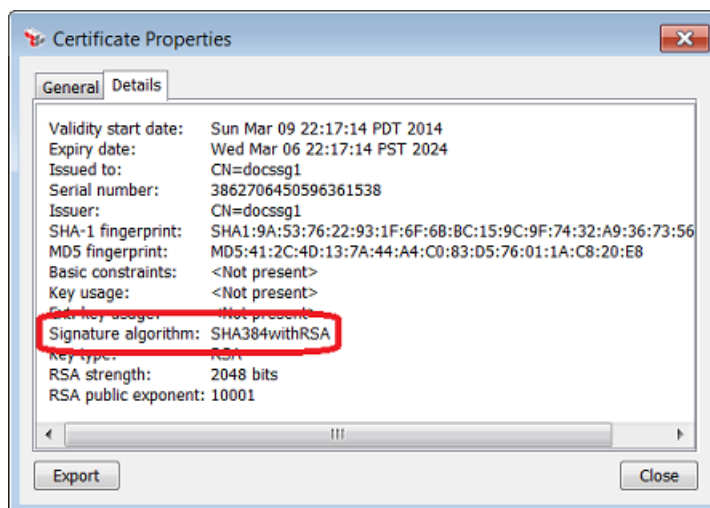
Figure 109: Create Private Key dialog - [Advanced] tab

5. Click **[Create]** to generate the new key pair. The new private key is added to the list of certificates on the Manage Private Keys dialog.

---

**Tip:** To verify the signature hash, look for the certificate's signature algorithm under the [Details] tab of the [certificate's properties](#):

---



## Importing a Private Key

You can import an existing certificate chain and private key from a PKCS#12 file into the Gateway keystore.

**Note:** If the Gateway uses a Thales nCipher HSM, you cannot import a key when the security world complies with FIPS 140-2 level 3.

➤ *To import a private key:*

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The [Manage Private Keys](#) dialog appears.
2. Click **[Import]**. You are prompted to identify the new private key with an alias.
3. Enter a description of the new private key as the alias. You are then prompted for the certificate file.
4. Navigate to the PKCS#12 certificate file and then click **[Load]**.
5. Enter the pass phrase for the private key and then click **[OK]**. The imported private key is added to the list.

**Note:** You will be warned if the certificate chain of the private key being imported contains any certificate that is either:

- expired
- not yet valid

- contains an Issuer DN that does not match the Subject DN of the next certificate in the chain
- contains a signature that does not verify using the public key of the next certificate in the chain

## Exporting a Private Key

You can export any [private key](#) that is [stored](#) in the software database, as either a \*.p12 or a \*.pfx file. The exported key is protected with a password.

---

**Note:** Private keys cannot be exported from a Hardware Security Module (HSM), due to the high-security mode of these type of keystores.

---

➤ *To export a private key:*

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The Manage Private Keys dialog appears.
2. Select the private key to be exported and then click **[Properties]**. The Private Keys Properties dialog appears.
3. Click **[Export Key]** in the **Other Actions** section. You are prompted to provide a password to protect the exported key.
4. Enter a password and then retype for confirmation.
5. Click **[OK]**. You are prompted for a location to save the exported key.
6. Navigate to the destination and then click **[Save]**.

## Deleting a Private Key

You can delete a private key along with its certificate chain from the keystore. Use this action with caution, as deleting a private key is permanent. If you delete a key that is the default SSL or CA key, be sure to designate a replacement immediately, otherwise the following will occur:

- If you delete the CA key and do not designate a replacement, CA services will be unavailable when the cluster is restarted.
- If you delete the SSL key and do not designate a replacement, the following will occur after the cluster is restarted: the first cluster node that starts up will automatically create a self-signed SSL key and configure the cluster to use that as its SSL key.

➤ To delete a private key:

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The Manage Private Keys dialog appears.
2. Select the private key to be deleted and then click **[Properties]**. The Private Keys Properties dialog appears.
3. Click **[Destroy Key]** in the **Other Actions** section. You are prompted to confirm:

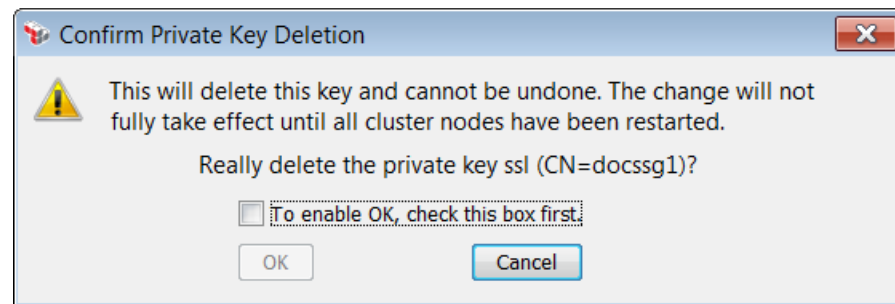


Figure 110: Special private key deletion confirmation

4. Select the check box to indicate that you are aware of the consequences of deleting a private key. The **[OK]** button is enabled only when the check box is selected.
5. Click **[OK]**. The private key is deleted. Note that all cluster nodes must be restarted before the deletion takes full effect.

## Generating a Certificate Signing Request (CSR)

You can use a [private key](#) to generate a new PKCS#10 certificate signing request (CSR). This CSR is then saved to the local hard disk of the machine running the Policy Manager, in either binary (\*.p10) or Base64 PEM (\*.pem) format. You can then send this CSR to a certificate authority (CA) to apply for an actual certificate.

---

**Tip:** Many CAs allow you to apply for a certificate by uploading a CSR file through a Web page.

---

➤ To generate a certificate signing request:

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The Manage Private Keys dialog appears.
2. Select the private key to be used to generate the CSR and then click **[Properties]**. The Private Keys Properties dialog appears.

3. Click **[Generate CSR]** in the **Other Actions** section. You are prompted to provide a subject DN for the CSR. The current subject DN is offered as a default.
4. Enter the **CSR Subject (DN)**. This specifies the owner of the initial self-signed certificate and should be in the form of an X.509 subject. For example:

*CN=ssl.layer7tech.com, O="CA Technologies, Inc", L=Vancouver, ST=British Columbia, C=CA*

**Note:** Fields that contain commas must be enclosed in quotes, as shown in the above example.

5. Choose the **Signature hash** to use from the drop-down list. The following options are available:

**Auto** (default)

**SHA-1**

**SHA-256**

**SHA-384**


**SHA-512**

**Tip:** Selecting "Auto" duplicates the automatic signature hash selection that occurred in versions prior to 7.1. With this setting, the Gateway uses the *com.l7tech.security.cert.alwaysSignWithSha1* system property to determine the hash.

6. Click **[OK]**. You are prompted for a location to save the file.
7. Navigate to the destination and then click **[Save]**. Note that by default, the file is saved as a Base64 PEM file; you can change this to PKCS #10 format if necessary.

## Signing a Certificate

➤ *To sign a CSR using a private key:*

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The [Manage Private Keys](#) dialog appears.
2. Select the private key to be used for the signing. Eligible keys are indicated by the  icon.

---

**Tip:** You can use a key that's not flagged as being eligible for signing, but you will be warned that certain software systems may reject certificates signed by that key.

---

3. Click **[Sign Cert]**. You are prompted to select the Certificate Signing Request to open. If you chose an ineligible key, click **[OK]** to acknowledge the consequences

or click **[No]** or **[Cancel]** to select another key.

4. Locate the .pem file that contains the CSR that you are accepting. This creates a new signing certificate using the private key that was selected in step 2.
5. The properties for the newly created signing certificate are displayed.

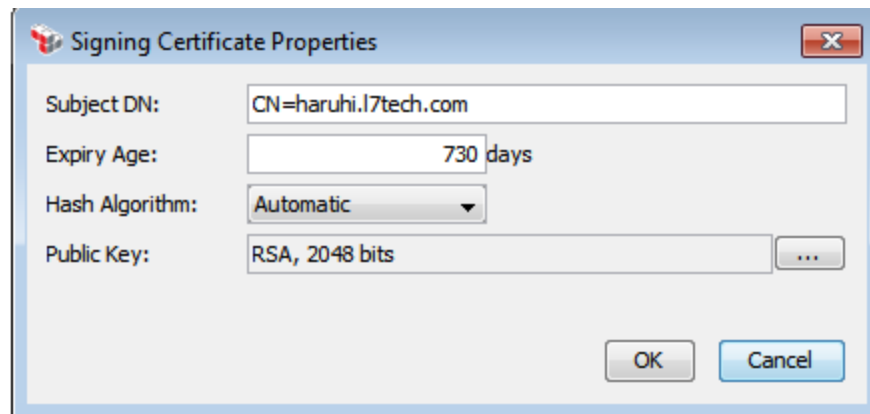



Figure 111: Signing Certificate Properties

Modify any settings as necessary.

Table 81: Signing Certificate Properties

| Setting               | Description   |
|-----------------------|---|
| <b>Subject DN</b>     | This field displays the subject DN of the certificate signing request.  |
| <b>Expiry Age</b>     | This field specifies the number of days before the certificate expires. By default, this is <b>730</b> days. You can change the default using <a href="#">pkix.csr.defaultExpiryAge</a> cluster property.   |
| <b>Hash Algorithm</b> | <p>Choose the Hash Algorithm to use: <b>Automatic, SHA-1, SHA-256, SHA-384, SHA-512.</b></p> <p>The default "&lt;Automatic&gt;" setting selects the algorithm as follows:</p> <ul style="list-style-type: none"> <li>• If the system property, <code>com.l7tech.security.cert.alwaysSignWithSha1</code> is defined, or if the issuer public key is a short key, then SHA-1 is used.</li> <li>• Otherwise, it will use SHA-384.</li> </ul> |
| <b>Public Key</b>     | This field displays brief details about the public key. Click  to view the full public key details.  |

6. Click **[OK]** to close and save the certificate properties. You are prompted to save the resulting certificate chain. Note that the destination file also uses the .pem extension, since the file is PEM-encoded. Browse to the location to save the .pem

file.

7. Enter a name for the signed certificate chain and then click **[Save]**.

A new certificate chain is created. You can see this chain in the "Private Key Properties" on page 271.

**Note:** The new certificate chain belongs to the client and is **not** kept by the Gateway. You can make the Gateway trust the newly signed certificate by doing one of the following:

- To trust the certificate as a client certificate, import it as an Internal or LDAP user's client certificate. For information on importing it for an internal user, see "Creating an Internal User" on page 286.
- To trust the certificate for some other purpose, import it using the [Manage Certificates](#) task.



## Private Key Properties

The Private Key Properties dialog displays overview information about a private key and provides access to other actions that are used infrequently (for example, generating a CSR or destroying a key).

The Private Key Properties dialog is accessed using the **[Properties]** button on the [Manage Private Keys](#) dialog.

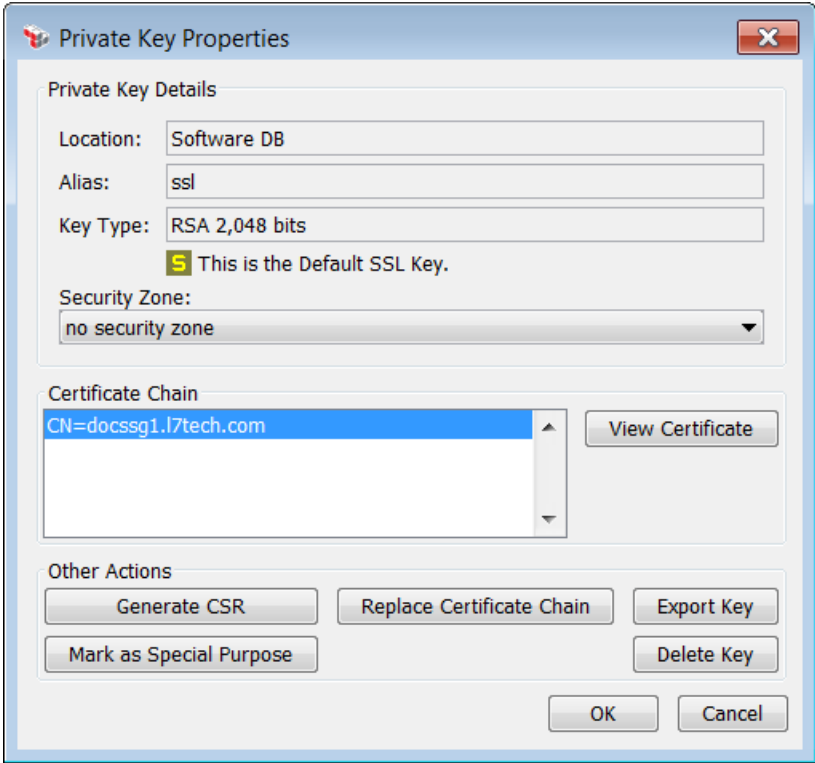


Figure 112: Private Key Properties

The following table describes the properties:

Table 82: Private key properties settings

| Label           | Description  |
|-----------------|--|
| <b>Location</b> | The name of the keystore holding the private key being stored. This is either the software database keystore or the cluster HSM keystore. For more information, see "Private Key Locations" on page 274. |
| <b>Alias</b>    | The name assigned to the key. Used to identify the key within the keystore when configuring a policy assertion to use that key.  |
| <b>Key Type</b> | The type of the private key.   |

| Label                            | Description  |
|----------------------------------|--|
| <b>Security Zone</b>             | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>                        |
| <b>Certificate Chain</b>         | <p>Displays the current certificate chain for the selected private key, beginning with the subject certificate. Every new private key created in the Gateway will initially have a certificate chain that consists of just a self-signed placeholder certificate. You can replace this with any other certificate chain that has a subject certificate that has the same public key as the initial subject certificate. The replacement certificate is based on the same key pair as the original certificate. See <b>"Replace Certificate Chain"</b> below.</p> |
| <b>View Certificate</b>          | <p>Opens the Certificate Properties dialog to display information about the certificate. For more information about this dialog, see "Editing a Certificate" on page 247. <b>Note:</b> The certificate is not editable when open from this location.</p>   |
| <b>Generate CSR</b>              | <p>Generates a new PKCS#10 certificate signing request (CSR) using the selected private key. For more information, see "Generating a Certificate Signing Request (CSR)" on page 267.</p>   |
| <b>Replace Certificate Chain</b> | <p>Replaces the existing certificate chain with a new chain that uses the same private key. For example, you will use this action to replace a placeholder certificate with an actual certificate returned from a CA.</p>  |
| <b>Export Key</b>                | <p>Exports a private key that is stored in the software database. For more information, see "Exporting a Private Key" on page 266.</p>   |
| <b>Mark as Special Purpose</b>   | <p>Sets the selected key as any one of the following special keys:</p> <div data-bbox="763 1434 1109 1621" data-label="Image"> </div> <ul style="list-style-type: none"> <li>• <b>Make Default SSL:</b> Makes the selected key the default SSL private key for the cluster. For more information, see "Setting a Default SSL or CA Private Key" on page 274.</li> <li>• <b>Make Default CA:</b> Makes the selected key the default CA private key for the cluster. For more information, see "Setting a Default SSL or CA Private Key" on page 274.</li> </ul>   |

| Label             | Description  |
|-------------------|--|
|                   | <ul style="list-style-type: none"> <li>• <b>Make Audit Signing Key:</b> Makes the selected key the default audit signing key. All internally-saved signed audit records will be signed with this key whenever internal audit signing is enabled (see the <a href="#">audit.signing</a> cluster property).<br/>If an audit signing key is not assigned, the Gateway will use the default SSL key to sign audit records.</li> </ul> <p><b>Notes:</b> (1) Avoid frequent changes to the audit signing key, as this may cause potential issues during verification. (2) Designating an audit signing key does not affect any signing that may be done with assertions in an <a href="#">audit sink policy</a>.</p> <ul style="list-style-type: none"> <li>• <b>Make Audit Viewer Key:</b><br/>Makes the selected key the audit viewer key, to be used to decrypt encrypted audits in the Audit Viewer policy.<br/>The audit viewer key is required when an authorized user attempts to view encrypted audit information in the Policy Manager. For more information, see "<a href="#">Invoking the Audit Viewer Policy</a>" in "Gateway Audit Events" on page 415.<br/>Keep in mind the following about the audit viewer key: <ul style="list-style-type: none"> <li>• Once a key is assigned, it cannot be used in any other policy or for any other task. This is to prevent encrypted audits from being decrypted using a normal service policy.</li> <li>• Keys cannot be designated as the audit viewer key at the same time as they are designated for some other special purpose.</li> <li>• A key should not be deleted while it is currently serving as the audit viewer key, as this will make encrypted audits unviewable. However, once a key ceases to be the audit viewer key, it is recommended that you delete it, to prevent unauthorized users from decrypting audit records that were encrypted with that key.</li> </ul> </li> </ul> |
| <b>Delete Key</b> | <p>Deletes the private key and certificate chain from the keystore. Use this action with caution, as deleting a private key is permanent. For more information, see "Deleting a Private Key" on page 266.</p> <p><b>IMPORTANT:</b> Do not delete a key that is currently serving as the audit viewer key. This will render your <a href="#">encrypted audits</a> unviewable. Reassign the audit viewer key to another key first.</p>   |

---

**Note:** Depending on where the private keys are stored, not all of the "Other Actions" buttons shown in Figure 112 may be available. For more information, see "Private Key Locations" on page 274.

---

## Private Key Locations

Where [private keys](#) are located will affect the [actions](#) that you can perform on the keys. Private keys are stored in the following locations:

Table 83: Private key locations

| Location                | Writable | Notes   |
|-------------------------|----------|---|
| <b>Software DB</b>      | Yes      | This is a software keystore that is stored in the database, as a PKCS#12 keystore.  |
| <b>SafeNet Luna HSM</b> | Yes      | This is an optional hardware security module that can be purchased and configured to work with the Gateway (all form factors). When enabled, the SafeNet HSM overrides any other keystore on the Gateway. |

By default, an SSL private key is created, with Alias "ssl" and Subject "CN= <gateway\_hostname>". This initial default SSL key, as well as any subsequent created keys, are all created in Software DB. Keys in the Software DB are writable, meaning they can be destroyed and their certificate chains can be destroyed. If all keys are destroyed using the [Manage Private Keys](#) task, the original default SSL key is recreated once the Gateway is restarted (with Alias="ssl"; Subject="<gateway\_hostname>").

A CA key is not created by default. You need a CA key only if the both the following apply:

- The Gateway cluster will be communicating with the Securespan XML VPN Client.
- You expect to use the automatic client certificate provisioning feature in the Securespan XML VPN Client.

For information on configuring a CA key for the cluster, see "Managing Private Keys" on page 260. You will use this task to create a new CA-capable key and then set it as the default.

If you [create or import](#) any custom private keys, they will be stored in the "Software DB" location. These keys can be destroyed or modified.



## Setting a Default SSL or CA Private Key

You can designate a [private key](#) to be the default SSL or CA private key for the cluster.

### W A R N I N G

Do not use the default CA key to be the default SSL key. Doing so will cause the Policy Manager to fail to connect to the Gateway.

➤ To set a default SSL or CA private key:

1. In the Policy Manager, select **[Tasks] > Manage Private Keys** from the [Main Menu](#). The Manage Private Keys dialog appears.
2. Select the private key to be used to generate the CSR and then click **[Properties]**. The Private Keys Properties dialog appears.
3. Click the **[Mark as Special Purpose]** button and then:
  - Select **Make Default SSL Key** to make this key the default SSL private key (indicated by  on the interface).  
**Note:** When an elliptic curve certificate (ECC) is designated as the default SSL key, the Require Encrypted Element assertion will not function when using Securespan XML VPN Client with the default WSS recipient. The Securespan XML VPN Client does not currently support encrypting XML for a recipient using an ECC key, and the Gateway does not currently support decrypting XML encrypted for an ECC key.
  - Select **Make Default CA Key** to make this key the default CA private key (indicated by  on the interface).
4. Click **[Yes]** to confirm. The key that previously held these functions is automatically unassigned. The change takes effect after all cluster nodes are restarted.

## Selecting a Custom Private Key

The following assertions can use [custom private keys](#):

- Route via HTTP(S): When using an HTTPS URL and the server sends a client certificate challenge, the Route via HTTP(S) assertion can now present a custom client certificate instead of using the standard Gateway SSL certificate as its client certificate.

---

**Note:** The **Select Private Key** option is available only when routing to an HTTPS address. It is disabled for HTTP.

---

- Sign Element: This assertion can use a custom private key to sign the response.
- Add Timestamp: This assertion can use a custom private key when adding a signed timestamp.
- Add Security Token: This assertion can use a custom private key when adding a signed security token.

- **Customize SOAP Fault Response:** This assertion can use a custom private key for signing SOAP faults.
- **Build SAML Protocol Response:** This assertion can use a custom private key for signing the response.

**Note:** The three signing assertions (Sign Element, Signed Timestamp, Signed Security Token) should use the same private key if they all target the same message and WSS recipient. The policy validator will warn you if the keys differ.

➤ To select a custom private key:

1. Right-click the assertion in the [policy window](#) and then choose **Select Private Key**. The Private Key Alias dialog is displayed.

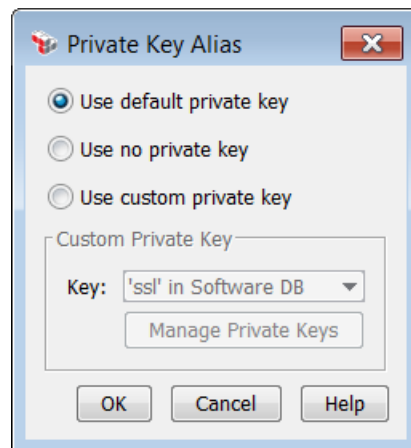


Figure 113: Private Key Alias dialog

2. Configure the dialog as follows:

Table 84: Private Key Alias dialog

| Setting                        | Description   |
|--------------------------------|---|
| <b>Use default private key</b> | Select this option to use the default Gateway SSL or CA certificate to respond to a client certificate challenge from the server. For more information about default keys, see "Private Key Properties" on page 271.  |
| <b>Use custom private key</b>  | Select this option to use a custom private key to respond to a client certificate challenge from the server. Select the key below.  |
| <b>Key</b>                     | From the drop-down list, select the custom key to use. The key must already be defined using the <a href="#">Manage Private Keys</a> task. To jump directly to that task, click <b>Manage Private Keys</b> .<br><br><b>Note:</b> If the assertion uses a private key that has since been deleted, |

| Setting | Description   |
|---------|---|
|         | you will receive a policy validator warning message and the Private Key Alias dialog will display '<keyname> in UNRECOGNIZED' in the Key drop-down list. If the policy is saved as-is, then the Gateway will consult the <code>keyStore.searchForAlias</code> <a href="#">cluster property</a> for the appropriate course of action during compilation time. Alternatively, you can select another custom private key to use. |

3. Click **[OK]** when done.





## Chapter 4:

# Working with Identity Providers

The Policy Manager can use the following types of identity providers:

- **Internal Identity Provider**

A single Internal Identity Provider (IIP) is pre-configured as the authentication database inside the Gateway. The Policy Manager allows you to modify the users and groups in the IIP. For information on adding users and/or groups to the IIP, see "Internal Identity Provider Users and Groups" on page 286.

- **LDAP Identity Providers**

You can configure and manage one or more LDAP Identity Providers in the Policy Manager. An LDAP Identity Provider is an LDAP connector that is used for authentication purposes.

A simplified variant of the LDAP Identity Provider is also available, if you wish to perform authentication via bindings only.

For information, see "LDAP Identity Providers" on page 303.

- **Federated Identity Providers**

A Federated Identity Provider (FIP) is exclusively used in an [identity bridging](#) configuration. Essentially, the FIP allows one security domain to authorize requests containing credentials originating from another security domain. For more information, see "Federated Identity Providers" on page 440.

- **Policy-Backed Identity Providers**

The Policy-Backed Identity Provider uses an underlying policy fragment to authenticate users, based on a username and password passed through via context variables. For more information, see "Policy-Backed Identity Providers" on page 325.

---

**Note:** The term *identity* includes both users and groups; *user* can represent an individual human or machine; *service* includes both web services and XML applications.

---

## Impact of Security Zones

The Federated and LDAP identity providers may be placed into [security zones](#). Once in a zone, only users who have the corresponding "Manage <zone>" or "View <zone>" [roles](#) can see these providers. However, when a "Manage <zone>" user publishes a service, that user is automatically assigned the "Manage <service>" [role](#). Among the permissions granted by this role is the ability to access *all* identity providers, regardless of security zone. The Policy Manager indicates this by showing the identity provider's security zone as the user's zone.

Example: Bob is in "Zone A" while Sue is in "Zone B". They both have published services and thus are able to view all identity providers. FIP "Alpha" has been placed in Zone C, while LDAP identity provider "Beta" has been placed in Zone D. However when Bob views Alpha and Beta, they will both appear to be in Zone A. Similarly, they will show Zone B when Sue does the same.

## Searching Identity Providers

The Policy Manager makes it easy to locate and view information about users and groups defined in the following [identity providers](#):

*Internal Identity Provider*

*LDAP Identity Provider*

*Federated Identity Provider*

---

**Note:** The Simple LDAP Identity Provider is not searchable and will not return meaningful results. The Policy-Backed Identity Provider has a slightly different use case that is described in more detail under "[Working with Policy-Backed Service Providers](#)" below.

---

➤ *To search identity providers:*

1. Do any of the following:
  - Click **Search Identity Provider** on the [Home Page](#).
  - Click [Tasks] > **Search Identity Provider** from the [Main Menu](#).
  - Right-click the identity provider to be searched in the [\[Identity Providers\] tab](#) and then select **Search Identity Provider**. The Search Identity Provider dialog appears.

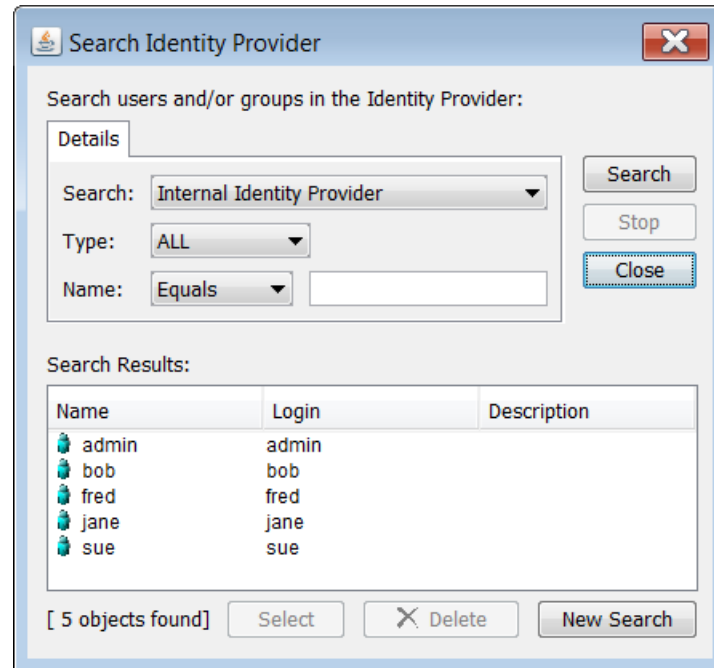




Figure 114: Search Identity Provider dialog, with sample search results

2. Configure the search settings as follows:

Table 85: Search Identity Provider settings

| Setting                           | Description   |
|-----------------------------------|---|
| <b>Search</b><br>(drop-down list) | Choose the <a href="#">identity provider</a> to be searched from the drop-down list. You can only search one identity provider at a time.<br><br><b>Tip:</b> The search behavior for <a href="#">Policy-Backed Identity Providers</a> works a bit differently. See " <a href="#">Working with Policy-Backed Identity Providers</a> " below for details. |
| <b>Type</b>                       | From the drop-down list, choose what you are searching for: <b>Groups</b> , <b>Users</b> , or <b>All</b> .  |
| <b>Name</b>                       | To refine your search, you can optionally specify that the name <b>Equals</b> or <b>Starts with</b> the string of characters that you specify. You can use the asterisk (*) wildcard to match any number of characters, or the question mark (?) to match any single character.   |
| <b>Search</b><br>(button)         | This starts the search. Any names found are displayed in the <b>Search Results</b> box.   |
| <b>Stop</b>                       | This halts the search before it is completed. You may wish to stop the search if the name you are seeking is already displayed or if the search is taking too long.   |
| <b>Close</b>                      | This closes the Search Identity Provider dialog.  |
| <b>New Search</b>                 | This clears the search criteria and search results fields.  |

3. The results appear in the Search Results window. Individual users are indicated by  while groups or **federated virtual groups** are denoted by .
  - To see detailed information about any user or group, double-click the name or click **[Select]** with the appropriate name selected. The properties for that user or group is displayed.
  - To edit or delete non-LDAP users or groups, see "Editing or Deleting a User or Group" on page 458.

---

**Note:** **LDAP Identity Provider** users and groups cannot be changed in the Policy Manager. To modify these users or groups, use the appropriate external management program. The Gateway uses a definition XML file to support IBM® Tivoli® Access Manager (Tivoli) directory searches.

---

## Working with Policy-Backed Identity Providers

A **Policy-Backed Identity Provider** cannot be searched in the conventional sense, because it is not designed to house a set list of users like the Internal Identity Provider. Instead, you can use the Search Identity Provider dialog to assign roles to *template users*. These are users that the Gateway may not "know" about yet, but you can assign roles to these users if and when they are authenticated via a Policy-Backed Identity Provider.

*Example:*

You can configure it such that when user "sally" is authenticated against a Policy-Backed Identity Provider, she will automatically be assigned the role of "Operator". It does not matter that "sally" is not defined in any other identity provider or whether she will access the Gateway at all.

➤ *To configure a role for a template user:*

1. Open the Search Identity Provider dialog.
2. Choose a Policy-Backed Identity Provider from the **Search** drop-down list.
3. Enter **sally** in the "Name" box, leaving all other settings at their default.
4. Click **[Search]**. This creates the template user "sally":

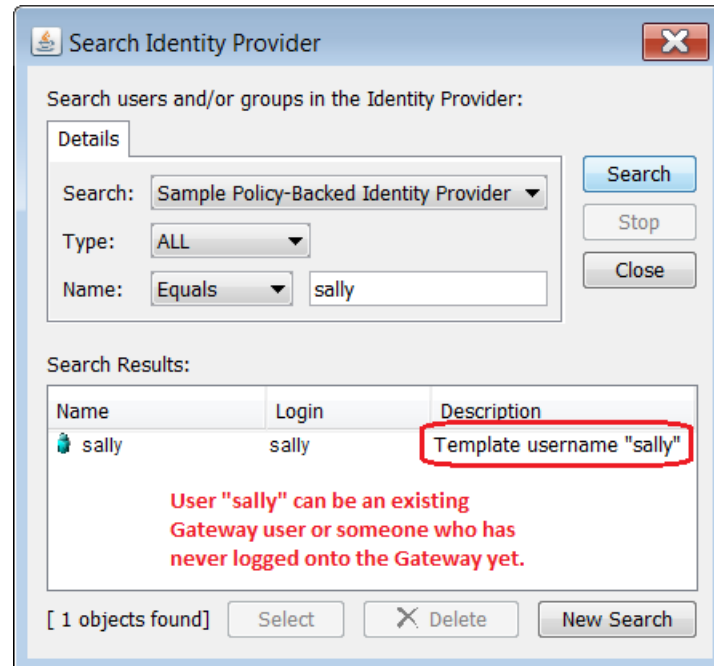


Figure 115: Creating a template user

5. Select "sally" and then click **[Select]**. This opens the properties dialog for "sally".
6. Select the [Roles] tab and then add the role(s) to be assigned to user "sally". For more information about this tab, see "[Configuring the \[Roles\] Tab](#)" under "Internal User Properties" on page 288.

---

**Note:** Any role(s) that you assign here to a template user will override a default role assigned through the "Policy-Backed Identity Provider Wizard" on page 327.

---

## Identity Tags

Identity tags are labels that you can optionally create to 'tag' authenticated users for later reference. It is a means to differentiate between identities that are not known at policy design time.

### Background

Without using identity tags, the identity assertions involving group membership cannot authenticate multiple users within the same policy (when identified by the same Group or Identity Provider). Consider the following example:

Request: WSS Signature (Gathers credentials)

Request: Group Membership: SampleGroup (Authenticates the user and checks that the user is a member of the group "SampleGroup")

Request: Group Membership: SampleGroup (Checks that the user is a member of "SampleGroup" but does not reauthenticate)

When identity tags are used, it is possible to authenticate multiple times for a single group or identity provider:

Request: WSS Signature (Gathers credentials)

Group Membership: SampleGroup as "tag1" (Authenticates user as "tag1" and checks for membership in group "SampleGroup")

Group Membership: SampleGroup as "tag1" (Checks that "tag1" is a member of group but does not re-authenticate)

Group Membership: SampleGroup as "tag2" (Authenticates user as "tag2" and checks for membership in group "SampleGroup")

In the example above, the identity tags "tag1" and "tag2" are used to distinguish between the two identities even though the specific identities involved are not known at the time the policy was created.

---

**Notes:** (1) It is not necessary to create identity tags unless multiple signatures are present in a message and you wish to use a tag to specify a target identity (versus selecting an explicit identity). (2) Once an identity tag is used for authentication, the regular identity (e.g., "User: bob") is no longer available to be selected as a target identity.

---

Signing credential sources (for example the Require Encrypted UsernameToken Profile Credentials, Require SAML Token Profile, Require WS-Secure Conversation, Require WS-Security Kerberos Token Profile Credentials assertions) also support identity tags. If the policy includes those credential sources along with an identity assertion, the identity tag will be used for a target identity when verifying signatures in the target message.

➤ *To create an identity tag:*

1. Add an identity assertion to a policy: either Authenticate User or Group or Authenticate Against Identity Provider.
2. Right-click the identity assertion and select **Identity Tag** from the context menu. The Change Identity Tag dialog is displayed.

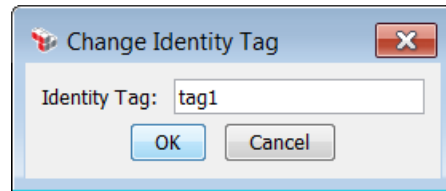


Figure 116: Adding or changing an identity tag

3. Enter a name for the identity tag. The name may include letters numbers and the characters: ' \_ - . , ' (the space character is permitted). Identity tags are not case sensitive, so the tag 'ABC' is the same as 'abc'.

---

**Tip:** There is no limit to the length of the tag, but for practical purposes it is best to keep the tag name short.

---

4. Click **[OK]**. The identity tag is appended to the end of the assertion name in the policy tree: "... as <Identity\_Tag>". For example:

```
User: Alice [Internal Identity Provider] as "First_User,
internal"
```

When you create an identity tag here, it can be later used to indicate the signing identity when multiple signatures are in effect. For more information, see *Selecting a Target Identity* in the *Layer 7 Policy Authoring User Manual*.

➤ *To edit or remove an identity tag:*

1. Right-click an identity assertion in the policy window and then select **Identity Tag**.
2. Edit the tag as necessary or clear the **Identity Tag** field to delete the tag.
3. Click **[OK]**. The tag is updated/removed in the policy window.

## Revoking User Certificates

You can revoke all user certificates issued by the Gateway certificate authority. This should be used when you need to revoke certificates for all users (perhaps due to compromise of the CA private key) and you need the system to issue new certificates.

---

**Note:** Revoking user certificates requires the "Administrator" [role](#). Passwords are not affected.

---

Once certificates are revoked, the Securespan XML VPN Client will detect that its certificate is no longer valid and will apply for a new certificate when required.

Revocation of user certificates will be listed in the [audit log](#) as a SEVERE event.

➤ *To revoke user certificates:*

1. Do one of the following:
  - Right-click **Identity Providers** in the [\[Identity Providers\] tab](#) and select **Revoke User Certificates**.
  - Select **[Tasks] > Revoke User Certificates** from the [Main Menu](#). (desktop client only)
2. Click **[OK]** to confirm. All user certificates are revoked immediately.

## Internal Identity Provider Users and Groups

The Internal Identity Provider (IIP) is configured during the installation and configuration of the Gateway. Use the Policy Manager to populate the IIP with users and groups.

---

**Notes:** (1) You need to define two types of IIP users: those who will be logging into Policy Manager and those who will only appear in messaging traffic. Users who require access to Policy Manager must also have a role assigned. For more information, see "Managing Roles" on page 130. (2) Users who [connect to the Gateway](#) via a client certificate must have a certificate with a 'CN' value that matches the username in order for the Internal Identity Provider to authenticate the user.

---

You can view information about the IIP by double-clicking the IIP name in the [\[Identity Providers\] tab](#). However, the IIP itself cannot be edited or deleted in the Policy Manager.

### Creating an Internal User

You need to define two types of Internal Identity Provider (IIP) users: users who need to [connect](#) to the Gateway from the Policy Manager (also known as administrative users), and those who will only appear in messaging traffic, to be used in the Authenticate User or Group or Authenticate Against Identity Provider assertions.

---

**Note:** To prevent potential unexpected results, do not replicate users from any other identity provider (for example, [LDAP](#)) in the Internal Identity Provider. The information for internal users in the Policy Manager must be unique.

---

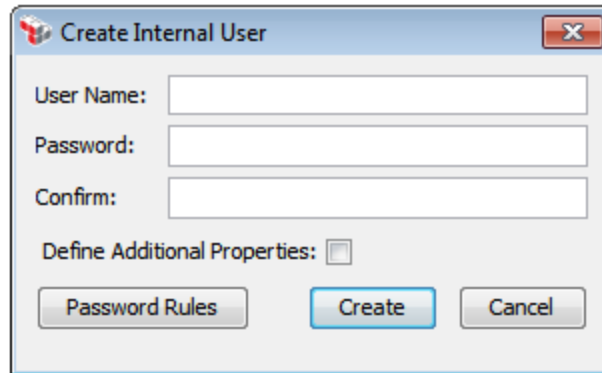
➤ *To add a new [internal user](#) to the Internal Identity Provider (IIP):*

1. Do one of the following:
  - Click **Create Internal User** on the [Home Page](#).
  - Click **[Tasks] > Create Internal User** from the [Main Menu](#).



- Right-click the IIP name in the **[Identity Providers]** tab and then select **Create User**.

The Create Internal User dialog appears.



The dialog box titled "Create Internal User" contains the following fields and controls:

- User Name:** A text input field.
- Password:** A password input field.
- Confirm:** A password input field.
- Define Additional Properties:** A checkbox.
- Buttons:** "Password Rules", "Create", and "Cancel".

Figure 117: Create Internal User dialog

2. Configure the dialog as follows:

Table 86: Internal user basic properties

| Setting                             | Description   |
|-------------------------------------|---|
| <b>User Name</b>                    | Enter the username for the user. The username cannot be changed once defined.<br><br><b>Note:</b> If this is a new administrative user who will be <a href="#">connecting to the Gateway</a> via a client certificate, ensure that the 'CN' value in the certificate matches the username entered here. The Internal Identity Provider requires matching values in order to authenticate the user. This does not apply to users who will only appear in messaging traffic or who will log in via username and password. |
| <b>Password</b>                     | Enter a password. The password can be changed later using the <a href="#">My Account</a> dialog.  |
| <b>Confirm</b>                      | Retype the password for confirmation.   |
| <b>Define Additional Properties</b> | Select this check box if you want to enter additional information about the user. All additional information is optional.   |
| <b>Password Rules</b>               | Displays a reminder of the password rules. For more information on how these rules are set, see "Managing Password Policy" on page 48.  |

---

**Using Non-English characters:** It is possible to add users with non-English single byte characters, or multi-byte characters in the User Name and Password fields. However these users will not authenticate successfully if HTTP Basic is used in a policy. This is a

---

---

limitation of the HTTP Basic standard, which limits characters to the ISO-8859-1 standard. The workaround is to use WSS Basic instead (see the Require WS-Security UsernameToken Profile Credentials assertion in the *Layer 7 Policy Authoring User Manual*).

---

3. Click **[Create]**.
  - If you are not defining additional properties, the dialog closes and the user is added to the Internal Identity Provider.
  - If you are defining additional properties, the Properties dialog for the user is displayed. For more detailed information about this dialog, see "Internal User Properties" on page 288.

## Internal User Properties

Every [internal user](#) has a set of extended user properties that can be set either when the user is first added to the system, or deferred until a later date. (During initial entry, only a minimal amount of user data is required, to facilitate rapid entry of many users.)

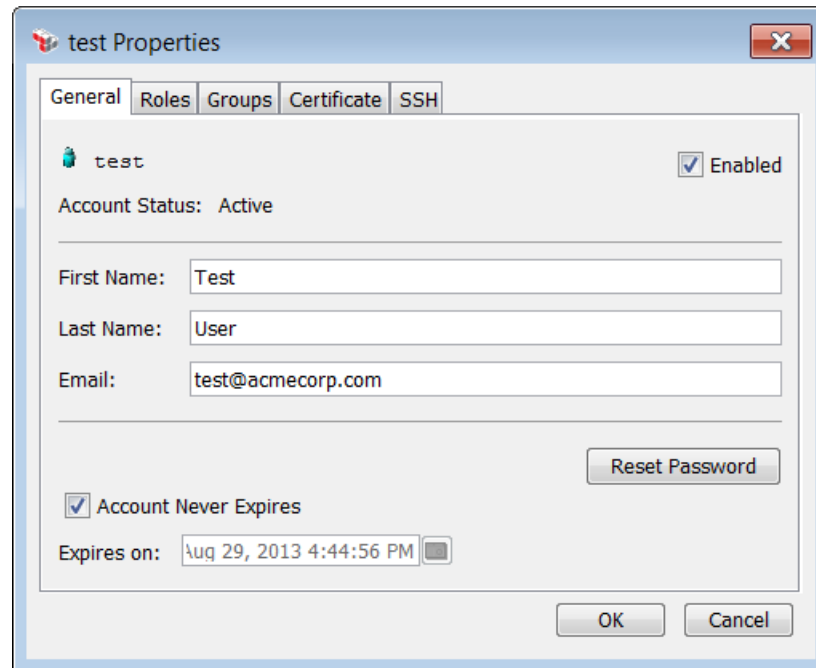
➤ *To access the properties for an internal user:*

1. Do one of the following:
  - [Create a new internal user](#), making sure to select the **Define Additional Properties** check box.
  - [Edit](#) an existing internal user.
  - Locate the user by [searching the identity provider](#).

The User Properties dialog appears.

3. Configure each tab within the properties as necessary. All information is optional. Refer to the appropriate section below for a complete description of each tab.
4. Click **[OK]** when done.

## Configuring the [General] Tab



The screenshot shows the 'test Properties' dialog box with the 'General' tab selected. The 'test' user is shown with an 'Enabled' status. The 'Account Status' is 'Active'. The 'First Name' is 'Test', 'Last Name' is 'User', and 'Email' is 'test@acmecorp.com'. There is a 'Reset Password' button. The 'Account Never Expires' checkbox is checked. The 'Expires on' field shows 'Aug 29, 2013 4:44:56 PM'. At the bottom are 'OK' and 'Cancel' buttons.

This tab is used to enter additional basic information about the user, as well as to modify the password that was initially entered.

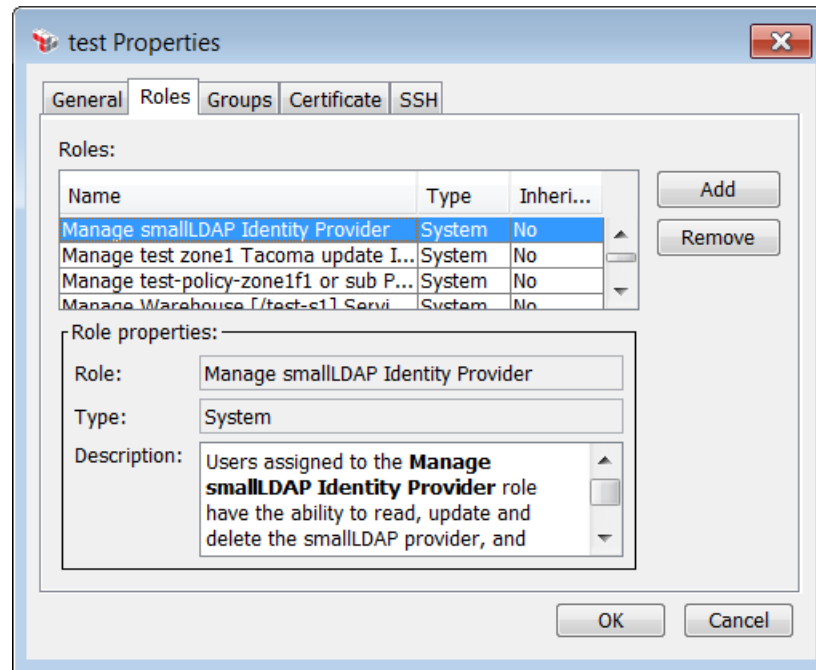
Table 87: User Properties - [General] tab

| Setting               | Description   |
|-----------------------|---|
| <b>Enabled</b>        | Indicates whether the account status is enabled or disabled. To enable the account, ensure this check box is selected. To disable an account, clear this check box. <b>Note:</b> If an account is expired, the check box is unavailable.  |
| <b>Account Status</b> | <p>Indicates the status of the account:</p> <ul style="list-style-type: none"> <li>• <b>Active:</b> The account is currently active and accessible to the user.</li> <li>• <b>Locked:</b> The user has attempted to log on incorrectly too many times. When the account is locked, an Administrator can unlock the account by clicking the <b>[Unlock]</b> button that is displayed.</li> <li>• <b>Inactive:</b> The user has not logged in for longer than the inactivity period set in the Administrative User Account Properties dialog or the cluster property <code>logon.inactivityPeriod</code>. The Administrator can reactivate the account by clicking <b>[Activate]</b> button that is displayed.</li> </ul> <p>Inactive or Locked users cannot log into the Policy Manager.</p> <p>If the user account is expired or disabled, the last known state is displayed but the controls are unavailable. Authentication against</p> |

Table 87: User Properties - [General] tab

| Setting               | Description   |
|-----------------------|---|
|                       | <p>Expired or Disabled accounts will also fail in message traffic. However, authentication against Active, Inactive, and Unlocked user accounts will be successful for message traffic.</p> <p><b>Note:</b> In order to activate or unlock an account, the user must have the <a href="#">role</a> "Administrator" or any custom role with Update permission for the entity type "Users". For more information, see "Managing Roles" on page 130.</p>   |
| First Name            | Enter the user's first name. Note that this is different from the username, which cannot be modified.   |
| Last Name             | Enter the user's last name.   |
| Email                 | Enter the user's email address.   |
| Reset Password        | <p>Click this button if you need to change the user password. Enter the new password, then retype to confirm. <b>Note:</b> For an internal user, resetting the password can both unlock a locked account and reactivate an inactive account.</p> <p>When a password is reset by an administrator, or when a new account is created, some password rules are temporarily relaxed. The password created by the administrator must satisfy the password requirements; however, the following rules will be temporarily ignored:</p> <ul style="list-style-type: none"> <li>• Character difference</li> <li>• Password Repeat Frequency</li> <li>• Allow One Password Change Per 24 Hours</li> </ul> <p>To ensure that all password rules are met before users access the Gateway, be sure to select <b>[Force password change for new user and reset]</b> in your password policy. For more information see "Managing Password Policy" on page 48.</p> |
| Account Never Expires | Select this check box if the account is permanent. Clear this check box if the account should expire on a certain date.   |
| Expires on            | <p>If the account will expire, enter the date or use the drop-down calendar control to select a date. <b>Note:</b> If an account has expired, this field appears red with the word "Expired" beside it. Credentials will not be accepted for an expired user.</p> <p>Expired users in a service being consumed will be flagged in the <a href="#">Policy Validation Messages</a> window and the <a href="#">Gateway Audit Events</a> window.</p>  |

## Configuring the [Roles] Tab



This tab is used to add or remove internal users from [roles](#). At least one role must be set if the user will be logging in to the Policy Manager. **Note:** If no roles are assigned, the user's name and password will not be recognized on the login screen.

**Tip:** This tab is also used to assign roles to template users for [Policy-Backed Identity Providers](#). A template user may have a default role, which is shown on this tab. This default is removed when any other role is added manually. For more information about template users, see "Searching Identity Providers" on page 459.

The table at the top lists the roles currently assigned to the user:

- **Name:** The name of the role.
- **Type:** "System" indicates a role that is either predefined or automatically generated (see ""Predefined Roles and Permissions" on page 132"). "Custom" indicates a role that has been defined by your organization (see ""Managing Roles" on page 130").
- **Inherited:** "No" means the user is assigned to the role directly; "Yes" means the user is a member of a group that has been assigned to that role.

The Role properties section at the bottom displays the complete description for the selected role.

➤ *To add the user to a role:*

1. Click **[Add]**. A list of eligible roles is displayed.
2. Select the role(s) to which to add the user. **Tip:** To locate a role more easily, enter some text in the "Filter on name" box. This filters the roles list to display only those roles containing the filter text. Delete the filter text to restore the full list of roles.
3. Click **[Add]** to close the dialog.

➤ *To remove a user from a role:*

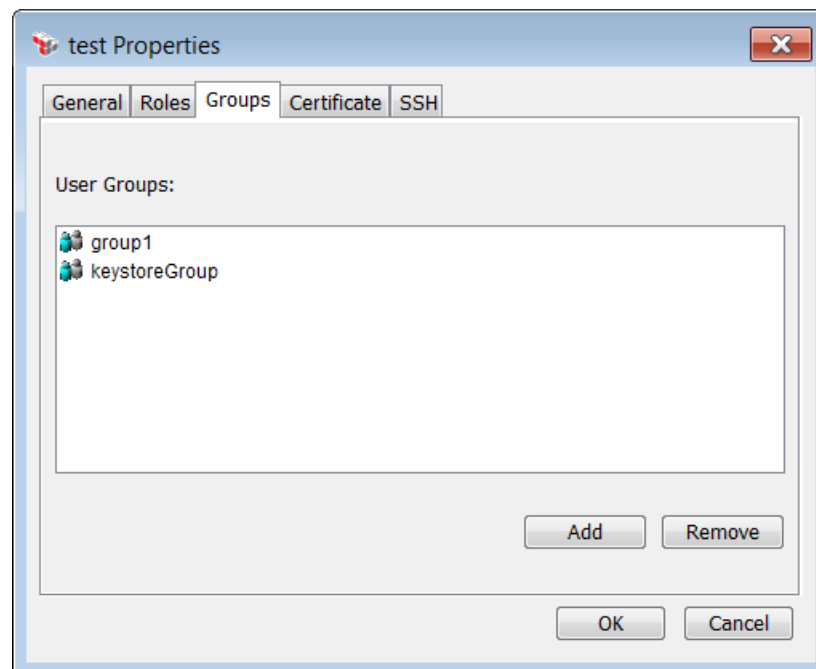
1. Select the role(s) to be removed from the user. Hold down the [Ctrl] key to select multiple roles. **Note:** You can only remove roles that are *not* inherited. To remove a user from an inherited role, remove the user from the group that has the role.
2. Click **[Remove]**.

---

**Notes:** (1) Users who need to log on to the Policy Manager must be assigned to at least one role. For more information, see "Managing Roles" on page 130. (2) If a role is both assigned and inherited, the interface will display "No" in the "Inherited" column and you are permitted to remove the role. Once removed, that role remains in the list, but the "Inherited" column changes to "Yes".

---

## Configuring the [Groups] Tab



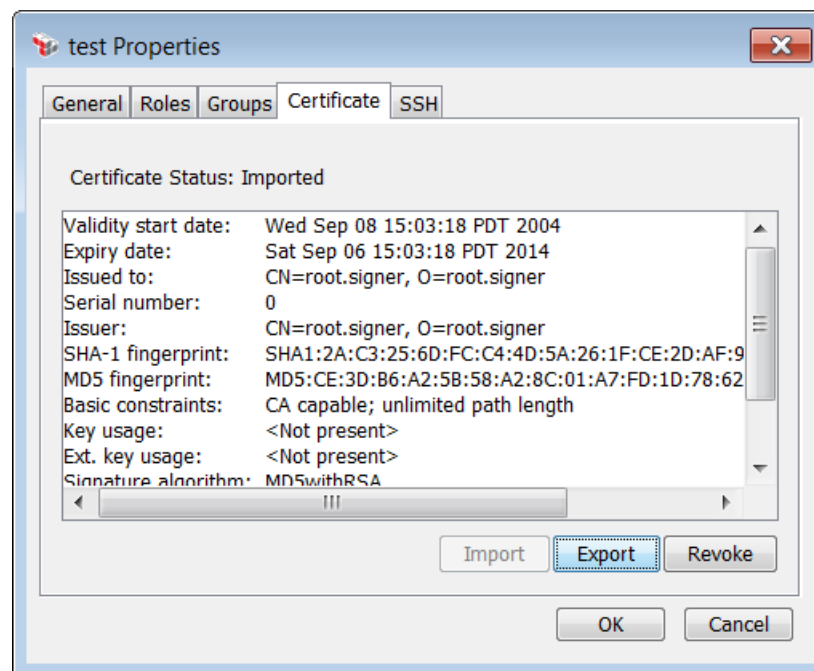
This tab is used to add or remove the user from [internal groups](#).

1. Click **[Add]**. A list of groups appear.
2. Select one or more groups that the user belongs to.

**Note:** If the group you want isn't in the list, define it first using the steps under ["Creating an Internal Group" on page 294](#).

3. Click **[Add]**. The user is added to the group.
4. If you need to remove a user from a group, select the group and then click **[Remove]**.

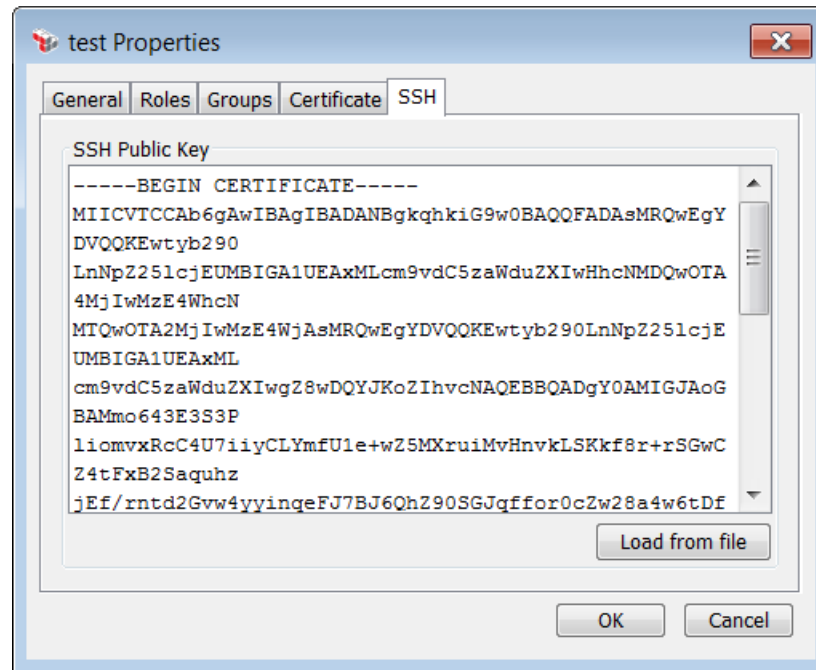
### Configuring the [Certificate] Tab



This tab is used to manage the certificate for the user.

- To import a certificate for the user, click **[Import]** and then complete the [Add Certificate Wizard](#).
- To export a certificate, click **[Export]** and then specify a file name and location.
- To revoke a certificate, click **[Revoke]** and then click **[OK]** to confirm. Revoking removes both the certificate and the user's password.

## Configuring the [SSH] Tab



This tab is used to upload the user's SSH public key into his or her user record in the Internal Identity Provider. During SSH processing, the inbound SSH server on the Gateway will then attempt to validate this public key when authenticating.

You can either paste the public key into the box or click **[Load from file]** to insert the key from a text file. The key may be in the RSA or DSA in PEM PKCS8 format.

For more information about SSH processing, see "Working with SCP/SFTP Messages" on page 206.

## Creating an Internal Group

Groups help you organize your users and they are a time-saving tool. For example, granting web service or XML application access to a group of users is much quicker than granting access individually.

➤ To add a new group to the Internal Identity Provider (IIP):

1. Do one of the following:
  - Click **Create Internal Group** on the [Home Page](#).
  - Click **[Tasks] > Create Internal Group** from the [Main Menu](#).
  - Right-click the IIP name in the **[Identity Providers]** tab and select **Create Group**.



The Create Internal Group dialog appears.

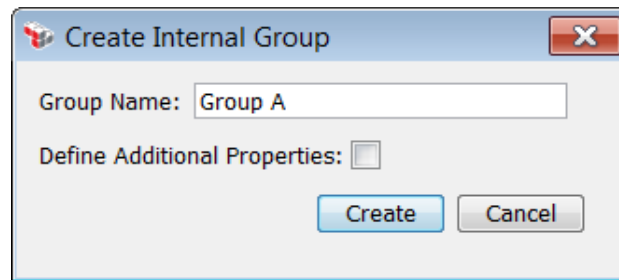


Figure 118: Create Internal Group dialog

2. Enter a name for the group in the **Group Name** field.
3. Select the **Define Additional Properties** check box if you wish to enter more information about the group. All additional information is optional.
4. Click [**Create**].
  - If you are not defining additional properties, the dialog closes and the group is added to the Internal Identity Provider.
  - If you are defining additional properties, the Properties dialog for the group is displayed. For more information about this dialog, see "Group Properties" on page 454.

## Group Properties

Every internal group or Federated group has a set of extended properties that can be set either when the group is first added to the system, or deferred until a later date. (During initial entry, only a minimal amount of group data is required, to facilitate rapid entry of many groups.)

Most properties for LDAP groups cannot be modified in the Policy Manager, with the exception being [roles](#).

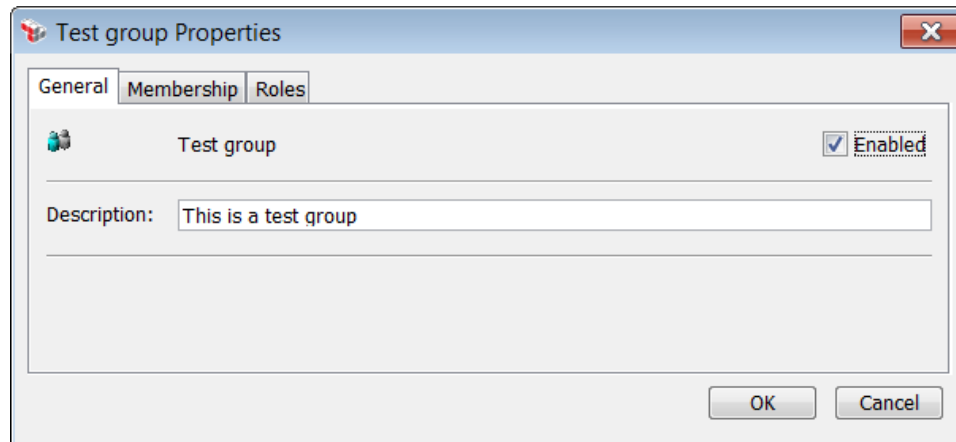
➤ *To access the properties for a group user:*

1. Do one of the following:
  - Create a new [internal or Federated group](#), making sure to select the **Define Additional Properties** check box.
  - [Edit](#) an existing internal or Federated group.
  - Locate the group by [searching the identity provider](#).

The Group Properties dialog appears.

3. Configure each tab within the properties as necessary, wherever possible. All information is optional. Refer to the appropriate section below for a complete description of each tab.
4. Click **[OK]** when done.

### Configuring the [General] Tab



This tab is used to enter additional basic information about the group.

- **Enabled:** *This applies to internal groups only.* Select this check box to enable the group. Clear this check box to disable the group.

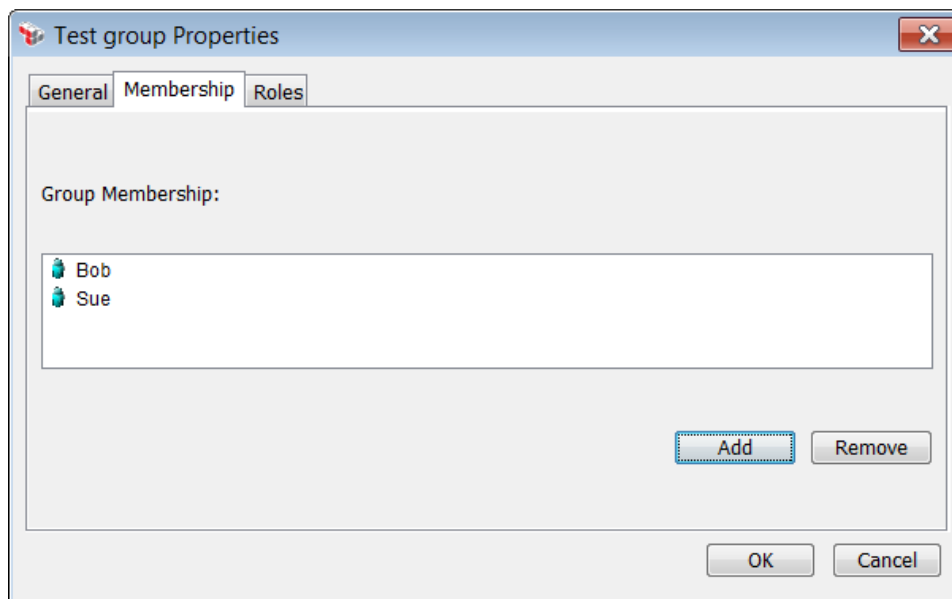
---

**Note:** When a group is disabled, it cannot be used to authenticate message traffic and its permissions are suspended. A user's set of permissions is a combination of his or her role assignments, plus any role assignments inherited from the group. When a group is disabled, the inherited assignments no longer apply. If a user has no other role assignments, then that user will no longer be able to [connect](#) to the Gateway using the Policy Manager.

---

- **Description:** Enter a description of the group.

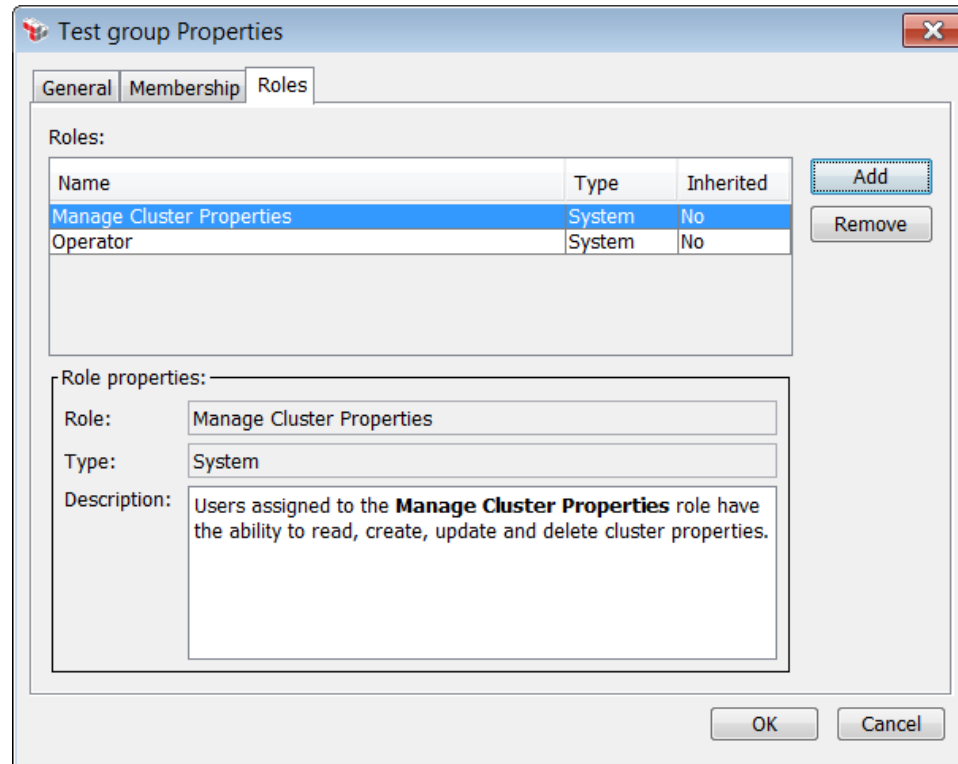
## Configuring the [Membership] Tab



This tab is used to add or remove users to or from the group.

1. Click [**Add**]. A list of eligible users not currently assigned to that group appears.
2. Select one or more users who should be added to the group. Hold down the [Ctrl] key to select multiple users.
3. Click [**Add**]. The user(s) are added to the group.
4. If you need to remove a user from the group, select the user and then click [**Remove**].

## Configuring the [Roles] Tab



This tab is used to add or remove groups from [roles](#). Roles may be assigned to internal or LDAP groups.

The table at the top lists the roles currently assigned to the group:

- **Name:** The name of the role.
- **Type:** "System" indicates a role that is either predefined or automatically generated (see ""Predefined Roles and Permissions" on page 132"). "Custom" indicates a user-defined role (see ""Managing Roles" on page 130").
- **Inherited:** "No" means the group is assigned to the role directly; "Yes" means the group is part of another group that is assigned to that role .

The Role properties section at the bottom displays the complete description for the selected role.

➤ *To add the group to a role:*

1. Click **[Add]**. A list of eligible roles is displayed.
2. Select the role(s) to which to add the group. **Tip:** To locate a role more easily, enter some text in the "Filter on name" box. This filters the roles list to display only those roles containing the filter text. Delete the filter text to restore the full list of roles.
3. Click **[Add]** to close the dialog.

➤ *To remove a user from a group:*

1. Select the role(s) to be removed from the group. Hold down the [Ctrl] key to select multiple roles. **Note:** You can only remove roles that are *not* inherited.
2. Click **[Remove]**.

---

**Note:** If a role is both assigned and inherited, the interface will display "No" in the "Inherited" column and you are permitted to remove the role. Once removed, that role remains in the list, but the "Inherited" column changes to "Yes".

---

## Editing or Deleting a User or Group

The Policy Manager lets you modify or delete the following:

- Any Internal Identity Provider (IIP) [user or group](#)
- Any Federated Identity Provider (FIP) [user, group, or virtual group](#)

For [LDAP Identity Provider](#) users or groups, you must use the associated external management program to edit or delete. You cannot perform these tasks in the Policy Manager.

---

**Notes:** Be sure the user or group being deleted no longer appears in any policy. At least one administrative Internal Identity Provider user must be present in the Policy Manager.

---

➤ *To edit or delete a user, group, or federated virtual group:*

1. Locate the user or group, as described under "Searching Identity Providers" on page 459.
2. Choose one of the following actions:

Table 88: Editing a User or Group actions

| Action               | Steps   |
|----------------------|---|
| <b>Modify a User</b> | 1. In the Search Results box, double-click the user name or select it |

| Action  | Steps  |
|---|--|
|   | <p>and then click <b>[Select]</b>. The user properties appear.</p> <ol style="list-style-type: none"> <li>2. Modify the properties as necessary. For more information, see "Internal User Properties" on page 288 or "Federated User Properties" on page 448.</li> </ol>   |
| <b>Modify a Group</b>                         | <ol style="list-style-type: none"> <li>1. In the Search Results box, double-click the group name or select it and then click <b>[Select]</b>. The group properties appear.</li> <li>2. Modify the properties as necessary. For a description of the fields, refer to <a href="#">Creating a Federated Group</a> or <a href="#">Creating an Internal Group</a>, depending on the type of group being edited.</li> </ol> |
| <b>Modify a Virtual Group</b>                 | <ol style="list-style-type: none"> <li>1. In the Search Results box, double-click the federated virtual group name or select it and then click <b>[Select]</b>. The virtual group properties appear.</li> <li>2. Modify the properties as necessary. For a description of the fields, refer to <a href="#">Creating a Federated Virtual Group</a>.</li> </ol>  |
| <b>Delete a User, Group, or Virtual Group</b> | <ol style="list-style-type: none"> <li>1. Select the user, group, or virtual group to delete.</li> <li>2. Click <b>[Delete]</b>, then click <b>[OK]</b> to confirm.</li> </ol> <p>You cannot delete a user, group, or virtual group that is still in use in a policy.</p>  |

## Internal Identity Provider Wizard

The Gateway comes preconfigured with an Internal Identity Provider as the authentication database. You cannot remove or duplicate this provider, but you can set how the identity provider validates certificates when they are used during authentication.

➤ *To access the Internal Identity Provider Wizard:*

- In the [\[Identity Providers\] tab](#) on the Policy Manager [interface](#), right-click **Internal Identity Provider** and then select **Properties**. The Internal Identity Provider Wizard appears.

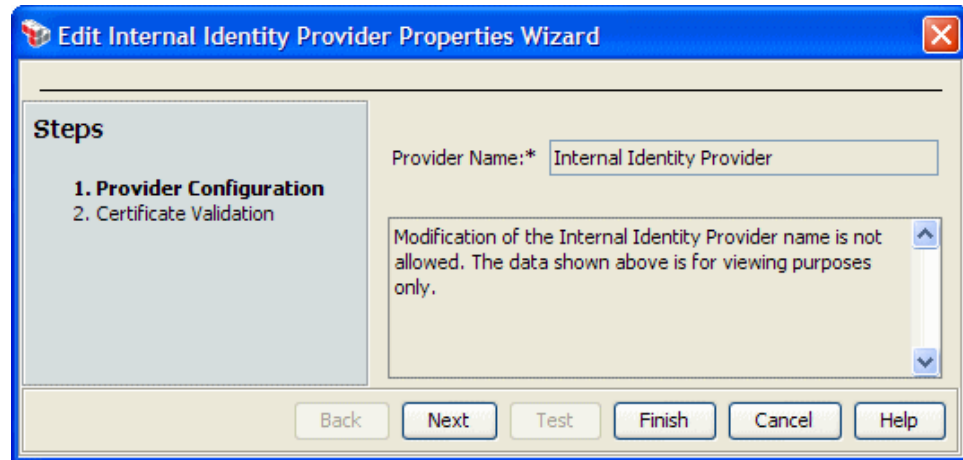


Figure 119: Internal Identity Provider Wizard

There are two steps to this wizard:

- Step 1 displays the preconfigured name for this provider. The name cannot be changed.
- Step 2 lets you specify how Internal Identity Provider certificates should be validated. By default, the method defined for Identity Providers in the [Manage Certificate Validation](#) dialog is used. To override this default, select another validation option from the drop-down list. For a description of each option, see "Managing Certificate Validation" on page 251.

## Managing Administrative User Account Policy

An administrative user is a person with an account on the Policy Manager that allows them access to the Gateway.

There are two types of administrative users:

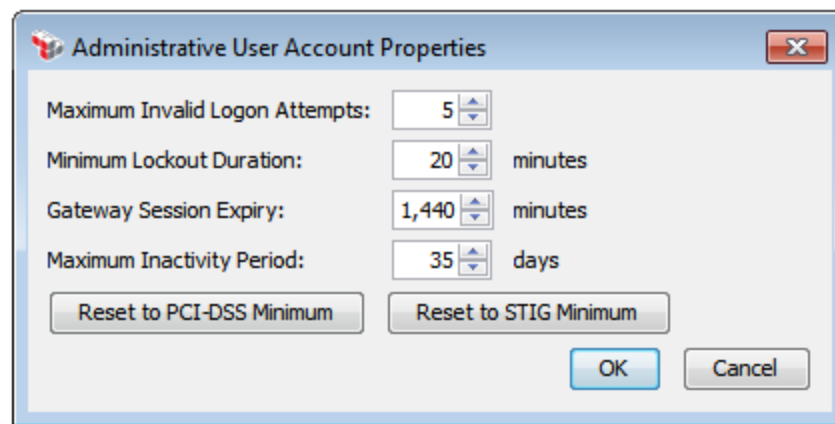
- **Internal:** Users who are entered into and maintained through the Gateway. For more information, see "Internal Identity Provider Users and Groups" on page 286.
- **LDAP:** Users who have access to the Gateway, but their information and details are maintained in an external LDAP directory. Their account status is set in the LDAP directory and is not viewable in Policy Manager. For more information on LDAP users, see "LDAP Identity Providers" on page 303.

In order to modify the account properties for administrative users, you must be assigned either the 'Administrator' or the 'Manage Administrative Accounts Configuration' role. For more information about roles, see "Predefined Roles and Permissions" on page 132.

➤ To manage administrative users:

1. In the Policy Manager, select **Tasks > Manage Account Policies > Manage Administrative User Account Policy** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu).

The Administrative User Account Properties dialog displays.



The dialog box titled "Administrative User Account Properties" contains four settings, each with a numeric input field and a unit label:

- Maximum Invalid Logon Attempts:** Input field shows 5.
- Minimum Lockout Duration:** Input field shows 20, followed by "minutes".
- Gateway Session Expiry:** Input field shows 1,440, followed by "minutes".
- Maximum Inactivity Period:** Input field shows 35, followed by "days".

At the bottom, there are two buttons: "Reset to PCI-DSS Minimum" and "Reset to STIG Minimum". At the bottom right are "OK" and "Cancel" buttons.

Figure 120: Administrative User Account Properties

2. Configure this dialog as follows:

Table 89: Administrative user account settings

| Setting                               | Description   |
|---------------------------------------|---|
| <b>Maximum Invalid Logon Attempts</b> | <p>Select the maximum number of failed login attempts before the account is locked.</p> <p>Choose a number between 1 and 20. The default is <b>5</b> attempts.</p> <p>For more information on unlocking locked accounts, see "Creating an Internal User" on page 286.</p> |
| <b>Minimum Lockout Duration</b>       | <p>Choose the number of minutes a user must wait to attempt to log on again after reaching the maximum number of invalid logon attempts. The options are from 1 to 1440 minutes (one day). The default is <b>20</b> minutes.</p>  |
| <b>Gateway Session Expiry</b>         | <p>Set the number of minutes, between 1 and 1440, that the administrative user can leave a Gateway session idle before being disconnected. The default is <b>30</b> minutes.</p>  |
| <b>Maximum Inactivity</b>             | <p>Set the number of days, between 1 and 365, that an account can be</p>  |



| Setting                         | Description   |
|---------------------------------|---|
| <b>Period</b>                   | inactive before it disables. The default is <b>35</b> days.<br><br><b>Note:</b> Users assigned the role of 'Administrator' are exempt from this inactivity timeout. For more information on roles, see "Predefined Roles and Permissions" on page 132.  |
| <b>Reset to PCI-DSS Minimum</b> | Click to reset all the administrative user account settings to meet the minimum acceptable level for PCI-DSS (Payment Card Industry Data Security Standard).<br><br><b>Tip:</b> If you subsequently change any setting that invalidates the PCI-DSS minimum, you will be prompted to confirm when clicking <b>[OK]</b> to dismiss the dialog box. |
| <b>Reset to STIG Minimum</b>    | Click to reset all the administrative user account settings to meet the minimum acceptable level for STIG (Secure Technical Implementation Guide ).<br><br><b>Tip:</b> If you subsequently change any setting that invalidates the STIG minimum, you will be prompted to confirm when clicking <b>[OK]</b> to dismiss the dialog box.             |

3. Click **[OK]** when done.

## LDAP Identity Providers

The Policy Manager allows you to base your LDAP connector configuration on a pre-defined template. Four templates are available at installation:

- Oracle (Oracle Internet Directory)
- TivoliLDAP (Tivoli Access Manager)
- MSAD (Microsoft Active Directory)
- GenericLDAP

The Policy Manager supports the LDAP 3.0 standard.

## Simple LDAP Identity Providers

The Policy Manager also supports Simple LDAP Identity Providers. This is designed for users who wish to use an existing LDAP server to authenticate requests to the CA API Gateway, but who do not want (or are not able) to configure mappings for users, groups, certificates, etc. The Simple LDAP Identity Provider only requires a DN pattern; the Gateway will use the user name provided by the client and attempt to do a bind with the client-provided password.

## LDAP Identity Provider Users and Groups

To add users and groups to an LDAP Identity Provider, you must use the tools provided with your LDAP directory. The Policy Manager cannot be used to add, edit, or delete LDAP Identity Provider users and groups. The reason for this is that the LDAP Identity Provider defined in the Policy Manager is only a connector to an existing LDAP directory.

## Creating an LDAP or Simple LDAP Identity Provider

Follow the appropriate instructions below to create an [LDAP Identity Provider](#) or a [Simple LDAP Identity Provider](#).

---

**Note:** An LDAP Identity Provider is only a connector to an existing LDAP directory. For this reason, the Policy Manager cannot be used to create, edit, or delete LDAP Identity Provider users or groups. To do so, you must use the tools provided with your LDAP directory.

---

➤ *To add a new LDAP Identity Provider in the Policy Manager:*

1. Do one of the following:
  - Click **Create LDAP Identity Provider** on the [Home Page](#).
  - Click **[Tasks] > Create Identity Provider > Create LDAP Identity Provider** from the [Main Menu](#).
  - Right-click the "Identity Providers" title at the top of the **[Identity Providers]** tab. A drop-down menu appears. Select **Create LDAP Identity Provider**.
2. Complete the [LDAP Identity Provider](#) wizard. The new LDAP Identity Provider is added to the **[Identity Providers]** tab.

➤ *To add a new Simple LDAP Identity Provider in the Policy Manager:*

1. Do one of the following:
  - Click **Create Simple LDAP Identity Provider** on the [Home Page](#).
  - Click **[Tasks] > Create Identity Provider > Create Simple LDAP Identity Provider** from the [Main Menu](#).
  - Right-click the "Identity Providers" title at the top of the **[Identity Providers]** tab. A drop-down menu appears. Select **Create Simple LDAP Identity Provider**.
2. Complete the [LDAP Identity Provider](#) wizard. The new Simple LDAP Identity Provider appears in the **[Identity Providers]** tab.

## Cloning an LDAP or Simple LDAP Identity Provider

A quick method to create a new *LDAP Identity Provider* is to clone an existing one. After cloning, simply update the appropriate settings. Note that the cloned identity provider has no connection to the original once it has been created.

➤ *To create a new LDAP or Simple LDAP Identity Provider based on an existing one:*

1. In the **[Identity Providers]** tab, right-click the LDAP or Simple LDAP identity provider you wish to clone.
2. Select **Clone Identity Provider**.
3. Complete the [LDAP Identity Provider](#) or [Simple LDAP Identity Provider](#) wizard by updating the settings as required. The new identity provider is added to the **[Identity Providers]** tab.

## Editing an LDAP or Simple LDAP Identity Provider

➤ *To modify the details of an [LDAP Identity Provider](#) or [Simple LDAP Identity Provider](#):*

1. Do one of the following:
  - In the [\[Identity Providers\] tab](#), double-click the name of the LDAP Identity Provider or Simple LDAP Identity Provider to edit. The appropriate wizard is displayed.
  - In the **[Identity Providers]** tab, right-click the LDAP Identity Provider or Simple LDAP Identity Provider to edit and then select **Properties**. The appropriate wizard is displayed.
2. Follow the steps in the wizard to make the appropriate changes.

## Deleting an LDAP or Simple LDAP Identity Provider

➤ To delete an [LDAP Identity Provider](#) or [Simple LDAP Identity Provider](#) from the Policy Manager:

1. In the [\[Identity Providers\] tab](#), right-click the LDAP Identity Provider or Simple LDAP Identity Provider to delete and then select **Delete**.
2. Click **[Yes]** to confirm. The identity provider is removed.

---

**Note:** You cannot delete an LDAP Identity Provider that has users and groups still attached to the policy. To delete the LDAP Identity Provider, you must first remove the LDAP Identity Provider users and groups from all policies.

---

## LDAP Identity Provider Wizard

The *LDAP Identity Provider Wizard* helps you add or edit an [LDAP Identity Provider](#) in the Federated Gateway B.

For more information on using wizards, see "[Wizards](#)" in "Interfaces" on page 13.

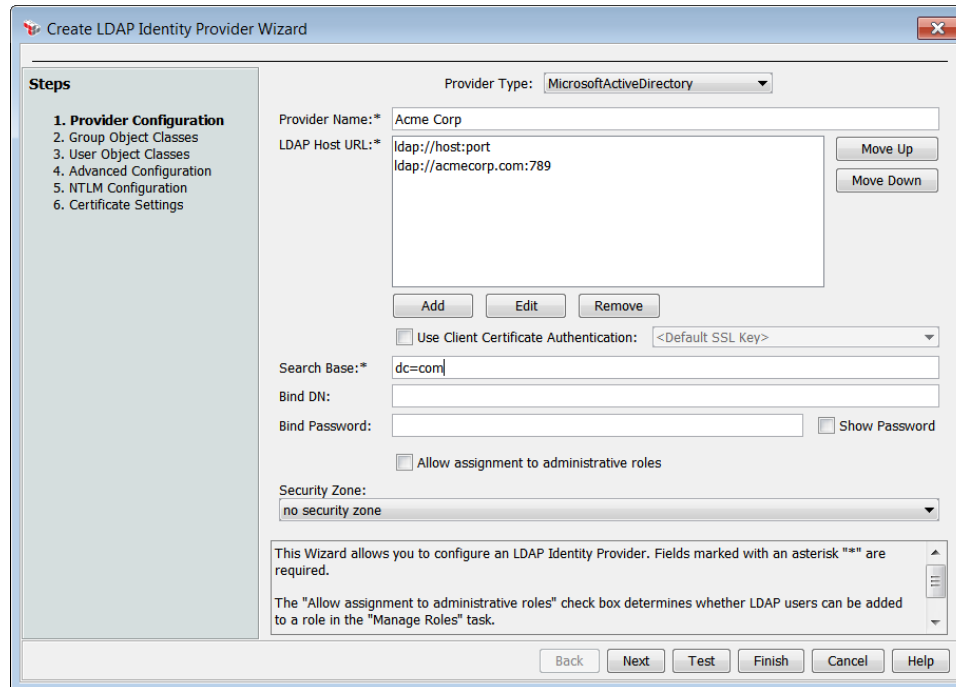
---

**Tip:** When the **[Test]** button is available, you can click it to test your configuration at any time.

---

### Step 1: Provider Configuration

This step defines the LDAP Identity Provider details.



**Create LDAP Identity Provider Wizard**

**Steps**

1. Provider Configuration
2. Group Object Classes
3. User Object Classes
4. Advanced Configuration
5. NTLM Configuration
6. Certificate Settings

Provider Type: **MicrosoftActiveDirectory**

Provider Name:\* Acme Corp

LDAP Host URL:\*  
 ldap://host:port  
 ldap://acmecorp.com:789

Move Up  
Move Down

Add Edit Remove

☐ Use Client Certificate Authentication: <Default SSL Key>

Search Base:\* dc=com

Bind DN:

Bind Password:  ☐ Show Password

☐ Allow assignment to administrative roles

Security Zone:  
no security zone

This Wizard allows you to configure an LDAP Identity Provider. Fields marked with an asterisk "\*" are required.

The "Allow assignment to administrative roles" check box determines whether LDAP users can be added to a role in the "Manage Roles" task.

Back Next Test Finish Cancel Help

Figure 121: LDAP Identity Provider Wizard - Step 1

Configure this step as follows:

1. Select the LDAP Identity Provider type from the **Provider Type** drop-down list.
2. Complete the following details. Fields marked with an asterisk (\*) are required.
  - **Provider Name:** Enter a descriptive name for the LDAP Identity Provider. This name will appear in the **[Identity Providers]** tab and on the Search Identity Providers dialog.
  - **LDAP Host URL:**
    - Click **[Add]** to enter the URL of the LDAP or LDAPS directory service you want to connect to—for example, `ldap://oracle.companyx.com:389` or `ldaps://oracle.companyx.com:636`

---

**Note:** When configuring using the IPv6 address space, the host URL must be enclosed within "[ ]" if a literal IPv6 address is used, for example:

`ldap://oracle.companyx.com:389` (no brackets required)

`ldap://[2222::22]:389` (brackets required)

---

- Click **[Remove]** to remove a URL from the list.
- Use **[Move Up]** and **[Move Down]** to change the order of the URLs.

- **Use Client Authentication:** Select this check box to present a certificate to the server during the SSL handshake, if one is requested. Clear this check box to never present a certificate, even if one is requested. Note that access may be denied in this case.

---

**Note:** When Client Authentication is enabled, it is used with the specified key when connecting to an LDAP server for any LDAP(S) connections. If there are no LDAP(S) connections, then the Client Certification options will have no effect.

---

- **Keystore:** From the drop-down list, select the keystore from which to retrieve the certificate. Used only if client certificates are used.
- **Search Base:** Enter the search base for users and groups in the LDAP—for example, *dc=companyx,dc=com*.
- **Bind DN:** Optionally enter a binding DN (Distinguished Name) identity for authenticating access to the LDAP directory—for example, *cn=manager*.
- **Bind Password:** Optionally enter a password if you entered a bind DN identity.
- **Allow assignment to administrative roles:** Select this check box to allow LDAP users to be assigned to [roles](#). Clear this check box to prevent the LDAP repository from being searched.

---

**IMPORTANT:** Clearing the **Allow assignment to administrative roles** check box will prevent any LDAP users who are currently assigned to a role from being able to log in.

---

- **Security Zone:** Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "**No security zone**". For more information about security zones, see [Understanding Security Zones](#) in the *Layer 7 Policy Manager User Manual*. **Note:** This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).

## Step 2: Group Object Classes

This step defines LDAP group object classes for the provider defined in Step 1.

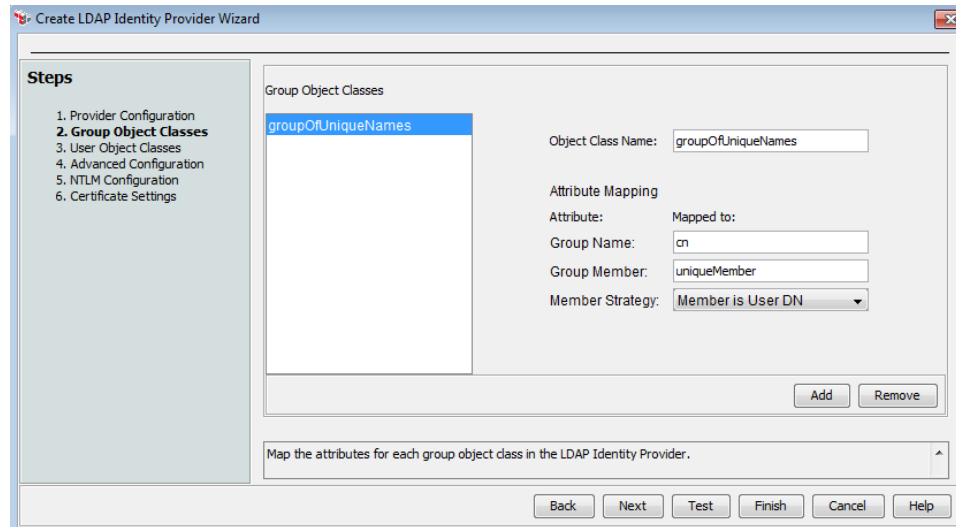


Figure 122: LDAP Identity Provider Wizard - Step 2

The wizard automatically populates default object classes based on the provider type. Review and modify as necessary.

---

**Note:** If unsure, you should consult your LDAP Identity Provider for information about supported group object classes and attribute mapping details before modifying this list.

---

- **Group Object Classes:** Select a group object class to see its details. To add a new class, click **[Add]** and then complete the fields below. To remove a class from the list, select it and then click **[Remove]**.
- **Object Class Name:** Enter the name of the group object class.

Map the attributes required by the group object class as described below. Mapping group object class attributes associates a Gateway attribute with the corresponding attribute in the LDAP schema.

- **Group Name:** Enter the attribute of the group object class that specifies the group name. For example, a "cn" attribute specifies the name of the group in the "groupOfUniqueNames" group object class.
- **Group Member:** Enter the attribute of the group object class that specifies the members of the group. For example, a "uniqueMember" attribute specifies the members of the group in the "groupOfUniqueNames" group object class.
- **Member Strategy:** Select a member strategy to use from the drop-down list. See Table 90 below for a description of each strategy.

### Step 3: User Object Classes

This step defines LDAP user object classes for the provider defined in Step 1.

Figure 123: LDAP Identity Provider Wizard - Step 3

The wizard automatically populates default object classes based on the provider type. Review and modify as necessary.

**Note:** If unsure, you should consult your LDAP Identity Provider for information about supported user object classes and attribute mapping details before modifying this list.

- **User Object Classes:** Select a user object class to see its details. To add a new class, click **[Add]** and then complete the fields below. To remove a class from the list, select it and then click **[Remove]**.
- **Object Class Name:** Enter the name of the user object class.

Map the attributes required by the user object class as described below. Mapping user object class attributes associates a Gateway attribute with the corresponding attribute in the LDAP schema.

- **User Name:** Enter the attribute of the user object class that specifies the user name. For example, the "cn" attribute specifies the name of the user in the "inetOrgPerson" user object class.
- **Login Name:** Enter the attribute of the user object class that specifies the user login name. For example, the "uid" attribute specifies the login name in the "inetOrgPerson" user object class.



---

**Tip:** If you are using MSAD (Microsoft Active Directory) as the LDAP provider and you need to support login names greater than 20 characters, change the mapping to **"userPrincipalName"**.

---

- **Password:** Enter the attribute of the user object class that specifies the user password. For example, the "userPassword" attribute specifies the user password in the "inetOrgPerson" user object class.
- **First Name:** Enter the attribute of the user object class that specifies the first name of the user. For example, the "givenName" attribute specifies the first name of the user in the "inetOrgPerson" user object class.
- **Last Name:** Enter the attribute of the user object class that specifies the last name of the user. For example, the "sn" attribute specifies the last name of the user in the "inetOrgPerson" user object class.
- **Email:** Enter the attribute of the user object class that specifies the user's email address. For example, the "mail" attribute specifies the user's email address in the "inetOrgPerson" user object class.
- **Certificate:** Enter the attribute of the user object class that contains the user's X.509 certificate. For example, the "userCertificate;binary" attribute specifies the user's X.509 certificate in the "inetOrgPerson" user object class. The wizard will prepopulate this value for known certificates such as MSAD, OpenLDAP.

This mapping enables certificates stored in the LDAP repository to be used by the Gateway at run time, rather than requiring you to first import the certificate into the Gateway's certificate store. All LDAP Identity Providers are periodically indexed for new certificates based on the interval specified by the [ldap.certificateIndex.interval](#) cluster property.

- **Kerberos Principal:** Enter the attribute of the user object class that specifies the unqualified standard principal name for the user. A standard principal name is in the form "user@REALM"; for this example name, the attribute value would be "user". The default is **sAMAccountName**.
- **Kerberos Enterprise Principal:** Enter the attribute of the user object class that specifies the unqualified enterprise principal name for the user. An enterprise principal name is in the form "user@domain@REALM"; for this example, the attribute value would be "user@domain". The default is **userPrincipalName**.

At this point, test the configuration before clicking **[Finish]** to close the wizard. See ["Testing the Configuration"](#) below for details.

## Step 4: Advanced Configuration

This step contains advanced settings that may improve performance during LDAP directory lookups.

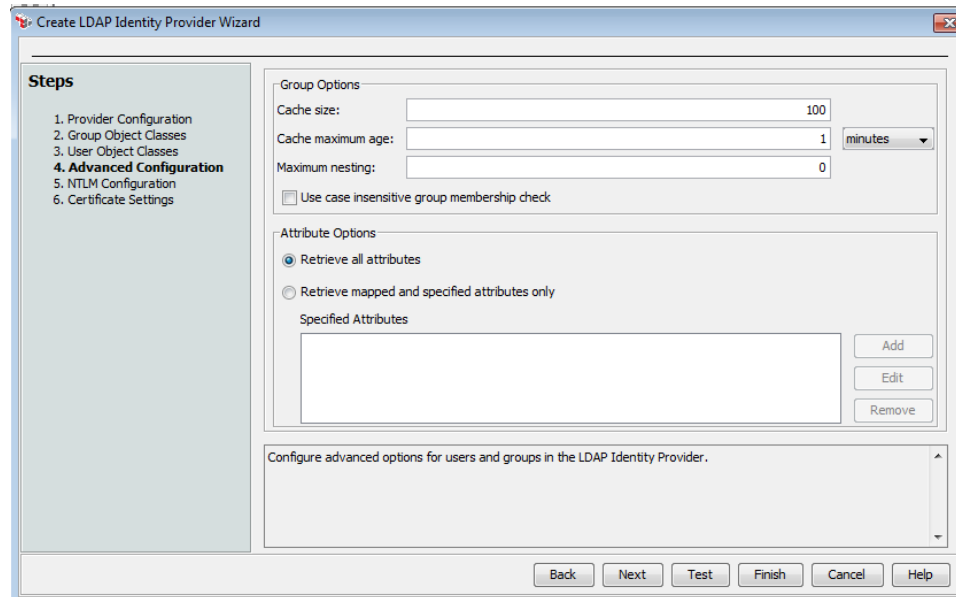


Figure 124: LDAP Identity Provider Wizard - Step 4

These settings are intended for advanced users experienced in LDAP directory configuration. Please consult your LDAP administrator before changing any of the settings.

There are two sections in this step:

- **Group Options:** Used to configure group caching and nesting.
  - **Cache size:** Enter the maximum number of groups to cache. For LDAP identity providers created prior to version 5.2, the default cache size is "0"(caching is disabled). For new LDAP identity providers, the default cache size is **100**.

---

**Tips:** The cache size should be based on the number of groups in frequent use. Using an abnormally large cache size will actually decrease system performance. For very large number of groups or when groups are used infrequently, consider disabling the cache.

---

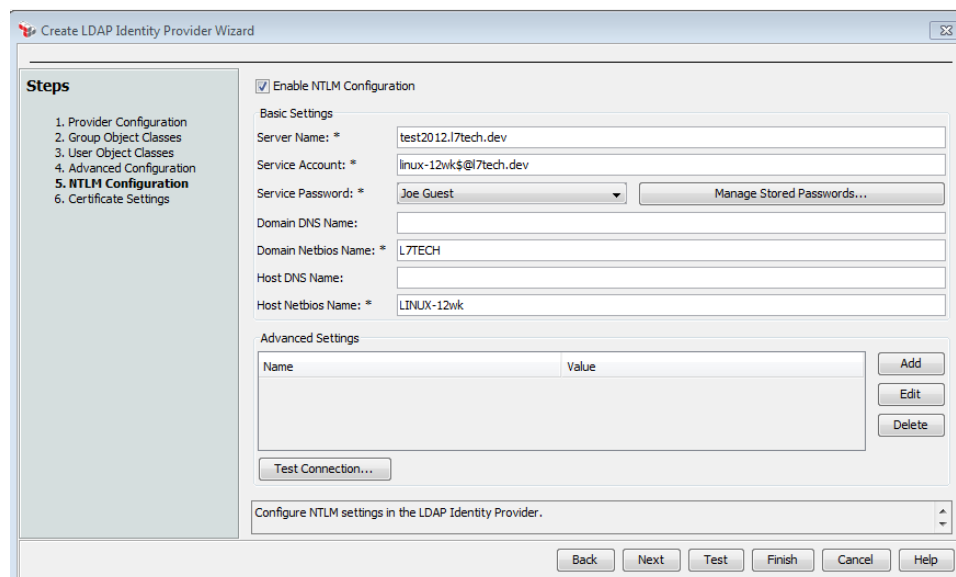
- **Cache maximum age:** Specify how long to cache each group before the information is discarded.

- **Maximum nesting:** Enter the number of nested groups to process. A nested group is a group that is a member of another group. You can enter "0" for unlimited group nesting or "1" to disable nesting if nested groups are not used. **Note:** Having many levels of group nesting can slow down authentication.
- **[Use case insensitive group membership check]:** Select this option to have the Policy Manager ignore case when checking for group membership.
- **Attribute Options:** Used to configure the extra attributes to retrieve, or to select all attributes for retrieval. You can use the Extract Attributes for Authenticated User assertion to retrieve the available attributes .
  - **Retrieve all attributes:** This option will retrieve all LDAP attributes. This setting is the default for LDAP identity providers created prior to version 5.2.
  - **Retrieve mapped and specified attributes only:** This option lets you specify which attributes to retrieve.
    - To enter an attribute, click **[Add]** and then type the name of the attribute to retrieve.
    - To modify an attribute, select the attribute and then click **[Modify]**.
    - To remove an attribute from the list, select the attribute and then click **[Remove]**.

## Step 5: NTLM Configuration

This step is used to enable NTLM configuration.

**Click to show/hide image**



The screenshot shows the 'Create LDAP Identity Provider Wizard' dialog box, specifically the '5. NTLM Configuration' step. The 'Steps' pane on the left lists the progression from Provider Configuration to Certificate Settings, with '5. NTLM Configuration' currently selected. The main area has a checkbox for 'Enable NTLM Configuration' which is checked. Below this, the 'Basic Settings' section contains fields for 'Server Name' (test2012.l7tech.dev), 'Service Account' (linux-12wk\$@l7tech.dev), 'Service Password' (Joe Guest), 'Domain DNS Name', 'Domain Netbios Name' (L7TECH), 'Host DNS Name', and 'Host Netbios Name' (LINUX-12wk). The 'Advanced Settings' section features a table with 'Name' and 'Value' columns, and 'Add', 'Edit', and 'Delete' buttons. A 'Test Connection...' button is also present. At the bottom, there is a text box for 'Configure NTLM settings in the LDAP Identity Provider.' and a row of navigation buttons: Back, Next, Test, Finish, Cancel, and Help.

Figure 125: LDAP Identity Provider Wizard - Step 5

There are two sections in this step:

- **Basic Settings:** Used to configure the NTLM configuration settings. Fields marked with an asterisk (\*) are required.
  - **Server Name:** Enter the DNS name of the server that is performing the NTLM client authentication.
  - **Service Account:** The computer account that has a trusted delegation to call a Netlogon service via the NTLM protocol.
  - **Service Password:** Choose the service password from the drop-down list. If the password you require is not listed, click **[Manage Stored Passwords]** to add it to the Gateway's password storage. For more information, see "Managing Stored Passwords" on page 42.

---

**Tip:** You cannot type the password directly here; it must be defined in the Gateway's [secure password storage](#).

---

- **Domain DNS Name:** Optionally, enter the DNS name of the authenticating domain.
- **Domain Netbios Name:** Enter the Windows name of the authenticating domain.
- **Host DNS Name:** Enter the DNS name of the host. In most cases, this is the CA API Gateway.
- **Host Netbios Name:** Enter the required Windows name of the computer account.

Once the Basic Settings are complete, you can either click **[Test Connection]** to verify the NTLM configuration or click **[Next]** to proceed to step 6.

- **Advanced Settings:** This section is used to add, edit, or remove any additional settings required to configure the NTLM protocol. This section is intended for advanced users and should be configured only as directed by [CA Technical Support](#).

### Error Conditions

The following error conditions can be returned by the CA API Gateway:

- **401 - Unauthorized:** This indicates that NTLM data was not present or not accepted yet.
- **402 - Authentication Failed:** This indicates that the client has presented invalid credentials.

## Step 6: Certificate Settings

This step is used to configure certificate settings for the LDAP identity provider.

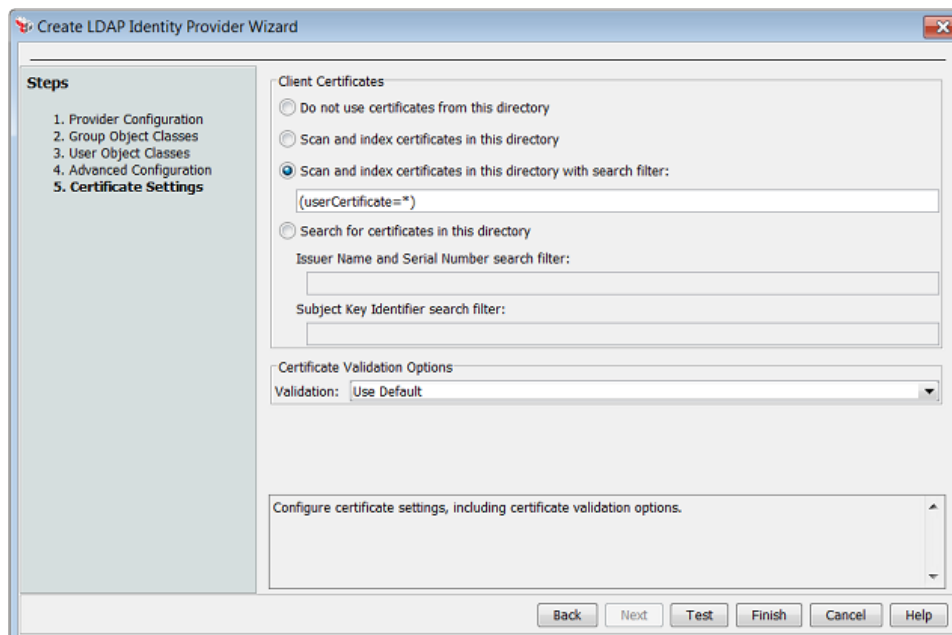


Figure 126: LDAP Identity Provider Wizard - Step 6

### Client Certificates

Select how certificates are used in an LDAP:

- **Do not use certificates from this directory:** Choose this option if certificates are not used from this directory.
- **Scan and index certificates in this directory:** Choose this option if certificate indexing should be enabled.
- **Scan and index certificates in this directory with search filter:** Choose this option if custom certificate indexing should be enabled. Enter the search filter for extracting the certificates from the directory.

An example of a simplistic filter for a single certificate attribute:

```
(<USER_CERTIFICATE_ATTRIBUTE>=*)
```

An example of a simplistic filter for multiple certificate attributes:

```
( | (<USER_CERT_ATTRIB1>=*) (<USER_CERT_ATTRIB2>=*) ... )
```

---

**Note:** The attributes returned from the search will be only the user certificate attributes. The search filter is included in the testing when the [Test] button is clicked.

---

- **Search for certificates in this directory:** Choose this option if certificate lookup should be enabled. You can search for certificates based on:
  - **Issuer Name and Serial Number** or **Subject Key Identifier.** The following variables can be used:
    - `${issuer}` : Issuer name in default format
    - `${issuer.canonical}` : Issuer name in canonical format
    - `${issuer.rfc2253}` : Issuer name in RFC 2253 format
    - `${serialNumber}` : Serial number
  - **Subject Key Identifier.** The following variables can be used:
    - `${subjectKeyIdentifier}` : Subject Key Identifier in Base 64 format
    - `${subjectKeyIdentifier.hex}` : Subject Key Identifier in hexadecimal string format

---

**Note:** The [Test] button will only validate the syntax of the search filters. It cannot fully test the search string because actual values are not available to insert into the filter.

---

#### Examples of search filters

The following filter finds an object that has a userCertificate attribute based on serial number and issuer if the directory supports RFC4523:

```
(&( objectclass = inetOrgPerson )( userCertificate = {
serialNumber ${serialNumber}, issuer "${issuer}" } ))
```

You could use the following syntax for either Open LDAP or Oracle Internet Directory 10g Release 2 or later:

```
(&( objectclass = inetOrgPerson )(
usercertificate=${serialNumber}${issuer} ))
```

Note that '\$' is the separator for *serialNumber* and *issuer*.

#### W A R N I N G :

The search string examples shown above include spaces to enhance readability. Actual search strings should not contain any spaces, except between name/values such as `serialNumber ${serialNumber}`.

#### Certificate Validation Options

This section specifies how certificates for this LDAP Identity Provider should be validated:

- **Use Default:** Use the method defined for Identity Providers, as described under "Managing Certificate Validation" on page 251.
- **Validate:** Ensure that the certificate is valid and trusted.
- **Validate Certificate Path:** Ensure that the certificate path is valid to a [trust anchor](#).
- **Revocation Checking:** Validate the certificate path *and* perform revocation checking according to the revocation checking policies.

## Member Strategies

The following table describes the different member strategies available. These strategies are used in Step 2 of the wizard.

Table 90: Member Strategies

| Strategy                    | Description  | Complications  |
|-----------------------------|--|--|
| <b>Member is User DN</b>    | Every value of the group's member attribute is a fully-formed DN (distinguished name) that is unique within the search base. | When selected, the corresponding attribute in the Group Member field should be something like "cn=user,dc=companyx,dc=com".  |
| <b>Member is User Login</b> | Every value of the group's member attribute is a unique attribute of a user in the directory.                                | When selected, the corresponding attribute in the Group Member field should be "user".   |
| <b>Member is NV Pair</b>    | Every value of the group's member attribute is a name=value pair such as "firstinitiallastname."                             | When selected, the corresponding attribute in the Group Member field should be "cn=user".  |
| <b>OU Group</b>             | If configuring an "organizationalUnit" group object class, then you must associate users to a group.                         | When an "ou" attribute is entered in the Group Name field, the membership of a user is not described in the group itself but rather by the DN (distinguished name) of the user. For example, the Group Name attribute "ou=group,dc=companyx,dc=com" hints at what the members are, but if you come across a user "cn=user,ou=group,dc=companyx,dc=com," then "user" is a member of that group. When selected, no attribute in the Group Member field is required because the group members |

| Strategy | Description | Complications  |
|----------|-------------|--|
|          |             | are implied by their DN, and if their DN includes the "ou", then the members are automatically considered part of the group. |

## Testing the Configuration

Click **[Test]** to verify the configuration before completing the wizard. You should see a message validating the configuration of the LDAP Identity Provider. If an error message displays instead, note the configuration problems and take the appropriate corrective actions:

Table 91: Troubleshooting LDAP configuration problems

| Configuration Error                    | Suggested Solution   |
|--|--|
| <b>Connection error</b>                | Return to Step 1 of the wizard and verify that all connection details are correct.   |
| <b>Group member retrieval warnings</b> | Either return to Step 2 of the wizard and adjust the group object class mappings, or you can leave the mappings as they are. Even with the warning, the Gateway will still be able to connect to the LDAP Identity Provider. |
| <b>User retrieval error</b>            | Return to Step 3 of the wizard and fix the incorrect user object class mappings.   |

Repeat the testing and fixing until no more errors appear. If you have difficulty resolving the errors, [contact](#) CA Technical Support for assistance.

The new LDAP Identity Provider appears in the [\[Identity Providers\] tab](#).

Click **[Finish]** when done.



## Simple LDAP Identity Provider Wizard

The *Simple LDAP Identity Provider Wizard* helps you [create](#) or [edit](#) a [Simple LDAP Identity Provider](#).

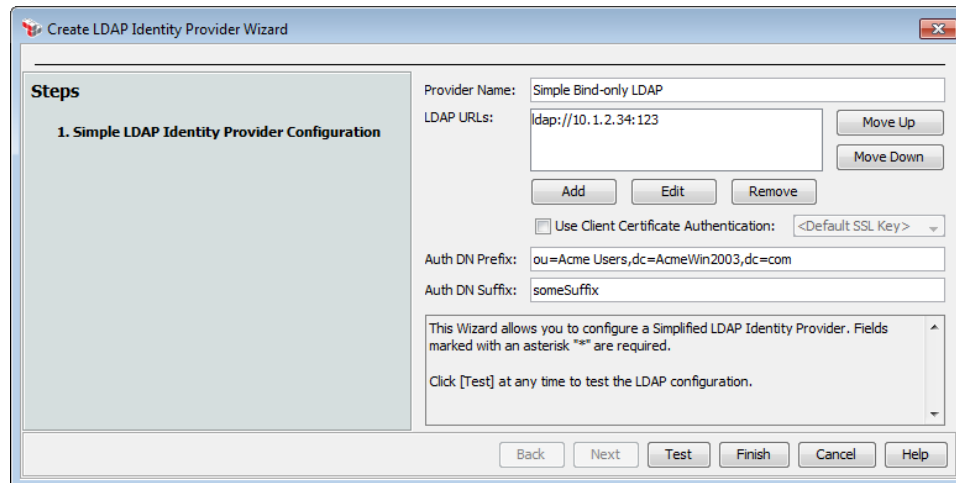


Figure 127: Simple LDAP Identity Provider Wizard

Complete the wizard step as follows:

Table 92: Configuring the Simple LDAP Identity Provider Wizard

| Setting                          | Description   |
|----------------------------------|---|
| <b>Provider Name</b>             | Enter a descriptive name for the LDAP Identity Provider. This name will appear in the [Identity Providers] tab and on the <a href="#">Search Identity Providers</a> dialog.   |
| <b>LDAP URLs</b>                 | <ul style="list-style-type: none"> <li>Click <b>[Add]</b> to enter the URL of the LDAP or LDAPS directory service you want to connect to.</li> <li><b>Note:</b> When configuring using the IPv6 address space, the host URL must be enclosed within '[' ]' if a literal IPv6 address is used, for example:<br/> <i>ldap://oracle.companyx.com:389</i> (no brackets required)<br/> <i>ldap://[2222::22]:389</i> (brackets required)</li> <li>Click <b>[Remove]</b> to remove a URL from the list.</li> <li>Use <b>[Move Up]</b> and <b>[Move Down]</b> to change the order of the URLs.</li> </ul> |
| <b>Use Client Authentication</b> | <p>Select this check box to present a certificate to the server during the SSL handshake, if one is requested.</p> <p>Clear this check box to never present a certificate, even if one is requested. Note that access may be denied in this case.</p> <p><b>Note:</b> When Client Authentication is enabled, it is used with the specified</p>  |

| Setting  | Description   |
|--|---|
|  | key when connecting to an LDAP server for any <i>ldaps</i> connections. If there are no <i>ldaps</i> connections, then the Client Certification options will have no effect.  |
| <b>Auth DN Prefix</b><br><b>Auth DN Suffix</b> | <p>Optionally enter a prefix and or a suffix for the authorization DN.</p> <p>The DN prefix and suffix are combined with the client-provided username to produce a DN that will be used to attempt to bind with the client-provided password in order to check whether the client-provided username is authenticated.</p> <p><i>Example:</i></p> <p>The Gateway uses a prefix ("CN=") and a suffix ("OU=Sales,O=Layer 7") to configure the provider. During runtime, say a request arrives with HTTP credentials: username=<i>bob</i>, password=<i>secret!123</i>. The username is used to build a DN:</p> <p style="text-align: center;"><i>CN=bob,OU=Sales,O=layer 7</i></p> <p>The Gateway then issues a "bind" request to the LDAP server using this DN and with the password "secret!123".</p> <p>If the prefix and suffix are omitted, the Gateway will use the raw login name as the login for the authentication bind.</p> <p><b>Tip:</b> The client-provided username must conform to the regular expression defined in the <a href="#">ldap.simple.username.pattern</a> cluster property before it can be used to produce a DN.</p> |

## Testing the Configuration

You can click **[Test]** to verify the configuration before completing the wizard. You will be prompted to enter the login credentials to the LDAP server. If the credentials and configuration are correct, you should see a message validating the configuration of the Simple LDAP Identity Provider. If an error message displays instead, note the configuration problems and take the appropriate corrective actions:

Table 93: Troubleshooting Simple LDAP configuration problems

| Configuration Error              | Suggested Solution  |
|----------------------------------|---|
| <b>Connection error</b>          | Verify that all connection details in the wizard are correct.   |
| <b>Test credentials rejected</b> | Verify that the login credentials for the LDAP server have been entered correctly and then try again. |

Repeat the testing and fixing until no more errors appear. If you have difficulty resolving the errors, [contact](#) CA Technical Support for assistance.

The new Simple LDAP Identity Provider appears in the **[Identity Providers]** tab.

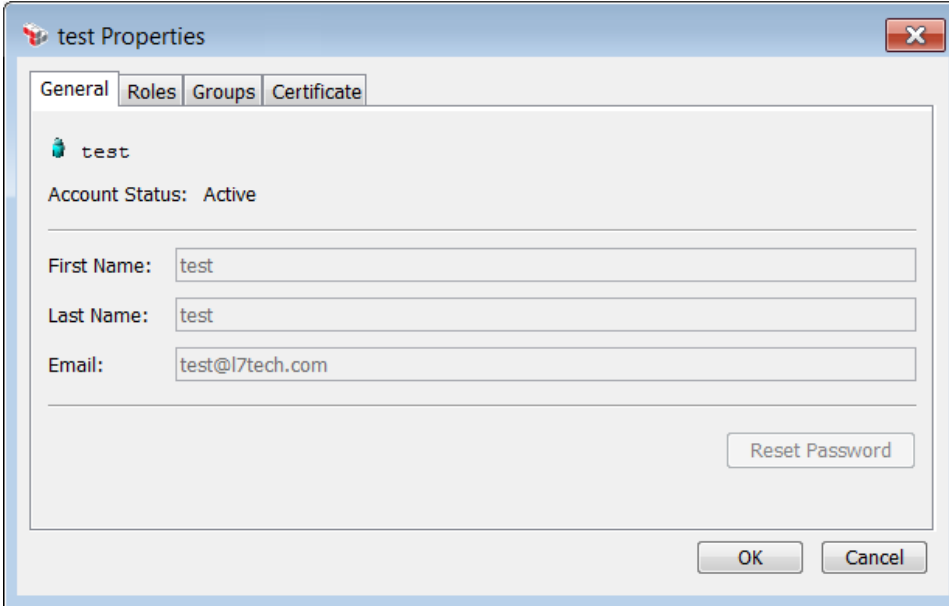
## LDAP User Properties

When an [LDAP Identity Provider](#) is configured, user details are stored and managed in the external LDAP server. The Policy Manager can display this information in read-only format, with the exception of user [roles](#).

➤ To access the properties for an LDAP user:

1. [Search](#) the LDAP identity provider;
2. Click the user to view and then click [**Select**]. The properties for that user are displayed.
3. Click [**OK**] when done.

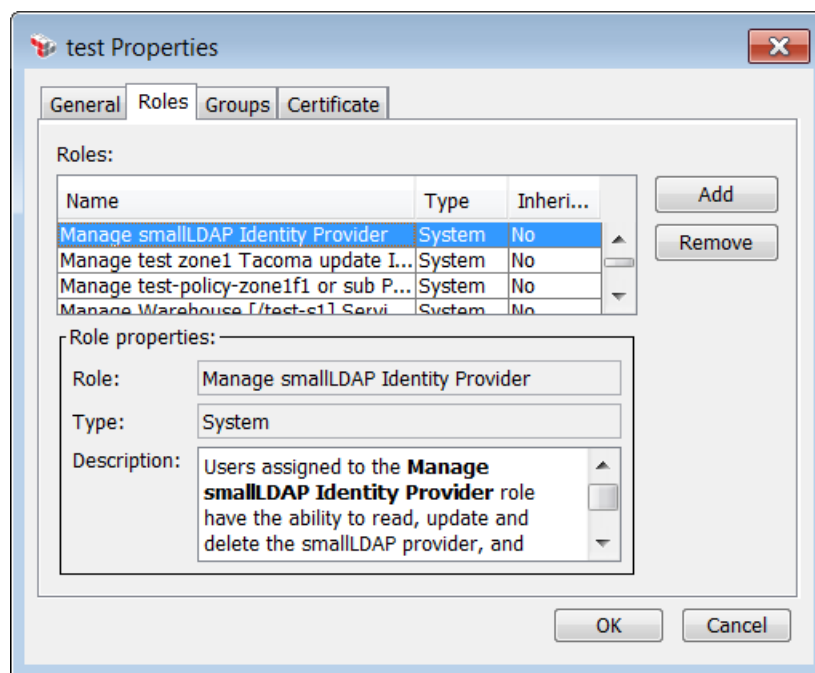
### Configuring the [General] Tab



The screenshot shows a window titled "test Properties" with a close button (X) in the top right corner. Inside the window, there are four tabs: "General", "Roles", "Groups", and "Certificate". The "General" tab is selected. Below the tabs, there is a user icon and the name "test". Underneath, it says "Account Status: Active". There are three text input fields: "First Name:" with the value "test", "Last Name:" with the value "test", and "Email:" with the value "test@l7tech.com". To the right of these fields is a "Reset Password" button. At the bottom right of the window are "OK" and "Cancel" buttons.

This tab displays the name and email address for the user. All information is managed on the LDAP repository and cannot be modified here.

## Configuring the [Roles] Tab



This tab is used to assign or remove LDAP users from [roles](#) and is available only when administrative access has been enable for the LDAP Identity Provider (set via the "[Allow assignment to administrative roles](#)" check box in Step 1 of the "LDAP Identity Provider Wizard" on page 306). At least one role must be set if the user will be logging in to the Policy Manager.

The table at the top lists the roles currently assigned to the user:

- **Name:** The name of the role.
- **Type:** "System" indicates a role that is either predefined or automatically generated (see ""Predefined Roles and Permissions" on page 132"). "Custom" indicates a user-defined role (see ""Managing Roles" on page 130").
- **Inherited:** "No" means the user is assigned to the role directly; "Yes" means the user is a member of a group assigned to that role .

The Role properties section at the bottom displays the complete description for the selected role.

➤ *To add the user to a role:*

1. Click **[Add]**. A list of eligible roles is displayed.
2. Select the role(s) to which to add the user. **Tip:** To locate a role more easily, enter some text in the "Filter on name" box. This filters the roles list to display only those roles containing the filter text. Delete the filter text to restore the full list of roles.
3. Click **[Add]** to close the dialog.

➤ *To remove a user from a role:*

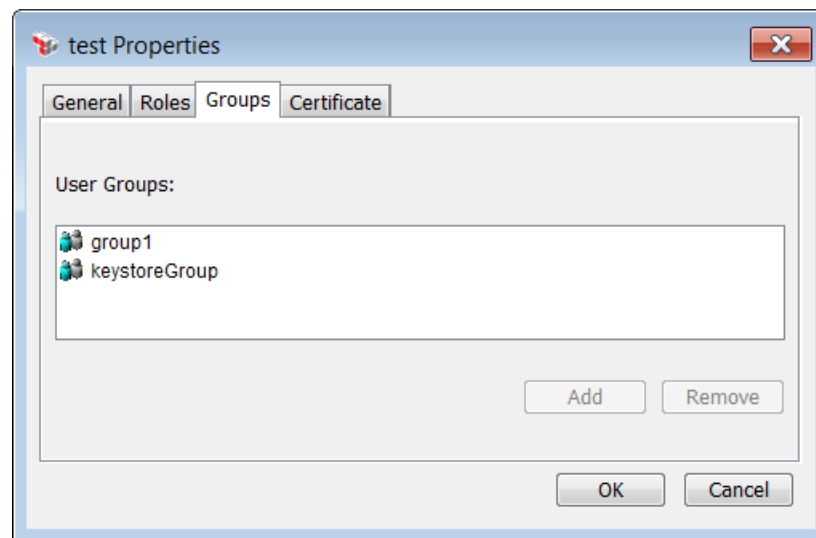
1. Select the role(s) to be removed from the user. Hold down the [Ctrl] key to select multiple roles. **Note:** You can only remove roles that are *not* inherited. To remove a user from an inherited role, remove the user from the group that has the role.
2. Click **[Remove]**.

---

**Notes:** (1) Users who need to log on to the Policy Manager must be assigned to at least one role. For more information, see "Managing Roles" on page 130. (2) If a role is both assigned and inherited, the interface will display "No" in the "Inherited" column and you are permitted to remove the role. Once removed, that role remains in the list, but the "Inherited" column changes to "Yes".

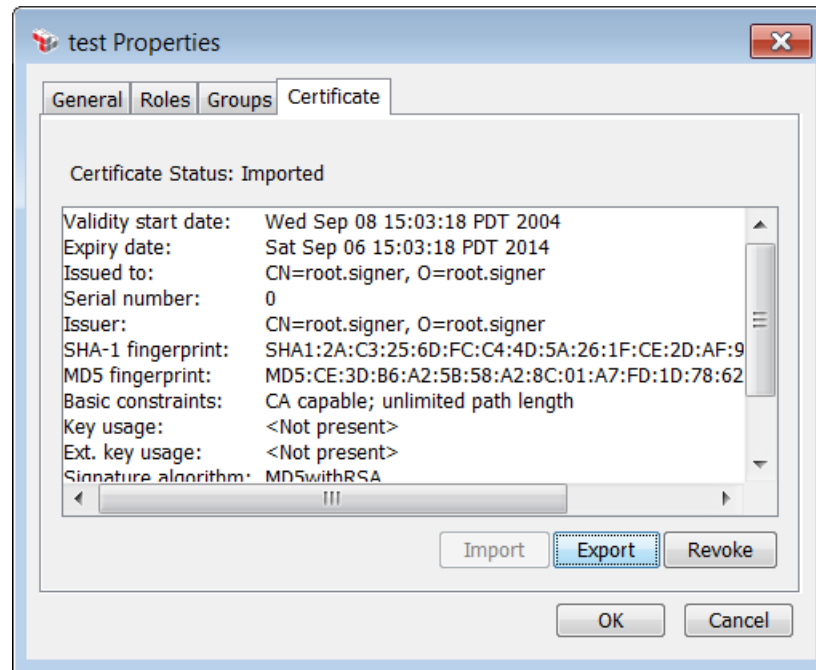
---

### Configuring the [Groups] Tab



This tab displays the groups to which the LDAP user belongs. The information is managed on the LDAP repository and cannot be modified here.

## Configuring the [Certificate] Tab



This tab is used to manage the certificate for the LDAP user.

- To import a certificate for the user, click **[Import]** and then complete the [Add Certificate Wizard](#). The import option is not available if the user already has a certificate in the LDAP repository.

If the user has no certificate in the LDAP or the "Enable user certificates in this LDAP" check box in the [LDAP Identity Provider Wizard](#) (Step 1) is not selected, then a certificate can be imported for this user. **Note:** The imported certificate is not stored on the LDAP repository but rather in the client certificate store within the Gateway.

- To export a certificate, click **[Export]** and then specify a file name and location.
- To revoke a certificate, click **[Revoke]** and then click **[OK]** to confirm. Revoking removes both the certificate and the user's password.

---

**Note:** The **Revoke** option is not available for LDAP users who have a client certificate in the LDAP repository. Revoking a certificate in this case requires either removing it from the LDAP repository or revoking the certificate and then specifying an appropriate [revocation checking policy](#).

---

## Policy-Backed Identity Providers

A Policy-Backed Identity Provider authenticates a user via an underlying policy fragment. This allows you to create authentication logic that is as complex or as basic as you need. You can even validate and authorize the user. Unlike the other [identity providers](#), this identity provider is not prepopulated with a list of authorized users. In fact, the Gateway does not need to know whether the user exists or will ever log on to the Gateway. You only need to configure template users based on a user name and optionally assign a role. When a user with a matching username is authenticated he or she can be allowed access to the Policy Manager based on the features permitted by that role.

Examples of where a Policy-Backed Identity Provider can be useful: contacting a Web service, using a custom assertion for a protocol such as RADIUS, or custom LDAP or JDBC authentication.

---

**Note:** The Policy-Backed Identity Provider only authenticates individual users, not groups.

---



### Backing Policy

The underlying policy fragment ("backing policy") receives these prepopulated variables containing the user's credentials:

- **`${idp.userid}`**: Returns the user's ID.
- **`${idp.password}`**: Returns the user's password.

The backing policy can contain any number of assertions to authenticate the username and password. The only thing to keep in mind is that the policy must not be able to succeed without authenticating the user.

The following is a very simple policy fragment that uses the `Compare Expressions` assertion to compare the username with "joe" and the password with "password":

-  Compare Expression: `${idp.userid}` is a String and is equal to joe (case sensitive)
-  Compare Expression: `${idp.password}` is a String and is equal to password (case sensitive)

### Hints and Tips

- A Policy-Backed Identity Provider is appropriate for you if you need *both* of the following:
  - You require password authentication implemented by a custom policy that will authenticate the credentials based on username and password.

- Ability for users authenticated via this policy to log in to the Policy Manager (or the Management API) and administer the Gateway, or use at least one of the Gateway's built-in services (for example, policy discovery or token service).
- If your authentication requirements do not require Policy Manager login or use of built-in services (in other words, users are only used in message processing traffic), consider using an encapsulated assertion or included policy fragment instead.
- If you do not require custom policy behavior during authentication, consider authenticating against an [LDAP server](#) or the [Internal Identity Provider](#) instead.
- Create a Policy-Backed Identity Provider only if you need an identity provider. If you only need a reusable policy snippet that hides its implementation details, use an encapsulated assertion instead.
- A Policy-Backed Identity Provider can be used with the Authenticate Against Identity Provider and Authenticate User or Group assertions like any other identity provider.
- It is possible to embed one of the above "Authenticate...." assertions within the backing policy of a Policy-Backed Identity Provider and then have that "Authenticate..." assertion authenticate against another identity provider (for example, LDAP or Federated). However, such a configuration is recommended only for advanced users and may be more difficult to troubleshoot.

## Creating a Policy-Backed Identity Provider

➤ To add a new [Policy-Backed Identity Provider](#) in the Policy Manager:

1. Do one of the following:
  - Click **[Tasks] > Create Identity Provider > Create Policy-Backed Identity Provider** from the [Main Menu](#)
  - Right-click the "Identity Providers" title at the top of the [\[Identity Providers\] tab](#) and then select **Create Policy-Backed Identity Provider**.
2. Complete the [Policy-Backed Identity Provider](#) wizard. The new identity provider is added to the [\[Identity Providers\] tab](#).



## Editing a Policy-Backed Identity Provider

➤ To modify the details of a [Policy-Backed Identity Provider](#):

1. Do one of the following:
  - In the [\[Identity Providers\] tab](#), double-click the name of the Policy-Backed Identity Provider to edit
  - In the [\[Identity Providers\] tab](#), right-click the Policy-Backed Identity Provider to edit and then select **Properties**. The *Edit Policy-BProvider Wizard* appears.
2. Update the information in the [Policy-Backed Identity Provider](#) wizard as required.

## Deleting a Policy-Backed Identity Provider

➤ To delete a [Policy-Backed Identity Provider](#) from the Policy Manager:

1. In the [\[Identity Providers\] tab](#), right-click the Policy-Backed Identity Provider to delete and then select **Delete**.
2. Click **[Yes]** to confirm. The identity provider is removed. The underlying authentication policy is not deleted.

---

**Tip:** Ensure that you are not currently logged in to the Policy Manager using a username that authenticates through the deleted identity provider. Doing so will cause you to be locked out of the Policy Manager upon removal of the identity provider.

---

## Policy-Backed Identity Provider Wizard

The *Policy-Backed Identity Provider* wizard is displayed when you [create](#) or [edit](#) a [Policy-Backed Identity Provider](#).

Before using this wizard, ensure that you have an appropriate policy fragment containing the logic to authenticate users. For more information, see "Policy-Backed Identity Providers" on page 325.

Figure 128: Policy-Backed Identity Provider wizard

1. Complete the wizard as follows:

Table 94: Policy-Backed Identity Provider settings

| Setting   | Description  |
|---|--|
| <b>Provider Name</b>                            | Enter a name for your Policy-Backed Identity Provider.   |
| <b>Authentication Policy</b>                    | <p>From the drop-down list, choose the policy fragment that contains the policy logic that will authenticate the users. <b>Note:</b> Only policy fragments of type "Policy-Backed Identity Provider Policy Fragment" can be selected.</p> <p>If the policy fragment has not been created yet, exit the wizard to create the fragment, then return to the wizard later. For more information about fragments, see <i>Working with Policy Fragments</i> in the <i>Layer 7 Policy Authoring User Manual</i> (you will be working with "included policy fragments").</p>                       |
| <b>Allow assignment to administrative roles</b> | <p>This check box determines whether an authenticated user can have an administrative role.</p> <ul style="list-style-type: none"> <li>• Select this check box to allow a user to be assigned a <a href="#">role</a> that will enable him or her to log into the Policy Manager. For more information, see "<a href="#">Working with Policy-Backed Identity Providers</a>" in "Searching Identity Providers" on page 459.</li> <li>• Clear this check box to not permit users to be assigned to a role. The authenticated user will not be able to log into the Policy Manager.</li> </ul> |
| <b>Use Default Role Assignment</b>              | <p>This check box determines whether a default role will be assigned. It is available only when "Allow assignment to administrative roles" above is selected.</p> <ul style="list-style-type: none"> <li>• Select this check box to assign a default role to all users authenticated by this identity provider.</li> </ul> <p><b>Note:</b> This default role is used only if the user has no other roles explicitly assigned. If a role is assigned via the Search</p>   |

Table 94: Policy-Backed Identity Provider settings

| Setting             | Description  |
|---------------------|--|
|                     | <p>Identity Provider dialog (see "<a href="#">Working with Policy-Backed Identity Providers</a>" in "Searching Identity Providers" on page 459), the default role is inactive for the user.</p> <ul style="list-style-type: none"> <li>• Clear this check box to not assign a default role automatically. In this case it will be up to you to assign a role to the template user, otherwise the user will not be able to log in.</li> </ul> <p><b>IMPORTANT:</b> Use the default role assignment with care. Once a user is authenticated, that user will be able to log in through the Policy Manager and administer the Gateway. This could allow untrusted users (current or future) to access the Gateway.</p> |
| <b>Default Role</b> | <p>If the "Use Default Role Assignment" check was selected above, choose the role from the drop-down list. For more information, see "Managing Roles" on page 130.</p>   |

2. Click **[Test]** to test your authentication policy.
  - a. Enter the **Username** and **Password** of known good credentials.
  - b. Click **[OK]**. The wizard will run the credentials through the authentication policy and report success or failure of the Policy-Backed Identity Provider. If authentication was not successful, you may need to adjust your authentication policy.
3. Click **[Finish]** to close the wizard.



## Chapter 5: Working with Services

The Policy Manager differentiates between SOAP web services and XML or non-SOAP applications. Collectively referred to as "services", each requires a different publication wizard:

- Web services from existing WSDL (Web Services Description Language) documents are published using the "Publish SOAP Web Service Wizard" on page 333.
- Web services that require the generation of a new WSDL document are published using the "Create WSDL Wizard" on page 337.
- Web APIs and non-SOAP applications are published using the "Publish Web API Wizard" on page 346.
- RESTful proxies are published using the "Publish REST Service Proxy Wizard" on page 352.

---

**Note:** The term *identity* includes both users and groups; *user* can represent an individual human or machine; *service* includes both web services and XML applications.

---

Both web services and XML applications appear in the [Services and Policies](#) list upon publication. Security policies for the services are configured in the policy development window.

### Working with SOAP Web Services

The Policy Manager guides you through the web service publication process:

- When publishing a web service that has an existing WSDL (Web Services Description Language) document, the [Publish SOAP Web Service Wizard](#) allows you to easily enter the location, access credentials, and Gateway access option for the web service
- When publishing a web service that does not have a WSDL document, the [Create WSDL Wizard](#) allows you to easily configure the WSDL elements that describe the business services, transactions, and electronic access instructions for the web service.

Publishing a web service does the following:

1. Adds a web service to the [Services and Policies](#) list of the Policy Manager.
2. Establishes the web service's initial policy in the policy development window
3. Allows authorized clients to access the web service through the Gateway.

The publishing process will add a Route via HTTP(S) assertion to the policy as long as there is at least one HTTP(S) endpoint declared in the WSDL document. If no HTTP(S) endpoints are defined in the WSDL, you must manually add an appropriate routing assertion to the policy.

---

**Note:** The Policy Manager differentiates between SOAP web services and non-SOAP applications. To publish or edit a non-SOAP application, see "Publishing a Non-SOAP Application" on page 346.

---

You can publish multiple instances of the same web service when each contains a [unique resolution URI](#). After publication, the Policy Manager allows you to view the web service WSDL code and change or reset the web service WSDL from an established WSDL document, without changing its existing policy.

---

**Tip:** Publishing a SOAP service creates a default policy that contains a Route via HTTP(S) assertion and an implicit "All Assertions Must Evaluate to True" composite folder that is not visible. If these assertions have been placed in security zones, you must have at least Read permission to the assertions in order to publish the service (for example, add yourself to the "Manage X Zone" role.)

---

Choose a task from the following table:

Table 95: SOAP web service tasks

| For information on how to...                                       | See  |
|--|--|
| <b>Publish a SOAP web service with an existing WSDL document</b>   | "Publish SOAP Web Service Wizard" on page 333                    |
| <b>Create a WSDL document before publishing a SOAP web service</b> | "Create WSDL Wizard" on page 337                                 |
| <b>Delete a published service</b>                                  | "Deleting a Published Service" on page 369                       |
| <b>Specify a custom routing URI</b>                                | Service Properties, "Configuring the [HTTP/FTP] tab" on page 360 |
| <b>View, edit, or reset a web service's WSDL</b>                   | Service Properties, "Configuring the [WSDL] tab" on page 362     |

## Publish SOAP Web Service Wizard

The *Publish SOAP Web Service Wizard* is used to [publish](#) a Web service with an existing WSDL document.

For more information about wizards, see "[Wizards](#)" under "Interfaces" on page 13. The *Publish SOAP Web Service Wizard* supports the WSDL 1.1 standard.

**Note:** If the web service does not have a WSDL document, use the [Create WSDL Wizard](#) instead.

➤ To access the *Publish SOAP Web Service Wizard*, do any of the following:

- Click **Publish SOAP Web Service** on the [Home Page](#)
- Select **[Tasks] > Publish SOAP Web Service** from the [Main Menu](#)
- Right-click a folder within the [Services and Policies](#) list and then select **Publish SOAP Web Service**.

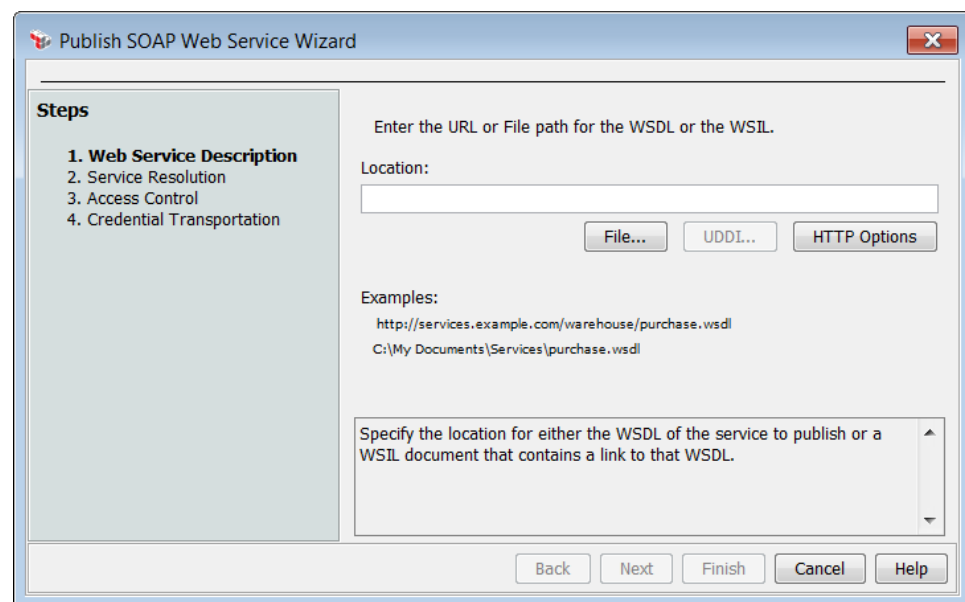


Figure 129: Publish SOAP Web Service Wizard

Complete the wizard as described below.

| Wizard Step                            | Description  |
|--|--|
| <b>Step 1: Web Service Description</b> | <p>The Web Service Description screen locates the WSDL document for the web service using one of the following methods:</p> <ul style="list-style-type: none"> <li>• If you know the URL for the WSDL, enter it in the <b>Location</b> field.</li> </ul> |

| Wizard Step            | Description   |
|------------------------|---|
|                        | <p>If you have a WSDL file, click <b>[File]</b> and then select the file.</p> <ul style="list-style-type: none"> <li>If you are extracting the WSDL URL from a WSIL (Web Services Inspection Language) URL, enter the WSIL URL in the <b>Location</b> field. If you have a WSIL file, click <b>[File]</b> and then select the file. Select the target web service when prompted.</li> <li>If you are searching a UDDI Registry for the web service, click <b>[UDDI]</b> and proceed to Searching the UDDI Registry for details. The <b>[UDDI]</b> button is available only when a UDDI registry has been configured on the Gateway. For more information, see Managing UDDI Registries in the <i>Layer 7 Policy Authoring User Manual</i>.</li> <li>To configure options for the URL (for example, to specify the credentials or configure a proxy), click <b>[HTTP Options]</b> to open the <a href="#">Manage HTTP Options</a> dialog.</li> </ul> <p>Note the following about the WSDL document:</p> <ul style="list-style-type: none"> <li>The WSDL document should <u>not</u> depend on any external documents, otherwise the import process may fail.</li> <li>The WSDL URL supports SSL, SSL + Client authentication, and URL authentication.</li> <li>The maximum size for a WSDL document is controlled by the <a href="#">wsdlDownload.maxSize</a> cluster property.</li> </ul> <p>Click <b>[Next]</b>. The wizard attempts to resolve the WSDL URL. If the resolution is successful, you proceed to Step 2 of the wizard. If the WSDL download fails, try the following troubleshooting steps:</p> <ul style="list-style-type: none"> <li>Note the errors and then re-enter the WSDL or WSIL URL or search the UDDI registry again, then click <b>[Next]</b> to try to move to the next step of the wizard.</li> <li>An error message "Unable to parse WSDL location" may indicate that authentication is required. If you see this message, click <b>[HTTP Options]</b> to configure options for the URL (for example, to specify the credentials, SSL, or proxy options). For more information, see "Managing HTTP Options" on page 188.</li> </ul> <p><b>Tip:</b> Once credentials have been supplied, if the UDDI is monitored for changes to this service, you will not be prompted for credentials in the future for WSDL downloads from that location.</p> <p>If you cannot resolve the WSDL URL, <a href="#">contact</a> CA Technical Support for assistance.</p> <p>Upon publication, the WSDL URL appears as a Route via HTTP(S) assertion in the web service's initial policy and the name of the web service is extracted from the resolved WSDL and added to the <a href="#">[Services] tab</a>.</p> |
| <b>Step 2: Service</b> | The Service Resolution screen lets you choose the service resolution  |



| Wizard Step                   | Description  |
|-------------------------------|--|
| <b>Resolution</b>             | <p>path:</p> <ul style="list-style-type: none"> <li>• <b>No resolution path:</b> Select this option to set the resolution path to the default Gateway URI "/smsg/soap". This setting is the default.</li> <li>• <b>Custom resolution path:</b> Select this option to specify a custom resolution URI. Choose a custom URI from the drop-down list or type in the URI if you require one that is not on the list.</li> </ul> <p><b>Tip:</b> You can change the resolution path later using the <a href="#">[HTTP/FTP] tab</a> in the <a href="#">service's properties</a>. Note that the service resolution path applies to both the HTTP and FTP protocols.</p>  |
| <b>Step 3: Access Control</b> | <p>The Access Control screen allows you to define simple Web service encryption, access control, and authentication rules.</p> <ol style="list-style-type: none"> <li>1. Optionally select the <b>Require SSL/TLS Encryption</b> check box to require that all requestors consume the web service through the SSL entry point.</li> <li>2. Select <b>Allow Anonymous Access</b> to permit requestors to access the web service anonymously (without credentials).</li> </ol> <p>OR:</p> <p>Select <b>Require Users to Authenticate</b> to require that requestors provide credentials to gain web service access. Define the authentication details for this option as follows:</p> <ul style="list-style-type: none"> <li>• <b>Authentication Method:</b> Select an authentication method from the drop-down list. This determines what information users and groups are required to provide to gain web service access.</li> <li>• <b>Identity Provider:</b> Select an <a href="#">identity provider</a> that contains the authorized users and groups from the drop-down list.</li> </ul> <p><b>Note:</b> When requiring users to authenticate, the Web access will be restricted to the identity providers indicated above. The policy will initially be populated with an authentication assertion for each Authenticate User or Group assertion corresponding to each selected identity.</p> <ol style="list-style-type: none"> <li>3. Specify which users and groups are authorized to use the web service by moving them between the <b>No Permission</b> and <b>Have Permission</b> lists. <ul style="list-style-type: none"> <li>• Grant permission by selecting entries from <b>No Permission</b> and then clicking <b>[Add]</b>. Alternatively, click <b>[Add All]</b> without selecting any entry to authorize everyone on the list.</li> <li>• Deny permission by selecting entries from <b>Have Permission</b> and then clicking <b>[Remove]</b>. Alternatively, click <b>[Remove All]</b> without selecting any entry to deny permission to everyone on the list</li> </ul> </li> </ol> <p><b>Tip:</b> You can select a continuous block of rows by dragging the</p> |

| Wizard Step                              | Description   |
|--|---|
|  | <p>mouse over the rows you want; or, select the first row, hold down the <b>[Shift]</b> key, then select the last row. You can select individual rows by holding down the <b>[Ctrl]</b> key while clicking on the rows you want.</p> <p>4. If you need to authorize users or groups from another identity provider, select the new provider name from the <b>Identity Provider</b> drop-down list and then repeat step 3.</p>   |
| <b>Step 4: Credential Transportation</b> | <p>The Credential Transportation screen specifies how the Gateway can gain access to the web service.</p> <ol style="list-style-type: none"> <li>1. Verify that the <b>Web Service URL</b> is correct. This URL is from the WSDL document and will be used by the Gateway to access the web service. To change the URL: <ol style="list-style-type: none"> <li>a. Click <b>[Change]</b> and modify the URL as necessary.</li> <li>b. Click <b>[Default]</b>.</li> </ol> </li> <li>2. Choose an access control option: <ul style="list-style-type: none"> <li>• Select <b>The Gateway can access this protected Web service anonymously</b> to instruct the Gateway to access the protected web service without authentication</li> <li>• Select <b>The Gateway will need to provide credentials to access this Web service</b> to instruct the Gateway to provide credentials when connecting to the web service.</li> </ul> </li> <li>3. Click <b>[Finish]</b>. The web service is published and added to the <b>[Services]</b> tab.</li> </ol> <p><b>Tips:</b> (1) If you've specified a conflicting service resolution, you are given the option to correct the conflict, proceed as is, or cancel the publishing.<br/> (2) It is recommended that you disable the published web service until its policy is completed. See "Service Properties" on page 357 for instructions.</p> |

When the wizard is complete, the newly published service appears in the policy development window, with a Route via HTTP(S) assertion already added. You can now begin constructing your new policy. For more information, see Policy Organization in the *Layer 7 Policy Authoring User Manual*.

---

**Note:** If the WSDL document did not declare any HTTP(S) endpoints, the Policy Manager will be unable to automatically add a routing assertion. In this case, manually add the appropriate routing assertion to the policy.

---

## Sending Requests to the Newly Published Service

After creating the new service, you can send requests to it by using one of the following URIs:

**http://<machinename.domain.com>:8080/ssg/soap**

**https://<machinename.domain.com>:8443/ssg/soap**

Where:

- <machinename.domain.com> is the name of the computer hosting the Gateway
- /ssg/soap is the default resolution URI on the Gateway

Then assign a different resolution URI, see "Service Properties" on page 357.

## Create WSDL Wizard

The *Create WSDL Wizard* is used to create a new WSDL document to be used for publishing a service. This WSDL document can be custom created or it can be composed from existing WSDL documents. The steps in the wizard correspond to the six main and child elements in a WSDL document.

For more information about wizards, see [Wizards](#) under "Interfaces" on page 13. The Create WSDL Wizard supports the WSDL 1.1 standard.

---

**Note:** The *Create WSDL Wizard* is intended for advanced users who are familiar with WSDL, XML, SOAP, and the SOAP protocols. If there is already a WSDL document that meets your needs, use the [Publish SOAP Web Service Wizard](#) instead.

---

### Using the Wizard

➤ To access the *Create WSDL Wizard*, do any of the following:

- Click **Create WSDL** on the [Home Page](#)
- Select **[Tasks] > Create WSDL** from the [Main Menu](#)
- Right-click the root folder at the top of the [Services and Policies](#) list and then select **Create WSDL**.

Complete the wizard as described below.

---

**Tip:** Click **[Preview]** at any time during the configuration process to view the in-progress WSDL for the web service.

---

### Step 1: Overview

This step introduces the wizard.

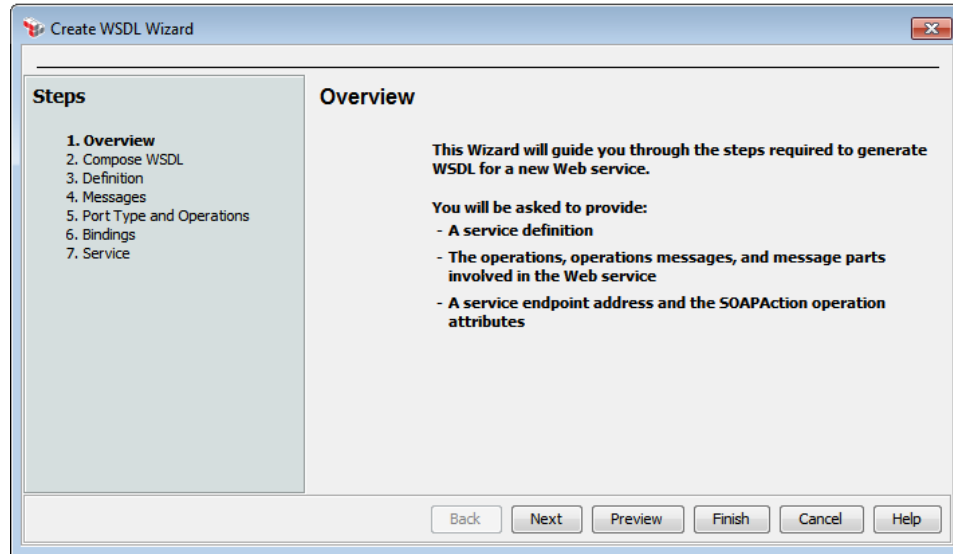


Figure 130: Create WSDL Wizard, Step 1

Click [**Next**] to continue.

## Step 2: Compose WSDL

The Compose WSDL screen lets you compose or aggregate existing WSDLs to create a WSDL document by copying elements from other WSDLs. Using this feature, it is possible to publish a "virtual service" to the gateway. This allows the gateway to proxy request for multiple services with distinct WSDLs.

If you do not wish to compose your own WSDL document and only want to define your own messages, operations, port types/bindings etc., click [**Next**] without entering anything to proceed to Step 3 of the wizard.

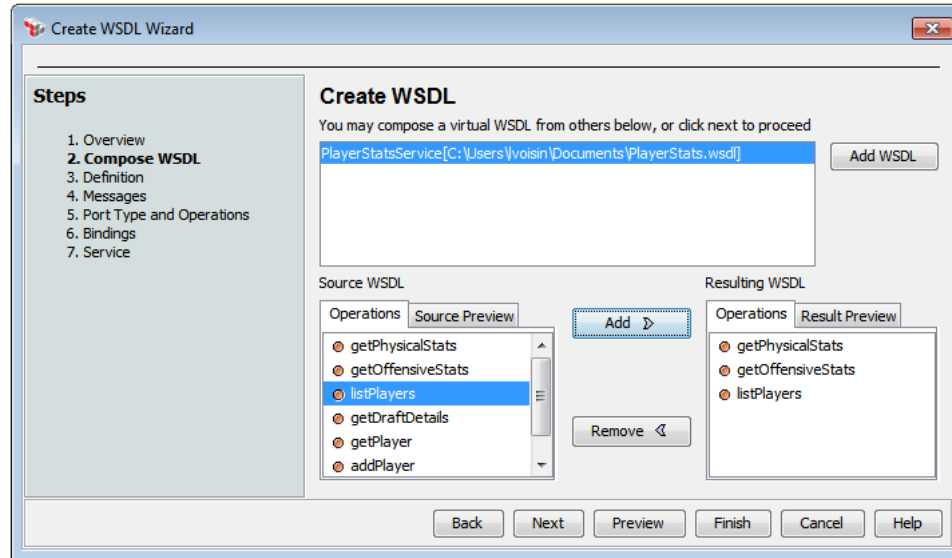


Figure 131: Create WSDL Wizard, Step 2

➤ To compose a WSDL document:

1. Populate the list at the top of the page with the WSDL(s) containing the elements you need to assemble your own WSDL.
  - To add a WSDL to the list, click **[Add WSDL]** to display the Choose WSDL dialog. In the Location field, enter the URL that will resolve the new web service WSDL.
  - To configure options for the URL (for example, to specify the credentials or configure a proxy), click **[HTTP Options]** to open the [Manage HTTP Options](#) dialog.

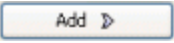
Alternatively:

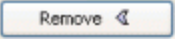
- If the WSDL is contained in a file, click **[File]** and select the file.
  - If the WSDL is from a UDDI registry, click **[UDDI]** and complete the Search UDDI dialog. For more information, see Searching the UDDI Registry in the *Layer 7 Policy Authoring User Manual*.
2. From the WSDL list, select a WSDL containing the operations that you wish to add to your WSDL. The Binding operations are shown in the **Source WSDL** list under the [Operations] tab.

---

**Tip:** To see a tree containing more details about other elements of the WSDL, select the [Source Preview] tab.

---

3. To add an operation in the target WSDL, select the operation from the [Operations] tab of the **Source WSDL** list and then click . This adds it to the **Resulting WSDL** list.

To remove an operation from the target WSDL, select the operation from the **Resulting WSDL** list and then click .

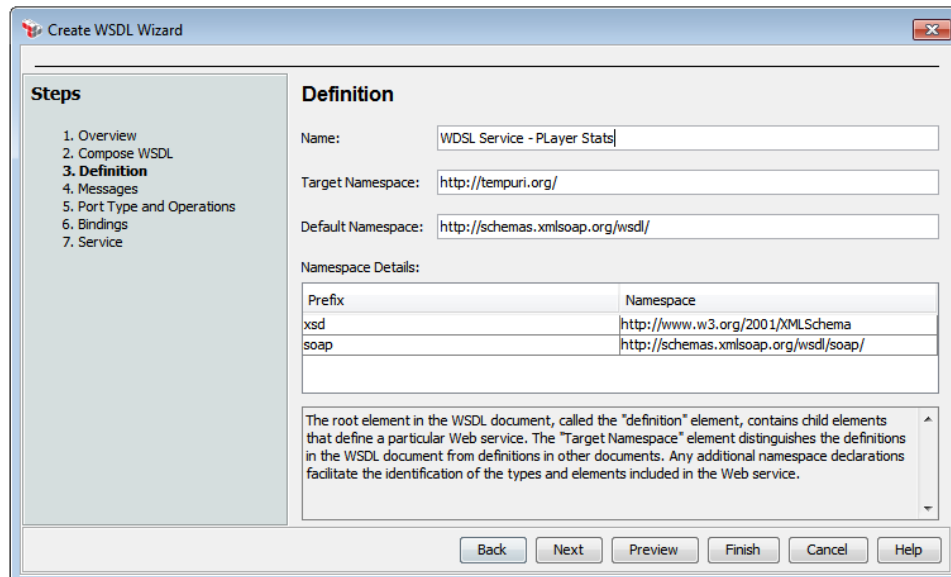
**Tip:** Adding and removing operations only affect what is populated in the WSDL document being constructed. It does not necessarily define which WSDL operations should be excluded in the policy; this depends on whether SOAPAction being defined in the service resolution of the Gateway. To properly constrain operation availability, you should include the Evaluate WSDL Operation assertion in the service policy.

4. Repeat steps 2 and 3 until you are satisfied with the resulting WSDL.

**Note:** The WSDL document that you compose here can be refined further as you navigate through the remaining steps of the wizard. All messages and operations that are required for the selected operations are added to the WSDL document being constructed.

### Step 3: Definition

The Definition screen configures the root definitions element and its child elements. These elements define the particulars of the Web service.



**Create WSDL Wizard**

**Steps**

1. Overview
2. Compose WSDL
- 3. Definition**
4. Messages
5. Port Type and Operations
6. Bindings
7. Service

**Definition**

Name:

Target Namespace:

Default Namespace:

Namespace Details:

| Prefix | Namespace                             |
|--------|---------------------------------------|
| xsd    | http://www.w3.org/2001/XMLSchema      |
| soap   | http://schemas.xmlsoap.org/wsdl/soap/ |

The root element in the WSDL document, called the "definition" element, contains child elements that define a particular Web service. The "Target Namespace" element distinguishes the definitions in the WSDL document from definitions in other documents. Any additional namespace declarations facilitate the identification of the types and elements included in the Web service.

Back Next Preview Finish Cancel Help

Figure 132: Create WSDL Wizard, Step 3

Configure this step of the wizard as follows:

- **Name:** Enter a descriptive name for the web service. This name will appear on the [Services and Policies](#) list.
- **Target Namespace:** The wizard pre-populates a suggested namespace that relates to your web service application. Make any adjustments if necessary. This namespace can be a URL or a SOAP payload namespace URI.

#### More Details

The namespace plus SOAPAction combination determines the uniqueness of the web service. The Policy Manager checks for uniqueness during the publication process and will prompt you for another URI if the web service WSDL is not unique.

A namespace that resembles a URL does not necessarily point to a Web-based resource. Avoid using relative URI namespaces, if possible. A URI namespace causes XML canonicalization problems and prevents the use of message-level security such as those found in the XML Security assertions.

- **Default Namespace:** Displays the default URI `http://schemas.xmlsoap.org/wsdl/`. The URI is the namespace convention for the main elements in the WSDL document. Make any adjustments if necessary.
- **Namespace Details:** Displays information about the namespaces. This information cannot be edited here.

### Step 4: Messages

The Messages screen configures the message elements. A Web service contains multiple messages with one or more logical parts that define the communication between the web service client and server.

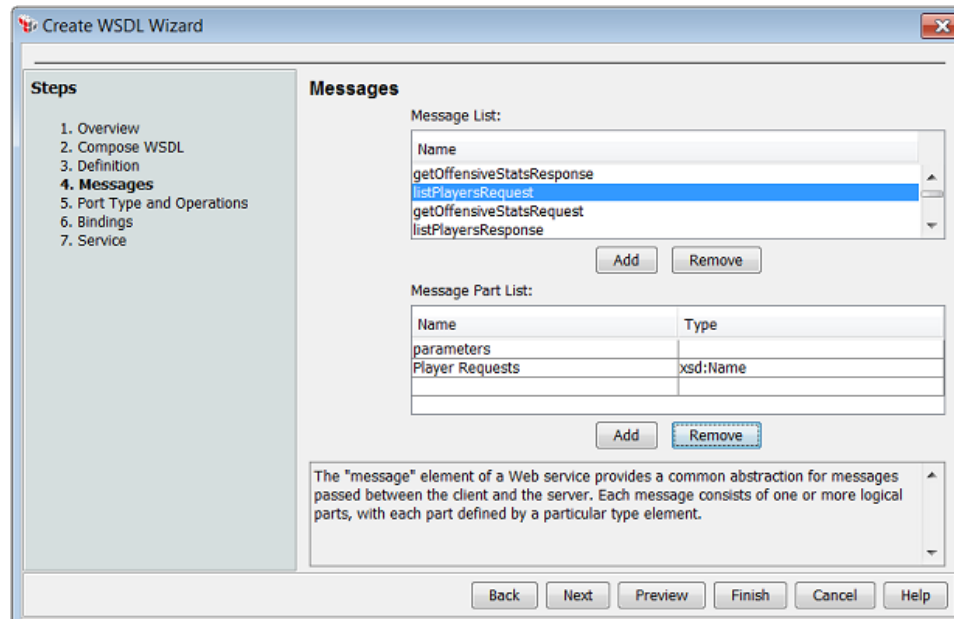


Figure 133: Create WSDL Wizard, Step 4

Configure this step of the wizard as follows:

- **Message List:** Double-click the default entry and replace it with a name that describes the message type; for example: "GetQuoteResponse". To add more message names, click **[Add]** and repeat the process. To remove a message name, select it and click **[Remove]**.
- **Message Part List:** Click **[Add]** to add a message part. Double-click the default name under **Name** and replace it with a name that describes the message part; for example: "stockSymbol". Select the part type from the **Type** drop-down list. To remove a message part, select it and click **[Remove]**.

Repeat to add as many messages and parts as necessary.

## Step 5: Port Type and Operations

The Port Type and Operations screen configures the port type element that includes the set of operations used in the web service. Each operation refers to one input message and one output message configured in the previous Messages screen.



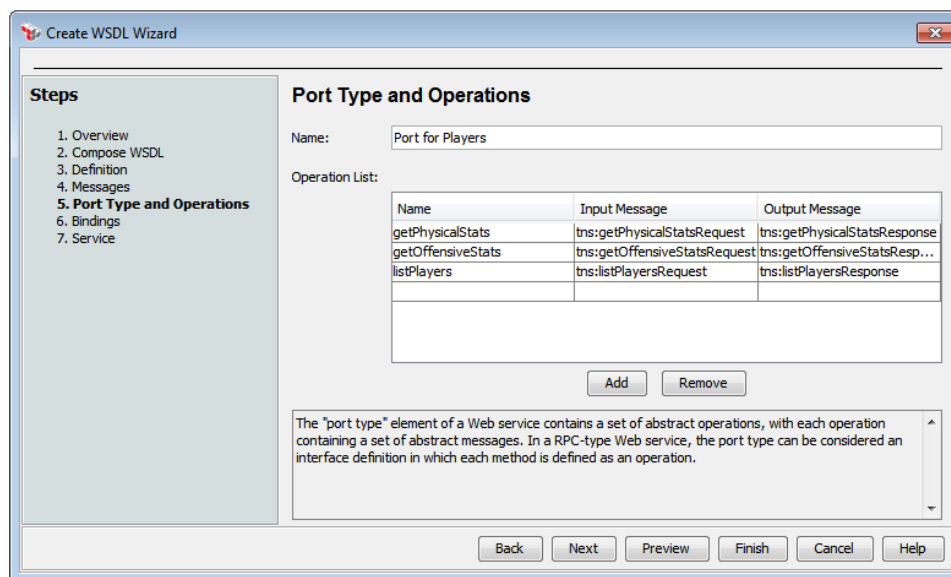


Figure 134: Create WSDL Wizard, Step 5

Configure this step of the wizard as follows:

- **Name:** Enter a descriptive name for the port type; for example, "StockInfo".
- **Operation List:** Click **[Add]** to add an operation. Double-click the default under **Name** and replace it with a name that describes the operation; for example, "getQuote". Select the appropriate **Input Message** and **Output Message** from the drop-down lists. (Note: These messages were defined in Step 4 of the wizard.) To remove an operation, select it and click **[Remove]**.

## Step 6: Bindings

The Port Type Bindings screen configures the binding element which specifies the binding definitions that govern message formatting and protocol details.

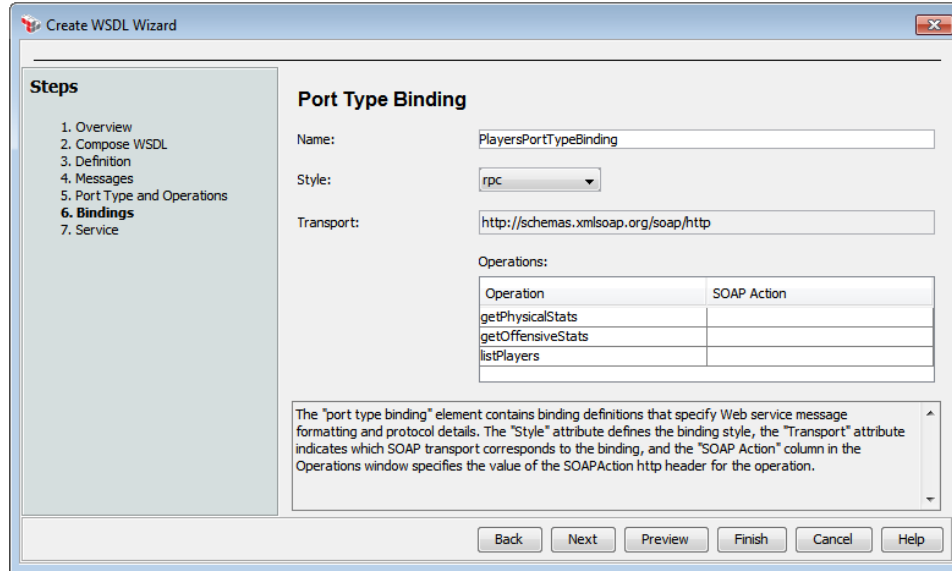


Figure 135: Create WSDL Wizard, Step 6

Configure this step of the wizard as follows:

- **Name:** Enter a descriptive name for the port type binding; for example, "StockServiceSOAPBinding".
- **Style:** Select a message format for the operations from the drop-down list.
- **Transport:** Displays the default namespace URI. The URI is the namespace of the transport-specific elements in the WSDL document. This field is display only.
- **Operations:** Lists the operations defined in Step 5 of the wizard. If you need to modify any of the SOAP Action shown, double-click an entry and edit as necessary.

## Step 7: Service

The Service screen configures the service element that defines the web service endpoint address (URL) and access port.

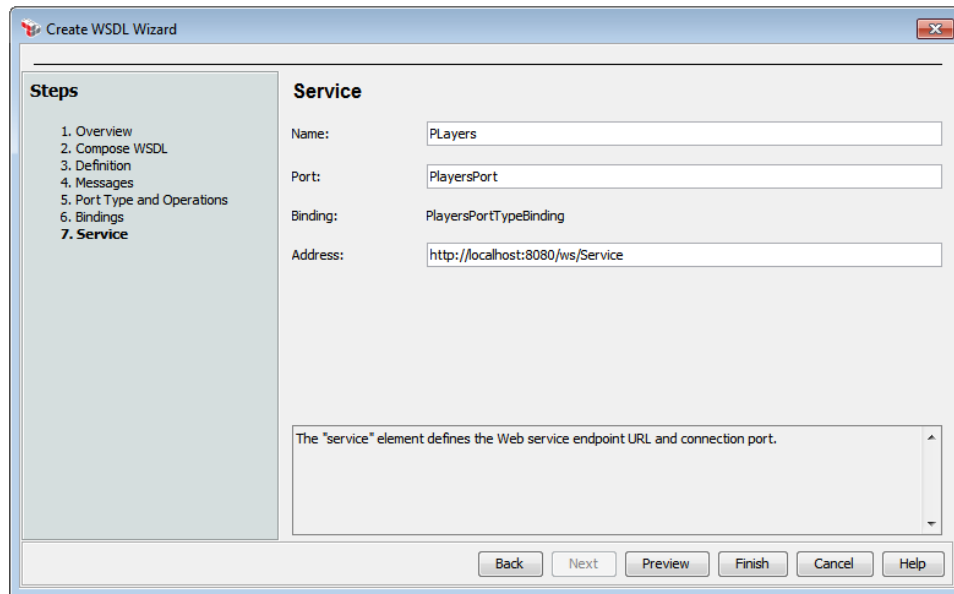


Figure 136: Create WSDL Wizard, Step 7

Configure this step of the wizard as follows:

- **Name:** Enter a descriptive name for the service element into the Name field; for example, "StockQuote".
- **Port:** Displays the default access port for the web service. Do not change this default.
- **Binding:** Displays the port type binding name, as entered in Step 6 of the wizard.
- **Address:** Displays the default URL `http://localhost:8080/ws/NewServiceName`, where:
  - "localhost" is the host name of the server hosting the web service
  - "8080" is the TCP port at which the web service can be reached
  - "ws/" is a sample folder that might contain the web service
  - "NewServiceName" is the web service name that was entered in the Name field.

Adjust the address as necessary to construct a valid URL for the web service.

The URL in the **Address** field determines the default web service Message Routing Assertion.

To update the default URL in the **Address** field with the information entered in the **Name** and **Port** fields, click **[Back]** and then **[Next]**.

When you are satisfied everything is correct, click **[Finish]** to publish the service. The disabled web service is added to the [Services and Policies](#) list. You should now:

- Construct a policy for the Web service, as described in Policies, then
- Enable the web service, as outlined in "Service Properties" on page 357.

---

**Tip:** If you've specified a conflicting service resolution, you are given the option to correct the conflict, proceed as is, or cancel the publishing.

---

## Publishing a Non-SOAP Application

In the Policy Manager, Web API and non-SOAP applications are published using the "Publish Web API Wizard" on page 346. This wizard guides you through the publication process, allowing you to enter connection and routing information and access credentials for the application. You can also publish a REST service proxy using the "Publish REST Service Proxy Wizard" on page 352.

Publishing the application adds it to the [Services and Policies](#) list, establishes the non-SOAP application's initial policy in the policy development window, and allows authorized clients to access the application through the Gateway. After publication, you can [modify](#) the Gateway URL that receives requests for the application, if necessary. You can also modify the [properties](#) of the service.

---

**Tips:** (1) The Policy Manager differentiates between SOAP web services and non-SOAP applications. To publish, edit, or view a SOAP web service, see "Working with SOAP Web Services" on page 331. Non-SOAP policies do not support the message-level security assertions found in the XML Security assertions. (2) Publishing a non-SOAP application creates a default policy that contains an implicit "All Assertions Must Evaluate to True" composite folder that is not visible. If this assertions has been placed in security zone, ensure that you have at least Read permission to that assertion (for example, you have the "Manage X Zone" role.)

---

### Publish Web API Wizard

The *Publish Web API Wizard* is used to [publish](#) any non-SOAP application.

For more information about wizards, see "[Wizard](#)" under "Interfaces" on page 13.

➤ To access the *Publish Web API Wizard*, do any of the following:

- Click **Publish Web API Wizard** on the Policy Manager [Home Page](#).
- Select [Tasks] > **Publish Web API Wizard** from the [Main Menu](#).
- Right-click a folder within the [Services and Policies](#) list and then select **Publish Web API Wizard**.



Figure 137: Publish Web API Wizard

Complete the wizard as described below.

Table 96: Publish Web API Wizard settings

| Wizard Step                        | Description  |
|------------------------------------|--|
| <b>Step 1: Service Information</b> | <p>The Service Information screen specifies the connection and routing information for the application or service.</p> <ul style="list-style-type: none"> <li>• <b>Service Name:</b> Enter a name for the non-SOAP application. Upon publication, this name will appear on the <a href="#">Services and Policies</a> list.</li> <li>• <b>Target URL:</b> Enter the full HTTP URL of the application. The Gateway will route service requests to this target URL. Upon publication, this URL will appear as a Route via HTTP(S) assertion in the application's initial policy. <ul style="list-style-type: none"> <li><b>Note:</b> You may leave the Target URL blank if you intentionally do not want to create an HTTP endpoint. For example, an endpoint is not necessary if you plan to use the Copy Request Message to Response or Return Template Response to Requestor assertions to the policy. In this case, you may disregard the validation warnings about missing routing assertions.</li> </ul> </li> <li>• <b>Gateway URL:</b> Complete the Gateway URL provided by the Policy Manager with a unique URI that corresponds to the unique address that will receive requests for the application. Only enter a URI that completes the embedded Gateway URL into the field. For example, if you are connected to Gateway <i>machinename.domain.com/xml/</i>, you might enter "Warehouse" as the URI into the Gateway URL field. In this example, the final application-specific URL that will receive requests would be <i>machinename.domain.com/xml/Warehouse</i>. <ul style="list-style-type: none"> <li><b>Note:</b> When publishing a RESTful web service, the Gateway URL</li> </ul> </li> </ul> |

| Wizard Step                   | Description  |
|-------------------------------|--|
|                               | must contain a wildcard (for example, <code>"/restentrypoint/*"</code> ).  |
| <b>Step 2: Access Control</b> | <p>The Access Control screen allows you to define access control and authentication rules for the non-SOAP application.</p> <ol style="list-style-type: none"> <li>1. Optionally select the <b>Require SSL/TLS Encryption</b> check box to require that all requestors consume the application through the SSL entry point.</li> <li>2. Choose an access control option: <ul style="list-style-type: none"> <li>• Select <b>Allow Anonymous Access</b> to permit requestors to access the application anonymously (without credentials)</li> <li>• Select <b>Require Users to Authenticate</b> to require that requestors provide credentials to gain application access. Define the authentication details for this option as follows: <p><b>Authentication Method:</b> Select an authentication method from the drop-down list. This determines what information users and groups are required to provide to gain application access.</p> <p><b>Identity Provider:</b> Select an <a href="#">identity provider</a> that contains the authorized users and groups from the drop-down list.</p> <p><b>Note:</b> When requiring users to authenticate, the access will be restricted to the identity providers indicated above. The policy will initially be populated with an authentication assertion for each Authenticate User or Group assertion corresponding to each selected identity.</p> </li> </ul> </li> <li>3. Specify which users and groups are authorized to use the application by moving them between the <b>No Permission</b> and <b>Have Permission</b> lists. <ul style="list-style-type: none"> <li>• Grant permission by selecting entries from <b>No Permission</b> and then clicking <b>[Add]</b>. Alternatively, click <b>[Add All]</b> without selecting any entry to authorize everyone on the list.</li> <li>• Deny permission by selecting entries from <b>Have Permission</b> and then clicking <b>[Remove]</b>. Alternatively, click <b>[Remove All]</b> without selecting any entry to deny permission to everyone on the list</li> </ul> <p><b>Tip:</b> You can select a continuous block of rows by dragging the mouse over the rows you want; or, select the first row, hold down the <b>[Shift]</b> key, then select the last row. You can select individual rows by holding down the <b>[Ctrl]</b> key while clicking on the rows you want.</p> </li> <li>4. If you need to authorize users or groups from another identity provider, select the new provider name from the <b>Identity Provider</b> drop-down list and then repeat step 3.</li> <li>5. Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>. For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>. <b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</li> </ol> |

| Wizard Step | Description   |
|-------------|---|
|             | <p>6. Click <b>[Finish]</b>. The application or service is added to the <a href="#">Services and Policies</a> list.</p> <p><b>Tips:</b> (1) If you've specified a conflicting service resolution, you are given the option proceed as is or cancel the publishing. (2) It is recommended that you disable the published application until its policy is completed. See "Service Properties" on page 357 for instructions.</p> |

## Working with RESTful Web Services

RESTful web services and resource orientation in general provide an alternative approach to exposing web services and web APIs. RESTful web services are an alternative to WS-\* style web services built respecting the guidelines and principles of REST (Representational State Transfer). Some of the properties of RESTful web services include:

- resources are uniquely identified through the HTTP URI
- the action on the resource is dictated by the HTTP verb (method)
- resource representations are the HTTP payload
- Content-Type not limited to XML; it can be anything else (for example, JSON)

The CA API Gateway can help you secure your RESTful web services to the same extent as WS-\* (using SOAP, WSDL) services.

### Additional Resources

For more information about REST principles and guidelines see [http://en.wikipedia.org/wiki/Representational\\_State\\_Transfer](http://en.wikipedia.org/wiki/Representational_State_Transfer)

For additional information regarding using the CA API Gateway with RESTful web services, see these resources from CA Technologies:

- **REST/SOAP Remapping** (<http://www.layer7tech.com/tutorials/rest-to-soap-remapping>)
- **Securing REST Interfaces** (<http://www.layer7tech.com/tutorials/securing-rest-interfaces>)
- **Using URI Templates** (<http://kscottmorrison.com/2009/12/11/using-uri-templates-on-xml-security-gateways/>)
- **Simplifying REST Adaptation** (<http://www.layer7tech.com/tutorials/simplifying-rest-adaptation>)

## Securing a RESTful Web Service

The following table summarizes the steps to secure your RESTful web service using the CA API Gateway.

**Note:** The term "XML application" has a legacy heritage. If your RESTful web service does not use XML, the CA API Gateway can support many other Content-Types.

Table 97: Steps to secure a RESTful web service

| To...  | Do this...   |
|--|--|
| Build a policy to route and validate traffic for an existing RESTful web service | <p><b>STEP 1:</b> Build a policy in the same manner as a SOAP policy, except use the <a href="#">Publish Web API Wizard</a> instead of the <a href="#">Publish SOAP Web Service Wizard</a>. Be sure to configure the resolution URI pattern to associate the policy with all possible URLs for that service, using the '*' wildcard character. (Reason: Unlike WS-* style web services that have a single URL entry point, RESTful web services refer to the resource ID being acted upon using the URI portion of the HTTP URL. Thus, the URL used is different for each resource, even though the same policy applies. You can specify a different policy for any different URL pattern.)</p> <p>After publishing, the CA API Gateway becomes the entry point for your RESTful web service. The Gateway reconstructs and proxies to the service endpoint for each incoming request. Responses are similarly reverse-proxied.</p> <p>For more information, see "Publishing a Non-SOAP Application" on page 346.</p> |
|  | <p><b>STEP 2:</b> The default behaviour of the Route via HTTP(S) assertion is to route to an explicit endpoint URL rather than the entry point URI of the RESTful web service. To replicate the URI downstream, specify it as part of the HTTP routing target using the context variable <code>\${request.http.uri}</code>. For example, specify a target URL as shown below:</p> <p><code>http://downstreamServiceHost/something\${request.http.uri}</code></p> <p>For more information about the <code>\${request.http.uri}</code> variable, see <a href="#">Transport Layer Variables</a>.</p> <p><b>Tip:</b> If you need to use a specific portion of the URI as part of the policy, you can extract it from the incoming URL (<code>\${request.http.uri}</code>) using the Evaluate Regular Expression assertion.</p>   |
|  | <p><b>STEP 3:</b> You can validate incoming content using any XML-related assertion if your RESTful web services format resources in XML. Examples of such assertions include the Validate XML Schema, Evaluate Request XPath, and Evaluate Response XPath assertions. If your service uses JSON, use the Validate JSON Schema assertion instead.</p> <p>For any text-based Content-Type, the Evaluate Regular Expression assertion can be used to evaluate specific patterns.</p> <p><b>Tip:</b> The Threat Protection Assertions may also be useful to help you</p>  |



| To...                                 | Do this...   |
|---------------------------------------|--|
|                                       | validate input for your RESTful web service.   |
| <b>Validate HTTP parameters</b>       | <p>Specific validation of HTTP parameters can be achieved with the help of the Validate HTML Form Data assertion. This assertion allows you to enforce:</p> <ul style="list-style-type: none"> <li>• which HTTP method is allowed (GET, POST)</li> <li>• which HTTP parameters must be present in the request</li> <li>• the number of occurrences of each parameter in the request</li> <li>• where the parameters occur in the request (in the URL, body, or anywhere within the request)</li> <li>• the presence of unnamed fields (allowed/disallowed)</li> </ul> <p>For more information, see Validate HTML Form Data Assertion in the <i>Layer 7 Policy Authoring User Manual</i>.</p> |
| <b>Validate JSON schema</b>           | <p>Add the Validate JSON Schema assertion to the policy if you need to validate JSON data structure and property types/values against a JSON schema.</p> <p>Use the context variable suffix ".mainpart" to access the JSON payload of a specific message (request, response, other). To learn more about this suffix, see <a href="#">"Context Variable Data Types"</a> under "Appendix C: Context Variables" on page 517.</p> <p>For more information, see Validate JSON Schema Assertion in the <i>Layer 7 Policy Authoring User Manual</i>.</p>   |
| <b>Transform between JSON and XML</b> | <p>Use the Apply XSL Transformation assertion to transform from XML to JSON. Please <a href="#">contact CA Technologies</a> if you require a stylesheet for such a transformation. Use the Set Context Variable assertion and context variables to transform from JSON to XML.</p>   |
| <b>Security options</b>               | <p>You can authenticate and authorize requestors using any authentication mechanism appropriate for HTTP. Examples of these include:</p> <ul style="list-style-type: none"> <li>Require SSL or TLS Transport</li> <li>Require SSL or TLS Transport with Client Authentication</li> <li>Require HTTP Basic Credentials</li> <li>Require Windows Integrated Authentication Credentials</li> </ul>  |
| <b>Caching</b>                        | <p>Cachable resources is a property of RESTful web services. The CA API Gateway offers these assertions to help you implement this aspect of your RESTful web services:</p> <ul style="list-style-type: none"> <li>Store to Cache</li> <li>Look Up in Cache</li> </ul>   |
| <b>Configure the policy</b>           | <p>Most assertions can be used for your RESTful web service, but SOAP-specific ones will not be appropriate. The policy validator will warn you.</p> <p>For more information, see Configuring a Policy in the <i>Layer 7 Policy Authoring User Manual</i>.</p>   |

| To...                      | Do this...   |
|----------------------------|--|
| <b>Restrict HTTP verbs</b> | <p>You can place restrictions on the HTTP methods (verbs) associated with the policy. For example, you can authorize different verbs for different URI patterns. A RESTful web service can use these methods: GET, PUT, POST, DELETE.</p> <p>To configure the HTTP method that is sent downstream, use the Route via HTTP(S) Assertion.</p> <p><b>Tip:</b> You can also branch your policy based on the incoming verb using the context variable <code>\${request.http.method}</code>.</p>   |
| <b>Access HTTP headers</b> | <p>You can access a variety of HTTP header values by using the context variable pattern below:</p> <pre><code>\${&lt;target&gt;.http.header.&lt;name&gt;}</code></pre> <p>Where "<code>&lt;target&gt;</code>" is either <b>request</b>, <b>response</b>, or a message context variable and "<code>&lt;name&gt;</code>" is the header value being retrieved.</p> <p><i>Examples:</i></p> <ul style="list-style-type: none"> <li><code>\${request.http.header.content-type}</code> retrieves the Content-Type from the header (for example, "text/xml")</li> <li><code>\${request.http.header.date}</code> retrieves the date from the HTTP header</li> </ul> <p><b>Tip:</b> The <code>\${&lt;target&gt;.http.header.&lt;name&gt;}</code> variables are only available for messages that arrive over HTTP, or from the default response to a request that arrived over HTTP. If the latter, the only headers that will be available are the ones destined to be added to the response headers when the response is eventually sent. For more information about this variable, see <a href="#">Transport Layer Variables</a>.</p> |

## Publish REST Service Proxy Wizard

The *Publish REST Service Proxy Wizard* is used to [publish](#) a REST service proxy on the Gateway.

For more information about wizards, see "[Wizard](#)" under "Interfaces" on page 13.

---

**Note:** It is recommended that you disable the new REST service proxy endpoint until its policy is completed. For information on disabling a service, see "Service Properties" on page 357.

---

➤ To access the *Publish REST Service Proxy Wizard*, do any of the following:

- Click **Publish RESTful Service Proxy** on the Policy Manager [Home Page](#).
- Select **[Tasks] > Publish RESTful Service Proxy** from the [Main Menu](#).

- Right-click a folder within the [Services and Policies](#) list and then select **Publish RESTful Service Proxy**.

Complete the wizard as described below. Once the wizard is complete, the new REST service proxy will appear in the Services and Policies list.

### Step 1: Deploy REST Service From

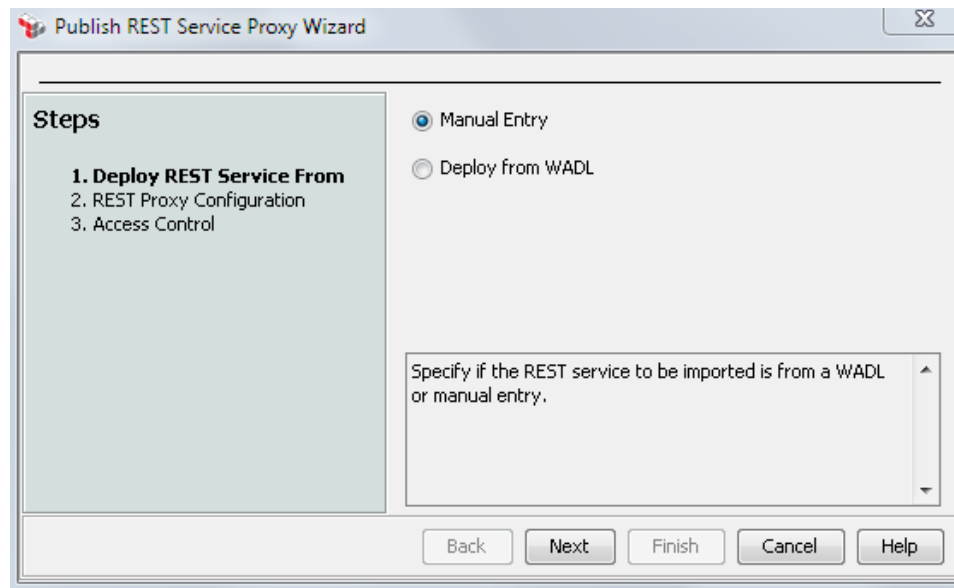


Figure 138: Publish REST Service Proxy Wizard - Step 1

Choose how to import the REST service:

- **Manual Entry:** Choose this to manually specify the Service Name and Resource Base URL.
- **Deploy from WADL:** Choose this to import information from a WADL.

## Step 2: REST Proxy Configuration

The screenshot shows the 'Publish REST Service Proxy Wizard' window, Step 2: REST Proxy Configuration. The 'Steps' pane on the left lists: 1. Deploy REST Service From, 2. REST Proxy Configuration (selected), and 3. Access Control. The main area contains the following fields:

- Service Name\*:** Twitter Search
- Resource Base URL\*:** http://search.twitter.com
- Gateway URI:** http(s)://docssg.l7tech.com:[port]/
- ☐ Override Gateway URI

Below these fields is a text box with the instruction: 'Specify a Service Name, Resource Base URL and optionally overriding the default Gateway URI. The Gateway URI will mimic the path from the Resource Base URL unless overridden.' Below that is a note: '\* denotes required fields.' At the bottom are buttons: Back, Next, Finish, Cancel, and Help.

Figure 139: Publish REST Service Proxy Wizard - Step 2 (manual entry)

In this step, configure the REST proxy:

If you are manually configuring the proxy, complete the following.

- **Service Name:** Enter a name for the non-SOAP application. Upon publication, this name will appear on the [Services and Policies](#) list.
- **Resource Base URL:** Enter the required Resource Base URL of the RESTful Service.
- **Gateway URI:** The default Gateway URI is displayed. This URI is based on the path from the Resource Base URL. If you need to override the Gateway URI, select the **Override Gateway URI** check box and type in a different URI.

The screenshot shows the 'Publish REST Service Proxy Wizard' window, Step 2: REST Proxy Configuration. The 'Steps' pane on the left lists: 1. Deploy REST Service From, 2. REST Proxy Configuration (selected), and 3. Access Control. The main area contains the following fields:

- Location\*:** C:\Users\Desktop\wadl\warehouse.wadl
- ☐ Override Gateway URI
- HTTP Options** button
- File...** button

| Resource Base URL      | Service Name  | Gateway URI    |
|------------------------|---------------|----------------|
| http://hugh:8082/AC... | ACMEWarehouse | ACMEWarehouse/ |

Below the table is a text box with the instruction: 'Specify the location to a WADL file and click Load to import the REST service endpoint(s). The Gateway URI must be unique and will mimic the Resource Base URL unless overridden.' Below that is a note: '\* denotes required fields.' At the bottom are buttons: Back, Next, Finish, Cancel, and Help.

Figure 140: Publish REST Service Proxy Wizard - Step 2 (load from WADL)

If you are deploying from a WADL, complete the following.

- **Location:** Enter the location of the WADL file or click **[File]** to locate it.
- **Load:** Click this button to load the WADL file once a valid location is entered. The button is disabled until a local existing file has been specified or a valid HTTP(S) URL has been specified in the location field.
- **HTTP Options:** To configure options for the URL (for example, to specify the credentials or configure a proxy), click **[HTTP Options]** to open the [Manage HTTP Options](#) dialog.
- **Override Gateway URI:** If you need to override the displayed URI for the Gateway, select this check box to make the Gateway URI column editable.  
**Tip:** Double-click in the Gateway column to enable editing. Press [Enter] when done.

---

**Note:** The Resource Base URL column is not editable. However, the Service Name column is editable by default, whereas the Gateway URI column is editable only when "Override Gateway URI" is checked.

---

### Step 3: Access Control

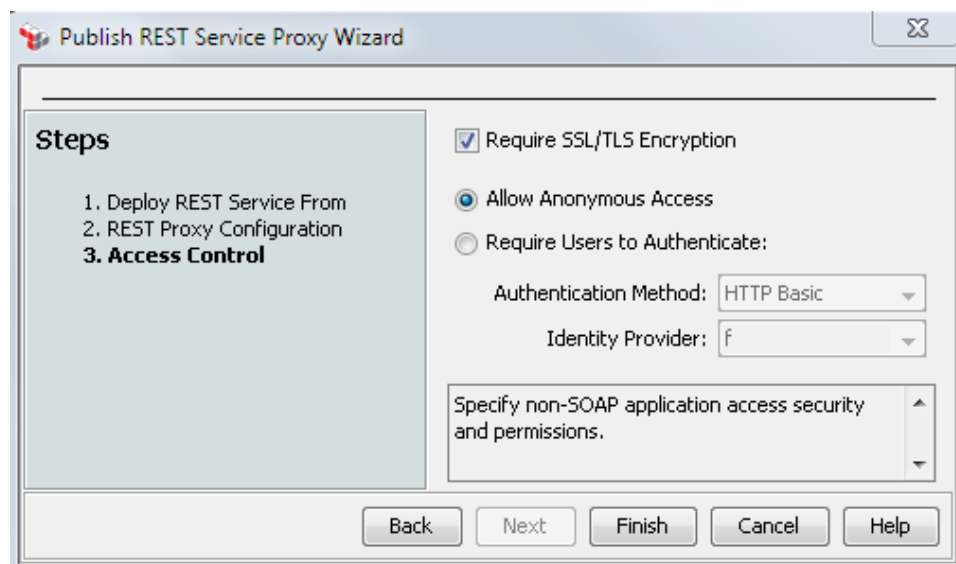


Figure 141: Publish REST Service Proxy Wizard - Step 3

The Access Control step allows you to define access control and authentication rules for the non-SOAP application.

1. Select the **Require SSL/TLS Encryption** check box to require that all requestors consume the application through the SSL entry point.

2. Choose an access control option:

- Select **Allow Anonymous Access** to permit requestors to access the application anonymously (without credentials).
- Select **Require Users to Authenticate** to require that requestors provide credentials to gain application access. Define the authentication details for this option as follows:
  - **Authentication Method:** Select an authentication method from the drop-down list. This determines what information users and groups are required to provide to gain application access.
  - **Identity Provider:** Select an [identity provider](#) that contains the authorized users and groups from the drop-down list.

---

**Note:** When requiring users to authenticate, the access will be restricted to the identity providers indicated above. The policy will initially be populated with an authentication assertion for each **Authenticate User or Group** assertion corresponding to each selected identity.

---

3. Specify which users and groups are authorized to use the application by moving them between the **No Permission** and **Have Permission** lists.

- Grant permission by selecting entries from **No Permission** and then clicking **[Add]**. Alternatively, click **[Add All]** without selecting any entry to authorize everyone on the list.
- Deny permission by selecting entries from **Have Permission** and then clicking **[Remove]**. Alternatively, click **[Remove All]** without selecting any entry to deny permission to everyone on the list

**Tip:** You can select a continuous block of rows by dragging the mouse over the rows you want; or, select the first row, hold down the [Shift] key, then select the last row. You can select individual rows by holding down the [Ctrl] key while clicking on the rows you want.

4. If you need to authorize users or groups from another identity provider, select the new provider name from the **Identity Provider** drop-down list and then repeat step 3.

## Managing Published Services

Once a service has been published, you can perform the following tasks:

|                           |     |
|---------------------------|-----|
| Service Properties .....  | 357 |
| Disabling a Service ..... | 367 |
| Enabling a Service .....  | 368 |

|  |     |
|--|-----|
| Renaming a Service .....                         | 368 |
| Deleting a Published Service .....               | 369 |
| Viewing the WSDL for a Service .....             | 369 |
| Resetting the WSDL for a Service .....           | 370 |
| Changing the Resolution Path for a Service ..... | 371 |

## Service Properties

In the Policy Manager, all your web services and XML applications are listed under the list of [Services and Properties](#). A different icon is used for each to help you quickly identify each:



icon = Web service



icon = XML application

You can access the properties of each service to do a variety of tasks, such as disabling/enabling a service, changing its name, setting a resolution URI, specifying allowed HTTP methods, or viewing/resetting its WSDL.

### Supporting JMS Requests

If a service is intended to receive JMS requests, ensure that the WSDL for every such service specifies unique values for the following attributes (where an empty string "" is considered a value):

*SOAP payload namespace URI (i.e., child elements of SOAP:Body)*  
*SOAPAction*

As messages received over JMS cannot be resolved using an HTTP resolution URI, they rely on a unique combination of payload namespace URI and SOAPAction. In practice, this means JMS messages cannot be resolved by the Gateway if multiple services have been published using identical\* WSDL documents.

\*In rare instances, even WSDL documents that are very similar (but not identical) may prevent JMS messages from being resolved. Specifically, the Gateway will allow two services to be published using WSDLs that have the same SOAP payload namespace URI, but with different SOAPAction values. However, unless the inbound JMS queues are configured with a SOAPAction attribute (see [Managing JMS Destinations](#), "Use JMS message property as SOAPAction in service resolution" setting) and the inbound JMS requests contain valid values in that attribute, the JMS requests will not be resolved to any service.

➤ *To access the properties for a service:*

- Do either of the following:
  - Right-click the web service or XML application under the [Services and Policies](#)

[list](#) and then select **Properties**.

- Select **[File] > Service Properties** from the [Main Menu](#).

The Published Service Properties are displayed. This dialog organizes the service properties across these tabs: **General**, **HTTP/FTP**, **WSDL**, and **UDDI**.

**Note:** All controls in the Published Service Properties are disabled if you do not have permission to edit service properties ("Manage [name] Service" role) or if the policy for the service is currently being editing and there are unsaved changes (you will be alerted by the message "Service has unsaved policy changes" next to the [OK] button in the properties dialog).

## Configuring the [General] tab

The screenshot shows the 'Published Service Properties' dialog box with the 'General' tab selected. The 'Service Display Name' is 'PlayerStatsService', 'Service ID' is '229376', and 'Policy GUID' is 'b95fbc9e-b28c-4301-b30e-d7c2cc51d197'. The 'Perform WS-Security processing for this service' checkbox is checked. The 'Enable' radio button is selected. The 'Enable policy debug tracing' checkbox is unchecked. The 'Security Zone' dropdown is set to 'no security zone'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.


Figure 142: Published Service Properties - [General] tab

The [General] tab contains basic information about the service, including settings to disable/enable the service.

Table 98: Service Properties - [General] tab

| Label                       | Description  |
|-----------------------------|--|
| <b>Service Display Name</b> | The name of the service as it appears in the <a href="#">services and policies list</a> and in the policy tabs. You can change this name if necessary. |
| <b>Service ID</b>           | The entity ID for the published service. This value is for displayed for   |



| Label  | Description   |
|--|---|
|  | reference only and cannot be modified.  |
| <b>Policy GUID</b>                                     | The GUID for the policy. This value is for displayed for reference only and cannot be modified.   |
| <b>Perform WS-Security processing for this service</b> | <p>Select this check box to perform WS-Security processing for the published service. By default, this is not enabled for XML services but is enabled for all other services.</p> <p><b>Note:</b> The Gateway will perform WS-Security processing on a request message as required by the services policy, even if <b>[Perform WS-Security processing for this service]</b> is not selected. This will allow assertions that require WS-Security processing on request messages to run, even when WS-Security processing has been disabled in a service.</p> <p><b>IMPORTANT:</b> If there are WS-Security assertions in an XML service, be sure to enable WS-Security processing, otherwise these assertions will not work.</p>  |
| <b>Enable</b>  | Select this option to enable a service that has been disabled. When enabled, the red "X" over the icon is removed and the service will accept requests. By default, all services are enabled after publication, except for those services created using the "Create WSDL Wizard" on page 337.   |
| <b>Disable</b>   | Select this option to disable a service. All requests for a disabled service are rejected. When disabled, a red "X" appears over the icon and the service will refuse all requests. Disabling is a good alternative to <a href="#">deleting</a> a service.  |
| <b>Enable policy debug tracing</b>                     | <p>Select this option to enable tracing of policy execution for the current service. This may help you debug problems in your policy. When tracing is enabled, a green "bug" icon  appears over the service icon. For more information, see Policy Debug Tracing in the <i>Layer 7 Policy Authoring User Manual</i>.</p> <p><b>Notes:</b> (1) Enabling debug tracing will create a debug trace policy, if one doesn't exist yet. Disabling debug tracing will not remove the debug trace policy. (2) You can optionally allow the trace to inspect the backing policy of an encapsulated assertion.</p> <p><b>IMPORTANT:</b> Policy tracing should be used only for troubleshooting purposes, as it will degrade policy performance significantly.</p> |
| <b>Security Zone</b>                                   | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).</p>   |

| Label | Description   |
|-------|---|
|       | <b>Tip:</b> If you are updating a service, you can only choose zones to which you are permitted to update services. |

## Configuring the [HTTP/FTP] tab

The screenshot shows the 'Published Service Properties' dialog box with the 'HTTP/FTP' tab selected. The 'Service Resolution' section has two radio buttons: 'No resolution path' and 'Custom resolution path'. The 'Custom resolution path' is selected, and the text field next to it contains '/Playerstats'. Below this, a text label says 'The Gateway URL that receives requests for this service:' followed by a blue hyperlink 'http(s)://docssg1.l7tech.com:[port]/Playerstats'. A note states 'Note: The resolution path applies to both HTTP and FTP transport protocols.' and there is a 'Check for resolution conflicts' button. The 'Allowed HTTP Methods' section has a list of checkboxes: GET, HEAD, PUT, DELETE, POST (checked), OPTIONS, PATCH, and Other. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

Figure 143: Published Service Properties - [HTTP/FTP] tab

The [HTTP/FTP] tab contains service resolution settings for both HTTP and FTP protocols and the HTTP methods permitted.

Table 99: Service Properties - [HTTP/FTP] tab

| Label                     | Description  |
|---------------------------|--|
| <b>Service Resolution</b> | <p>Use this section to view or change the resolution path for a service.</p> <ul style="list-style-type: none"> <li><b>No resolution path:</b> (Applies to web services only) Select this option to set the resolution path to the default Gateway URI "/sfg/soap".</li> <li><b>Custom resolution path:</b> Select this option to enter a custom resolution URI for the service. A custom resolution path is mandatory for XML applications, but optional for web services.</li> </ul> |

| Label                                   | Description   |
|---|---|
|   | <p><b>Note:</b> The Custom resolution path cannot begin with "/srg".</p> <p>For more information, see <a href="#">"About the Resolution Path"</a> below.</p> <p><b>Tip:</b> Only enter a path that <i>completes</i> the embedded Gateway URL into the field—make sure that it does not duplicate any other Gateway resolution paths. You may include the "*" (asterisk) wildcard in the path to allow for any incoming URL following a certain pattern to resolve to this service. For details on how the wildcards are interpreted, see <i>Understanding the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>   |
| <b>[Check for resolution conflicts]</b> | <p>Click this button to check whether the service is resolvable via HTTP/FTP and which other services have resolution conflicts with this service. If conflicting services are displayed, enter a different <b>Custom resolution path</b> and then check again.</p> <p>If there are no issues with the resolution path, you will see the message <i>"No Conflicts. The service resolves successfully."</i></p>  |
| <b>Allowable HTTP Methods</b>           | <p>Select which HTTP methods are permitted for incoming requests. The Gateway supports these verbs: <b>GET, PUT, POST, DELETE, HEAD, PATCH, OPTIONS</b>. Select <b>Other</b> to allow any HTTP method name not already listed above.</p> <p>By default, SOAP web services accept only POST requests, while non-SOAP applications support GET, PUT, POST, DELETE. If you select no HTTP method, the service will not be accessible through HTTP, but it could still allow access through non-HTTP transport methods (for example, JMS, FTP, SSH, or email).</p> <p><b>IMPORTANT:</b> Use the "Other" option with care, as it can permit any arbitrary string in the incoming request. Be sure to validate the method name in policy, via the <code>\${request.http.method}</code> context variable. You can place the validation the service policy or in a 'message-complete' global policy fragment.</p> |

## Configuring the [WSDL] tab

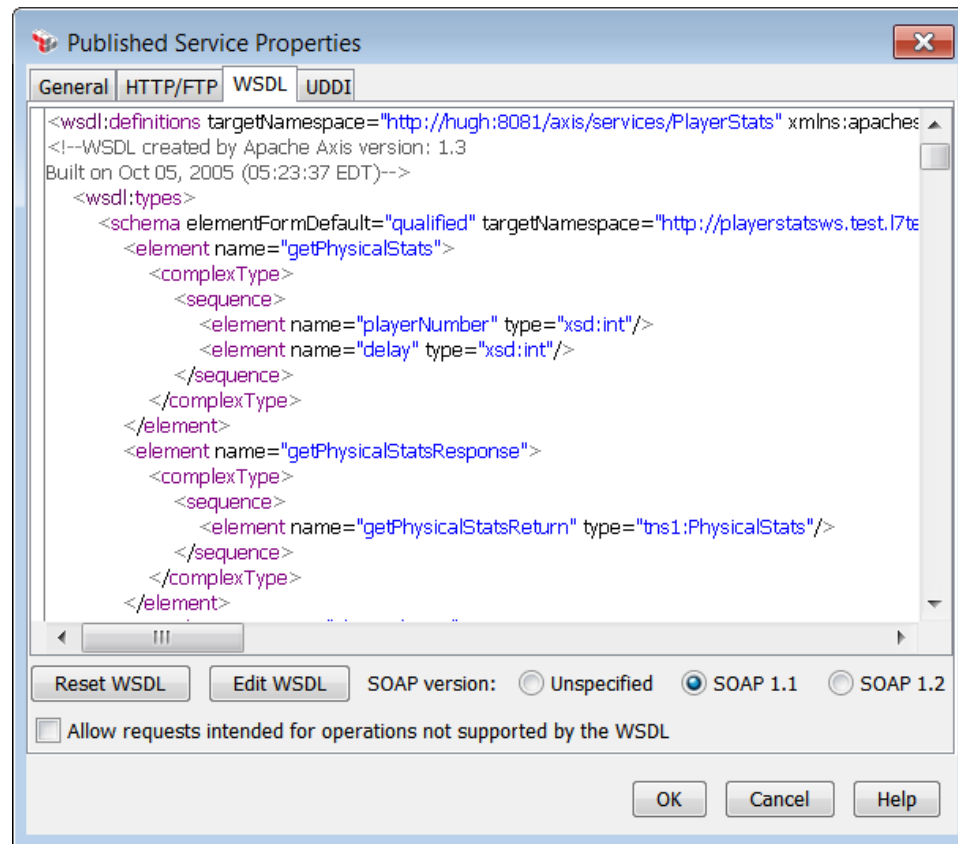


Figure 144: Published Service Properties - [WSDL] tab

The [WSDL] tab displays the WSDL document for a published web service. Scroll through the window to examine the WSDL. You can also right-click within the WSDL window to do the following:

- **Search the WSDL:** Select **Search a node** from the context menu to quickly jump to a specific node within the WSDL.
- **Copy lines from the WSDL:** Select **Copy** from the context menu to copy the selected lines from the WSDL. You can then paste these lines as text in another application.

**Note:** The [WSDL] tab is available only for SOAP web services.

Table 100: Service Properties - [WSDL] tab

| Label      | Description  |
|------------|--|
| Reset WSDL | You can change the WSDL for a published web service with another |

| Label   | Description   |
|---|---|
|   | <p>WSDL document. Once reset, the existing policy will become active for the resolution parameters extracted from the new WSDL document.</p> <p>For more information, see "Resetting the WSDL for a Service" on page 370.</p> <p><b>Note:</b> Resetting the WSDL is not possible for an <a href="#">internal service</a> or if the WSDL is under UDDI control (see the <a href="#">UDDI</a> tab).</p>   |
| <b>Edit WSDL</b>  | <p>You can modify the existing WSDL document for the service by clicking <b>[Edit WSDL]</b>. This opens the <i>Edit WSDL Wizard</i>, which leads you through the editing process. The wizard will be prepopulated with the contents of the WSDL document. You can add or remove operations by following the wizard.</p> <p>For more information, see "Create WSDL Wizard" on page 337.</p> <p><b>Note:</b> Editing the WSDL is not possible for an <a href="#">internal service</a> or if the WSDL is under UDDI control (see the <a href="#">UDDI</a> tab).</p>  |
| <b>SOAP version</b>   | <p>Select the SOAP version to be supported by the service:</p> <p><b>SOAP 1.1</b><br/> <b>SOAP 1.2</b><br/> <b>Unspecified</b> (either SOAP version is accepted)</p> <p><b>Note:</b> When a service is first published, the initial SOAP version is based on the bindings that are present in the WSDL and the order in which they appear.</p>  |
| <b>Allow requests intended for operations not supported by the WSDL</b> | <p>By default, the Gateway only permits SOAP requests for operations supported by the service's WSDL. If you need to override this behaviour for the selected web service, select the <b>[Allow requests intended for operations not supported by the WSDL]</b> check box.</p> <p>You should select this check box only if you need to do any of the following:</p> <ul style="list-style-type: none"> <li>• Allow SOAP messages that are not explicitly supported in the WSDL.</li> <li>• Allow non-SOAP messages to be sent to a SOAP service.</li> <li>• Allow encryption of the Body element in the SOAP request to pass through the Gateway (for example, if the Gateway is unable to decrypt the contents of the Body element).</li> <li>• Bypass the SOAP version check (e.g., allows a SOAP 1.1 request to be sent to a service marked as SOAP 1.2, although warning messages will continue to appear about incompatible XPath namespaces).</li> </ul> <p>To learn more about how the Gateway resolves a request, see <i>Understanding the Service Resolution Process</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <p><b>Note:</b> You should specify a custom resolution path (in the <a href="#">[HTTP]</a> tab) if</p> |

| Label | Description  |
|-------|--|
|       | <p>you are enabling the "<b>Allow requests intended for...</b>" feature. Otherwise, a request could fail under the following conditions:</p> <ul style="list-style-type: none"> <li>• A service uses distinct SOAPAction values in its operations, AND</li> <li>• A request arrives with a SOAPAction value that is not supported by the service's WSDL.</li> </ul> <p>A custom resolution path is optional if the WSDL for a service does not specify any SOAPAction values or uses the same SOAPAction value for all operations.</p> |

## Configuring the [UDDI] tab

Published Service Properties

General HTTP/FTP WSDL **UDDI**

Original UDDI Business Service

UDDI Registry

BusinessService Name

BusinessService serviceKey

wsdl:port

wsdl:binding

wsdl:binding namespace

Select Clear

UDDI Settings

WSDL under UDDI control ☐

Monitoring Enabled ☐

Update WSDL ☐

Disable service if WSDL has changed ☐

View Publish to UDDI Settings

OK Cancel Help

Figure 145: Published Service Properties - [UDDI] tab

The [UDDI] tab displays which Business Service and UDDI registry were used to find the WSDL used to create the service. The settings here will affect the available options in the Publish to UDDI dialog.

Table 101: Service Properties - [UDDI] tab

| Label                                 | Description  |
|---------------------------------------|--|
| <b>Original UDDI Business Service</b> | This section is the Gateway's record of how the published service was created. The information makes it possible to place the WSDL under the control of the UDDI registry, enabling the Gateway to monitor it for changes to the endpoint and WSDL.  |
| <b>Select</b>                         | <p>Click <b>[Select]</b> to associate the service with a UDDI Business Service. Do this if you wish to place an existing service under UDDI control, or to change an existing association.</p> <p>Use the Search UDDI dialog to locate the Business Service to associate with. For more information, see Searching the UDDI Registry in the <i>Layer 7 Policy Authoring User Manual</i>.</p> <p><b>Tip:</b> If there is an existing association, you must click <b>[Clear]</b> first to clear it before selecting another one. If you receive a message stating that the Gateway WSDL is stale, you can refresh it by using <b>[Reset]</b> on the <b>[WSDL]</b> tab of this dialog.</p>  |
| <b>Clear</b>                          | <p>Click <b>[Clear]</b> to remove an association between the published service and a UDDI Business Service.</p> <p>You must clear an existing association before you can use <b>[Select]</b> to establish a new association.</p> <p><b>Note:</b> It is not possible to clear the original business service if a Gateway endpoint has been published to it or if the original service has been overwritten. In those cases, the publish must be reversed using the <b>[Don't Publish]</b> option in the [Service] tab of the Publish to UDDI Settings dialog before <b>[Clear]</b> can be used to clear the association.</p>  |
| <b>UDDI Settings</b>                  | When a service was created from a WSDL found in a UDDI registry, this section is enabled and the <b>WSDL under UDDI control</b> check box is selected by default.  |
| <b>WSDL under UDDI control</b>        | <p>When selected, this check box indicates that the service is associated with a UDDI Business Service and a wsdl:port (binding template). When the WSDL is under UDDI control, the following options are not available:</p> <ul style="list-style-type: none"> <li>[Service] tab of the Publish to UDDI Settings dialog: <ul style="list-style-type: none"> <li>Publish Gateway endpoint as BindingTemplate</li> <li>Overwrite existing BusinessService with Gateway URLs</li> </ul> </li> <li><b>[WSDL]</b> tab of Service Properties: <ul style="list-style-type: none"> <li>Reset WSDL</li> <li>Edit WSDL</li> </ul> </li> </ul> <p>If the WSDL cannot be placed under UDDI control, this check box is disabled. For example, if the existing service is overwritten, it is no longer under UDDI control. This check box is also disabled when the action <b>[Publish Gateway endpoint as BindingTemplate]</b> is taken in the [Service] tab of the Publish to UDDI Settings dialog.</p> <p>You may also clear this check box yourself if you wish to manually</p> |

| Label                                      | Description   |
|--|---|
|  | remove the WSDL from under UDDI control. This will re-enable all the disabled controls described above.   |
| <b>Monitoring Enabled</b>                  | <p>This check box is enabled only when <b>[WSDL under UDDI control]</b> is selected. It enables monitoring at the service level. The type of monitoring is determined by the UDDI registry configuration.</p> <p>When monitoring is enabled, any changes to the Business Service in the UDDI registry are detected by the Gateway and the following will occur:</p> <ul style="list-style-type: none"> <li>• The Gateway downloads the UDDI Business Service. The values from UDDI are validated to match the Gateway's WSDL. If they do not match, the association with the original Business Service is deleted. If they do match, the value of the accessPoint which belongs to the monitored bindingTemplate is checked. If it differs from the existing known endpoint value, the service.defaultRoutingURL context variable is updated to contain the new value.</li> <li>• If the <b>[Update WSDL]</b> check box is selected, the Gateway updates its WSDL.</li> <li>• If the <b>Disable service if WSDL has changed</b> check box is selected, the Gateway disables the published service when the WSDL changes.</li> </ul> |
| <b>Update WSDL</b>                         | <p>Select this check box to instruct the Gateway to update its WSDL document if changes in the WSDL under UDDI control are detected. The Gateway downloads and checks the WSDL for changes.</p> <ul style="list-style-type: none"> <li>• If there are no changes, no further action is taken.</li> <li>• If changes have occurred, then the published service's WSDL is updated.</li> </ul> <p>The Gateway logs and audits at the "Warning" level that the WSDL has changed. The Gateway then updates the <i>service.defaultRoutingURL</i> context variable with the service endpoint. <b>Note:</b> This will occur if the endpoint URL changes in the UDDI even when the WSDL itself has not changed.</p>  |
| <b>Disable service if WSDL has changed</b> | Select this check box to instruct the Gateway to disable the published service if changes in the WSDL under UDDI control are detected.  |
| <b>View Publish to UDDI Settings</b>       | Click this button to view the settings in the Publish to UDDI Settings dialog. The information is read only when displayed in this manner. To make changes to the settings, see Publish to UDDI Settings in the <i>Layer 7 Policy Authoring User Manual</i> .   |



## About the Resolution Path

A resolution path must be specified when a web service is [published](#). If a custom resolution path was not specified, the default URI `"/ssg/soap"` is used and only requests directed to this URI will be consumed. Should you attempt to republish the same web service, you must specify a different resolution path in order to differentiate between the two services.

When an XML application is published, specifying a custom resolution path is mandatory. Some resolution paths are reserved for internal use. If you enter a custom resolution path that conflicts with an internal one, you will see a warning message.

The custom resolution path can be entered using the [Publish SOAP Web Service Wizard](#) and can be entered, changed, or removed using the [Service Properties](#) ([HTTP/FTP] tab). It is displayed in the [Services and Policies list](#) next to the service name. For example, the name will appear as `"ServiceName [/customPath]"` instead of simply `"ServiceName"`.


For information on how the Gateway resolves the destination web service, see *Understanding the Service Resolution Process* in the *Layer 7 Installation and Maintenance Manual*.

---

**Tips:** (1) The resolution path for published services apply to both HTTP and FTP-based transports. This allows (for example) consumption of non-SOAP traffic over FTP, multiple versions of the same service consumed over FTP, etc. (2) Since the default service resolution process uses SOAP payload namespace URI and SOAPAction values, customizing the resolution path of a web service allows the same WSDL to be published more than once. Without a customized resolution path, duplication would result in runtime ambiguity.

---

## Disabling a Service

You may disable a service if you need to make it unavailable temporarily. When disabled, the service's icon appears as  and the service will refuse all requests.

Disabling is a good alternative to [deleting](#) a service.

---

**Tip:** Disabling a service occurs immediately on the node that your Policy Manager is connected to. For other nodes in the cluster, it may take approximately 20 seconds for the disabling to take effect.

---

➤ *To disable a service:*

1. Open the service properties by doing one of the following:

- Right-click the web service or XML application under the [Services and Policies list](#) and then select **Properties**.
  - Select **[File] > Service Properties** from the [Main Menu](#).
2. In the [\[General\] tab](#), select **[Disable]**.
  3. Click **[OK]**. The service is now disabled and all requests to this service will be rejected.

## Enabling a Service

You can enable any disabled service. Once enabled, a service will respond to requests.

---

**Tip:** Enabling a service occurs immediately on the node that your Policy Manager is connected to. For other nodes in the cluster, it may take approximately 20 seconds for the enabling to take effect.

---

➤ *To enable a service:*

1. Open the service properties by doing one of the following:
  - Right-click the web service or XML application under the [Services and Policies list](#) and then select **Properties**.
  - Select **[File] > Service Properties** from the [Main Menu](#).
2. In the [\[General\] tab](#), select **[Enable]**.
3. Click **[OK]**. The service is now enabled.

## Renaming a Service

You can change the display name for a service. This name appears in the [services and policies list](#) and in the policy tabs.

➤ *To rename a service:*

1. Open the service properties by doing one of the following:
  - Right-click the web service or XML application under the [Services and Policies list](#) and then select **Properties**.
  - Select **[File] > Service Properties** from the [Main Menu](#).
2. In the [\[General\] tab](#), edit the **Service Display Name** field as required.
3. Click **[OK]**. The service name is updated on the interface.

## Deleting a Published Service

Deleting a published service removes the service properties, settings, and service policy from the Policy Manager and Gateway.

### W A R N I N G

Deleting a service is permanent and cannot be reversed. A safe alternative to deleting is to disable the service instead.

➤ *To delete a published service:*

1. In the [Services and Policies](#) list, right-click the service name and then select **Delete**. Alternatively, select [**File**] > **Delete Service** from the [Main Menu](#).
2. Click [**Yes**] to confirm. The service is removed and all policy tabs for that service are removed. Metric data for the deleted service is not deleted immediately and will gradually age out as time passes. If the service has data published to UDDI, you will be warned that the UDDI data will be left behind in the UDDI registry after the service is deleted from the Gateway.

## Viewing the WSDL for a Service

You can view the WSDL document for any [published web service](#).

➤ *To view the WSDL for a service:*

1. Open the service properties by doing one of the following:
  - Right-click the web service or XML application under the [Services and Policies](#) list and then select **Properties**.
  - Select [**File**] > **Service Properties** from the [Main Menu](#).
2. Select the [\[WSDL\] tab](#). The WSDL document is displayed in the tab. From this tab, you can do the following tasks:
  - Reset the WSDL for the service.
  - Edit the WSDL for the service.

For more information, see ""[Configuring the \[WSDL\] tab](#)" on page 362" under [Service Properties](#).

## Resetting the WSDL for a Service

You can change the WSDL for a [published web service](#) with another WSDL document. Once reset, the existing policy will become active for the resolution parameters extracted from the new WSDL document.

---

**Note:** Resetting the WSDL is not possible for an [internal service](#) or if the WSDL is under UDDI control (see the [\[UDDI\] tab](#) of a service's properties).

---

➤ *To reset a web service WSDL:*

1. Open the properties for a service and then select the [WSDL] tab. For more information, see "Service Properties" on page 357.
2. Click **[Reset WSDL]**. The Reset WSDL dialog appears.
3. In the **Location** field, enter the URL that will resolve the new web service WSDL. Alternatively:
  - If the WSDL is contained in a file, click **[File]** and select the file.
  - If the WSDL is from a UDDI registry, click **[UDDI]** and complete the Search UDDI dialog. For more information, see Searching the UDDI Registry in the *Layer 7 Policy Authoring User Manual*.
  - To configure options for the URL (for example, to specify the credentials or configure a proxy), click **[HTTP Options]** to open the "Managing HTTP Options" on page 188 dialog.

---

**IMPORTANT:** If you are specifying a URL and that URL uses SSL (e.g., <https://webserver/service.wsdl>), the SSL certificate for that secure server (e.g., <https://webserver>) must first be added to the federated gateway trust store. To do this:

---

- a. Follow "Adding a New Certificate" on page 239 to add the SSL certificate.
- b. In Step 3 of the "Add Certificate Wizard" on page 240, be sure to select the **Outbound SSL Connections** option.

Once this is done, the SSL WSDL can be successfully retrieved.

3. Click **[OK]**. The service is updated with the new WSDL URL.

## Changing the Resolution Path for a Service

A web service may be configured to either have no resolution path (in which case the default Gateway URI `/sso/soap` is used) or it may have a custom resolution path. For more information, see ["About the Resolution Path"](#) in [Service Properties](#).

➤ *To change the resolution path for a service:*

1. Open the service properties by doing one of the following:
  - Right-click the web service or XML application under the [Services and Policies list](#) and then select **Properties**.
  - Select **[File] > Service Properties** from the [Main Menu](#).
2. Select the **[HTTP/FTP]** tab. The current resolution path is displayed under **Service Resolution**.
3. Change the resolution path as necessary. For a description of the settings, see ["Configuring the \[HTTP/FTP\] tab"](#) in [Service Properties](#).

## Working with Internal Services

An internal service is a category of [published services](#) within the CA API Gateway that has all associated information and WSDL information predefined. An internal service is like a standard web service that is defined in the Gateway.

Certain internal services may automatically insert assertions into your policy. These assertions can be used as a starting point for you to customize the service logic to meet your needs.

---

**Tip:** Do not confuse internal services with *internal use policies*. The former are web services that require publishing, while the latter are like policy fragments that are inserted into a service policy. An internal service may or may not insert assertions into your service policy. For more information, see [Working with Internal Use Policies](#) in the *Layer 7 Policy Authoring User Manual*.

---

For information on how to publish an internal service, see ["Publishing an Internal Service"](#) on page 374. Note that certain internal services may be set up via auto-provisioning, meaning they can be set up by the Gateway administrator, without using the ["Publish Internal Service Wizard"](#) on page 375 in the Policy Manager. These are noted below.

The following internal services are currently available:

### Gateway Management Service

This service can be used to remotely administer the Gateway (cluster) using a SOAP client.

Examples of clients include the Java API or the Management Client command line utility, both supplied by CA Technologies.

For information on using the Gateway Management interface, refer to the document *"Using the Gateway Management Interface"*. This document is available from CA Technical Support.

---

**Tip:** The Gateway Management Service may be set up via auto-provisioning. For more information, see "Auto-Provisioning an Internal Service" in the *Layer 7 Installation and Maintenance Manual*.

---

### Gateway REST Management Service

This service provides a REST API for managing the Gateway.

For information on using the Gateway REST Management interface, refer to the document *"Using the Gateway Management Interface"*. This document is available from CA Technical Support.

---

**Tip:** The Gateway REST Management Service may be set up via auto-provisioning. For more information, see "Auto-Provisioning an Internal Service" in the *Layer 7 Installation and Maintenance Manual*.

---

### Generic Identity Management Service

This is a generic service that provides a standardized way of authenticating users and extracting authorization information using facilities provided by the CA API Gateway.

---

**Tip:** When publishing the Generic Identity Management Service, CA Technologies recommends using the default routing URI.

---

For information on using the Generic Identity Management Service, see "Working with the Generic Identity Management Service" on page 382.

### Security Token Service

This service is used to control the security tokens that have been issued or will be issued. This service requires a WSDL for publishing and it will add a default policy for low level details such as customizing various token requirements (types of tokens issued, authentication mechanisms, etc.). For example, the policy uses the Create SAML Token assertion for creating SAML Tokens with various SAML specification options (e.g., a choice of SAML AuthenticationStatement or AttributeStatement). It uses the Create Security Context Token assertion to create a Security Context Token and applies different authentication as needed.

For information on using the Security Token Service, see "Working with the Security Token Service" on page 377.

### UDDI Notification Service

This service allows a client to be notified when there are changes to the UDDI registry. It will create an internal notification policy with a single Handle UDDI Subscription Notification assertion. **Note:** Ensure that the UDDI Notification service has also been published to a UDDI registry. This will enable the **[Subscribe for notification]** setting in the UDDI Registry Properties. For more information, see Publish to UDDI Settings in the *Layer 7 Policy Authoring User Manual*.

### WSDM QosMetrics Service

This service allows a client to request metrics data for a given managed resource. It has one method: *GetMultipleResourceProperties*. To specify the resource from which you are requesting metrics, see "[Specifying a Resource for a WSDM Service](#)" below. For a list of supported metrics, refer to Collect WSDM Metrics assertion.

### WSDM Subscription Service

This service allows a client to subscribe to receive notifications about changes in a resource. It has three methods: *Subscribe*, *Renew*, *Unsubscribe*. To specify the resource to which you are subscribing, see "[Specifying a Resource for an WSDM Service](#)" below.

## Specifying a Resource for an WSDM Service

To specify a resource for either of the WSDM internal services, you can use any of the following techniques:

### Include the resource ID within the URL

The resource ID is appended to the query string as follows:

*http://<gateway\_host>:8080/wsdm/qosmetrics?serviceoid=12345*

where '12345' is the resource entity ID. To locate your resource entity ID, access the [service's properties](#) and look for the "Service GOID" in the [General] tab.

### Include the resource ID as part of the SOAP message

A message is sent to *http://<gateway\_host>:8080/wsdm/qosmetrics*, with the resource ID embedded within the message:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
  xmlns:wsrf-rp="http://docs.oasis-open.org/wsrf/rp-2"
  xmlns:muws1="http://docs.oasis-open.org/wsdm/muws1-2.xsd"
  xmlns:muws2="http://docs.oasis-open.org/wsdm/muws2-2.xsd"
  xmlns:mows="http://docs.oasis-open.org/wsdm/mows-2.xsd">
  <soap:Header>
    <wsa:Action>
      http://docs.oasis-open.org/wsrf/rpw-2/GetMultipleResourceProperties ...
    </wsa:Action>
    <muws1:ResourceId>
      http://ssghost:8080/service/12345
    </muws1:ResourceId>
    ...
  </soap:Header>
</soap:Envelope>
```

### Include the resource URI within the URL of the query string

The resource URI is appended to the query string as follows:

*http://<gateway\_host>:8080/wsdm/qosmetrics?serviceuri=/myuris/service1uri*

This technique requires that the service URI resolves to exactly one service, otherwise a SOAP fault will be returned.

---

**Tip:** If the URI resolves to multiple services, try using the serviceoid method instead (see "Include the resource ID within the URL" above).

---

### Case Sensitivity for Locating WSDM Services

By default, matching of resource URIs is done in a case-sensitive manner. If case sensitivity for service resolution is disabled, the matching of resource URIs is affected accordingly.

For example, the service can be identified by a path ("Include the resource URI within the URL of the query string") and a request may be sent to:

*http://localhost:8080/wsdm/qosmetrics?serviceuri=/warehouse*

In the example above, the value "warehouse" will be compared case sensitively or case insensitively, depending on the resolution settings.

For information on case sensitivity during service resolution, see "Managing Service Resolution" on page 196.

### Publishing an Internal Service

Publishing an internal service does the following:

1. Adds the service to the [Services and Policies](#) list on the Policy Manager interface.
2. Establishes the service's initial policy in the policy development window.



For the WSDM internal services, the publishing process will automatically add a Collect WSDM Metrics or Subscribe to WSDM Resource assertion to the policy, depending on the service published. These assertions should not be deleted from the policies, as they are necessary for connecting to the WSDM metrics calculation service.

For the UDDI service, the publishing will process will automatically add a Handle UDDI Subscription Notification assertion to the policy.

As with all Gateway-published services, you can publish multiple instances of the same internal service—simply ensure that each contains a [unique resolution URI](#). After publication, you can view the service's WSDL code from within the [service properties](#).

---

**Notes:** (1) You must have a role of *Administrator* to publish or modify an internal service. Once a service is published, the *Manage [serviceName] Service* role can be used to give users Administrator-like powers for that specific service only. For more information, see "Predefined Roles and Permissions" on page 132. (2) If the internal service was auto-provisioned, you do not need to run the "Publish Internal Service Wizard" on page 375 as described below. For more information, see "Auto-Provisioning an Internal Service" in the *Layer 7 Installation and Maintenance Manual*.

---

Choose a task to perform:

Table 102: Internal service tasks

| For information on how to...                            | See   |
|---|---|
| <b>Publish an internal service</b>                      | "Publish Internal Service Wizard" on page 375 |
| <b>Delete an internal service</b>                       | "Deleting a Published Service" on page 369    |
| <b>Change the routing URI for an internal service</b>   | "Service Properties" on page 357              |
| <b>View the predefined WSDL for an internal service</b> | "Service Properties" on page 357              |

## Publish Internal Service Wizard

The *Publish Internal Service Wizard* is used to [publish an internal service](#) onto the Gateway. Publishing an internal service is very similar to publishing a normal SOAP web service, except the WSDL is predefined and the necessary assertions are automatically added. The only input required for this wizard is the routing URI.

To learn about the internal services currently available, see "Working with Internal Services" on page 371.

---

**Note:** To publish an internal service, you must have the Administrator role. For more information, see "Predefined Roles and Permissions" on page 132.

---

➤ To run the Publish Internal Service Wizard:

1. Do any of the following:

- Click **Publish Internal Service** on the [Home Page](#)
- Select [Tasks] > **Publish Internal Service** from the [Main Menu](#)
- Right-click a folder within the [Services and Policies](#) list and then select **Publish Internal Service**.

The Publish Internal Service Wizard appears.

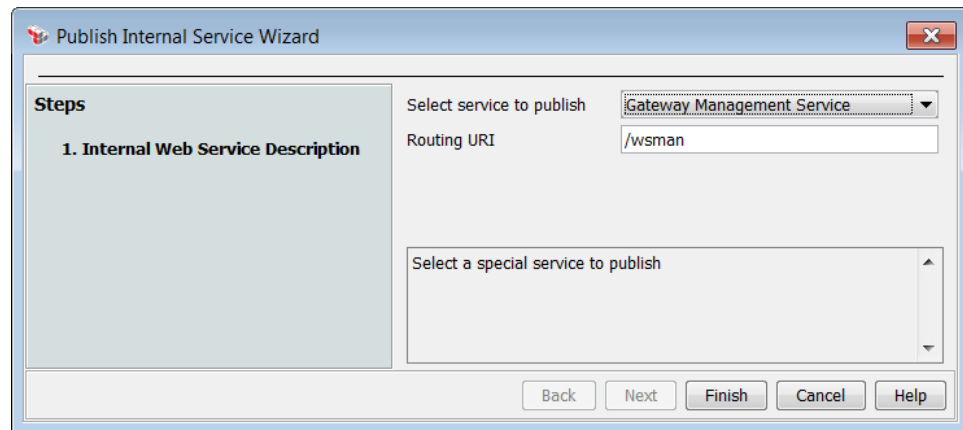


Figure 146: Publish Internal Service Wizard

2. Complete the wizard as described below.

Table 103: Using the Publish Internal Service Wizard

| Setting  | Description  |
|--|--|
| <b>Select service to publish</b>                           | From the drop-down list, select the internal service to publish. For a description of each service, see "Working with Internal Services" on page 371.  |
| <b>Routing URI</b>   | Each internal service has its own default routing URI. Either accept this URI or enter a custom routing URI. Every service URI prefix must be unique. The Policy Manager will warn you if the routing URI is already in use. You can change the routing URI later through the [HTTP/FTP] tab of the <a href="#">service properties</a> .<br><br><b>Notes:</b> (1) Internal services cannot use the "ssg/soap" prefix used by <a href="#">SOAP web services</a> . (2) The routing URI for the Gateway REST Management Service must end with "/*". |
| <b>WS-Trust Namespace</b><br>(Security Token Service only) | When publishing a 'Security Token Service', select the WS-Trust namespace to use from the drop-down list. If the namespace you need is not listed, type the namespace in the field.  |

3. When you are satisfied everything is correct, click [**Finish**] to publish the service.  
**Tip:** If you've specified a conflicting service resolution, you are given the option to correct the conflict, proceed as is, or cancel the publishing.

When the wizard is complete, the newly published service appears in the [Services and Policies](#) list and in the policy development window, with any required accompanying assertion already added. You can now begin constructing your new policy. For more information, see Policy Organization in the *Layer 7 Policy Authoring User Manual*.

After creating the new internal service, you can send requests to it by using one of the following URIs:

**http://**<machinename.domain.com>:**8080**<serviceURIsuffix>

**https://**<machinename.domain.com>:**8443**<serviceURIsuffix>

Where:

- <machinename.domain.com> is the name of the computer hosting the Gateway
- <serviceURIsuffix> is the Routing URI entered in the Publish Internal Service Wizard or in the [service properties](#).

## Working with the Security Token Service

The CA API Gateway has a Security Token Service (STS) that can issue the following types of tokens:

- SAML Tokens (via the Create SAML Token assertion)
- Security Context Tokens (via the Create Security Context Token assertion)

Issued tokens can be returned in a Request Security Token Response (RSTR) using the Build RSTR SOAP Response assertion. Security Context Tokens can be cancelled using the Cancel Security Context assertion.

The Security Token Service can be published in a policy using the "Publish Internal Service Wizard" on page 375.

## Understanding the Security Token Service Default Policy

Table 104 describes the default policy that is created when you [publish](#) the Security Token Service internal policy. The comments provide additional detail to help you understand the logic behind the policy.

**Tip:** The default policy is intended to help you get started using the Security Token Service. Though useful, this policy may or may not satisfy your security requirements. Feel free to modify it as required to suit your needs.

Table 104: Security Token Service default policy

| Policy line   | Comment  |
|---|--|
| Audit Messages in Policy  |  |
| Set Context Variable 'Flag_Enable_Response_Decoration' as false | The flag is used to determine if enabling or disabling the RSTR response decoration  |
| All Assertion...  | <i>Block for any Authentication/Authorization Mechanisms (so it is customizable)</i> |
| At Least One...   |  |
| All Assertion...  | Authentication Option #1: Credentials over Message Level                             |
| At Least One...   |  |
| Require Encrypted UsernameToken Profile Credentials             |  |
| Require WS-Security Signature Credentials                       |  |
| Require SAML Token Profile                                      |  |
| Require WS-SecureConversation                                   |  |
| Require Signed Timestamp  |  |
| At Least One...   |  |
| Require Signed Element on the SOAP1.1 body                      |  |
| Require Signed Element on the SOAP1.2 body                      |  |
| Set Context Variable 'Flag_Enable_Response_Decoration' as true  | Enable the RSTR response decoration  |
| All Assertion...  | Authentication Option #2: Credentials over SSL transport                             |
| Require SSL or TLS Transport                                    |  |
| At Least One...   |  |

| Policy line   | Comment  |
|---|--|
| Require HTTP Basic Credentials  |  |
| Require WS-Security UsernameToken Profile Credentials                     |  |
| Require SSL or TLS Transport with Client Authentication                   |  |
| Set Context Variable 'Flag_Enable_Response_Decoration' as false           | Disable the RSTR response decoration   |
| Comment   | Add any extra authentication assertions into the "At least one ..." folder below   |
| At Least One...   |  |
| Authenticate against Internal Identity Provider                           |  |
| Evaluate Request XPath  | Retrieve the value of <i>RequestType</i> in the request message and save it into a variable <code>\${requestType.result}</code>  |
| At Least One...   |  |
| All Assertions...   | Branch for SAML token issuance   |
| Compare Expression: <code>\${requestType.result}</code> contains "/Issue" | Confirm that the request is for issuing a security token   |
| Evaluate Request XPath  | Retrieve the value of <i>TokenType</i> in the request message and save it into the variable <code>\${tokenType.result}</code>  |
| All Assertions...   | Verify the <i>TokenType</i> if matching one of two SAML token URIs (v1.1 and v2.0).  |
| At Least One...   |  |
| All Assertions...   |  |
| Compare: <code>\${tokenType.result}</code> contains "SAML2.0"             | Confirm that the value of <i>TokenType</i> matches <a href="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0">http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0</a> |
| Create SAML Token   | Create a SAML v2.0 token and save it into the context variable <code>\${issuedSamlAssertion}</code>  |
| All Assertions...   |  |

| Policy line   | Comment   |
|---|---|
| Compare: \${tokenType.result}<br>contains "SAML 1.1"            | Confirm that the value of <i>TokenType</i> matches<br><a href="http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1">http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV1.1</a> |
| Create SAML Token   | Create a SAML v1.1 token and save it into the context variable <i>\${issuedSamlAssertion}</i>   |
| At Least One...   |   |
| Build RSTR SOAP Response  | Build an RSTR SOAP response containing the issued SAML token represented by <i>\${issuedSamlAssertion}</i>  |
| Continue Processing   | Handle the failure of the previous assertion; enables a SOAP fault response to be passed to the <i>Return Template Response to Requestor</i> assertion  |
| All Assertions...   | <i>Branch for Security Context Token issuance (SCT)</i>   |
| Compare Expression: \${requestType.result}<br>contains "/Issue" | Confirm that the request is for issuing a security token  |
| Evaluate Request XPath  | Retrieve the value of <i>TokenType</i> in the request message and save it into the variable <i>\${tokenType.result}</i>   |
| Compare Expression: \${tokenType.result}<br>contains "/sct"     | Confirm that the request is for issuing a SCT   |
| Create Security Context Token                                   | Create an SCT and save it to the context variable <i>\${sctBuilder.issuedSCT}</i>   |
| At Least One...   |   |
| Build RSTR SOAP Response  | Build an RSTR SOAP response containing the issued SCT   |
| Continue Processing   | Handle the failure of the previous assertion; enables a SOAP fault response to be passed to the <i>Return Template Response to Requestor</i> assertion  |
| All Assertions...   | <i>Branch for Security Context Cancellation</i>   |
| Compare Expression: \${request.result}<br>contains "/Cancel"    | Confirm that the request is for cancelling an SCT   |
| Cancel Security Context   | Cancel the security context identified by the <i>cancelTarget</i> element   |

| Policy line   | Comment  |
|---|--|
| At Least One...   |  |
| Build RSTR SOAP Response  | Build an RSTR SOAP response containing the result of the token cancellation  |
| Continue Processing   | Handle the failure of the previous assertion; enables a SOAP fault response to be passed to the <i>Return Template Response to Requestor</i> assertion |
| All Assertions...   | <i>Branch for any other requests</i>   |
| Stop Processing   | This stops processing if any other requests are encountered  |
| All Assertions...   |  |
| Request: Require WS-Addressing                                    | Get the message ID, which will be passed into the assertion below  |
| Add WS-Addressing   | Add WS-Addressing into the RSTR response   |
| Return Template Response to Requestor                             | <i>Make a template response; this will be decorated in the next step and sent back to the requestor</i>  |
| At Least One...   | <i>Decorate the RSTR response message before sending it back to the requestor</i>  |
| All Assertions...   |  |
| Compare Expression: \${Flag_Enable_Response_Decoration} is "true" | Check if RSTR Response Decoration is enabled or disabled   |
| All Assertions...   |  |
| Comment   | Add, remove, or modify decoration requirement as needed  |
| Response: Sign Element: Body                                      | Sign the SOAP Body   |
| Response: Encrypt Element: Body                                   | Encrypt the SOAP Body  |
| Response: Configure WS-Security Decoration                        | Add signed Timestamp, sign WS-Addressing, and encrypt Signature  |
| Response: Apply WS-Security                                       | Apply all WS-Security decoration requirements  |
| Continue Processing   | If the decoration is disabled, then continue policy processing   |

In the sample policy in Table 104, *wsa:Action* is used to distinguish the request type. However note that while WS-Trust uses the same *Action URI* for different request types (see Table 105 and Table 106), WS-Secure Conversation requires different *Action URIs* for different request types. As a result, if the internal service is used in a WS-Trust context, the *Action URI* alone is insufficient for verifying a request type; further verification will be needed—for example, using *TokenType* in the RST to verify what type of token will be issued.

**Note:** The WS-Trust entries shown in the tables below are for WS-Trust 1.2. Requests for Security Token Services corresponding to other versions of WS-Trust will use different URIs. These URIs are used as values in the *<RequestType>* element of the request. The WS-SecureConversation entries in the tables below are for WS-SecureConversation 1.2, but this version can be used in regardless of the WS-Trust version.

Table 105: Action URIs for request type 'issue SAML token'

| Request Type                        | Request to issue SAML                                 |
|-------------------------------------|---|
| Action URI in WS-Trust              | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue |
| Action URI in WS-SecureConversation | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue |

Table 106: Action URIs for request type 'issue SCT'

| Request Type                        | Request to issue Security Context Token (SCT)         |
|-------------------------------------|---|
| Action URI in WS-Trust              | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue |
| Action URI in WS-SecureConversation | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT   |

Table 107: Actions URLs for request type 'cancel token'

| Request Type                        | Request to cancel token                                    |
|-------------------------------------|--|
| Action URI in WS-Trust              | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Cancel     |
| Action URI in WS-SecureConversation | http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel |

## Working with the Generic Identity Management Service

The Generic Identity Management Service (GIMS) is an [internal service](#) that provides a standardized way of authenticating users and extracting authorization information (such as group membership) using the facilities provided by the CA API Gateway. The GIMS provides a set of APIs that can be consumed by an external application to authenticate a user against custom identity providers and retrieve authorization information.



By default, the GIMS only supports only authentication operations against the [Internal Identity Provider](#). Support for other providers (such as LDAP or Federated) will require policy modifications. Please [contact](#) CA Technical Support for assistance with other providers or if you need to perform user/group management operations with the GIMS.

---

**Tip:** The Generic Identity Management Service is configured as a service; at the policy level, you can authenticate users with the `Authenticate Against Identity Provider` or `Authenticate User or Group` assertions.

---

## Using the Generic Identity Management Service

➤ To authenticate a user via the Generic Identity Management Service:

1. Publish the GIMS in a policy using the "Publish Internal Service Wizard" on page 375. This is the internal service that will perform user authentication against identity provider(s):

**`/gims/<version>/authenticate`**

where "`<version>`" is the version of the service deployed ("1" if the default routing URL is used)

2. Modify the template policy to configure an identity provider. **Tip:** [Search](#) the policy for "Comment". The Add Comment to Policy assertion is used to provide placeholders in the places where the identity provider is defined.
3. From the client side, call the service using the POST method to authenticate a user:

**`POST /gims/<version>/authenticate`**

The following table describes the parameters to be provided during authentication. **Tip:** These parameters are used by the default policy, but you may modify the default policy to meet your needs.

Table 108: Parameters for GIMS user authentication

| Parameter       | Type   | Required | Comment                                    |
|-----------------|--------|----------|--|
| <b>username</b> | string | Yes      | login name of the user to be authenticated |
| <b>password</b> | string | Yes      | user password credential                   |
| <b>format</b>   | string | No       | XML/JSON; default is XML                   |

**Note:** The user account locks after 10 failed authentication attempts. The default lockup period is 1 hour, during which all authentication attempts will fail, even with the correct credentials. The lockout counter resets after every successful authentication. The lockout does not affect Internal Identity Provider accounts accessed via the Policy Manager, it only affects the Generic Identity Management Service.

4. After successful authentication, the CA API Gateway will return user authorization information in the format specified (XML/JSON).

#### Example of authorization info

```
<L7gims:service xmlns:L7gims="http://www.layer7tech.com/2012/12/L7gims">
  <L7gims:users>
    <L7gims:user>
      <L7gims:version>1</L7gims:version>
      <L7gims:dn>295403520</L7gims:dn>
      <L7gims:attr>
        <L7gims:attr-name>login</L7gims:attr-name>
        <L7gims:attr-value>user</L7gims:attr-value>
      </L7gims:attr>
      <L7gims:attr>
        <L7gims:attr-name>givenName</L7gims:attr-name>
        <L7gims:attr-value>First</L7gims:attr-value>
      </L7gims:attr>
      <L7gims:attr>
        <L7gims:attr-name>sn</L7gims:attr-name>
        <L7gims:attr-value>Last</L7gims:attr-value>
      </L7gims:attr>
      <L7gims:attr>
        <L7gims:attr-name>mail</L7gims:attr-name>
        <L7gims:attr-value>user@domain</L7gims:attr-value>
      </L7gims:attr>
      <L7gims:attr>
        <L7gims:attr-name>accountExpires</L7gims:attr-name>
        <L7gims:attr-value>1969-12-31T23:59:59.999Z</L7gims:attr-value>
      </L7gims:attr>
    </L7gims:user>
  </L7gims:users>
</L7gims:service>
```

The returned authorization information is defined as a list of attributes in XML or JSON form. Table 109 lists the standard attributes. Except for **dn**, all attributes are optional. Any additional attributes can be added for the specific client via policy.

**Tip:** The following is the XML schema that describes the GIMS authorization information response: *gims.xsd*: <https://wiki.l7tech.com/mediawiki/images/8/87/Gims.xsd>  
*gims.xsd*: <https://wiki.l7tech.com/mediawiki/images/8/87/Gims.xsd>.

Table 109: Attributes for returned authentication information

| Attribute | Type   | Required | Comment   |
|-----------|--------|----------|---|
| <b>dn</b> | string | yes      | Distinguished name of the authenticated user. For some providers, this is the same as <b>login</b> ; for others such as LDAP, it is a string containing a path to a specific folder where the |

| Attribute             | Type   | Required | Comment  |
|-----------------------|--------|----------|--|
|                       |        |          | resource is located.   |
| <b>login</b>          | string | no       | Login name of the authenticated user   |
| <b>givenName</b>      | string | no       | First name of the authenticated user   |
| <b>sn</b>             | string | no       | Last name of the authenticated user  |
| <b>mail</b>           | string | no       | Email address of the user  |
| <b>accountExpires</b> | string | no       | Date and time when account expires, in GMT .<br>When it is set to "1969-12-31T23:59:59.999Z", the account never expires. |

## Error Conditions

The following table summarizes the errors returned by the Gateway when using the Generic Identity Management Service:

Table 110: Error cases for GIMS

| Condition  | Error  |
|--|--|
| <b>Non-secure protocol is used</b>               | When HTTP protocol is used, the Gateway returns HTTP code 500: "HTTP protocol is not supported. Use HTTPS instead" |
| <b>Incorrect user credentials entered</b>        | The Gateway returns HTTP code: 401 "Authentication Required"   |
| <b>Required parameters are missing</b>           | The Gateway returns HTTP code 401: "Authentication Required"   |
| <b>Token parameter is present in the request</b> | The Gateway returns HTTP code 401: "Authentication Required"   |
| <b>Incorrect provider name is present</b>        | The Gateway returns HTTP code 401: "Authentication Required"   |
| <b>Policy Error</b>                              | The Gateway returns HTTP code 500: "Internal Server Error"   |

## Sample Messages

The Policy Manager uses the web service's WSDL document to generate a sample message for each operation of the service. However, these sample messages are limited to elements declared in the WSDL and will not contain security-related headers. To allow the point-and-click selection of nodes in documents that cannot be generated automatically, you can configure your own sample messages.

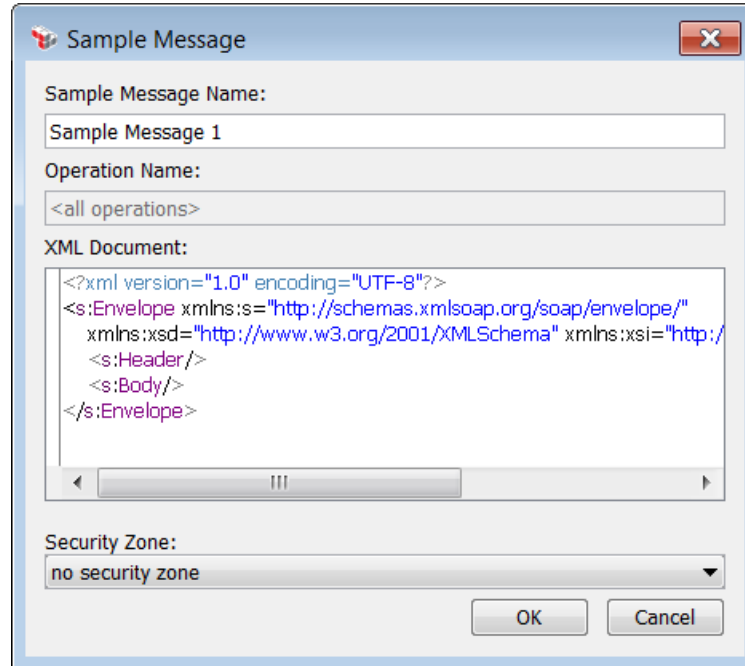
You can configure sample messages in the following assertions:

- Encrypt Element
- Evaluate Request XPath
- Evaluate Response XPath
- Sign Element
- (Non-SOAP) Decrypt XML Element
- (Non-SOAP) Encrypt XML Element
- (Non-SOAP) Sign XML Element
- (Non-SOAP) Verify XML Element

### Adding a Sample Message

➤ *To create a sample message:*

1. Open the properties for any of the assertions listed in "Sample Messages" on page 386.
2. In the **Sample Messages** section of the dialog, click **[Add]**. The Sample Message dialog appears.



The dialog box is titled "Sample Message" and contains the following fields:

- Sample Message Name:** A text box containing "Sample Message 1".
- Operation Name:** A dropdown menu showing "<all operations>".
- XML Document:** A text area containing the following XML code:
 

```
<?xml version="1.0" encoding="UTF-8"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://
  <s:Header />
  <s:Body />
</s:Envelope>
```
- Security Zone:** A dropdown menu showing "no security zone".

At the bottom right are "OK" and "Cancel" buttons.

Figure 147: Sample Message dialog

3. Configure the dialog as follows:

Table 111: Configuring a sample message

| Field                      | Description   |
|----------------------------|---|
| <b>Sample Message Name</b> | Enter a descriptive name for the message. For example, "getQuote with UsernameToken".   |
| <b>Operation Name</b>      | <p>Displays any Web Service Operation that was selected prior to opening the Sample Message dialog. If none selected, this field is blank.</p> <p>The Operation Name is only used to organize sample messages. It has no effect on message processing in the Gateway.</p>   |
| <b>XML Document</b>        | Displays an automatically generated message. Edit the XML code if necessary. You can right-click within the box to access the XML Editor features.  |
| <b>Security Zone</b>       | <p>Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose <b>"No security zone"</b>.</p> <p>For more information about security zones, see <a href="#">Understanding Security Zones</a> in the <i>Layer 7 Policy Manager User Manual</i>.</p> <p><b>Note:</b> This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the</p> |

| Field | Description   |
|-------|---|
|       | <p>zones).</p> <p><b>Tip:</b> The default security zone of a sample message will differ as follows:</p> <ul style="list-style-type: none"> <li>If you also have the "Manage Service &lt;name&gt;" role, you are able to set the security zone of the sample to any zone to which you have Read permission. In this case the first eligible zone (most like the "no security zone" option) is used as the default.</li> <li>If you do not also have the "Manage Service &lt;name&gt;" role, then the zone defaults to your "Manage Zone &lt;name&gt;" zone.</li> </ul> |

- Click **[OK]** when done. The new sample message is available from the **Sample Messages** drop-down list on the dialog.

## Editing a Sample Message

➤ To edit a [sample message](#):

- Open the properties for any of the assertions listed in "Sample Messages" on page 386.
- From the **Sample Messages** drop-down list, select the message to edit.

---

**Note:** You cannot modify the automatically generated message.

---

- Click **[Modify]**. The Sample Message dialog appears.
- Edit the message as required. See "Adding a Sample Message" on page 386 for more details.
- Click **[OK]** to close the dialog.

## Deleting a Sample Message

➤ To delete a [sample message](#):

- Open the properties for any of the assertions listed in [Sample Messages](#).
- From the **Sample Messages** drop-down list, select the message to delete.

**Note:** You cannot delete the automatically generated message.

- Click **[Remove]**. You are prompted for confirmation.
- Click **[OK]** to confirm. The message is deleted.

## Working with FTP Requests

The Gateway can be configured as an FTP(S) server. This allows it to communicate with legacy applications where EDI-like bulk XML data transactions are required.

---

**Note:** To enable the FTP feature, please contact CA Technologies for licensing information.

---

When configured as an FTP server, the Gateway will support the following:

- FTP requests into the Gateway, FTP out from the Gateway to a backend FTP server ("FTP in/FTP out")
- FTP requests into the Gateway, HTTP out from the Gateway to a backend SOAP web service or XML application ("FTP in/HTTP(S) out")
- FTP requests into the Gateway, JMS Routing from the Gateway via a JMS queue ("FTP in/JMS out")
- HTTP(S) requests into the Gateway, FTP out from the Gateway to a backend FTP server ("HTTP(S) in/FTP out")
- JMS requests into the Gateway, FTP out from the Gateway to a backend FTP server ("JMS in/FTP out")

For each of the above, requests can be anonymous, authenticated, or authenticated over SSL (see "[Configuring a Policy for FTP](#)" below for details).

### *Prerequisites:*

- The "SOA Gateway" version of the Gateway is used (FTP endpoints not supported in the other Gateway versions).
- The Gateway is deployed with a load balancer that supports session affinity for FTP (S) data transfers. For more information, see *Configuring the Load Balancer* in the *Layer 7 Installation and Maintenance Manual*.
- A SOAP web service or an XML application has been published. For more information, see "Working with SOAP Web Services" on page 331 and "Publishing a Non-SOAP Application" on page 346.

---

**IMPORTANT:** The remote path in the FTP client must be set to the service's resolution path. If a web service is published without a resolution path, the FTP client should use `/ssg/soap` as the remote path. For more information, see "About the Resolution Path" on page 367 under [Service Properties](#).

---

The Gateway supports the following protocols when configured as an FTP(S) server:

- RFC 959 - File Transfer Protocol
- RFC 2389 - Feature Negotiation Mechanism for the File Transfer Protocol
- RFC 2640 - Internationalization of the File Transfer Protocol
- RFC 3659 - Extensions to FTP

## Setting Up the FTP Server

You should have the following information before setting up an FTP server:

- IP address for the FTP service to monitor
- Port number to listen on for control connections
- Starting port number to listen on for passive data connections
- Number of ports for use with passive connections

➤ *To set up an FTP server on the Gateway:*

- Run the **Manage Listen Ports** task and configure a listener using the FTP protocol. For more information, see "Managing Listen Ports" on page 54.

## Configuring a Policy for FTP

Once the FTP server has been set up, configuring a policy to accept FTP requests is similar to one that uses conventional HTTP requests. (See Configuring a Policy for general policy configuration information.)

There are two assertions specifically designed for FTP:

- **Require FTP Credentials:** Used to authenticate FTP requests. The user name and password are retrieved from the FTP session for later authentication and authorization using the Authenticate User or Group assertion. Not used for anonymous FTP requests. This is the FTP equivalent of the Require HTTP Basic Credentials assertion.
- **Route via FTP(S):** Used to route requests to a backend FTP server, using passive mode FTP. This is the FTP equivalent to the Route via HTTP(S) assertion.

Other assertions not specific to FTP that are also useful in a policy involving FTP include:

- **Require SSL or TLS Transport:** Used to enforce FTP requests over a secure connection. If this assertion is used, ensure that the **Require Client Certificate Authentication** check box is not selected.
- **Authenticate User or Group:** Used to authorize users or groups when FTP requests are authenticated.



- **Require HTTP Basic Credentials:** Used to authenticate HTTP requests for the “HTTP (S) in/FTP out” scenarios.
- **Route via HTTP(S):** Used to route requests to an HTTP endpoint for the “FTP in/HTTP(S) out” scenarios.
- **Route via JMS:** Used to route requests to a JMS endpoint for the “FTP in/JMS out” scenario.

---

**Note:** FTP authentication is deferred since the identity provider to be verified against is unknown until a policy is resolved. This means that any login/password is accepted initially, but access will be denied if the credentials do not match the policy.

---

## Context Variables Used

The FTP service references the following context variables:

*request.tcp.remoteAddress*  
*request.tcp.remoteHost*  
*request.ftp.path*  
*request.ftp.file*  
*request.ftp.unique*  
*request.ftp.secure*

For more information about these and the other context variables available in the system, see "Appendix C: Context Variables" on page 517.

## Limitations and Considerations

Note the following when using the Gateway as an FTP server:

- Only streaming and implicit FTP(S) and passive FTP are supported
- Multipart/MIME files are not supported
- The FTP(S) server will validate using the existing SSL keystore; client certificates not used
- Response messages will not be returned to the FTP client, but they will be audited; to view them, use the Gateway Audit Events windows
- For every FTP request, the Content-Type is assumed to be “text/xml”, while the SOAPAction header is assumed to be empty (this information is not extracted from the HTTP transport)
- When connected to the backend FTP server, you can use the “cd” command to change directories to upload a file. However, it is not possible to “list” these virtual directories.

## Configuring a Reverse Web Proxy

You can configure the Gateway to behave as a reverse-web proxy, allowing you to manipulate the request and/or response headers, cookies, and content:

- To proxy only a single web application at a time, use the Publish Reverse Web Proxy Wizard to generate the appropriate service policy. For details, see ["Using the Publish Reverse Web Proxy Wizard"](#) below.
- To proxy multiple web applications, do the following:
  - a. Run the Publish Reverse Web Proxy Wizard once for each web application to be proxied. This will create one service per web proxy.
  - b. Configure a global policy or configure multiple listen ports. For details, see ["Using a Global Policy to Proxy Multiple Web Applications"](#) or ["Using Multiple Listen Ports to Proxy Multiple Web Applications"](#) below.

---

**Tip:** If you intend to analyze the web app response, ensure that the Content-Type of the response is defined in the [contentType.otherTextualTypes](#) cluster property.

---

### Using the Publish Reverse Web Proxy Wizard

Running the Publish Reverse Web Proxy Wizard does the following:

1. Adds the reverse proxy web service to the [Services and Policies](#) list on the Policy Manager interface.
2. Opens the policy for editing in the policy development window.

As with all Gateway-published services, you can publish multiple instances of the reverse proxy service—simply ensure that each contains a [unique resolution URI](#).

---

**Note:** Ensure that you have the correct security permissions to publish or modify a reverse proxy service. Once a service is published, the *Manage [serviceName] Service* role can be used to give users Administrator-like powers for that specific service only. For more information, see "Predefined Roles and Permissions" on page 132.

---

Choose a task to perform:

Table 112: Reverse proxy service tasks

| For information on how to...               | See  |
|--|--|
| <b>Publish a reverse proxy web service</b> | "Publish Reverse Web Proxy Wizard" on page 395 |

| For information on how to...                           | See  |
|--|--|
| Delete a reverse proxy web service                     | "Deleting a Published Service" on page 369 |
| Change the routing URI for a reverse proxy web service | "Service Properties" on page 357           |

## Using a Global Policy to Proxy Multiple Web Applications

One way to proxy multiple web applications is to use a global policy after creating a web proxy service with the Publish Reverse Web Proxy Wizard. This global policy will resolve a proxy service based on the host URL of the request, which is accessed through the `${request.url.host}` context variable. For example:

If `request.url.host = WebAppProxy1` then resolve to service `WebAppProxyService1`,  
otherwise if `request.url.host = WebAppProxy2` then resolve to service  
`WebAppProxyService2`.

The following is a sample global policy for multiple reverse web proxy service resolution. For more information about global policies, see Working with Global Policy Fragments in the *Layer 7 Policy Authoring User Manual*.

```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy xmlns:L7p="http://www.layer7tech.com/ws/policy"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
  <wsp:All wsp:Usage="Required">
    <wsp:OneOrMore wsp:Usage="Required">
      <wsp:All wsp:Usage="Required">
        <L7p:ComparisonAssertion>
          <L7p:CaseSensitive booleanValue="false"/>
          <L7p:Expression1 stringValue="${request.url.host}"/>
          <L7p:Expression2 stringValue="sharepointProxy2010"/>
          <L7p:Predicates predicates="included">
            <L7p:item binary="included">
              <L7p:CaseSensitive booleanValue="false"/>
              <L7p:RightValue stringValue="sharepointProxy2010"/>
            </L7p:item>
          </L7p:Predicates>
        </L7p:ComparisonAssertion>
        <L7p:ResolveService>
          <L7p:Uri stringValue="/2010"/>
        </L7p:ResolveService>
      </wsp:All>
    </wsp:OneOrMore>
  </wsp:All>
  <wsp:All wsp:Usage="Required">
    <L7p:ComparisonAssertion>
      <L7p:CaseSensitive booleanValue="false"/>
      <L7p:Expression1 stringValue="${request.url.host}"/>
      <L7p:Expression2 stringValue="sharepointProxy2013"/>
      <L7p:Predicates predicates="included">
        <L7p:item binary="included">
          <L7p:CaseSensitive booleanValue="false"/>
          <L7p:RightValue stringValue="sharepointProxy2013"/>
        </L7p:item>
      </L7p:Predicates>
    </L7p:ComparisonAssertion>
    <L7p:ResolveService>
```

```
<L7p:Uri stringValue="/2013"/>
</L7p:ResolveService>
</wsp:All>
<L7p:TrueAssertion/>
</wsp:OneOrMore>
</wsp:All>
</wsp:Policy>
```

## Using Multiple Listen Ports to Proxy Multiple Web Applications

Another method to proxy multiple web applications is to configure multiple listen ports after creating a web proxy service with the Publish Reverse Web Proxy Wizard. Each listen port will resolve to specific proxy services. For example, all HTTP requests on port 8888 resolve to *WebappProxyService1*, while all HTTP requests on port 9999 resolve to *WebappProxyService2*.

➤ To configure multiple listen ports:

1. Configure a listen port for the first port; see Figure 148 and Figure 149 below:

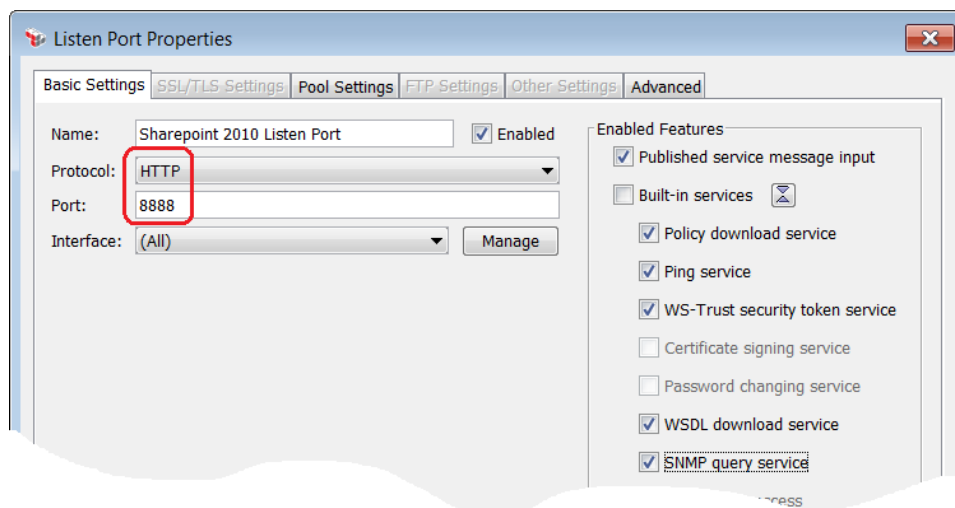


Figure 148: Configuring a listen port to proxy multiple web applications - [Basic Settings] tab

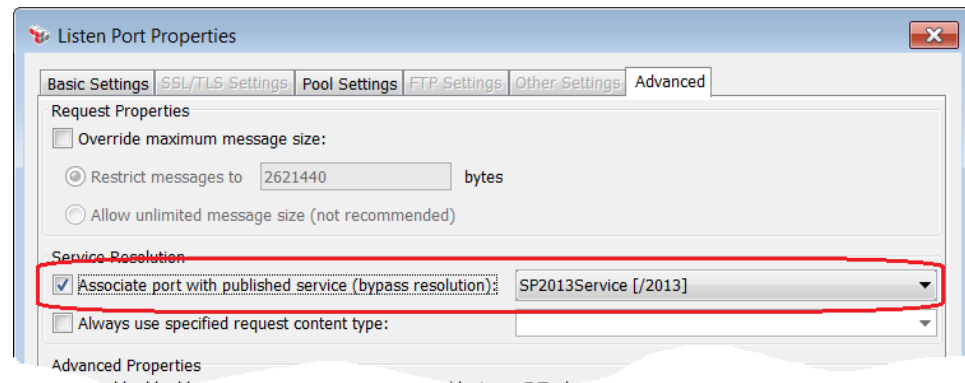


Figure 149: Configuring a listen port to proxy multiple web applications - [Advanced] tab

2. Configure a listen port for the second port in a similar fashion.

For information on configuring listen ports, see "Managing Listen Ports" on page 54.

## Publish Reverse Web Proxy Wizard

The *Publish Reverse Web Proxy Wizard* is used to publish a policy that enables the Gateway to behave as a reverse web proxy, allowing you to manipulate the request and/or response headers, cookies, and content. **Tip:** It is possible to manually create a reverse web proxy policy without this wizard, however it will require significantly more effort.

This wizard can create a generic reverse-proxy policy, or one specifically for SharePoint 2013.

This wizard requires a [role](#) that has permissions to create services and policies, as well as access to all assertions in the generated policy.

---

**Notes:** (1) The Publish Reverse Web Proxy Wizard is not designed to proxy multiple web applications at once, but you can do so by executing the wizard multiple times. For more information, see "Configuring a Reverse Web Proxy" on page 392. (2) The SharePoint 2013 examples shown in this topic are based on a simple configuration of SharePoint that uses default settings. These examples may not apply if your configuration is more advanced.

---

For more information about wizards, see "[Wizard](#)" under "Interfaces" on page 13.

➤ To access the *Publish Reverse Web Proxy Wizard*, do either of the following:

- Click **Publish Reverse Web Proxy** on the [Home Page](#)
- Select **[Tasks] > Publish Reverse Web Proxy** from the [Main Menu](#).
- Right-click a folder within the [Services and Policies](#) list and then select **Publish Reverse Web Proxy**.

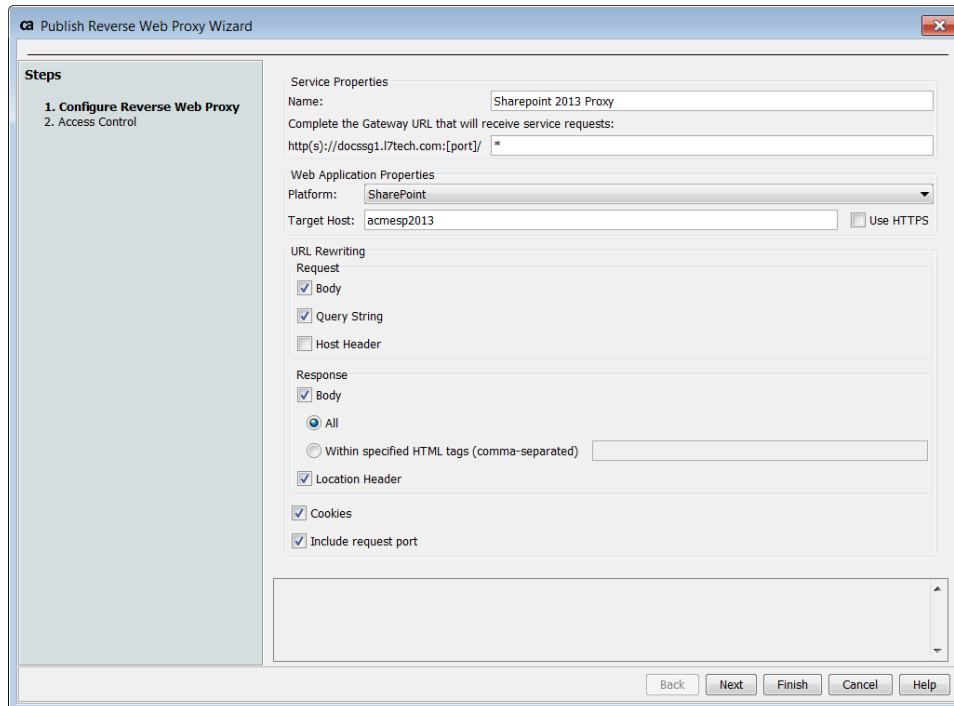
Complete the wizard as described below. Once the wizard is complete, a new service is published containing a policy for the Gateway to behave as a reverse web proxy.

## Recommended Wizard Configurations

The following settings are recommended if SharePoint is the web app being proxied:

- If the SharePoint server is unaware of the Gateway proxy, it is recommended that you accept all the default values in the wizard (with the exception of Name and Target Host, which must be completed).
- If the SharePoint server expects all traffic on port 80 and all Gateway traffic on port 80 has been configured to redirect to the default HTTP port (via "Managing Listen Ports" on page 54, [Manage Firewall Rules]), it is recommended that you deselect the **Include request port** check box.
- If the SharePoint server is configured with an alternate access mapping for the proxy, it is recommended that you do not configure any URL rewriting *except* for the Host header.
- When proxying for SharePoint, you need to add the following [advanced property](#) to the HTTP [listen port](#):  
**trimContentType=false**
- When proxying for SharePoint, it is recommended that you set the [mtom.decodeSecuredMessages](#) cluster property to 'false'.

## Step 1: Configure Reverse Web Proxy



**Publish Reverse Web Proxy Wizard**

**Steps**

1. Configure Reverse Web Proxy
2. Access Control

**Service Properties**

Name:

Complete the Gateway URL that will receive service requests:  
 http(s)://docssg1.i7tech.com:[port]/

**Web Application Properties**

Platform:

Target Host:  ☐ Use HTTPS

**URL Rewriting**

**Request**

☒ Body

☒ Query String

☐ Host Header

**Response**

☒ Body

☒ All

☐ Within specified HTML tags (comma-separated)

☒ Location Header

☒ Cookies

☒ Include request port

Back Next Finish Cancel Help

Figure 150: Publish Reverse Web Proxy Wizard - Step 1

The Configure Reverse Web Proxy step collects information required to build the correct service policy.

1. Enter the **Name** of the published service that will be created. This name will be displayed in the [services and policies list](#).
2. Enter the resolution URI for the service. This is the endpoint that will receive the service requests. The default is **\***.
3. Specify the Web Application Properties:
  - Choose the type of web app from the **Platform** drop-down list: **SharePoint** or **Generic**. This determines whether a web app-specific policy is created.

---

**Notes :** (1) Only SharePoint 2013 is currently supported. (2) The 'Generic' option will produce a generic proxy policy that will likely need to be modified for your web application before it can be used.

---

- Enter the **Target Host**. This is the host for which the Gateway will be serving as a reverse proxy. Include the port number if applicable.

- Select **Use HTTPS** to use a secure connection when routing to the web application.

The remaining settings in this wizard step are used to configure URL Rewriting.

4. Configure whether URL Rewriting should be performed on the **Request**. **Tip:** To reverse any of the settings below after the policy has been created, simply disable or enable the associated assertion.
  - Select the **Body** check box to replace all occurrences of the Gateway host in the request body with the web application host, using the Evaluate Regular Expression Assertion in the generated service policy.  
Clear this check box to disable the above assertion in the generated service policy and not rewrite the request body. **Tip:** To enable request rewriting, simply re-enable this assertion.
  - Select the **Query String** check box to rewrite the request query string to reference the web application host instead of the request host, using the Evaluate Regular Expression Assertion in the generated service policy.  
Clear this check box to disable the above assertion in the generated service policy and not rewrite the query string.
  - Select the **Host Header** check box to rewrite the request Host header to reference request host, using the Manage Transport Properties/Headers Assertion.  
Clear this check box to disable the above assertion in the generated service policy and not rewrite the Host Header.
5. Configure whether URL Rewriting should be performed on the **Response**:
  - Select the **Body** check box to enable URL rewriting on the Response body, using the Evaluate Regular Expression Assertion in the generated service policy. Clear the check box to disable the assertion and not permit rewriting.
    - If rewriting is permitted, indicate whether to replace **All** occurrences of the web application host in the response body with the Gateway host, or whether to replace only **Within specified HTML tags** in the adjacent box.
  - Select the **Location Header** check box to rewrite the response location headers (in other words, enable assertions that will replace specific instances of the web application host in the location header with the Gateway host).  
Clear this check box to disable the location-rewriting assertions in the resulting service policy.
6. Select the **Cookie** check box to rewrite the request Cookie and response Set-Cookie headers (in other words, reconfigure the domain and path—and name if



SharePoint is selected—of the cookies).

Clear this check box to disable the cookie-rewriting assertions in the resulting service policy.

7. Select the **Include request port** check box to include the request port during URL rewriting.

Clear this check box to exclude the request port during URL rewriting. **Tip:** Clear this check box if the web application expects all HTTP traffic on port 80 and there is an alternate access mapping for the proxy

## Step 2: Access Control

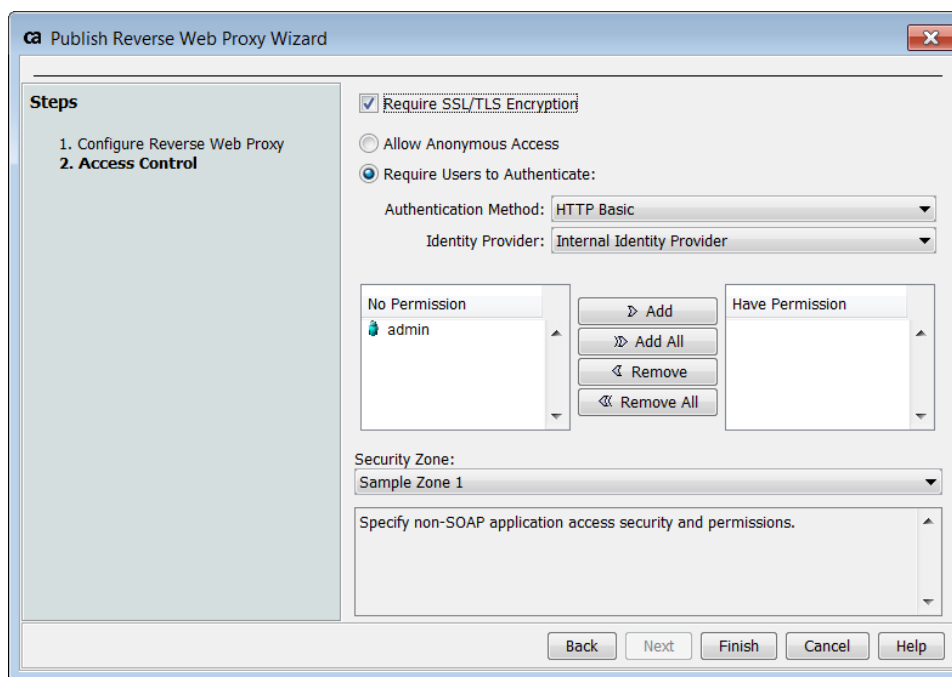


Figure 151: Publish Reverse Web Proxy Wizard - Step 2

The Access Control step allows you to define access control and authentication rules for non-SOAP applications.

1. Optionally select the **Require SSL/TLS Encryption** check box to require that all requestors consume the reverse web proxy service through the SSL entry point.
2. Choose an access control option:
  - **Allow Anonymous Access:** Permit requestors to access the service anonymously (without credentials).

- **Require Users to Authenticate:** Require that requestors provide credentials to gain web service access. Define the authentication details for this option as follows:
  - **Authentication Method:** Choose an authentication method from the drop-down list. This determines what information users and groups are required to provide to gain application access.
  - **Identity Provider:** Choose an [identity provider](#) from the drop-down list that contains the authorized users and groups.

---

**Note:** When requiring users to authenticate, the access will be restricted to the identity providers indicated above. The policy will initially be populated with an authentication assertion for each Authenticate User or Group assertion corresponding to each selected identity.

---

3. Specify which users and groups are authorized to use the reverse proxy web service by moving them between the **No Permission** and **Have Permission** lists.
  - Grant permission by selecting entries from **No Permission** and then clicking **[Add]**. Alternatively, click **[Add All]** without selecting any entry to authorize everyone on the list.
  - Deny permission by selecting entries from **Have Permission** and then clicking **[Remove]**. Alternatively, click **[Remove All]** without selecting any entry to deny permission to everyone on the list

**Tip:** You can select a continuous block of rows by dragging the mouse over the rows you want; or, select the first row, hold down the [Shift] key, then select the last row. You can select individual rows by holding down the [Ctrl] key while clicking on the rows you want.
4. If you need to authorize users or groups from another identity provider, select the new provider name from the **Identity Provider** drop-down list and then repeat step 3.
5. Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "**No security zone**". For more information about security zones, see [Understanding Security Zones](#) in the *Layer 7 Policy Manager User Manual*. **Note:** This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).

## Chapter 6: Analyzing Gateway Performance

The Policy Manager provides the following features to monitor performance across one or more Gateways:

- **Dashboard window**

This window displays [service metrics](#) and [cluster statistics](#) in real time. This is useful for quickly identifying and correcting policy violations or routing failures. This window is described below.

- **Gateway Audit Events window**

This window displays system events (for example, a server startup), administrative events (such as login or editing a services policy), and service-specific message processing events. This window is described under "Gateway Audit Events" on page 415.

These windows allow you to monitor the following metrics:

- Gateway cluster node statistics
- Service message statistics
- Service policy changes
- Gateway connectivity and communication policies
- General transaction traffic
- Service-specific message processing event policies
- Administrative event-specific auditing policies

## Dashboard - Service Metrics

The Service Metrics window in the Dashboard allows you to continuously monitor performance statistics of a Gateway cluster. Message processing rates and response times are displayed in real time, in a dynamic chart that can be filtered by cluster node, published service, or resolution. Policy violations and routing failures are highlighted for greater visibility.

You can print the Service Metrics window by selecting **File > Print**.

**Notes:** (1) The Policy Manager [connection timeout](#) is disabled when the Dashboard is open, to allow for uninterrupted viewing of metrics. If nothing is displayed in the Dashboard, check whether service metrics have been disabled on the Gateway (see the setting [serviceMetrics.enabled](#) in [Gateway Cluster Properties](#)). (2) Collection of service metrics is disabled if an embedded database is in use on the Gateway. For more information, see "Using the Embedded Database" in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

➤ To open the Service Metrics window:

- From the Policy Manager [Main Menu](#), click **[View] > Dashboard** (on the [browser client](#), from the **Monitor** menu). The Service Metrics window is displayed.

The Service Metrics window displays traffic flow based on the default settings of All Nodes, All Services, and Fine resolution.

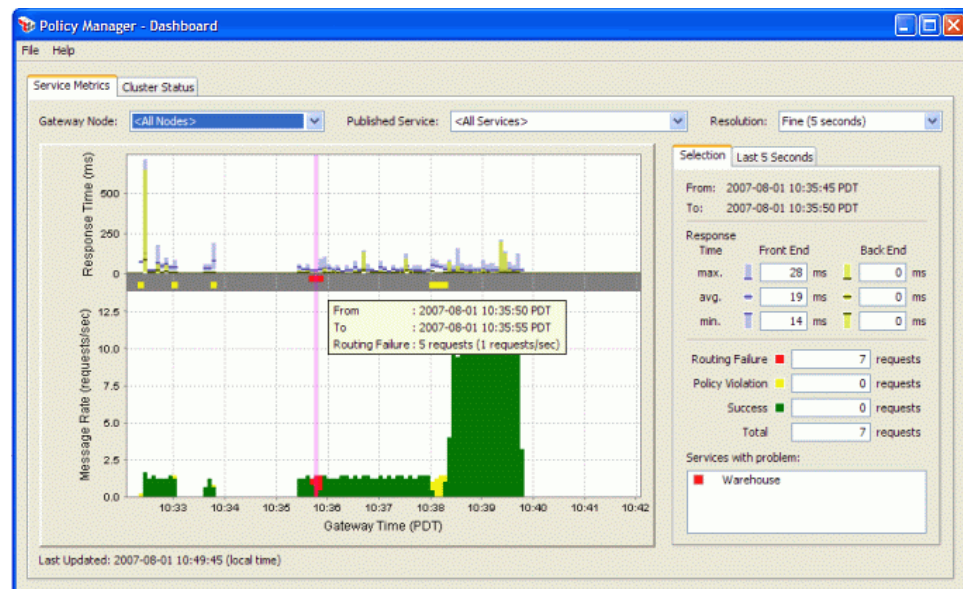


Figure 152: Dashboard - Service Metrics

The Service Metrics window is divided into the following sections:

- The filters across the top let you select the node, service, and resolution for the graph
- A moving chart containing three plots: response times (top), notification indicators (middle strip), and message rates (bottom)
- A summary at the right, containing tabs for the selected interval or latest interval

The following mouse actions are available to interact with the display:

Table 113: Dashboard - Service Metrics mouse actions

| Mouse action   | Description   |
|--|---|
| <b>Left click anywhere in moving chart</b>           | Selects a time interval. Statistics about that interval are displayed in the [Selected] tab in the <a href="#">Interval Summary</a> section.  |
| <b>Right click anywhere in moving chart</b>          | Lets you view the audit events that have occurred during the time interval. Select <b>Show Audit Events (&lt;time&gt;)</b> from the menu that pops up. The events are displayed in a <a href="#">Gateway Audit Events</a> window. |
| <b>Point at any bar</b>                              | Positioning the mouse pointer over any coloured bar displays a tooltip containing more information about what is happening.   |
| <b>Drag mouse pointer left to right over any bar</b> | Zooms in for a closer look within a time period (see " <a href="#">Zooming Time Intervals</a> " below).   |
| <b>Drag mouse point right to left</b>                | Zooms out (see " <a href="#">Zooming Time Intervals</a> " below).   |

## Filters

Select the information you wish to view from the drop-down lists:

- **Gateway Node:** Select the gateway node to monitor or use the default "<All Nodes>" to view data combined from all nodes.
- **Published Service:** Select the service to monitor or use the default "<All Services>" to view data combined from all services.

---

**Tip:** Clicking on a service name in the "Services with problems" box will highlight an interval and bring the "Selection" tab to the front with statistics of that interval. If there are routing failures or policy violations in that interval, services with those problems will be listed in the "Services with problem" list box. Clicking on a service name in that list box will select a single service, as if a service name was selected from the Published Service list.

---

---

**Note:** "<All Services>" is defined as all services in which the user has 'Read' permission. For more information, see "Predefined Roles and Permissions" on page 132.

---

- **Resolution:** Select a resolution for the graph: **Fine** (5 sec), **Hourly**, or **Daily**.

## Response Times

The **Response Time** plot at the top of the chart shows the front end and back end response times, with minimum, maximum, and average values for each time increment. The graph is updated based on the selected **Resolution**: **Fine** = every 5 seconds; **Hourly** = every clock hour, **Daily** = every calendar day. The response times are expressed in milliseconds and the corresponding numeric values are shown in the details section.

---

**Tip:** The Fine interval can be changed using the [metrics.fineInterval](#) cluster property. Restart the gateway cluster for this property change to take effect.

---

The **Front End** response time is the time it takes for Gateway to receive a request from a client, then send a response back to the client. The **Back End** response time is the time it takes for Gateway to forward the request to the web service, then receive a response from the web service. Thus, the front end time always includes the back end time.

---

**Note:** The Back End response time includes all routings, if there are multiple routing assertions in the policy.

---

To see the data collected for a particular time interval, point to the corresponding bar and the information will be displayed in a tooltip.

## Notification Bar

The notification bar is the horizontal strip in the middle of the moving chart. Its purpose is to alert you to potential problems: a red square indicates a time interval where routing failures occurred, while a yellow square indicates policy violations have occurred. The services with the problems are listed in the [Interval Summary](#) area.

## Message Rates

The **Message Rate** plot at the bottom of the chart shows the message rate, broken down by routing failure, policy violation, and successful requests. The coloured bars show at a glance where problems may be occurring. The corresponding numeric values for message rates are shown in the details section. Note that the time axis displays the Gateway time, which may not be in the same time zone as the machine running the Policy Manager.

To see the data collected for a particular time interval, point to the corresponding bar and the information will be displayed in a tooltip. You can also right-click any time period and select **Show Audit Events**. This displays a static [Gateway Audit Events](#) window containing only the audit messages for the selected time interval. This can help you isolate and troubleshoot any problems quickly. Repeat this procedure on any other time periods that you want to investigate—there is no need to close the Gateway Audit Events window first.

---

**Note:** If auditing has been disabled for the service or the entire cluster, the Gateway Audit Events window will show no records. For more information, see *Configuring the Gateway Logging Functionality* in the *Layer 7 Installation and Maintenance Manual*.

---

## Interval Summary

The panel to the right of the moving chart contains two tabs:

- The [Selection] tab displays information about the selected time interval on the Message Rate Chart. This tab expands on the information presented in the tooltip.
- The [Last <resolution>] tab displays information for the last resolution interval.

The following information is displayed in either tab:

- Interval period. This is fixed for the [Selected] tab, but updated dynamically when the [Last <resolution>] tab is selected. Note that the Gateway time zone is used; this may differ from the local time if the Policy Manager is run on a different machine.
- The minimum, maximum, and average response times for the indicated time period. These are categorized by front end and back end processing, broken down by minimum, maximum, and average values.
- The message processing statistics for the indicated time period, broken down by routing failures, policy violations, and successful requests.
- Any services with routing failures or policy violations (shows red or yellow in the [Notification Bar](#) and [Message Rates](#) chart) in the "Services with problems" box. When the [Selection] tab is currently selected, the problem applies to the bin currently selected. When the [Last...] tab is current selected, the problem applies to the latest bin. **Tips:** You can always click any bin to see the service names with problems again. You can click on a service name to [filter](#) the published services to only that service.

## Zooming Time Intervals

You can zoom both the Response Time or Message Rate plots for a closer look at the time intervals.

- To zoom in, press and hold the left mouse button while dragging the pointer from left to right across one or more bars, then release the mouse button. The plot re-scales to the width of the mouse drag. You can repeat the zoom multiple times.

For example, using the hourly resolution, each bar represents a one hour period and the labels are four hours apart. If you zoom into three bars, the resulting graph shows ten minute increments along the time line.

- To zoom out, press and hold the left mouse button and perform a short left drag motion anywhere within the chart, then release the mouse button; it is not necessary to drag over a bar. The plot re-scales back to its original resolution.

## Dashboard - Cluster Status

The Cluster Status window in the Dashboard displays the status of the Gateway cluster node(s) and provides service statistics. The information in this window is automatically updated every few seconds, with the last update time shown at the bottom left corner of the window.

---

**Note:** The Policy Manager [connection timeout](#) is disabled when the Dashboard is open, to allow for uninterrupted viewing of cluster status. For more information about the connection timeout, see "Configuring Preferences" on page 210.

---

The Cluster Status window contains two tables:

- The **Gateway Status** table at the top displays node information and CPU and server statistics by gateway node.
- The **Service Statistics** table at the bottom displays service activity statistics.

In either table, you can click a column heading to sort the rows in ascending or descending order based on that heading. You can print the Cluster Status window by selecting **File > Print**.

➤ *To open the Cluster Status window:*

1. From the Policy Manager [Main Menu](#), click **[View] > Dashboard** (on the [browser client](#), from the **Monitor** menu).
2. Click the **[Cluster Status]** tab.



The Cluster Status window appears.

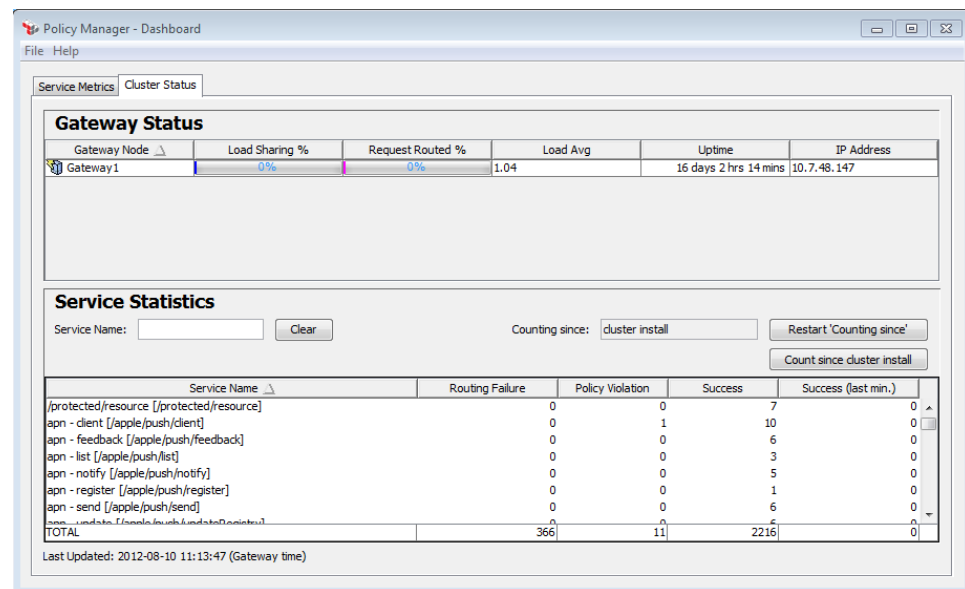





Figure 153: Dashboard - Cluster Status

## Gateway Status Table

The Gateway Status table displays information about each gateway node. You can also rename or remove a node.


Table 114: Gateway Status table

| Column Name             | Description   |
|-------------------------|---|
| <b>Gateway Node</b>     | <p>Name of the cluster node assigned during configuration. Displays three status icons:</p> <ul style="list-style-type: none"> <li>: Node is active.</li> <li>: Node is inactive. When inactive nodes are detected, the tab name changes to <b>Cluster Status</b> to bring this to your attention.</li> <li>: Node status is undetermined. Policy Manager is in the process of assessing the status of the node and will change the icon to active or inactive once the status is determined.</li> </ul> |
| <b>Load Sharing %</b>   | <p>Indicates the percentage of total cluster traffic being handled by the node over the past 60 seconds, expressed both as a percentage and as a dynamic bar graph.</p> <p>A value of "0" indicates no activity.</p>  |
| <b>Request Routed %</b> | <p>Indicates the percentage of current routing activity being handled by the node over the past 60 seconds, expressed both as a percentage and as a dynamic bar graph.</p>  |

| Column Name       | Description  |
|-------------------|--|
|                   | A value of "0" indicates no activity.  |
| <b>Load Avg</b>   | The average number of work processes completed over the last 60-second period. For Gateway appliance installations, values reaching or exceeding 4.0 indicates that the Gateway is under heavy load and overall server performance will be slow. This does not apply to software installations of the Gateway. |
| <b>Uptime</b>     | Server start time to the current time. Use this information to analyze the number of requests processed by the node per time period.   |
| <b>IP Address</b> | The IP address for the direct Gateway to Gateway connection.   |

You can perform the following operations on a node:

Table 115: Node operations

| To...                                  | Do this...  |
|--|---|
| <b>Rename a node</b>                   | <ol style="list-style-type: none"> <li>Right-click anywhere within the node's row and then select <b>[Rename Node]</b>.</li> <li>Type a new node name (maximum 128 characters) and then click <b>[OK]</b>.</li> </ol> <p>The new node name is immediately reflected in the Gateway Node column and throughout the Policy Manager.</p> <p><b>Note:</b> Renaming a node only changes how the name is <i>displayed</i> in the Policy Manager. It does <u>not</u> affect the actual host name of the Gateway node.</p>  |
| <b>Delete a node</b>                   | <p>You can delete inactive nodes so that they no longer appear in the Gateway Cluster table. For information on making a node inactive, see <i>Deactivating a Cluster Node</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <p><i>To delete an inactive node:</i></p> <ol style="list-style-type: none"> <li>Right-click any anywhere within an inactive (  ) node row and then select <b>Delete Node</b>.</li> <li>Click <b>[Yes]</b> to confirm the deletion.</li> </ol> <p>The node is immediately removed from the Gateway Status window.</p> <p><b>Note:</b> Deleting a node removes it from the Gateway Cluster. If a deleted node is reactivated, you must stop and restart the applicable Gateway in order to see the node in the Cluster Status window.</p> |
| <b>View log information for a node</b> | <p>When you are setting up the Gateway, use the logs to help you diagnose issues for a Gateway node.</p> <p><i>To view log information for any gateway node:</i></p> <ul style="list-style-type: none"> <li>Select <b>Tasks &gt; View Logs</b> from the Policy Manager menu (in</li> </ul>  |

| To... | Do this...   |
|-------|--|
|       | <p>the <a href="#">browser client</a>, this is under <b>Monitor &gt; View Logs</b>)</p> <p>For more information, see "Viewing Logs" on page 409.</p> |

## Service Statistics Table

The Service Statistics table initially displays information for all services.

- To filter the list of services shown, enter a service name in the **Service Name** box. You may also enter a partial name, wildcards, or a regular expression to achieve broader matches.

By default, the statistics reflect what has occurred since the cluster started.

- To restart all counters, click [**Restart 'Counting since'**]. This resets all values to zero and begins counting from that moment on. This is useful to get a "snapshot" of the statistics, without losing the cluster cumulative totals.
- To see the statistics accumulated since the cluster was installed, click [**Count since cluster install**]. This is a cumulative total that is not affected by cluster starts and shutdowns.

The following table describes the columns in the Service Statistics table.

Table 116: Cluster Status Service Statistics

| Column Name                | Description  |
|----------------------------|--|
| <b>Service Name</b>        | Name of the service assigned during configuration.   |
| <b>Routing Failure</b>     | Number of requests that passed policy assertions but failed at the back end web service.     |
| <b>Policy Violation</b>    | Number of requests that failed policy assertions.  |
| <b>Success</b>             | Number of request messages that have been successfully routed (completed).                   |
| <b>Success (last min.)</b> | Number of request messages that have been successfully routed in the last minute of up time. |

## Viewing Logs

The Policy Manager has a built-in log viewer that you can use to view Gateway node logs from any cluster node, provided that the log files are associated with an existing [log sink](#). Use the logs to help you diagnose and resolve problems for a node.

---

**Tip:** Logs may also be viewed on the Gateway appliance, from the Gateway main menu. For more information, see *Viewing Logs on the Gateway Appliance* in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

---

➤ To view logs:

1. In the Policy Manager, select **[View] > View Logs** from the [Main Menu](#) (on the [browser client](#), from the **Monitor** menu). The available logs to view are listed. If the list of logs is long, you can filter the display by entering some text into the **Filter** box. The filter string is matched against all columns, except for "Last Modified". **Tip:** When a filter is in place, the following message is displayed to remind you that the list is filtered: "Caution! Filter may exclude some logs."

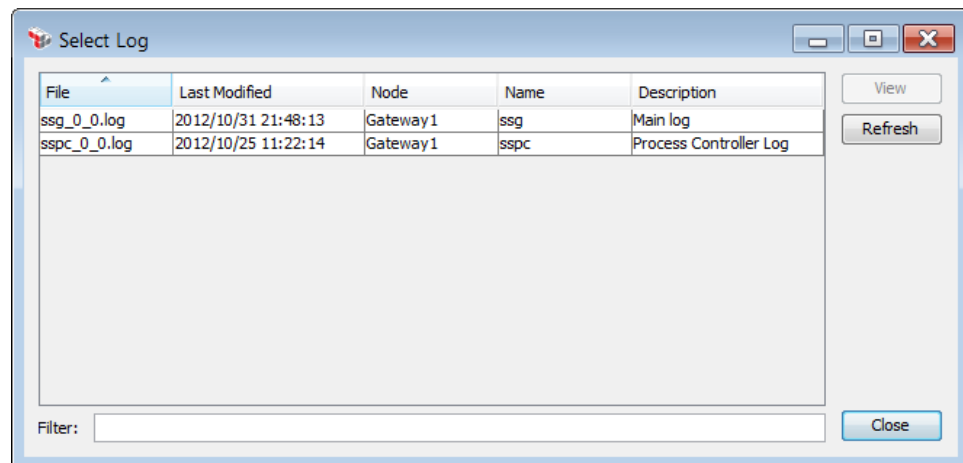


Figure 154: Select Log dialog

---

**Note:** Only local logs are listed in the Select Log dialog. Local logs are those of [type "File"](#) in the [Log Sink Properties](#).

---

2. Select one or more log file(s) to view, then click **[View]**. **Tip:** Hold down the **[Ctrl]** key to select multiple files.

The log details are displayed in the Log Viewer dialog.

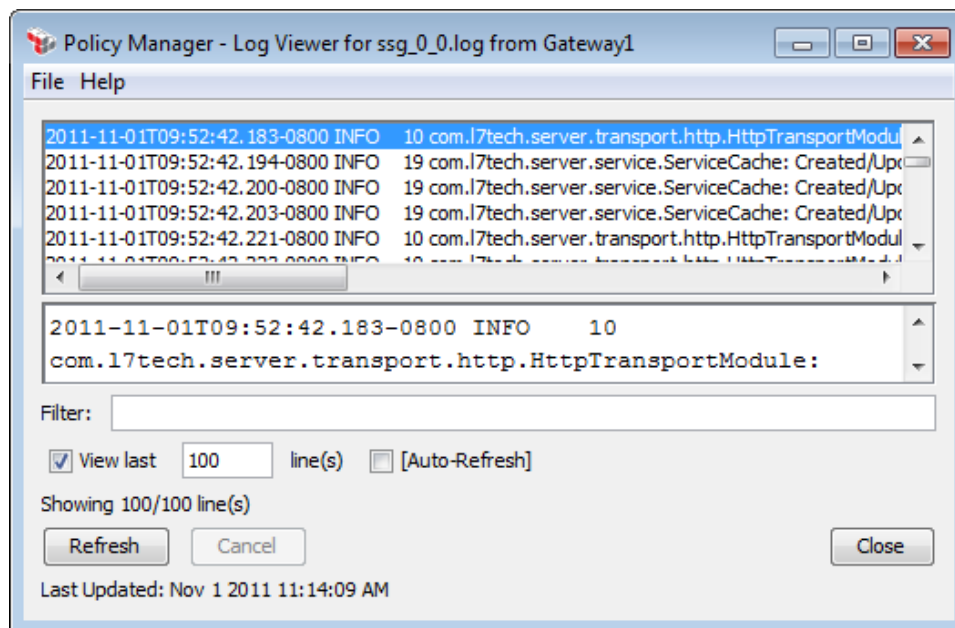


Figure 155: Log Viewer dialog

The following table describes each part of the Log Viewer dialog:

Table 117: Log Viewer settings

| Setting             | Description   |
|---------------------|---|
| <log entries>       | <p>The box at the top of the dialog displays all the entries in the selected log. You can click on any line to view it in the log entry details box below.</p> <p>If the Tail option is selected, the list of log entries is updated dynamically, displaying the X most recent log entries.</p> <p>If a <b>Filter</b> is in place, this box displays only those log entries with text matching the filter string.</p>   |
| <log entry details> | <p>When you select a log entry to view, the details are displayed in a more readable line-wrapped format in this details box.</p> <p><b>Tip:</b> You can copy any part of the log entry detail by selecting the desired text and then pressing <b>[Ctrl]-C</b>.</p>   |
| <b>Filter</b>       | <p>To filter the list of log entries, type a filter string. The display is automatically updated to show only those lines containing the string. For example, to see only log entries with the severity WARNING, type 'warning' in the box.</p> <p>A message is displayed when a filter is in effect, to remind you that not all entries are visible.</p> <p>To clear the filter, delete the string.</p> <p><b>Tip:</b> The filter string is matched anywhere within the log entry, with no case sensitivity.</p> |

| Setting                      | Description   |
|------------------------------|---|
| <b>View last xxx line(s)</b> | Select this check box to display only the most xxx recent log entries . New lines are displayed as they become available (if not filtered) . Enter how many recent entries to show , maximum 100.<br><br>Clear this check box to display the entire contents of the log. <b>Tip:</b> You will need to click <b>[Refresh]</b> to update the display after clearing this check box. |
| <b>Auto-Refresh</b>          | Select this check box to have new log data retrieved from the Gateway every few seconds. The log display will scroll automatically to display the latest lines in the log.<br><br>Clear this check box to update the log only when the <b>[Refresh]</b> button is clicked.  |
| <b>Showing xx/xx line(s)</b> | Displays the total number of events currently displayed in the log window , out of the total number of viewable entries. This is useful to see how many lines are displayed when a filter is used.  |
| <b>Refresh</b>               | Click this button to update the log data displayed.<br><br><b>Tip:</b> The <b>[Refresh]</b> button is not necessary when <b>Auto-Refresh</b> is enabled, but you can still use it to update the display in between auto refreshes.  |
| <b>Cancel</b>                | Click this button to cancel a manual refresh. For example, you may wish to cancel if a refresh is taking too long to complete.  |
| <b>Last Updated</b>          | Displays the date and time of the most recent update, whether auto or manual refresh.   |

3. Click **[Close]** to close the Log Viewer and the Select Log dialogs when done.

## Saving the Log

Before saving the log, be sure the entries you want to save are currently displayed. Data that is filtered out will not be saved. For example, if you were viewing 'Severe' events, only 'Severe' events will be saved. If you wish to save the entire log, be sure to clear the filter first.

➤ *To save the log:*

1. In the Log Viewer dialog, select **[File] > Save as**.
2. Specify a file name and location or use the defaults presented.

**Tip:** Accepting the suggested file name makes it easier to sort and organize your saved logs. Be sure to preserve the **".txt"** file extension.

3. Click **[Save]**.

➤ To view the saved log:

- Open the saved log file using any text editor.

## FTP Audit Archiver

The FTP Audit Archiver is used to back up the audit logs on the Gateway via FTP to a specified host. The backups are stored as plain text files compressed into .ZIP archives with a name in the following format:

<[audit.archiver.ftp.fileprefix](#)> cluster property + <date & time stamp>.zip

When the audit records are successfully backed up, the archiver automatically deletes the records to save disk space.

---

**Tip:** Ensure that the FTP server receiving the archive is fast enough to accept the largest audit entry within the MySQL timeout period.

---

Once the FTP Audit Archiver is configured, it will automatically run as follows:

- Each time the Gateway is started
- At a preset interval specified by the [audit.ArchiverTimerPeriod](#) cluster property

The archiver can also be manually invoked using the "Start Archiver" command in the "Gateway Audit Events" on page 415 window. If the archiver is configured but you do not want it to run, you can disable it using its properties dialog.

---

**Notes:** (1) In addition to the configuration described here, there are several cluster properties that can be used to further control the behavior of the archiver. For more information, see the "Audit Archiver Cluster Properties" on page 568. (2) The FTP Audit Archiver is not supported when an embedded database is in use on the Gateway. For more information, see "Using the Embedded Database" in the *Layer 7 Installation and Maintenance Manual (Appliance Edition)*.

---

➤ To configure the FTP Audit Archiver:

1. In the Policy Manager, select [Tasks] > **Configure FTP Audit Archiver** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The FTP(S) Audit Archiver Properties appear.

Figure 156: FTP(S) Audit Archiver Properties dialog

2. Configure the properties as follows:

Table 118: FTP(S) Audit Archiver settings

| Field                     | Description   |
|---------------------------|---|
| <b>Security</b>           | Specify which form of security to use: <ul style="list-style-type: none"> <li>• <b>FTP (unsecured):</b> Information is submitted unencrypted.</li> <li>• <b>FTPS with Explicit SSL:</b> Information is encrypted using explicit SSL (RFC2228).</li> <li>• <b>FTPS with Implicit SSL:</b> Information is encrypted using implicit SSL.</li> <li>• <b>Verify server certificate:</b> If encryption is used, select this check box to verify the server's certificate against the trust store in the Gateway. For more information, see "Chapter 3: Managing Certificates" on page 237.</li> </ul> |
| <b>Host name</b>          | Enter the hostname of the FTP server. This name is verified against the X.509 certificate.  |
| <b>Port number</b>        | Enter the port number to use. The default port number is 21.  |
| <b>Directory</b>          | Specify the name of the directory on the FTP server to place the audit archive.   |
| <b>User name/Password</b> | Enter the login credentials if connecting a secure server.  |
| <b>Timeout</b>            | Specify the number of seconds to wait during FTP connection before the archiver times out.  |
| <b>Enabled</b>            | The archiver is enabled by default. Clear the check box to disable the archiver. When disabled, the archiver will not run when the Gateway is   |



| Field                  | Description   |
|------------------------|---|
|                        | <p>started nor can it be manually run from the <a href="#">Gateway Audit Events</a> window. Scheduled archives will not occur as well.</p> <p><b>Tips:</b> (1) If an archive is in progress when the archiver is disabled, the change will not take effect until the transfer is finished. (2) To just cancel the automatically scheduled archives, set the cluster property <a href="#">audit.ArchiverTimerPeriod</a> to "0" (zero) instead.</p> |
| <b>Test Connection</b> | Click this button to test the settings. You should see a success message if the settings are correct.   |

- Click **[OK]** when done.

## Gateway Audit Events

In the Policy Manager, the Gateway Audit Events window displays detailed audit messages for services, administrative, and internal system messages from the Gateway cluster.

---

**Note:** System audit events (those generated by the Gateway itself) will always be available for viewing within the Gateway Audit Events window. Message auditing events (those triggered by the Audit Messages in Policy assertion) may or may not appear, depending on the level set within the Audit Messages in Policy assertion. For more information, see *Message Auditing* in the *Layer 7 Policy Authoring User Manual*.

---

If you need to view logged messages for an individual gateway node instead, please see "Viewing Logs" on page 409.

The Gateway can record audit events until the audit logs consume a predefined percentage of the hard disk space. Once this threshold is reached, all message processing ceases until the log size drops below the threshold. The threshold is defined in the [audit.archiverShutdownThreshold](#) cluster property; default: **90%**.

The Gateway Audit Events window provide the following panels to let you search for the following:

- The *Audit Record Search Parameters* panel lets you filter audit events based on a variety of audit parameters.
- The *Entity Search Parameters* panel lets you search the history of the selected entity.
- The *Associated Logs Search Parameters* lets you search based on the audit code.

These panels are collectively referred to as the "audit search panels".

Additionally, the Gateway Audit Events window lets you perform the following tasks:

- Download audit events to an external file
- Delete audit events more than 7 days old
- Start the audit archiver
- Save the audit events to review later.

**Note:** The system timeout is disabled when the Gateway Audit Events window is open. For more information about the timeout, see "Configuring Preferences" on page 210.

➤ To open the Gateway Audit Events window, do one of the following:

- From the [Main Menu](#), click [View] > **Gateway Audit Events** (on the [browser client](#), from the **Monitor** menu).

The Gateway Audit Events window opens. Audit events from the previous session are shown by default.

- In the [Service Metrics](#) window of the Dashboard, right-click anywhere in the moving chart and then select **Show Audit Events <time interval>**.

The Gateway Audit Events window opens loaded with the audit events from the time period selected.

Policy Manager - Gateway Audit Events

File View Help

Source: ☐ Internal database ☒ Via audit lookup policy [Configure Audit Lookup Policy](#)

Time Range: ☒ Last  hours  minutes ☒ Auto-Refresh ☐ From: Oct 16, 2012 4:43:01 PM To: Oct 16, 2012 4:43:01 PM  (GMT-08:00/-07:00)

Audit Record Search Parameters

Level:  Service:  Message:  Request ID:   
 Audit Type:  Node:  User Name:  User ID or User DN:

Entity Search Parameters

Entity Type:  Entity ID:  Associated Logs Search Parameter:  Message Operation Search Parameter:   
☐ Validate Signatures [Clear Search Criteria](#) [Cancel](#) [Search](#)

| Sig     | AuditRecord | Node                  | Time    | Severity | Service  | Message |
|---------|-------------|-----------------------|---------|----------|--|---------|
| 2130025 | Gatew...    | 20121016 16:43:01.293 | WARNING |          | Audit sink policy failed; status = 601   |         |
| 2130024 | Gatew...    | 20121016 16:43:01.269 | INFO    |          | View audit data - Start Time: Tue Oct 16 13:43:01 PDT 2012                       |         |
| 2130023 | Gatew...    | 20121016 16:42:58.908 | WARNING |          | Audit sink policy failed; status = 601   |         |
| 2130022 | Gatew...    | 20121016 16:42:58.881 | INFO    |          | ClusterProperty #2031616 (audit.acknowledge.highestTime) updated (changed value) |         |

Event Details Panel

Node : Gateway1  
 Time : 20121016 16:43:01.293  
 Severity : WARNING  
 Message : Audit sink policy failed; status = 601  
 Audit Record ID: 2130025

Total: 4  
 Last Updated: Oct 16 2012 05:28:35 PM [Auto-Refresh]

Figure 157: Gateway Audit Events window


## Showing/Hiding Panels

The following panels in the Gateway Audit Events window can be hidden when not required:

- Time Range panel plus all the audit search panels (all hidden/revealed at once)
- Event details panel

Hiding a panel is convenient when you do not need the controls in that section or if you want to increase screen space for the other panels.

➤ *To hide or show a panel, do any of the following:*

- Click the appropriate arrow  just above the pane. It is useful to remember that the Time Range Panel hides by collapsing *upward*, while the Details Panel hides by collapsing *downward*.
- Click **[View] > Controls** or **[View] > Event Details**.
- Use the keyboard shortcuts **[Alt + C]** (toggle Controls) or **[Alt + E]** (toggle Event Details)

## Source Panel

The Source panel is used to select the source of the audit records to display:

- **Internal database:** Select this to view audits sent to the internal Gateway database. You should select this option if you have not set up an external audit store.
- **Via audit lookup policy:** Select this to view audits that were sent to an external audit store. To use this option, ensure that an external audit store and its associate lookup policy has been correctly configured. For more information, see "Managing the Audit Sink" on page 175 and "Working with the Audit Lookup Policy" on page 182.

To view or configure the lookup policy for the audit store, click **[Configure Audit Lookup Policy]** to load the lookup policy in the policy window.

---

**Note:** When viewing audits from an audit lookup policy, the following actions are unavailable from the File menu: Download Audit Events, Delete Old Audit Events, and Start Archiver. For more information, see "[Gateway Audit Event Actions](#)" below.


---

## Time Range Panel

**Note:** The Time Range panel is not available when viewing a saved audit file using the [Saved Events](#) task in Policy Manager or when the Gateway Audit Events window is [opened](#) from the [Service Metrics](#) window in the Dashboard.

The Time Range panel is used to narrow the audit events to a specified time period.

Table 119: Gateway Audit Events: Time Range

| Setting                       | Description   |
|-------------------------------|---|
| <b>Last x hours y minutes</b> | Select this option to specify the most recent number of <b>hours</b> and/or <b>minutes</b> . All audit events generated within this period are eligible to be displayed.  |
| <b>Auto-Refresh</b>           | Specify whether the Gateway Audit Events window should refresh automatically: <ul style="list-style-type: none"> <li>If auto-refresh is enabled, the list of audit events updates every 3 seconds, as shown in the <b>Last Updated</b> indicator at the bottom right corner of the window.</li> <li>If auto-refresh is disabled, the list updates only when you press <b>[F5]</b> or click <b>[View] &gt; Refresh</b>. Disabling auto-refresh is useful when you are attempting to troubleshoot.</li> </ul> |
| <b>From/To</b>                | Select this option to choose a time range to display audits. Specify the <b>From</b> and <b>To</b> dates either by typing or by clicking  and using the calendar control. Optionally modify the time, if necessary.  |
| <b>Time zone</b>              | If searching based on a different time zone, select it from the drop-down list. <p><b>Tip:</b> The results are displayed in the time zone selected for the search. If a non-default time zone was used, the time zone is noted next to the time in the <b>[Details]</b> tab.</p>  |

## Audit Record Search Parameters

The Audit Record Search Parameters panel lets you refine the audit events to display.

Table 120: Gateway Audit Events - Search Parameters

| Setting      | Description  |
|--------------|--|
| <b>Level</b> | From the drop-down list, select the severity of the events displayed: <ul style="list-style-type: none"> <li><b>All:</b> Display events of all severity levels. Use this setting to see the system messages generated by the gateway.</li> <li><b>Info:</b> Display events rated INFO, WARNING, or SEVERE.</li> <li><b>Warning:</b> Display events rated WARNING or SEVERE.</li> <li><b>Severe:</b> Display only SEVERE events.</li> </ul> |

| Setting                   | Description   |
|---------------------------|---|
| <b>Service</b>            | Display all events from the specified service. You can use wildcards here (for an example, see the <a href="#">Message</a> field).  |
| <b>Message</b>            | <p>Display all events with the specified message.</p> <p><b>Tip:</b> Use the wildcard '*' (asterisk) character to locate messages more easily. Examples:</p> <ul style="list-style-type: none"> <li><b>exported*</b> displays all messages that begin with the word 'exported'; no match is made if 'exported' appears in the middle of the message</li> <li><b>*exported*</b> displays all messages with the word 'exported', regardless of its position within the message.</li> </ul> <p>The search text is not case sensitive.</p>  |
| <b>Request ID</b>         | <p>Displays only audit events with the specified request identifier.</p> <p>You can use wildcards here (for an example, see the <a href="#">Message</a> field).</p> <p><b>Tip:</b> You can use the <a href="#">context variable</a> <code>\${requestId}</code> to access the request identifier.</p>  |
| <b>Audit Type</b>         | From the drop-down list, select the type of audit events to be displayed. For more information about each audit type, see Message Auditing in the <i>Layer 7 Policy Authoring User Manual</i> .   |
| <b>Node</b>               | Display all events from the specified node.   |
| <b>User Name</b>          | <p>Displays only audit events caused by the user with the specified user name. This is the user name used to log onto the Gateway via the Policy Manager. You can use wildcards here (for an example, see the <a href="#">Message</a> field).</p> <p>Note that this may return multiple users if more than one person has the same name or if wildcards are used (for example, if the user with the user name "john_smith" exists on more than one configured LDAP, or you search for "**Smith**").</p> <p>The user name applies as follows for each type of audit:</p> <ul style="list-style-type: none"> <li><i>Administrative audits:</i> The administrative user who carried out the action.</li> <li><i>Policy message audits:</i> The last authenticated user, if any.</li> </ul> <p>For more information about the audit types, see Message Auditing in the <i>Layer 7 Policy Authoring User Manual</i>.</p> |
| <b>User ID or User DN</b> | <p>Displays only audit events caused by the user with the specified User ID (for internal users defined in the <a href="#">Internal Identity Provider</a>) or User DN (for users defined in an external LDAP). Unlike user names, entering a User ID or User DN uniquely identifies a user. You can use wildcards here (for an example, see the <a href="#">Message</a> field).</p> <p><b>Tip:</b> See "User Name" above for information on how a user is interpreted for each audit type.</p>  |

## Entity Search Parameters

The Entity Type Search Parameters panel lets you optionally search the history of a selected entity. You can see everything that has happened to that entity and you can see all audits belonging to that entity.

- **Entity Type:** Choose the type of entity to search from the drop-down list.
- **Entity ID:** Enter the ID of the entity to search on.

## Associated Logs Search Parameter

The Associated Logs Search Parameter panel lets you search the contents of the [\[Associated Log\] tab](#) at the bottom of the viewer window.

- **Audit Code:** Enter the code of the audit message to search for. For a list of all the audit message codes, see "Appendix F: Audit Message Codes" on page 627.

## Message Operation Search Parameter

The Message Operation Search Parameter panel lets you search for audits based on a specific SOAP operation in the message.

- **Operation:** Enter the SOAP operation to search by.

## Validate Signatures

The **Validate Signatures** check box allows you to verify the signatures of the audits displayed in the Audit Events Panel.

When you select **Validate Signatures**, validation begins immediately and may take a moment to complete, depending on how many audit events were found and how many of those contain signatures. The status bar displays: "Signature validation is on" and the Audit Events Panel displays "Signature validation is on [In Progress]" to indicate that verification is in progress. "[In Progress]" is cleared when all audit records in the search result have been validated. While verification is in progress, you can manually clear this check box to suspend signature validation and reselect it to resume.

When signature validation is on, the "Sig" column of the [Audit Events Panel](#) displays the appropriate icon as each audit is verified. For a description of each icon, see the "Sig" column in Table 121.

The **Validate Signatures** check box is available only when there is a connection to the Gateway. Validating signatures may impact Gateway performance if audit records for the time period contain large request or response messages or large audit details.

---

**Note:** The **Validate Signature** check box is automatically cleared when you perform a new search and when the Gateway Audit Events window is opened. This ensures that validation will occur only when you explicitly select the check box.

---

## Audit Events Panel

The audit events panel displays the events for the given time period or filter criteria once **[Search]** is clicked. To help you analyze the events, you can click a column heading to re-sort the list based on that column.

To clear all search text fields and reset all the drop-down lists to their default settings, click **[Clear Search Criteria]**.

To cancel a search in progress, click **[Cancel]**.

---

**Tips:** (1) When a search filter is in effect, the following message displays above the Audit Events Panel to indicate that only a subset of records is being shown: "Caution! Constraint may exclude some events." (2) Audit events are displayed only if you have Read permission for "<Any Cluster Node Information>". Some predefined roles (such as "Manage X Service") include this permission. Custom roles may also include this permission.

---

The following table describes each column.

Table 121: Gateway Audit Events - Audit events

| Column Name        | Description  |
|--------------------|--|
| <b>Sig</b>         | <p>Indicates the signature status of the audit record:</p> <ul style="list-style-type: none"> <li><b>Red:</b> Audit record is signed, but the signature cannot be verified. This may indicate tampering of the audit record. <b>Note:</b> This may also indicate that the default SSL key used to sign the audit record is an ECC key, which is not supported.</li> <li><b>Yellow:</b> Audit signing is enabled, but the audit record is not signed.</li> <li><b>Green (check mark):</b> Audit record is signed and the signature is valid.</li> <li><b>Green (down arrow):</b> Audit record is signed, but the signature was not validated because the message exceeds 2.5MB in size.</li> <li><b>No symbol:</b> Audit signing is disabled and the audit record is not signed.</li> </ul> <p>Audit signing is controlled by the <a href="#">audit.signing</a> cluster property.</p> |
| <b>AuditRecord</b> | <p>Displays the internal audit record number. This number is useful when an audit record refers to another audit record by ID and you want to find that other audit record.</p>  |

| Column Name     | Description  |
|-----------------|--|
| <b>Node</b>     | Displays the Gateway node that the event applies to.   |
| <b>Time</b>     | Displays the time that the event took place in the Gateway. This time is displayed in the time zone selected for the search (if not searching by date then the time is displayed in the default time zone). Note that if a non-default time zone is selected, this is not displayed in the event listing but will be displayed in the <b>[Details]</b> tab.  |
| <b>Severity</b> | <p>Displays the severity rating for the event, as assigned by the Gateway.</p> <ul style="list-style-type: none"> <li>• <b>FINE, FINER, FINEST:</b> Internal system messages from the Gateway.</li> <li>• <b>INFO:</b> Reasonably significant informational messages.</li> <li>• <b>WARNING:</b> Indicates a potential problem.</li> <li>• <b>SEVERE:</b> Indicates a serious failure that requires immediate attention.</li> </ul> <p><b>Tip:</b> It is possible to override the severity of the Gateway audit messages, to help you exclude certain material from appearing in the audits. For more information, see "Overriding the Audit Level" on page 427.</p> <p>Note that the events that are displayed depend on the <a href="#">Time Range</a> and <a href="#">Audit Record Search Parameters</a>.</p> |
| <b>Service</b>  | The service that generated the event, if any.  |
| <b>Message</b>  | The actual event message.  |


## Event Details Panel

Select an audit event to see detailed information about the event. Information is organized across the tabs shown in Table 122.

Table 122: Gateway Audit Events - Event details

| Tab                    | Description   |
|------------------------|---|
| <b>Details</b>         | Displays detailed information about the audit event.  |
| <b>Associated Logs</b> | <p>Displays any associated logs for the event, if applicable. All audit codes from "Appendix F: Audit Message Codes" on page 627 can appear here.</p> <p>If the log information is encrypted, see below.</p> <p><b>Tips:</b></p> <ul style="list-style-type: none"> <li>• The <b>Code</b> column shows the associated <a href="#">Audit Message Code</a> for the audit message. This is to assist you if you wish to modify the audit message text using the <code>auditmsg.override.XXXX</code> <a href="#">cluster property</a>, or if you wish to reduce its runtime audit level so that it no longer appears here (see "Overriding the Audit</li> </ul> |



| Tab                                       | Description   |
|---|---|
|   | <p>Level" on page 427 for details).</p> <ul style="list-style-type: none"> <li>The <b>Detail</b> column will display a  button if there are further details about the event that are too large to display in a tooltip. Clicking this button will display comprehensive log information in a new window. If the details have been protected by an Audit Message Filter policy and your role permits it, clicking on the <b>[Invoke Audit Viewer Policy]</b> button will invoke the Audit Viewer policy for the audit detail. For more information, see <a href="#">"Invoking the Audit Viewer Policy"</a> below.</li> <li>Messages may convert non-identifiable characters into a string literal of their Unicode value. For example, if "null" is being expressed in a message, it will be displayed as "\u0000", which is the Unicode representation for null</li> </ul> |
| <b>Request</b>                            | <p>Displays the request message received by the Gateway after any required message processing (for example, WS-Security). Selecting <b>Reformat Request XML</b> will reformat the message for improved readability if XML.</p> <p>If the details have been protected by an Audit Message Filter policy and your role permits it, clicking on the <b>[Invoke Audit Viewer Policy]</b> button will invoke the Audit Viewer policy for the audit detail. For more information, see <a href="#">"Invoking the Audit Viewer Policy"</a> below.</p> <p><b>Note:</b> You can see the request message only if the <b>Save request</b> option is enabled in the Audit Messages in Policy assertion.</p>  |
| <b>Response</b>                           | <p>Displays the response message. Selecting <b>Reformat Response XML</b> will reformat the message for improved readability if XML.</p> <p>If the details have been protected by an Audit Message Filter policy and your role permits it, clicking on the <b>[Invoke Audit Viewer Policy]</b> button will invoke the Audit Viewer policy for the audit detail. For more information, see <a href="#">"Invoking the Audit Viewer Policy"</a> below.</p> <p><b>Note:</b> You can see the response message only if the <b>Save response</b> option is enabled in the Audit Messages in Policy assertion.</p>   |
| <b>Total</b><br>(bottom of window)        | <p>Displays the total number of records returned for a search. If there is a large number of records, the Gateway Audit Events window will display "(truncated)" next to the total number. Note that if <a href="#">auto-fresh</a> is enabled, the "(truncated)" label will disappear as soon as new records arrive, even though the display is still truncated.</p>  |
| <b>Last Updated</b><br>(bottom of window) | <p>Displays when the log was last updated. When the Gateway Audit Events window is <a href="#">opened</a> from the <a href="#">Service Metrics</a> window of the Dashboard, the time range from the selected bar is displayed here instead.</p>   |

## Invoking the Audit Viewer Policy

Information in the [Associated Logs], [Request], or [Response] tabs may be protected by the Audit Message Filter policy, if one was used to encrypt them. Click **[Invoke Audit Viewer Policy]** to invoke the Audit Viewer policy for the audit record or detail. The output of the Audit Viewer policy will be displayed in place of the original text. For more information about the Audit Message Filter and Audit Viewer policies, see Working with Internal Use Policies in the *Layer 7 Policy Authoring User Manual*.

---

**Note:** Only users with the [role](#) "Invoke Audit Viewer Policy" can invoke this policy via the audit viewer. For all other roles, the **[Invoke Audit Viewer Policy]** button is unavailable. For more information on security roles, see "Managing Roles" on page 130. To protect usages of any private key used in the Audit Viewer policy, see "Make Audit Viewer Key" in "Private Key Properties" on page 271.

---

## Gateway Audit Event Actions

While the Gateway Audit Events window is primarily for display, you can perform the following actions:


### Download Audit Events

---

**Note:** The Download Audit Events option is not available when the Gateway Audit Events window is [opened](#) from the [Service Metrics window](#) of the Dashboard. In the browser client version of the Policy Manager, downloading is possible only when the Java applet is running in the trusted mode. For more information, see "Starting the Policy Manager" on page 5.

---

➤ *To download audit events in the database to an external file:*

1. From the Gateway Audit Events window, select **[File] > Download Audit Events**. The Download Audit Events window appears.
2. Specify the **Time Range** for audit events to be downloaded:
  - **All:** Download all audit events in the database.
  - **From/To:** Download only those events that fall within the time range. You can either type the time values or click  to select the date from the calendar control. You can also change the time zone if necessary.
3. Specify the **Published Services** to be included:
  - **All:** Include all services. Note that this option will include all the system events that are automatically generated.

- **Selected:** Select one or more services to include (hold down the [Ctrl] key to select multiple services).
4. Do one of the following to specify the destination file:
    - Type the full path and name of the file.
    - Click [**Browse**] and then navigate to the target location, then enter a file name.

The system will add the ".zip" extension to the file name for you.

5. Click [**Download**]. The audit events are saved to the specified zip file.
6. Click [**Close**] when done.

The audit events are saved as a colon-delimited text file within a zip file. The file is accompanied by a digitally-signed XML file containing checksum and metadata information about the exported audit records. The XML file is signed using the Gateway's SSL certificate.

### Delete Audit Events

---

**Note:** The Delete Old Audit Events option is not available when the Gateway Audit Events window is [opened](#) from the [Service Metrics window](#) of the Dashboard.

---

It is recommended that you purge old audit records periodically to free up hard disk space and to prevent performance issues. When deleting, the Policy Manager will purge all audit records older than seven days. Audit events marked "Severe" will be retained.

➤ *To delete audit events:*

1. From the Gateway Audit Events window, select [**File**] > **Delete Old Audit Events**.
2. Click [**Delete Events**] when prompted to confirm.

Deletion will occur in the background, so that you can keep working. An audit event is created immediately and refreshes itself after every 10,000 events are deleted. This lets you monitor the progress of the deletion.

If the deletion is interrupted before it is complete (for example, a system failure occurs), the audit event will show the number of events purged up to that point.

When the system restarts, run **Delete Old Audit Events** again to finish the purge.

### Start Archiver

---

**Note:** The Start Archiver option is not available when the Gateway Audit Events window is [opened](#) from the [Service Metrics window](#) of the Dashboard.

---

This command is used to manually start the audit archiver if it is not already running, based on the settings in the [Configuring FTP Audit Archive](#) task. The status of the archive will be displayed on the Audit Events window.

This manual archive will not affect the scheduled archive task. For example, the default as specified by the [audit.archiverTimerPeriod](#) cluster property is to archive every 10 minutes. This will occur regardless of how many manual archive requests were made.

### Save Displayed Events

---

**Note:** In the browser client version of the Policy Manager, saving displayed events is possible only when the Java applet is running in the trusted mode. For more information, see "Starting the Policy Manager" on page 5.

---

Before saving audit events, be sure the events you want to save are currently displayed. Data that is filtered out will *not* be saved.

➤ *To save the currently displayed audit events:*

1. From the Gateway Audit Events window, select **[File] > Save as**.
2. Specify a file name and location or accept the defaults shown.

Accepting the suggested file name makes it easier to sort and organize your saved events. Be sure to preserve the **".ssga"** file extension.

3. Click **[Save]**.

---

**Note:** Saved audit events do not include the time zone. This means that when the events are viewed, they will be displayed in the default time zone.

---

➤ *To view the saved events:*

- See "Saved Events" on page 426 for details.

## Saved Events

You can view saved events even when not connected to the Gateway.

➤ *To view saved [audit](#) events:*

1. From the Policy Manager [Main Menu](#), click **[View] > Saved Events** (on the [browser client](#), from the **Monitor** menu).
2. Navigate to the appropriate ".ssga" file.
3. Click **[Open]**.

The saved audit events are displayed. You can view and filter the saved events in the same manner as live events.

---

**Note:** The saved data uses the node names that were in effect at the time of saving. This may differ from node names currently in use.

---

## Overriding the Audit Level

It is possible to change the severity of [audit messages](#) at run time to suit your needs. For example, you are finding that the auditing system is flagging material that you do not wish to appear in the audit logs. To solve this, identify the messages to suppress and then reassign them to a lower severity level to prevent them from being logged.

The following [cluster properties](#) are used to override audit levels:

```
audit.setDetailLevel.SEVERE  
audit.setDetailLevel.WARNING  
audit.setDetailLevel.INFO  
audit.setDetailLevel.CONFIG  
audit.setDetailLevel.FINE  
audit.setDetailLevel.FINER  
audit.setDetailLevel.FINEST  
audit.auditDetailExcludeList
```

Add the number of the audit message code to the appropriate property to reassign the code to that level. Separate multiple codes with commas. If a code appears in more than one property, the Gateway will use them in this order: SEVERE --> FINEST.

Note that codes entered into the property *audit.auditDetailExcludeList* will be excluded from auditing entirely.

---

**Note:** Overriding an audit level only changes the severity at run time. It does not change the level of the audit when displayed in the [Gateway Audit Events](#) window.

---



## Chapter 7: Identity Bridging

### The Identity Silo Problem

Controlling access to applications exposed as web services requires the authentication and authorization of requesting identities. Authentication involves validating the credentials that are presented, while authorization involves granting access, rights, or entitlements based on the interpretation of the authentication results. For consistent management, identities are typically stored in the same security domain as the application. During the authentication and authorization process, the exact elements in an identity are matched to the functional requirements of the services served by the identity provider. Identities from one identity provider rarely have much relevance outside of their local security domain. This leads to the creation of “identity silos”. Identity silos are a serious problem for enterprises wanting to integrate applications residing in different security domains.

If a legitimate requestor authenticates against a corresponding identity provider in one identity silo, its identity, or any evidence of the authentication may have no relevance when requesting access to another web service in another identity silo inside or outside the enterprise. Disparate identity providers within an enterprise or between partners complicates the authentication and authorization process, resulting in broken integrations and failed authorizations in one silo even when authentication succeeded in another silo.

### Identity Bridging for Cross-Domain Application Integration

Identity bridging is a powerful mechanism for merging identities from different security domains and breaking down identity silos. During identity bridging, the requestor domain is responsible for authenticating, while authorization is handled by the provider domain hosting the web service or it is entrusted at the source. In a mergers and acquisitions scenario, for example, Enterprise A merges with Enterprise B. Each enterprise has its own identity provider, but would like to share identities with minimum resources and no interruption to their existing security architectures. Using CA's products, identity bridging is configured between Enterprise A and Enterprise B using one of two credential source types: a [SAML](#) (Security Assertion Markup Language) token or an [X.509 certificate](#).

**Note:** For brevity, the generic "Trusted Authority" and "Federated Gateway" references are used in all identity bridging examples, workflows, and instructions. The Trusted Authority is the certificate authority (CA) that issues and manages security credentials and is responsible for authentication. The Federated Gateway is the web service provider that is responsible for authorization. The words "trusted" and "federated" are used from the point of view of the service requestor.

## Identity Bridging Using the SAML Credential SourceCA Technologies

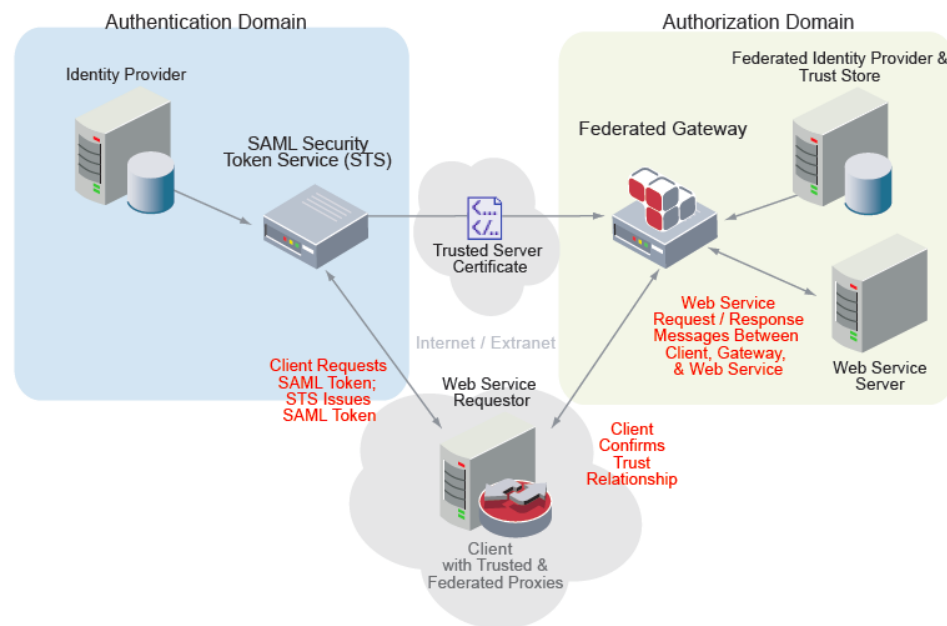


Figure 158: An Identity Bridging Configuration Using a SAML Token

A description of the data flow:

- Trust is established at design time. A Federated Identity Provider is mapped to the trust certificate.
- At design time, the Federated Gateway policy is configured with constraints requiring a SAML token signed by the Federated Identity Provider authority.
- At run time, the client requests a signed SAML token from the Security Token Service and then attaches it to the message as the SAML token profile. The Gateway confirms the signature and routes the message.



## Identity Bridging Using the X.509 Certificate Credential Source

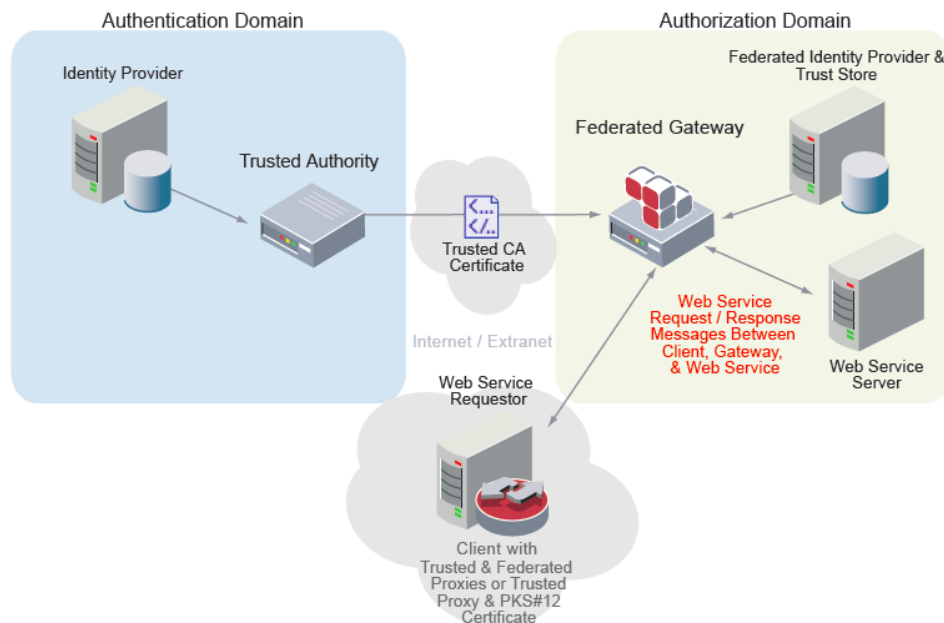


Figure 159: An Identity Bridging Configuration Using an X.509 Certificate

A description of the data flow:

- Trust is established at design time; a Federated Identity Provider is created.
- A Federated Gateway policy contains a SSL CMA or WS Signature.

## Identity Bridging with CA Products

### SecureSpan Gateway

The required provider-side Gateway, known as the "Federated Gateway" is used for authorization in an identity bridging configuration. The Federated Gateway establishes a certificate-based trust relationship with the authentication source by importing trusted certificates into its trust store. The authentication source can be any certificate authority (CA) or another Gateway that acts as a CA\*. For more information, see the *Securespan XML VPN Client User Manual*.

\*A Gateway acting as a certificate authority is available only for Securespan XML VPN Client use cases.

The Federated Gateway uses three types of federated identities for mediating requestor credentials: [federated users](#), [federated groups](#), and [virtual groups](#). It delegates authentication to one or more Trusted Authorities while preserving authorization for the Federated Gateway.

---

**Note:** Any of the Gateway products can be used for identity bridging. When SAML is used as a credential source in an identity bridging configuration, the authentication source must be able to issue a SAML token. If another Gateway is used as the credential source, then it is already able to issue a SAML token. See "Workflow Using SAML" on page 436 for more information.

---

## Securespan XML VPN Client

The requestor-side Securespan XML VPN Client is responsible for decorating request messages based on the web service policy assertions defined in the Federated Gateway. Decorated messages are sent from the Securespan XML VPN Client to the Federated Gateway for web service authorization. If a policy contains a Require SAML Token Profile assertion, then part of the client's decorating task may involve getting a SAML token from the Trusted Authority during the initial connection or if the original SAML token has expired.

## CA API Gateway Policy Manager

The Policy Manager provides the interface for [importing](#) trusted certificates (CA certificates and/or server certificates extracted from the Trusted Authority) into the Federated Gateway trust store. The Policy Manager also provides the interface to configure and manage one or more Federated Identity Providers (FIPs), link trust store certificate(s) to FIPs, and configure the Federated Gateway SAML policy.

## Identity Bridging Requirements

---

**Note:** For brevity, the generic "Trusted Authority" and "Federated Gateway" references are used in the identity bridging examples, workflows, and instructions. The Trusted Authority is the certificate authority (CA) that issues and manages security credentials and that is responsible for authentication. The Federated Gateway is the web service provider that is responsible for authorization.

---

The following items are required to configure identity bridging using a SAML or X.509 certificate credential source:

### Web Service Requestor-Side Requirements

- When SAML is used as the credential source in an identity bridging configuration, the client should be configured to retrieve a token from the Security Token Service.
- When an X.509 certificate is used as the credential source in an identity bridging configuration, the client should be configured with a client certificate pair signed by the Trusted Authority.

---

**Note:** For Securespan XML VPN Client use cases, refer to the *Securespan XML VPN Client User Manual*.

---

### Trusted Authority (Authentication Domain) Requirements

The Trusted Authority can be any of the following:

- When SAML is used as the credential source in an identity bridging configuration, the Trusted Authority may be any of the following:
  - another Gateway installed and configured (see the *Layer 7 Installation and Maintenance Manual* for details)
  - an identity provider that supports WS-Trust
  - an identity provider that supports WS-Federation Passive Requestors; for example, Active Directory Federation Services (ADFS)
- When an X.509 certificate is used as the credential source in an identity bridging configuration, any certificate authority (CA) that issues certificates (such as a system employing the "OpenSSL" toolkit) can be used to sign client certificates.
- One CA certificate (to be imported into the Federated Gateway trust store when using an X.509 certificate credential source; see "Workflow Using an X.509 Certificate" on page 437)

- One server certificate (to be imported into the Federated Gateway trust store when using the SAML credential source; see "Workflow Using SAML" on page 436)
- Individual client certificates signed by the CA certificate. For additional confidence in authorizing identities by users' X.509 client certificates, these certificates may be imported into the Federated Gateway trust store for the Federated Identity Provider; see "Workflow Using an X.509 Certificate" on page 437. These certificates may also be imported into the Internal Identity Provider or the LDAP Identity Provider.

## Federated Gateway (Authorization Domain) Requirements

- Gateway installed and configured
- Policy Manager installed and configured
- CA certificate(s) imported from trusted credential source(s) (imported from the Trusted Authority when configuring an X.509 certificate credential source; see ["Workflow Using an X.509 Certificate" on page 437](#))
- Imported server certificate(s) imported from trusted credential source(s) (imported from the Trusted Authority when configuring a SAML credential source; see "Workflow Using SAML" on page 436)
- Individual client certificates (optionally imported for the federated users; see ["Workflow Using an X.509 Certificate" on page 437](#)).

## Verifying Hostnames for Outbound SSL Connections

Part of the SSL Trust behaviour in the Gateway is to ensure that the hostname in a server's SSL certificate matches the hostname used in the outbound SSL request. However, you can suppress this verification for testing purposes or for added flexibility in your production environment, if you are confident that allowing mismatched hostnames will not impair security.

The Gateway uses a two layer system to determine when hostnames should be verified:

- the setting **Verify Hostnames for Outbound SSL Connections** in the [Options] tab of a certificate's [properties](#)
- the setting of the [io.httpsHostVerify](#) cluster property

---

**Note:** Hostname verification is only performed once the server's SSL certificate is accepted. If a certificate is not trusted then the connection will fail and hostname verification will not be performed.

---

The hostname verification procedure applies whenever any of the following assertions are present in a policy:

Exchange Credentials using WS-Trust

Route via HTTP(S)

Retrieve SAML Browser Artifact

Use WS-Federation Credential (both Request and Exchange modes)

The following diagram describes how the Gateway determines whether to use the certificate setting or the gateway cluster property:

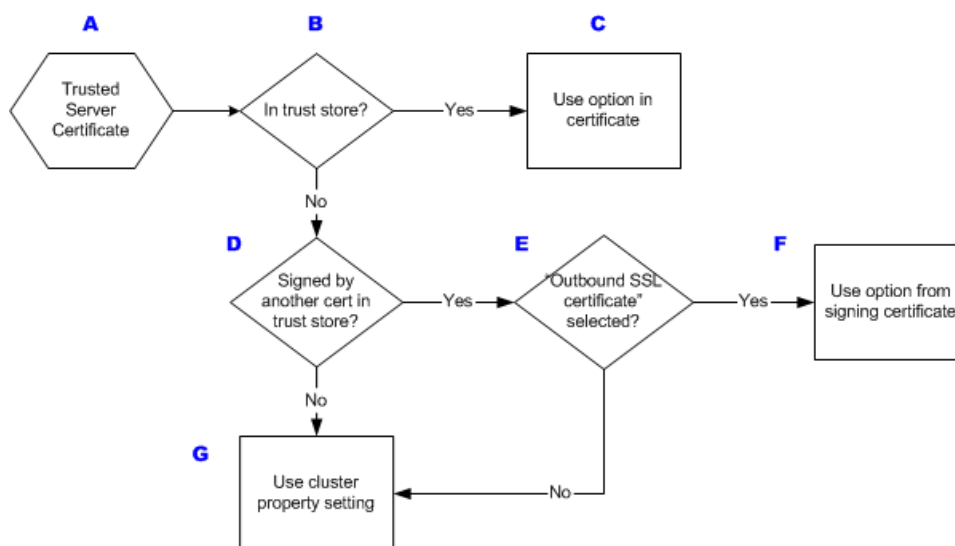


Figure 160: How the Gateway determines when to verify hostnames

The following table describes each step in the process:

Table 123: Verifying hostnames flowchart explanation

| Flowchart step                                   | Description  |
|--|--|
| <b>A. Trusted Server Certificate</b>             | This is a certificate that is either issued by a trusted certificate authority, by another trusted certificate in the Gateway, or has been added to the Gateway's trust store.                   |
| <b>B. In trust store?</b>                        | Has the certificate in (A) been added to the Gateway's trust store?  |
| <b>C. Use option in certificate</b>              | If (B) is 'Yes', then the <b>Verify Hostnames for Outbound SSL Connections</b> setting in the certificate properties is used. The gateway cluster property is <u>not</u> consulted in this case. |
| <b>D. Signed by another cert in trust store?</b> | If (B) is 'No', is the certificate signed by another certificate in the trust store?   |

| Flowchart step                                 | Description  |
|--|--|
| <b>E. "Outbound SSL certificate" selected?</b> | If (D) is 'Yes', does the signing certificate have its <b>Signing Certificates for Outbound SSL Connections</b> option selected? This option appears in the <a href="#">certificate properties</a> , under the [Options] tab.                |
| <b>F. Use option from signing certificate</b>  | If (E) is 'Yes', then the <b>Verify Hostnames for Outbound SSL Connections</b> setting from the signing certificate is used. The gateway cluster property is <u>not</u> consulted in this case.  |
| <b>G. Use cluster property setting</b>         | All other scenarios will use the cluster property setting. For example, the certificate is signed by an external trust authority, or the certificate is signed by a trusted certificate that is not configured for outbound SSL connections. |

## Workflow Using SAML

**Note:** In the workflow below, the "Trusted Authority" is the certificate authority (CA) that issues and manages security credentials and is responsible for authentication. The "Federated Gateway" is the web service provider that is responsible for authorization.

The table below summarizes how to configure [identity bridging](#) using a SAML credential source. Follow the cross references for more details of each step.

Table 124: Identity Bridging workflow using SAML

| Step  | For more information, see...  |
|---|---|
| <b>Step 1:</b> Confirm that your system meets the requirements for configuring identity bridging with SAML.   | "Identity Bridging Requirements" on page 433  |
| <b>Step 2:</b> Connect to the Federated Gateway B.  | "Connecting to the Gateway" on page 8   |
| <b>Step 3:</b> Add the signing certificate from the Trusted Authority (issued by the Trusted Authority's CA) to the trust store of Federated Gateway. | "Adding a New Certificate" on page 239 <ul style="list-style-type: none"> <li>In Step 3 of the <a href="#">Add Certificate Wizard</a>, select the <b>Signing SAML Tokens</b> check box.</li> </ul>  |
| <b>Step 4:</b> Create a new Federated Identity Provider (FIP) in Federated Gateway.   | "Creating a Federated Identity Provider" on page 441 <ul style="list-style-type: none"> <li>In Step 1 of the <a href="#">Federated Identity Provider Wizard</a>, select the <b>SAML Token</b> check box.</li> <li>In Step 2 of the wizard, click <b>[Add]</b> to attach the Trusted Authority signing certificate that was imported in Step 2 above.</li> </ul> |

| Step   | For more information, see...                                  |
|--|---|
| <b>Step 5:</b> Configure a policy with the SAML Token for the shared web service.      | "Configuring SAML Policies for Identity Bridging" on page 462 |
| <b>Step 6:</b> Configure authentication against the Federated Identity Provider (FIP). | Authenticate Against Identity Provider Assertion              |
| <b>Step 7:</b> Consume the shared web service.   |   |

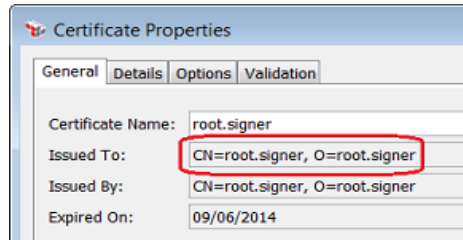
## Workflow Using an X.509 Certificate

**Note:** The "Trusted Authority" is the certificate authority (CA) that issues and manages security credentials and which is responsible for authentication. The "Federated Gateway" is the web service provider that is responsible for authorization.

The table below summarizes how to configure [identity bridging](#) using an X.509 Certificate credential source. Follow the cross references for more details of each step.

Table 125: Identity Bridging workflow using an X.509

| Step   | For more information, see...   |
|--|--|
| <b>Step 1:</b> Confirm that your system meets the requirements for configuring identity bridging with SAML.  | "Identity Bridging Requirements" on page 433   |
| <b>Step 2:</b> Import one or more Trusted Gateway A certificates into the Federated Gateway B trust store.   | See " <a href="#">Certificate Usage Scenarios</a> " below for the correct procedure based on the type of certificate.  |
| <b>Step 3:</b> Create a new Federated Identity Provider.   | <p>"Creating a Federated Identity Provider" on page 441</p> <ul style="list-style-type: none"> <li>In Step 1 of the <a href="#">Create Federated Identity Provider Wizard</a>, select [<b>X.509 Certificate</b>] for <b>Credential Source Type Allowed</b>.</li> <li>For the "CA Certificate ONLY" and "Both CA Certificate and Client Certificates" scenarios, click [<b>Add</b>] in Step 2 of the Wizard to attach the imported Trusted Gateway A CA certificate.</li> </ul> <p><b>IMPORTANT:</b> Do <u>not</u> click [<b>Add</b>] if your scenario is "Individual Client Certificate ONLY".</p> |
| <b>Step 4:</b> If using the "CA Certificate ONLY" and "Both CA Certificate and Client Certificates" scenarios, create a new federated user for each client certificate that you want to trust, then import the client certificate. | <p>"Creating a Federated User" on page 446</p> <ul style="list-style-type: none"> <li>In the Create Federated User dialog, <b>X509 Subject DN</b> field: Enter the subject DN that corresponds to the <b>Issued to:</b> value in the client certificate (see "Editing a Certificate" on page 247):</li> </ul>  |

| Step   | For more information, see...  |
|--|---|
|  |  <ul style="list-style-type: none"> <li>Select the <b>Define Additional Properties</b> option and then import the target client certificate (see step 3 under "Creating a Federated User" on page 446).</li> </ul>  |
| <b>Step 5:</b> Add additional federated users, federated groups, and/or virtual groups as required.  | <p>"Creating a Federated User" on page 446</p> <p>"Creating a Federated Group" on page 451</p> <p>"Creating a Federated Virtual Group" on page 452</p> <ul style="list-style-type: none"> <li>You cannot create a virtual group for a federated identity provider (FIP) unless it contains at least one trusted certificate. In this workflow, this is a CA certificate that is attached to the FIP using the "Federated Identity Provider Wizard" on page 442.</li> <li>A virtual group cannot be created in the "Client Certificate ONLY" scenario, because a trusted certificate does not exist in the FIP.</li> </ul> |
| <b>Step 6:</b> In the Securespan XML VPN Client, configure Gateway Accounts use either the Full Identity Bridging or Ad-Hoc Identity Bridging methods. | <p>See <i>Configuring Gateway Accounts</i> in the Securespan XML VPN Client documentation for more information on which method to choose.</p> <p>See <i>Full Identity Bridging</i> or <i>Ad-Hoc Identity Bridging</i> in the Securespan XML VPN Client documentation for details of each method.</p>  |
| <b>Step 7:</b> Consume the shared web service.   |   |

## Certificate Usage Scenarios

The following table summarizes how to import Trusted Authority certificates into the Federated Gateway trust store based on the certificate involved.

The certificate importation occurs in [Step 3](#) of the workflow. Be sure to resume the workflow at [Step 4](#) when done.



### Scenario 1: CA Certificates ONLY

When only CA (Certificate Authority) certificates are involved, import them into the Federated Gateway B trust store using the [Add Certificate Wizard](#). In Step 3 of the wizard, be sure to select the **Signing Client Certificates** option. This signifies that the CA certificate is trusted to authenticate identities in this FIP by signing their X.509 certificates.

### Scenario 2: Individual Client Certificates ONLY

When only client certificate are involved, import them via the Additional Properties dialog of a Federated Identity Provider User (step 3 of [Creating a Federated User](#)). You can do this when performing Step 6 of the workflow. Do not attach imported client certificates to the FIP in the [Create Federated Identity Provider Wizard](#).

Additional notes about this scenario:

- The Federated Identity Provider (FIP) must not contain any trusted certificates (either CA or server). To confirm this, the Trusted Certificates box in Step 2 of the [Create Federated Identity Provider Wizard](#) must be empty when you are performing workflow [Step 4](#).

If trusted certificates are added to the FIP, the Gateway will assume you are using "Scenario 3: CA Certificate and Individual Client Certificates" instead.

- Since no trusted certificates are attached to the FIP, you cannot create a [virtual group](#) for the FIP.
- When no CA certificates are trusted by the FIP, federated users must have client certificates in order to be authorized.
- When a client certificate is imported for a federated user, incoming certificate-based credentials will be compared against the stored client certificate. Any mismatch will cause an authorization failure, even if the certificate in the request was signed by a trusted CA.

### Scenario 3: Both CA Certificate and Individual Client Certificates

When both CA and client certificates are involved, do the following:

- Import the CA certificate as described in [Adding a New Certificate](#). When you reach Step 3 of the [Add Certificate Wizard](#), select the **Signing Client Certificates** option. This signifies that the CA certificate is trusted to sign the client certificates for federated users in this FIP.

- Import the client certificates as described in [Step 5](#) of the workflow. Do not attach imported client certificates to the FIP in the [Create Federated Identity Provider Wizard](#).

Additional notes about this scenario:

- The individual client certificates must be signed by the CA certificate.
- When a client certificate is imported for a federated user, incoming certificate-based credentials will be compared against the stored client certificate. Any mismatch will cause an authorization failure, even if the certificate in the request was signed by a trusted CA.

## Federated Identity Providers

---

**Note:** The generic "Trusted Authority" and "Federated Gateway" references are used in the identity bridging examples, workflows, and instructions. The Trusted Authority is the certificate authority (CA) that issues and manages security credentials and that is responsible for authentication. The Federated Gateway is the web service provider that is responsible for authorization.

---

In an [identity bridging](#) configuration, the Federated Identity Provider (FIP) is an essential element when bridging disparate security domains. It allows the Federated Gateway (authorization domain) to authorize requests containing credentials originating in the Trusted Authority (authentication domain). Credentials may be X.509 certificates signed by trusted certificate authorities (CAs) or SAML tokens signed by a Security Token Service. Alternatively, a Federated Identity Provider may not contain any certificates.

The trust store in the Federated Gateway is the repository for the certificates from other security domains that may be required by the FIP in an identity bridging configuration. Certificates are defined and added to the trust store with the [Add Certificate Wizard](#) prior to creating the FIP in the Federated Gateway. The chosen credential source and optional configuration elements outlined in [Workflow Using an X.509 Certificate](#) or [Workflow Using SAML](#) determine certificate and FIP configuration details. Once the trusted certificates are added to a new FIP, federated users, groups, and/or virtual groups can be created to authorize corresponding users, groups, or credential patterns in the Federated Gateway security domain.

---

**Note:** For the SAML credential source, SAML constraints are defined in the Require SAML Token Profile assertion that is included in the Web service policy. Ensure that all required certificates are added to the trust store prior to creating a Federated Identity Provider.

---

## Creating a Federated Identity Provider

➤ To add a new [Federated Identity Provider](#) in the Policy Manager:

1. Do one of the following:
  - Click **Create Federated Identity Provider** on the [Home Page](#)
  - Click **[Tasks] > Create Identity Provider > Create Federated Identity Provider** from the [Main Menu](#)
  - Right-click the "Identity Providers" title at the top of the [\[Identity Providers\] tab](#) and then select **Create Federated Identity Provider**.
2. Complete the [Federated Identity Provider](#) wizard. The new FIP is added to the [\[Identity Providers\]](#) tab.

## Cloning a Federated Identity Provider

A quick method to create a new Federated Identity Provider is to clone an existing one. After cloning, simply update the appropriate settings. Note that the cloned identity provider has no connection to the original once it has been created.

➤ To create a new Federated Identity Provider based on an existing one:

1. In the **[Identity Providers]** tab, right-click the federated Identity provider you wish to clone and select **Clone Identity Provider**.
2. Complete the [Federated Identity Provider](#) wizard by updating the settings as required. The new identity provider is added to the **[Identity Providers]** tab.

## Editing a Federated Identity Provider

➤ To modify the details of a [Federated Identity Provider](#):

1. Do one of the following:
  - In the [\[Identity Providers\] tab](#), double-click the name of the Federated Identity Provider to edit
  - In the [\[Identity Providers\] tab](#), right-click the Federated Identity Provider to edit and then select **Properties**.
2. Update the identity provider by completing the "Federated Identity Provider Wizard" on page 442.

## Deleting a Federated Identity Provider

➤ To delete a [Federated Identity Provider](#) from the Policy Manager:

1. In the [\[Identity Providers\] tab](#), right-click the Federated Identity Provider to delete and then select **Delete**.
2. Click **[Yes]** to confirm. The identity provider is removed.

---

**Note:** You cannot delete a Federated Identity Provider that has users and groups still attached to the policy. To delete the FIP, you must first [delete](#) the FIP users and groups from all policies.

---

## Federated Identity Provider Wizard

The *Federated Identity Provider Wizard* helps you [add](#) or [edit](#) an identity provider in the Federated Gateway.

For more information on using wizards, see "[Wizards](#)" under "Interfaces" on page 13.

### Step 1: Enter Provider Information

This step of the wizard lets you specify a name for the Federated Identity Provider and select which credential source types to allow.

Figure 161: Create Federated Identity Provider Wizard - Step 1

Configure this step as follows:

- **Provider Name:** Enter the name of the Federated Identity Provider. This name will appear in the [Identity Providers] tab.
- **Credential Source Type Allowed:**
  - Select **X.509 Certificate** if using X.509 certificates for credential authorization.
  - Select **SAML Token** if using a Require SAML Token Profile assertion for credential authorization.
- **Security Zone:** Optionally choose a security zone. To remove this entity from a security zone (security role permitting), choose "**No security zone**". For more information about security zones, see [Understanding Security Zones](#) in the *Layer 7 Policy Manager User Manual*. **Note:** This control is hidden if either: (a) no security zones have been defined, or (b) you do not have Read access to any security zone (regardless of whether you have Read access to entities inside the zones).

## Step 2: Select the Trusted Certificates

This step lets you add trusted certificates to be used by the Federated Identity Provider.

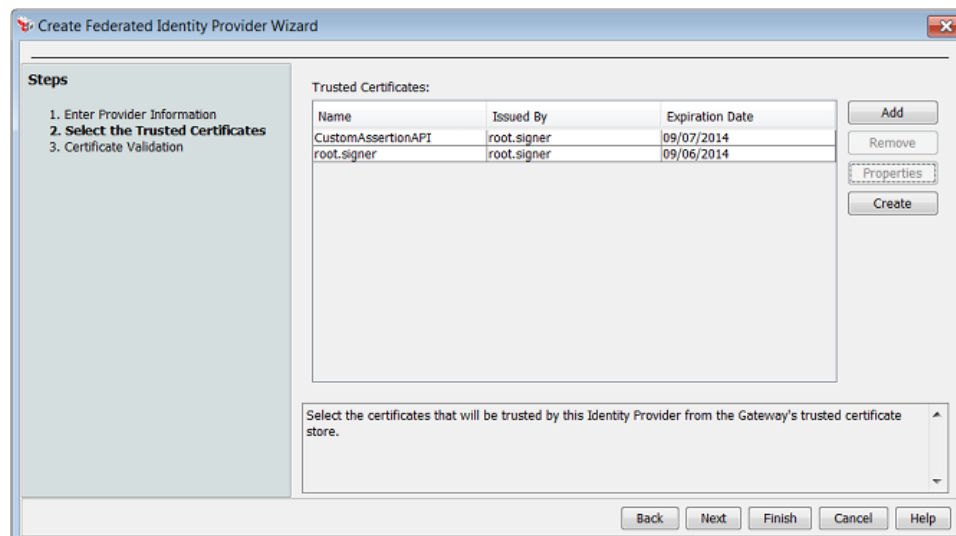


Figure 162: Create Federated Identity Provider Wizard - Step 2

➤ To add an existing certificate:

1. Click **[Add]**. The Search Trusted Certificates dialog appears.
2. Optionally specify a **Subject DN** or **Issuer Name** to filter the search.
3. Click **[Search]**. The results appear in the **Search Results** list.
4. Select one or more certificates to add, then click **[Select]**.

**Note:** You will be warned if you select a trusted certificate already in use by another Federated Identity Provider. If this was intentional and your policies allow this, click **[OK]** to continue with the duplicates. Otherwise, click **[Cancel]** and specify another certificate.

➤ *To remove a certificate:*

1. Select the certificate to remove.
2. Click **[Remove]**. The certificate is removed immediately.

➤ *To view details about a certificate:*

1. Select the certificate to view.
2. Click **[Properties]**. The certificate details are displayed. You cannot modify any of the certificate properties.

➤ *To add a new certificate:*

1. Click **[Create]**. The [Add Certificate Wizard](#) appears.
2. Complete the wizard to create the new certificate.

### Step 3: Certificate Validation

This step lets you specify how certificates for this Federated Identity Provider should be validated.

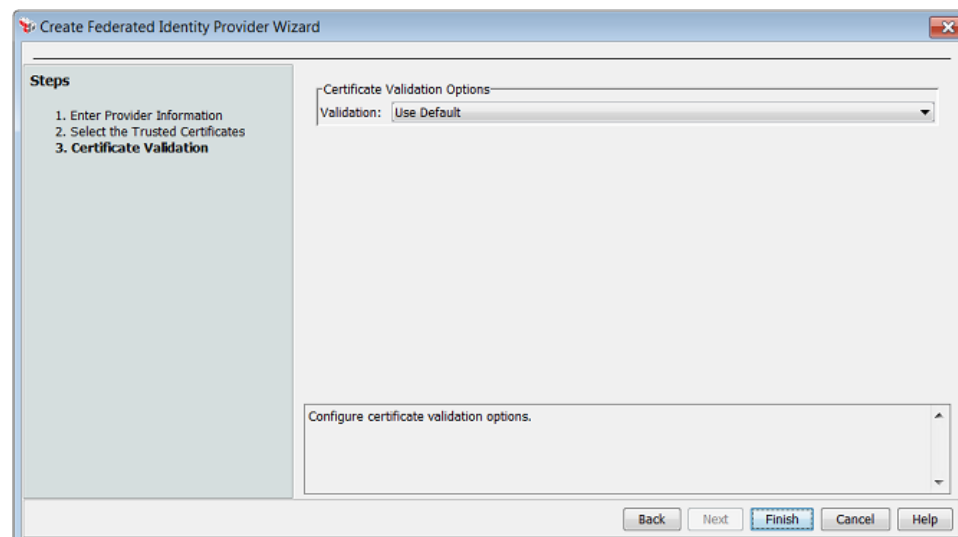


Figure 163: Create Federated Identity Provider Wizard - Step 3

By default, the method defined for Identity Providers in the [Manage Certificate Validation](#) dialog is used. To override this default, choose another validation option from the drop-down list.

For a description of each option, see "Managing Certificate Validation" on page 251.

## Federated Identity Provider Users and Groups

In an [identity bridging](#) configuration, the federated users, groups, and virtual groups added to the [Federated Identity Provider](#) (FIP) serve to authorize corresponding users, groups, or credential patterns in other trust domains. Each FIP can contain zero or more federated users, groups and/or virtual groups:

### Federated Users

A federated user contains a number of attributes relating to users in other trust domains, including:

- A DN (distinguished name). The subject of the signed certificate in an incoming request must exactly match the DN of the federated user
- A login that may be found in the NameIdentifier of an incoming SAML NameIdentifier with the "windowsDomain" format. (SAML credential source only; see [Workflow Using SAML](#))
- An email address, if applicable, that may be found in the NameIdentifier of an incoming SAML assertion with the "emailAddress" format. (SAML credential source only; see [Workflow Using SAML](#))
- An X.509 certificate that may be found in an incoming WS-Security X.509 BinarySecurityToken or HTTPS client certificate. (Self-signed or otherwise explicitly trusted; see [Workflow Using an X.509 Certificate](#)).

Only request credentials that exactly match the federated user DN and other information will pass the corresponding user assertion that is required to gain web service access.

### Federated Groups

Federated groups allow administrators to organize federated users into groups that have local relevance.

### Federated Virtual Groups

A federated virtual group is a pattern that incoming request credentials must match. The pattern may include:

- The subject of a signed certificate
- A regular expression describing a pattern that the NameIdentifier value in incoming SAML tokens (with the corresponding NameIdentifier format) must match (SAML credential source only; see [Workflow Using SAML](#))
- A set of attribute names and values that must be present in incoming SAML tokens that have an AttributeStatement. The allowable attribute names must have been previously registered with the FIP. (SAML credential source only; see [Workflow Using SAML](#)).

Virtual groups allow authorization of users who are not explicitly defined in the Federated Identity Provider by matching the attributes of the users' credentials. Users authorized in this manner are known as *federated virtual users*. Virtual groups can also include users explicitly defined in the Federated Identity Provider, though such users are not virtual.

In order to authorize users in a virtual group, a Federated Identity Provider (FIP) must contain the CA root certificate of the issuer of the certificates belonging to the identities in the virtual group. See [Adding a New Certificate](#) for information on adding a certificate to the trust store.

## Federated Virtual Users

A federated virtual user is someone who is authenticated as a member of a *federated virtual group* by matching attributes of the user's credentials, or someone who is authenticated against the FIP, but whose credentials do not match those of any user explicitly defined in the FIP. Virtual users are not explicitly defined in the Federated Identity Provider (FIP) and will not appear when [searching](#) the provider.

## Creating a Federated User

---

**Tip:** Before creating a new federated user, it is recommended that you view the properties of the signed certificates attached to the [Federated Identity Provider](#). Note the values, such as the "Issued to" value, that must be configured in the Create Federated User dialog. For information on viewing certificate properties, see "Editing a Certificate" on page 247.

---

➤ To create a new [federated user](#) in the Federated Identity Provider (FIP):

1. On the Policy Manager interface, select the **[Identity Providers]** tab. One or more Federated Identity Providers should be visible.

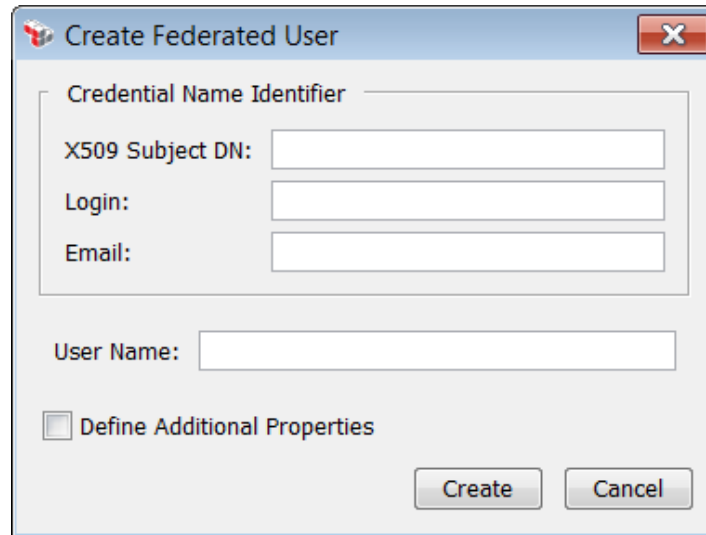
---

**Note:** If no FIP is listed, then you must [create](#) one before you can add a federated user.

---



- Right-click the appropriate FIP and then select **Create User**. The Create Federated User dialog appears.



The dialog box is titled "Create Federated User" and contains the following fields and controls:

- Credential Name Identifier** (group box):
  - X509 Subject DN:
  - Login:
  - Email:
- User Name:
- ☐ Define Additional Properties
- Create** and **Cancel** buttons.

Figure 164: Create Federated User dialog

- Configure the dialog as follows:

Table 126: Federated user basic properties

| Setting                             | Description   |
|-------------------------------------|---|
| <b>X509 Subject DN</b>              | Enter the DN value that incoming certificate-based credentials must match in order to be authorized as this federated user. For example: <i>CN=user A</i> .   |
| <b>Login</b>                        | Optionally, enter a value into the <b>Login</b> field, to allow this user to be authorized based on incoming SAML tokens with "windowsDomain" NameIdentifier formats.   |
| <b>Email</b>                        | Optionally, enter a value into the <b>Email</b> field. allow this user to be authorized based on incoming SAML tokens with the "emailAddress" NameIdentifier format.  |
| <b>User Name</b>                    | <p>Optionally, replace the user name that was derived from the <b>Subject DN</b> and placed in the <b>User Name</b> field with a name unique to the federated user.</p> <p><b>Note:</b> The User Name is displayed on the <a href="#">Search Identity Provider</a> dialog when searching and/or adding federated users to a policy. The User Name is a human readable value that does not impact the usage or validity of the federated user in an identity bridging configuration.</p> |
| <b>Define Additional Properties</b> | Select this check box if you want to enter additional information about the user. All additional information is optional.   |

- Click [**Create**].

- If you are not defining additional properties, the dialog closes and the user is added to the Federated Identity Provider.
  - If you are defining additional properties, the Properties dialog for the user is displayed. For more detailed information about this dialog, see "Federated User Properties" on page 448.
5. Click **[OK]**. The dialog closes and the user is added to the Federated Identity Provider.

The user is now available for adding to policies. If this user will need to log into the Policy Manager, you must assign this person to at least one role. For more information, see "Managing Roles" on page 130.

## Federated User Properties

Every [federated user](#) has a set of extended user properties that can be set either when the user is first added to the system, or deferred until a later date. (During initial entry, only a minimal amount of user data is required, to facilitate rapid entry of many users.)

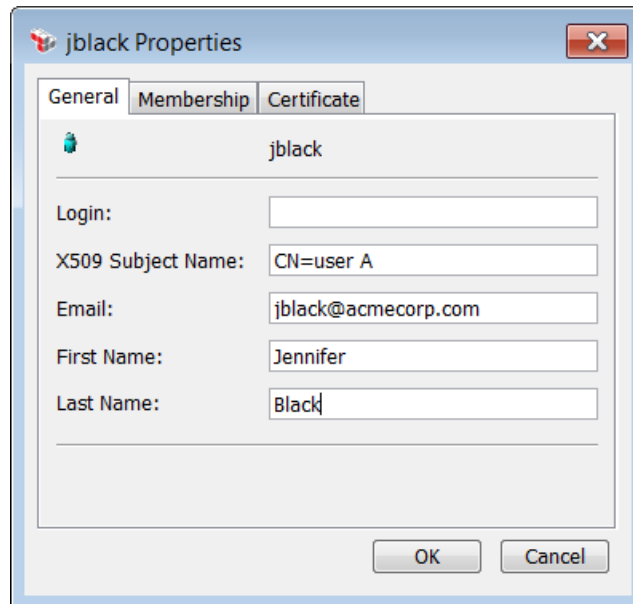
➤ *To access the properties for a federated user:*

1. Do one of the following:
  - [Create a new federated user](#), making sure to select the **Define Additional Properties** check box.
  - [Edit](#) an existing federated user.
  - Locate the group by [searching the identity provider](#).

The User Properties dialog appears.

3. Configure each tab within the properties as necessary. All information is optional. Refer to the appropriate section below for a complete description of each tab.
4. Click **[OK]** when done.

### Configuring the [General] Tab

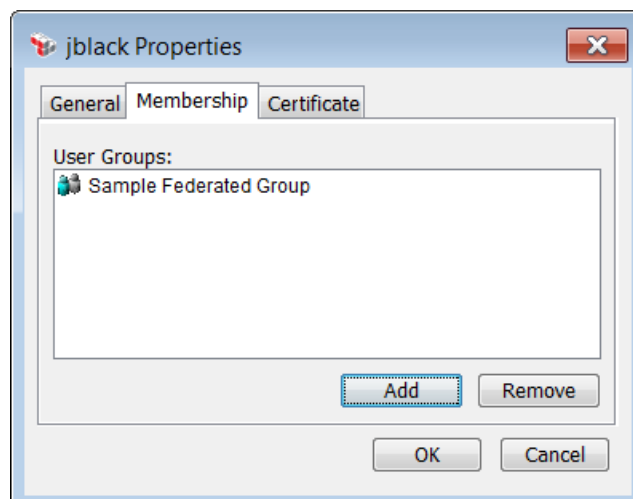


The screenshot shows the 'jblack Properties' dialog box with the 'General' tab selected. The dialog has three tabs: 'General', 'Membership', and 'Certificate'. The 'General' tab contains a user icon and the name 'jblack'. Below this are several text input fields: 'Login:' (empty), 'X509 Subject Name:' (containing 'CN=user A'), 'Email:' (containing 'jblack@acmecorp.com'), 'First Name:' (containing 'Jennifer'), and 'Last Name:' (containing 'Black'). At the bottom right are 'OK' and 'Cancel' buttons.

This tab is used to enter the user's full name, as well as enter or modify any of the fields entered in the basic properties (see "Creating a Federated User" on page 446).

- **First Name:** Enter the user's first name.
- **Last Name:** Enter the user's last name.

### Configuring the [Membership] Tab



The screenshot shows the 'jblack Properties' dialog box with the 'Membership' tab selected. The dialog has three tabs: 'General', 'Membership', and 'Certificate'. The 'Membership' tab contains a section titled 'User Groups:' with a list box below it. The list box contains one entry: 'Sample Federated Group'. Below the list box are 'Add' and 'Remove' buttons. At the bottom right are 'OK' and 'Cancel' buttons.

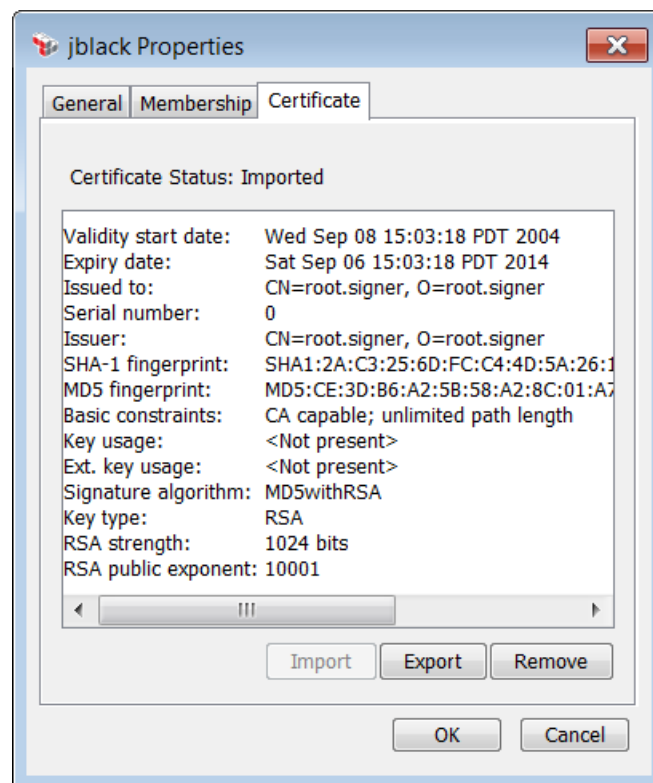
This tab displays the [federated groups](#) to which the user belongs.

1. Click **[Add]**. A list of federated groups is displayed.
2. Select one or more groups that the user belongs to.

**Note:** If the group you want isn't in the list, define it first using the steps under [Adding a New Federated Group](#).

3. Click **[Add]**. The user is added to the group.
4. If you need to remove a user from a group, select the group and then click **[Remove]**.

### Configuring the [Certificate] Tab



This tab is used to manage the certificate for the user.

- To import a certificate for the user, click **[Import]** and then complete the [Add Certificate Wizard](#).
- To export a certificate, click **[Export]** and then specify a file name and location.
- To remove a certificate, click **[Remove]** and then click **[OK]** to confirm. Removing a certificate removes both the certificate and the user's password.

---

**Note:** It is only necessary to import client certificates for federated users when the Federated Identity Provider (FIP) is configured with no trusted CA certificates. When the FIP is configured with one or more CA certificates, then federated users can be successfully authorized based only on the attributes entered in the Create Federated User dialog, as long as the certificate presented along with their request was signed by one of the CAs whose certificates are trusted by the FIP. For more information on the different X.509 certificate credential source scenarios, see "Workflow Using an X.509 Certificate" on page 437.

---

## Creating a Federated Group

Groups help you organize your users and they are a time-saving tool. For example, granting web service or XML application access to a group of users is much quicker than granting access individually.

➤ To add a new group to the Federated Identity Provider (FIP):

1. On the Policy Manager interface, select the **[Identity Providers]** tab. One or more Federated Identity Providers should be visible.

---

**Note:** If no FIP is listed, then you must [create](#) one before you can add a federated group.

---

2. Right-click the FIP name in the **[Identity Providers]** tab and select **Create Group**. The Create Federated Group dialog appears.

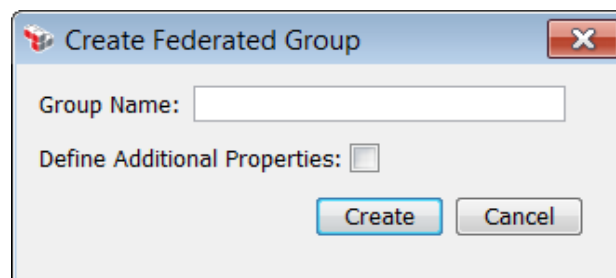


Figure 165: Create Federated Group dialog

3. Enter a name for the group in the **Group Name** field.
4. Select the **Define Additional Properties** check box if you wish to enter additional information about the group at this time. All additional information is optional.
5. Click **[Create]**.
  - If you are not defining additional properties, the dialog closes and the group is added to the Internal Identity Provider.

- If you are defining additional properties, the assertion properties are displayed. Complete each tab as necessary. All fields are optional.

Table 127: Federated group additional properties

| Tab        | Description   |
|------------|---|
| General    | <ul style="list-style-type: none"> <li>• <b>Description:</b> Enter a description of the group.</li> </ul>   |
| Membership | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>. A list of users appear.</li> <li>2. Select one or more users who belong to this group.</li> <li>3. Click <b>[Add]</b>. The user(s) are added to the group.</li> <li>4. If you need to remove a user from a group, select that user and then click <b>[Remove]</b>.</li> </ol> |

6. In the Group Properties dialog, click **[OK]**. The dialog closes and the group is added to the Federated Identity Provider.

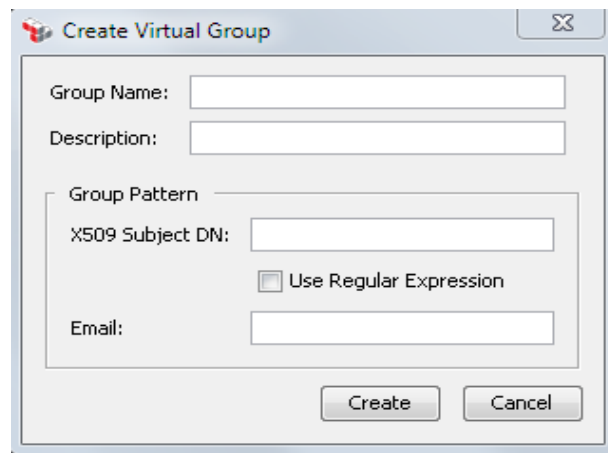
## Creating a Federated Virtual Group

Specific conditions must exist before you can create a [federated virtual group](#):

- The [Federated Identity Provider \(FIP\)](#) must contain a trusted certificate (In the [X.509 certificate workflow](#), the trusted certificate is a CA root certificate attached to the FIP. As for the [SAML workflow](#), the trusted certificate is an SSL server certificate attached to the FIP. These certificates are attached with the [Create Federated Identity Provider Wizard](#)).
- Since the imported certificate will have been used to sign client certificates, the **[Signing Client Certificates]** setting in Step 3 of the [Add Certificate Wizard](#) must also have been selected.
- A virtual group cannot be created under the "[Client Certificate Only](#)" scenario in the X.509 certificate workflow, since trusted certificates do not exist in the FIP.

➤ To add a new virtual group to the Federated Identity Provider (FIP):

1. Right-click the FIP name in the **[Identity Providers]** tab and select **Create Virtual Group**. The Create Virtual Group dialog appears.



The dialog box titled "Create Virtual Group" contains the following fields and controls:

- Group Name:** A text input field.
- Description:** A text input field.
- Group Pattern:** A section containing:
  - X509 Subject DN:** A text input field.
  - Use Regular Expression:** A checkbox.
- Email:** A text input field.
- Create** and **Cancel** buttons at the bottom right.

Figure 166: Create Virtual Group dialog

2. Configure the dialog as follows:

Table 128: Federated Virtual Group properties

| Setting                | Description   |
|------------------------|---|
| <b>Group Name</b>      | <p>Enter a name for the group.</p> <p>This name will appear in the <a href="#">Search Identity Provider</a> dialog when searching and/or adding virtual groups to a policy. The name is a human readable value that does not impact the validity of the virtual group in an identity bridging configuration.</p>  |
| <b>Description</b>     | <p>Optionally, enter a description for the group.</p>   |
| <b>X509 Subject DN</b> | <p>Enter the pattern that the subject DN values of signed client certificates must match in order to be authorized as a member of this virtual group. You may use a regular expression.</p> <p>The <b>X509 Subject DN</b> must at least partially match the "Issued to:" value in the CA root certificate attached to the Federated Identity Provider. Use the asterisk truncation operator (*) to retrieve DN's with a common initial spelling. The (*) substitutes a string of zero or more characters in a subject DN.</p> <p>For example, a virtual group could contain the partial DN "O=ACME Inc., OU=Anvils, CN=*" Request messages in which the Subject DN was "O=ACME Inc., OU=Anvils, CN=Name" or "O=ACME Inc., OU=Anvils, CN=Name2" would both pass the corresponding group assertion that is required to gain web service access. However, request messages carrying the Subject DN "O=ACME Inc., CN=Name" would not pass. Every attribute specified in the subject DN pattern of a virtual group must be present in incoming certificates in order to be authorized.</p> <p><b>Special Characters in the Subject DN</b></p> <p>Special care must be taken if the following special characters are used</p> |

| Setting                       | Description   |
|-------------------------------|---|
|                               | <p>in the Subject DN name:</p> <p>, \ # + &lt; &gt; ; " =</p> <p>These characters, plus any leading or trailing spaces must escaped in order to be interpreted correctly.</p> <p>The DN value can be quoted with a quotation pair. This allows all special characters <i>except</i> the backslash to be treated as literal characters and does not require escaping. When quoted, the backslash still require escaping.</p> |
| <b>Use Regular Expression</b> | <p>Select this check box to evaluate the Subject DN as a regular expression. Clear this check box to employ a simple pattern match that uses the "*" character as a wildcard.</p>   |
| <b>Email</b>                  | <p>Optionally, enter an email pattern. This authorizes incoming requests with incoming SAML tokens using the "emailAddress" NameIdentifier format with email addresses matching a regular expression pattern.</p>   |

3. Click **[Create]**. The dialog closes and the virtual group is added to the Federated Identity Provider.

## Group Properties

Every internal group or Federated group has a set of extended properties that can be set either when the group is first added to the system, or deferred until a later date. (During initial entry, only a minimal amount of group data is required, to facilitate rapid entry of many groups.)

Most properties for LDAP groups cannot be modified in the Policy Manager, with the exception being [roles](#).

➤ *To access the properties for a group user:*

1. Do one of the following:
  - Create a new [internal or Federated group](#), making sure to select the **Define Additional Properties** check box.
  - [Edit](#) an existing internal or Federated group.
  - Locate the group by [searching the identity provider](#).

The Group Properties dialog appears.

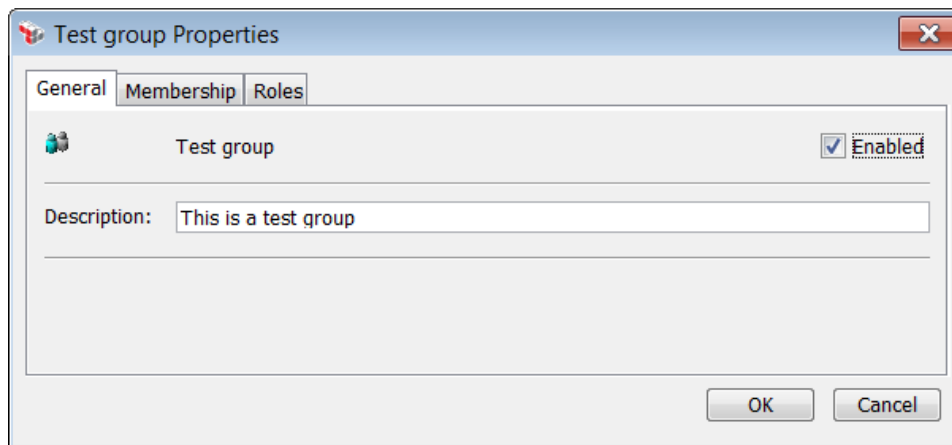
3. Configure each tab within the properties as necessary, wherever possible. All information is optional. Refer to the appropriate section below for a complete



description of each tab.

4. Click **[OK]** when done.

### Configuring the [General] Tab



This tab is used to enter additional basic information about the group.

- **Enabled:** *This applies to internal groups only.* Select this check box to enable the group. Clear this check box to disable the group.

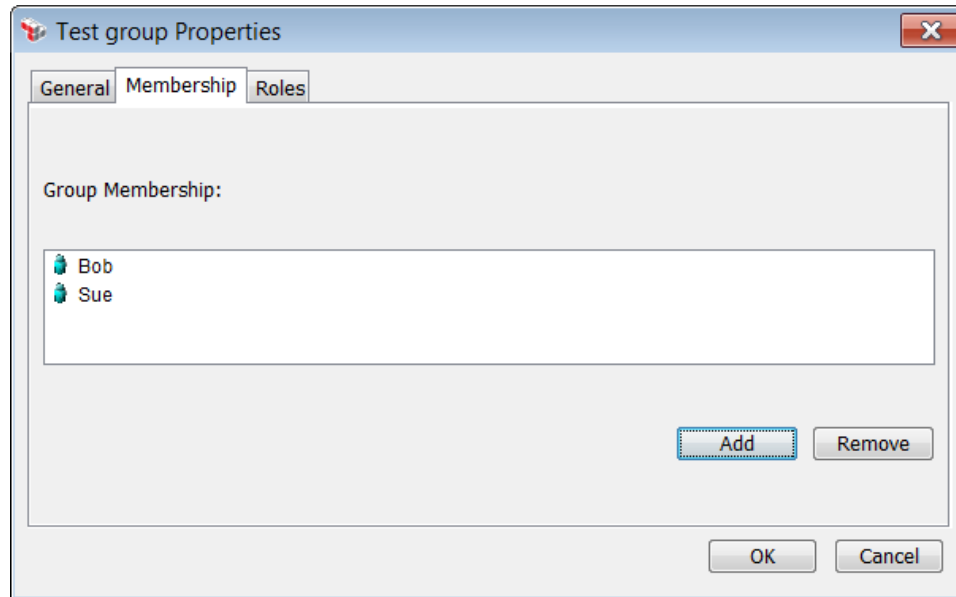
---

**Note:** When a group is disabled, it cannot be used to authenticate message traffic and its permissions are suspended. A user's set of permissions is a combination of his or her role assignments, plus any role assignments inherited from the group. When a group is disabled, the inherited assignments no longer apply. If a user has no other role assignments, then that user will no longer be able to [connect](#) to the Gateway using the Policy Manager.

---

- **Description:** Enter a description of the group.

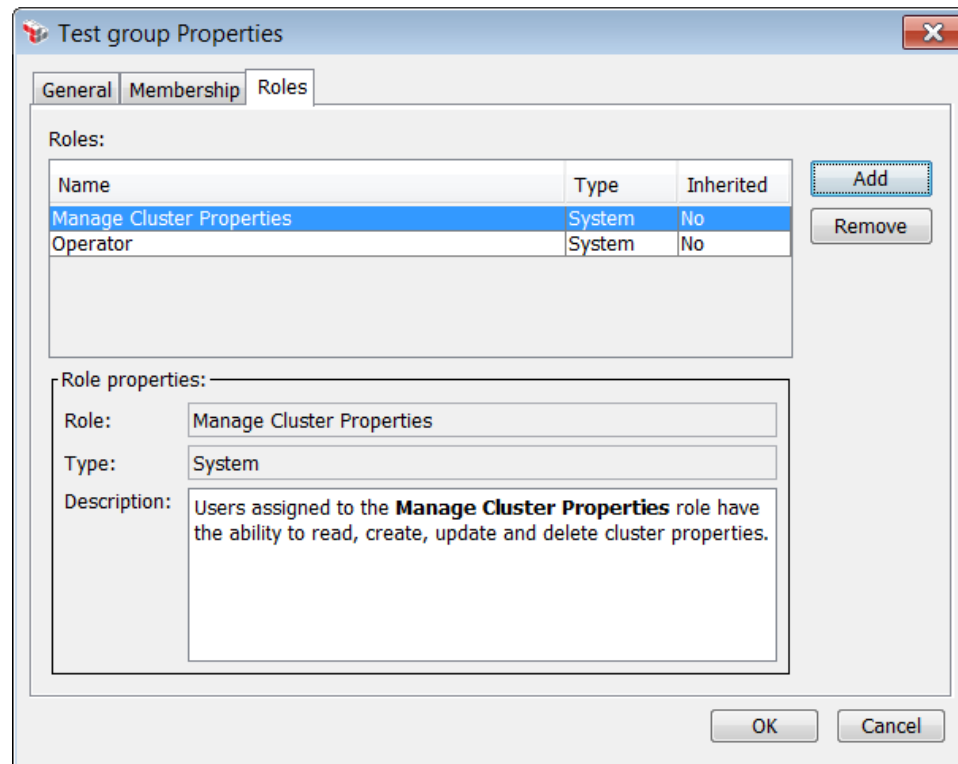
## Configuring the [Membership] Tab



This tab is used to add or remove users to or from the group.

1. Click **[Add]**. A list of eligible users not currently assigned to that group appears.
2. Select one or more users who should be added to the group. Hold down the [Ctrl] key to select multiple users.
3. Click **[Add]**. The user(s) are added to the group.
4. If you need to remove a user from the group, select the user and then click **[Remove]**.

## Configuring the [Roles] Tab



This tab is used to add or remove groups from [roles](#). Roles may be assigned to internal or LDAP groups.

The table at the top lists the roles currently assigned to the group:

- **Name:** The name of the role.
- **Type:** "System" indicates a role that is either predefined or automatically generated (see ""Predefined Roles and Permissions" on page 132"). "Custom" indicates a user-defined role (see ""Managing Roles" on page 130").
- **Inherited:** "No" means the group is assigned to the role directly; "Yes" means the group is part of another group that is assigned to that role .

The Role properties section at the bottom displays the complete description for the selected role.

➤ *To add the group to a role:*

1. Click **[Add]**. A list of eligible roles is displayed.
2. Select the role(s) to which to add the group. **Tip:** To locate a role more easily, enter some text in the "Filter on name" box. This filters the roles list to display only those roles containing the filter text. Delete the filter text to restore the full list of roles.
3. Click **[Add]** to close the dialog.

➤ *To remove a user from a group:*

1. Select the role(s) to be removed from the group. Hold down the [Ctrl] key to select multiple roles. **Note:** You can only remove roles that are *not* inherited.
2. Click **[Remove]**.

---

**Note:** If a role is both assigned and inherited, the interface will display "No" in the "Inherited" column and you are permitted to remove the role. Once removed, that role remains in the list, but the "Inherited" column changes to "Yes".

---

## Editing or Deleting a User or Group

The Policy Manager lets you modify or delete the following:

- Any Internal Identity Provider (IIP) [user or group](#)
- Any Federated Identity Provider (FIP) [user, group, or virtual group](#)

For [LDAP Identity Provider](#) users or groups, you must use the associated external management program to edit or delete. You cannot perform these tasks in the Policy Manager.

---

**Notes:** Be sure the user or group being deleted no longer appears in any policy. At least one administrative Internal Identity Provider user must be present in the Policy Manager.

---

➤ *To edit or delete a user, group, or federated virtual group:*

1. Locate the user or group, as described under "Searching Identity Providers" on page 459.
2. Choose one of the following actions:

Table 129: Editing a User or Group actions

| Action               | Steps   |
|----------------------|---|
| <b>Modify a User</b> | 1. In the Search Results box, double-click the user name or select it |

| Action  | Steps   |
|---|---|
|   | <p>and then click <b>[Select]</b>. The user properties appear.</p> <p>2. Modify the properties as necessary. For more information, see "Internal User Properties" on page 288 or "Federated User Properties" on page 448.</p>   |
| <b>Modify a Group</b>                         | <p>1. In the Search Results box, double-click the group name or select it and then click <b>[Select]</b>. The group properties appear.</p> <p>2. Modify the properties as necessary. For a description of the fields, refer to <a href="#">Creating a Federated Group</a> or <a href="#">Creating an Internal Group</a>, depending on the type of group being edited.</p> |
| <b>Modify a Virtual Group</b>                 | <p>1. In the Search Results box, double-click the federated virtual group name or select it and then click <b>[Select]</b>. The virtual group properties appear.</p> <p>2. Modify the properties as necessary. For a description of the fields, refer to <a href="#">Creating a Federated Virtual Group</a>.</p>  |
| <b>Delete a User, Group, or Virtual Group</b> | <p>1. Select the user, group, or virtual group to delete.</p> <p>2. Click <b>[Delete]</b>, then click <b>[OK]</b> to confirm.</p> <p>You cannot delete a user, group, or virtual group that is still in use in a policy.</p>  |

## Searching Identity Providers

The Policy Manager makes it easy to locate and view information about users and groups defined in the following [identity providers](#):

*Internal Identity Provider*

*LDAP Identity Provider*

*Federated Identity Provider*

---

**Note:** The Simple LDAP Identity Provider is not searchable and will not return meaningful results. The Policy-Backed Identity Provider has a slightly different use case that is described in more detail under "[Working with Policy-Backed Service Providers](#)" below.

---

➤ *To search identity providers:*

- Do any of the following:
  - Click **Search Identity Provider** on the [Home Page](#).
  - Click **[Tasks] > Search Identity Provider** from the [Main Menu](#).
  - Right-click the identity provider to be searched in the [\[Identity Providers\] tab](#) and then select **Search Identity Provider**. The Search Identity Provider dialog appears.

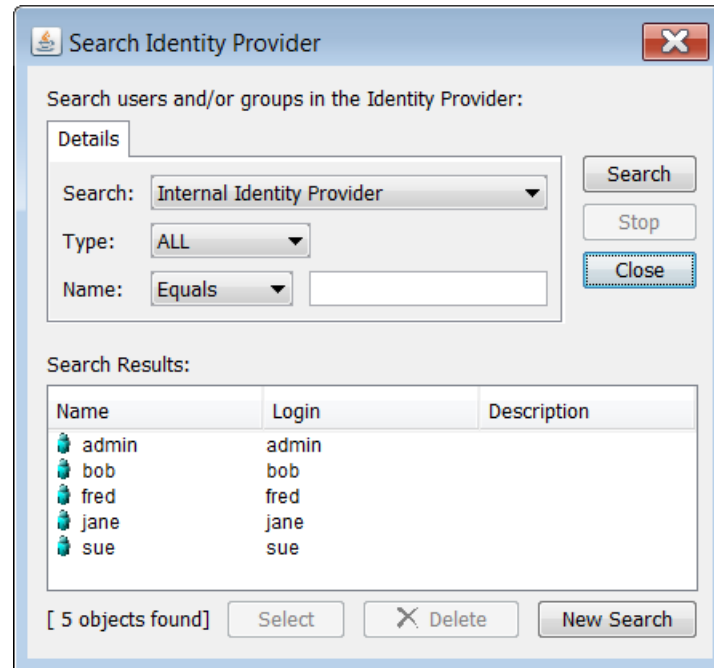




Figure 167: Search Identity Provider dialog, with sample search results

2. Configure the search settings as follows:

Table 130: Search Identity Provider settings

| Setting                           | Description   |
|-----------------------------------|---|
| <b>Search</b><br>(drop-down list) | Choose the <a href="#">identity provider</a> to be searched from the drop-down list. You can only search one identity provider at a time.<br><br><b>Tip:</b> The search behavior for <a href="#">Policy-Backed Identity Providers</a> works a bit differently. See " <a href="#">Working with Policy-Backed Identity Providers</a> " below for details. |
| <b>Type</b>                       | From the drop-down list, choose what you are searching for: <b>Groups</b> , <b>Users</b> , or <b>All</b> .  |
| <b>Name</b>                       | To refine your search, you can optionally specify that the name <b>Equals</b> or <b>Starts with</b> the string of characters that you specify. You can use the asterisk (*) wildcard to match any number of characters, or the question mark (?) to match any single character.   |
| <b>Search</b><br>(button)         | This starts the search. Any names found are displayed in the <b>Search Results</b> box.   |
| <b>Stop</b>                       | This halts the search before it is completed. You may wish to stop the search if the name you are seeking is already displayed or if the search is taking too long.   |
| <b>Close</b>                      | This closes the Search Identity Provider dialog.  |
| <b>New Search</b>                 | This clears the search criteria and search results fields.  |

3. The results appear in the Search Results window. Individual users are indicated by  while groups or **federated virtual groups** are denoted by .

  - To see detailed information about any user or group, double-click the name or click **[Select]** with the appropriate name selected. The properties for that user or group is displayed.
  - To edit or delete non-LDAP users or groups, see "Editing or Deleting a User or Group" on page 458.

---

**Note:** **LDAP Identity Provider** users and groups cannot be changed in the Policy Manager. To modify these users or groups, use the appropriate external management program. The Gateway uses a definition XML file to support IBM® Tivoli® Access Manager (Tivoli) directory searches.

---

## Working with Policy-Backed Identity Providers

A **Policy-Backed Identity Provider** cannot be searched in the conventional sense, because it is not designed to house a set list of users like the Internal Identity Provider. Instead, you can use the Search Identity Provider dialog to assign roles to *template users*. These are users that the Gateway may not "know" about yet, but you can assign roles to these users if and when they are authenticated via a Policy-Backed Identity Provider.

*Example:*

You can configure it such that when user "sally" is authenticated against a Policy-Backed Identity Provider, she will automatically be assigned the role of "Operator". It does not matter that "sally" is not defined in any other identity provider or whether she will access the Gateway at all.

➤ *To configure a role for a template user:*

1. Open the Search Identity Provider dialog.
2. Choose a Policy-Backed Identity Provider from the **Search** drop-down list.
3. Enter **sally** in the "Name" box, leaving all other settings at their default.
4. Click **[Search]**. This creates the template user "sally":

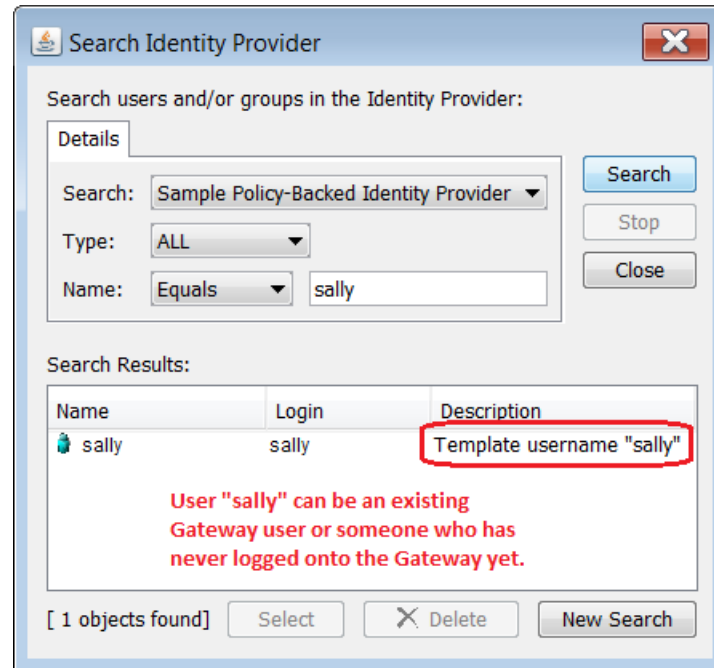


Figure 168: Creating a template user

5. Select "sally" and then click **[Select]**. This opens the properties dialog for "sally".
6. Select the [Roles] tab and then add the role(s) to be assigned to user "sally". For more information about this tab, see "[Configuring the \[Roles\] Tab](#)" under "Internal User Properties" on page 288.

---

**Note:** Any role(s) that you assign here to a template user will override a default role assigned through the "Policy-Backed Identity Provider Wizard" on page 327.

---

## Configuring SAML Policies for Identity Bridging

As part of the required SAML credential source [workflow](#), a Policy Manager policy must be configured for the shared web service with:

- The Require SAML Token Profile assertion
- The federated identities (users, groups, and/or virtual groups) containing credentials shared by the Trusted Authority and Federated Gateway.

Before constructing a policy, ensure that the [Policy Validation Messages window](#) is enabled. This window provides you with policy and assertion-level confirmation, warning, or error messages that you can use during the configuration process.



The Policy Manager's policy development window is the repository for the assertions used to develop a policy for a [published web service](#). Most assertions require configuration either before or after being added to the policy development window. After adding the Require SAML Token Profile assertion and federated users, groups, and/or virtual groups to the policy, configure additional policy assertions for the web service as outlined in Policy Assertions Overview and Configuring a Policy, both found in the *Layer 7 Policy Authoring User Manual*. CA Technologies

➤ *To configure a SAML policy for identity bridging:*

1. Add Require SAML Token Profile assertion to a policy.
2. Configure the SAML Token Profile Wizard as follows:

Table 131: Configuring the SAML Token Profile Wizard for identity

| Wizard Step                           | Description   |
|---------------------------------------|---|
| <b>Step 2: SAML Version</b>           | Specify which SAML versions will be accepted by the Gateway: version 1.x, version 2.x, or any supported version.  |
| <b>Step 3: SAML Statement Type</b>    | Select the <b>Authentication Statement</b> option.  |
| <b>Step 4: Authentication Methods</b> | <ol style="list-style-type: none"> <li>1. Select at least one check box that corresponds to a SAML-specified authentication method that must be enforced by the Require SAML Token Profile assertion.</li> <li>2. Click <b>All</b> to select all of the supported authentication methods or <b>None</b> to clear all the check boxes. Select the <b>Unspecified</b> check box to allow authentication by an unspecified method. This page only allows selection of methods applicable to the SAML version chosen in Step 2 of the wizard.</li> </ol> <p><b>Note:</b> The "SSL/TLS Certificate Based Client Authentication" method is not related to the Require SSL or TLS Transport assertion in the Policy Manager. This method refers to the original authentication, not to the current request which may or may not have used SSL. The SAML-supported authentication methods are outlined in the SAML 1.x and 2.0 specification documents provided at <a href="http://www.oasis-open.org">http://www.oasis-open.org</a>.</p> <p>Proceed to Step 7: Subject Confirmation.</p> |
| <b>Step 7: Subject Confirmation</b>   | <p>Select one or both of the following subject confirmation methods:</p> <p><b>Holder-of-Key</b></p> <p>Select the <b>Holder-of-Key</b> check box to allow SAML tokens that use the Holder-of-Key subject confirmation method (with the standard URI <code>urn:oasis:names:tc:SAML:1.0:cm:holder-of-key</code> or <code>urn:oasis:names:tc:SAML:2.0:cm:holder-of-key</code>, depending on the selected SAML version in Step 2 of the wizard). For such assertions, the Gateway will require that the subject demonstrate possession of</p>  |

| Wizard Step | Description   |
|-------------|---|
|             | <p>the private key corresponding to the public key in the Subject certificate.</p> <p>The Holder-of-Key subject confirmation method currently requires that the request ticket's "SubjectConfirmation" element contain a "KeyInfo" element that contains a complete copy of the Subject's X.509 certificate. Any other type of Holder-of-Key ticket will be rejected by the Gateway.</p> <p>The request Subject may use one of two methods to prove that they hold this key:</p> <ul style="list-style-type: none"> <li>• The request includes at least one element covered by a valid WSS message signature, and the signing certificate is the Subject certificate. Or,</li> <li>• The request arrived over SSL/TLS with client certificate authentication, and the client certificate exactly matches the Subject certificate.</li> </ul> <p>When the Holder-of-Key subject confirmation method is selected, you can optionally select the <b>Require Message Signature</b> check box to require proof-of-possession using a WSS message signature. If the <b>Require Message Signature</b> check box is not selected, then the policy must contain the Require SSL or TLS Transport assertion.</p> <p><b>Sender Vouches</b></p> <p>Select the <b>Sender Vouches</b> check box to allow SAML tokens that use the Sender Vouches subject confirmation method (with the standard URI <code>urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</code> or <code>urn:oasis:names:tc:SAML:2.0:cm:sender-vouches</code>, depending on the selected SAML version in Step 2 of the wizard). For such assertions, the Gateway will require that the sender, presumably different from the subject, vouches for the verification of the subject.</p> <p>The Sender Vouches subject confirmation method is typically used only in a SAML <a href="#">identity bridging</a> policy.</p> <p>Three conditions must be met in order to use the Sender Vouches confirmation method:</p> <ul style="list-style-type: none"> <li>• An existing trust relationship with the sender ("Attesting Entity") must be configured in the Gateway. To do this, import the sender's certificate, configured as a "SAML Attesting Entity" certificate, into the Trust Store. For more information, see "Adding a New Certificate" on page 239.</li> <li>• The SAML ticket used by the SAML Assertion must be bound to the request message by one of the following methods: <ul style="list-style-type: none"> <li>• Send the request over SSL using the sender certificate as the SSL client certificate, or</li> <li>• If SSL is not used, then the SAML ticket needs to be bound to the message with a WSS signature. One complication here is that the SAML ticket does not</li> </ul> </li> </ul> |

| Wizard Step                    | Description   |
|--------------------------------|---|
|                                | <p>necessarily contain or refer to the sender certificate; it usually contains or refers to the subject certificate and, assuming that the ticket is signed, contains or refers to the certificate of the ticket issuer. In this method, therefore, the WSS signature must cover both the SAML token and the relevant portions of the rest of the message that use the sender certificate as the signing certificate.</p> <ul style="list-style-type: none"> <li>The format of the request message must conform to the OASIS Web Services Security standards: SAML Token Profile 1.0 (for SAML 1.x) or SAML Token Profile 1.1 (for SAML 2.x). The Gateway does not support references to SAML tokens that are not included with the request message.</li> </ul> <p>The OASIS Web Services Security: SAML Token Profile 1.0 standards document is available online at: <a href="http://www.oasis-open.org/committees/download.php/1048/WSS-SAML-06.pdf">www.oasis-open.org/committees/download.php/1048/WSS-SAML-06.pdf</a>.</p> <p>You can optionally select the <b>Require Message Signature</b> check box to require proof-of-possession using an SSL client certificate. If this check box is not selected, then the policy must contain the Require SSL or TLS Transport assertion.</p> |
| <b>Step 8: Name Identifier</b> | <ul style="list-style-type: none"> <li>If incoming messages must contain a particular NameQualifier value, enter the value into the <b>Name Qualifier</b> field (for example, "www.example.com").</li> <li>Select the <b>X.509 Subject Name</b>, <b>Email Address</b>, and/or <b>Windows Qualified Domain Name</b> check boxes. If configuring one or more virtual groups for the Federated Identity Provider, you must select the <b>X.509 Subject Name</b> option.</li> </ul>   |

- Complete the remainder of the wizard as outlined in SAML Token Profile Wizard.
- Add one of these assertions to the policy: Authenticate User or Group or Authenticate Against Identity Provider.
- In the [Search Identity Provider](#) dialog that appears, add the shared federated user configured in [Workflow Using SAML](#) to the policy as follows:

Table 132: Adding a shared federated user

| Field         | Description  |
|---------------|--|
| <b>Search</b> | Select the Federated Identity Provider name from the drop-down list.   |
| <b>Type</b>   | Select the "Users" search target from the <b>Type</b> drop-down list.  |
| <b>Name</b>   | If necessary, specify any search criteria using the <b>Name</b> drop-down list and field. You can use the asterisk (*) wildcard to match any number of characters, or the question mark (?) to match any single character. |

6. Click **[Search]**. The search results are displayed.
7. In the Search Results window, select the target federated user either by double-clicking the name, or selecting it and clicking **[Select]**.
8. Repeat to add additional federated users, groups, and/or virtual groups as required.

---

**Note:** A policy with more than one Authenticate User or Group or Authenticate Against Identity Provider assertions must organize the identities into "At least one assertion must evaluate to true" assertion folders. To quickly add one of these folders to the policy development window, right-click anywhere within the window and select **Add 'At least one...' Folder** from the context menu. Drag and drop federated users, groups, and/or virtual groups into the individual folders as required.

---

9. Configure additional policy assertions for the web service. When completed, click **[Save]** in the [Policy Tool Bar](#). Note any error or warning messages in the Policy Validation Messages window. If necessary, correct policy errors as outlined in *Validating a Policy* in the *Layer 7 Policy Authoring User Manual*.

Proceed to configure the required Gateway Accounts in the Securespan XML VPN Client. For more information, see *Configuring Gateway Accounts* in the Securespan XML VPN Client documentation.

## Using the Securespan XML VPN Client for Identity Bridging

In an [identity bridging](#) configuration, the Securespan XML VPN Client can be used to delegate authentication to the Trusted Authority, while preserving authorization for the Federated Gateway hosting the web service.

The Securespan XML VPN Client interfaces with the requestor's SAML or X.509 certificate authorization source that validates an authentication. Once the Securespan XML VPN Client receives the authentication assertion or token, it embeds this evidence and then signs the SOAP message. The Federated Gateway then uses this evidence to securely authorize access to the protected web service.

## Chapter 8: Tutorials

The following tutorials offer a basic introduction to the CA API Gateway. You can use the tutorials either with your installed Gateway or with the trial Gateway virtual appliance. If using the trial virtual appliance, please ensure that it has been configured as described in the *SecureSpan XML Virtual Appliance Getting Started*.

For assistance with any of the tutorials, please contact [CA Technical Support](#).

## Tutorial #1: How to Configure Your System to Work with the Demo Environment

**Note:** Configuring your system is necessary only if you are using your own Gateway to access the demo environment. It is not required if you are using the sample Gateway hosted by CA Technologies.

If you intend to use the *Layer 7 SecureSpan Demonstration Environment* (SDE) to learn about the Gateway features, it is recommended that you modify your local hosts file to map the IP address to the SDE image. This will allow the Gateway to find the SDE by various system names.

While it is possible to evaluate the CA API Gateway using only IP addresses, it is helpful to map host names for certificate validation and ease of use (all tutorials assume that the host names have been mapped).

### Prerequisite:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- Access to the *SecureSpan Demonstration Environment* (SDE), which is hosted by CA Technologies. For more information about the SDE, please contact CA Technical Support.

### Step 1: Locate the hosts file

The location of the hosts file varies depending on your operating system. Table 133 describes the locations for the various operating systems. Please contact your system administrator if you require assistance locating the file.

Table 133: Location of Hosts file

| Operating System                       | Location   |
|--|--|
| Windows (NT, 2000, XP, 2003, Vista, 7) | <p>Default location:</p> <p><b>%SystemRoot%\system32\drivers\etc\hosts</b></p> <p>Actual location is defined by this registry key:</p> <p><b>\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DataBasePath</b></p> |
| Mac OS X                               | <b>/private/etc/hosts</b>  |
| Linux, Solaris, etc.                   | <b>/etc/hosts</b>  |

## Step 2: Edit the hosts file

1. Open the hosts file in a text editor. To access this file from the Gateway, do the following:
  - a. Access the main menu for your installed CA API Gateway. This is the menu that appears when you log in as *ssgconfig*.
  - b. Select option **3** (Use a privileged shell (root)) to access the Linux command line.
  - c. Enter the password for *ssgconfig*. The default password is **7layer**. (**Tip:** This may have been changed to **L7Secure\$0@** if you were following a previous tutorial.)
  - d. Access the hosts file as listed under "Linux, Solaris, etc." in Table 133.
2. Verify that the first line after the "localhost" entry defines the IP address of the CA API Gateway you are using (see Figure 169).
3. Add the following lines after the name of your Gateway:

```

10.7.2.28      sde.l7tech.com    sde
10.7.2.28      services.l7tech.com    services
10.7.2.28      ldap.l7tech.com      ldap
10.7.2.28      curl.l7tech.com      curl
10.7.2.28      ocsp.l7tech.com      ocsp
10.7.2.28      jms.l7tech.com       jms
10.7.2.28      mail.l7tech.com      mail
10.7.2.28      ftp.l7tech.com       ftp
10.7.2.28      syslog.l7tech.com    syslog
10.7.2.28      snmp.l7tech.com      snmp

```

Be sure to update the hosts file on both the Gateway and in the host operating system (if running the Virtual Environment).

Your hosts file should look similar to the following after editing (image is from the hosts file in Windows):

```

hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#
#       127.0.0.1         localhost
#       ::1               localhost
75.1.2.33 myssg.company.com myssg
10.7.2.28 sde.17tech.com sde
10.7.2.28 services.17tech.com services
10.7.2.28 ldap.17tech.com ldap
10.7.2.28 crl.17tech.com crl
10.7.2.28 ocsp.17tech.com ocsp
10.7.2.28 jms.17tech.com jms
10.7.2.28 mail.17tech.com mail
10.7.2.28 ftp.17tech.com ftp
10.7.2.28 syslog.17tech.com syslog
10.7.2.28 snmp.17tech.com snmp
  
```

Figure 169: Sample hosts file in Windows

## Next Steps

In this exercise, you learned how to configure your system to work with the Layer 7 demo environment. Next, you can try creating a simple test service and accessing it directly to receive an expected response. To learn how to do this, please refer to the tutorial [How to Access the Test Service Using soapUI](#).



## Tutorial #2: How to Access a Test Service Using soapUI

This tutorial is designed for first time CA API Gateway users, especially for those evaluating the Gateway using the Virtual Appliance. It describes how you can access an unprotected service directly using soapUI and view the expected response.

### Prerequisites:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- Access to the *Layer 7 SecureSpan Demonstration Environment* (SDE) is desirable, but not mandatory. For more information about the SDE, please contact CA Technical Support.
- If using the SDE, your hosts file has been correctly configured. For more information, see the tutorial [How to Configure Your System to Work with the Demo Environment](#).
- The soapUI application has been installed. You can download this at no cost from [www.soapui.org](http://www.soapui.org).

### Step 1: Load WSDL in soapUI

1. Start soapUI and close the "soapUI Starter Page" when it appears.

Under the File menu, select **New soapUI Project**. The New soapUI Project dialog appears.

2. For the **Project Name**, type **ACME Warehouse**.
3. For the **Initial WSDL/WADL**, enter the following URL:

**`http://services.l7tech.com:6060/ACMEWarehouse/services/WarehouseSoap?wsdl`**

**Tip:** If you are not using the demo environment, click **[Browse]** and navigate to a WSDL document to use.

Leave all other settings are their default.

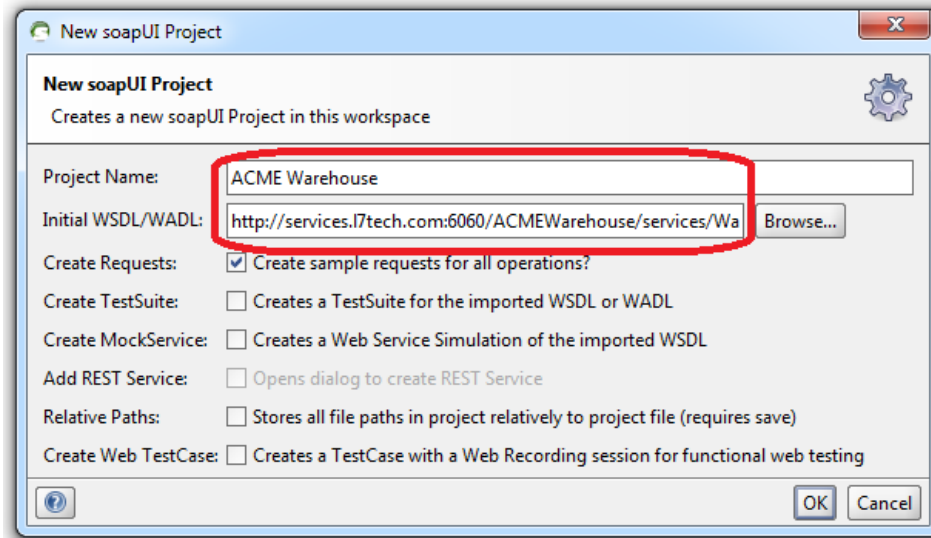


Figure 170: New soapUI Project with sample ACME Warehouse

4. Click **[OK]**. The new project appears in the left pane:

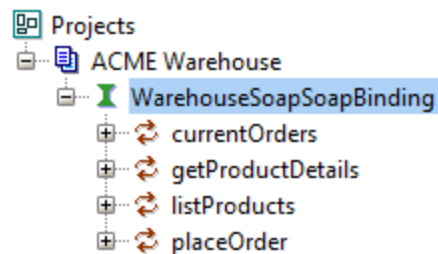


Figure 171: Sample ACME Warehouse project

## Step 2: Send a request and view the response

1. Expand the "listProducts" branch and then double-click **Request1** to bring up the request window.

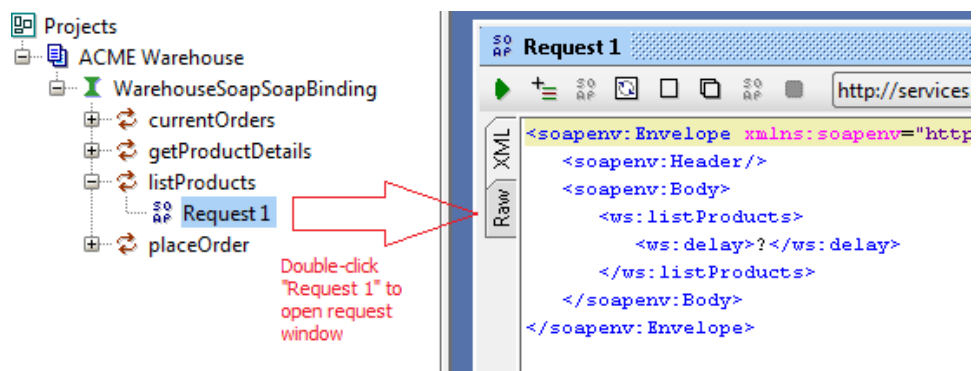



Figure 172: Opening the Request window

- The automatically generated request message uses '?' characters as placeholders for actual values. In the request message, replace the ? character with **1** and then click the  button. This sends the request to the service URL listed by **3** and the "expected response" will be returned in the right pane of the window. **Tip:** When you see the "expected response", it indicates a successfully routed request (Figure 174).

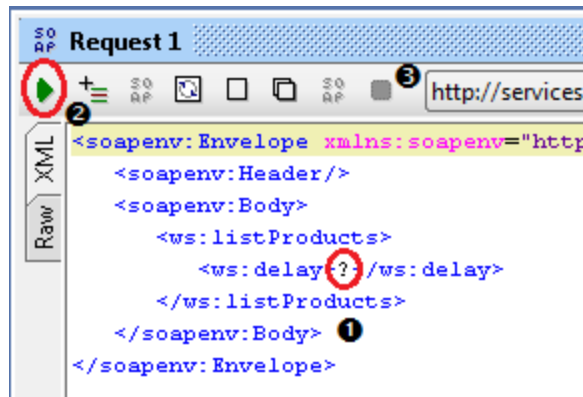


Figure 173: Sending a request

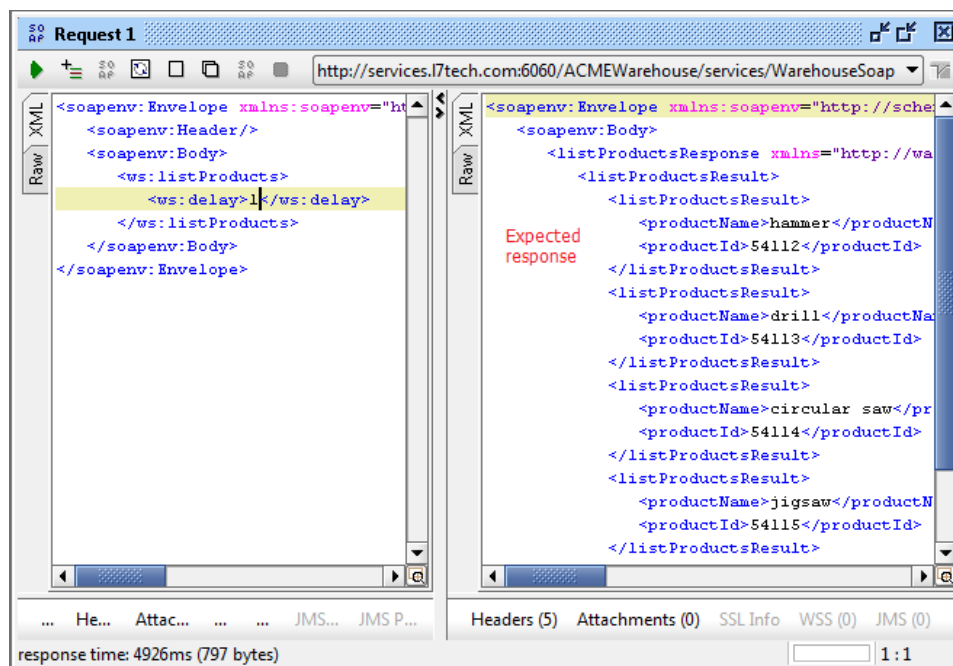


Figure 174: Receiving the expected response

- You may exit soapUI when done, or leave it open if you are proceeding the next tutorial.

## **Next Steps**

In this exercise, you learned how to access a raw, unprotected service, using soapUI as the back end service. Next, you can try publishing a service's WSDL on your CA API Gateway and then route a message through it. To learn how to do this, please refer to the tutorial [How to Access a Test Service via the Gateway](#).

## Tutorial #3: How to Access a Test Service via the Gateway

This tutorial describes how to publish and configure a sample service to the CA API Gateway. You will finish by sending a test message through the Gateway.

### Prerequisites:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- Access to the *Layer 7 SecureSpan Demonstration Environment* (SDE) is desirable, but not mandatory. For more information about the SDE, please contact CA Technical Support.
- If using the SDE, your hosts file has been correctly configured. For more information, see the tutorial [How to Configure Your System to Work with the Demo Environment](#).
- Policy Manager desktop client has been installed, or you have a compatible browser to run the Policy Manager browser client.

For information on installing the desktop client, see Chapter 7 in the *Layer 7 Installation and Maintenance Manual*.

- soapUI is installed.
- Completing the prior exercise in the tutorial [How to Access the Test Service Using soapUI](#) is recommended.

### Step 1: Publish and configure the service

1. Start the Policy Manager. For more information on how to do this, see "Starting the Policy Manager" in the *Layer 7 Policy Manager User Manual*.
2. When the Policy Manager interface appears, familiarize yourself with the three main regions shown in Figure 175
  - **Assertions Palette:** An expandable tree containing the policy assertions, which are the building blocks for constructing a service policy. Each assertion performs a function and will return either "true" or "false" (with the exception of the Add Comment to Policy assertion). An assertion may also set variables (known as "[context variables](#)") and may alter the message. When constructing a policy, it is import to consider the impact of the policy logic caused by the assertions.

- **Home Page:** This starting page lists the common tasks that you can perform. The complete list of tasks is accessed from the **Tasks** menu (desktop client) or **Manage** menu (browser client).
- **Services Window:** This window lists the services, policies, and fragments that are published on the Gateway. Each service has one master policy, which in turn may contain multiple policy fragments. Additionally, each SOAP-based service is represented by a single WSDL document.

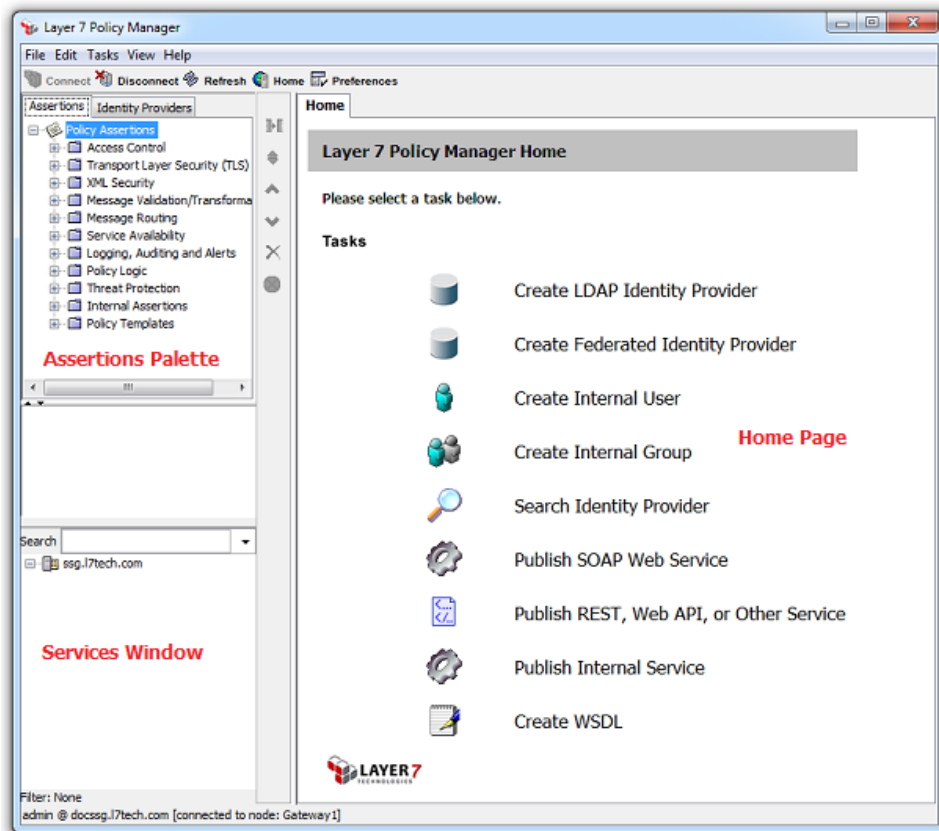


Figure 175: The Policy Manager main interface

3. When exposing a Web service on the CA API Gateway, the first step is to load the service's WSDL as a new SOAP Web service. This process is known as "*publishing the service*". To do this, simply click **Publish SOAP Web Service** from the Home Page (Figure 175), or select it from the menu. This starts the Publish SOAP Web Service Wizard.
4. Enter the following URL for the sample ACME Warehouse service's WSDL:

**`http://services.l7tech.com:6060/ACMEWarehouse/services/WarehouseSoap?wsdl`**

**Tip:** If you are not using the demo environment, click **[File]** and navigate to a WSDL document to use.

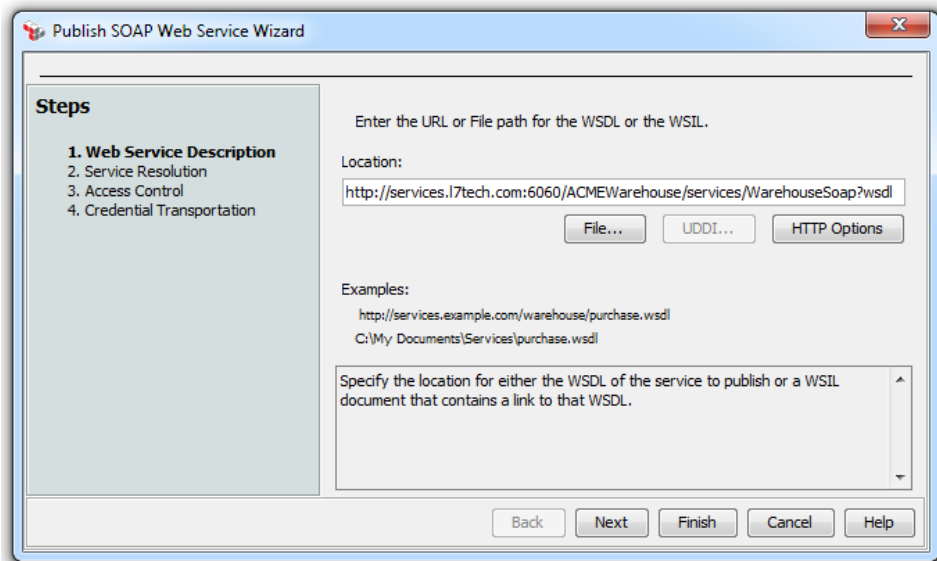


Figure 176: Publish SOAP Web Service Wizard - step 1

5. Click **[Next]**. The wizard may take a moment to resolve the target. When this is done, the wizard advances to step 2 (Service Resolution).
6. By default, the resolution path is `/ssg/soap`, which means the Gateway will try to determine the correct service to use for each request. This process is known as *service resolution* and the mechanism is described in detail in the *Layer 7 Installation and Maintenance Manual*. For this tutorial, we will use a custom resolution path.
  - Select **Custom resolution path** and then type `/Warehouse` in the adjacent box.

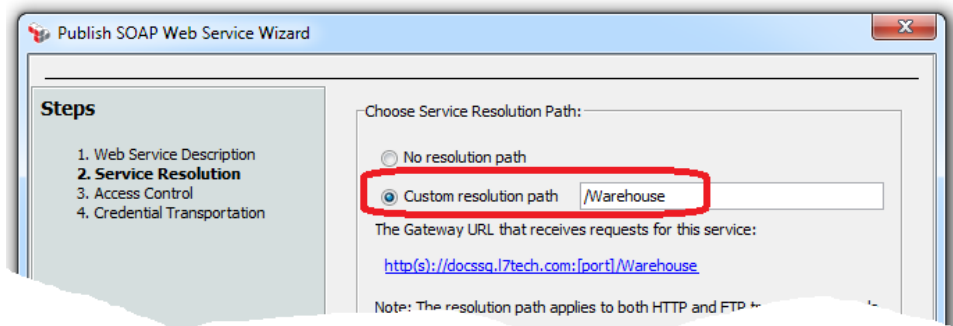


Figure 177: Publish SOAP Web Service Wizard - step 2

7. We will leave all other settings in the wizard at the default settings, so click **[Finish]** to close the wizard. Your new service appears in the **Services** window in the lower left and the Home Page is replaced with the **Policy Editor** and **Policy Validation** windows. The new policy automatically contains a single Route via HTTP(S) assertion with the default binding address defined in the WSDL.

**Tip:** Every policy should have a routing assertion. This defines "what happens to the message policy if the policy succeeds". Typically, a Route via HTTP(S) assertion is used, but it can be any assertion from the Message Routing category. For more information, see "Chapter 8: Message Routing Assertions" in the *Layer 7 Policy Authoring User Manual*.

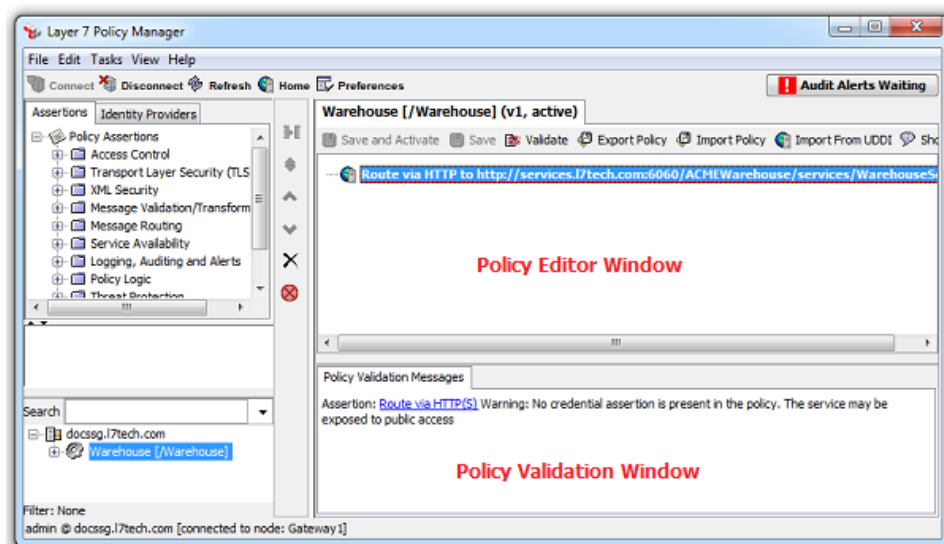


Figure 178: Newly published SOAP Web service

**Tip:** Although no explicit security is being added to this simple sample policy, all CA API Gateways are automatically protected against the following threats:

**TCP/IP Based Attacks**

*Coercive Parsing and XML Bomb*

*External Entity Attack*

*External Entity Attack*

*Schema Poisoning*

*WSDL Scanning*

*XML Routing Detours*

For more information, see *Automatic Threat Protection* in the *Layer 7 Policy Authoring User Manual*.



## Step 2: Send a test message through the CA API Gateway

1. Open soapUI, if it was closed after the last exercise. The ACME Warehouse project should open automatically.
2. The first step is to add a new endpoint instructing soapUI to send the request message to your Gateway:
  - a. If the request window is not visible, expand the "listProducts" branch and then double-click **Request1**.
  - b. Click the destination field and select **[add new endpoint]** from the drop-down list.

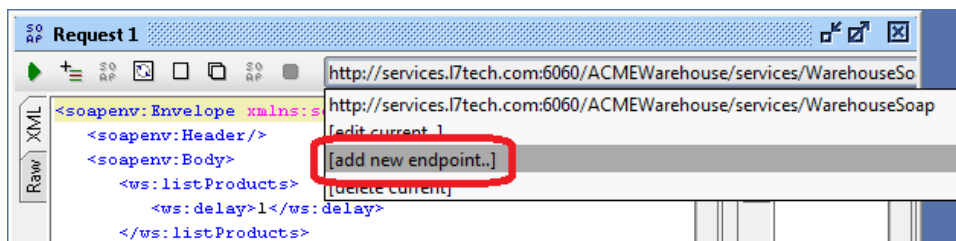


Figure 179: Adding a new endpoint in soapUI

- c. The **Add new endpoint** dialog is displayed. Enter this endpoint address:

**http://<gatewayHost>:8080/Warehouse**

where "<gatewayHost>" is the fully qualified domain name of your host Gateway (for example, "ssg.l7tech.com").

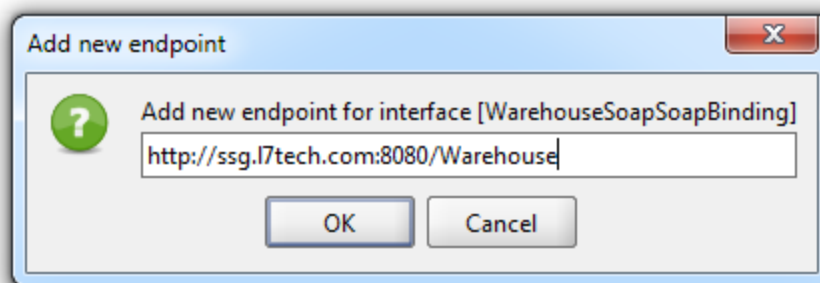



Figure 180: Add new endpoint dialog

- d. Click **[OK]** to close the dialog and then
3. Click  in the request window. The "expected response" should load in the response pane.

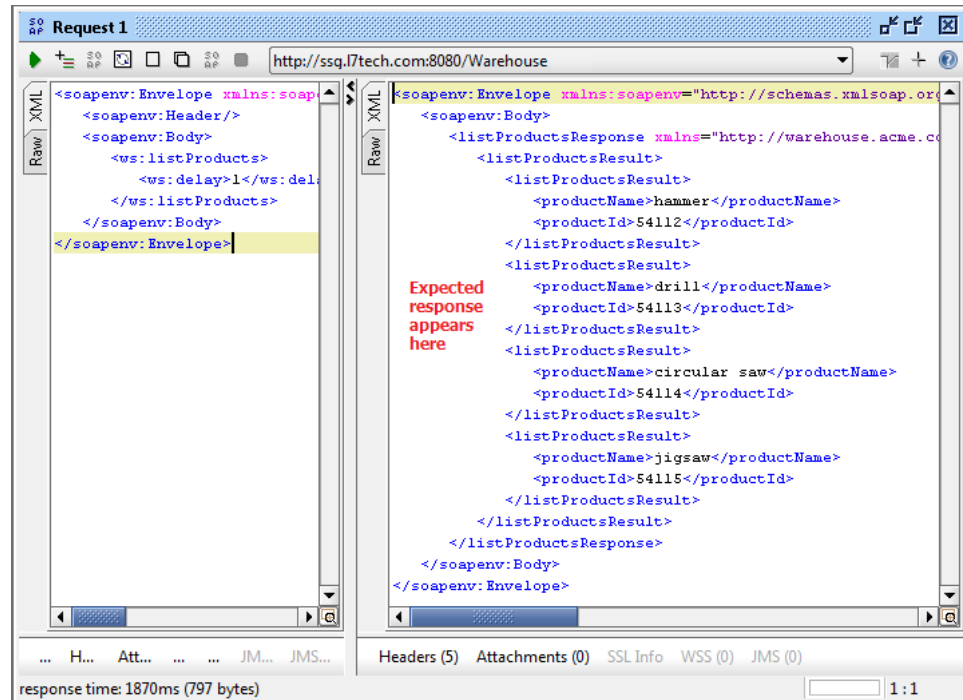


Figure 181: Expected response after routing request through Gateway

## Next Steps

In this exercise, you learned how to publish a service's WSDL on the CA API Gateway, how to assign it a custom path for the service, and how to route a message through the policy to the back end service.

Next, you will learn more about the internal identity provider and how to configure an external LDAP identity provider. To learn how to do this, please refer to the tutorial [How to Manage Identity Providers](#).

## Tutorial #4: How to Manage Identity Providers

This tutorial will explore the Internal Identity Provider and teach you how to configure your Gateway to use an LDAP Identity Provider for identity-based functionality.

### Prerequisites:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- The Policy Manager desktop client has been installed, or you have a compatible browser to run the Policy Manager browser client.

For information on installing the desktop client, see Chapter 7 in the *Layer 7 Installation and Maintenance Manual*.

- Access to the *Layer 7 SecureSpan Demonstration Environment* (SDE) is desirable, but not mandatory. For more information about the SDE, please contact CA Technical Support.
- Completing the prior exercise in the tutorial [How to Access the Test Service via the Gateway](#) is recommended.

### Using the Internal Identity Provider

All CA API Gateways have an identity provider built in to the database, referred to as the **Internal Identity Provider** (IIP). The IIP is a convenient location to store test identities and other identities that are not managed in separate identity stores.

### Adding a New User to the IIP

1. In the Policy Manager, click the [Identity Providers] tab to reveal the Internal Identity Provider.

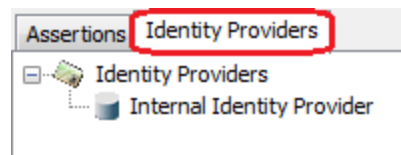


Figure 182: The [Identity Providers] tab

2. Right-click **Internal Identity Provider** and then select **Create User**.

---

**Tip:** You can also use [Tasks] > **Create New User** or click **Create Internal User** from the Home page to create a user.

---

The Create Internal User dialog appears.

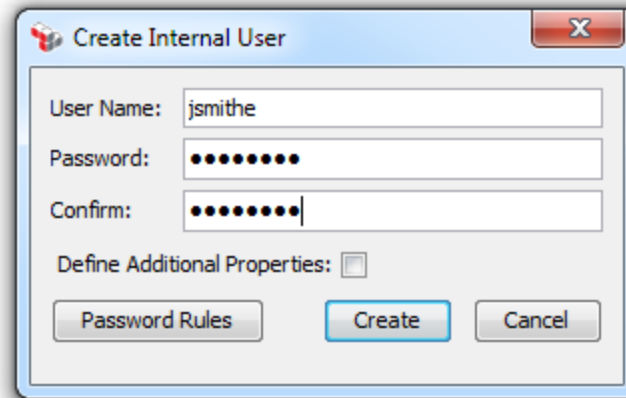


Figure 183: Create Internal User dialog

3. Enter a **User Name** and **Password** for your new user. Note that the password must meet the minimum rules described by the **[Password Rules]** button.
4. If you want to add additional information about the user right now, select the **Define Additional Information** check box. This will allow you to enter properties such as the user's name, email address, account expiry, group membership, and certificate. **Tip:** You can enter the additional properties later if you choose to not enter them now.
5. Click **[Create]** to add the user to the IIP. If you are defining additional information, the properties dialog for the user is displayed. Complete each tab as necessary; all information is optional. To learn more about the user properties, see [Creating an Internal User](#) in the *Layer 7 Policy Manager User Manual*.

## Creating a New Group in the IIP

1. Right-click **Internal Identity Provider** in the [Identity Providers] tab and then select **Create Group**.

---

**Tip:** You can also use **[Tasks] > Create New Group** or click **Create Internal Group** from the Home page to create a group.

---

The Create Internal Group dialog appears.

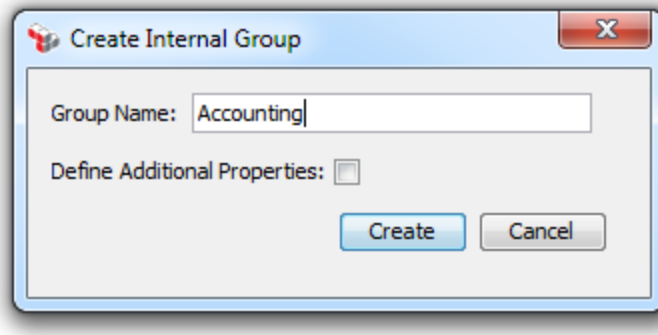


Figure 184: Create Internal Group dialog

2. Enter name for the group and optionally select the check box if you are ready to assign members to the group or if you wish to enter a group description. These can be entered later if necessary.
3. Click [**Create**] to add the group to the IIP. If you are defining additional information, the properties dialog for the group is displayed. Complete each tab as necessary; all information is optional. To learn more about the group properties, see [Creating an Internal Group](#) in the *Layer 7 Policy Manager User Manual*.

## Querying the IIP

1. Right-click **Internal Identity Provider** in the [Identity Providers] tab and then select **Search Identity Provider**. This displays the Search Identity Provider dialog. Spend a moment to review this dialog as it is used to search all identity providers configured on the CA API Gateway.

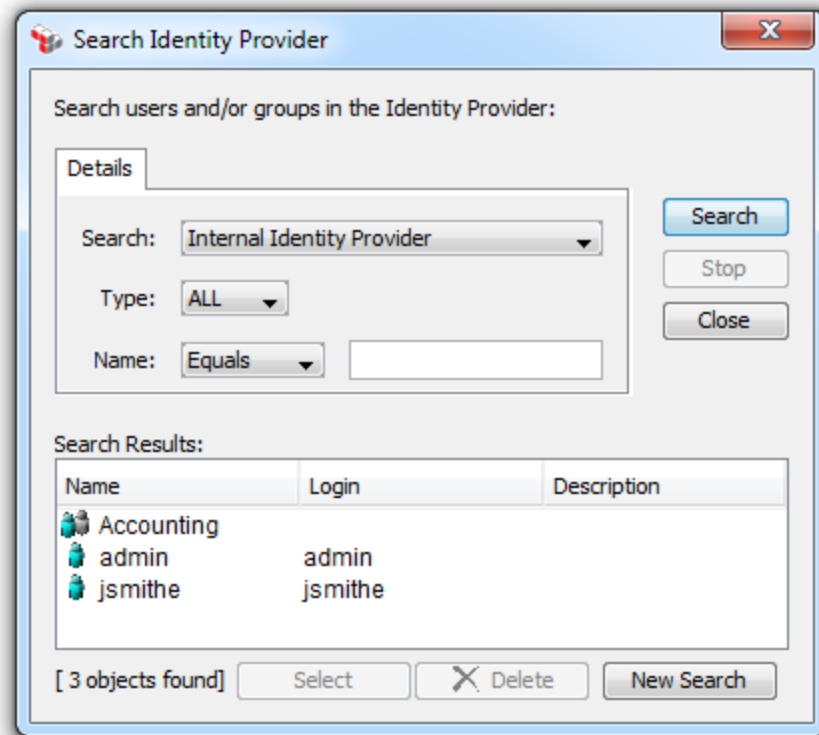


Figure 185: Search Identity Provider dialog

2. Ensure that **Internal Identity Provider** is selected for the **Search** drop-down.
3. Leave all other fields at the default settings and then click [**Search**]. This will perform a global search and return the entire contents of the IIP.
4. Select the user or group you want in the **Search Results** and then click [**Select**] to view or edit the properties.

---

**Tip:** The [**Select**] button has a dual purpose: if you are simply querying an identity provider, clicking [**Select**] after locating your user or group will display the properties for that user or group. However if you are searching for someone to authenticate (i.e., this dialog appears as a result of dragging the Authenticate User or Group assertion into a policy), clicking [**Select**] will select that user/group for authentication and close the dialog.

---

## Authenticating a Message Against the IIP

Message authentication is a two step process: First, the credentials are acquired using one of the "Require ... Credentials" assertions, then the credentials are authenticated against an identity provider.

Make sure a service policy is open (double-click the Warehouse service if it isn't).

Drag the Require HTTP Basic Credentials assertion into the policy (before the routing assertion) to enforce credential gathering using HTTP Basic Authentication.

There are several possible methods for authenticating credentials:

- **To authenticate any user in the IIP:** Drag the Authenticate Against Identity Provider assertion into the policy and select **Internal Identity Provider** from the list.



Figure 186: Authenticating any user in the IIP

- **To authenticate a specific user or group in the IIP:** Drag the Authenticate User or Group assertion into the policy. In the Search Identity Provider dialog that appears, locate the user or group to authenticate from the Internal Identity Provider.



Figure 187: Authenticating a specific user in the IIP

- **To authenticate several users or groups in the IIP:** Insert several Authenticate User or Group assertions within a At Least One Assertion Must Evaluate to True folder.

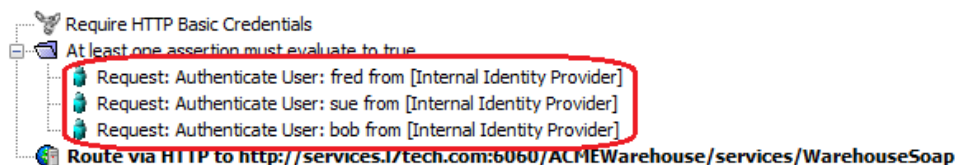


Figure 188: Authenticating multiple users in the IIP

## Configuring an LDAP Connection

Lightweight Directory Access Protocol (LDAP) directories are a very common mechanism for storing identity information. Examples of LDAP-based directories include Microsoft Active Directory, Tivoli Directory Server, Oracle Internet Directory, Novell eDirectory, openLDAP and many others. If you have access to the Layer 7 Demo Environment, there is a preconfigured openLDAP directory can be used in this exercise. You can also use your own LDAP directory if you wish, or simply read along to learn.

1. In the Policy Manager, select the [Identity Providers] tab (see Figure 182).
2. Right-click **Identity Providers** and then select **Create LDAP Identity Provider**. The Create LDAP Identity Provider Wizard starts.

---

**Tip:** You can also use [Tasks] > **Create Identity Provider** > **Create LDAP Identity Provider** or click **Create LDAP Identity Provider** from the Home page to create a new identity provider.

---

3. Select the **Provider Type** that matches your LDAP directory. If you do not see yours listed or if you are using the LDAP in the Demo Environment, select **GenericLDAP**.

Once the Provider Type is selected, complete the remaining fields in Step 1 with the settings in Table 134 if you are using the LDAP in the Demo Environment. (If you are using your own LDAP directory, refer to [LDAP Identity Provider Wizard](#) in the *Layer 7 Policy Manager User Manual* for a description of each setting.)

*Table 134: LDAP Provider Configuration for Demo Environment*

| Setting                                  | Enter this value                       |
|--|--|
| Provider Name                            | L7 Demo LDAP                           |
| LDAP Host URL                            | ldap://ldap.l7tech.com                 |
| [Use Client Certificate Authentication]  | not selected                           |
| Search Base                              | dc=l7tech, dc=com                      |
| Bind DN                                  | leave blank to permit anonymous access |
| Bind Password                            | leave blank to permit anonymous access |
| Allow assignment to administrative roles | not selected                           |



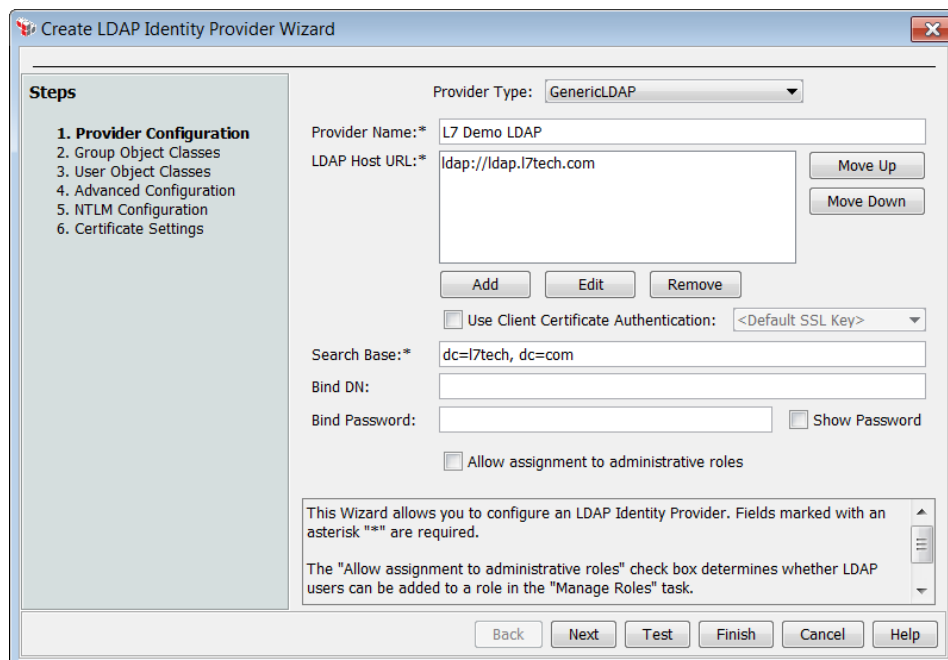


Figure 189: Create LDAP Identity Provider Wizard - Step 1

4. Click **[Test]** to confirm connectivity with the LDAP directory. If everything resolves correctly, you should see the following message:

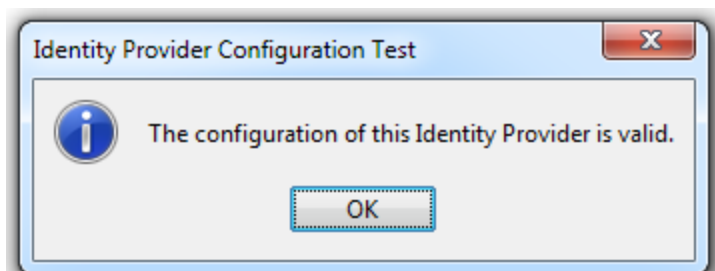


Figure 190: LDAP test success

5. Click **[Next]** to proceed to Step 2 - Group Object Classes. You should not need to change anything here unless you have group object class definitions in the LDAP.
6. Click **[Next]** to proceed to Step 3 - User Object Classes. You should not need to change anything here unless you have user object class definitions in the LDAP.

7. Click **[Next]** to proceed to Step 4 - Advanced Configuration. Here you can define how attributes are retrieved by the CA API Gateway. By default, only the attributes mapped in the previous page are retrieved. If you need to retrieve other attributes for authentication (for example), you can retrieve all attributes (which will impact performance) or configure only specific attributes.

For this exercise, you will add the **clearance** and **entitlement** attributes to the list:

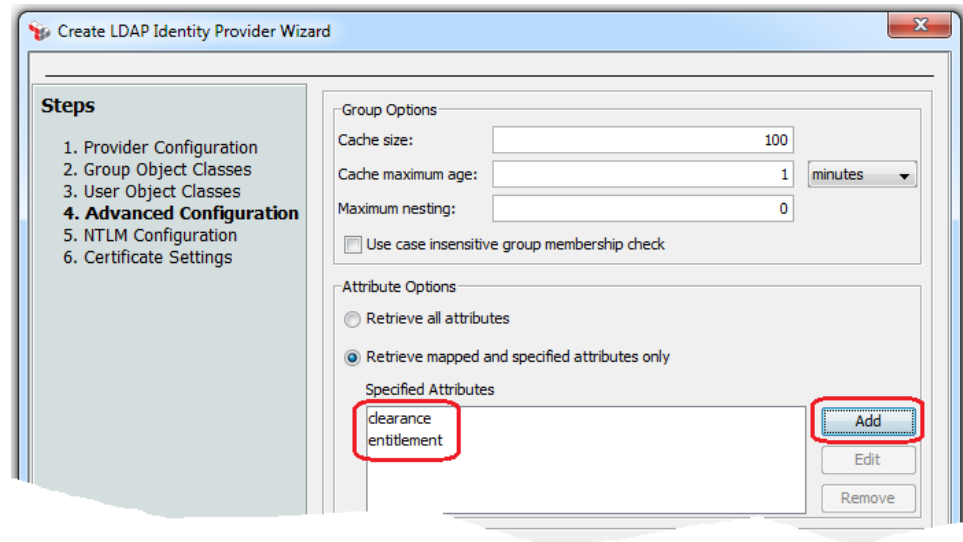


Figure 191: Create LDAP Identity Provider Wizard - Step 4

8. Click **[Next]** to proceed to Step 5 - NTLM Configuration. You should not need to change anything here unless you require NTLM configuration in the LDAP
9. Click **[Next]** to proceed to Step 6 - Certificate Settings. Here you can define how X.509 certificates in the LDAP directory are used and validated. For this exercise, leave all settings at the default and then click **[Finish]**. This closes the wizard and adds your new LDAP identity provider to the list of configured identity providers:

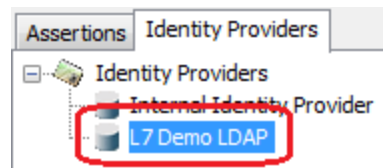


Figure 192: New LDAP identity provider added to the Policy Manager

Now that the LDAP connection is defined, you can search the LDAP directory in the same way as the Internal Identity Provider described above.

## Next Steps

In this exercise, you learned how to add and search users and groups in the Internal Identity Provider built into the CA API Gateway database. You also learned how to configure a connection to an external LDAP directory.

Next, you can try adding basic security for the service by using SSL and HTTP Basic Authentication. To learn how to do this, please refer to the tutorial [How to Add SSL and HTTP Basic Authentication](#).

## Tutorial #5: How to Add SSL and HTTP Basic Authentication

This tutorial will teach you how to add security constraints to require that the message be sent over an encrypted channel using SSL and that the username and password are provided using the HTTP Basic Authentication mechanism.

### Prerequisites:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- Access to the *Layer 7 SecureSpan Demonstration Environment* (SDE) is desirable, but not mandatory. For more information about the SDE, please contact CA Technical Support.
- If using the SDE, your hosts file has been correctly configured. For more information, see the tutorial [How to Configure Your System to Work with the Demo Environment](#).
- The Policy Manager desktop client has been installed, or you have a compatible browser to run the Policy Manager browser client.

For information on installing the desktop client, see Chapter 7 in the *Layer 7 Installation and Maintenance Manual*.

- soapUI is installed.
- Completing the prior exercise in the tutorial [How to Manage Identity Providers](#) is recommended.


### Step 1: Add SSL constraint and send a test message

Adding assertions to a policy is a simple drag-and-drop process.

1. Start the Policy Manager if it is not already running and ensure the Warehouse service is active (double-click on "Warehouse [/Warehouse]" in the Services window).

For details, see "Starting the Policy Manager" in the *Layer 7 Policy Manager User Manual*.

2. When the Policy Manager interface appears, expand the **Transport Layer Security (TLS)** category in the **Assertions** palette (Figure 193), and then drag the Require SSL or TLS Transport assertion into the policy, placing it above the routing assertion (Figure 194).

**Tip:** If the assertion ends up after the routing assertion, simply click  to move it back up.

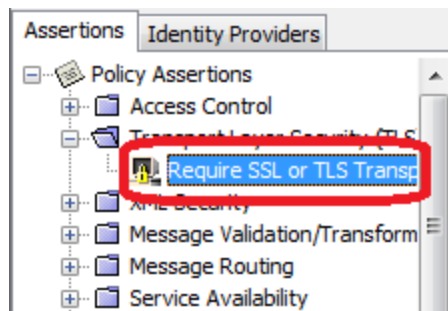


Figure 193: Accessing the Require SSL or TLS Transport assertion

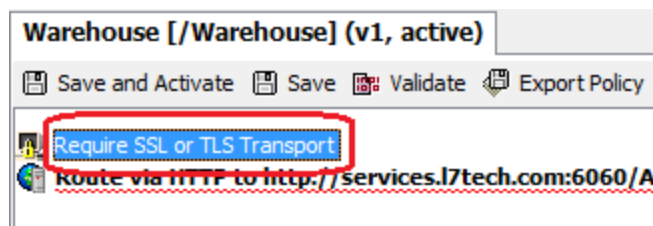




Figure 194: Positioning the Require SSL or TLS Transport assertion in the policy

3. Click  **Save and Activate**. This saves the policy, makes it active, and then deploys it to the CA API Gateway.
4. Open soapUI, if it was closed after the last exercise. Verify that:
  - The ACME Warehouse project is open.
  - The Request window is visible (ACME Warehouse > listProducts > double-click Request1).
  - The endpoint URL shows **http://<gatewayHost>:8080/Warehouse** (where "<gatewayHost>" is the fully qualified domain name of your Gateway, for example: *ssg.l7tech.com*)
5. Click  to send the message to **http://<gatewayHost>:8080/Warehouse**. The response message should be a SOAP Fault message, indicating that your policy does not comply with the SSL constraint (as dictated by the *Require SSL or TLS* assertion).

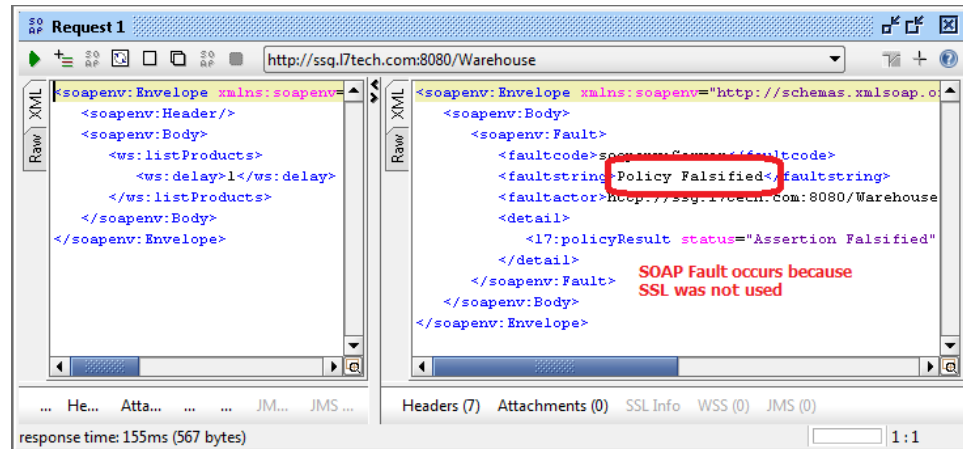


Figure 195: SOAP Fault caused by missing SSL in message

6. To configure soapUI to send the message using SSL:
  - a. Click the endpoint drop-down and then select **[add new endpoint]**. The *Add new endpoint* dialog appears.
  - b. Enter **https://<gatewayHost>:8443/Warehouse** (where "<gatewayHost>" is the fully qualified domain name of your Gateway, e.g., *ssg.l7tech.com*) and then click **[OK]**.

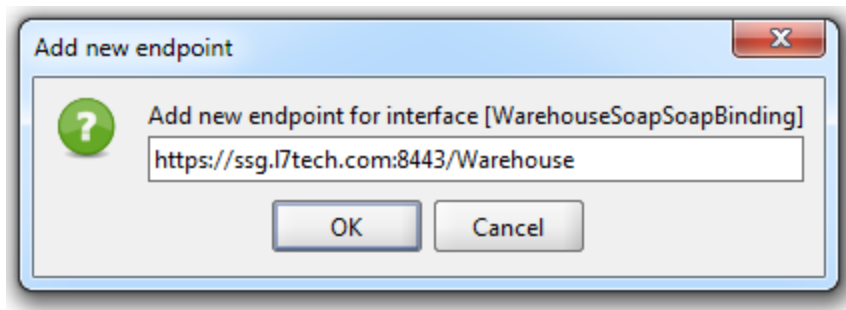


Figure 196: Creating an HTTPS endpoint in soapUI


**Tip:** By default, the CA API Gateway enables these three ports ("listeners") for receiving messages:

**8080:** for non-SSL messages

**8443:** for SSL messages with Client certificate challenge

**9443:** for SSL messages with no Client certificate challenge

To learn how to enable new listen ports or modify the existing ones, use the [Manage Listen Ports](#) task.

7. Click  again. The "expected response" should appear now that the SSL constraint from the *Require SSL or TLS* assertion is satisfied.

## Step 2: Add HTTP Basic Authentication

1. In the Policy Manager, expand the **Access Control** category from the **Assertions** palette and drag the *Require HTTP Basic Credentials* assertion into the policy, placing it immediately below the *Require SSL or TLS Transport* assertion.

---

**Tip:** To learn more about the various mechanisms used to authenticate an identity, see *Authentication in a Policy* in the *Layer 7 Policy Authoring User Manual*.

---

2. Also from the Access Control category, drag the *Authenticate User or Group* assertion into the policy, placing it immediately below the *Require HTTP Basic Credentials* assertion. This triggers the Search Identity Provider dialog, which you will use to select the users/groups to be authenticated.
3. If you are using the demo environment, change the **Search** list to **L7 Demo LDAP**, otherwise leave it at **Internal Identity Provider**.
  - a. Click [**Search**] to view a list of users in the **Search Results** box.
  - b. Click on the user you wish to authenticate (for example, "sarek") and then click [**Select**]. This closes the dialog and adds your authenticated user in the policy.

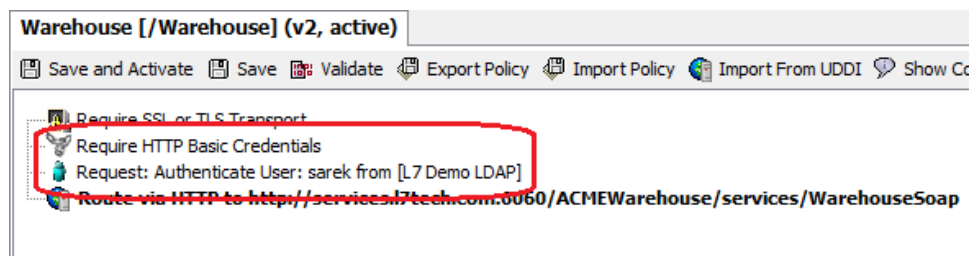





Figure 197: Policy updated with HTTP Basic Authentication

4. Click  **Save and Activate** to deploy the new policy to the Gateway.
5. In soapUI, click  in the request window. You should now see "Authentication Required" in the response pane.

---

**Note:** When most assertions fail at the root level of policy, the response is usually a SOAP Fault. However, the *Require HTTP Basic Credentials* assertion is a special case whereby if credentials are required but missing, it will return a challenge for the credentials.

---

6. In soapUI, there is a **Request Properties** pane (Figure 198) in the lower left corner where you can enter the **Username** and **Password** to authenticate the user (for example, **sarek/7layer**). When this is done, click  again and you should get the "expected response" once again. (Figure 199)

**Tip:** If you do not see the Request Properties pane in Figure 198, ensure that "Request 1" is selected under ACME Warehouse in the upper left pane.

| Request Properties |                       |
|--------------------|-----------------------|
| Property           | Value                 |
| Name               | Request 1             |
| Description        |                       |
| Message Size       | 275                   |
| Encoding           | UTF-8                 |
| Endpoint           | https://docssg.l7t... |
| Timeout            |                       |
| Bind Address       |                       |
| Follow Redirects   | true                  |
| Username           | sarek                 |
| Password           | *****                 |
| Domain             |                       |

Figure 198: Entering credentials of authenticated user in soapUI

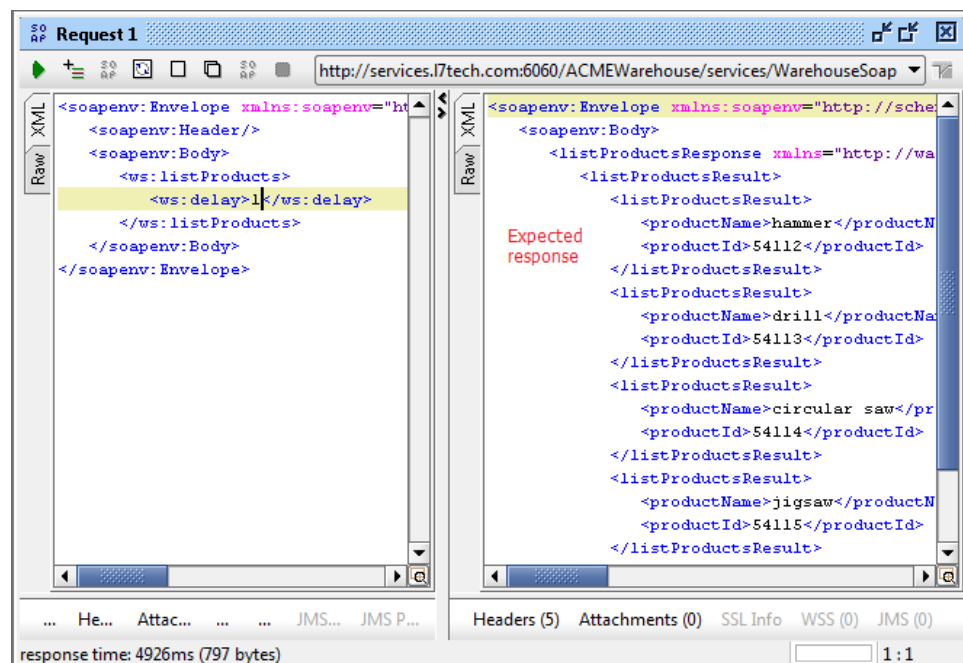


Figure 199: The expected response is displayed after credentials are entered



## Introduction to the SecureSpan Policy Language

The SecureSpan Policy language is read from top to bottom, like a book. Each assertion in a policy can be thought of as a function that will return true or false, depending upon the content of the message and other factors. In addition, an assertion may alter the request message and/or set "[context variables](#)". If an assertion returns false at the "root level" of the policy, the policy will typically return a SOAP Fault, unless precluding standards (such as HTTP Basic Authentication) dictate otherwise. To learn more, see *SOAP Faults* in the *Layer 7 Policy Authoring User Manual*.

This approach allows for a high degree of flexibility in creating policy. It is important to become familiar with the policy language in order to implement specific requirements. Many of the tutorials from CA Technologies focus on writing policies to accomplish requirements for specific use cases.

## Next Steps

In this exercise, you learned how to add security constraints to an unprotected web service by creating a policy that requires the message to be sent over an encrypted channel. You also learned how to provide a username and password that are then authenticated against an [LDAP identity provider](#).

Next, you can explore the SecureSpan Policy Language in more detail. To learn how to do this, please refer to the tutorial [How to Use the SecureSpan Policy Language](#).

## Tutorial #6: How to Use the SecureSpan Policy Language

This tutorial will teach you the fundamentals of the SecureSpan Policy Language.

### Prerequisites:

- A CA API Gateway has been installed and configured (you may use the Virtual Appliance supplied in the trial download from CA Technologies).
- The Policy Manager desktop client has been installed, or you have a compatible browser to run the Policy Manager browser client.

For information on installing the desktop client, see Chapter 7 in the *Layer 7 Installation and Maintenance Manual*.

- Completing the prior exercise in the tutorial [How to Add SSL and HTTP Basic Authentication](#) is recommended.

### Basic Concepts

The SecureSpan Policy language is a deterministic language made up of *policy assertions* as its building blocks. Each of these blocks can return either true or false after being evaluated; they may set [context variables](#), transform the message in some way, or may act upon an external system (such as an HTTP target, message queue, database, etc). There are two basic types of assertions:

- **Constraint assertions:** These assertions apply constraints to a policy, such as requiring a message to be sent over SSL, requiring a specific type of credentials, requiring elements to be signed or encrypted, etc.
- **Action assertions:** These assertions perform actions, such as authenticating credentials, transforming messages, turning on auditing and routing messages, etc.

---

**Tip:** A few assertions fit into both categories, like the Evaluate Request XPath assertion, which requires the content to be defined in the message (by XPath) and may set a context variable based upon that content.

---

Consider the following simple policy:

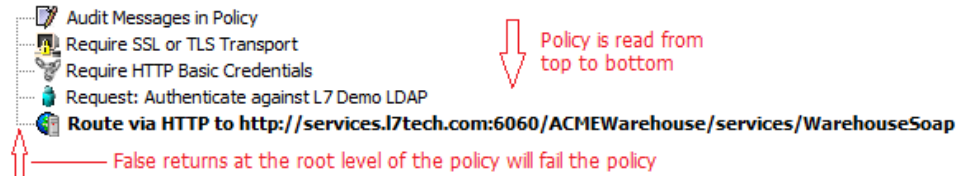


Figure 200: Simple policy example

Each assertion in this policy is evaluated from top to bottom. The *root level* of the policy is indicated by the line along the left-most edge of the policy. In most cases, an assertion that returns "false" at the root level of the policy will cause the policy to fail, resulting in a SOAP Fault. The sample policy in Figure 200 will perform the following actions in this order:

1. Audit Messages in Policy forces an audit record to be created every time this policy is executed. This assertion always returns "true".
2. Require SSL or TLS Transport enforces that the request was sent over SSL. If it was not, a SOAP Fault occurs and the assertion returns "false".
3. Require HTTP Basic Credentials ensures that username and password are presented in the HTTP header. If not, an *HTTP 401 Authentication Required* response will be sent and the assertion will return "false".
4. Request: Authenticate against *<identity provider>* validates the credentials gathered by the previous *Require HTTP Basic Credentials* assertions against the specified identity provider (in this case, the "L7 Demo LDAP" identity provider). Failure to authenticate the credentials will result in an "Authentication Failure" SOAP Fault and the assertion will return "false".
5. Route via HTTP to *<URL>* sends the request message to the URL over HTTP. Failure to route the message will result in a SOAP Fault and the assertion will return false.

## Editing a Policy

The Assertions palette contains the following expandable categories:

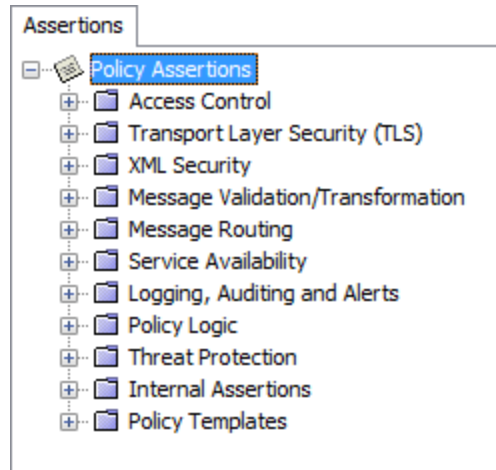






Figure 201: Assertions palette in the Policy Manager


You can add an assertion to a policy by doing either of the following:

- Drag the assertion you want and drop it into the policy editing window.
- Click once on the assertion you want and then click  to add it to the policy editing window.

If an assertion requires some input from you, it will automatically open a properties dialog.

In either case, the assertion will be added below the assertion highlighted in the policy editing window. If this is not where you want it, you can move the assertion by using  or  or by dragging and dropping.

You can temporarily disable an assertion by either selecting it and then clicking , or by right-clicking the assertion and selecting **Disable Assertion**. Disable an assertion when you need to retain its settings or if you intent to reactivate it later.

You can delete an assertion by either selecting it and then clicking , or by right-clicking the assertion and selecting **Delete Assertion**. Delete an assertion when you no longer need it or if you added it in error.

---

**Tip:** You can disable or delete several assertions as once by holding down the [Shift] or [Ctrl] keys while selecting them.

---

You can also duplicate assertions within a policy by selecting them and pressing [Ctrl]-**C** to copy, then selecting the assertion immediately before where you want to paste, and then pressing [Ctrl]-**V**. You may replace the [Ctrl] key commands by right-clicking and selecting **Copy** or **Paste** if you wish.

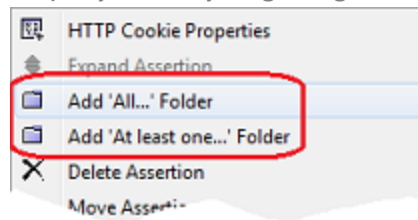
For assertions that have configurable parameters, you can access the properties dialog by double-clicking the assertion or by right-clicking and selecting the "<assertion> **Properties**" option from the context menu. (If no such option exists, then there are no configurable parameters for that assertion.)

## Policy Branching

A very powerful concept in the SecureSpan Policy Language is *policy branching*. This is accomplished by using the two special "folder" assertions within the Policy Logic category. These folder assertions return "true" or "false" depending on their child assertions:

- "At least one assertion must evaluate to true": Each child assertion within this folder is evaluated until one returns "true". At this point, processing of the child assertions stop and the "At least one..." folder assertion returns "true". If all the child assertions return "false", then the folder assertion returns "false".
- "All assertions must evaluate to true": Each child assertion within this folder is evaluated until one returns "false". At this point, processing of the child assertions stop and the "All assertions..." folder assertion returns "false". If all the child assertions return "true", then the folder assertion returns "true".

**Tip:** These assertions are used so frequently that you can access them from any assertion in the policy window by using the right-click context menu:



Consider the following policy example:

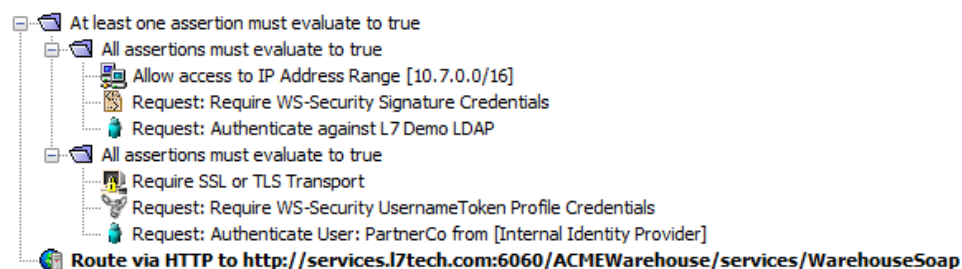


Figure 202: Folder assertions policy example

In plain English, this is what the policy in Figure 202 is designed to do:

*Access to the ACME Warehouse Service is available to internal users (i.e., those who are calling from an IP address in recognized IP space) who present credentials per the WS-Security Signature standard and successfully authenticate against the "L7 Demo LDAP" identity provider. Additionally there is a single external user, PartnerCo, who also has rights to access the service but must submit the request over SSL and send WS-Security UsernameToken Profile credentials that authenticate to an identity in the Internal Identity Provider.*

This policy example sets up the two possible cases as two "All..." folders nested within a single "At least one..." folder.

- If all of the child assertions in the first "All..." folder succeed, then the conditions of that folder are met, which in turn satisfies the "At least one..." folder's requirement and the message will be routed *without* evaluating the second "All..." folder.
- If any assertion within the first "All..." folder fails, then the first "All..." folder fails and the second folder will then be evaluated. Similarly, if any child assertion in the second "All..." folder returns false, then that folder will also fail. With both folders failing, the parent "At least one..." folder at the root level will also fail and a SOAP Fault will be returned without the routing assertion being run.

## Hints and Tips

- Many assertions, such as the Audit Messages in Policy, Send Email Alert, etc, will always return "true", so you should keep this in mind when writing policy logic. Only the Add Comment to Policy assertion has no impact on the policy (i.e., returns neither "true" nor "false").
- When writing complex policy, be sure to carefully walk through the policy and evaluate the conditions all the way back to the root level of the policy. There is no equivalent to a "break" statement, so policy must be fully evaluated.
- You can use the Continue Processing (which always returns "true") and Stop Processing (which always returns "false") assertions to negate the results of the "At least one..." and "All..." folders if required.
- Always organize policies with security as the first concern, then performance.
- For better performance, try to arrange the assertions so that the most "common" situations are evaluated first. For example, in the policy fragment in Figure 202, the most common access will be from internal users, not the external PartnerCo, so the internal user scenario appears first.

For more information on policy organization, see Policy Organization in the *Layer 7 Policy Authoring User Manual*.

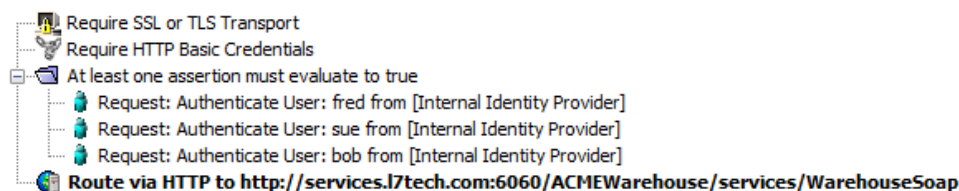
## Exercises

To reinforce what you've learned, construct policy fragments for each of the following scenarios:

### #1: Multiple User Authentication

Create a policy that will gather credentials using HTTP Basic over SSL and authenticate any three specific users in the Internal Identity Provider before routing to the ACME Warehouse service.

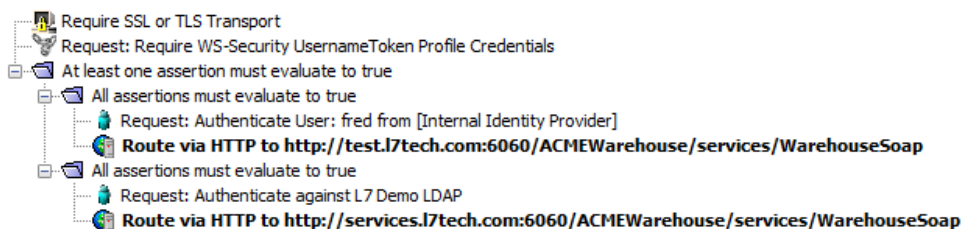
#### Solution:



### #2: Identity-Based Routing

Create a policy that gathers credentials using WS UsernameToken Profile over SSL and routes to a test service at *http://test.l7tech.com:6060/ACMEWarehouse/services/WarehouseSoap* if the user is 'fred' in the Internal Identity Provider, otherwise the policy confirms that the user is in the LDAP and routes the message to the default service.

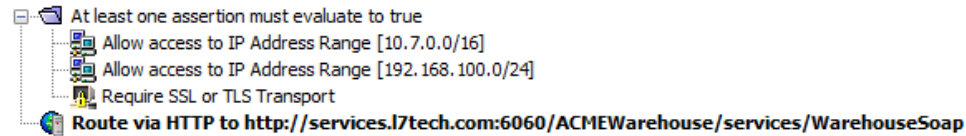
#### Solution:



### #3: Trusted Networks "In the Clear"

Create an anonymous policy that requires traffic from untrusted networks to be sent over SSL. Define two trusted networks as 10.7.0.0/16 and 192.168.100.0/24 before routing to the default service.

### Solution:



**Tip:** The "Allow access..." lines are from the Restrict Access to IP Address Range assertion.

## Client vs. Server View of Policy

When discussing policy, especially with client application developers, it is important to understand that there are two different views of a policy:

- **Server View:** This is the policy as displayed in the Policy Manager and is the policy to which the CA API Gateway has access. In other words, *the Server View of the policy is the full policy itself.*
- **Client View:** This is a subset of the Server View *that a requesting client will need to know in order to craft a message that can satisfy the full policy*—for example, what credential mechanisms are required, whether SSL is required, what elements need to be encrypted and/or signed, etc. The requesting client will never see the full policy.

## Next Steps

In this exercise, you learned the fundamentals of the SecureSpan Policy Language. You should now have a reasonable understanding of how to write basic policies and be able to further explore the flexibility of the SecureSpan Policy Language.

Please contact CA Technical Support for the availability of more advanced tutorials. In the meanwhile, you are ready to explore the power and flexibility the Policy Manager. Consult the Policy Manager online help to continue your learning or read the user manuals:

*Layer 7 Policy Manager User Manual*

*Layer 7 Policy Authoring User Manual*



## Chapter 9: Solution Kits

This chapter describes the various Solution Kits that you can optionally license to extend the functionality of the CA API Gateway.

For more information on obtaining a Solution Kit, please contact [CA Technical Support](#).

### Salesforce Integration Solution Kit

The Sales Integration Solution Kit is an optional add-on that allows the CA API Gateway to configure connections to Salesforce.com<sup>®</sup> and execute Salesforce operations.

For information on obtaining this Solution Kit, please [contact](#) CA Technologies.

### Managing Salesforce Operation Service Connections

The *Manage Salesforce Operation Service Connections* task in the Policy Manager is used to create, edit, remove, or test connections to Salesforce.com. These connections are used in the Execute Salesforce Operation assertion.

➤ To manage Salesforce connections:

1. In the Policy Manager, select **[Tasks] > Additional Actions > Manage Salesforce Operation Service Connections** from the [Main Menu](#) (on the [browser client](#), from the **Manage** menu). The Manage Salesforce Operation Service Connections dialog appears.

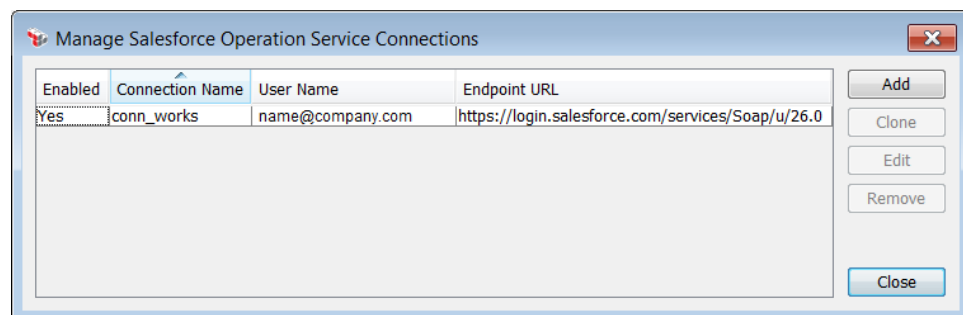


Figure 203: Manage Salesforce Operation Service Connections dialog

2. The Salesforce connections that have been configured are displayed. Choose an action to perform:

Table 135: Managing Salesforce connections tasks

| To...   | Do this...   |
|---|--|
| <b>Create a new Salesforce connection</b>                                 | <ol style="list-style-type: none"> <li>1. Click <b>[Add]</b>. The <a href="#">Salesforce Connection Properties</a> are displayed.</li> <li>2. Complete the properties for the connection.</li> </ol>                                   |
| <b>Create a new Salesforce connection based on an existing connection</b> | <ol style="list-style-type: none"> <li>1. Select the connection to copy.</li> <li>2. Click <b>[Clone]</b>. The <a href="#">Salesforce Connection Properties</a> are displayed.</li> <li>3. Edit the properties as required.</li> </ol> |
| <b>Edit a Salesforce connection</b>                                       | <ol style="list-style-type: none"> <li>1. Select the connection to edit.</li> <li>2. Click <b>[Edit]</b>. The <a href="#">Salesforce Connection Properties</a> are displayed.</li> <li>3. Edit the properties as required.</li> </ol>  |
| <b>Remove a Salesforce connection</b>                                     | <ol style="list-style-type: none"> <li>1. Select the connection to remove.</li> <li>2. Click <b>[Remove]</b>. The Salesforce connection is removed from the list.</li> </ol>   |

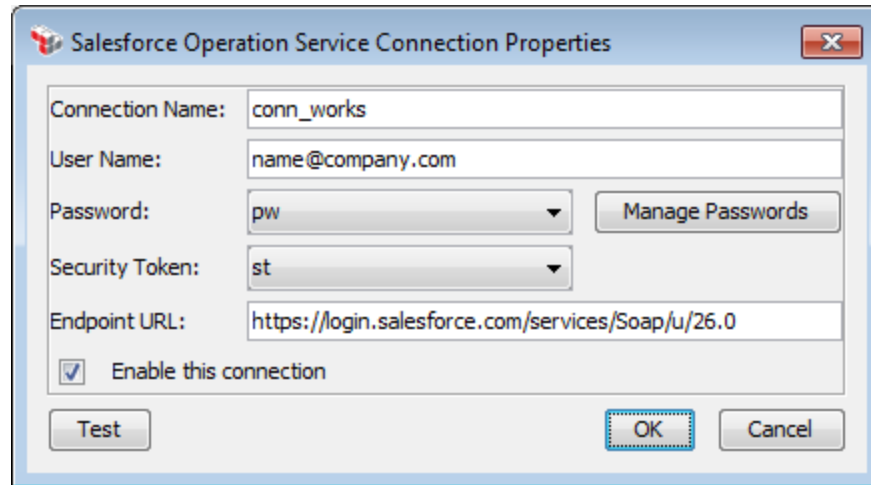
3. Click **[Close]** when done.

## Salesforce Connection Properties

When creating, cloning, or editing a [Salesforce connection](#), the Salesforce Connection Properties appear.

➤ *To access the properties for a Salesforce connection:*

1. Run the [Manage Salesforce Operation Service Connections](#) task.
2. Choose a connection from the list and then click **[Edit]**. You can also click **[Add]** to define a new connection or **[Clone]** to quickly define a connection based on an existing one. The Salesforce Operation Service Connection Properties appear.



The dialog box is titled "Salesforce Operation Service Connection Properties". It contains the following fields and controls:

- Connection Name:** A text field containing "conn\_works".
- User Name:** A text field containing "name@company.com".
- Password:** A dropdown menu showing "pw". To its right is a button labeled "Manage Passwords".
- Security Token:** A dropdown menu showing "st".
- Endpoint URL:** A text field containing "https://login.salesforce.com/services/Soap/u/26.0".
- Enable this connection:** A checked checkbox.
- Buttons:** "Test", "OK", and "Cancel" are located at the bottom.

Figure 204: Salesforce Operation Service Connection Properties dialog box

3. Configure the properties as follows:

Table 136: Salesforce connection settings

| Setting                       | Description   |
|-------------------------------|---|
| <b>Connection Name</b>        | Enter a name to identify the Salesforce connection.   |
| <b>User Name</b>              | Enter the username of the Salesforce account.   |
| <b>Password</b>               | Choose the stored password of the Salesforce account from the drop-down list.<br>To define a stored password, click <b>[Manage Passwords]</b> . For more information, see "Managing Stored Passwords" on page 42.             |
| <b>Security Token</b>         | Choose the stored security token of the Salesforce account from the drop-down list.<br>To define a stored security token, click <b>[Manage Passwords]</b> . For more information, see "Managing Stored Passwords" on page 42. |
| <b>Endpoint URL</b>           | Enter the URL of the Salesforce Login Server.   |
| <b>Enable this connection</b> | Select this check box to enable the connection.<br>Clear this check box to disable the connection, keeping the settings intact.   |
| <b>Test</b>                   | Click <b>[Test]</b> to validate the settings as configured for the Salesforce connection. If the test is not successful, the Policy Manager will display error messages to help you correct the problem.                      |

**Note:** Context variables cannot be used in the Salesforce Connection Properties, because the variables cannot be evaluated until runtime. Use of context variables will cause the Salesforce connection to fail.

4. Click **[OK]** when done.

## Appendix A:

# Contacting CA Technologies

### Technical Support

At CA Technologies, our commitment to exceptional service culminates in the advanced level of technical support that we provide for our products.

You can email support at [l7support@ca.com](mailto:l7support@ca.com) or call the number near your region.

| Area          | Phone                             |
|---------------|-----------------------------------|
| North America | 1-800-225-5224                    |
| Federal       | 1-800-225-5224 (press option '7') |
| UK            | 0845 161 0038                     |
| France        | 081 102 5146                      |
| Germany       | 0800 101 4666                     |
| Italy         | 84032 0057                        |
| Spain         | 90188 8125                        |
| Switzerland   | 084 400 0092                      |
| Australia     | 1800 023 386                      |

For more details, please refer to your Service Level Agreement.

### Contact Information

CA Technologies welcomes your questions, comments, enhancement requests, and general feedback.

|       |  |
|-------|--|
| Phone | 1-800-225-5224   |
| Web   | <a href="http://www.layer7tech.com">www.layer7tech.com</a> |
| Email | <a href="mailto:layer7-info@ca.com">layer7-info@ca.com</a> |



## Appendix B: Features by Product

The following table summarizes the features available in each version of the CA API Gateway.

**Notes:** (1) Some of the features referenced below are described in the *Layer 7 Installation and Maintenance Manual*. Refer to the edition for your Gateway form factor. (2) Each category may also include custom-created encapsulated assertions. For more information, see *Working with Encapsulated Assertions* in the *Layer 7 Policy Authoring User Manual*.

Table 137: Features available in each version of the Gateway

|   | API Proxy | XML Firewall | SOA Gateway |
|---|-----------|--------------|-------------|
| <b>Software form factor</b>               |           | <b>X</b>     | <b>X</b>    |
| <b>Appliance form factor</b>              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
|   |           |              |             |
| <b>General</b>                            |           |              |             |
| Systinet UDDI Policy Management           | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| CentraSite UDDI Policy Management         | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <a href="#">WSDL Builder</a>              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| WSIL Browser (part of WSDL Proxy)         | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Service Creation Wizard                   | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Service Virtualization                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Policy Templates                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Policy Fragments                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <a href="#">Role-Based Access Control</a> | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| XML Co-Processor Mode                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Clustering / Scalability                  | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Auto-Failover                             | <b>A</b>  | <b>A</b>     | <b>A</b>    |
| <a href="#">Certificate Management</a>    | <b>X</b>  | <b>X</b>     | <b>X</b>    |

|   | API Proxy | XML Firewall | SOA Gateway |
|---|-----------|--------------|-------------|
| FIPS 140.2 Level 1 Compliant Crypto                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| FIPS 140.2 Level 3 Compliant Crypto with HSM        | <b>A</b>  | <b>A</b>     | <b>A</b>    |
| Use Post-release Modular Assertions                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Custom Assertion SDK                                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| SNMP MIB  | <b>A</b>  | <b>A</b>     | <b>A</b>    |
| <a href="#">Log to External Sink</a>                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <a href="#">Email Listener</a>                      |           |              | <b>X</b>    |
| Encapsulated Assertions                             | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| OAuth Toolkit Installer                             | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <a href="#">Security Zones</a>                      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <b>Access Control</b>                               |           |              |             |
| Authenticate User or Group                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Authenticate Against Identity Provider              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Authenticate Against Radius Server                  |           |              | <b>X</b>    |
| Authenticate Against SiteMinder                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Authorize via SiteMinder                            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Check Protected Resource Against SiteMinder         | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Exchange Credentials using WS-Trust                 |           | <b>X</b>     | <b>X</b>    |
| Extract Attributes for Authenticated User           | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Extract Attributes from Certificate                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Perform JDBC Query                                  | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Query LDAP  | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require Encrypted UsernameToken Profile Credentials |           | <b>X</b>     | <b>X</b>    |
| Require FTP Credentials                             |           |              | <b>X</b>    |
| Require HTTP Basic Credentials                      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require HTTP Cookie                                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |



|   | API Proxy | XML Firewall | SOA Gateway |
|---|-----------|--------------|-------------|
| Require NTLM Authentication Credentials                 |           | <b>X</b>     | <b>X</b>    |
| Require Remote Domain Identity                          |           | <b>X</b>     | <b>X</b>    |
| Require SAML Token Profile                              |           | <b>X</b>     | <b>X</b>    |
| Require SSH Credentials                                 |           |              | <b>X</b>    |
| Require SSL or TLS Transport with Client Authentication | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require Windows Integrated Authentication Credentials   |           | <b>X</b>     | <b>X</b>    |
| Require WS-Secure Conversation                          |           | <b>X</b>     | <b>X</b>    |
| Require WS-Security Kerberos Token Profile Credentials  |           | <b>X</b>     | <b>X</b>    |
| Require WS-Security Password Digest Credentials         |           | <b>X</b>     | <b>X</b>    |
| Require WS-Security Signature Credentials               |           | <b>X</b>     | <b>X</b>    |
| Require WS-Security UsernameToken Profile Credentials   |           | <b>X</b>     | <b>X</b>    |
| Require XPath Credentials                               | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Retrieve Credentials from Context Variable              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Retrieve Kerberos Authentication Credentials            |           | <b>X</b>     | <b>X</b>    |
| Retrieve SAML Browser Artifact                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Use WS-Federation Credential                            |           | <b>X</b>     | <b>X</b>    |
| <b>Transport Layer Security (TLS)</b>                   |           |              |             |
| Require SSL or TLS Transport                            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <b>XML Security</b>                                     |           |              |             |
| (Non-SOAP) Check Results from XML Verification          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| (Non-SOAP) Decrypt XML Element                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| (Non-SOAP) Encrypt XML Element                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| (Non-SOAP) Sign XML Element                             | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| (Non-SOAP) Validate SAML Token                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| (Non-SOAP) Verify XML Element                           | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Add or Remove WS-Security                               |           | <b>X</b>     | <b>X</b>    |
| Add Security Token                                      |           | <b>X</b>     | <b>X</b>    |

|  | API Proxy | XML Firewall | SOA Gateway |
|--|-----------|--------------|-------------|
| Add Timestamp                                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Build RST SOAP Request                       |           | <b>X</b>     | <b>X</b>    |
| Build RSTR SOAP Response                     |           | <b>X</b>     | <b>X</b>    |
| Build SAML Protocol Request                  |           | <b>X</b>     | <b>X</b>    |
| Build SAML Protocol Response                 |           | <b>X</b>     | <b>X</b>    |
| Cancel Security Context                      |           | <b>X</b>     | <b>X</b>    |
| Configure WS-Security Decoration             |           | <b>X</b>     | <b>X</b>    |
| Create SAML Token                            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Create Security Context Token                |           | <b>X</b>     | <b>X</b>    |
| Create XACML Request                         |           |              | <b>X</b>    |
| Encrypt Element                              |           | <b>X</b>     | <b>X</b>    |
| Establish Outbound Secure Conversation       |           | <b>X</b>     | <b>X</b>    |
| Evaluate SAML Protocol Response              |           | <b>X</b>     | <b>X</b>    |
| Evaluate XACML Policy                        |           |              | <b>X</b>    |
| Generate OAuth Signature Base String         | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Generate Security Hash                       | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Look Up Certificate                          |           | <b>X</b>     | <b>X</b>    |
| Look Up Outbound Secure Conversation Session |           | <b>X</b>     | <b>X</b>    |
| Process RSTR Response                        |           | <b>X</b>     | <b>X</b>    |
| Protect Against Message Replay               | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require Encrypted Element                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require Signed Element                       | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require Timestamp                            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Sign Element                                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Use WS-Security v1.1                         |           | <b>X</b>     | <b>X</b>    |
| <b>Message Validation/Transformation</b>     |           |              |             |
| Add or Remove XML Elements                   | <b>X</b>  | <b>X</b>     | <b>X</b>    |

|  | API Proxy | XML Firewall | SOA Gateway |
|--|-----------|--------------|-------------|
| Add WS-Addressing                        |           | <b>X</b>     | <b>X</b>    |
| Apply JSON Transformation                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Apply XSL Transformation                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Compress Messages to/from SecureSpan XVC |           | <b>X</b>     | <b>X</b>    |
| Decode MTOM Message                      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Encode/Decode Data                       | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Encode to MTOM Format                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Enforce WS-I BSP Compliance              |           | <b>X</b>     | <b>X</b>    |
| Enforce WS-I SAML Compliance             |           | <b>X</b>     | <b>X</b>    |
| Enforce WS-Security Policy Compliance    |           | <b>X</b>     | <b>X</b>    |
| Evaluate JSON Path Expression            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Evaluate Regular Expression              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Evaluate Request XPath                   | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Evaluate Response XPath                  | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Evaluate WSDL Operation                  |           | <b>X</b>     | <b>X</b>    |
| Process SAML Attribute Query Request     |           | <b>X</b>     | <b>X</b>    |
| Process SAML Authentication Request      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Replace Tag Content                      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Require WS-Addressing                    |           | <b>X</b>     | <b>X</b>    |
| Set SAML Response Status Code            | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Translate HTTP Form to MIME              |           |              | <b>X</b>    |
| Translate MIME to HTTP Form              |           |              | <b>X</b>    |
| Validate Certificate                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Validate HTML Form Data                  | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Validate JSON Schema                     | <b>X</b>  |              | <b>X</b>    |
| Validate MTOM Message                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Validate or Change Content Type          | <b>X</b>  | <b>X</b>     | <b>X</b>    |

|                                       | API<br>Proxy | XML<br>Firewall | SOA<br>Gateway |
|---------------------------------------|--------------|-----------------|----------------|
| Validate SOAP Attachments             | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Validate XML Schema                   | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| <b>Message Routing</b>                |              |                 |                |
| Configure Message Streaming           | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Copy Request Message to Response      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Execute Salesforce Operation          | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Manage Cookie                         | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Manage Transport Properties/Headers   | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Return Template Response to Requestor | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Route via FTP(S)                      |              |                 | <b>X</b>       |
| Route via HTTP(S)                     | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Route via JMS                         |              |                 | <b>X</b>       |
| Route via MQ Native                   |              |                 | <b>X</b>       |
| Route via Raw TCP                     |              |                 | <b>X</b>       |
| Route via SSH2                        |              |                 | <b>X</b>       |
| <b>Service Availability</b>           |              |                 |                |
| Apply Rate Limit                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Apply Throughput Quota                | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Limit Availability to Time/Days       | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Look Up in Cache                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Query Rate Limit                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Query Throughput Quota                | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Resolve Service                       | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Restrict Access to IP Address Range   | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Store to Cache                        | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| <b>Logging, Auditing and Alerts</b>   |              |                 |                |
| Add Audit Detail                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |

|  | API Proxy | XML Firewall | SOA Gateway |
|--|-----------|--------------|-------------|
| Audit Messages in Policy                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Capture Identity of Requestor                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Customize Error Response                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Customize SOAP Fault Response                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Send Email Alert                             | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Send SNMP Trap                               | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| <b>Policy Logic</b>                          |           |              |             |
| Add Comment to Policy                        | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| All Assertions Must Evaluate to True         | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| At Least One Assertion Must Evaluate to True | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Compare Expression                           | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Continue Processing                          | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Create Routing Strategy                      | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Execute Routing Strategy                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Export Variables from Fragment               | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Generate UUID                                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Include Policy Fragments                     | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Join Variable                                | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Look Up Context Variables                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Look Up Item by Value                        | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Look Up Item by Index Position               | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Manipulate Multivalued Variable              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Map Value                                    | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Process Routing Strategy Result              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Run All Assertions Concurrently              | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Run Assertions for Each Item                 | <b>X</b>  | <b>X</b>     | <b>X</b>    |
| Set Context Variable                         | <b>X</b>  | <b>X</b>     | <b>X</b>    |

|   | API<br>Proxy | XML<br>Firewall | SOA<br>Gateway |
|---|--------------|-----------------|----------------|
| Split Variable                                  | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Stop Processing                                 | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| <b>Threat Protection</b>                        |              |                 |                |
| Limit Message Size                              | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against Code Injection                  | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against Cross-Site Request Forgery      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against Document Structure Threats      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against JSON Document Structure Threats | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against Message Replay                  | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Protect Against SQL Attack                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Scan Using ICAP-Enabled Antivirus               | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Validate JSON Schema                            | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Validate OData Request                          | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Validate or Change Content Type                 | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Validate XML Schema                             | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| <b>Internal Assertions</b>                      |              |                 |                |
| Collect WSDM Metrics                            | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Convert Audit Record to XML                     | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Handle UDDI Subscription Notification           | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Manage Gateway                                  | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| REST Manage Gateway                             | <b>X</b>     | <b>X</b>        | <b>X</b>       |
| Subscribe to WSDM Resource                      | <b>X</b>     | <b>X</b>        | <b>X</b>       |

## Appendix C: Context Variables

Context variables relate to the request being processed by the Gateway. These variables can reveal a wealth of information about what is happening at the Gateway and are invaluable in helping you resolve issues.

Assertions can read context variables. In this case, the value of the variable is resolved at runtime when the assertion is executed. Assertions can also write variables to the request context, making them available to other assertions.

When embedding a context variable within a string, use the following format:

```
${context.variable.name}
```

*Example:* In the Send Email Alert or Return Template Response to Requestor assertions, you create this message: *"This transaction is being denied because the account `${request.authenticateduser}` has exceeded quota. Please contact customer support at `${gateway.supportnumber}` for assistance."* The delimiter characters are required in this case.

When an assertion requires just the name of a context variable, enter the name without the delimiters:

```
context.variable.name
```

*Example:* In the Restrict Access to IP Address Range assertion, you wish to resolve the IP address from this context variable: `request.http.header.remoteip`. In this case, the delimiter characters are not required.

---

**Tips:** (1) When a context variable fails, the default behavior is to log a warning and use an empty string. The assertion calling the context variable does not fail. To cause the assertion to fail when a context variable fails, set the [template.strictMode](#) cluster property to "true". Some examples of context variable failures: a) Calling `"${request.http.header.abc}"` but the request has no "abc" header. b) Requesting a context variable that doesn't exist: `"${someNonExistentVariable}"`. (2) You can access cluster property values by using the built-in context variable `${gateway.<propertyName>}`. To learn more about using the built-in gateway prefix, see below. For more information about cluster properties, see "Managing Cluster-Wide Properties" on page 40. (3) You can see the context variables set and used for any assertion by displaying the Assertion Information dialog. For more information, see "Viewing Assertion Information" on page 32.

---

## Multivalued Context Variables

All the context variables described below can hold only a single value at a time. However, there is a special class of variables called *multivalued context variables* that can contain any number of values. These context variables are created using the Join Variable, Extract Attributes for Authenticated User, Listen Ports, or Query LDAP assertions and can be used wherever the single-value context variables are used.

For more information, see "Working with Multivalued Context Variables" on page 558.

## Where Context Variables are Defined

The Gateway includes a set of built-in context variables described under "[Predefined Context Variables](#)" below. Additionally, many assertions also define their own context variables when used in a policy. These variables are available to subsequent assertions in the policy tree. See the respective assertion topics for information about these variables.

The following topics also describe context variables used in specific scenarios:

- "Context Variables for XPath" on page 560
- "Context Variables for CA SiteMinder" on page 562
- Working with the Debug Trace Policy in the *Layer 7 Policy Authoring User Manual*

## Context Variable Naming Rules

When an assertion allows you to type in the name of a new context variable (versus creating one using a system defined naming pattern), it is important to observe the following naming rules:

- The first character must be either a letter or the underscore ("\_") character.
- After the first character, the variable name may be any combination of letters, digits, underscore ("\_"), or period (".").
- The dollar sign ("\$") is a reserved character and cannot be used anywhere within the name.
- Context variables may not begin with "*request.*" or "*response.*"—these are reserved for system use.
- Multi-byte characters are currently not supported within context variable names.

*Examples:*

- Valid context variable names: *\_counter*, *request.url*, *layer7*
- Invalid context variable names: *.request*, *7layer*



## Context Variable Data Types

Context variables can technically be of any type. They can hold anything from a number, to a string, to an entire message complete with attachments and headers. The assertions in the Policy Manager can create variables with the following data types:

- **String:** The variable contains a string. This is the most common data type used in the Gateway. Most of the predefined variables are of this type.
- **Message:** The variable contains a complete message, complete with attachments (if present). To access the body of the main/root MIME portion of the message as a string, add the ".mainpart" suffix to the context variable. For more information on the ".mainpart" suffix, see "Message Layer Variables" on page 544.

Message type context variables are created by the Set Context Variable assertion and by the Route via HTTP(S) Assertion ("Response Destination"). They can also be accessed using any built-in variable with the prefix "\${request.\*}" or "\${response.\*}".

- **Number:** The variable contains a number. These variables are created by an XPath assertion (Evaluate Request XPath or Evaluate Response XPath) when evaluating an XPath expression such as "0.14 \* //item/@price". A context variable with type Number can be interpreted as a String in almost all cases.
- **X.509 Certificate:** The variable contains one or more X.509 certificates. These variables are created by the (Non-SOAP) Verify XML Element and Look Up Certificates assertion. They can also be accessed by the *"Credential Certificates Variables" on page 537*.
- **Element:** The variable contains a reference to a specific XML element from the message. These variables can be created by the following assertions:
  - (Non-SOAP) Verify XML Element
  - (Non-SOAP) Decrypt XML Element
  - Evaluate Request XPath
  - Evaluate Response XPath
  - Require WS-Security Signature Credentials
- **AuditDetail** and **AuditRecord:** These variables are accessed using the built-in **\${audit.\*}** variables within an audit sink policy. For more information, see "Working with the Audit Sink Policy" on page 178.
- **Date/Time:** The variable will contain date/time information. These variables will behave similar to the built-in variables described under ["Date/Time Variables"](#).

---

**Tip:** Context variables created by a custom or a modular assertion (either from CA or from a third party) may have data types other than those listed above.

---

## Context Variable Validation

When you enter a context variable or a prefix for a context variable, the Policy Manager validates your entry and displays an instant feedback message in the dialog. Table 138 explains the various messages that may appear.

Table 138: Context variable validation messages

| Validation                     | Description  |
|--------------------------------|--|
| <b>OK</b>                      | The name entered is valid; a new context variable will be created.   |
| <b>OK (Overwrite)</b>          | The name entered matches a context variable that was already defined in a previous assertion in the policy. That variable will be overwritten.   |
| <b>OK (Built-in, settable)</b> | The name entered matches a built-in context variable for which you can assign a value.   |
| <b>Built-in, not settable</b>  | The name entered matches a built-in context variable for which you cannot assign a value. Try another name.  |
| <b>OK (New Prefix)</b>         | The name is valid; a new prefix will be created.   |
| <b>Invalid syntax</b>          | The field has been left empty or the name entered contains illegal characters. Try another name. For more information, see <a href="#">"Context Variable Naming Rules"</a> .                         |
| <b>No such variable</b>        | The specified variable does not exist.<br><br>This message is used in instances where you are expected to reference an existing variable from which to obtain a value, not to create a new variable. |

## Checking for Existence of Context Variables

Sometimes a policy may need to determine whether a context variable exists in order to branch correctly—for example, to check whether a certain header or parameter exists. There are two ways you can do this, depending on your policy logic requirements:

### Method 1: Use the Look Up Context Variable assertion by itself

Example, to determine whether the variable "test" exists:

1. Add the Look Up Context Variable assertion as the first item in an "All Assertions Must Evaluate to True" folder.

2. Configure Look Up Context Variable as follows:

- Select the **Fail if not found** check box.
- Enter **test** in the Expression field.

Using this logic, the branch will not execute if the variable does not exist.

### Method 2: Use Look Up Context Variable in conjunction with the Compare Expression assertion

As above, determining whether the variable "test" exists:

1. Add Look Up Context Variable before the Compare Expression assertion in the policy.
2. Configure Look Up Context Variable as follows:
  - Clear the **Fail if not found** check box.
  - Enter **test** in the Expression field.
3. Configure the Compare Expression assertion to check whether the variable `${lookup.found}` = **true** or **false**

For more information, see Look Up Context Variable assertion in the *Layer 7 Policy Authoring User Manual*.

## Predefined Context Variables

The following tables describe the context variables that can be used in the above assertions.

---

**Tip:** Some context variables can target a specific message. These are indicated by the prefix "<target>" in the variable name, where "<target>" is either **request**, **response**, or a message context variable that has been set in the policy prior to the assertion. For more information on message context variables, see "[Context Variable Data Types](#)" above.

---

## General Context Variables

Table 139 lists general predefined context variables available on the Gateway.

Table 139: General context variables

| Variable  | Description  |
|---|--|
| XPATH results variables                           | <p>For a list of the context variables created when evaluating an XPath expression, see:</p> <ul style="list-style-type: none"> <li>Evaluate Request XPath Assertion</li> <li>Evaluate Response XPath Assertion</li> </ul> <p>For more information, see also "Context Variables for XPaths" on page 560.</p>   |
| WS-Addressing variables                           | <p>For a list of the context variables created for WS-Addressing, see Require WS-Addressing Assertion in the <i>Layer 7 Policy Authoring User Manual</i>.</p>  |
| JDBC connection variables                         | <p>For a list of the context variables created during a JDBC connection, see Perform JDBC Query Assertion in the <i>Layer 7 Policy Authoring User Manual</i>.</p>  |
| Non-SOAP XML element variables                    | <p>For a list of the context variables created during a JDBC connection, see (Non-SOAP) Verify XML Element Assertion in the <i>Layer 7 Policy Authoring User Manual</i>.</p>   |
| <code>\${documentDownload.maxSize}</code>         | <p>Contains the maximum allowable size of a document download. This variable is used in various cluster properties involving "maxSize" and "maxDownloadSize" (for example, wsdlDownload.maxSize). This variable contains the default value <b>10485760</b> bytes (10MB).</p>   |
| <code>\${gateway.&lt;cluster_property&gt;}</code> | <p>In this context variable, "gateway" is the context variable prefix that resolves a cluster-wide property value.</p> <p>For example, the administrator adds the property "company" with the value of "Acme Inc." in the <a href="#">cluster properties table</a>. Assertions now have access to the context variable <code>\${gateway.company}</code>, which resolves to the value "Acme Inc."</p> <p><b>Another example:</b> Define a cluster variable <code>customersupport.phonenumber</code> with the value <code>1-800-GET-ACME</code>. You can then use this variable when creating a template SOAP fault in the Customize SOAP Fault Response assertion:</p> <pre>&lt;faultdetail&gt; Please contact Customer Support at \${gateway.customersupport.phonenumber} for assistance. &lt;/faultdetail&gt;</pre> |

| Variable                                       | Description   |
|--|---|
|  | Should the phone number ever change, you only need to edit the property value once and the change will be reflected in all policies that use this variable.   |
| <b><code>\${jsonschema.failure}</code></b>     | Contains the reason for the last JSON schema validation failure (s). This is set by the Validate JSON Schema assertion.   |
| <b><code>\${requestId}</code></b>              | <p>Returns the unique identifier generated for each request message, within a given Gateway node. The identifier is comprised of two zero-filled hexadecimal strings in this format:</p> <pre>xxxxxxxxxxxxxxxxxx-xxxxxxxxxxxxxxxxxx</pre> <p>where:</p> <ul style="list-style-type: none"> <li>the <code>x</code> symbols represent the date and time when Gateway service was started</li> <li>the <code>y</code> symbols represent a sequential counter</li> </ul> <p><b>Tip:</b> Normally, every request is associated with one unique request identifier. But there may be instances where a single request can have more than one unique identifier—for example: HTTP Basic authentication credentials are missing in the initial request; a second request is initiated, which causes the Gateway to generate a new <code>\${requestId}</code>. This results in the client having two different <code>\${requestId}</code> for one initial request.</p> |
| <b><code>\${schema.failure}</code></b>         | Contains the reason for the last schema validation failure. This is set by the Validate XML Schema assertion.   |
| <b><code>\${trafficlogger.select}</code></b>   | <p>Works in conjunction with the <a href="#">trafficlogger.selective</a> cluster property to determine whether traffic events will be logged.</p> <p>If <code>trafficlogger.selective = true</code>, then the Gateway will check the <code>\${trafficlogger.select}</code> context variable:</p> <ul style="list-style-type: none"> <li>If the variable is <b>true</b>, then traffic events will be logged.</li> <li>If the variable contains any other value or is undefined, then traffic events will <u>not</u> be logged.</li> </ul> <p>If <code>trafficlogger.selective = false</code>, all events are logged, provided that the traffic logger is enabled; the <code>\${trafficlogger.select}</code> variable is not consulted.</p> <p>For information on enabling/disabling a logger, see "Log Sink Properties" on page 167.</p>   |
| <b><code>\${uddi.centrasite.target}</code></b> | Contains the target to reference for CentraSite ActiveSOA UDDI Registry metrics. This value should match the value configured in the CentraSite web interface.  |

## Audit Variables

Table 140 lists the predefined context variables related to auditing.

**Tip:** For additional auditing-related context variables, see "Working with the Audit Sink Policy" on page 178.

Table 140: Context variables for auditing

| Variable                                     | Description   |
|--|---|
| <code>\${auditLevel}</code>                  | Returns the current audit level of the request; for example: INFO, WARNING.   |
| <code>\${audit.code.####}</code>             | Returns the message text for audit code "####". For example, <code>\${audit.code.4331}</code> will return "{0} message not XML. {1}". |
| <code>\${audit.details}</code>               | Contains all audit detail subrecords; multivalued, may be empty.  |
| <code>\${audit.details.0.componentId}</code> | The ID of the component the first detail relates to.  |
| <code>\${audit.details.0.exception}</code>   | Information about a stack trace, if one is associated with this detail record.  |
| <code>\${audit.details.0.fullText}</code>    | Returns the formatted text for the audit detail, including parameters.  |
| <code>\${audit.details.0.messageId}</code>   | The ID of the detail message, which can be looked up to determine what is being recorded.   |
| <code>\${audit.details.0.ordinal}</code>     | The ordinal of the detail message—in this case, "0".  |
| <code>\${audit.details.0.params}</code>      | Contains any parameter strings to flesh out the detail message; multivalued and may be empty.   |
| <code>\${audit.details.0.params[0]}</code>   | The first parameter of the first detail message.  |
| <code>\${audit.details.0.params[1]}</code>   | The second parameter of the first detail message.   |
| <code>\${audit.details.0.properties}</code>  | The audit detail parameters in XML form   |
| <code>\${audit.details.0.time}</code>        | When the request was authenticated  |
| <code>\${audit.details.1.params[0]}</code>   | The first parameter of the second detail message.   |

## Audit Lookup Variables

Table 141 lists context variables that the CA API Gateway uses to reconstruct the audits coming in from an audit lookup policy. The policy must populate these context variables when queried. The query is accessible thru the `${audit.recordQuery.*}` context variables in Table 142 and Table 143.

These context variables contain values only when used in an audit lookup policy only, or within a policy fragment that is included in an audit lookup policy. If called from any other policy, these variables will not exist and will be interpolated as blank (unless the [template.strictMode](#) cluster property is enforced, in which case the calling assertion will fail).

In the variables in Table 141, "X" refers to the number for each count. The referenced mapped context variables are described in "Working with the Audit Sink Policy" on page 178.

Table 141: Context variables used to reconstruct audits from an audit lookup policy

| Variable                                       | Description   |
|--|---|
| <code>\${recordQuery.queryresult.count}</code> | The number of records   |
| <code>\${recordQuery.id.X}</code>              | The entity ID of the audit record, referenced by the audit detail results |
| <code>\${recordQuery.nodeid.X}</code>          | Maps to <i>audit.nodeId</i>   |
| <code>\${recordQuery.time.X}</code>            | Maps to <i>audit.time</i>   |
| <code>\${recordQuery.type.X}</code>            | Maps to <i>audit.type</i>   |
| <code>\${recordQuery.audit_level.X}</code>     | Maps to <i>audit.audit_level</i>  |
| <code>\${recordQuery.name.X}</code>            | Maps to <i>audit.name</i>   |
| <code>\${recordQuery.message.X}</code>         | Maps to <i>audit.message</i>  |
| <code>\${recordQuery.ip_address.X}</code>      | Maps to <i>audit.ipAddress</i>  |
| <code>\${recordQuery.user_name.X}</code>       | Maps to <i>audit.user.name</i>  |
| <code>\${recordQuery.user_id.X}</code>         | Maps to <i>audit.user.id</i>  |
| <code>\${recordQuery.provider_oid.X}</code>    | Maps to <i>audit.user.idProv</i>  |
| <code>\${recordQuery.signature.X}</code>       | Maps to <i>audit.signature</i>  |
| <code>\${recordQuery.entity_class.X}</code>    | Maps to <i>audit.entity.class</i>   |
| <code>\${recordQuery.entity_id.X}</code>       | Maps to <i>audit.entity.oid</i>   |
| <code>\${recordQuery.status.X}</code>          | Maps to <i>audit.responseStatus</i>                                       |
| <code>\${recordQuery.request_id.X}</code>      | Maps to <i>audit.requestId</i>  |
| <code>\${recordQuery.service_oid.X}</code>     | Maps to <i>audit.serviceOid</i>   |
| <code>\${recordQuery.operation_name.X}</code>  | Maps to <i>audit.operationName</i>  |
| <code>\${recordQuery.authenticated.X}</code>   | Maps to <i>audit.authenticated</i>  |

| Variable   | Description   |
|--|---|
| <code>\${recordQuery.authenticationType.X String}</code> | Maps to <i>audit.authType</i>                                 |
| <code>\${recordQuery.request_saved.X}</code>             | Maps to <i>audit.savedRequestContentLength</i>                |
| <code>\${recordQuery.response_saved.X}</code>            | Maps to <i>audit.savedResponseContentLength</i>               |
| <code>\${recordQuery.request_length.X}</code>            | Maps to <i>audit.requestContentLength</i>                     |
| <code>\${recordQuery.response_length.X}</code>           | Maps to <i>audit.responseContentLength</i>                    |
| <code>\${recordQuery.request_xml.X}</code>               | Maps to <i>audit.reqZip</i>                                   |
| <code>\${recordQuery.response_xml.X}</code>              | Maps to <i>audit.reqZip</i>                                   |
| <code>\${recordQuery.response_status.X}</code>           | Maps to <i>audit.responseStatus</i>                           |
| <code>\${recordQuery.routing_latency.X}</code>           | Maps to <i>audit.routingLatency</i>                           |
| <code>\${recordQuery.properties.X}</code>                | Maps to <i>audit.properties</i>                               |
| <code>\${recordQuery.component_id.X}</code>              | Maps to <i>audit.componentId</i>                              |
| <code>\${recordQuery.action.X}</code>                    | Maps to <i>audit.action</i>                                   |
| <code>\${detailQuery.queryresult.count}</code>           | The number of details (associated logs)                       |
| <code>\${detailQuery.audit_oid.X}</code>                 | The entity ID of the audit record that this detail belongs to |
| <code>\${detailQuery.time.X}</code>                      | Maps to <i>audit.details.X.time</i>                           |
| <code>\${detailQuery.component_id.X}</code>              | Maps to <i>audit.details.X.componentId</i>                    |
| <code>\${detailQuery.ordinal.X}</code>                   | Maps to <i>audit.details.X.ordinal</i>                        |
| <code>\${detailQuery.message_id.X}</code>                | Maps to <i>audit.details.X.messageId</i>                      |
| <code>\${detailQuery.exception_message.X}</code>         | Maps to <i>audit.details.X.exception</i>                      |
| <code>\${detailQuery.properties.X}</code>                | Maps to <i>audit.details.X.properties</i>                     |

## Retrieving an Audit Record

The following variables are used for *retrieving* an entire audit record (all values are null if *searching* for an audit):

Table 142: Context variables used to retrieve an entire audit record

| Variable                                | Description  |
|---|--|
| <code>\${audit.recordQuery.guid}</code> | The list of GUID of the audits to retrieve; returns null if searching for audits |



| Variable  | Description   |
|---|---|
| <code>\${audit.recordQuery.maxMessageSize}</code> | The maximum size of an audit response/request XML to retrieve; returns null if not applicable |

## Searching for an Audit Record

The following variables in Table 143 are used for *searching* audits (all values are null when *retrieving* an audit):

Table 143: Context variables used for searching audits

| Variable   | Description   |
|--|---|
| <code>\${audit.recordQuery.minTime}</code>         | The start time, in milliseconds                             |
| <code>\${audit.recordQuery.maxTime}</code>         | The end time, in milliseconds                               |
| <code>\${audit.recordQuery.levels}</code>          | The list of log level numbers                               |
| <code>\${audit.recordQuery.auditType}</code>       | The audit type ('%' for all)                                |
| <code>\${audit.recordQuery.nodeId}</code>          | The node id ('%' for all)                                   |
| <code>\${audit.recordQuery.serviceName}</code>     | The service name ('%' for all)                              |
| <code>\${audit.recordQuery.userName}</code>        | The user name ('%' for all)                                 |
| <code>\${audit.recordQuery.userIdOrDn}</code>      | The user provider ('%' for all)                             |
| <code>\${audit.recordQuery.entityClassName}</code> | The entity class name for admin audit record ('%' for all)  |
| <code>\${audit.recordQuery.entityId}</code>        | The entity ID for admin audit record ('%' for all)          |
| <code>\${audit.recordQuery.requestId}</code>       | The request ID for a message audit record ('%' for all)     |
| <code>\${audit.recordQuery.operation}</code>       | The operation name for a message audit record ('%' for all) |
| <code>\${audit.recordQuery.messageId}</code>       | The audit detail message ID (null = any)                    |
| <code>\${audit.recordQuery.operation}</code>       | The operation name for message audit record ('%' for all)   |

## Audit Sink Variables

The following context variables in Table 144 contain values only when used in an audit sink policy, or within a policy fragment that is included in an audit sink policy. If called from any other policy, these variables will not exist and will be interpolated as blank (unless the [template.strictMode](#) cluster property is enforced, in which case the calling assertion will fail).

Table 144: Context variables for audit sink policy

| Variable                            | Description   |
|-------------------------------------|---|
| <code>\${audit.action}</code>       | For system audit records (audit.type="system"): This returns short description of the action that was happening when the audit event was generated; for example: "Initializing".<br><br>For administrative audit records (audit.type="admin"): This returns the type of event that generated this record (C=Created, U=Updated, D=Deleted, L=Login, X=Logout, O=Other). |
| <code>\${audit.authType}</code>     | How the user was authenticated (for example, "HTTP Basic").   |
| <code>\${audit.component}</code>    | The component, e.g., "Certificate Signing Service" (for audit.type="system").   |
| <code>\${audit.componentId}</code>  | For system audit records (audit.type="system"): This returns the ID of the component this audit record relates to.  |
| <code>\${audit.entity.class}</code> | The entity class changed by the admin request (for audit.type="admin"); for example: "com.l7tech.identity.User".  |
| <code>\${audit.entity.oid}</code>   | The ID of the entity instance changed by the admin request (for audit.type="admin").  |
| <code>\${audit.ipAddress}</code>    | IP address of client (if audit.type="message" or "admin") or Gateway node (if audit.type="system").   |
| <code>\${audit.level}</code>        | The numeric value of the audit level:<br><br>1000 = SEVERE<br>900 = WARNING<br>800 = INFO<br>700 = CONFIG<br>500 = FINE<br>400 = FINER<br>300 = FINEST  |
| <code>\${audit.levelStr}</code>     | The string value of the audit level (for example, "INFO").  |
| <code>\${audit.message}</code>      | The audit message in human-readable format.   |
| <code>\${audit.name}</code>         | The name of the service (if audit.type="message"), admin user (if audit.type="admin"), or subsystem (if audit.type="system").   |

| Variable  | Description  |
|---|--|
| <code>\${audit.nodeId}</code>                   | The ID of the Gateway cluster node that produced this audit record.  |
| <code>\${audit.policyExecutionAttempted}</code> | Initially "false"; set to "true" if processing reached the point of resolving and running a target policy for the request. <b>Tip:</b> When this variable returns "true", you may assume that further audit decisions could have been made by the policy; if it returns "false", then the request has relevance only in the audit sink policy. |
| <code>\${audit.properties}</code>               | The mapping values and any additional fields in XML form   |
| <code>\${audit.requestId}</code>                | The Gateway-assigned internal ID of the request that was processed (if <code>audit.type="message"</code> or <code>"admin"</code> ).  |
| <code>\${audit.sequenceNumber}</code>           | The sequence number assigned to this audit record, useful for ordering the records later.  |
| <code>\${audit.signature}</code>                | The signature of the audit   |
| <code>\${audit.time}</code>                     | The timestamp of the audit record, in milliseconds since 1970-Jan-01.  |
| <code>\${audit.type}</code>                     | The type of audit record: "message", "system", or "admin". For more information about the different types, see Message Auditing in the <i>Layer 7 Policy Authoring User Manual</i> .   |
| <code>\${audit.user.id}</code>                  | The ID of the last authenticated user (if <code>audit.type="message"</code> ) or the administrator (if <code>audit.type="admin"</code> ).  |
| <code>\${audit.user.idProv}</code>              | The ID of the <a href="#">identity provider</a> in which the user ID and user name is meaningful.  |
| <code>\${audit.user.name}</code>                | The name of the last authenticated user (if <code>audit.type="message"</code> ) or the administrator (if <code>audit.type="admin"</code> ).  |

For message audit records (`audit.type="message"`), Table 145 lists additional context variables that are available. The values from the Request and Response messages are as of the end of message processing.

Table 145: Context variables for message audit records in an audit sink policy

| Variable                               | Description   |
|--|---|
| <code>\${audit.authenticated}</code>   | The request was authenticated for an identity.  |
| <code>\${audit.filteredrequest}</code> | <p>The request message after it has been processed by an audit message filter (AMF) internal use policy. This means the message is most likely encrypted.</p> <p>If no AMF policy is present, then <code>audit.filteredrequest = audit.request</code>.</p> <p><b>Note:</b> Unlike <code>audit.request</code>, the <code>audit.filteredrequest</code> variable is type String rather than type Message. This</p> |

| Variable  | Description   |
|---|---|
|   | means you cannot use the <i>.mainpart</i> suffix when interpolating the variable.   |
| <code>\${audit.filteredresponse}</code>           | <p>The response message after it has been processed by an audit message filter (AMF) internal use policy. This means the message is most likely encrypted.</p> <p>If no AMF policy is present, then <i>audit.filteredresponse</i> = <i>audit.response</i>.</p> <p><b>Note:</b> Unlike <i>audit.response</i>, the <i>audit.filteredresponse</i> variable is type String rather than type Message. This means you cannot use the <i>.mainpart</i> suffix when interpolating the variable.</p> |
| <code>\${audit.mappingValuesOid}</code>           | The ID of the custom mapping value in effect when this record was processed (if any).   |
| <code>\${audit.operationName}</code>              | The name of the SOAP operation that was invoked.  |
| <code>\${audit.requestContentLength}</code>       | The size of the final request message, in bytes.  |
| <code>\${audit.requestSavedFlag}</code>           | Whether the audit record flags that the final request should be saved (true/false).   |
| <code>\${audit.responseContentLength}</code>      | The size of the final response message, in bytes.   |
| <code>\${audit.responseSavedFlag}</code>          | Whether the audit record flags that the final response should be saved (true/false).  |
| <code>\${audit.responseStatus}</code>             | The HTTP status code of the back-end response   |
| <code>\${audit.reqZip}</code>                     | The zipped request message in binary array  |
| <code>\${audit.resZip}</code>                     | The zipped response message in binary array   |
| <code>\${audit.routingLatency}</code>             | The number of milliseconds that elapsed inside the last outbound routing assertion.   |
| <code>\${audit.savedRequestContentLength}</code>  | The size of the saved request message, in bytes, -1 for not saved   |
| <code>\${audit.savedResponseContentLength}</code> | The size of the saved response message, in bytes, -1 for not saved  |
| <code>\${audit.serviceOid}</code>                 | The ID of the service that accepted the request.  |
| <code>\${audit.status}</code>                     | The final assertion status returned by the original policy.   |
| <code>\${audit.request}</code>                    | The original request message. See also <i>audit.filtered request</i> above.   |
| <code>\${audit.response}</code>                   | The original response message. See also <i>audit.filtered response</i> above.   |

| Variable  | Description  |
|---|--|
| <code>\${audit.var.&lt;originalContextVar&gt;}</code> | <p>The "\${audit.var}" prefix provides access to the original message processing <a href="#">context variables</a>. For example, <code>\${audit.var.httpRouting.latency}</code> would return the number of milliseconds it took to do downstream routing of the original request.</p> <p><b>Tip:</b> Avoid using the "\${audit.var}" prefix to access time-related variables. For example, the variables <code>\${audit.var.request.elapsedTime}</code> vs. <code>\${request.elapsedTime}</code> may return slightly different values, even though both return the "elapsed time" of the request. In this example, it is best to use the Add Audit Detail Assertion in the service policy to display the value for <code>\${request.elapsedTime}</code>, rather than using <code>\${audit.var.request.elapsedTime}</code> in an <a href="#">audit sink policy</a>.</p> |

## Authentication Variables

Table 146 lists the predefined context variables related to authentication requests.

Table 146: Context variables for authentication

| Variable  | Description   |
|---|---|
| <code>\${&lt;target&gt;.authenticateduser}</code> | <p>Returns the name of the most recently authenticated user by the Gateway for the target message. This name may differ from that returned by <code>\${&lt;target&gt;.username}</code>, which is the "raw" name retrieved from the credentials.</p> <p>You can access additional user details about the authenticated user by appending the following suffixes:</p> <ul style="list-style-type: none"> <li>• <b>.providerId:</b> user's identity Provider ID</li> <li>• <b>.id:</b> user's identifier</li> <li>• <b>.login:</b> user's login ID</li> <li>• <b>.firstName:</b> user's first name</li> <li>• <b>.lastName:</b> user's last name</li> <li>• <b>.email:</b> user's email address</li> <li>• <b>.department:</b> user's department</li> <li>• <b>.subjectDn:</b> user's X.509 subject DN</li> </ul> <p>For example, <code>\${request.authenticateduser.id}</code> retrieves the user's ID from the request message.</p> <p><b>Tip:</b> If the policy is configured for multiple authentications, you can further append '.0', '.1', '.2', etc., suffixes to the context variable to retrieve the <i>n</i>th authenticated identity in the context. For example, use <code>\${request.authenticateduser.0}</code> for the first authenticated identity, <code>\${request.authenticateduser.1}</code> for the second</p> |

| Variable   | Description   |
|--|---|
|  | authenticated identity in the context, etc.   |
| <code>\${&lt;target&gt;.authenticatedusers}</code> | <p>This is the multivalued version of <code>\${&lt;target&gt;.authenticateduser}</code>. It returns all the authenticated user names in a true <a href="#">multivalued context variable</a> that supports delimiters and indexing.</p> <p><b>Tip:</b> The indexing feature works similar to the numerical suffixes in <code>&lt;target&gt;.authenticateduser</code>. For example:<br/> <code>\${request.authenticateduser.0} = \${request.authenticatedusers.[0]}</code>, <code>\${request.authenticateduser.1} = \${request.authenticatedusers.[1]}</code>, etc.</p> |
| <code>\${&lt;target&gt;.authenticateddn}</code>    | <p>Returns the DN (Distinguished Name) of the most recently authenticated user for the request by the Gateway.</p> <p><b>Note:</b> If the policy is configured for multiple authentications, you can append '.0', '.1', '.2', etc., suffixes to the context variable to retrieve the <i>n</i>th authenticated DN in the context. For example, use <code>\${request.authenticateddn.0}</code> for the first authenticated DN, <code>\${request.authenticateddn.1}</code> for the second authenticated DN in the context, etc.</p>                                      |
| <code>\${&lt;target&gt;.authenticateddns}</code>   | <p>This is the multivalued version of <code>\${&lt;target&gt;.authenticateddn}</code>. It returns all the authenticated DN in a true <a href="#">multivalued context variable</a> that supports delimiters and indexing.</p> <p><b>Tip:</b> The indexing feature works similar to the numerical suffixes in <code>&lt;target&gt;.authenticateddn</code>. For example:<br/> <code>\${request.authenticateddn.0} = \${request.authenticateddns.[0]}</code>, <code>\${request.authenticateddn.1} = \${request.authenticateddns.[1]}</code>, etc.</p>                     |
| <code>\${&lt;target&gt;.buffer.allowed}</code>     | <p>Returns one of the following strings:</p> <ul style="list-style-type: none"> <li><b>true:</b> Buffering is permitted for this message. This is the default setting. If the buffer status is currently "unread", using the message will move it to "buffered".</li> <li><b>false:</b> Buffering is not allowed for this message. If the buffer status is currently "unread", using the message will move it to "gone".</li> </ul>   |
| <code>\${&lt;target&gt;.password}</code>           | <p>Returns the password (if available) as a plaintext string from the user credentials for the target.</p> <p><b>Note:</b> The Require HTTP Basic Credentials assertion must be present in the policy when using the <code>\${&lt;target&gt;.password}</code> variable.</p>   |
| <code>\${&lt;target&gt;.username}</code>           | <p>Returns the user name as a plaintext string from the user credentials for the target. This name may differ from the name returned by <code>\${&lt;target&gt;.authenticateduser}</code>, which is the name on the authenticated user's account in an identity provider.</p>   |

| Variable  | Description  |
|---|--|
|   | <b>Note:</b> The Require HTTP Basic Credentials assertion must be present in the policy if using the <code>\${&lt;target&gt;.username}</code> variable.  |
| <code>\${secpass.&lt;name&gt;.description}</code> | Returns the description of the password with the name <code>&lt;name&gt;</code> .<br><b>Note:</b> This variable is available <i>only</i> if the password has been enabled for context variable reference. If not, it will return no values. For more information, see "Stored Password Properties" on page 45.           |
| <code>\${secpass.&lt;name&gt;.plaintext}</code>   | Returns the actual stored password with the name <code>&lt;name&gt;</code> , in plain text.<br><b>Note:</b> This variable is available <i>only</i> if the password has been enabled for context variable reference. If not, it will return no values. For more information, see "Stored Password Properties" on page 45. |

## Certificate Attributes Variables

Table 147 lists the predefined context variables related to certificate attributes .

In the tables below, "`${prefix}`" represents any prefix that references a certificate variable. For example:

```
myCertificate.signatureAlgorithmName
request.wss.signingcertificates.value.X.signatureAlgorithmName
mySignature.token.attributes.signatureAlgorithmName
```

where "**X**" is the number for each count of certificates. (To retrieve the total number of signing certificates found in the target message, use:

```
"${<target>.wss.signingcertificates.count}").
```

In the example above, you will have previously defined the prefix "myCertificate" in the Set Context Variable assertion as:

```
Set myCertificate = ${request.wss.signingcertificates.value.1}
```

---

**Note:** If a certificate contains EMAILADDRESS in the Subject DN and if EMAILADDRESS is used to sign the message using Issuer Name/Serial Number signature key reference, the Gateway cannot recognize this credential. In this case, use one of the other signature key reference options (BST or SKI). For more information on the signature key reference, see Sign Element assertion in the *Layer 7 Policy Authoring User Manual*.

---

For each certificate variable (e.g., `request.wss.signingcertificates.value.1`) the following suffixes are available:

Table 147: Context variables for certificate attributes

| Variable  | Description   |
|---|---|
| <code>\${prefix}.base64</code>                      | The BASE64 encoded certificate (without whitespace)   |
| <code>\${prefix}.certificatePolicies</code>         | The certificate policies information. Each value is an entity ID.   |
| <code>\${prefix}.countryOfCitizenship</code>        | An array of countries for which the certificate is reporting  |
| <code>\${prefix}.der</code>                         | The DER encoded certificate   |
| <code>\${prefix}.extendedKeyUsageCriticality</code> | Criticality of the extended key usage field (none, noncrit, critical)   |
| <code>\${prefix}.extendedKeyUsageValues</code>      | The key usage information. Each value is an entity ID.  |
| <code>\${prefix}.issuer</code>                      | The Issuer DN (e.g., "CN=OASIS Interop Test CA, O=OASIS")   |
| <code>\${prefix}.issuer.canonical</code>            | The Issuer DN in canonical format: for comparisons; limited subset of entity ID names; strict sorting, whitespace, and case rules |
| <code>\${prefix}.issuer.rfc2253</code>              | The Issuer DN in RFC 2253 format: for correct but still reasonably pretty output (only includes RFC 2253 entity ID names)         |
| <code>\${prefix}.issuer.dn.\${key}</code>           | An array of values for parts of the Issuer DN parts that have the key <code>\${key}</code>  |
| <code>\${prefix}.issuerAltNameEmail</code>          | Email address (if any) for the Issuer Alternative Name (rfc288) (e.g., "example@ca.oasis-open.org")                               |
| <code>\${prefix}.issuerAltNameDNS</code>            | DNS Name address (if any) for the Issuer Alternative Name (e.g., "ca.oasis-open.org")   |
| <code>\${prefix}.issuerAltNameOther</code>          | The OTHER type for the Issuer Alternative Name, as a Base-64 encoded string.  |
| <code>\${prefix}.issuerAltNameURI</code>            | Uniform Resource Identifier (if any) for the Issuer Alternative Name (e.g., "http://ca.oasis-open.org/")                          |
| <code>\${prefix}.keyUsage.crlSign</code>            | CRL Sign (true/false)   |
| <code>\${prefix}.keyUsage.dataEncipherment</code>   | Data Encipherment (true/false)  |
| <code>\${prefix}.keyUsage.decipherOnly</code>       | Decipher Only (true/false)  |
| <code>\${prefix}.keyUsage.digitalSignature</code>   | Digital Signature (true/false)  |
| <code>\${prefix}.keyUsage.encipherOnly</code>       | Encipher Only (true/false)  |
| <code>\${prefix}.keyUsage.keyAgreement</code>       | Key Agreement (true/false)  |



| Variable  | Description   |
|---|---|
| <b><code>\${prefix}.keyUsage.keyCertSign</code></b>     | Key Certificate Sign (true/false)   |
| <b><code>\${prefix}.keyUsage.keyEncipherment</code></b> | Key Encipherment (true/false)   |
| <b><code>\${prefix}.keyUsage.nonRepudiation</code></b>  | Non Repudiation (true/false)  |
| <b><code>\${prefix}.keyUsageCriticality</code></b>      | Whether the extension is present; if so whether it is critical. The following values are used: <ul style="list-style-type: none"> <li><b>none</b> = extension not present</li> <li><b>noncrit</b> = extension is present but not critical</li> <li><b>critical</b> = extension is present and critical</li> </ul> |
| <b><code>\${prefix}.notAfter</code></b>                 | The Certificate Not After Date (e.g., "2018-03-19T23:59:59.000Z")   |
| <b><code>\${prefix}.notBefore</code></b>                | The Certificate Not Before Date (e.g., "2005-03-19T00:00:00.000Z")  |
| <b><code>\${prefix}.pem</code></b>                      | The PEM encoded certificate   |
| <b><code>\${prefix}.serial</code></b>                   | The Certificate Serial# (e.g., "68652640310044618358965661752471103641")  |
| <b><code>\${prefix}.signatureAlgorithmName</code></b>   | The Name of the Signature Algorithm for the certificate (e.g., "SHA1withRSA")   |
| <b><code>\${prefix}.signatureAlgorithmOID</code></b>    | The entity ID of the Signature Algorithm for the certificate (e.g., "1.2.840.113549.1.1.5")   |
| <b><code>\${prefix}.subject</code></b>                  | The Subject DN (e.g., "CN=Alice, OU=OASIS Interop Test Cert, O=OASIS")  |
| <b><code>\${prefix}.subject.canonical</code></b>        | The Subject DN in canonical format: for comparisons; limited subset of entity ID names; strict sorting, whitespace, and case rules  |
| <b><code>\${prefix}.subject.dn.\${key}</code></b>       | An array of values for the subject DN parts that have the key <code>\${key}</code>  |
| <b><code>\${prefix}.subject.rfc2253</code></b>          | The Subject DN in RFC 2253 format: for correct but still reasonably pretty output (only includes RFC 2253 entity ID names)  |
| <b><code>\${prefix}.subjectAltNameEmail</code></b>      | E-Mail address (if any) for the Subject Alternative Name (rfc288) (e.g., "example2@oasis-open.org")   |
| <b><code>\${prefix}.subjectAltNameDNS</code></b>        | DNS Name address (if any) for the Subject Alternative Name (e.g., "example2.oasis-open.org")  |
| <b><code>\${prefix}.subjectAltNameOther</code></b>      | The OTHER type for the Subject Alternative Name, as a Base-64 encoded string.   |

| Variable   | Description  |
|--|--|
| <b><code>\${prefix}.subjectAltNameURI</code></b>         | Uniform Resource Identifier (if any) for the Subject Alternative Name (e.g., "http://example2.oasis-open.org/")          |
| <b><code>\${prefix}.subjectKeyIdentifier</code></b>      | The BASE64 encoded value of the subject key identifier (SKI) extension or the derived SKI if an extension is not present |
| <b><code>\${prefix}.subjectPublicKeyAlgorithm</code></b> | The Name of the Algorithm used for the Subject's Public Key (e.g., "RSA")  |
| <b><code>\${prefix}.thumbprintSHA1</code></b>            | The BASE64 encoded value of the SHA-1 hash for the DER encoded certificate   |

### Attributes for Subject/Issuer DN

To extract the attributes for the Subject DN or Issuer DN, the Gateway parses and groups them based on the type and/or position. Consider the following sample Subject DN:

|          | 7   | 6 | 5 | 4 | 3 | 2 | 1 |
|----------|---|---|---|---|---|---|---|
| Position |   |   |   |   |   |   |   |
| DN       | CN=fred, OU=support+EMAIL=support@acme.org, OU=IT, OU=Services, DC=acme, DC=org, C=US |   |   |   |   |   |   |

The sample above will produce the following context variables, any of which can have multiple values:

Table 148: Context variables for Subject/Issuer DN attributes

| Name                                     | Value(s)               |
|--|------------------------|
| <code>\${prefix}.subject.dn.c</code>     | US                     |
| <code>\${prefix}.subject.dn.cn</code>    | fred                   |
| <code>\${prefix}.subject.dn.email</code> | support@acme.org       |
| <code>\${prefix}.subject.dn.dc</code>    | acme, org              |
| <code>\${prefix}.subject.dn.ou</code>    | support, IT , Services |
| <code>\${prefix}.subject.dn.1</code>     | C=US                   |
| <code>\${prefix}.subject.dn.2</code>     | DC=org                 |
| <code>\${prefix}.subject.dn.3</code>     | DC=acme                |
| <code>\${prefix}.subject.dn.4</code>     | OU=Services            |
| <code>\${prefix}.subject.dn.5</code>     | OU=IT                  |

| Name                                       | Value(s)                           |
|--|------------------------------------|
| <code>\${prefix}.subject.dn.6</code>       | OU=support, EMAIL=support@acme.org |
| <code>\${prefix}.subject.dn.7</code>       | CN=fred                            |
| <code>\${prefix}.subject.dn.1.c</code>     | US                                 |
| <code>\${prefix}.subject.dn.2.dc</code>    | org                                |
| <code>\${prefix}.subject.dn.3.dc</code>    | acme                               |
| <code>\${prefix}.subject.dn.4.ou</code>    | Services                           |
| <code>\${prefix}.subject.dn.5.ou</code>    | IT                                 |
| <code>\${prefix}.subject.dn.6.email</code> | support@acme.org                   |
| <code>\${prefix}.subject.dn.6.ou</code>    | support                            |
| <code>\${prefix}.subject.dn.7.cn</code>    | fred                               |

**Notes:** (1) If the Gateway cannot recognize an attribute entity ID, it will use the name "old.1.2.3", where "1.2.3" is the dotted-decimal entity ID of the attribute. If there is no string representation for an attribute value, the variable value will be set to the "#" encoding as defined in [RFC 2253](#). (2) If there is no string representation for an attribute value (for example, "DC"), then it is simply encoded as an octothorpe character ('#' ASCII 35) followed by the hexadecimal representation of each of the bytes of the BER encoding as defined in [RFC2253](#).

## Credential Certificates Variables

Table 149 lists the predefined context variables related to credential certificates.

Table 149: Context variables for credential certificates

| Variable   | Description   |
|--|---|
| <code>\${request.ssl.clientCertificate}</code>   | Returns the client side SSL certificate presented by the requestor (this is an X509Certificate object).   |
| <code>\${request.ssl.clientCertificate.base64}</code>  | Returns the same certificate as above, but as a Base64-encoded string with no white spaces.   |
| <code>\${request.ssl.clientCertificate.pem}</code>   | Returns the same certificate as above, but as a PEM-encoded string; this is formatted in Base64 with newlines, enclosed in the following wrapper:<br><br>-----BEGIN CERTIFICATE-----<br><br>-----END CERTIFICATE----- |
| <code>\${request.wss.signingcertificate}</code><br><code>\${request.wss.signingcertificate.base64}</code><br><code>\${request.wss.signingcertificate.pem}</code> | <i>These context variables have been replaced by the equivalent versions containing "value.1" (see</i>  |

| Variable  | Description   |
|---|---|
|   | <i>below). Though these variables still work, it is highly recommended that you adjust your service policies to use the new variables instead.</i>  |
| <code>\${request.wss.signingcertificates.value.1}</code>        | Returns the signing certificate of the WSS signature in the original request message.   |
| <code>\${request.wss.signingcertificates.value.1.base64}</code> | Returns the same certificate as above, but as a Base64-encoded string with no white spaces.   |
| <code>\${request.wss.signingcertificates.value.1.pem}</code>    | Returns the same certificate as above, but as a PEM-encoded string; this is formatted in Base64 with newlines, enclosed in the following wrapper:<br><br>-----BEGIN CERTIFICATE-----<br><br>-----END CERTIFICATE-----   |
| <code>\${&lt;target&gt;.wss.certificates.count}</code>          | Returns the number of certificates found for X.509 tokens.<br><br><b>WARNING:</b> The presence of a certificate in a message does not mean it should be trusted. It is recommended that these values are <b>not</b> used for trust decisions.   |
| <code>\${&lt;target&gt;.wss.certificates.value.X}</code>        | Returns the value of each certificate found for X.509 tokens, with one context variable created for each count. For a complete list of the attributes available for each value, see "Certificate Attributes Variables" on page 533.<br><br>For example, if:<br><br><code>request.wss.certificates.count = 1</code><br><br>Then this variable might be created:<br><br><code>request.wss.certificates.value.1.subject.dn = CN=MyUser,OU=MyGroup,DC=MyCompany,DC=com</code> |
| <code>\${&lt;target&gt;.wss.signingcertificates.count}</code>   | Returns the number of certificates found for X.509 tokens that have been used in valid signatures.<br><br><b>WARNING:</b> The presence of a certificate in a message does not mean it should be trusted. It is recommended that these values are <b>not</b> used for trust decisions.   |
| <code>\${&lt;target&gt;.wss.signingcertificates.value.X}</code> | Returns the value of each certificate found for X.509 tokens that have been used in valid signatures. For a complete list of the attributes available for each value, see "Certificate Attributes Variables" on page 533.   |

Note that the certificate s will contain credential information only when a credential source assertion has been executed in a policy (either Set SSL or TLS Transport or Require WS-Security Signature Credentials).

## Date and Time Variables

Table 150 lists the predefined context variables related to date and time.

**Tip:** In addition to the two built-in variables, you can create your own date and time variables by using the Set Context Variable assertion (choose [data type](#) "Date/Time").

Table 150: Built-in context variables for date and time

| Variables                                    | Description  |
|--|--|
| <code>\${gateway.time.&lt;suffix&gt;}</code> | Returns the current time on the Gateway; suffix is optional.   |
| <code>\${request.time.&lt;suffix&gt;}</code> | Returns the time the request was received; suffix is optional. |

There are a variety of suffixes that you can append (to both the built-in variables or to custom date/time variables) to modify or reformat the time that is returned. These suffixes are summarized in Table 151.

**Tip:** When a date/time variable is used without a suffix, the time value returned is in ISO 8601 format, in the UTC (Coordinated Universal Time) time zone.

Table 151: Suffixes for date and time variables

| Suffix  | Description  |
|---|--|
| <code>.local</code>                               | Returns the value in local time.   |
| <code>.utc</code>                                 | Returns the value in UTC time. This is the same as using no suffix at all.   |
| <code>.&lt;SimpleDateFormat&gt;</code>            | <p>Returns the value in a specified format. You can append a format to the above suffixes (or on its own) to create unstructured suffixes using symbols from <code>java.text.SimpleDateFormat</code>. Examples:</p> <pre> \${request.time.local.MM/dd/yyyy} \${gateway.time.MM/dd/yyyy} </pre> <p>For more information on the <code>SimpleDateFormat</code>, see <a href="http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html">http://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html</a></p> |
| <code>.millis</code>                              | Access a timestamp in milliseconds for the variable. This suffix must appear directly after the variable (for example, <code>\${mydate.millis}</code> ).   |
| <code>.seconds</code>                             | Access a second timestamp for the variable. This suffix must appear directly after the variable (for example, <code>\${gateway.time.seconds}</code> ).   |
| <code>.&lt;timezone&gt;.&lt;formatting&gt;</code> | <p>Returns the value in the specified time zone (case insensitive) with optional custom formatting. Examples:</p> <pre> \${myvar.BST} - value of myvar is in British Standard Time </pre>  |

| Suffix                           | Description  |
|----------------------------------|--|
|                                  | <p>formatted as an ISO 8601 string</p> <p><i>\${request.time.BST.hh:mm:ss}</i> - request is in British Standard Time with specified custom formatting</p> <p>Time zone suffixes are all those supported by the <code>java.util.TimeZone.getAvailableIDs()</code> utility.</p>  |
| <i>.&lt;offset&gt;</i>           | <p>Returns the value in the local time offset by the specified <i>&lt;offset&gt;</i> value. Examples of valid values:</p> <p><i>\${gateway.time.+07:00}</i><br/> <i>\${gateway.time.-0700}</i><br/> <i>\${gateway.time.+05:30}</i><br/> <i>\${gateway.time.-0530}</i><br/> <i>\${gateway.time.+07}</i><br/> <i>\${gateway.time.-07}</i></p> <p>The following are examples of invalid <i>&lt;offset&gt;</i> values:</p> <p><i>\${gateway.time.+7:00}</i><br/> <i>\${gateway.time.-530}</i><br/> <i>\${gateway.time.+7}</i></p>  |
| <i>.&lt;StructuredFormat&gt;</i> | <p>Returns the value in any of the following structured formats:</p> <ul style="list-style-type: none"> <li>• <b>.iso8601</b> - yyyy-MM-ddTHH:mm:ss.SSSX</li> <li>• <b>.rfc1123</b> - E, dd MM yyyy hh:mm:ss Z</li> <li>• <b>.rfc850</b> - EEEE, dd-MM-yy hh:mm:ss Z</li> <li>• <b>.asctime</b> - E MMM d hh:mm:ss yyyy</li> </ul> <p>These suffixes can be used directly after the variable name or after a timezone:</p> <p><i>\${myvar.BST.rfc1123}</i> - BST date string formatted according to rfc1123</p> <p><i>\${myvar.rfc1123}</i> - Date string formatted according to GMT (Zulu) time zone.</p> |

## Kerberos Ticket Authorization Info Variables

Table 152 lists the predefined context variables related to Kerberos Ticket Authorization Info.

Table 152: Context variables for Kerberos Ticket Authorization Info

| Variable                                       | Description   |
|--|---|
| <b><i>\${kerberos.data.authorizations}</i></b> | <p>Returns a list of authorization data stored in the ticket. Can be accessed using index; for example:</p> <p><i>\${kerberos.data.authorizations.0.pac.logoninfo.user.name}</i>.</p> |

| Variable   | Description  |
|--|--|
| <i>Logon Information Attributes</i>  |  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.logontime}</code></b>         | Returns the user logon time since Jan 1, 1970, in milliseconds.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.logofftime}</code></b>        | Returns the time since Jan 1, 1970 at which the client's logon session should expire, in milliseconds.   |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.kickofftime}</code></b>       | Returns the time since Jan 1, 1970 at which the server should forcibly log off the client, in milliseconds. If the client should not be forced off, this variable returns null.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.pwdlastchangetime}</code></b> | Returns the time since Jan 1, 1970 at which the client's password was last set, in milliseconds. If password was never set, this variable returns null.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.pwdcanchangetime}</code></b>  | Returns the time since Jan 1, 1970 at which the client's password is allowed to change, in milliseconds. If there is no restriction on when the client may change its password, this variable is set to the time of the logon. |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.pwdmustchangetime}</code></b> | Returns the time since Jan 1, 1970 at which the client's password expires, in milliseconds. If the password does not expire, this variable returns null.   |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.user.displayname}</code></b>  | Returns the friendly name of the client if this has been defined in the Active Directory. This name is used only for display purpose and not security purposes.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.user.name}</code></b>         | Returns the client's Windows 2000 UserName in the SamAccountName property, if this has been defined in the Active Directory.   |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.logonscript}</code></b>       | Returns the path to the client's logon script, if this has been defined in the Active Directory.   |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.profilepath}</code></b>       | Returns the path to the client's profile, if this has been defined in the Active Directory.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.homedir}</code></b>           | Returns the path to the client's home directory, if this has been defined in the Active Directory. This may be either a local path name or a UNC path name.  |
| <b><code>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.homedirshare}</code></b>      | If the client's home directory is a UNC path name, this variable returns the share on the remote file  |

| Variable  | Description  |
|---|--|
| <code>&lt;index&gt;.pac.logoninfo.homedrive</code>  | server that is mapped to the local drive letter specified in this variable. This variable will return a value only if it has been defined in the Active Directory.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.logoncount}</code>       | Returns the count of how many times the client is currently logged on.<br><b>Note:</b> This statistic is not accurately maintained by Windows 2000 and may not be reliable.  |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.badpasswordcount}</code> | Returns the number of logon or password change attempts with bad passwords, since the last successful attempt.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.userid}</code>           | Returns the relative ID for the client.  |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.groupid}</code>          | Returns the relative ID for this client's primary group.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.groupcount}</code>       | Returns the number of groups, within the client's domain, of which the client is a member.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.groupids}</code>         | Returns an array of the relative IDs and attributes of the groups in the client's domain of which the client is a member.  |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.user.flags}</code>       | Returns information about which fields in this structure are valid. The two bits that may be set are indicated below. Having these flags set indicates that the corresponding fields in the KERB_VALIDATION_INFO structure are present and valid.<br><br>define LOGON_EXTRA_SIDS 0x0020<br>define LOGON_RESOURCE_GROUPS 0x0200 |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.servername}</code>       | Returns the NETBIOS name of the KDC which performed the AS ticket request.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.domain}</code>           | Returns the NETBIOS name of the client's domain.   |
| <code>#{kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.</code>                  | Returns a bitfield of information about the client's account. The value may be any of the following:   |



| Variable  | Description  |
|---|--|
| <b>user.accountcontrol}</b>   | USER_ACCOUNT_DISABLED (0x00000001)<br>USER_HOME_DIRECTORY_REQUIRED (0x00000002)<br>USER_PASSWORD_NOT_REQUIRED (0x00000004)<br>USER_TEMP_DUPLICATE_ACCOUNT (0x00000008)<br>USER_NORMAL_ACCOUNT (0x00000010)<br>USER_MNS_LOGON_ACCOUNT (0x00000020)<br>USER_INTERDOMAIN_TRUST_ACCOUNT (0x00000040)<br>USER_WORKSTATION_TRUST_ACCOUNT (0x00000080)<br>USER_SERVER_TRUST_ACCOUNT (0x00000100)<br>USER_DONT_EXPIRE_PASSWORD (0x00000200)<br>USER_ACCOUNT_AUTO_LOCKED (0x00000400)<br>USER_ENCRYPTED_TEXT_PASSWORD_ALLOWED (0x00000800)<br>USER_SMARTCARD_REQUIRED (0x00001000)<br>USER_TRUSTED_FOR_DELEGATION (0x00002000)<br>USER_NOT_DELEGATED (0x00004000)<br>USER_USE_DES_KEY_ONLY (0x00008000)<br>USER_DONT_REQUIRE_PREAUTH (0x00010000) |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.extrasids}</b>             | Returns list of SIDs for groups to which the user is a member. This variable returns a value only if the LOGON_EXTRA_SIDS flag has been set in the UserFlags field in the Active Directory.  |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.pac.logoninfo.resourcesids}</b>          | Returns an array of the relative IDs and attributes of the groups in the resource domain of which the resource is a member.  |
| <i>Signature Attributes</i>   |  |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.pac.kdc.signature.checksum}</b>          | Returns an array of bytes containing the checksum data. The value is Base64 encoded.   |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.pac.kdc.signature.type}</b>              | Returns the type of checksum used to create a signature. The checksum will be a keyed checksum.  |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.pac.server.signature.checksum}</b>       | Returns an array of bytes containing the checksum data. The value is Base64 encoded.   |
| <i>Relevant Attributes</i>  |  |
| <b>\${kerberos.data.authorizations.&lt;index&gt;.relevant.&lt;pac authorizations&gt;}</b> | Returns the relevant portion containing the authorizations, in a form of PAC authorization data that may include logoninfo or signatures as well. For example:<br><pre>{kerberos.data.authorizations.1.relevant.authorizations.0.pac.logoninfo.user.name}</pre> - contains PAC logoninfo user name attribute   |

## Message Layer Variables

Table 153 lists the predefined context variables related to the message layer.

**Note:** The variables in Table 153 are valid only for SOAP web services. They do not apply to XML applications.

Table 153: Context variables for message layer

| Variable   | Description  |
|--|--|
| <code>\${&lt;target&gt;.buffer.status}</code>        | Returns one of the following strings: <ul style="list-style-type: none"> <li><b>uninitialized:</b> Not yet initialized. This is the default Response before a routing assertion is executed.</li> <li><b>unread:</b> Initialized but the message body has not been read yet. This is the default Request at the start of policy processing.</li> <li><b>buffered:</b> This is the first part of message that has been read and stashed to the Stash Manager, and is available for processing.</li> <li><b>gone:</b> This is the first part of message that has been read and consumed and is no longer available.</li> </ul> |
| <code>\${&lt;target&gt;.contentType}</code>          | Content-Type the Gateway is using for the specified message; this may be a transport-specific default. Unlike the Content-Type HTTP header, this value is guaranteed to be present and non-empty for any message in the Gateway. This will always start with "multipart/" if the message has attachments.  |
| <code>\${&lt;target&gt;.mainpart}</code>             | Returns the body of the main/root MIME part, including any attachments; turns the message into a String.   |
| <code>\${&lt;target&gt;.mainPart.contentType}</code> | Content-Type the Gateway is using for the specified message's first part; this may be a transport-specific default. Unlike the Content-Type HTTP header, this value is guaranteed to be present and non-empty for any message in the Gateway. This will typically be the same as <code>\${foo.contentType}</code> unless the message has attachments.  |
| <code>\${&lt;target&gt;.mainpart.size}</code>        | Returns the actual size of the first (XML) part of the message in bytes, not including attachments.  |
| <code>\${&lt;target&gt;.originalmainpart}</code>     | Body of the main/root MIME part before any modifications made by the Gateway through DOM (such as WSS Processor decryption of encrypted elements). This is only available if the <code>audit.originalMainPart.enable</code> cluster property is set to "true".   |
| <code>\${&lt;target&gt;.parts.1}</code>              | Returns the content of the main/root MIME part of the  |

| Variable  | Description  |
|---|--|
|   | message, if it is accessible as binary data.   |
| <code>\${&lt;target&gt;.parts.1.body}</code>                | Returns the content of the main/root MIME part of the message, if it is accessible as text.  |
| <code>\${&lt;target&gt;.parts.1.contentType}</code>         | Returns the full Content-Type of the main/root MIME part of the message.   |
| <code>\${&lt;target&gt;.parts.1.header.&lt;name&gt;}</code> | Returns the main/root MIME part of the header values (for example, "header.content-id").   |
| <code>\${&lt;target&gt;.parts.1.size}</code>                | Returns the size of the main/root MIME part in bytes.  |
| <code>\${&lt;target&gt;.parts.X}</code>                     | <p>Returns the content of the <i>X</i>th MIME part of the message, if it is accessible as binary data.</p> <p><b>Tips:</b> (1) This built-in variable can be used as a multivalued context variable, with the "X" reference used in the same manner as the "[0]" indexing option. This allows you (for example) to use the variable with a Run Assertions for Each Item assertion to parse a request for a specific value. (2) When using this variable in the Run Assertions for Each Item assertion, do not include the "X" in the variable name—for example, enter "request.parts" in the "Name of Existing Multivalued Variable" field, not "request.parts.X".</p> |
| <code>\${&lt;target&gt;.parts.X.body}</code>                | Returns the content of the <i>X</i> th MIME part of the message, if it is accessible as text.  |
| <code>\${&lt;target&gt;.parts.X.contentType}</code>         | Returns the full Content-Type of the <i>X</i> th MIME part of the message.   |
| <code>\${&lt;target&gt;.parts.X.header.&lt;name&gt;}</code> | Returns the <i>X</i> th MIME part of the header values (for example, "header.content-id").   |
| <code>\${&lt;target&gt;.parts.X.size}</code>                | Returns the size of the <i>X</i> th MIME part in bytes.  |
| <code>\${&lt;target&gt;.size}</code>                        | Actual size of the entire message, including all attachments. Ignores Content-Length headers.  |
| <code>\${request.soap.envelopeNs}</code>                    | <p>Returns the namespace of the SOAP envelope in the request. Possible values include:</p> <p><i>http://schemas.xmlsoap.org/soap/envelope/</i><br/> <i>http://www.w3.org/2003/05/soap-envelope</i><br/>           null ("")</p>  |
| <code>\${request.soap.version}</code>                       | Returns the SOAP version in the request. Possible values include: 1.1, 1.2, or null ("").  |
| <code>\${request.soap.namespace}</code>                     | Returns the value of the SOAP payload namespace URI.   |

| Variable  | Description   |
|---|---|
| <code>\${request.soap.operation}</code>         | Returns the name of the SOAP operation.   |
| <code>\${response.cookie.overrideDomain}</code> | <p>Controls whether cookie domains will be overwritten. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = The Gateway may overwrite the response cookie domain with the Gateway request domain. This setting is the default.</li> <li><b>false</b> = Keep the original cookie domain.</li> </ul> <p><b>Notes:</b> (1) It is recommended that this variable be set prior to routing. This variable has no effect if there is no cookie in the context. (2) In some <a href="#">reverse proxy</a> scenarios, this variable may need to be set to 'false'.</p>  |
| <code>\${response.cookie.overridePath}</code>   | <p>Controls whether cookie paths will be overwritten. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = The Gateway may overwrite the response cookie path with the Gateway service path. This setting is the default.</li> <li><b>false</b> = Keep the original cookie path. If this path is null, then the target service path will be used (see the following example).</li> </ul> <p><i>Example of a null path:</i> Consider the HTTP routing to <code>http://host/example/test.jsp</code>. If "test.jsp" returns a null cookie path, then if <code>\${response.cookie.overridePath}</code> is set to "false", the cookie path that will be returned from the Gateway will be "/example".</p> <p><b>Notes:</b> (1) It is recommended that this variable be set prior to routing. This variable has no effect if there is no cookie in the context. (2) In some <a href="#">reverse proxy</a> scenarios, this variable may need to be set to 'false'.</p> |
| <code>\${response.soap.envelopeNs}</code>       | <p>Returns the namespace of the SOAP envelope in the response. Possible values include:</p> <p><code>http://schemas.xmlsoap.org/soap/envelope/</code><br/> <code>http://www.w3.org/2003/05/soap-envelope</code><br/> <code>null ("" )</code></p>  |
| <code>\${response.soap.version}</code>          | <p>Returns the SOAP version in the response. Possible values include: 1.1, 1.2, or null ("" ).</p>  |

## Message Routing Variables

Table 154 lists the predefined context variables related to message routing.

Table 154: Context variables for message routing

| Variable                                | Description  |
|---|--|
| <code>\${httpRouting.latency}</code>    | <p>Returns the amount of time it took, in milliseconds, to send a request to its downstream endpoint and receive a response back.</p> <p>This variable is only available after a message has been routed.</p>  |
| <code>\${httpRouting.reasonCode}</code> | <p>Returns one of the following reason codes when the HTTP routing fails:</p> <ul style="list-style-type: none"> <li>• <b>-1 (Host Not Found):</b> The Server referenced in the URL (for example, nonexistentServer.l7tech.com) cannot be reached. This code can be returned if either the host does not exist or the host is simply down.</li> <li>• <b>-2 (Bad URL):</b> The URL is incorrect. This could be caused by an incorrect character such as "#".</li> <li>• <b>-3 (Connection timeout):</b> An initial message was sent to the URL but no response was received before the connection timeout expired. The connection timeout value is defined in the assertion properties.</li> <li>• <b>-4 (Read timeout):</b> One of packets being received from the URL took longer than the read timeout value to be received. The read timeout value is defined in the assertion properties.</li> <li>• <b>-5 (Undefined):</b> An unknown type of error has occurred.</li> </ul> <p><b>Tip:</b> When the HTTP routing succeeds, this variable returns the HTTP status, which is often the same as <code>\${response.http.status}</code>.</p> |
| <code>\${httpRouting.url}</code>        | <p>Returns the Protected Service URL from the last routing assertion. This variable should be used after a routing assertion.</p> <p>When used without a suffix, the entire URL is returned. When used with one of the following optional suffixes, only that part of the URL is returned:</p> <ul style="list-style-type: none"> <li>.file</li> <li>.fragment</li> <li>.host</li> <li>.path</li> <li>.port</li> <li>.protocol</li> <li>.query</li> </ul> <p><b>Examples:</b></p> <p><code>\${httpRouting.url}</code> returns the entire Protected Service URL</p>   |

| Variable                                   | Description  |
|--|--|
|  | <p><code>\${httpRouting.url.host}</code> returns only the host name portion of the URL</p> <p><b>Note:</b> The <code>.file</code> and <code>.path</code> suffixes will usually return the same values.</p>   |
| <code>\${rawtcp.reasonCode}</code>         | <p>Sets the numeric value of the reason codes which are set regardless of the routing outcome. Below are the codes.</p> <ul style="list-style-type: none"> <li>• <b>0 (Success Route):</b> Successfully routed.</li> <li>• <b>-1 (Host Not Found):</b> The server cannot be reached. This code is returned if either the host does not exist or the host is simply down.</li> <li>• <b>-2 (Connection refused):</b> The server does not accept the connection. An incorrect port number may have been used.</li> <li>• <b>-3 (Socket timeout):</b> No response was received before the connection timeout expired.</li> <li>• <b>-4 (Data size limit exceeded):</b> The message size has exceeded the data size limit.</li> <li>• <b>-5 (Undefined):</b> An unknown type of error has occurred.</li> </ul> |
| <code>\${request.elapsedTime}</code>       | <p>Returns the amount of time, in milliseconds, between receiving the request and the time the assertion that uses the variable is executed.</p>   |
| <code>\${routingStatus}</code>             | <p>Returns the routing status:</p> <ul style="list-style-type: none"> <li>• <b>None (-1):</b> The policy contains no routing assertion or the routing assertion was never reached.</li> <li>• <b>Attempted (0):</b> The routing service was reached, but the message could not be routed successfully.</li> <li>• <b>Routed (1):</b> The routing assertion was able to successfully route the message.</li> </ul>  |
| <code>\${service.defaultRoutingURL}</code> | <p>This variable allows routing assertions to be updated when a service endpoint changes following a change in UDDI.</p> <ul style="list-style-type: none"> <li>• When the <a href="#">WSDL is under UDDI control</a>, this variable holds the value of the <code>accessPoint</code> from the <code>bindingTemplate</code> from the UDDI registry. The variable is updated when there is a change in the UDDI.</li> <li>• When the Gateway WSDL is not under UDDI control, this variable holds the value of the default routing URL from the WSDL.</li> </ul> <p>The value of this variable is used in the routing assertion when publishing a new SOAP service.</p> <p>This context variable is read only .</p>   |

| Variable                     | Description  |
|------------------------------|--|
| <code>\${service.url}</code> | <i>This context variable has been replaced by the variable <code>\${httpRouting.url}</code>. Though this variable still works, it is highly recommended that you adjust your service policies to use the new variable instead.</i> |

## Service/Policy Variables

Table 155 lists the predefined context variables related to services and policies.

Table 155: Variables for services and policies

| Variable                                | Description  |
|---|--|
| <code>\${assertion.latency.ms}</code>   | Returns the assertion latency in milliseconds.   |
| <code>\${assertion.latency.s}</code>    | Returns the assertion latency in seconds.  |
| <code>\${assertion.number}</code>       | Returns the number of the current assertion. This is a multivalued variable.   |
| <code>\${assertion.numberstr}</code>    | Returns the number of the current assertion as a string (e.g., "1.2.1.4"). This is useful for locating an assertion when viewing a service policy. For more information, see "Assertion Numbering" on page 30).            |
| <code>\${policy.guid}</code>            | Returns the GUID of the current policy. When not part of a policy fragment, this is the same as <code>\${service.policy.guid}</code> .   |
| <code>\${policy.name}</code>            | Returns the name of the current policy.  |
| <code>\${policy.version}</code>         | Returns the active revision of the current policy. When not part of a policy fragment, this is the same as <code>\${service.policy.version}</code> .   |
| <code>\${service.name}</code>           | Returns the name of the protected service (i.e., the service published on the Gateway).  |
| <code>\${service.oid}</code>            | Returns the entity ID of the service policy. This entity ID is also displayed on the [General] tab of the <a href="#">Published Service Properties</a> dialog. For more information, see "Service Properties" on page 357. |
| <code>\${service.policy.guid}</code>    | Returns the GUID of the service policy. This GUID is also displayed on the [General] tab of the Published Service Properties dialog. For more information, see "Service Properties" on page 357.                           |
| <code>\${service.policy.version}</code> | Returns the active revision of the service policy.   |

## System Variables

Table 156 lists the predefined context variables related to the Gateway nodes.

Table 156: Variables for the system

| Variable  | Description   |
|---|---|
| <code>\${ssgnode.build.detail}</code>           | Returns verbose details about the build (e.g., Layer 7 SecureSpan Suite 6.2.0 build 1234, built 20111231225544 by build at build.l7tech.com). |
| <code>\${ssgnode.build.label}</code>            | Returns the build label (e.g., 6.2m1a).   |
| <code>\${ssgnode.build.number}</code>           | Returns the build number (e.g., 1234).  |
| <code>\${ssgnode.build.version}</code>          | Returns the build version (e.g., 6.2.0).  |
| <code>\${ssgnode.build.version.major}</code>    | Returns the build major version (e.g., version 6.2.0, would return "6").  |
| <code>\${ssgnode.build.version.minor}</code>    | Returns the build minor version (e.g., version 6.2.0, would return "2").  |
| <code>\${ssgnode.build.version.subminor}</code> | Returns the build subminor version (e.g., version 6.2.0, would return "0").   |
| <code>\${ssgnode.hostname}</code>               | Returns the hostname of the node (e.g., me.l7tech.local).   |
| <code>\${ssgnode.id}</code>                     | Returns the identifier of the node in the CA API Gateway cluster.   |
| <code>\${ssgnode.ip}</code>                     | Returns the IP address of the node in the CA API Gateway cluster.   |
| <code>\${ssgnode.name}</code>                   | Returns the name of the node in the CA API Gateway cluster.   |

## Transport Layer Variables

Table 157 lists the predefined context variables related to the transport layer.

Table 157: Context variables for transport layer

| Variable  | Description  |
|---|--|
| <code>\${&lt;target&gt;.http.allheadervalue}</code> | Returns all HTTP headers and values in an array, in the format " <i>&lt;name&gt;:&lt;value&gt;</i> ".  |
| <code>\${&lt;target&gt;.http.cookies}</code>        | <p>Returns all cookies and their attributes.</p> <p>In the following example, "Cookie1" and "Cookie2" are the cookie names, while '123', '456' are the values:</p> <pre>Cookie1=123; Version=1; Domain=localhost; Path=/; Comment=test; Max-Age=60; Secure, Cookie2=456; Version=1; Domain=localhost; Path=/; Comment=test; Max-Age=60; Secure</pre> |



| Variable   | Description   |
|--|---|
|  | <p>Additional information:</p> <ul style="list-style-type: none"> <li>For the <code>\${request.http.cookies}</code>, this returns the same value as <code>\${request.http.headervalue.cookies}</code>.</li> <li>For <code>\${response.http.cookies}</code>, this returns the same value as <code>\${response.http.headervalue.set-cookies}</code>.</li> <li>If the <code>&lt;target&gt;</code> is a Message variable, then: <ul style="list-style-type: none"> <li>If the variable was saved by a response, then <code>\${MsgVar.http.cookies}</code> returns the same value as <code>\${MsgVar.http.headerValues.set-cookie}</code>.</li> <li>If the variable was <i>not</i> saved by a response, then <code>\${MsgVar.http.cookies}</code> returns the same value as <code>\${MsgVar.http.headerValues.cookie}</code>.</li> </ul> </li> </ul> |
| <code>\${&lt;target&gt;.http.cookieNames}</code>               | Returns all cookie names (repeated names are possible). For example: <i>Cookie1, Cookie2</i>  |
| <code>\${&lt;target&gt;.http.cookies.&lt;name&gt;}</code>      | <p>Returns all cookies with the given <code>&lt;name&gt;</code> and their attributes. Useful for finding cookies with the same name.</p> <p>In the following example, "repeatedName" represents a cookie name that appears more than once and '234', '567' represent the values for each instance of the repeated cookie name:</p> <pre>repeatedName=234; Version=1; Domain=localhost; Path=/; Comment=test; Max-Age=60; Secure, repeatedName=567; Version=1; Domain=layer7; Path=/; Comment=test; Max-Age=60; Secure</pre>   |
| <code>\${&lt;target&gt;.http.cookieValues.&lt;name&gt;}</code> | <p>Returns all values for cookies with the given name (repeated names are possible).</p> <p>Using the name "repeatedName" from the example above, this variable will return:</p> <pre>234, 567</pre>  |
| <code>\${&lt;target&gt;.http.header.&lt;name&gt;}</code>       | <p>Retrieves the value of the HTTP header <code>&lt;name&gt;</code> (case insensitive) for the message. For example:</p> <pre>\${request.http.header.soapaction}</pre> <p>will return the value of the SOAPAction header for that request.</p>  |
| <code>\${&lt;target&gt;.http.headerValues.&lt;name&gt;}</code> | Returns a list of all the values for the specified header   |

| Variable  | Description  |
|---|--|
|   | <p><code>&lt;name&gt;</code>, in the format:</p> <p>[value1, value2, ... , valuen]</p> <p>For requests, this variable may be useful while investigating audit details, email issues, etc. For example, you are communicating with a service on an IIS server that has NTLM enabled. There are two WWW-Authenticate headers, with the values <i>NTLM</i> and <i>Negotiate</i>. Using the <code>\$(request.http.header.www-authenticate)</code> variable will return only the <i>NTLM</i> value. Using <code>\$(request.http.headerValues.www-authenticate)</code> instead will return the literal string <i>[NTLM, Negotiate]</i>.</p> <p>For responses, this variable is useful for documentation purposes, to enumerate the contents of a header.</p> |
| <code>\$(&lt;target&gt;.jms.allpropertyvalues)</code>   | Returns all JMS properties and values in an array, in the format " <code>&lt;name&gt;:&lt;value&gt;</code> ".  |
| <code>\$(&lt;target&gt;.tcp.localAddress)</code><br><code>\$(&lt;target&gt;.tcp.localIP)</code>   | <p>Either of these variables returns the local (Gateway) side of the TCP connection's IPv4 or IPv6 address in conventional notation, or null if not applicable or unknown.</p> <p>This will be the TCP connection through which the message arrived.</p>   |
| <code>\$(&lt;target&gt;.tcp.localHost)</code>   | Returns the local (Gateway) side of the TCP connection's hostname, or else the IP address, or else null.   |
| <code>\$(&lt;target&gt;.tcp.remoteAddress)</code><br><code>\$(&lt;target&gt;.tcp.remoteIP)</code> | Either of these variables returns the remote IPv4 or IPv6 address of the TCP connection through which the Message arrived, in conventional (dotted or colon) notation, or null if not known.   |
| <code>\$(&lt;target&gt;.tcp.remoteHost)</code>  | <p>By default, this returns the IP address of the client (same as "<code>*.tcp.remoteIP</code>"). To return the hostname, enable reverse lookup by doing the following:</p> <ol style="list-style-type: none"> <li>1. Open the <a href="#">properties</a> for the <a href="#">listen port</a> whose clients should be looked up in the DNS.</li> <li>2. Select the [Advanced] tab in the properties.</li> <li>3. Click [Add] and then enter this new property:<br/> Property Name: <b>enableLookups</b><br/> Value: <b>true</b></li> <li>4. Click [OK] to close the dialogs.</li> </ol>  |
| <code>\$(&lt;target&gt;.tcp.remotePort)</code>  | Returns the TCP port number of the remote (non-Gateway) side of the TCP connection through which the   |

| Variable   | Description  |
|--|--|
|  | message arrived, or null if not known or not applicable.   |
| <code>\${request.clientid}</code>                  | <p><b>If the user has been authenticated:</b></p> <p>Returns "AuthUser:" followed by the identity provider entity ID, followed by a user identifier.</p> <ul style="list-style-type: none"> <li>For <a href="#">internal users</a>, the user identifier is the user entity ID. <b>Example:</b> internal user Alice has an entity ID = a5f3g62h221, with identity provider ID = -2. What is returned: <i>AuthUser:-2:a5f3g62h221</i>.</li> <li>For <a href="#">LDAP users</a>, the user identifier is the same as the context variable <code>\${request.authenticateduser}</code>. <b>Example:</b> <i>AuthUser:3:cn=John Smith, o=AcmeTech LLC</i>, where the identity provider ID = 3, and user identifier = cn=John Smith, o=AcmeTech LLC.</li> </ul> <p><b>If the user has not been authenticated:</b></p> <p>Returns "ClientIp:\${request.tcp.remoteAddress}", assuming the client IP is known. <b>Example:</b> <i>ClientIp:10.77.33.21</i>.</p> <p><b>If the client IP is unknown:</b></p> <p>Returns "ProtocolID:" followed by the protocol name, followed by a client endpoint identifier from the request's transport protocol.<br/><b>Example:</b> <i>ProtocolId:XMPP:johnsmith@acmetech.com</i>.</p> <p><b>If the client endpoint identifier is unknown:</b></p> <p>Returns "Protocol:" followed by the name of the transport protocol. <b>Example:</b> <i>Protocol:JMS</i>.</p> <p><b>If the protocol is unknown:</b></p> <p>Returns "ClientId:Unknown".</p> |
| <code>\${request.command.parameter.length}</code>  | Returns the length parameter to be used in PUT and GET requests.   |
| <code>\${request.command.parameter.offset}</code>  | Returns the offset parameter to be used in PUT and GET requests.   |
| <code>\${request.command.parameter.newFile}</code> | Returns the new file name parameter to be used in MOVE requests.   |
| <code>\${request.command.parameter.newPath}</code> | Returns the new file path parameter to be used in MOVE requests.   |
| <code>\${request.command.type}</code>              | Returns the values GET, PUT, LIST, STAT, MOVE, DELETE, MKDIR, or RMDIR.  |

| Variable   | Description   |
|--|---|
| <code>\${request.compression.gzip.found}</code>      | Returns a Boolean value: <ul style="list-style-type: none"> <li><b>true</b> = A message compressed with the <i>gzip</i> algorithm has been received by the Gateway</li> <li><b>false</b> = No <i>gzip</i>-compressed message has been received</li> </ul>   |
| <code>\${request.ftp.command}</code>                 | Returns the raw FTP command submitted; for example "MDTM".<br><br><b>Note:</b> In upload-only mode, this variable will always be set to STOR.   |
| <code>\${request.ftp.argument}</code>                | Returns any argument submitted with the FTP command; for example, "*.log".<br><br><b>Note:</b> This variable supersedes <code>\${request.ftp.file}</code> , which returns the same value as <code>\${request.ftp.argument}</code> .   |
| <code>\${request.ftp.file}</code>                    | Returns the same value as <code>\${request.ftp.argument}</code> above.  |
| <code>\${request.ftp.path}</code>                    | Returns the current working directory for the FTP session.  |
| <code>\${request.ftp.secure}</code>                  | Used to check if a secure transport is in use; returns a Boolean value: <ul style="list-style-type: none"> <li><b>true</b> = FTPS used</li> <li><b>false</b> = FTP used</li> </ul>  |
| <code>\${request.ftp.unique}</code>                  | <b>NOTE:</b> This variable is no longer used as of version 8.2. To determine whether the 'STOU' command was used, test for <code>\${request.ftp.command}=STOU</code> .<br><br>Returns a Boolean value: <ul style="list-style-type: none"> <li><b>true</b> = Client has used the 'STOU' command to upload a unique file.</li> <li><b>false</b> = Client has used any other command (for example, LIST, SIZE, RETR, MDTM, etc.).</li> </ul> |
| <code>\${request.http.method}</code>                 | Returns the HTTP verb for the request, if it arrived over HTTP; for example, GET, POST or DELETE. If the published service enables "Other" HTTP methods, then any arbitrary string may be returned as the HTTP verb. In this case, the method should be validated in policy before being passed through to a protected service.   |
| <code>\${request.http.parameter.&lt;name&gt;}</code> | Retrieves the value of an HTTP parameter with the name "<name>" for the request. Request parameters are extra information sent with the request. For HTTP   |

| Variable  | Description   |
|---|---|
|   | <p>servlets, parameters are contained in the query string or posted form data.</p> <p><b>Note:</b> If the parameter contains multiple values and you wish to capture all the values, use the following context variable instead. Otherwise, only the first value in the parameter will be captured in this variable.</p> <p><b>Tip:</b> If the parameter contains multiple values and you wish to only one of the values, use the indexing feature—for example, "<i>name[0]</i>" to retrieve the first value, "<i>name[1]</i>" to retrieve the second value, etc. For more information on using this feature, see "Working with Multivalued Context Variables" on page 558.</p> |
| <code>\${request.http.parameters.&lt;name&gt;}</code> | <p>Same as <code>\${request.http.parameter.&lt;name&gt;}</code>, except this variable allows you to retrieve all values from an HTTP parameter with multiple values. This creates a multivalued context variable.</p> <p>For more information on multivalued variables, see "Working with Multivalued Context Variables" on page 558.</p>   |
| <code>\${request.http.secure}</code>                  | <p>Returns a Boolean value:</p> <p><b>true</b> = request came through an SSL port</p> <p><b>false</b> = request did not come through an SSL port</p>  |
| <code>\${request.http.uri}</code>                     | <p>Returns the HTTP URI for the request; for example: <code>/sso/soap</code></p> <p>For more information about the URI, see <a href="http://en.wikipedia.org/wiki/Uniform_Resource_Identifier">http://en.wikipedia.org/wiki/Uniform_Resource_Identifier</a></p>   |
| <code>\${request.jms.property.&lt;name&gt;}</code>    | <p>Retrieves the value of a JMS property (case sensitive) for the request. For example:</p> <p><code>\${request.jms.property.SOAPJMS_soapAction}</code></p> <p>will return the value of the SOAPAction property for that request.</p>   |
| <code>\${request.ssh.file}</code>                     | <p>Returns the name of the file being uploaded (for example, 'message.xml').</p>  |
| <code>\${request.ssh.path}</code>                     | <p>Returns the upload directory for the file; this is '/' on initial login.</p>   |
| <code>\${request.ssl.ciphersuite}</code>              | <p>Returns the name of the cipher suite in use for the TLS connection over which this request arrived, if any. Valid only for HTTPS connections.</p>  |

| Variable                                | Description   |
|---|---|
|   | Example: "TLS_DHE_RSA_WITH_AES_256_CBC_SHA".  |
| <code>\${request.ssl.keysize}</code>    | Returns the SSL/TLS key size in bits, if available. May only work with certain JSSE providers (SunJSSE or SSL-J). This is an indication of the security strength of the cipher suite (for example, it will show "128" for AES 128 and "256" for AES 256). It does not provide any indication of the size of the server (or client) private keys. Valid only for HTTPS connections.  |
| <code>\${request.ssl.sessionid}</code>  | Returns the SSL/TLS session identifier as a hex string, if available. May only work with certain JSSE providers (SunJSSE or SSL-J). Can be passed through to backend services in order to detect session hijacking attacks. Valid only for HTTPS connections.   |
| <code>\${request.tcp.localPort}</code>  | Returns the TCP port number of the local (Gateway) side of the TCP connection through which the Message arrived, or null if not applicable or not known. For example, this could be 8443, 8080 or any port configured on that server.<br><br><b>Note:</b> This variable is not meaningful for FTP, since there is a control and a data port.  |
| <code>\${request.tcp.listenPort}</code> | Returns the listen port number used by the Gateway. This differs from the <code>\${request.tcp.localPort}</code> variable in that it returns the actual listen port on which the request was received, not the port number in the HTTP header of the received request.<br><br><b>Note:</b> This variable is not meaningful for FTP.   |
| <code>\${request.url}</code>            | Returns the Gateway URL where the message was received. When used without a suffix, the entire URL is returned. When used with one of the following optional suffixes, only that part of the URL is returned:<br><br><ul style="list-style-type: none"> <li>.file</li> <li>.fragment</li> <li>.host</li> <li>.path</li> <li>.port</li> <li>.protocol</li> <li>.query</li> </ul> <b>Examples:</b><br><code>\${request.url}</code> returns the entire Requesting Client URL<br><code>\${request.url.host}</code> returns only the host name |

| Variable   | Description   |
|--|---|
|  | <p>portion of the URL</p> <p><code>\${request.url.query}</code> returns the query portion of the URL for the HTTP request</p> <p><b>Note:</b> The <i>.file</i> and <i>.path</i> suffixes will usually return the same values.</p>   |
| <code>\${request.url.query}</code>   | <p>Returns the query portion of the URL for the HTTP request; for example: <code>?blah=foo</code></p> <p>This variable is the same as using <code>\${request.url}</code> with the ".query" suffix.</p>  |
| <code>\${response.ftp.replycode}</code><br><code>\${&lt;variable&gt;.ftp.replycode}</code> | <p>Returns the FTP reply code of the response received over the control connection from the remote FTP server; for example: "150".</p> <p><b>Note:</b> This variable is set to "0" if the Route via FTP(S) Assertion did not receive a response or has not run yet.</p>   |
| <code>\${response.ftp.replytext}</code><br><code>\${&lt;variable&gt;.ftp.replytext}</code> | <p>Returns the message portion of the response received over the control connection from the remote FTP server; for example: "/home/user".</p> <p><b>Note:</b> This variable returns null if no data was returned or if the Route via FTP(S) Assertion did not receive a response or has not run yet.</p>   |
| <code>\${response.http.status}</code><br><code>\${&lt;variable&gt;.http.status}</code>     | <p>Returns the HTTP response status code of the message.</p> <p>If the message has been the target of the Route via HTTP(S) Assertion (that is, the HTTP response was fetched <u>to</u> this message—not to be confused with using the message as the source for the Route via HTTP(S) assertion), then the <code>http.status</code> suffix variable will record the HTTP status of the last Route via HTTP(S) assertion that targeted to this message. Otherwise, the <code>http.status</code> suffix variable will be "0" (zero).</p> |
| <code>\${response.jms.property.&lt;name&gt;}</code>  | <p>Retrieves the value of JMS property (case sensitive) for the response.</p> <p><b>Example:</b></p> <p><code>\${response.jms.property.Blah}</code> will return the value of the Blah property for that response.</p>   |

## Working with Multivalued Context Variables

Most of the predefined [context variables](#) are designed to hold only one value at a time. However, a few assertions can create context variables that can contain multiple values. These variables are known as *multivalued context variables* and they have some special handling characteristics when interpolated.

### Concatenation Options during Interpolation

When a multivalued context variable is interpolated during runtime, the default behavior is to concatenate all the values, delimited by a comma and a space. For example, the multivalued context variable `${fruits}` contains three values:

```
apple
pear
banana
```

When `${fruits}` is used inside a field in the Policy Manager, it will be expanded to this at run time:

```
apple, pear, banana
```

You can change the delimiter character by adding a pipe character ("`|`") and an optional delimiter string to the end of the context variable name, before the closing curly brace. For example, using `${fruits|!}` will return:

```
apple!pear!banana
```

You can concatenate all values without a delimiter by omitting the delimiter string:

```
${fruits} = applepearbanana
```

---

**Tip:** To change the default delimiter, set the `template.defaultMultiValueDelimiter` [cluster property](#).

---

### Converting Multivalued Context Variables into XML

Using the concatenation delimiters, it is possible to convert a multivalued context variable into valid XML code. Continuing with the example above, using `${fruits|</i><i>}` will return:

```
apple</i><i>pear</i><i>banana
```



This is nearly valid XML code. What is missing are the opening and closing tags. To do this, simply enclose the context variable within these tags: `<i>${fruits}</i><i></i></i>`. This yields:

```
<i>apple</i><i>pear</i><i>banana</i>
```

To make this a well-formed XML fragment, it needs an enclosing element for the whole list. To do this, simply add another layer of open and close tags—these tags can be anything: `<all><i>${fruits}</i><i></i></all>`. The resulting well-formed XML fragment can be used in the Set Context Variable assertion (for variables of type Message) or in the Return Template Response to Requestor assertion.

## Indexing Options during Interpolation

To extract a single value from a multivalued context variable, use the form: `"${contextVariable[n]}"`, where [n] indicates the zero-based position of the value being extracted. Using the example from above, `${fruits[0]}` will return `"apple"`, while `${fruits[1]}` will return `"pear"`.

If you specify a position that doesn't exist in the context variable, an empty string is returned and a warning is logged.

---

**Tip:** To cause the policy to fail—rather than log a warning and return an empty string—when a non-existent position is requested of the context variable, set the cluster property `template.strictMode` to `"true"`. This cluster property also determines what happens when interpolation of a regular [context variable](#) fails (for example, if you attempt to interpolate a nonexistent variable).

---

## Retrieving Number of Values in a Multivalued Variable

To retrieve the number of values stored in a multivalued context variable, use the `".length"` suffix. For example, the variable `${manyValueVariable}` contains 15 values. Using the syntax `${manyValueVariable.length}` will return `"15"`.

---

**Note:** If the `".length"` suffix is added to a single value context variable, no value will be returned and the Gateway will log a warning message.

---

## Multivalued Variables and Selectors

Some context variables can accept a suffix that you can append to modify or reformat the value that is returned. A common use of suffixes are the [Date and Time](#) variables (see "Appendix C: Context Variables" on page 517). For example, `"${myDate.millis}"` will return the millisecond timestamp for `myDate`. However, note that if `myDate` is a multivalued

variable, you cannot use a selector to return a specific value within the array—for example, "\${myDate[2].millis}" cannot be used to return the millisecond timestamp of the third date in the array. The workaround is to create a new variable to hold the value of the multivalued variable that you wish to work with.

## Context Variables for XPath

Using context variables, you can create XPath expressions that reference values that may not be known at design time. For example, you wish to create an XPath into an element whose name comes from a message and is not known in advance. For detailed information on creating and using context variables, see "Appendix C: Context Variables" on page 517.

You may use context variables in the XPath expressions of the following assertions:

- Encrypt Element
- Evaluate Request Element
- Evaluate Response Element
- Sign Element
- Require XPath Credentials

---

**IMPORTANT:** Context variables in XPath expressions are not supported in the Securespan XML VPN Client. This means that integrity or confidentiality assertions containing XPath expressions with context variables will work on the Gateway, but the assertions will fail on the Securespan XML VPN Client.

---

## Format of Context Variables in an XPath Expression

Context variables in an XPath expression require a slightly different format compared to context variables used elsewhere. For example, the standard "\${varName}" structure does not apply, so these are not valid uses of a context variable in an XPath expression:

```
/foo/bar/${varName}
/foo/bar/$varName
```

Variables in an XPath expression must follow the same format as variables used in an XPath within an XSL transformation. Using the example above, this format will achieve the desired results:

```
/foo/bar/*[local-name() = $varName]
```

**Note:** In general, context variables can be used wherever XPath function calls inside a predicate can be used. The exact rules dictating where a context variable may appear in an XPath expression is given by the XPath 1.0 grammar. For more information, see <http://www.w3.org/TR/xpath/>.

The following table lists the expressions that are supported.

Table 158: Context variables in XPath expressions

| Expression  | Context Variable Value | Result of Evaluating Expression   |
|---|------------------------|---|
| <b>\$booleanContextVar</b>  | boolean                | The Boolean value of \$booleanContextVar (true/false), similar to evaluating expressions such as "1=1" or "1=0".  |
| <b>\$stringContextVar</b>   | string                 | The string value of \${stringContextVar}, similar to evaluating an expression such as "Foo" (including the quotes).   |
| <b>\${nodeContextVar}</b>   | DOM Node               | A nodeset containing the single node contained in \${nodeContextVar}, similar to matching it in the target document. The node does not need to be from the same document as the target message.   |
| <b>//*[local-name()=\$stringContextVar]</b>   | string                 | A nodeset containing all nodes in the target message with the local name equal to the value of \${stringContextVar}.  |
| <b>/s:Envelope/s:Body/*[local-name()=\$payloadLocalName and namespace-uri()=\$payloadUri]</b> | string,<br>string      | A nodeset containing the SOAP payload element(s).<br><br>This assumes the context variables <i>\${payloadLocalName}</i> and <i>\${payloadUri}</i> are set to the expected payload element local name and namespace URI respectively, and the target message contains the expected payload element(s). |

## Fully Dynamic XPath Expressions

The Gateway also supports "fully dynamic XPath expression" from a context variable, where the entire XPath expression is given by a variable whose name is enclosed between "\${" and "}". During runtime, this expression is treated as a standard context variable, where the value is looked up and parsed as an XPath for every invocation.

*Example:*

The XPath expression `"/book/author[last()]"` can be turned into a fully dynamic XPath expression with this example policy snippet:

```
set variable ${xpathVar} as String "/book/author[last()]"
Evaluate Request XPath ${xpathVar}
```

Note that the Evaluate Response XPath assertion may also be used. The variable "\${xpathVar}" is entered into the "XPath" field in the assertion properties.

---

**Notes:** (1) Fully dynamic XPath expressions are valid only in an XPath context. (2) Currently, only these two XPath assertions support fully dynamic XPath expression: Evaluate Request XPath and Evaluate Response XPath.

---

## Context Variables for CA SiteMinder

The topic describes the context variables that are common to all the CA SiteMinder assertions:

- Check Protected Resource Against SiteMinder
- Authenticate Against SiteMinder
- Authorize via SiteMinder

All three SiteMinder assertions can set and reference the following variable:

**`${<prefix>.smcontext}`**

where the "<prefix>" is specified in the assertions. This variable contains a SiteMinder context object that can be queried for the following information using these variable:

Table 159: Context variables for CA SiteMinder

| Context Variable  | Description   |
|---|---|
| <b><code>\${&lt;prefix&gt;.smcontext.authschemes}</code></b>        | Returns an array of the authentication schemes supported by the Policy Server. The Gateway supports the following authentication schemes:<br><br>BASIC<br>SSL<br>X509CERT<br>X509CERTISSUEDN<br>X509CERTUSERDN  |
| <b><code>\${&lt;prefix&gt;.smcontext.authschemes.length}</code></b> | Returns the size of the authentication schemes array.   |
| <b><code>\${&lt;prefix&gt;.smcontext.attributes}</code></b>         | Returns the SiteMinder attributes that contain information from the CA SiteMinder Policy Server as a result of authentication/authorization attempts.<br><br>Attributes that are known to the agent have names similar to "ATTR_USERDN".<br><br>Attributes that are not known to the agent have names that begin with "ATTR" followed by a number returned from the |

Table 159: Context variables for CA SiteMinder

| Context Variable  | Description   |
|---|---|
|   | <p>Policy Server, for example: "ATTR_161".</p> <p>For a list of the attributes, see "<a href="#">SiteMinder Attributes</a>" below.</p>  |
| <code>\${&lt;prefix&gt;.smcontext.attributes.length}</code>                 | Returns the size of the attribute list.   |
| <code>\${&lt;prefix&gt;.smcontext.attributes.&lt;index&gt;.name}</code>     | <p>Returns the name of the <code>&lt;index&gt;</code> attribute.</p> <p>Example: <code>\${siteminder.smcontext.attributes.0.name}</code></p>  |
| <code>\${&lt;prefix&gt;.smcontext.attributes.&lt;index&gt;.value}</code>    | <p>Returns the value of the <code>&lt;index&gt;</code> attribute.</p> <p>Example: <code>\${siteminder.smcontext.attributes.0.value}</code></p>  |
| <code>\${&lt;prefix&gt;.smcontext.attributes.&lt;attribute_name&gt;}</code> | <p>Returns the value of the attribute specified or null if the attribute not found.</p> <p>For example, <code>\${siteminder.smcontext.attributes.SESS_DEF_REASON}</code> returns a reason value of the failed authentication/authorization session.</p>   |
| <code>\${&lt;prefix&gt;.smcontext.sourceIpAddress}</code>                   | <p>Returns the originating source IP address from the SiteMinder context. This source IP is determined as follows:</p> <ul style="list-style-type: none"> <li>• If a source IP address was specified in the Check Protected Resource Against SiteMinder Assertion, it is returned here.</li> <li>• If not specified, the remote IP of the request or response message is returned instead.</li> <li>• If the remote IP is null, then the Address value from the "SiteMinder Configuration Properties" on page 222 is returned instead (assuming the "Check IP" check box in the properties has been selected; if it has not been selected, then this variable will return NULL).</li> </ul> |
| <code>\${&lt;prefix&gt;.smcontext.ssotoken}</code>                          | <p>Returns the third party SSO Token generated by the CA SiteMinder Policy Server. This token is used to authenticate a user and can be either returned via a HTTP response or stored in a context variable for subsequent SiteMinder session validation.</p> <p>The token is set only when authentication/authorization is successful.</p>   |

Table 159: Context variables for CA SiteMinder

| Context Variable  | Description  |
|---|--|
| <code>\${&lt;prefix&gt;.smcontext.transactionid}</code> | Returns the transaction ID used by the agent to associate application activity with security activity. This ID is generated by the Check Protected Resource Against SiteMinder assertion and is used by the other SiteMinder assertions. |

## SiteMinder Attributes

The following is a list of the SiteMinder attributes that can be returned by the `${<prefix>.smcontext.attributes.<attribute_name>}` variable.

Table 160: SiteMinder attributes

| Attribute                      | Description   |
|--------------------------------|---|
| <b>ATTR_USERDN</b>             | The user's distinguished name as recognized by SiteMinder.  |
| <b>ATTR_USERNAME</b>           | The user's display name.  |
| <b>ATTR_USERMSG</b>            | This is text presented to the user as a result of authentication. Some authentication schemes supply challenge text or a reason why a authentication has failed.  |
| <b>ATTR_USERUNIVERSALID</b>    | This is the user's universal ID. It could be the name from the LDAP.  |
| <b>ATTR_CLIENTIP</b>           | The IP address of the machine where the user initiated a request for a protected resource.<br><b>Note:</b> This attribute returns a value only when the "Check IP" option is selected in the "SiteMinder Configuration Properties" on page 222. |
| <b>ATTR_DEVICENAME</b>         | The name of the agent device. In case of decoding existing SSO token, this attribute represents the CA API Gateway.   |
| <b>ATTR_IDENTITYSPEC</b>       | ID for the user identity ticket. This attribute is returned if the Web server's user-tracking feature is enabled and the Gateway receives the SSO token from another agent  |
| <b>ATTR_SESSIONID</b>          | The SiteMinder session identifier. The session identifier is returned together with ATTR_SESSIONSPEC as a result of authentication.   |
| <b>ATTR_SESSIONSPEC</b>        | The SiteMinder session specification returned from the login call.  |
| <b>ATTR_LASTSESSIONTIME</b>    | The time that the Policy Sever was last accessed within the session.  |
| <b>ATTR_STARTSESSIONTIME</b>   | The time the session started after a successful login.  |
| <b>ATTR_IDLESESSIONTIMEOUT</b> | Maximum idle time for a session. This attribute is currently available as ATTR_225.   |

Table 160: SiteMinder attributes

| Attribute   | Description   |
|---|---|
| <b>ATTR_MAXSESSIONTIMEOUT</b>                     | Maximum time a session can be active.   |
| <b>ATTR_STATUS_MESSAGE</b>                        | Status of the authentication/authorization failure.   |
| <b>ATTR_AUTH_DIR_NAME</b>                         | The name specification of the directory where the user has been authenticated.  |
| <b>ATTR_AUTH_DIR_NAMESPACE</b>                    | The namespace specification of the directory where the user has been authenticated.   |
| <b>ATTR_AUTH_DIR_OID</b>                          | The object ID of the directory where the user has been authenticated.   |
| <b>ATTR_AUTH_DIR_SERVER</b>                       | The server specification of the directory where the user has been authenticated.  |
| <b>&lt;WebAgent-HTTP-Header-Variable-Name&gt;</b> | The value returned for a configured WebAgent-HTTP-Header-Variable (defined under the "Rules" section in the Policy Server). |

## Authenticate with SiteMinder R12 Assertion

The following context variables can be set when the Authenticate with SiteMinder R12 Protected Resource assertion is used.

**Note:** The "siteminder.ATTR.\*" variables in Table 161 are valid variables that may or may not return data, depending on the configuration of the SiteMinder server. Please consult with your SiteMinder administrator to verify which attributes are available.

Table 161: Context variables created by the Authenticate with SiteMinder R12 Protected Resource assertion

| Context Variable                   | Description  |
|------------------------------------|--|
| <b>siteminder.smsession</b>        | Returns the SSO Token for the authorization. This variable is set after the assertion authenticates and authorizes the credentials provided. |
| <b>siteminder.ATTR_USERDN</b>      | Returns the distinguished name for the user, decoded from the SSO Token.   |
| <b>siteminder.ATTR_SESSIONSPEC</b> | Returns the session specification returned from the login call, decoded from the SSO Token.  |
| <b>siteminder.ATTR_SESSIONID</b>   | Returns the session ID returned from the login call, decoded from the SSO Token.   |
| <b>siteminder.ATTR_USERNAME</b>    | Returns the user's name, decoded from the SSO Token.   |
| <b>siteminder.ATTR_CLIENTIP</b>    | Returns the IP address of the machine where the user initiated   |

Table 161: Context variables created by the Authenticate with SiteMinder R12 Protected Resource assertion

| Context Variable  | Description   |
|---|---|
|   | a request for a protected resource, decoded from the SSO Token.   |
| <b>siteminder.ATTR_DEVICENAME</b>   | Returns the name of the agent that is decoding the token, decoded from the SSO Token. .                   |
| <b>siteminder.ATTR_IDLESESSIONTIMEOUT</b>                                 | Returns the maximum idle time for a session, decoded from the SSO Token.                                  |
| <b>siteminder.ATTR_MAXSESSIONTIMEOUT</b>                                  | Returns the maximum time a sessions can be active, decoded from the SSO Token.                            |
| <b>siteminder.ATTR_STARTSESSIONTIME</b>                                   | Returns the time the session started after a successful login, decoded from the SSO Token.                |
| <b>siteminder.ATTR_LASTSESSIONTIME</b>                                    | Returns the time that the Policy Server was last accessed within the session, decoded from the SSO Token. |
| <b>siteminder.response.attribute.headerVar.&lt;variable_name&gt;</b>      | Returns the HTTP header attributes from the authorization response, converted to context variables.       |
| <b>siteminder.response.attribute.headerVar.siteminder.SESS_DEF_REASON</b> | Returns the reason for an authentication or authorization failure (if failure occurred).                  |



## Appendix D: Gateway Cluster Properties

Cluster properties can be configured using the [Manage Cluster-Wide Properties](#) task. These properties affect all nodes in a cluster.

### Time Units

For cluster properties that involve time units, a shorthand abbreviation may be used for each unit; for example:

**1h** = one hour

**10m** = ten minutes

**1.5d** = 1 day 12 hours

Table 162: Gateway Cluster Properties - Time

| Unit      | Description  |
|-----------|--------------|
| <b>ms</b> | milliseconds |
| <b>s</b>  | seconds      |
| <b>m</b>  | minutes      |
| <b>h</b>  | hours        |
| <b>d</b>  | days         |

The following cluster properties are predefined in the Gateway:

### Administrative Account Cluster Properties

The following cluster properties are used to control administrative user accounts.

---

**Tip:** The "Managing Administrative User Account Policy" on page 301 task provides a convenient graphical front end to change these settings.

---

Table 163: Gateway Cluster Properties - Password

| Property                      | Description  |
|-------------------------------|--|
| <b>logon.inactivityPeriod</b> | <p>The number of days, between 0 and 365, that an account can be inactive before it disables.</p> <p>Default: <b>35</b> (days)</p> |

| Property                          | Description   |
|-----------------------------------|---|
| <b>logon.lockoutTime</b>          | The lockout time interval a user must wait after reaching the <i>logon.maxAllowableAttempts</i> before another login attempt can be made.<br>Default: <b>1200</b> (seconds)   |
| <b>logon.maxAllowableAttempts</b> | The maximum number of failed login attempts before the account is locked. For the lockout period, refer to the <i>logon.lockoutTime</i> setting.<br>Default: <b>5</b>   |
| <b>logon.sessionExpiry</b>        | The number of minutes, between 1 and 1440, that the administrative user can leave their Gateway session idle before being disconnected.<br>Default: <b>30</b> (minutes)<br><br><b>Special Note for Browser Client Users:</b> User activity may not be correctly detected when the <i>browser client</i> is used. For example, session expiry may occur even when the browser client is being used (such as during policy editing) but not accessing the Gateway. For this reason, it is recommended to avoid setting <i>logon.sessionExpiry</i> to a low value if the browser client is used. |
| <b>logon.warningBanner</b>        | A warning message that will be displayed to the user after logging into the Policy Manager. The user must accept this warning to continue or be disconnected.<br>Default: blank (no warning banner will be displayed)   |

## Audit Archiver Cluster Properties

The following cluster properties configure the FTP Audit Archiver. For more information, see [FTP Audit Archiver](#) in the *Layer 7 Policy Manager User Manual*.

Table 164: Gateway Cluster Properties - Audit Archiver

| Property                              | Description  |
|---------------------------------------|--|
| <b>audit.archiver.ftp.fileprefix</b>  | A prefix to be applied to the archived .ZIP files on the FTP server. This will make it easier to locate the audit archive files.<br>Default: <b>SSGAuditArchive-</b>   |
| <b>audit.archiver.ftp.maxfilesize</b> | The maximum file size to be uploaded. This should be large enough to accommodate the largest audit record and smaller than the file size limit of the FTP server. When this maximum is reached, a new archive file is created.<br>Default: <b>2000000000</b> (bytes) |
| <b>audit.archiverBatchSize</b>        | The number of audit records to be processed by one archiver job. Maximum is 10000.<br>Default: <b>1000</b>   |

| Property                               | Description   |
|--|---|
| <b>audit.archiverShutdownThreshold</b> | The <a href="#">FTP Audit Archiver</a> will suspend processing when the database disk usage on the Gateway exceeds this level.<br>Default: <b>90</b> (percent)            |
| <b>audit.archiverStaleTimeout</b>      | The timeout period before an in-progress archive job is considered "hung" , allowing other nodes to release the lock on the database.<br>Default: <b>120</b> (minutes)    |
| <b>audit.archiverStartThreshold</b>    | Archiving of audit records will start when database disk usage is above this threshold.<br>Default: <b>75</b> (percent)   |
| <b>audit.archiverStopThreshold</b>     | Archiving of audit records will stop when database disk usage drops below this threshold.<br>Default: <b>50</b> (percent)   |
| <b>audit.archiverTimerPeriod</b>       | The time period for scheduling the <a href="#">FTP Audit Archiver</a> task. A value of "0" (zero) disables the audit archiver scheduler.<br>Default: <b>600</b> (seconds) |
| <b>audit.archiverWarningThreshold</b>  | The Audit Archiver will issue an early warning to alert users if the current database usage is above this threshold.<br><br>Default: <b>50</b> (percent)                  |

## Audit Cluster Properties

The following cluster properties configure the various thresholds used for auditing. For more information, see Message Auditing in the *Layer 7 Policy Authoring User Manual*. Valid severity levels are listed in the [Audit Events Panel](#) of the Gateway Audit Events window.

Table 165: Gateway Cluster Properties - Audit settings

| Property                     | Description  |
|------------------------------|--|
| <b>audit.adminThreshold</b>  | The minimum level required of an administrative audit record for it to be saved to the database. Value must be a valid <a href="#">severity level</a> .<br>Default: <b>INFO</b><br><b>Note:</b> Setting this threshold to a level above INFO will prevent most administrative audits from being saved or sent to an <a href="#">audit sink</a> . |
| <b>audit.assertionStatus</b> | Use the highest <a href="#">assertion status</a> level when checking if a record should be saved. When "true", the highest level assertion status from the policy will cause the audit level for   |

| Property                                 | Description   |
|--|---|
|  | <p>the policy to be raised to be the same level. This can cause INFO messages to be logged when the audit threshold is set to WARNING. Value is a Boolean.</p> <p>Default: <b>true</b></p>  |
| <b>audit.auditDetailExcludeList</b>      | <p>Lists the <a href="#">audit message codes</a> that will be excluded during runtime. Separate each code with a space. The codes here will not be logged or visible in the <a href="#">Gateway Audit Events</a> window.</p>  |
| <b>audit.batchExternal</b>               | <p>Controls whether audit details are sent immediately or are batched when processed by any configure <a href="#">log sinks</a>.</p> <ul style="list-style-type: none"> <li><b>true</b> = audits are only output when message processing is complete; when batched, the severity filters for audits are applied</li> <li><b>false</b> = audits are output immediately; in this mode, filtering is not applied for audit details</li> </ul> <p>Default: <b>true</b></p> <p>For more information, see Audit Messages in Policy assertion and Message Auditing in the <i>Layer 7 Policy Authoring User Manual</i>.</p> |
| <b>audit.clientServicesThreshold</b>     | <p>The minimum level required for a token or policy request for it to be saved to the database. The default level of 'WARNING' effectively turns auditing off for all client services, as token/policy requests have an audit level of 'INFO'.</p> <p>Value must be a valid <a href="#">severity level</a>.</p> <p>Default: <b>WARNING</b></p>  |
| <b>audit.detailThreshold</b>             | <p>The minimum level required of an audit detail message for it to be saved to the database. Value must be a valid <a href="#">severity level</a>.</p> <p>Default: <b>INFO</b></p>  |
| <b>audit.detailThresholdRespected</b>    | <p>Use the audit detail level when checking if a record should be saved. Value is a Boolean.</p> <p>Default: <b>true</b></p>  |
| <b>audit.export.group_concat_max_len</b> | <p>The session value for the MySQL group_concat_max_len server variable set when exporting audits. Minimum value is 1024 bytes.</p> <p>Default: <b>1048576</b> (bytes)</p>  |
| <b>audit.hinting</b>                     | <p>Enable audit messages to provide hints for audited information (such as save code for the request). Value is a Boolean.</p>  |

| Property   | Description   |
|--|---|
|  | Default: <b>false</b>   |
| <b>Tip:</b> For more information on how to use the following five <i>"audit.log.*"</i> cluster properties, see "Customizing the Audit Format for Logging" on page 651. |   |
| <b>audit.log.service.headerFormat</b>  | Format for the first log message of a service audit.<br>Default: <b>Processing request for service: {3}</b>   |
| <b>audit.log.service.footerFormat</b>  | Format for the final (summary) log message of a service audit.<br>Default: <b>{1}</b>   |
| <b>audit.log.service.detailFormat</b>  | Format for details related to a service audit.<br>Default: <b>{0}: {1}</b>  |
| <b>audit.log.other.format</b>  | Format used for other (non-service) audit logs.<br>Default: <b>{1}</b>  |
| <b>audit.log.other.detailFormat</b>  | Format used for other (non-service) audit details.<br>Default: <b>{0}: {1}</b>  |
| <b>audit.lookup.cache.messageSizeLimit</b>   | The maximum audit message size the Gateway will cache from the <a href="#">audit lookup policy</a> . A value of "0" (zero) indicates unlimited size.<br>Default: <b>10485760</b> bytes  |
| <b>audit.lookup.policy.guid</b>  | The GUID of the internal policy to use for audit lookup. This property is empty if no audit lookup policy is to be used (that is, the <b>Output audit records via audit sink policy</b> check box in the <a href="#">Manage Audit Sink</a> dialog is not selected).   |
| <b>audit.messageSizeLimit</b>  | The maximum size of a message to be included in an audit event. Messages that exceed this size will not be audited; instead, "Message not audited, message size exceeds limit." will be logged. A value of "0" (zero) indicates unlimited size.<br>Default: <b>10485760</b> bytes<br><b>Note:</b> This cluster property does not apply to audits sent to an <a href="#">external audit sink</a> . |
| <b>audit.messageThreshold</b>  | The minimum level for a message at the end of processing before it will be saved to the database. Value must be a valid severity level.<br>Default: <b>WARNING</b>  |
| <b>auditmsg.override.XXXX</b>  | Override the text of audit message 'XXXX' with text of your choice. Value of this setting is the new audit message text. See "Appendix F: Audit Message Codes" on page 627 for a  |

| Property  | Description   |
|---|---|
| <p><b>Note:</b> This property is not selected from the drop-down list. Manually type in this property in the 'Key' field to use it.</p> | <p>list of all the audit message codes. Changes take effect within 30 seconds, without needing to restart the Gateway.</p> <p><b>Example:</b></p> <p>Message 6701 default text is: "Bad destination email address". Using <code>auditmsg.override.6701</code>, you change the message to "Cannot resolve the destination email address".</p> <p><b>Tip:</b> The code for an audit message is also displayed in the <a href="#">Event Details Panel</a> of the <a href="#">Gateway Audit Events</a> window.</p>  |
| <b>audit.originalMainPart.enable</b>  | <p>Enable saving the original document for requests and responses. This enables use of the ".originalMainPart" suffix for context variables of <a href="#">type</a> Message.</p> <p>Requires a Gateway restart for changes to take effect.</p> <p>Default: <b>false</b></p> <p><b>Note:</b> Enabling this option reduces performance of the Gateway and it may increase the amount of memory used during message processing. Consider reducing the maximum concurrency to compensate (see Apply Rate Limit Assertion in the <i>Layer 7 Policy Authoring User Manual</i>).</p> |
| <b>audit.purgeMinimumAge</b>  | <p>The minimum age of audit records that can be purged. Value is a positive integer.</p> <p>Default: <b>168</b> (hours)</p>   |
| <b>audit.setDetailLevel.&lt;level&gt;</b>   | <p>These cluster properties are used to override the audit level of a particular audit code. Enter a list of audit codes, separated by commas, into the appropriate <code>&lt;level&gt;</code> cluster property. The audit code will be overridden to that level for auditing purposes.</p> <p><b>Note:</b> The original levels from <a href="#">Audit Message Codes</a> will still be shown when the audits are viewed in the <a href="#">Gateway Audit Events</a> window.</p> <p>For more information, see "Overriding the Audit Level" on page 427.</p>                    |
| <b>audit.signing</b>  | <p>Controls whether audit records are signed. The signed status of an audit record is shown in the <a href="#">Gateway Audit Events</a> window. Value is a Boolean.</p> <p>Default: <b>false</b></p> <p><b>Note:</b> The Gateway currently does not support the signing of audit records using an ECC key.</p>  |
| <b>audit.sink.fallbackToInternal</b>  | <p>Controls whether auditing should fall back to the internal database if the configured <a href="#">audit sink policy</a> fails:</p>   |

| Property                             | Description   |
|--------------------------------------|---|
|                                      | <ul style="list-style-type: none"> <li><b>true</b> = audit records will be saved to the database</li> <li><b>false</b> = an error will be logged and the audit record will be lost</li> </ul> <p>Default: <b>true</b></p> <p><b>Note:</b> If the <a href="#">Audit Sink Properties</a> is configured for <i>both</i> the internal database and the audit sink, the audit record will always be saved to the database regardless of the outcome of the audit sink policy.</p>  |
| <b>audit.sink.url</b>                | <p>The default destination URL used by the audit sink policy, if the route was not customized.</p> <p>Default: <b>http://localhost:4680/</b></p>  |
| <b>log.buffer.messageSizeLimit</b>   | <p>The maximum permitted size for unformatted log messages. The minimum value is 128; any value lower than this is rounded up to 128.</p> <p>Default: <b>4096</b> (characters)</p>  |
| <b>log.buffer.parameterSizeLimit</b> | <p>The maximum permitted size for unformatted log message parameter. The minimum value is 128; any value lower than this is rounded up to 128.</p> <p>Default: <b>4096</b> (characters)</p>   |
| <b>log.filenameTemplate</b>          | <p>Defines a template of the file name pattern used for log file names.</p> <p>Default: <b>{1}_{2}_{3}.log</b></p> <p>Where:</p> <ul style="list-style-type: none"> <li><b>{1}</b> = sink name</li> <li><b>{2}</b> = generation number to distinguish rotated logs</li> <li><b>{3}</b> = unique number to resolve conflicts</li> </ul> <p>To change the format, either omit or rearrange the placeholders. For example:</p> <ul style="list-style-type: none"> <li><b>{2}_{3}.log</b> will exclude the sink name</li> <li><b>{1}_{2}_{3}_QA_Environment.log</b> will append "QA_Environment" to the log name</li> </ul> |
| <b>log.levels</b>                    | <p>Sets the logger level for a specific node.</p> <p>Default: <b>com.i7tech.level = CONFIG</b></p> <p>Multiple levels may be defined. For more information, see <i>Understanding Logging Thresholds</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <p><b>WARNING:</b> This cluster property should be modified only as directed by CA Technical Support.</p>  |
| <b>log.stdoutLevel</b>               | <p>Defines the log level to use when logging messages</p>   |

| Property               | Description  |
|------------------------|--|
|                        | captured from standard output. Value is one of: FINEST, FINER, FINE, INFO, WARNING, SEVERE.<br>Default: <b>INFO</b>  |
| <b>log.stderrLevel</b> | Defines the log level to use when logging messages captured from standard error. Value is one of: FINEST, FINER, FINE, INFO, WARNING, SEVERE.<br>Default: <b>WARNING</b> |

## Certificate Validation Cluster Properties

The following cluster properties configure the settings used for [certificate validation](#) and expiration checking:

**Note:** For a listing of the acceptable time units, see Table 162.

Table 166: Gateway Cluster Properties - Certificate Validation

| Property                         | Description   |
|----------------------------------|---|
| <b>pkix.crl.cacheExpiryAge</b>   | The expiry age used by Certificate Revocation Lists (CRL), for both LDAP and HTTP caches. Value is a time unit.<br>Default: <b>5m</b>   |
| <b>pkix.crl.defaultExpiryAge</b> | The default expiry age for Certificate Revocation Lists (CRL), if the CRL does not have one already. The expiry age instructs the Gateway when to refresh the list. Value is a time unit.<br>Default: <b>1h</b>   |
| <b>pkix.crl.maxExpiryAge</b>     | The maximum allowable expiry age for a Certificate Revocation List (CRL). This value is used if the CRL's expiry age is greater than that defined by this cluster property. Value is a time unit.<br>Default: <b>7d</b>   |
| <b>pkix.crl.maxSize</b>          | The maximum size for a Certificate Revocation List (CRL). A value of "0" (zero) indicates unlimited size.<br>Default: <b>1048576</b>  |
| <b>pkix.crl.minExpiryAge</b>     | The minimum allowable expiry age for a CRL. This value is used if the CRL's expiry age is less than that defined by this cluster property. Value is a time unit.<br>Default: <b>1h</b><br><b>Note:</b> If this minimum expiry age is used, then there is a chance the Gateway is using a "stale" CRL. |
| <b>pkix.csr.defaultExpiryAge</b> | The default certificate expiry age on the CSR server, in days.  |



| Property                          | Description  |
|-----------------------------------|--|
|                                   | <p>The default expiry is used for internal users without a configured expiry time or for certificates issued for LDAP users.</p> <p>Default: <b>730</b></p>  |
| <b>pkix.keyUsage</b>              | <p>Determines whether the Gateway will apply rigid enforcement of X.509 key usage. Values are:</p> <ul style="list-style-type: none"> <li>• <b>IGNORE:</b> The Gateway will accept and use certificates for purposes other than for what they were designated to be used.</li> <li>• <b>ENFORCE:</b> The Gateway will only use certificates for their stated purposes, as described in the "Key usage" and "Ext. key usage" sections in the [Details] tab of a certificate's properties. For more information, see "Chapter 3: Managing Certificates" on page 237. If a certificate does not contain key usage or extended key usage information marked as critical, then that certificate will be treated as if all possible usages are enabled (in other words, the same as the 'IGNORE' setting).</li> </ul> <p>Default: <b>ENFORCE</b></p> <p>Requires a Gateway restart for changes to take effect.</p> |
| <b>pkix.keyUsagePolicy</b>        | <p>A long XML string defining a key usage enforcement policy. Used to override the default key usage policy. For detailed information on using this cluster property, see "Appendix G: Key Usage Enforcement Policy" on page 653.</p> <p>Default: &lt;empty&gt; (system default policy will be used)</p>   |
| <b>pkix.ocsp.defaultExpiryAge</b> | <p>The default cache time for Online Certificate Status Protocol (OCSP) responses. This specifies how long the system will keep an OCSP response for an individual certificate validation attempt before discarding it and retrieving a new one. Value is a time unit.</p> <p>This default is used if the OCSP response does not include its own expiry age.</p> <p>Default: <b>1m</b></p>   |
| <b>pkix.ocsp.maxExpiryAge</b>     | <p>The maximum allowable expiry age for a cached OCSP response. This value is used if the OCSP response's expiry age is greater than that defined by this cluster property. Value is a time unit.</p> <p>Default: <b>15m</b></p>   |
| <b>pkix.ocsp.minExpiryAge</b>     | <p>The minimum allowable expiry age for a cached OCSP response. This value is used if the OCSP response's expiry age is less than that defined by this cluster property. Value is a time unit.</p> <p>Default: <b>1s</b></p>   |

| Property   | Description  |
|--|--|
| <b>pkix.ocsp.useNonce</b>                        | Specifies whether to include a nonce in the OCSP requests to protect against replay attacks. Value is a Boolean.<br>Default: <b>true</b>   |
| <b>pkix.permittedCriticalExtensions</b>          | The list of critical extensions that will be permitted when validating certificates. The value is a list of entity IDs, separated by spaces.<br>Default: <empty>   |
| <b>pkix.validation.identityProvider</b>          | The validation method for identity provider certificates. This can also be set using the <a href="#">Manage Certificate Validation</a> dialog. <ul style="list-style-type: none"> <li>• <b>validate</b> = Ensure that the certificate is valid and trusted.</li> <li>• <b>validatepath</b> = Ensure that the certificate path is valid to a <a href="#">trust anchor</a>.</li> <li>• <b>revocation</b> = Validate the certificate path and perform a revocation check using the <a href="#">revocation checking policies</a>.</li> </ul> Default: <b>validate</b>  |
| <b>pkix.validation.other</b>                     | The validation method for all certificates except for identity provider and routing. This can also be set using the <a href="#">Manage Certificate Validation</a> dialog.<br>See <i>pkix.validation.identityProvider</i> above for a description of each setting.<br>Default: <b>validate</b>  |
| <b>pkix.validation.routing</b>                   | The validation method for certificates used by the server for routing purposes (i.e., HTTPS, FTPS). This can also be set using the <a href="#">Manage Certificate Validation</a> dialog.<br>See <i>pkix.validation.identityProvider</i> above for a description of each setting.<br>Default: <b>validate</b>   |
| <b>services.<br/>certificateDiscoveryEnabled</b> | Allows the Securespan XML VPN Clients that send requests to this Gateway to securely discover this Gateway's SSL certificate without user intervention. Value is a Boolean. <ul style="list-style-type: none"> <li>• <b>true</b> = Automatic certificate discovery is enabled, without user intervention required.</li> <li>• <b>false</b> = Automatic certificate discovery is disabled. The following will need to be done in this case: <ul style="list-style-type: none"> <li>• <i>Securespan XML VPN Client running as an application:</i> When the Securespan XML VPN Client attempts to trust a server certificate for the first time, a confirmation dialog is displayed and you must explicitly accept or reject the certificate.</li> <li>• <i>Securespan XML VPN Client running as a service:</i> You must manually configure the server certificate</li> </ul> </li> </ul> |

| Property                             | Description   |
|--------------------------------------|---|
|                                      | <p>for the Securespan XML VPN Client using one of the following methods:</p> <ul style="list-style-type: none"> <li>- If the server certificate has been established, you can manually trust it by using the <b>"discover"</b> Gateway command.</li> <li>- If the server certificate has not been established, you need to manually import it using the <b>"import"</b> Gateway command.</li> </ul> <p>For information about these commands, see <i>Gateway Commands</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> <p>Default: <b>true</b></p> <p><b>Tip:</b> See also the cluster property <a href="#">admin.certificateDiscoveryEnabled</a>.</p> <p><b>Note:</b> The "Policy download service" must be enabled for the port in order for server certificate discovery to work.</p> |
| <b>trustedCert.expiryCheckPeriod</b> | <p>The delay to wait between successive trusted certificate expiry checks. Value is a time unit.</p> <p>Default: <b>12h</b></p> <p>For more information, see "Chapter 3: Managing Certificates" on page 237.</p>  |
| <b>trustedCert.expiryFineAge</b>     | <p>The period of time prior to the expiration of a trusted certificate before the Gateway logs a FINE audit event. Value is a time unit.</p> <p>Default: <b>30d</b></p>   |
| <b>trustedCert.expiryInfoAge</b>     | <p>The period of time prior to the expiration of a trusted certificate before the Gateway logs a INFO audit event. Value is a time unit.</p> <p>Default: <b>7d</b></p>  |
| <b>trustedCert.expiryWarningAge</b>  | <p>The period of time prior to the expiration of a trusted certificate before the Gateway logs a WARNING audit event. Value is a time unit.</p> <p>Default: <b>2d</b></p>   |

## Credential Caching Cluster Properties

The following cluster properties configure the caching of credentials in the Gateway.

Table 167: Gateway Cluster Properties - Credential Caching

| Property                          | Description   |
|-----------------------------------|---|
| <b>authCache.failureCacheSize</b> | The number of failed authentications to cache in memory, per Gateway node. When the cache fills up, the least recently used |

| Property                                  | Description  |
|---|--|
|   | <p>failed authentication is discarded.</p> <p>This value should be a fraction of <i>authCache.successCacheSize</i>, depending on how frequently failed authentications are retried by users, scripts, or attackers. For example, the default value of the failure cache is 10% the size of the default success cache. If you want it to be 15% the size, set this cluster property to '300'. Enter '0' (zero) to disable caching.</p> <p>Default: <b>200</b></p> <p>Requires a Gateway restart for changes to take effect.</p>   |
| <b>authCache.groupMembershipCacheSize</b> | <p>The number of group membership checks to cache, globally. Group membership information is only cached for identities that have been successfully authenticated.</p> <p>Use the following general rule to determine the membership cache size:</p> $(Groups + Failed\_Tests) * Users$ <p>Where:</p> <ul style="list-style-type: none"> <li><i>Groups</i> = Maximum number of groups that may be active at once.</li> <li><i>Failed_Tests</i> = Maximum number of failed group membership tests a user may encounter in any policy path.</li> <li><i>Users</i> = Number of users that may be active at once.</li> </ul> <p>Default: <b>5000</b></p> |
| <b>authCache.maxFailureTime</b>           | <p>The period of time to cache failed authentications.</p> <p>Set this to the maximum amount of time users must wait before their accounts can be used after any of the following actions:</p> <ul style="list-style-type: none"> <li>Account has just been unlocked</li> <li>Account has just been created</li> <li>Account has just had its password reset</li> </ul> <p>Default: <b>30000</b> (milliseconds)</p>  |
| <b>authCache.maxSuccessTime</b>           | <p>The period of time to cache successful authentications.</p> <p>Set this to the maximum amount of time you are willing to allow access to a user whose password has just been changed or account that has just been locked.</p> <p>Default: <b>60000</b> (milliseconds)</p>  |
| <b>authCache.successCacheSize</b>         | <p>The number of successful authentications to cache in memory, per Gateway node. When the cache fills up, the least recently used authentication result is discarded.</p> <p>Set this to the maximum number of user sessions that will be</p>   |

| Property  | Description  |
|---|--|
|   | <p>actively using this cluster (without load balancer node affinity) or just this node (with node affinity).</p> <p>Default: <b>2000</b></p>   |
| <b>principalSessionCache.cacheSize</b>          | <p>The maximum number of concurrent users for which the Gateway will cache group membership information. Having this information in the cache improves performance. If the number of concurrent users exceed this cluster property value, there will be a slight performance penalty as the Gateway updates the cache with new group information, replacing group membership information from the least recently used user.</p> <p>Default: <b>100</b></p> <p><b>Tip:</b> For optimal performance, adjust this cache size to match the expected number of concurrent users.</p>  |
| <b>principalSessionCache.maxPrincipalGroups</b> | <p>The maximum number of groups to cache for each user.</p> <p><i>Example:</i> The default '50' instructs the Gateway to download the first 50 groups that a user belongs to. When a user performs an action in the Policy Manager requiring a permission (for example, viewing a service policy), the downloaded groups are checked for the appropriate role assignments. However, if that user belongs to 51 groups and the desired action requires a permission from a role assignment from the 51st group, then the Gateway will be unaware of this role assignment for the user. As a result, the user would be denied permission to perform that action, plus any other actions which depend on the permissions contained in the 51st group.</p> <p>Default: <b>50</b></p> <p><b>Tip:</b> For optimal performance, adjust this cache size to the maximum number of group memberships for any one user.</p> |
| <b>principalSessionCache.maxTime</b>            | <p>How often the Gateway should check a user's group membership to obtain the relevant <a href="#">roles</a> and <a href="#">permissions</a>. The default 5 minutes provides a reasonable balance between security and performance. A value of 0 is the most secure, as this will check a user's group memberships on every action by the user. However, this setting will decrease the responsiveness of the Policy Manager (the Gateway performance is unaffected).</p> <p>Default: <b>300000</b> (milliseconds)</p>   |

## Email Cluster Properties

The following cluster properties control various aspects of mail behavior.

Table 168: Gateway Cluster Properties - Email

| Property                         | Description  |
|----------------------------------|--|
| <b>email.listenerThreadLimit</b> | The global limit on the number of processing threads that can be created to work off all email endpoints. Value must be $\geq 5$ .<br>Default: <b>25</b>                           |
| <b>mail.inConnectTimeout</b>     | The timeout period for negotiating an inbound connection for retrieving emails. Value is a time unit—see Table 162 for allowable time units.<br>Default: <b>30s</b>                |
| <b>mail.inTimeout</b>            | The timeout period when waiting for a response from the mail server to retrieve inbound email. Value is a time unit—see Table 162 for allowable time units.<br>Default: <b>60s</b> |
| <b>mail.outConnectTimeout</b>    | The timeout period for negotiating an outbound connection for sending emails. Value is a time unit—see Table 162 for allowable time units.<br>Default: <b>30s</b>                  |
| <b>mail.outTimeout</b>           | The timeout period when waiting for a response from the mail server to send outbound email. Value is a time unit—see Table 162 for allowable time units.<br>Default: <b>60s</b>    |

## Enterprise Service Manager Cluster Properties

The following cluster properties control how the Gateway interacts with the Enterprise Service Manager.

Table 169: Gateway Cluster Properties - ESM

| Property                     | Description   |
|------------------------------|---|
| <b>admin.esmInterfaceTag</b> | The name of the Interface Tag used to identify the IP address for ESM administration requests.  |
| <b>admin.esmPort</b>         | The port number used by the Enterprise Service Manager to communicate with the Gateway cluster. The port used for this cluster property must be defined as a listen port with the <b>Enable Enterprise Manager access</b> option selected.<br>For more information, see "Managing Listen Ports" on page 54 and "Listen Port Properties" on page 57.<br>Default: value from the <a href="#">cluster.httpsPort</a> property |

| Property                                  | Description   |
|---|---|
| <b>admin.esmRequestSizeLimit</b>          | The size limit in bytes for ESM administration and Node Control requests, or 0 for unlimited (Integer). A value less than 0 is invalid (the default value would be used instead).<br><br>Default: <b>10485760</b>   |
| <b>node.processControllerExternalPort</b> | The port number used by the Enterprise Service Manager to remotely manage cluster node process managers.<br><br>Default: The port that was specified when configuring the Gateway for remote access<br><br>For more information, see <i>Configuring the Gateway for Remote Access</i> in the <i>Layer 7 Installation and Maintenance Manual (Appliance Edition)</i> . |

## Fault Level Cluster Properties

The following cluster properties are the fault level defaults on the Gateway. For more information, see the Customize SOAP Fault Response assertion.

Table 170: Gateway Cluster Properties - Fault level

| Property                         | Description  |
|----------------------------------|--|
| <b>soapfault.level</b>           | Specifies the level of detail returned in a SOAP fault by the Gateway:<br><br>0 = Drop connection<br>1 = Template response<br>2 = Generic SOAP fault<br>3 = Medium details<br>4 = Full details<br><br>This level is overridden by the Customize SOAP Fault Response assertion. If returning a template response, define the template in the <i>soapfault.template</i> property.<br><br>Default: <b>2</b> |
| <b>soapfault.policyurl</b>       | Indicates whether the Gateway includes the policy download URL when returning SOAP faults. Value is a Boolean.<br><br>Default: <b>true</b>   |
| <b>soapfault.privateKeyAlias</b> | The name or alias of the private key to use when signing SOAP faults. This cluster property is only relevant when <i>soapfault.sign</i> is set to "true". The private key alias is overridden when the Customize SOAP Fault Response assertion is present.<br><br>Default: <empty> (default SSL key is used)<br><br><b>Note:</b> If the private key cannot be found, then signing will not occur.        |
| <b>soapfault.sign</b>            | Indicates whether SOAP faults should be digitally signed. This property will be used unless overridden by a Customize SOAP Fault Response  |

| Property                  | Description   |
|---------------------------|---|
|                           | <p>assertion in the policy. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = SOAP faults are digitally signed, using the key alias specified in the <i>soapfault.privateKeyAlias</i> property</li> <li><b>false</b> = SOAP faults are not signed</li> </ul> <p>Default: <b>false</b></p>  |
| <b>soapfault.template</b> | <p>Specifies the template to be used for SOAP faults returned by the Gateway. The default template is:</p> <pre>&lt;s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"&gt;   &lt;s:Body&gt;     &lt;s:Fault&gt;       &lt;faultcode&gt;s:Client&lt;/faultcode&gt;       &lt;faultstring&gt;Client Error&lt;/faultstring&gt;     &lt;/s:Fault&gt;   &lt;/s:Body&gt; &lt;/s:Envelope&gt;</pre> <p>This setting is used only when <b>soapfaultlevel</b> = 1 (Template response).</p> |

## FTP Cluster Properties

The following cluster properties define default FTP(S) listen port behavior.

The values specified below are the defaults. These values can be overridden for individual listen ports by specifying advanced properties in the [\[Advanced\]](#) tab of the [listen port properties](#).

Table 171: Gateway Cluster Properties - FTP

| Property                               | Description  |
|--|--|
| <b>ftp.anonymousLoginsEnabled</b>      | <p>The default setting indicating whether anonymous logins are permitted. Value is a Boolean.</p> <p>Default: <b>true</b></p>                                |
| <b>ftp.maxAnonymousLogins</b>          | <p>The default maximum number of concurrent anonymous users. A value of "0" (zero) indicates no limit.</p> <p>Default: <b>10</b></p>                         |
| <b>ftp.maxConcurrentLogins</b>         | <p>The default maximum number of current users permitted, including anonymous users. A value of "0" (zero) indicates no limit.</p> <p>Default: <b>10</b></p> |
| <b>ftp.maxRequestProcessingThreads</b> | <p>The default maximum number of threads the server may create to process client requests.</p> <p>Default: <b>10</b></p>                                     |
| <b>ftp.sessionIdleTimeout</b>          | <p>The default period of time the Gateway will wait before closing</p>   |



| Property                                | Description   |
|---|---|
|   | a session due to network inactivity. Enter "0" (zero) to never time out.<br>Default: <b>60</b> (seconds)                                  |
| <b>ftp.userMaxConcurrentLogins</b>      | The default maximum number of concurrent logins per user. A value of "0" (zero) indicates no limit.<br>Default: <b>10</b>                 |
| <b>ftp.userMaxConcurrentLoginsPerIp</b> | The default maximum number of concurrent logins per user, per IP address. A value of "0" (zero) indicates no limit.<br>Default: <b>10</b> |

## Global Cluster Properties

The following cluster properties affect the entire Gateway cluster.

Table 172: Gateway Cluster Properties - Global

| Property  | Description   |
|---|---|
| <b>cluster.AdminAppletPort</b>                    | The port that will be used when the Policy Manager is launched from within the Enterprise Service Manager.<br>Default: <b>9443</b><br><b>Note:</b> The port specified here must be defined as a listen port in the Policy Manager, with "Browser-based administration" enabled. For more information, see "Managing Listen Ports" on page 54 and "Listen Port Properties" on page 57.   |
| <b>cluster.hostname</b>                           | The external hostname for the cluster. This is the fully qualified domain name of the system.<br>Default: <b>\${defaultClusterHost}</b>   |
| <b>cluster.httpPort</b>                           | The external HTTP port for the cluster. It is set dynamically based on the configured HTTP listener.<br>Default: <b>\${httpPort}</b>  |
| <b>cluster.httpsPort</b>                          | The external HTTPS port for the cluster. It is set dynamically based on the configured HTTP listener.<br>Default: <b>\${httpsPort}</b>  |
| <b>cluster.replayProtection.multicast.enabled</b> | Controls whether the Protect Against Message Replay assertion will use multicast traffic to catch message IDs replayed to a different cluster node. You should set this to "false" if your Gateway is standalone. Value is a Boolean. <ul style="list-style-type: none"> <li><b>true</b> = Enable cluster-wide multicast replay protection</li> <li><b>false</b> = Disable cluster-wide multicast replay protection. In this mode, the Gateway will perform replay protection on each node</li> </ul> |

| Property | Description  |
|----------|--|
|          | <p>individually.</p> <p>Default: <b>true</b></p> <p><b>Note:</b> The Gateway cluster nodes must be restarted for changes to take effect.</p> |

## Input/Output Cluster Properties

The following cluster properties configure input/output behavior on the Gateway node or node cluster.

Table 173: Gateway Cluster Properties - I/O

| Property                               | Description   |
|--|---|
| <b>concall.globalCoreConcurrency</b>   | <p>The core number of assertions that may execute concurrently when using the Run All Assertions Concurrently assertion. This is the number of concurrent threads normally available to the assertion.</p> <p>Default: <b>32</b></p>  |
| <b>concall.globalMaxConcurrency</b>    | <p>The maximum number of assertions that may execute concurrently when using the Run All Assertions Concurrently assertion. This is a global limit across all such assertions.</p> <p>Default: <b>64</b></p> <p><b>Tip:</b> The value of <i>concall.globalMaxConcurrency</i> should not exceed twice that of <i>concall.globalCoreConcurrency</i>.</p>  |
| <b>concall.globalMaxWorkQueue</b>      | <p>The maximum number of assertions that may be waiting to execute concurrently. When this limit is reached, and the <i>concall.globalMaxConcurrency</i> value is already reached, assertions will be run serially (i.e., non concurrently) until the system catches up.</p> <p>Default: <b>64</b></p> <p><b>Tip:</b> The value of <i>concall.globalMaxWorkQueue</i> should not exceed twice that of <i>concall.globalMaxConcurrency</i>.</p> |
| <b>io.debugSsl</b>                     | <p>Indicates whether to log debug information for SSL and TLS operations. Value is a Boolean.</p> <p>Default: <b>false</b></p>  |
| <b>io.EmailListenerMessageMaxBytes</b> | <p>The maximum size of an email message, including all MIME parts. A value of "0" (zero) indicates unlimited size.</p> <p>This property affects only request messages (inbound from the client to the Gateway, outbound from the Gateway to the backend system, and inbound from the</p>  |

| Property                           | Description   |
|------------------------------------|---|
|                                    | <p>backend system to the Gateway). It has no effect on the size of response messages returned to the client via the Gateway.</p> <p>Default: <b>2621440</b> (bytes)</p>   |
| <b>io.failoverServerRetryDelay</b> | <p>The delay before retrying a failed server when using a "Round-Robin" or "Ordered Sticky with Failover" failover strategy. This setting is used by assertions with a failover strategy such as the Route via HTTP(S) and Scan Using ICAP-Enabled Antivirus assertions.</p> <p>A value of "0" (zero ) indicates that the following default delays will be used for each failover strategy:</p> <ul style="list-style-type: none"> <li>• "Ordered Sticky with Failover": <b>15m</b></li> <li>• "Round Robin": <b>5m</b></li> </ul> <p>The maximum allowable server retry delay is <math>2^{63}-1</math> milliseconds.</p> <p>Default: <b>0</b> (milliseconds)</p> |
| <b>io.httpAllowBackslash</b>       | <p>Determines whether the backslash ('\') character is permitted URLs. Values is a Boolean.</p> <p>Default: <b>false</b></p>  |
| <b>io.httpChallengeOrder</b>       | <p>Defines whether the legacy order is used in HTTP response challenges. The valid values are:</p> <ul style="list-style-type: none"> <li>• <b>reverse</b>: Use the legacy challenge order (NTLM, Negotiate, Digest, Basic)</li> <li>• <b>windows</b>: Use the Windows challenge order (Negotiate, NTLM, Digest, Basic). This setting is the default.</li> </ul>  |
| <b>io.httpCoreConcurrency</b>      | <p>The core number of concurrent active HTTP connections per node. This is a soft limit that can be temporarily exceeded if necessary. A negative number means to use a fraction of <i>io.httpMaxConcurrency</i>. For example, "-5" would mean 1/5 of the maximum.</p> <p>Default: <b>185</b></p>   |
| <b>io.httpDefaultContentType</b>   | <p>The value of the "Content-Type" HTTP header to use if a response does not have a "Content-Type" header.</p> <p>If a value is configure for this cluster property and the Gateway encounters a response without a "Content-Type" header, <a href="#">audit message 4049</a> is generated.</p> <p>The value can include parameters, such as "text/xml; charset=utf-8". If the value is not valid, it is ignored and a warning is logged.</p>   |

| Property                              | Description  |
|---------------------------------------|--|
|                                       | There is no default value for this property.   |
| <b>io.httpDisableKeepAlive</b>        | <p>Disable HTTP Keep-Alive connections for outbound HTTP connections (other than routing assertions. Value is a Boolean.</p> <p>Default: <b>false</b></p>  |
| <b>io.httpExpectContinue</b>          | <p>Use an "Expect: 100-continue" header during HTTP routing, which can improve efficiency when authenticating. Value is a Boolean.</p> <p>Default: <b>false</b></p>  |
| <b>io.httpMaxConcurrency</b>          | <p>The maximum number of concurrent HTTP and HTTPS connections (per node) that can be active simultaneously without causing delays. Changes to this setting will take effect within 30 seconds.</p> <p>Default: <b>215</b></p> <p><b>IMPORTANT:</b> The value of <i>io.httpMaxConcurrency</i> is closely linked to the <i>c3p0DataSource.maxPoolSize</i> setting within the <i>node.properties</i> file. If you need to increase the value of <i>io.httpMaxConcurrency</i>, please contact <a href="#">CA Technical Support</a> for assistance.</p>  |
| <b>io.httpResponseStreamUnlimited</b> | <p>Allows the Gateway to ignore the message size limit when streaming HTTP responses. Value is a Boolean.</p> <p>Default: <b>true</b></p>  |
| <b>io.httpResponseStreaming</b>       | <p>Allows the Gateway to stream responses back to the client in some cases. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true:</b> The Gateway will stream a response to a request that arrived over HTTP if the response is produced by a routing assertion that supports streaming (such as HTTP or SSH routing) and there is nothing in the service policy that requires examination of the response by the Gateway. When streaming is in effect, the response body is not buffered by the Gateway before being returned to the client. This can greatly reduce the overall latency, especially for large responses. This setting is the default.</li> </ul> <p>Observe the following issues when enabling streaming: (1) streamed responses may not be accessible by the <a href="#">Audit Sink</a> policy, and (2) the client should have its own provisions for protecting itself if your service policy contains no logic for checking the response.</p> <ul style="list-style-type: none"> <li><b>false:</b> The Gateway will always buffer the entire</li> </ul> |

| Property  | Description   |
|---|---|
|   | response before returning it to the client, regardless of whether the policy requires an examination of the response. This setting restores pre-v6.1.5 behavior.  |
| <b>io.httpVersion</b>                                 | <p>Sets the HTTP version used by the routing assertions.</p> <p><b>Note:</b> If set to "1.0", the cluster property <i>io.httpExpectContinue</i> will be ignored.</p> <p>Default: <b>1.1</b></p> <p><b>Tip:</b> The default value may be overridden during HTTP (S) routing through the <b>[Request HTTP Rules]</b> tab in the Route via HTTP(S) assertion.</p>  |
| <b>io.https.response.truncationProtection.disable</b> | <p>Disables response truncation attack protection for outbound HTTPS. Value is a Boolean.</p> <ul style="list-style-type: none"> <li>• <b>true:</b> A "possible truncation attack?" exception while reading a response from a TLS server will be treated as an end-of-file indication.</li> <li>• <b>false:</b> Truncation attacks will be handled normally. This setting is the default.</li> </ul> <p><b>IMPORTANT:</b> Do not change this property unless directed by CA Technical Support.</p>  |
| <b>io.httpsHostAllowWildcard</b>                      | <p>Determines whether wildcards are permitted when verifying hostnames:</p> <ul style="list-style-type: none"> <li>• <b>true</b> = the wildcard character "*" is permitted when verifying server hostnames against the certificate name</li> <li>• <b>false</b> = the wildcard character is not permitted; the server hostname must be explicit</li> </ul> <p>Default: <b>false</b></p> <p>For more information, see "Wildcard Matching of Hostnames" on page 234.</p>  |
| <b>io.httpsHostVerify</b>                             | <p>Enables verification of server names against certificates, for certificates that are not trusted and which have not been signed by another trusted certificate.</p> <ul style="list-style-type: none"> <li>• <b>true</b> = The server name is verified against the name on the certificate. A mismatch will cause a validation failure.</li> <li>• <b>false</b> = The server name is not verified against the name on the certificate. A mismatch will not result in a validation failure.</li> </ul> <p>Default: <b>true</b></p> <p><b>Note:</b> This setting works in conjunction with the "Verify</p> |

| Property                                | Description   |
|---|---|
|   | Hostnames for Outbound SSL Connections" setting for a certificate. For more information, see "Editing a Certificate" on page 247.   |
| <b>io.jmsConnectionCacheMaxAge</b>      | <p>The maximum age for a cached JMS connection. Enter '0' (zero) for no time limit. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>10m</b></p>   |
| <b>io.jmsConnectionCacheMaxIdleTime</b> | <p>The maximum time an idle JMS connection will be cached. Enter '0' (zero) for no time limit. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>5m</b></p>   |
| <b>io.jmsConnectionCacheMaxSize</b>     | <p>The number of JMS connections to cache; this is not a hard limit. Enter "0" (zero) to disable caching for JMS connections. This is required when WebLogic JMS destinations are involved.</p> <p>Default: <b>100</b></p> <p><b>Note:</b> The cache size is a "soft" limit that may be exceeded under certain circumstances; the following are two examples:</p> <ul style="list-style-type: none"> <li>• There are hundreds of concurrent requests using JMS routing, each with a distinct connection. In this case, there would be as many JMS connections as there are requests, even if this exceeds the <i>io.jmsConnectionCacheMaxSize</i> property.</li> <li>• If <a href="#">template outbound destinations</a> are used, it is possible to create new queue connections dynamically (one per request). In this case, the cache size may be exceeded until eligible cached connections are removed.</li> </ul> |
| <b>io.jmsConsumerConnections</b>        | <p>Sets the default number of inbound JMS consumer connections allowed for a particular JMS destination, across the entire cluster.</p> <p>This value can be overridden for individual JMS destinations via the <a href="#">[Inbound Options] tab</a> of the "JMS Destination Properties" on page 96.</p> <p>Default: <b>1</b></p>  |
| <b>io.jmsMessageMaxBytes</b>            | <p>The maximum size of a JMS message, including all MIME parts. A value of "0" (zero) indicates unlimited size.</p> <p>This property affects only request messages (inbound from the client to the Gateway, outbound from the</p>   |

| Property                               | Description   |
|--|---|
|  | <p>Gateway to the backend system, and inbound from the backend system to the Gateway). It has no effect on the size of response messages returned to the client via the Gateway.</p> <p>Default: <b>2621440</b> (bytes)</p>   |
| <b>io.jmsRoutingMaxRetries</b>         | <p>The maximum number of connection attempts for an outbound <a href="#">JMS Queue</a>.</p> <p>Default: <b>5</b></p>  |
| <b>io.jmsRoutingRetrySleep</b>         | <p>The length of time to sleep after a connection error for an outbound <a href="#">JMS Queue</a>.</p> <p>Default: <b>1s</b></p>  |
| <b>io.mqConnectionCacheMaxAge</b>      | <p>The maximum age for a cached MQ native connection. Enter '0' (zero) for no time limit. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>10m</b></p>   |
| <b>io.mqConnectionCacheMaxIdleTime</b> | <p>The maximum time an idle MQ native connection will be cached. Enter "0" (zero) for no time limit. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>5m</b></p>   |
| <b>io.mqConnectionCacheSize</b>        | <p>The number of MQ native connections to cache; this is not a hard limit. Enter "0" (zero) to disable caching for MQ native connections.</p> <p>Default: <b>100</b></p> <p><b>Note:</b> The cache size is a "soft" limit that may be exceeded under certain circumstances; the following are two examples:</p> <ul style="list-style-type: none"> <li>• There are hundreds of concurrent requests using MQ native routing, each with a distinct connection. In this case, there would be as many MQ connections as there are requests, even if this exceeds the <i>io.mqConnectionCacheMaxSize</i> property.</li> <li>• If <a href="#">template outbound queues</a> are used, it is possible to create new queue connections dynamically (one per request). In this case, the cache size may be exceeded until eligible cached connections are removed.</li> </ul> |
| <b>io.mqMessageMaxBytes</b>            | <p>The maximum size of an MQ Native message, including all MIME parts. A value of "0" (zero) indicates unlimited size.</p>  |

| Property                         | Description  |
|----------------------------------|--|
|                                  | <p>This property affects only request messages (inbound from the client to the Gateway, outbound from the Gateway to the backend system, and inbound from the backend system to the Gateway). It has no effect on the size of response messages returned to the client via the Gateway.</p> <p>Default: <b>2621440</b> (bytes)</p>   |
| <b>io.mqResponseTimeout</b>      | <p>The length of time the Route via MQ Native assertion will wait for a response on the replyTo queue before timing out.</p> <p>This value may be overridden in the "MQ response timeout" field in the assertion's properties.</p> <p>Default: <b>10000</b> (milliseconds)</p>   |
| <b>io.mqRoutingMaxRetries</b>    | <p>The maximum number of connection attempts for an outbound <a href="#">MQ Queue</a>.</p> <p>Default: <b>5</b></p>  |
| <b>io.mqRoutingRetrySleep</b>    | <p>The length of time to sleep after a connection error for an outbound <a href="#">MQ Queue</a>.</p> <p>Default: <b>1s</b></p>  |
| <b>io.mqRoutingSetAllContext</b> | <p>Determines which MQ message descriptors can be set. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = All MQ message descriptors can be set, with the exception of the following: <ul style="list-style-type: none"> <li><i>backoutCount</i></li> <li><i>messageSequenceNumber</i></li> <li><i>originalLength</i></li> </ul> </li> <li><b>false</b> = When adding a new message descriptor, only the MQ message descriptors visible in the "Name" drop-down list can be set (see "Customizing MQ Messages" on page 122). This setting is the default.</li> </ul> <p><b>Tip:</b> For a list of all the MQ message descriptors, refer to the "Class MQMessage" page on the IBM WebSphere web site.</p> |
| <b>io.outConnectTimeout</b>      | <p>The maximum time to wait for a connection to be established for routing. If exceeded, routing will fail (or failover). This timeout can be overridden for a specific routing assertion through the HTTP(S) Routing Properties.</p> <p>Default: <b>30000</b> (milliseconds)</p>  |



| Property                     | Description   |
|------------------------------|---|
| <b>io.outTimeout</b>         | <p>The maximum time allowed for some response data to be read for the outbound request. If exceeded, routing will fail (or failover). This timeout can be overridden for a specific routing assertion through the HTTP(S) Routing Properties.</p> <p>Default: <b>60000</b> (milliseconds)</p>   |
| <b>io.rateLimit</b>          | <p>The minimum permissible rate for incoming requests.</p> <p>Default: <b>1024</b> (bytes per second)</p>   |
| <b>io.rateTimeout</b>        | <p>The IO time-out period for incoming request rate checking.</p> <p>Default: <b>60000</b> (milliseconds)</p>   |
| <b>io.signedPartMaxBytes</b> | <p>The maximum size of attachments permitted for signature processing. A value of "0" (zero) indicates unlimited size.</p> <p>This property is enforced for any signed message part that is processed for security.</p> <p>Default: <b>5242880</b> (bytes)</p>  |
| <b>io.staleCheckCount</b>    | <p>Number of stale checked connections per interval.</p> <p>Default: <b>1</b></p>   |
| <b>io.staleCheckHosts</b>    | <p>Maximum number of stale checked hosts.</p> <p>Default: <b>10</b></p>   |
| <b>io.timeout</b>            | <p>The IO time-out for incoming requests. This is the amount of time the Gateway will wait for data from the client before timing out.</p> <p>Default: <b>60000</b> (milliseconds)</p>  |
| <b>io.xmlPartMaxBytes</b>    | <p>The maximum size of the XML part of a message (part 1). When the maximum message size is reached, a SOAP fault '500' is returned. A value of "0" (zero) indicates unlimited size.</p> <p>This property is enforced for any message (if not MIME), or the first part of a MIME message if XML.</p> <p>This property is not enforced for responses or requests set within the policy. For example, a response created by the Return Template Response to Requestor or Copy Request Message to Response assertions that exceeds the size specified by <i>io.xmlPartMaxBytes</i> will not trigger an error.</p> <p>Note that this property is not intended to be used with small values; the setting is intended to constrain usage of</p> |

| Property                                   | Description   |
|--|---|
|  | <p>Gateway resources, rather than enforcing an arbitrary size limit (use the Limit Message Size assertion for that).</p> <p>Default: <b>2621440</b> (bytes)</p> <p><b>Notes:</b> (1) If compression is in effect, this cluster property applies to the <i>uncompressed</i> message size. (2) The Route via Raw TCP assertion uses a different method of restricting message size. (3) If <i>io.xmlPartMaxBytes</i> is not returning correct results, try setting <a href="#">io.httpResponseStreamUnlimited</a> to "false".</p> |
| <b>jms.connectErrorSleep</b>               | <p>The amount of time to wait after an inbound JMS connection error before attempting to connect again. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>60s</b></p>   |
| <b>jms.listenerThreadLimit</b>             | <p>The global limit on the number of processing threads that can be created to work off all JMS endpoints. Value must be <math>\geq 5</math>.</p> <p>Default: <b>25</b></p>   |
| <b>jms.ResponseTimeout</b>                 | <p>The length of time the Route via JMS assertion will wait for a response on the replyTo queue before timing out.</p> <p>This value may be overridden in the "JMS response timeout" field in the assertion's properties.</p> <p>Default: <b>10000</b> (milliseconds)</p>   |
| <b>mq.connectErrorSleep</b>                | <p>The amount of time to wait after an inbound MQ Native connection error before attempting to connect again. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>60s</b></p> <p><b>Note:</b> Changes to this cluster property require a listener or Gateway restart to take effect. One way to restart the listener is to edit and save the <a href="#">MQ Native configuration</a>.</p>   |
| <b>mq.listenerMaxConcurrentConnections</b> | <p>The maximum number of concurrent connections allowed for any inbound MQ Native queue.</p> <p>Default: <b>1000</b></p> <p><b>Notes:</b> (1) The limit specified here will override any larger value specified in the queue properties (in the <a href="#">[Inbound Options]</a> tab of "MQ Native Queue Properties" on page 114). (2) Changes to this cluster property require a listener or Gateway restart to take effect.</p>  |
| <b>mq.listenerPollingInterval</b>          | <p>The time to wait when polling for messages on an empty</p>   |

| Property                                    | Description   |
|---|---|
|   | <p>queue. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>5s</b></p> <p><b>Note:</b> Changes to this cluster property require a listener or Gateway restart to take effect. One way to restart the listener is to edit and save the <a href="#">MQ Native configuration</a>.</p>  |
| <b>mq.listenerThreadLimit</b>               | <p>The global limit on the number of processing threads that can be created to work off all MQ endpoints. Value must be <math>\geq 5</math>. Requires a Gateway restart for changes to take effect.</p> <p>Default: <b>25</b></p> <p><b>Note:</b> Changes to this cluster property require a Gateway restart to take effect.</p>  |
| <b>mq.preventAuditFloodPeriod</b>           | <p>A time period used to prevent audit message flooding by the MQ Native listener. If the most recent listener audit message occurred within this period, the next listener message will just be logged (no audit record will be created). A value of "0" (zero) indicates not audit flood throttling. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>0s</b></p> <p><b>Note:</b> Changes to this cluster property require a listener or Gateway restart to take effect. One way to restart the listener is to edit and save the <a href="#">MQ Native configuration</a>.</p> |
| <b>sftpPolling.ignoredFileExtensionList</b> | <p>Defines the list of file extensions to be ignored during <a href="#">SFTP polling</a>.</p> <p>Default: <b>.filepart</b></p> <p><b>Note:</b> Changes to this cluster property require any SFTP polling listeners to be restarted before the new setting takes effect.</p>   |
| <b>ssh.routingEnabledCiphers</b>            | <p>Defines the list of ciphers to enable for SSH2 routing (comma separated). The following are the permitted values:</p> <ul style="list-style-type: none"> <li>aes128-ctr</li> <li>aes192-ctr</li> <li>aes256-ctr</li> <li>aes128-cbc</li> <li>aes192-cbc</li> <li>aes256-cbc</li> <li>blowfish-cbc</li> <li>3des-cbc</li> </ul> <p>Default: <b>aes128-ctr, aes128-cbc, 3des-cbc,</b></p>  |

| Property  | Description   |
|---|---|
|   | <b>blowfish-cbc, aes192-ctr, aes192-cbc, aes256-ctr, aes256-cbc</b>   |
| <b>ssh.routingExplicitlyValidateDeleteFile</b>        | <p>During SSH routing, this property determines the validation during file deletion. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true:</b> The Gateway verifies that a file to be deleted actually exists and that is a file. This setting is the default.</li> <li><b>false:</b> No verification is performed on whether or not a file being deleted actually exists.</li> </ul>   |
| <b>ssh.routingExplicitlyValidateDeleteDir</b>         | <p>During SSH routing, this property determines the validation during directory deletion. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true:</b> The Gateway verifies that a directory to be deleted actually exists and that is a directory. This setting is the default.</li> <li><b>false:</b> No verification is performed on whether or not a directory being deleted actually exists.</li> </ul>                             |
| <b>ssh.session.pool.maxActive</b>                     | <p>The maximum number of sessions (per key) that can be allocated by the pool (checked out to client threads) at one time. Set to <b>-1</b> for no limit to the number of sessions per key.</p> <p>Once the maximum number of sessions is reached, the session pool is exhausted, at which point the assertion fails. The maximum value is 1000.</p> <p>Default: <b>10</b></p>  |
| <b>ssh.session.pool.minEvictableIdleTimeMillis</b>    | <p>The minimum amount of time an object can remain idle in the pool before it is eligible for eviction.</p> <p>Default: <b>600000</b> (milliseconds)</p>  |
| <b>ssh.session.pool.timeBetweenEvictionRunsMillis</b> | <p>The amount of time to sleep between examining idle objects for eviction. Set to <b>0</b> or <b>-1</b> to have the session remain idle forever.</p> <p>Default: <b>1800000</b> (milliseconds)</p>   |
| <b>ssh.sftpRoutingExplicitlyValidateMkdir</b>         | <p>During SSH routing, this property determines that a directory of the same name does not exist before attempting to create it. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true:</b> The Gateway verifies that a directory or file of the same name does not exist. This setting is the default.</li> <li><b>false:</b> No verification is performed on whether or not a directory of the same name actually exists.</li> </ul> |

## JDBC Cluster Properties

The following cluster properties are used in JDBC connections and JDBC queries.

Table 174: Gateway Cluster Properties - JDBC

| Property   | Description  |
|--|--|
| <b>jdbcConnection.driverClass.defaultList</b>          | <p>The list of supported database driver classes for <a href="#">JDBC connections</a>. Enter each driver class on a new line.</p> <p>Default:</p> <pre>com.mysql.jdbc.Driver com.l7tech.jdbc.mysql.MySQLDriver com.l7tech.jdbc.db2.DB2Driver com.l7tech.jdbc.oracle.OracleDriver com.l7tech.jdbc.sqlserver.SQLServerDriver</pre> <p><b>Note:</b> Before attempting to modify the default list of supported driver classes, be sure to see "<a href="#">Understanding the Driver Classes</a>" in "JDBC Connection Properties" on page 83.</p> |
| <b>jdbcConnection.pooling.maxPoolSize.defaultValue</b> | <p>The default maximum number of connections a pool will maintain at any given time. Used in the "JDBC Connection Properties" on page 83.</p> <p>Default: <b>15</b></p>  |
| <b>jdbcConnection.pooling.minPoolSize.defaultValue</b> | <p>The default minimum number of connections a pool will maintain at any given time. Used in the "JDBC Connection Properties" on page 83.</p> <p>Default: <b>3</b></p>   |
| <b>jdbcQuery.maxBlobSizeOut</b>                        | <p>The maximum size allowed for a BLOB output variable from a Procedure or Function call. The default is 10MB. Enter <b>0</b> (zero) for no maximum size.</p> <p>Default: <b>10485760</b> (bytes)</p>  |
| <b>jdbcQuery.maxClobSizeOut</b>                        | <p>The maximum size allowed for a CLOB output variable from a Procedure or Function call. The default is 10MB. Enter <b>0</b> (zero) for no maximum size.</p> <p>Default: <b>10485760</b> (bytes)</p>  |
| <b>jdbcQuery.maxRecords.defaultValue</b>               | <p>The default maximum number of records allowed to return from querying a <a href="#">JDBC connection</a>. Used in the Perform JDBC Query assertion.</p> <p>Default: <b>10</b></p>  |
| <b>jdbcQueryManager.cacheCleanUpInterval</b>           | <p>Interval between when the background cleanup task is run to clear cached exceptions. The default is 1 minute. Enter <b>0</b> (zero) to disable cache cleanup.</p> <p>Default: <b>60000</b> (milliseconds)</p>   |

| Property  | Description   |
|---|---|
| <b>jdbcQueryManager.<br/>cacheKeyNoUsageExpiration</b>  | Maximum expiration for a managed meta data cache key. The default is 31 days. Set to <b>0</b> (zero) for no expiration.<br><br>Default: <b>2678400</b> (seconds)  |
| <b>jdbcQueryManager.<br/>cacheMetaData.enable</b>       | Permit or disallow caching of procedure or function metadata. If enabled, lazy caching will happen as meta data is downloaded. Connections referenced via a context variable will always require lazy caching. Value is a Boolean.<br><br>Default: <b>true</b><br><br><b>Tip:</b> This property does not affect existing cached data and does not stop background tasks from checking cached data. This allows caching to be turned on and off without causing all existing cached data to be lost. For more information about caching, see "Caching Metadata" in the Perform JDBC Query assertion. |
| <b>jdbcQueryManager.<br/>cacheMetaDataTask.enable</b>   | Enable or disable the background task to eagerly cache procedure or function meta data. Value is a Boolean.<br><br>Default: <b>true</b>   |
| <b>jdbcQueryManager.<br/>cacheRefreshInterval</b>       | Interval in milliseconds between when background task to update meta data cache is ran. The default is 10 minutes. Set to <b>0</b> (zero) for no refresh.<br><br>Default: <b>600000</b> (milliseconds)  |
| <b>jdbcQueryManager.<br/>cacheStaleTimeout</b>          | Maximum cache age of meta data. Any cached meta data older than this value will be cleared from the cache. The default is 30 minutes. Set to <b>0</b> (zero) for no timeout.<br><br>Default: <b>1800</b> (seconds)  |
| <b>jdbcQueryManager.<br/>cacheTaskStatementTimeout</b>  | The maximum statement query time allowed for queries from the meta data cache background task. Set to <b>0</b> (zero) to use the Gateway-wide timeout.<br><br>Default: <b>120</b> (seconds)<br><br><b>Note:</b> This property is ignored if it is larger than the Gateway-wide timeout defined by <a href="#">queryManager.maxGatewayStatementTimeout</a> .   |
| <b>jdbcQueryManager.<br/>maxGatewayStatementTimeout</b> | The maximum statement query time allowed on the Gateway. This is a Gateway-wide timeout. The default is 5 minutes. Minimum is 1 second.<br><br>Default: <b>300</b> (seconds)  |
| <b>jdbcQueryManager.<br/>minCacheConcurrency</b>        | The number of threads used by the background cache meta data task. Maximum value is 200, minimum value is 1.<br><br>Default: <b>10</b><br><br><b>Note:</b> When changing the value of this property, consider the number of JDBC connections in use for procedures and functions  |

| Property | Description  |
|----------|--|
|          | on the Gateway, and how this background task will affect available connections for those JDBC connections. For example, if all JDBC connections in use are for a single database, then its pool size needs to accommodate the number of connections this background metadata task will create. |

## Kerberos Cluster Properties

The following cluster properties are used during Kerberos authentication.

Table 175: Gateway Cluster Properties - Kerberos

| Property                            | Description   |
|-------------------------------------|---|
| <b>kerberos.referral.limit</b>      | <p>Sets the maximum number of referrals the Gateway will perform as it attempts to discover the true realm of the user. <b>Note:</b> Increasing the maximum number of referrals may affect performance.</p> <p>Default: <b>5</b></p>  |
| <b>kerberos.krb5Config.override</b> | <p>Whether the Gateway will overwrite an existing <i>krb5.conf</i> configuration file. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = The Gateway will overwrite the <i>krb5.conf</i> file when updating the Kerberos configuration.</li> <li><b>false</b> = The Gateway will not overwrite the <i>krb5.conf</i> file if the file exists.</li> </ul> <p>Default: <b>true</b></p>  |
| <b>kerberos.cache.size</b>          | <p>Sets the maximum number of referral tickets retained in the cache. Value is an integer. A value of "0" (zero) indicates no caching. A value of "-1" indicates an unlimited cache. <b>Note:</b> An unlimited cache is not recommended, as this can impact Gateway performance. Use with caution.</p> <p>The maximum should be large enough to store entire chain of referral tickets, since the entire chain of referral tickets is stored in the ticket cache. For example: If you intend to store 1000 user credentials in the cache and each referral chain consists of 5 tickets, then the cache size should be &gt; 5000.</p> <p><b>Tip:</b> Tickets are automatically purged when they expire, regardless of the cache size.</p> <p>Default: <b>0</b></p> |
| <b>kerberos.cache.timeToLive</b>    | <p>Determines how long a ticket will be stored in the cache (in seconds). Value is an integer. This is a global setting for the entire cache and each individual ticket may have its own time-to-live value. A ticket is purged from the cache based on the earlier of these two settings. A value of "0" (zero) indicates no caching. A value of "-1" indicates no time limit.</p>   |

| Property          | Description   |
|-------------------|---|
|                   | <p>Default: <b>0</b> (seconds)</p> <p><b>Tip:</b> In addition to this cluster property, a ticket is also removed from the cache under any of the following conditions:</p> <ul style="list-style-type: none"> <li>• Ticket has expired</li> <li>• Ticket's "time to live" has been exceeded</li> <li>• Kerberos caching properties have been updated</li> <li>• Gateway is restarted</li> <li>• When a single ticket from the referral chain is purged from the cache, the entire chain is also removed.</li> </ul> |
| <b>krb5.kdc</b>   | <p>Sets the "kdc" value in the <i>krb5.conf</i> (Kerberos configuration) file. The default value is determined by parsing the user's domain in the <i>kerberos.keytab</i> file, then performing a host/IP lookup to determine the KDC value.</p>  |
| <b>krb5.realm</b> | <p>Sets the "default_realm" value in the <i>krb5.conf</i> (Kerberos configuration) file. The default value is determined by parsing the user's domain in the <i>kerberos.keytab</i> file, then performing a host/IP lookup to determine the realm.</p>  |

## LDAP Cluster Properties

The following cluster properties control various aspects of Gateway behavior.

Table 176: Gateway Cluster Properties - LDAP

| Property                              | Description  |
|---------------------------------------|--|
| <b>ldap.certificate.cachetime</b>     | <p>The length of time to keep LDAP certificates in the LDAP certificate cache.</p> <p>Default: <b>600000</b> (milliseconds)</p>  |
| <b>ldap.certificateIndex.interval</b> | <p>The period of time between indexing or reindexing the LDAP certificates.</p> <p>Default: <b>600000</b> (milliseconds)</p>   |
| <b>ldap.connection.timeout</b>        | <p>The timeout for an LDAP connection. If the LDAP provider cannot establish a connection within that period, it aborts the connection attempt. A value less than or equal to zero means to use the network protocol's (for example, TCPs) timeout value.</p> <p>Default: <b>5</b> (seconds)</p> |
| <b>ldap.group.searchMaxResults</b>    | <p>The maximum number of results to return in an LDAP group membership search.</p> <p>By default, this setting uses the value from the <i>ldap.searchMaxResults</i> property. Enter a different value if you do not want the two values to be the same.</p>                                      |



| Property                            | Description   |
|-------------------------------------|---|
|                                     | Default: ( <b>ldap.searchMaxResults</b> setting)  |
| <b>ldap.read.timeout</b>            | <p>The read timeout for LDAP operations. If the LDAP provider cannot get a LDAP response within that period, it aborts the read attempt. A value less than or equal to zero means no read timeout is specified which is equivalent to waiting for the response infinitely until it is received.</p> <p>Default: <b>30</b> (seconds)</p> |
| <b>ldap.referral</b>                | <p>Defines how the Gateway handles LDAP referrals. Possible values are <b>follow</b> or <b>ignore</b>. Set this property to <b>ignore</b> if LDAP referrals are causing problems.</p> <p>Default: <b>follow</b></p>   |
| <b>ldap.searchMaxResults</b>        | <p>The maximum number of results to return in an LDAP Identity Provider search.</p> <p>Default: <b>50</b></p>   |
| <b>ldap.simple.username.pattern</b> | <p>Defines the regular expression that all usernames must match before the Gateway will allow them to be used to construct a DN using the Simple LDAP Identity Provider.</p> <p>Default: <b>^[p{Anum}\\.\\-\\_]+\$</b></p>  |

## Message Validation Cluster Properties

The following cluster properties configure message validation behavior on the Gateway node or node cluster. Changes to a "schemacache" property will take effect within 15 seconds and does not require a Gateway restart.

Table 177: Gateway Cluster Properties - Message validation

| Property                                | Description  |
|---|--|
| <b>json.schemaCache.maxAge</b>          | <p>The maximum age of a cached JSON schema.</p> <p>Default: <b>300000</b> (milliseconds)</p> <p>Requires a Gateway restart for changes to take effect.</p>   |
| <b>json.schemaCache.maxStaleAge</b>     | <p>The maximum age of stale (expired) cached JSON schema documents loaded from URLs. A setting of "-1" indicates no expiry.</p> <p>Default: <b>-1</b> (milliseconds)</p> <p>Requires a Gateway restart for changes to take effect.</p> |
| <b>json.schemaCache.maxDownloadSize</b> | <p>The maximum size of a downloaded JSON schema. Enter "0" (zero) for an unlimited size.</p> <p>Default: uses the predefined context variable <code>\${documentDownload.maxSize}</code>, which has a default of <b>10485760</b></p>    |

| Property                                    | Description   |
|---|---|
|   | (bytes).  |
| <b>json.schemaCache.<br/>maxEntries</b>     | <p>The maximum number of cached schemas. Enter "0" (zero) to disable caching.</p> <p>Default: <b>100</b></p> <p>Requires a Gateway restart for changes to take effect.</p>  |
| <b>messageCache.<br/>diskThreshold</b>      | <p>The threshold for size of messages to be cached on disk. Used by the Store to Cache assertion.</p> <p>Default: <b>8096</b> (bytes)</p>   |
| <b>messageCache.<br/>resetGeneration</b>    | <p>Used to clear the caches created by the Store to Cache assertion, without needing to restart the Gateway.</p> <p>To clear the caches, increment the value of this property. All caches created under a different generation number will be cleared. For example, changing this property to "1" will clear all caches created when this property was set to "0". Changing it to "2" will clear the caches created under "1", etc.</p> <p>Default: <b>0</b></p>  |
| <b>schema.allowDoctype</b>                  | <p>Allow use of a document type definition (DTD) in XML schemas.</p> <p>Default: <b>false</b></p>   |
| <b>schema.<br/>hardwareTargetNamespaces</b> | <p>The XML schemas that will always be loaded to hardware, identified by their target namespace. Separate each schema with a space.</p> <p>Default: <b>http://schemas.xmlsoap.org/soap/envelope/<br/>http://www.w3.org/2003/05/soap-envelope</b></p>  |
| <b>schema.<br/>remoteResourceRegex</b>      | <p>A regular expression matching the URLs from which remote XML schema dependencies may be downloaded.</p> <p>Default: <b>.*</b> (period followed by an asterisk)</p>   |
| <b>schema.<br/>softwareFallback</b>         | <p>Determines whether to use software XML parsing when hardware parsing fails. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = try software parsing if hardware parsing fails</li> <li><b>false</b> = do not try software parsing; return failure if hardware parsing fails</li> </ul> <p>Default: <b>true</b></p> <p><b>Tip:</b> Disabling the fallback to software can increase performance in situations where you expect frequent XML failures. However under certain circumstances, the XML may fail even though it is actually correct. For more information, please <a href="#">contact</a> CA Technical Support.</p> |
| <b>schemacache.<br/>maxAge</b>              | <p>The maximum age of cached XML schema documents that have been downloaded from a URL.</p> <p>Default: <b>30000</b> (milliseconds)</p>   |

| Property                            | Description   |
|-------------------------------------|---|
| <b>schemacache.maxEntries</b>       | The maximum number of cached XML schema documents loaded from URLs. Enter "0" (zero) to disable caching.<br>Default: <b>100</b>   |
| <b>schemacache.maxSchemaSize</b>    | The maximum size of a schema document download. Enter "0" (zero) for an unlimited size.<br>Default: <b>10485760</b> (bytes)   |
| <b>schemacache.maxStaleAge</b>      | The maximum age of stale (expired) cached XML schema documents loaded from URLs. A setting of "-1" indicates no expiry.<br>Default: -1 (milliseconds)   |
| <b>schemacache.recompileLatency</b> | The minimum time that must elapse in between two consecutive rebuilds of the hardware schema table (to prevent continuous rebuilding).<br>Default: <b>10000</b> (milliseconds)  |
| <b>schemacache.recompileMaxAge</b>  | The maximum time a needed schema hardware cache rebuild can be held to wait for additional schemas to stop arriving.<br>Default: <b>20000</b> (milliseconds)  |
| <b>schemacache.recompileMinAge</b>  | The amount of time after a schema becomes hardware eligible to wait for additional schemas to become eligible before triggering a batch rebuild of the hardware schema table (schema status changes often occur in clumps).<br>Default: <b>500</b> (milliseconds) |
| <b>xsltcache.maxAge</b>             | The maximum age of cached stylesheets loaded from URLs. Enter "0" (zero) to disable caching.<br>Default: <b>300000</b> (milliseconds)<br>Requires a Gateway restart for changes to take effect.   |
| <b>xsltcache.maxEntries</b>         | The maximum number of cached stylesheets loaded from URLs.<br>Default: <b>100</b><br>Requires a Gateway restart for changes to take effect.   |
| <b>xsltcache.maxStaleAge</b>        | The maximum age of stale (expired) cached stylesheets loaded from URLs. A setting of "-1" indicates no expiry.<br>Default: -1 (milliseconds)<br>Requires a Gateway restart for changes to take effect.  |

## Rate Limit Cluster Properties

The following cluster properties configure the various limits used in the Apply Rate Limit assertion.

Table 178: Gateway Cluster Properties - Rate Limit

| Property                               | Description  |
|--|--|
| <b>ratelimit.cleanerPeriod</b>         | The time interval for removing rate limit counters that have not been used recently. The node counters are created in the Apply Rate Limit assertion. Purging unused node counters will free up memory on the Gateway.<br>Default: <b>13613</b> (milliseconds) |
| <b>ratelimit.clusterPollInterval</b>   | The time interval between checks of the cluster status table, to check how many cluster nodes are up.<br>Default: <b>43000</b> (milliseconds)  |
| <b>ratelimit.clusterStatusInterval</b> | A cluster node posts its status periodically to indicate that it is operational. This is the maximum allowable elapsed time since the last posting for a node to be considered "up".<br>Default: <b>8000</b> (milliseconds)                                    |
| <b>ratelimit.maxNapTime</b>            | The maximum time a request subject to traffic shaping will wait before awaking to check its status.<br>Default: <b>4703</b> (milliseconds)   |
| <b>ratelimit.maxQueuedThreads</b>      | The maximum number of threads permitted to be queued in a node. Used to delay requests for the Apply Rate Limit assertion.<br>Default: <b>70</b>   |
| <b>ratelimit.maxTotalSleepTime</b>     | The maximum total time a request subject to traffic shaping will wait before giving up and failing.<br>Default: <b>18371</b> (milliseconds)  |

## SAML Cluster Properties

The following cluster properties control various aspects of SAML behavior.

Table 179: Gateway Cluster Properties - Miscellaneous

| Property  | Description  |
|---|--|
| <b>samlAssertion.<br/>NotAfterOffsetMinutes</b> | The number of minutes to offset the "not on or after" aspect of the validity of the SAML statements created by the token service. Must be a positive integer.<br>Default: <b>5</b> (minutes) |
| <b>samlAssertion.</b>                           | The number of minutes to offset the "not before" aspect of   |

| Property   | Description   |
|--|---|
| <b>NotBeforeOffsetMinutes</b>                            | the validity of the SAML statements created by the token service. Must be a positive integer.<br>Default: <b>2</b> (minutes)  |
| <b>samlAssertion.validate.<br/>notBeforeOffsetMin</b>    | The number of minutes to subtract from the "not before" restriction of a SAML token during validation. This can be used to relax the validity window to allow for clock skew.<br>Default: <b>0</b> (minutes)  |
| <b>samlAssertion.validate.<br/>notOnOrAfterOffsetMin</b> | The number of minutes to add to the "not on or after" restriction of a SAML token during validation. This can be used to relax the validity window to allow for clock skew.<br>Default: <b>0</b> (minutes)  |
| <b>saml.generation.includeDNSAddress</b>                 | Controls whether the subject locality for SAML authentication statements include a DNS address. Value is a Boolean. <ul style="list-style-type: none"> <li><b>true</b> = the DNSAddress attribute is set in the SubjectLocality element; for example:<br/> <pre>&lt;saml:SubjectLocality   DNSAddress="sample.l7tech.com"   IPAddress="10.7.99.123"/&gt;</pre> </li> <li><b>false</b> = no DNSAddress attribute is set in the SubjectLocality element; for example:<br/> <pre>&lt;saml:SubjectLocality IPAddress="10.7.99.123"/&gt;</pre> </li> </ul> Default: <b>false</b> |

## Service Cluster Properties

The following cluster properties configure services on the Gateway.

Table 180: Gateway Cluster Properties - Services

| Property                             | Description  |
|--------------------------------------|--|
| <b>service.anonFederatedPolicies</b> | Configure how to treat policies that contain only federated identity assertions. Value is a Boolean. <ul style="list-style-type: none"> <li><b>true</b> = Treat the policy as though it contains no identity assertions, for purposes of checking whether a policy allows anonymous access. In an <a href="#">identity bridging</a> environment, this will allow a Securespan XML VPN Client from another trust domain to download the policy for a federated service.</li> <li><b>false</b> = Maintain the federated identity assertions as is.</li> </ul> Default: <b>true</b> |

| Property                               | Description  |
|--|--|
| <b>service.disabledDownloads</b>       | <p>Defines which requestors can download WSDL and policy documents for disabled services. The values are:</p> <ul style="list-style-type: none"> <li>• <b>none</b> = forbid all requestors</li> <li>• <b>all</b> = allow all requestors</li> <li>• <b>passthrough</b> = permit requestors defined by the cluster property <a href="#">service.passthroughdownloads</a> (described next)</li> </ul> <p>Default: <b>none</b></p>   |
| <b>service.passthroughdownloads</b>    | <p>Defines the remote IPs of requestors allowed to download WSDL and policy documents without credentials. Separate each entry with a space. You may optionally add a netmask to the IP address. Both IPv4 and IPv6 addresses are supported.</p> <p>Default: <b>127.0.0.1</b></p> <p>The default value only allows pass-through from the localhost. The full IP address of a client must match one of the items in the list before a download is permitted.</p> <p>Here are more sample values:</p> <p><i>127.0.0.1 192.168.1</i> allows pass-through from localhost and from any remote address beginning with 192.168.1</p> <p><i>127.0.0.1 10.5.4.41 192.168.1</i> allows pass-through from localhost, from 10.5.4.41, and from any remote address beginning with 192.168.1</p> <p><i>10.7.32.0/24</i> allows pass-through from remote addresses <i>10.7.32.0</i> with a 24-bit network mask (which translates to a permitted address range of 10.7.32.0 to 10.7.32.254)</p> <p>For more information, see "Managing Interfaces" on page 76.</p> |
| <b>service.validateWssTimestamps</b>   | <p>Controls whether the built-in services (token service, policy service) on the Gateway validate WS-Security timestamps. Value is a Boolean.</p> <p>Default: <b>true</b></p>  |
| <b>service.wsdlDependenciesEnabled</b> | <p>Permit download of WSDL dependencies (WSDL/Schema).</p> <ul style="list-style-type: none"> <li>• <b>true</b> = Available WSDL dependencies can be downloaded.</li> <li>• <b>false</b> = Only the primary WSDL document for a service is served by the Gateway.</li> </ul> <p>Default: <b>false</b></p> <p><b>Note:</b> This cluster property must be set to "true" to permit a WSDL with dependencies to be published to UDDI.</p>  |
| <b>service.wsdlQueryEnabled</b>        | <p>Permit download of WSDL using the "?wsdl/" URL suffix. When enabled, the WSDL document can be downloaded using the</p>  |

| Property                      | Description  |
|-------------------------------|--|
|                               | <p>resolution path of the service. Value is a Boolean.</p> <p>Default: <b>true</b></p> <p>For more information, see "WSDL URL by Resolution URI" under <i>Downloading a WSDL</i> in the <i>Layer 7 Installation and Maintenance Manual</i>.</p>  |
| <b>serviceMetrics.enabled</b> | <p>Specify whether service metrics are collected. These metrics can be viewed in the <a href="#">Service Metrics</a> window of the Dashboard.</p> <ul style="list-style-type: none"> <li><b>true</b> = metrics are collected; adds the log entry: <i>INFO: Enabling service metrics collection</i></li> <li><b>false</b> = metrics are not collected; adds the log entry: <i>INFO: Disabling service metrics collection.</i>; a setting of "false" will also make new data unavailable for the Collect WSDM Metrics assertion (if present) and stop further notifications for metrics from being sent</li> </ul> <p>Default: <b>true</b></p> |

## Traffic Logger Cluster Properties

The following cluster properties configure how traffic should be logged on the Gateway node or node cluster.

Table 181: Gateway Cluster Properties - Traffic logger

| Property                       | Description   |
|--------------------------------|---|
| <b>trafficlogger.detail</b>    | <p>A string that contains <a href="#">context variables</a> to express information relating to the request (i.e., what actually gets logged).</p> <p>Default: <b>\${request.time}, \${request.soap.namespace}, \${request.soap.operationname}, \${response.http.status}</b></p>   |
| <b>trafficlogger.recordreq</b> | <p>Specifies whether the request is recorded. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = the actual contents of the request, as received by the Gateway, is appended to the end of each record</li> <li><b>false</b> = the request is not recorded</li> </ul> <p>Default: <b>false</b></p>    |
| <b>trafficlogger.recordres</b> | <p>Specifies whether the response is recorded. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = the actual contents of the response, as returned by the Gateway, is appended to the end of each record</li> <li><b>false</b> = the response is not recorded</li> </ul> <p>Default: <b>false</b></p> |
| <b>trafficlogger.selective</b> | <p>Defines how the traffic logger chooses to log an entry. Value is a Boolean.</p>  |

| Property | Description  |
|----------|--|
|          | <ul style="list-style-type: none"> <li><b>true</b> = traffic is logged only when the <code>\${trafficlogger.select}</code> context variable is defined in a policy and its value is "true"</li> <li><b>false</b> = traffic is logged if the traffic logger is enabled</li> </ul> <p>Default: <b>false</b></p> <p><b>Note:</b> If the traffic logger is disabled, no logging will occur, regardless of the setting for <code>trafficlogger.selective</code>. For information on enabling/disabling a logger, see "Log Sink Properties" on page 167.</p> |

## UDDI Cluster Properties

The following cluster properties are used to configure how the Gateway works with UDDI registries.

Table 182: Gateway Cluster Properties - UDDI

| Property   | Description  |
|--|--|
| <b>uddi.auto_republish</b>                                 | Automatically republish to UDDI as needed (for example, when the cluster hostname or port number changes).<br>Default: <b>true</b>   |
| <b>uddi.batch</b>  | The number of records to retrieve at a time. This value is effective only if less than or equal to the <code>uddi.limit</code> value.<br>Default: <b>100</b>   |
| <b>uddi.centrasite.activesoa.target</b>                    | The target to reference for CentraSite ActiveSOA UDDI metrics. The value should match the value that is configured in the CentraSite web interface.  |
| <b>uddi.centrasite.activesoa.virtual.service.tmodelkey</b> | The tModelKey to add to virtual published business services in CentraSite ActiveSOA. The value of this key is added as a keyedReference to each published business service, when the original business service and the published business services are contained in the same CentraSite ActiveSOA registry.<br>Default: <b>uddi:9de0173b-5117-11de-8cf9-da0192ff3739</b> |
| <b>uddi.connectTimeout</b>                                 | The IO timeout for a UDDI connection. The value must be greater than '0' (zero).<br>Default: <b>30000</b> (milliseconds)   |
| <b>uddi.limit</b>  | The maximum number of records to retrieve for any UDDI inquiry.<br>Default: <b>100</b>   |
| <b>uddi.policyUrlTemplate</b>                              | The template to use for building the WS-Policy Attachment URL.   |



| Property   | Description  |
|--|--|
|  | Default:<br><b>http://{0}:{1}/ssg/policy/disco?serviceoid={3}&amp;fulldoc={4}&amp;inline={5}</b>   |
| <b>uddi.systinet.gif.management.system</b><br>(This property must be manually entered to be used.) | The key value for keyed reference to tModel with key <i>uddi:systinet.com:management:system</i> . There is no default value for this property.<br>Sample value: <i>Layer7 Gateway</i>  |
| <b>uddi.timeout</b>  | The IO timeout for the UDDI response. The value must be greater than '0' (zero).<br>Default: <b>60000</b> (milliseconds)   |
| <b>uddi.wsdlpublish.maxretries</b>   | The maximum number of retry attempts when publishing Gateway WSDL information to UDDI.<br>Default: <b>3</b><br>For more information on when this property is used, see Publish to UDDI Settings in the <i>Layer 7 Policy Authoring User Manual</i> . |

## WS-Security Cluster Properties

The following cluster properties control various aspects of WS-Security behavior on the Gateway.

Table 183: Gateway Cluster Properties - WS-Security

| Property  | Description  |
|---|--|
| <b>outbound.secureConversation.defaultSessionDuration</b> | Defines the system default for the token lifetime. Value is a time unit—see Table 162 for allowable time units. Valid range is 1 minute to 24 hours.<br>Default: <b>2h</b><br>This property is used in the following assertions:<br>Build RST SOAP Request<br>Establish Outbound Secure Conversation     |
| <b>outbound.secureConversation.maxSessions</b>            | Defines the maximum number of outbound secure conversation sessions that can be created. Enter a range between 1 and 1000000.<br>Default: <b>10000</b>   |
| <b>outbound.secureConversation.sessionPreExpiryAge</b>    | Defines a pre-expiry age for outbound secure conversation sessions. This is used to "move up" the supplied expiry time and can help prevent the use of an expired session. For example, if the maximum expiry period is 20 minutes and the value of this cluster property is 5 minutes, the Gateway will |

| Property   | Description   |
|--|---|
|  | <p>use 15 minutes (20-5) as the final expiry period</p> <p>Value is a time unit—see Table 162 for allowable time units. Maximum is 2 hours.</p> <p>Default: <b>1m</b></p> <p>This property is used in the following assertion:</p> <p>Establish Outbound Secure Conversation</p>  |
| <b>security.wss.timestamp.createdFutureGrace</b> | <p>To accommodate clock skew, WSS timestamp created dates are permitted to be up to this far into the future.</p> <p>Default: <b>60000</b> (milliseconds)</p>   |
| <b>security.wss.timestamp.expiresPastGrace</b>   | <p>To accommodate clock skew, WSS timestamp created dates are permitted to be up to this far in the past.</p> <p>Default: <b>60000</b> (milliseconds)</p>   |
| <b>wss.decorator.digsig.messagedigest</b>        | <p>Specifies the default digital signature message digest algorithm that will be used by the following assertions:</p> <ul style="list-style-type: none"> <li>(Non-SOAP) Sign XML Element</li> <li>Add Security Token</li> <li>Add Timestamp (when timestamp is signed)</li> <li>Sign Element</li> </ul> <p>Valid algorithms are: SHA-1, SHA-256, SHA-384, SHA-512.</p> <p>Default: <b>SHA-1</b></p> <p>Requires a Gateway restart for changes to take effect.</p>  |
| <b>wss.decorator.mustUnderstand</b>              | <p>Controls the “mustUnderstand” setting in a Security header. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = The Gateway will generate Security headers with “mustUnderstand” asserted.</li> <li><b>false</b> = The Gateway will generate Security headers without “mustUnderstand” asserted.</li> </ul> <p>Default: <b>true</b></p> <p><b>Note:</b> This setting only affects Security headers generated by the Gateway itself. When the Gateway adds to an existing Security header, that header retains its existing “mustUnderstand” setting. The Gateway must be restarted for changes to this property to take effect.</p> |
| <b>wss.decorator.soap.soapActorNamespaced</b>    | <p>Controls whether the SOAP 1.1 actor attribute created by the WSS decorator is in the SOAP namespace. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Actor attribute is in the SOAP namespace; example: <code>&lt;wsse:Security soapenv:actor="secure_span"&gt;</code></li> </ul>   |

| Property   | Description  |
|--|--|
|  | <ul style="list-style-type: none"> <li><b>false</b> = Actor attribute is <u>not</u> in the SOAP namespace; example: <code>&lt;wsse:Security actor="secure_span"&gt;</code></li> </ul> <p>Default: <b>true</b></p>  |
| <b>wss.decorator.omitNanos</b>                             | <p>Controls whether dates created by WS-Security timestamps should omit nanoseconds. Value is a Boolean.</p> <p>Default: <b>false</b></p>  |
| <b>wss.decorator.wsTrustRequestTypeIndex</b>               | <p>Sets the WS-Trust request type:</p> <ul style="list-style-type: none"> <li><b>0</b> = 2005/02 version of WS-Trust</li> <li><b>1</b> = IBM TFIM (Tivoli Federated Identity Manager) compatible</li> </ul> <p>Default: <b>0</b></p> <p>Requires a Gateway restart for changes to take effect.</p>   |
| <b>wss.processor.allowMultipleTimestampSignatures</b>      | <p>Controls whether security headers should be permitted to contain multiple Signatures covering the timestamp. Value is a Boolean.</p> <p>Default: <b>false</b></p>   |
| <b>wss.processor.allowUnknownBinarySecurityTokens</b>      | <p>Controls how the Gateway responds to Binary Security Tokens of an unknown type. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Unknown tokens are permitted</li> <li><b>false</b> = Unknown tokens will cause security processing to fail</li> </ul> <p>Default: <b>false</b></p>   |
| <b>wss.processor.strictSignatureConfirmationValidation</b> | <p>Controls how signature confirmation validation is performed. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Signature confirmation validation is strictly enforced. All WSS 1.1 signature confirmation checks are performed. All checks are also performed on responses that are detected as using WSS 1.1.</li> <li><b>false</b> = Signature confirmation validation is more lenient. The following conditions are permitted and will <u>not</u> cause validation to fail: <ul style="list-style-type: none"> <li>no SignatureConfirmation element in a WSS 1.1 response</li> <li>SignatureConfirmation element with no Value attribute is not the only SignatureConfirmation element</li> <li>signature confirmation values that are not found in the request</li> <li>unencrypted signature confirmations</li> </ul> </li> </ul> |

| Property   | Description   |
|--|---|
|  | <p>corresponding to encrypted signatures in the request</p> <p>Default: <b>true</b></p>   |
| <b>wss.secureConversation.clusterSessions</b>        | <p>Indicates whether WS-SecureConversation sessions should be shared between cluster nodes. Value is a Boolean.</p> <p>Default: <b>false</b></p> <p><b>Note:</b> WS-SecureConversation session persistence may not be required when using a load balancer with node affinity.</p>   |
| <b>wss.secureConversation.defaultSessionDuration</b> | <p>The default duration for WS-SecureConversation sessions. Minimum is one minute, while the maximum is one day. Value is a time unit—see Table 162 for allowable time units.</p> <p>Default: <b>2h</b></p> <p><b>Note:</b> If the value is outside of the minimum/maximum range or is otherwise invalid, then the default value is used.</p> |
| <b>wss.secureConversation.maxSessions</b>            | <p>The maximum number of WS-SecureConversation sessions permitted at any one time.</p> <p>Default: <b>10000</b></p>   |

## XML Security Cluster Properties

The following cluster properties are used to configure XML security.

Table 184: Gateway Cluster Properties - XML Security

| Property                                  | Description  |
|---|--|
| <b>security.xml.dsig.idAttributeNames</b> | <p>List of attribute names that will be recognized as ID attributes for purposes of locating Signature Reference URI targets during WS-Security processing. The special prefix 'local:' matches the namespace URI against the owning element rather than the attribute. All other prefixes are ignored.</p> <p>Default:</p> <p><b>{http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd}Id</b></p> <p><b>{http://schemas.xmlsoap.org/ws/2002/07/utility}Id</b></p> <p><b>{http://schemas.xmlsoap.org/ws/2003/06/utility}Id</b></p> <p><b>{urn:oasis:names:tc:SAML:1.0:assertion}local:AssertionID</b></p> <p><b>{urn:oasis:names:tc:SAML:2.0:assertion}local:ID</b></p> <p><b>Id</b></p> <p><b>id</b></p> <p><b>ID</b></p> |

| Property   | Description  |
|--|--|
|  | <p><b>Note:</b> This property is for WSS processing and will affect all WSS processing across the cluster after a Gateway restart.</p>   |
| <b>security.xml.dsig.<br/>permittedDigestAlgorithms</b>    | <p>List of message digest algorithm names that will be respected when verifying XML digital signatures. DigestMethod and SignatureMethod references that require algorithms not on this list will not be respected. Separate each entry with a comma.</p> <p>Default: <b>MD5,SHA,SHA-1,SHA-256,SHA-384,SHA-512</b></p> <p>Requires a Gateway restart for changes to take effect.</p> <p><b>Note:</b> When using this cluster property, observe the following:</p> <ul style="list-style-type: none"> <li>• If the Securespan XML VPN Client is involved in any message sending, ensure that SHA is enabled in the cluster property.</li> <li>• If the Securespan XML VPN Client will be decorating messages for the Gateway, SHA-1 must be enabled; otherwise, all WS-Security decorated messages will fail.</li> </ul>  |
| <b>security.xml.dsig.<br/>permittedTransformAlgorithms</b> | <p>List of transform algorithm URIs that will be permitted when verifying XML digital signatures. Transforms that require algorithms not on this list will fail. Separate each URI with a comma.</p> <p>The following signature transforms are accepted by default when this cluster property is not populated:</p> <p><b>"http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#STR-Transform," +</b><br/> <b>"http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-swa-profile-1.0#Attachment-Complete-Transform," +</b><br/> <b>"http://docs.oasis-open.org/wss/2004/XX/oasis-2004XX-wss-swa-profile-1.0#Attachment-Content-Only-Transform," +</b><br/> <b>"http://www.w3.org/2000/09/xmldsig#enveloped-signature," +</b><br/> <b>"http://www.w3.org/2001/10/xml-exc-c14n#," +</b><br/> <b>"http://www.w3.org/2001/10/xml-exc-c14n#WithComments"</b></p> |
| <b>security.xml.xenc.<br/>blacklist.capacity</b>           | <p>The number of entries permitted in the decryption key blacklist.</p> <p>Default: <b>50000</b></p>   |
| <b>security.xml.xenc.<br/>blacklist.enabled</b>            | <p>Determines whether symmetric keys should be blacklisted.</p> <p>Value is a Boolean.</p>   |

| Property  | Description  |
|---|--|
|   | <ul style="list-style-type: none"> <li><b>true</b> = Symmetric keys that fail to successfully decrypt XML (in the number of times specified by the <a href="#">security.xml.xenc.blacklist.maxFailures</a> property) are blacklisted on this node for a period of time (set in the <a href="#">security.xml.xenc.blacklist.maxAge</a> property). This makes it more difficult to use the Gateway as a decryption oracle. This setting is the default.</li> <li><b>false</b> = Symmetric keys will never be blacklisted, even upon failure to decrypt XML.</li> </ul>   |
| <b>security.xml.xenc.blacklist.failWhenFull</b>   | <p>Controls the response should the blacklist reach capacity. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = All XML decryption attempts will fail immediately once the blacklist has reached its capacity (as set in the <a href="#">security.xml.xenc.blacklist.capacity</a> property).</li> <li><b>false</b> = XML decryption will continue even if the blacklist is full. This setting is the default.</li> </ul>  |
| <b>security.xml.xenc.blacklist.maxAge</b>         | <p>The minimum period of time a blacklisted key must remain on the blacklist. Value is a timeunit—see Table 162 for allowable time units.</p> <p>Default: <b>7d</b></p> <p><b>Note:</b> The blacklist is cleared when a node is restarted. Blacklisted keys are released, regardless of whether the blacklist period has been observed.</p>  |
| <b>security.xml.xenc.blacklist.maxFailures</b>    | <p>The maximum number of XML decryption attempts that may fail before a key is blacklisted on a node.</p> <p>Default: <b>5</b></p>   |
| <b>security.xml.xenc.decryptionAlwaysSucceeds</b> | <p>Determines whether XML decryption should appear to succeed once the Gateway has obtained the symmetric key and attempted to decrypt the CipherValue. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Decryption will always be successful. XML that cannot be decrypted will be replaced with a dummy element named <i>L7xenc:DecryptionFault</i> in the namespace <a href="http://layer7tech.com/ns/xenc/decryptionfault">http://layer7tech.com/ns/xenc/decryptionfault</a>. This makes it more difficult to use the Gateway as a decryption oracle. This setting is the default.</li> <li><b>false</b> = The Gateway will return its normal response for decryption success and failure. The dummy element is not used.</li> </ul> |
| <b>security.xml.xenc.encryptEmptyElements</b>     | <p>Determines whether the Encrypt Element assertion should encrypt the content of empty elements. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = The content of empty elements are encrypted</li> </ul>  |

| Property | Description   |
|----------|---|
|          | <p>when the assertion is run. This setting is the default.</p> <ul style="list-style-type: none"> <li><b>false</b> = The empty elements are left unencrypted. Setting this to "false" restores pre-v6.1.5 behaviour and may be required for interoperability with earlier versions of the SecureSpan XML VPN Client.</li> </ul> |

## Miscellaneous Cluster Properties

The following cluster properties control various aspects of Gateway behavior.

Table 185: Gateway Cluster Properties - Miscellaneous

| Property  | Description  |
|---|--|
| <b>admin.<br/>certificateDiscoveryEnabled</b>       | <p>Allows the Policy Manager to securely discover this Gateway's SSL certificate without user intervention. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Automatic certificate discovery is enabled, without user intervention required.</li> <li><b>false</b> = Automatic certificate discovery is disabled. When the Policy Manager attempts to trust a server certificate for the first time, a confirmation dialog is displayed and you must explicitly accept or reject the certificate.</li> </ul> <p>Default: <b>true</b></p> <p><b>Tip:</b> See also <a href="#">services.certificateDiscoveryEnabled</a>.</p> |
| <b>attachment.diskThreshold</b>                     | <p>The threshold for bytes of attachments in a single request to keep in RAM.</p> <p>Default: <b>1048576</b></p>   |
| <b>builtinService.snmpQuery.enabled</b>             | <p>Controls the availability of the <b>SNMP query service</b> check box in the <a href="#">Listen Port Properties [Basic Settings] tab</a>.</p> <ul style="list-style-type: none"> <li><b>true</b> = The check box displays among the other built-in service check boxes.</li> <li><b>false</b> = The check box is suppressed.</li> </ul> <p>Default: <b>true</b></p>  |
| <b>contentType.otherTextualTypes</b>                | <p>By default, the Gateway recognizes these Content-Types: <b>text</b>, <b>xml</b>, <b>json</b> and <b>form encoded</b>. Use this cluster property to define other textual Content-Types. Each Content-Type should be on a separate line and may include a charset, for example:</p> <p><i>application/custom; charset="UTF-8"</i></p>   |
| <b>customerMapping.<br/>addToGatewayAuditEvents</b> | <p>Determines whether the Gateway will save the mapping information with the audits:</p>   |

| Property                                   | Description   |
|--|---|
|  | <ul style="list-style-type: none"> <li><b>true</b> = The mapping information will be saved in the Gateway audit, enabling them to be viewed in the <a href="#">Gateway Audit Events</a> window.</li> <li><b>false</b> = The mapping information will not be saved in the Gateway audit.</li> </ul> <p>Default: <b>true</b></p>  |
| <b>customerMapping.addToServiceMetrics</b> | <p>Determines whether the Gateway will save the mapping information with the service metrics:</p> <ul style="list-style-type: none"> <li><b>true</b> = The mapping information will be saved with the service metrics, allowing them to be used in the <a href="#">Dashboard</a>.</li> <li><b>false</b> = The mapping information will not be saved with the service metrics.</li> </ul> <p>Default: <b>true</b></p>  |
| <b>datetime.autoFormats</b>                | <p>Used to configure the built-in set of supported date formats. This property determines the values that the Set Context Variable assertion can parse by default when "&lt;auto&gt;" is selected and what values the Compare Expression assertion can automatically convert when "Date/Time" is selected as the data type.</p> <p>This is a hidden property that is editable by typing in its name in the <b>Key</b> field. By default, these formats are supported:</p> <p><i>Example:</i> 1997-07-16T 19:20:30.45-1:00</p> <ul style="list-style-type: none"> <li>W3C ISO 8601 (<a href="http://www.w3.org/TR/NOTE-datetime">http://www.w3.org/TR/NOTE-datetime</a> )</li> <li>HTTP-Date (RFC1123, RFC 850, asc time)</li> <li>RFC 1123 <i>Example:</i> Sun, 06 Nov 1994 08:49:37 GMT</li> <li>RFC 822 (and RFC1036) <i>Example:</i> Sun, 06 Nov 94 08:49:37 GMT</li> <li>RFC 850 <i>Example:</i> Friday, 19-Nov-82 16:14:55 EST</li> <li>asc time <i>Example:</i> Fri Nov 12 13:02:02 2012</li> </ul> <p>For information on the default values and how to edit this property, see "Configuring the Auto Date Format" on page 622.</p> |
| <b>datetime.customFormats</b>              | <p>Used to customize the values displayed in the "Format" drop-down list in the Set Context Variable assertion. User can modify datetime.customFormats by adding new formats or by removing the existing formats. If you wish to add additional formats, enter them here, separating each format with a semicolon. Changing datetime.customFormats does not affect values in datetime.autoFormats.</p>  |



| Property                                | Description  |
|---|--|
| <b>db.replicationDelayThreshold</b>     | <p>The threshold for auditing a warning due to slow or failed replication. Enter "0" (zero) to disable audits. Value is a time unit.</p> <p>Default: <b>60s</b></p>  |
| <b>db.replicationErrorAuditInterval</b> | <p>The minimum interval between successive database replication failure audits. This allows the number of audits to be restricted, so auditing will occur only once per hour (or whatever is configured) when replication is failing. Value is a time unit.</p> <p>Default: <b>60m</b></p>   |
| <b>ekeycache.maxEntries</b>             | <p>Maximum number of cached ephemeral key thumbprints (per-node).</p> <p>Default: <b>1000</b></p>  |
| <b>icap.channelIdleTimeout</b>          | <p>The maximum idle time for a connected channel in the connection pool to an ICAP server. Any channels exceeding this timeout value will be disconnected and removed from the pool. Value is a time unit; the allowable range is between 1 second and 1 hour.</p> <p>Default: <b>1m</b></p>   |
| <b>keyStore.searchForAlias</b>          | <p>Determines how the Gateway should search for key aliases:</p> <ul style="list-style-type: none"> <li>• <b>true</b> = If an assertion refers to a private key in a non-existent keystore, the Gateway will check all other keystores for an identical private key alias. If one is found, it will be used instead. In the Policy Manager, a warning validator message is displayed for any affected assertions.</li> <li>• <b>false</b> = If an assertion refers to a private key in a non-existent keystore, an error is returned and the policy containing this assertion will be inoperative. Other keystores are not examined.</li> </ul> <p>Default: <b>true</b></p> <p>For more information about private keys, see "Managing Private Keys" on page 260. For more information on how to select a private key to use, see "Selecting a Custom Private Key" on page 275.</p> |
| <b>keyStore.signWithSha1</b>            | <p>Sets the default signature hash to use for the message digest when signing certificates. Value is a Boolean.</p> <ul style="list-style-type: none"> <li>• <b>true</b> = use SHA-1</li> <li>• <b>false</b> = use SHA-384</li> </ul> <p>Default: <b>false</b></p>   |
| <b>krb5.kdc</b>                         | <p>Sets the "kdc" value in the <i>krb5.conf</i> (Kerberos configuration)</p>   |

| Property                           | Description  |
|------------------------------------|--|
|                                    | file. The default value is determined by parsing the user's domain in the <i>kerberos.keytab</i> file, then performing a host/IP lookup to determine the KDC value.  |
| <b>krb5.realm</b>                  | Sets the "default_realm" value in the <i>krb5.conf</i> (Kerberos configuration) file. The default value is determined by parsing the user's domain in the <i>kerberos.keytab</i> file, then performing a host/IP lookup to determine the realm.  |
| <b>license.expiryWarningPeriod</b> | How far in advance to display impending expiration of the Gateway license or SSL certificate. Value is a time unit—see Table 162 for allowable time units.<br>Default: <b>30d</b>  |
| <b>metrics.fineInterval</b>        | The time interval for Service Metrics fine resolution bins.<br>Default: <b>5000</b> (milliseconds)<br><br>For more information about service metrics bins, see "Dashboard - Service Metrics" on page 402. A cluster-wide restart is required if this value is changed.   |
| <b>mtom.decodeSecuredMessages</b>  | Controls whether secured MTOM-encoded message are automatically decoded. Value is a Boolean. <ul style="list-style-type: none"> <li><b>true</b> = MTOM-encoded messages containing a WS-Security header that will be processed by the Gateway will be automatically decoded to a regular SOAP message for security processing.</li> <li><b>false</b> = MTOM-encoded messages will not be automatically decoded prior to WS-Security processing. An undecoded secure MTOM message may cause WS-Security processing to fail.</li> </ul> Default: <b>true</b><br><br><b>Note:</b> This cluster property only acts on messages containing a WS-Security destined for the Gateway. All other message are unaffected by this property and MTOM decoding will occur only when a Decode MTOM Message assertion is present in the policy. |
| <b>pingServlet.mode</b>            | Determines how the Gateway responds to PING commands. Values are: <ul style="list-style-type: none"> <li><b>OFF</b>: No response to any ping attempts.</li> <li><b>REQUIRE_CREDS</b>: Responds only when request is submitted using SSL on port 8443, with credentials in the request.</li> <li><b>OPEN</b>: Minimal response when request is submitted without SSL (port 8080); full response when request is submitted with SSL (port 8443).</li> </ul>  |

| Property                               | Description   |
|--|---|
|  | <ul style="list-style-type: none"> <li>• <b>MONITOR:</b> Under this mode, the PingServlet will do the following. <ul style="list-style-type: none"> <li>• Allow access to <code>/ssg/ping</code> on port 8080 or 8443 without requiring credentials</li> <li>• Return only simple status message (OK/FAILURE) to request for <code>/ssg/ping</code></li> <li>• Return nothing to request for <code>/ssg/ping/systemInfo?node=Gateway1</code> regardless of port</li> </ul> </li> </ul> <p>Default: <b>REQUIRE_CREDS</b></p> <p>For more information, see "Ping URL Test" in the <i>Layer 7 Installation and Maintenance Manual</i>.</p> |
| <b>policyValidation.maxConcurrency</b> | <p>The maximum number of server-side policy validation jobs that may be active simultaneously.</p> <p>Default: <b>15</b></p> <p>Requires a Gateway restart for changes to take effect.</p>  |
| <b>policyValidation.maxPaths</b>       | <p>The maximum number of possible paths through a policy before the policy is considered to be too complex to attempt server-side validation.</p> <p>Default: <b>500000</b></p>   |
| <b>policyVersioning.maxRevisions</b>   | <p>The maximum number of policy revisions to retain. Only revisions that are not active and which do not have a comment count toward the maximum. If set to '0' (zero), only the active version and commented versions are retained.</p> <p>Default: <b>20</b></p> <p><b>Note:</b> Revisions with comments are always retained, regardless of the setting of this cluster property.</p>   |
| <b>request.compress.gzip.allow</b>     | <p>Determines whether GZIP compressed requests are accepted:</p> <ul style="list-style-type: none"> <li>• <b>true</b> = compressed requests are accepted by the Gateway</li> <li>• <b>false</b> = all compressed requests are rejected</li> </ul> <p>Default: <b>true</b></p>   |
| <b>response.compress.gzip.allow</b>    | <p>Determines whether GZIP compressed responses can be returned to the client:</p> <ul style="list-style-type: none"> <li>• <b>true</b> = compressed response can be returned to the client</li> <li>• <b>false</b> = force a non-compressed response from the Gateway to the client, regardless of the accept-encoding requested response</li> </ul>   |

| Property  | Description  |
|---|--|
|   | Default: <b>true</b>   |
| <b>rbac.autoRole.managePolicy.<br/>autoAssign</b>   | <p>Determines if a non-admin user should be added to the auto-created Manage Policy role, when a new Policy is successfully created.</p> <ul style="list-style-type: none"> <li>• <b>true</b> = the non-admin user is assigned to the Manage Policy role</li> <li>• <b>false</b> = the non-admin user is not assigned to the Manage Policy role</li> </ul> <p>Default: <b>true</b></p>   |
| <b>rbac.autoRole.manageProvider.<br/>autoAssign</b> | <p>Determines if a non-admin user should be added to the auto-created Manage Provider role, when a new Policy is successfully created.</p> <ul style="list-style-type: none"> <li>• <b>true</b> = the non-admin user is assigned to the Manage Provider role</li> <li>• <b>false</b> = the non-admin user is not assigned to the Manage Provider role</li> </ul> <p>Default: <b>true</b></p>   |
| <b>rbac.autoRole.manageService.<br/>autoAssign</b>  | <p>Determines if a non-admin user should be added to the auto-created Manage Service role, when a new Published Service is successfully created.</p> <ul style="list-style-type: none"> <li>• <b>true</b> = the non-admin user is assigned to the Manage Service role</li> <li>• <b>false</b> = the non-admin user is not assigned to the Manage Service role</li> </ul> <p>Default: <b>true</b></p>   |
| <b>rsasigcache.maxEntries</b>                       | <p>Sets the size of the RSA signature cache, which keeps track of recently-verified XML snippets. When caching is enabled, the RSA decrypt operation will be skipped and the signature is assumed verified if the exact same signed XML is presented, verified with exactly the same public key and signature value. The cached signature will not be used if there are changes to the XML, public key, or signature value.</p> <p><b>Note:</b> Only the SHA1 hash is cached, not the entire XML snippet.</p> <p>This cluster property lets you balance performance vs. security. By default, the cached is disabled, which enhances overall security at the expense of a slight performance penalty. You should enable the cache if the following reasons apply to you:</p> <ul style="list-style-type: none"> <li>• Your Gateway is expected to repeatedly validate the same signed XML snippets (for example, SAML</li> </ul> |

| Property                                | Description   |
|---|---|
|   | <p>assertions) and maximum throughput is important.</p> <ul style="list-style-type: none"> <li>Your organization's security policy permits the use of cached signatures.</li> <li>You are willing to have caching code in the signature validation code path.</li> </ul> <p>The value is the number of verified signatures to cache. A setting of "0" (zero) disables the cache.</p> <p>Requires a Gateway restart for changes to take effect.</p> <p>Default: <b>0</b> (caching disabled)</p>  |
| <b>security.fips.enabled</b>            | <p>Enable FIPS-compliant cryptographic algorithms. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> = Places the RSA software cryptographic provider into FIPS mode, but security providers from the runtime environment continue to be available. If there is a Gateway feature enabled that requires a non-FIPS algorithm (for example, the Certificate Discovery Service or an SSL cipher that uses RC4 or MD5), then the Gateway will attempt to use the built-in security provider for that feature.</li> </ul> <p><b>Note:</b> When the <i>security.fips.enabled</i> property is set to "true", non-FIPS ciphers will not be accepted. There is no assurance that the built-in TLS implementation will be able to correctly process all non-FIPS algorithms.</p> <ul style="list-style-type: none"> <li><b>false</b> = The built-in non-FIPS Sun provider is always used; FIPS mode is never enabled.</li> </ul> <p>Default: <b>false</b></p> |
| <b>siteminder12.agent.configuration</b> | <p>This property is used to configure agent information for the Authenticate with SiteMinder R12 Protected Resource assertion. For detailed information on using this property, see "Installing the SiteMinder R12 Assertion" in the <i>Custom Assertions Installation Manual</i>.</p>  |
| <b>soap.actors</b><br><b>soap.roles</b> | <p>The SOAP actors or roles in the security header that will be processed by the Gateway. Each actor or role should be separated with a space or placed on a separate line.</p> <p>Default:</p> <p><b>secure_span</b><br/><b>http://www.layer7tech.com/ws/policy</b></p> <p>Notes about these two cluster properties:</p> <ul style="list-style-type: none"> <li>If the Securespan XML VPN Client is used, it is recommended that the "secure_span" actor or role not be removed.</li> </ul>  |

| Property                                   | Description  |
|--|--|
|  | <ul style="list-style-type: none"> <li>Any new actor or role added to these properties will be treated in the same manner as the "secure_span" actor when it comes to processing of security headers in routing assertions (that is, if the <i>"Remove Layer 7 actor and mustUnderstand attributes from processed Security header"</i> option is chosen for WSS header handling in a routing assertion property).</li> </ul> <p>Unless otherwise configured in the policy, response messages will use the actor/role value from the request message (if the request message uses one of the configured additional values).</p> |
| <b>soap.rejectMustUnderstand</b>           | <p>Controls how messages with unrecognized SOAP headers addressed to the Gateway will be handled:</p> <ul style="list-style-type: none"> <li><b>true</b> = Messages containing "mustUnderstand" SOAP headers other than "Security" and "Timestamp" that are addressed to the Gateway role will be rejected immediately, during security processing.</li> <li><b>false</b> = Messages containing such SOAP headers will be passed through security processing and into policy processing.</li> </ul> <p>Default: <b>true</b></p>  |
| <b>sophos.failover.retries</b>             | <p>The number of times the Scan using Sophos Antivirus assertion will attempt to contact the Sophos Antivirus machine during failover attempts.</p> <p>Default: <b>5</b></p>   |
| <b>sophos.socket.connect.timeout</b>       | <p>The maximum amount of time the Sophos Antivirus assertion will wait for a response after connecting with the Sophos server. When this period is reached, the assertion will disconnect the socket to that server and try the next server (if applicable).</p> <p>Default: <b>50000</b> (milliseconds)</p>   |
| <b>sophos.socket.read.timeout</b>          | <p>The maximum amount of time the Scan using Sophos Antivirus assertion will wait for a read response after connecting with the Sophos server. When this period is reached, the assertion will disconnect the socket to that server and try the next server (if applicable).</p> <p>Default: <b>50000</b> (milliseconds)</p>   |
| <b>sophos.virus.found.log.level</b>        | <p>The severity level assigned to audit events logged when a virus is found by the Scan using Sophos Antivirus assertion.</p> <p>Default: <b>WARNING</b></p>   |
| <b>template.defaultMultivalueDelimiter</b> | <p>The delimiter to use between values when a <a href="#">multivalued context variable</a> is interpolated.</p>  |

| Property                            | Description   |
|-------------------------------------|---|
|                                     | <b>Default:</b> , (comma space)   |
| <b>template.partBodyMaxSize</b>     | The maximum size of message part bodies to interpolate in memory.<br>Default: <b>5242880</b> (bytes)  |
| <b>template.strictMode</b>          | Determines what happens when a <a href="#">context variable</a> cannot be resolved for whatever reason. Value is a Boolean. <ul style="list-style-type: none"> <li>• <b>true</b> = Nonexistent variables in a template can cause assertions or policy processing to fail.</li> <li>• <b>false</b> = Nonexistent variables in a template will trigger a warning audit event and an empty string is used instead; this will not cause assertions or policy processing to fail.</li> </ul> Default: <b>false</b> |
| <b>wSDLDownload.maxSize</b>         | The maximum permitted size of a WSDL document download. A value of "0" (zero) indicates unlimited size.<br>Default: uses the predefined context variable <a href="#">\${documentDownload.maxSize}</a> , which has a default of <b>10485760</b> (bytes).   |
| <b>wsdm.notification.enabled</b>    | Enable notifications when subscribing to a WSDM resource. Value is a Boolean.<br>Default: <b>true</b>   |
| <b>wsdm.notification.interval</b>   | The interval between WSDM subscription notifications attempts.<br>Default: <b>60000</b> (milliseconds)<br><b>Note:</b> This only applies to metrics notifications; status changes are sent as they occur.   |
| <b>xslDownload.maxSize</b>          | The maximum size in bytes of a XSL document download. A value of "0" (zero) indicates unlimited size.<br>Default: uses the predefined context variable <a href="#">\${documentDownload.maxSize}</a> , which has a default of <b>10485760</b> (bytes).   |
| <b>xacml.pdp.maxDownloadSize</b>    | Maximum size in bytes of a XACML policy document download. A value of "0" (zero) indicates unlimited size.<br>Default: uses the predefined context variable <a href="#">\${documentDownload.maxSize}</a> , which has a default of <b>10485760</b> (bytes) .   |
| <b>xacml.pdp.policyCache.maxAge</b> | The period of time to cache a XACML policy in memory. When the Evaluate XACML Policy assertion is processed within the policy, the policy is re-downloaded if the cached policy is older  |

| Property                                 | Description  |
|--|--|
|  | <p>than the value of this cluster property.</p> <p>Default: <b>300000</b> (milliseconds)</p> <p>Requires a Gateway restart for changes to take effect.</p>   |
| <b>xacml.pdp.policyCache.maxEntries</b>  | <p>The maximum number of cached XACML policies loaded from URLs across all Evaluate XACML Policy assertions on a single Gateway node. Enter '0' (zero) to disable caching.</p> <p>Default: <b>100</b></p> <p>Requires a Gateway restart for changes to take effect.</p>  |
| <b>xacml.pdp.policyCache.maxStaleAge</b> | <p>The maximum age of stale (expired) cached policies loaded from URLs. A setting of "-1" indicates no expiry.</p> <p>Default: <b>-1</b></p> <p>Requires a Gateway restart for changes to take effect.</p>   |
| <b>xslt.engine.force20</b>               | <p>Determines when the XSLT 2.0 engine (currently Saxon) will be used to process XSLT/XPath stylesheets. Value is a Boolean.</p> <ul style="list-style-type: none"> <li><b>true</b> – Forces the use of the XSLT 2.0 engine to process v1.0 stylesheets in software.</li> <li><b>false</b> – Uses the XSLT 2.0 engine only for v2.0 XSLT/XPath operations. This setting is the default.</li> </ul> <p>Requires a Gateway restart for changes to take effect.</p> |

## Configuring the Auto Date Format

Observe the following guidelines when configuring the "datetime.autoFormats" on page 614 cluster property:

- The string must be formatted as `<format><^pattern$>`.
- The pattern must begin with the ^ character and end with the \$ character.
- White space is not required and will be ignored if present.
- Any pairs with either an invalid format or pattern will be ignored and an audit will be generated.
- The Policy Manager does not validate the value for this property.

The default value for the cluster property is as follows (line breaks added for readability):

```
yyyy-MM-dd'T'HH:mm:ss.SSSXXX ^\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d{3}(?:Z|(?:\+|-)\d{2}:\d{2})$
yyyy-MM-dd'T'HH:mm:ss.SSXXX ^\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d{2}(?:Z|(?:\+|-)\d{2}:\d{2})$
yyyy-MM-dd'T'HH:mm:ss.SXXX ^\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}\.\d{1}(?:Z|(?:\+|-)\d{2}:\d{2})$
yyyy-MM-dd'T'HH:mm:ssXXX ^\d{4}-\d{2}-\d{2}T\d{2}:\d{2}:\d{2}(?:Z|(?:\+|-)\d{2}:\d{2})$
```



```

yyyy-MM-dd'T'HH:mmXXX ^\d{4}-\d{2}-\d{2}T\d{2}:\d{2}(\?:Z|(\?:\+|-)\d{2}:\d{2})$
yyyy-MM-dd ^\d{4}-\d{2}-\d{2}$
yyyy-MM ^\d{4}-\d{2}$
yyyy ^\d{4}$
EEE, dd MMM yyyy HH:mm:ss z ^[a-zA-Z]{3},\s\d{2}\s[a-zA-Z]{3}\s\d{4}\s\d{2}:\d{2}:\d{2}
\s(\?:[a-zA-Z]{3}|(\?:\+|-)\d{4})$
EEE, dd MMM yy HH:mm:ss Z ^[a-zA-Z]{3},\s\d{2}\s[a-zA-Z]{3}\s\d{2}\s\d{2}:\d{2}:\d{2}\s
(\?:[a-zA-Z]{3}|(\?:\+|-)\d{4})$
EEE, dd-MMM-yy HH:mm:ss z ^
(\?:Monday|Tuesday|Wednesday|Thursday|Friday|Saturday|Sunday),\s\d{2}-[a-zA-Z]{3}-\d{2}
\s\d{2}:\d{2}:\d{2}\s(\?:[a-zA-Z]{3}|(\?:\+|-)\d{4})$
EEE MMM dd HH:mm:ss yyyy ^[a-zA-Z]{3}\s[a-zA-Z]{3}\s(\d{2}|\s\d)\s\d{2}:\d{2}:\d{2}\s\d
{4}$

```

## Other Cluster Properties

Refer to the following sections for additional cluster properties:

- For cluster properties specific to the *CA WSDM Gateway Observer*, see the *Layer 7 Installation and Maintenance Manual*.
- For cluster properties used by the integration with the *Progress Actional for SOA Operations*, refer to "Appendix H: Actional Integration" on page 657.



## Appendix E: Assertion Status Codes

The table below lists all the status codes that are returned by policy assertions. These codes sometime appear the server [log](#).

Table 186: Assertion status codes

| Code | Severity | Message                             | Explanation   |
|------|----------|-------------------------------------|---|
| -1   | INFO     | Undefined                           |   |
| 0    | FINE     | No Error                            | Assertion finished successfully   |
| 400  | INFO     | Bad Request                         | Message is not valid syntactically or semantically  |
| 401  | INFO     | Authentication Required             | Credentials required but missing  |
| 402  | WARNING  | Authentication Failed               | Credentials present but erroneous   |
| 402  | INFO     | Unauthorized                        | Credentials present but erroneous   |
| 403  | INFO     | Service Disabled                    |   |
| 404  | INFO     | Service Not Found                   | Unable to resolve a service for request   |
| 500  | INFO     | Internal Server Error               |   |
| 501  | INFO     | Access Denied by Protected Service  |   |
| 502  | INFO     | Bad Response from Protected Service |   |
| 503  | INFO     | Service Temporarily Unavailable     | Request temporarily cannot proceed, but may be successful if retried in the near future. Possible causes: the Gateway is overloaded or out of resources, or rate quota has been reached for this web service, client, user, or SOAPAction |
| 600  | INFO     | Assertion Falsified                 | Message may be valid, but does not satisfy a logical predicate  |
| 601  | INFO     | Error in Assertion Processing       | Assertion unable to determine whether message is acceptable; no implications on validity of message   |
| 1000 | INFO     | Not yet implemented!                | Assertion not yet implemented   |

| Code | Severity | Message                        | Explanation |
|------|----------|--------------------------------|-------------|
| 1001 | INFO     | Not applicable in this context |             |
| 1002 | INFO     | Invalid XPath Pattern          |             |
| 1003 | INFO     | Unresolvable Namespace Prefix  |             |

## Appendix F: Audit Message Codes

The table below lists all the audit messages used by the Gateway when reporting audit events. These messages are organized into the following high level groupings:

Table 187: Audit message groupings

| Type of audit message                                       | Code range      |
|---|-----------------|
| Messages (for example, generic messages such as Exceptions) | 0001 - 0099     |
| Common messages   | 0100 - 0999     |
| Boot messages   | 1000 - 1999     |
| System messages   | 2000 - 2999     |
| Message Processing messages                                 | 3000 - 3499     |
| Service messages  | 3500 - 3999     |
| Assertion messages  | 4000 - 9999     |
| Enterprise Service Manager messages                         | 100000 - 109999 |

For more information about audit records, see the Audit Messages in Policy Assertion in the *Layer 7 Policy Authoring User Manual*.

For information on how to override the severity of an audit during run time, see "Overriding the Audit Level" on page 427.

**Tips:** (1) In the list of message codes, "{0}", "{1}", etc., are placeholders for messages that may vary depending on the context of the audit. (2) Messages may convert non-identifiable characters into a string literal of their Unicode value. For example, if "null" is being expressed in a message, it will be displayed as "\u0000", which is the Unicode representation for null.

Table 188: Audit message codes

| CODE | SEVERITY | MESSAGE                                |
|------|----------|--|
| -1   | FINEST   | {0}                                    |
| -2   | FINER    | {0}                                    |
| -3   | FINE     | {0}                                    |
| -4   | INFO     | {0}                                    |
| -5   | WARNING  | {0}                                    |
| -6   | FINE     | No such variable: {0}                  |
| -7   | FINE     | Variable exists but has no value: {0}  |
| -8   | WARNING  | Required variable not found: {0}       |
| -9   | FINE     | Variable '{0}' should be of type '{1}' |
| -10  | WARNING  | No such variable: {0}                  |

|      |         |   |
|------|---------|---|
| 1    | WARNING | Exception caught!   |
| 2    | WARNING | {0}. Exception caught!  |
| 3    | WARNING | Exception caught!   |
| 4    | WARNING | Invalid Encapsulated Assertion Config: {0}<br>Exception caught! Unable to read variable: {0}<br>Exception caught! Unable to set variable: {0} |
| 5    | INFO    | Exception caught!   |
| 6    | INFO    | {0}. Exception caught!  |
| 100  | INFO    | Couldn't get style for BindingOperation {0}; assuming<br>\"document\"   |
| 101  | INFO    | Part {0} has both an element and a type   |
| 102  | INFO    | Unsupported style '{0}' for {1}   |
| 103  | INFO    | Unable to find payload element QNames for<br>BindingOperation {0}   |
| 104  | INFO    | Part {0} not found  |
| 150  | WARNING | Array subscript ({0}) in {1} out of range ({2} values);<br>returning no values  |
| 151  | WARNING | Variable '{0}' is a {1}, which is not known to have a<br>useful toString()  |
| 152  | WARNING | Unsupported variable: {0}   |
| 503  | WARNING | No useable connections, please ensure server entries<br>are correct and valid.  |
| 1000 | INFO    | Deleting leftover attachment cache file: {0}  |
| 1001 | INFO    | Initializing hardware XML acceleration  |
| 1002 | WARNING | Error initializing Tarari board   |
| 1003 | INFO    | Hardware XML acceleration disabled  |
| 1004 | WARNING | Unable to retrieve local IP address - 127.0.0.1 will be<br>used in audit records  |
| 1005 | INFO    | Initializing cryptography subsystem   |
| 1006 | INFO    | Using asymmetric cryptography provider: {0}   |
| 1007 | INFO    | Using symmetric cryptography provider: {0}  |
| 1008 | WARNING | Could not initialize server component '{0}'   |
| 1009 | WARNING | Ignoring upgrade task: {0}  |
| 1010 | WARNING | Upgrade task failed, but will attempt to boot anyway: {0}   |
| 1011 | WARNING | Upgrade task failed; unable to proceed: {0}   |
| 1012 | WARNING | Upgrade task warning: {0}   |
| 1013 | WARNING | Unable to retrieve local IP address; audit records will use {0}   |
| 1015 | INFO    | Full Details of Audit Search Criteria: {0}<br>(where: {0} presents the full details of Audit Search Criteria)                                 |
| 2000 | WARNING | Database error  |
| 2001 | WARNING | {0}. Database error   |
| 2005 | INFO    | FIPS mode enabled   |
| 2006 | INFO    | FIPS mode disabled  |
| 2010 | WARNING | Database error reading license file. will keep current license<br>and retry.  |
| 2011 | WARNING | Database error reading license file. Current license was too stale<br>to keep. will keep trying.  |
| 2012 | WARNING | No valid license is installed. Some product features may be<br>disabled.  |
| 2013 | INFO    | Valid license found   |
| 2014 | WARNING | License file is not valid   |
| 2015 | INFO    | License updated   |
| 2016 | WARNING | Service '{0}' WSDL error '{1}'  |
| 2017 | WARNING | A remote network connection timed out   |
| 2020 | INFO    | Not starting FTP server (no listeners enabled)  |
| 2021 | INFO    | Starting FTP server with listeners {0}  |

|      |         |   |
|------|---------|---|
| 2022 | INFO    | Stopping FTP server   |
| 2023 | WARNING | FTP server error {0}  |
| 2030 | WARNING | Unable to locate Trusted Cert Entry for issuer with DN {0} of certificate with DN {1}                                     |
| 2031 | FINE    | Certificate validated and verified  |
| 2032 | FINE    | Certificate {0} is not revoked  |
| 2033 | WARNING | Certificate {0} is revoked  |
| 2034 | WARNING | Unable to build path for Certificate {0}: {1}   |
| 2035 | WARNING | Invalid setting for validation level {0}: {1}   |
| 2036 | WARNING | Certificate {0} has expired   |
| 2037 | WARNING | Certificate {0} is not yet valid  |
| 2040 | WARNING | Certificate {1} contained multiple {0} URLs   |
| 2041 | WARNING | Certificate {1} contained no {0} URL  |
| 2042 | FINE    | Using static {0} URL: {1}   |
| 2043 | WARNING | Invalid {0} URL: {1}  |
| 2044 | WARNING | Couldn't get {0} response from URL {1}: {2}   |
| 2045 | WARNING | {0} URL(s) could not be parsed from certificate {1}   |
| 2046 | WARNING | No {0} URLs from Certificate {1} matched regex  |
| 2047 | FINE    | {0} URL {1} from Certificate {2} matches regex  |
| 2048 | WARNING | Unable to locate {0} issuer certificate {1}   |
| 2049 | INFO    | No {0} cache for {1}; refreshing  |
| 2050 | FINE    | Using {0} cache for {1}   |
| 2051 | INFO    | {0} cache for {1} refresh due at {2}; refreshing  |
| 2052 | FINE    | {0} cache for {1} refresh due at {2}; using cache   |
| 2053 | FINE    | Using issuer '{1}' as {0} signer.   |
| 2054 | FINE    | Using issuer authorized certificate '{1}' as {0} signer   |
| 2055 | FINE    | Using trusted certificate '{1}' as {0} signer   |
| 2070 | FINE    | CRL scope does not cover certificate '{0}', CRL URL is '{1}'  |
| 2071 | WARNING | CRL at {0} is invalid: {1}  |
| 2085 | WARNING | Error during OSCP check for responder '{0}':{1}   |
| 2086 | WARNING | OCSP responder '{0}' signing certificate '{1}' is revoked   |
| 2087 | WARNING | Bad status in OSCP check for responder '{0}':{1}  |
| 2088 | WARNING | Circular OSCP check for responder '{0}'';   |
| 2090 | INFO    | Activating version {0} of policy {1}  |
| 2100 | INFO    | User {0} is disabled  |
| 2101 | INFO    | User {0} is locked  |
| 2102 | INFO    | User {0} has expired  |
| 2103 | INFO    | User [0] has exceeded max. number of failed logon attempts. User has attempted {1} out of {2} allowable failure attempts. |
| 2150 | WARNING | Unable to find trusted certificates to check for upcoming expirations; skipping this check                                |
| 2151 | WARNING | Unable to parse trusted certificate #{0} ({1}) in order to check for expiration; skipping                                 |
| 2152 | FINE    | Trusted certificate #{0} ({1}) will expire in {2}   |
| 2153 | INFO    | Trusted certificate #{0} ({1}) will expire in {2}   |
| 2154 | WARNING | Trusted certificate #{0} ({1}) will expire in {2}   |
| 2155 | WARNING | Trusted certificate #{0} ({1}) expired {2} ago  |
| 2156 | WARNING | New expiry period value {0} is not a valid time unit; using {1} instead   |
| 2205 | WARNING | Audit Archiver error: Receiver not enabled  |
| 2207 | WARNING | Audit Archive current database size {0}% has reached and/or exceeded the soft limit of {1}.                               |
| 2270 | WARNING | Error processing subscription notification {0}  |
| 2271 | WARNING | Subscription key not recognized for notification {0}  |
| 2272 | WARNING | Error polling subscription {0}  |
| 2273 | WARNING | Error adding/renewing subscription {0}  |
| 2274 | WARNING | Error removing subscription {0}   |
| 2275 | WARNING | Error publishing metrics {0}  |

|      |         |  |
|------|---------|--|
| 2276 | WARNING | Error publishing metrics for service {0} {1}   |
| 2277 | WARNING | Error removing metrics {0}   |
| 2278 | WARNING | Unexpected error while publishing {0}  |
| 2279 | WARNING | Error rolling back publishing endpoint {0} {1}   |
| 2280 | WARNING | Could not delete binding templates from Service with serviceKey '{0}'. {1}   |
| 2281 | WARNING | Error removing endpoint {0}  |
| 2282 | WARNING | Error publishing service {0}.  |
| 2283 | WARNING | Error rolling back publishing service {0}  |
| 2284 | WARNING | Error publishing endpoint {0}  |
| 2285 | WARNING | Could not delete proxied BusinessService {0}   |
| 2286 | WARNING | Error publishing ws-policy attachment {0}  |
| 2287 | WARNING | Error processing UDDI notification: {0}  |
| 2288 | WARNING | UDDI Notification has caused Published Service to be disabled. Published Service ID {0}  |
| 2289 | WARNING | UDDI Notification that monitored BusinessService has been deleted. Deleting Gateway records for serviceKey {0}   |
| 2290 | WARNING | Error deleting record of proxied business service which has been deleted from UDDI Registry #{0}) with serviceKey {1}  |
| 2291 | INFO    | Service WSDL updated from UDDI {0}   |
| 2292 | WARNING | Error updating service WSDL from UDDI {0}  |
| 2293 | WARNING | Error finding endpoint for business service {0}, wsdl:port {1}, wsdl:binding {2} {3} for UDDI registry {4}   |
| 2294 | INFO    | Updated endpoint from UDDI {0} for business service {1}, wsdl:port {2} for UDDI registry {3}   |
| 2295 | WARNING | Error firing monitoring update events for UDDI Registry with id#{0})   |
| 2296 | WARNING | Original Business Service in UDDI can no longer be monitored. serviceKey: {0} UDDI Registry with id#{1})   |
| 2297 | WARNING | Service is configured to publish a GIF '{0}' endpoint which is no longer available on the Gateway. UDDI is now out of date. To fix either add / enable the listener or republish the GIF endpoint. |
| 2298 | INFO    | Updated context variable service.defaultRoutingURL for published service #{0}) with updated endpoint from UDDI '{1}' for business service '{2}', wsdl:port '{3}' for UDDI registry '{4}'           |
| 2299 | INFO    | Original Business Service '{0}' in UDDI Registry '{1}' is no longer eligible to be monitored. Published Service #{2}) can no longer be under UDDI Control  |
| 2320 | WARNING | Reusing previously-cached copy of remote {0}: URL {1}: {2} (where {0} is the type (e.g., "XSL-T", "JSON Schema", "XACML Policy"), {1} is the URL and {2} is the detail)                            |
| 2380 | WARNING | Error accessing host/database {0}: {1} (where {0} is the hostname (or IP)/database name, {1} is the error detail)  |
| 2381 | WARNING | Replication failing for host/database {0}: {1} (where {0} is the hostname (or IP)/database name, {1} is the error detail)  |
| 2382 | WARNING | Replication recovered for host/database {0} (where {0} is the hostname (or IP)/database name)  |
| 2400 | INFO    | Starting {0} listener: {1} (where {0} is the scheme (e.g., SSH), {1} is a description of the connector)  |
| 2401 | INFO    | Stopping {0} listener:{1} (where {0} is the scheme (e.g., SSH), {1} is a description of the  |



|      |         |  |
|------|---------|--|
|      |         | connector)   |
| 2402 | WARNING | {0} listener error: {1}<br>(where {0} is the relevant scheme(s) (e.g., SSH) and {1} is a description of the error) |
| 3000 | WARNING | Request XML is not well formed   |
| 3001 | FINE    | Message is not SOAP  |
| 3002 | FINE    | Message is not SOAP and will not produce any WSS results   |
| 3003 | WARNING | Error in WSS processing of request   |
| 3004 | WARNING | Error getting XML document from request  |
| 3005 | INFO    | Service not found  |
| 3006 | INFO    | Service disabled   |
| 3007 | FINE    | Resolved service {0} #{1}  |
| 3008 | FINE    | ST Policy version passed is invalid: {0} instead of {1} {2}  |
| 3009 | FINE    | Wrong format for policy version  |
| 3010 | FINE    | Requestor did not provide policy ID  |
| 3011 | WARNING | Cannot get policy  |
| 3012 | FINE    | ST Run the server policy   |
| 3013 | WARNING | Cannot get statistics for published service  |
| 3014 | FINE    | Request was completed with status {0} ({1})  |
| 3015 | WARNING | Policy status was NONE but routing was attempted anyway!   |
| 3016 | WARNING | Request routing failed with status {0} ({1})   |
| 3017 | INFO    | Policy evaluation for service {0} resulted in status {1} ({2})   |
| 3018 | WARNING | EventManager threw exception when logging message<br>processing result   |
| 3019 | FINE    | ST WSS processing of request complete  |
| 3020 | WARNING | Message processor not enabled by license: {0}  |
| 3021 | INFO    | HTTP method {0} not allowed for service {1}  |
| 3022 | INFO    | Invalid request: [{0}]   |
| 3023 | INFO    | Service does not accept multipart data   |
| 3024 | INFO    | HTTP method {0} not allowed  |
| 3025 | INFO    | Error in WSS signature processing: {0}   |
| 3026 | INFO    | Message did not contain any WSS level security   |
| 3031 | WARNING | Certificate key usage or extended key usage disallowed<br>by key usage enforcement policy for activity:{0}         |
| 3034 | WARNING | Error in WSS processing of response: {0}   |
| 3043 | FINEST  | Processing message-received server policies  |
| 3044 | WARNING | Error processing message-received policy: {0}  |
| 3045 | FINEST  | Processing message-completed server policies   |
| 3046 | WARNING | Error processing message-completed policy: {0}   |
| 3047 | WARNING | Error while decrypting encrypted XML   |
| 3100 | FINE    | Using cached failure @\"{0}\"  |
| 3101 | FINE    | Found a non-wildcard match for \"{0}\"   |
| 3102 | FINE    | No match possible with URI \"{0}\"   |
| 3103 | FINE    | One wildcard matched with URI \"{0}\"  |
| 3104 | FINE    | Multiple wildcard matches; using \"{0}\"   |
| 3105 | FINE    | Returning real URI: \"{0}\"  |
| 3106 | FINE    | Returning URI from header: \"{0}\"   |
| 3107 | FINE    | Invalid L7-Original-URL value: \"{0}\"   |
| 3110 | FINEST  | The header \"{0}\" is not present  |
| 3111 | FINEST  | Matched against the header \"{0}\" URL: \"{1}\"  |
| 3112 | FINEST  | Not Matched against the header \"{0}\" URL: \"{1}\"  |
| 3113 | FINEST  | Matched against the Request URI: \"{0}\"   |
| 3114 | FINEST  | Not Matched against the request URI: \"{0}\"   |
| 3120 | FINE    | SOAPAction not present   |
| 3121 | FINE    | Request is not SOAP or was not received via HTTP; no<br>SOAPAction expected  |
| 3130 | FINE    | Service is not SOAP  |

|      |         |  |
|------|---------|--|
| 3131 | FINE    | Service is SOAP but has no WSDL  |
| 3132 | FINE    | WSDL has no bindings   |
| 3133 | FINE    | Couldn't get style for BindingOperation {0}; assuming "document"   |
| 3138 | INFO    | Unable to find any payload element QNames for service {0} ({1})  |
| 3139 | INFO    | Unable to parse WSDL for {0} service ({1})   |
| 3140 | FINE    | Found payload QName \"{0}\"  |
| 3200 | INFO    | Recompiling all published services due to module unload  |
| 3201 | INFO    | License changed/module loaded -- resetting {0} affected services   |
| 3202 | WARNING | Unable to re-enable service after license changed/<br>module loaded: {0}: {1}                                  |
| 3203 | FINEST  | Resolution failed; no Published Services   |
| 3204 | FINEST  | Service resolved early by {0}  |
| 3205 | FINE    | {0} eliminated all possible services   |
| 3206 | FINE    | Resolvers find no match for request  |
| 3207 | FINEST  | Resolved request for \"{0}\" service ({1})   |
| 3208 | INFO    | Resolution failed; multiple services match the current request   |
| 3209 | WARNING | {0}\" service ({1}) will be disabled; it has an unsupported policy<br>format                                   |
| 3210 | WARNING | {0}\" service ({1}) cannot be read properly and will be discarded<br>from the service cache                    |
| 3211 | INFO    | Non-SOAP request resolved to SOAP service  |
| 3212 | INFO    | Resolved \"{0}\" service ({1}) but request does not match any<br>operation in the service's WSDL               |
| 3213 | INFO    | Renable service after license or policy changed/module loaded:<br>{0}: {1}                                     |
| 3250 | INFO    | Recompiling all policies due to module unload  |
| 3251 | INFO    | License changed/module loaded -- resetting {0} affected policies   |
| 3252 | WARNING | Error accessing policy ({1})   |
| 3253 | INFO    | (Re)building policy cache  |
| 3254 | INFO    | Policy \"{0}\" ({1}) is invalid: {2}   |
| 3255 | WARNING | Policy \"{0}\" ({1}) contains an unlicensed assertion: {2}   |
| 3300 | INFO    | Element was signed, but tokens were gathered as credentials and the<br>signing token did not match any of them |
| 3301 | INFO    | Element was signed, but by a different signature   |
| 3302 | INFO    | Element was signed, but no token was gathered as a credential  |
| 3500 | WARNING | Admin applet authentication policy failed: assertion status: {0}   |
| 3501 | INFO    | Admin applet authentication policy error: {0}  |
| 3502 | WARNING | Admin applet authorization failed: user not in any admin role: {0}   |
| 3503 | WARNING | Admin applet authorization error: could not check admin roles: {0}   |
| 3504 | FINE    | Admin applet request to download custom assertion class: {0}   |
| 3505 | WARNING | Admin applet request rejected: request did not arrive over SSL   |
| 3506 | FINE    | Admin applet request authorized for user {0}   |
| 3507 | FINE    | Admin applet request authorized for user {0} (using session cookie)  |
| 3508 | FINE    | Admin applet request: replying with authentication challenge   |
| 3509 | FINE    | Admin applet authentication filter passed  |
| 3510 | INFO    | Admin applet session created for user {0}  |
| 3511 | FINE    | Admin applet request to download assertion module class: {0} from<br>module: {1}                               |
| 3512 | WARNING | Admin applet requests not permitted on this port   |
| 3600 | INFO    | Backup for node {0} downloaded by {1} to {2}   |
| 3601 | WARNING | Backup request blocked: request did not arrive over SSL  |
| 3602 | WARNING | Backup request blocked: invalid credentials  |
| 3603 | WARNING | Backup request blocked: no client cert provided  |
| 3604 | WARNING | Backup request blocked: feature not licensed   |
| 3605 | WARNING | Backup request blocked: request did not arrive over a connector<br>configured for backup                       |

|      |         |  |
|------|---------|--|
| 3606 | WARNING | Backup request blocked: no authenticated user found in credentials   |
| 3607 | WARNING | Backup request blocked: user does not have Administrator role: {0}   |
| 3608 | WARNING | Backup request permission checked failed   |
| 3609 | WARNING | Backup for node {0} failed: cannot create backup image   |
| 3610 | WARNING | Backup for node {0} failed: cannot read backup image   |
| 3611 | WARNING | Backup for node {0} failed: file size too big: {1} bytes   |
| 3612 | WARNING | Backup request routing failed: cannot get cluster nodes information  |
| 3613 | WARNING | Backup request routing failed: no such node: {0}   |
| 3614 | WARNING | Backup request routing failed  |
| 3616 | WARNING | Backup request routing failed: {0}<br>(where: {0} is the reason it failed)                                   |
| 4000 | WARNING | Could not initialize SSL Context   |
| 4001 | INFO    | Processing HTTP(S) Routing assertion   |
| 4002 | WARNING | SOAP message expected but not found; requested option not supported by non-SOAP messages                     |
| 4003 | WARNING | Option not supported by non-SOAP messages; check policy for errors   |
| 4004 | FINE    | Promoting actor {0}  |
| 4005 | INFO    | Routing assertion requested promotion of security header with actor {0}, but no such header found in message |
| 4006 | WARNING | Error reading response   |
| 4007 | WARNING | Could not resolve client IP address  |
| 4008 | FINE    | TAI credential chaining requested, but request was not authenticated   |
| 4009 | FINE    | TAI credential chaining requested; will chain username {0}   |
| 4010 | WARNING | TAI credential chaining requested, but requesting user does not have a unique identifier: ID is {0}          |
| 4011 | FINE    | TAI credential chaining requested, but there is no user; will chain pc.login {0}                             |
| 4012 | WARNING | TAI credential chaining requested, and request was authenticated, but had no user or pc.login                |
| 4013 | FINE    | Adding outgoing cookie: name = {0}   |
| 4014 | FINE    | Using login '{0}'  |
| 4015 | FINE    | Request routed successfully  |
| 4016 | WARNING | Protected service ({0}) responded with status {1}  |
| 4017 | FINE    | Adding outgoing cookie: name = {0}, version = {1}  |
| 4018 | FINE    | Updating cookie: name = {0}  |
| 4021 | WARNING | Invalid original request URI -- using default  |
| 4023 | WARNING | Unable to route to the service after multiple failed attempts  |
| 4024 | WARNING | SAML Sender-Vouches forwarding requested, but request was not authenticated                                  |
| 4025 | INFO    | Protected service ({0}) responded with status {1}; retrying.   |
| 4026 | WARNING | Invalid routing failover strategy name: {0}; using default strategy  |
| 4027 | WARNING | Routing failed to host = {0}, retrying to host = {1}   |
| 4028 | WARNING | Routing failed, unable to resolve IP for host = {0}  |
| 4029 | WARNING | Routing failed, connection error: {0}  |
| 4030 | INFO    | Passthrough selected; adding request credentials to routed request   |
| 4031 | FINE    | Passthrough selected but no credentials in Gateway request to pass along                                     |
| 4032 | INFO    | Passthrough selected; adding challenge to Gateway response   |
| 4033 | FINE    | Passthrough selected but no challenge in routed response   |
| 4034 | WARNING | Downstream service returned status ({0}) but is missing a content type header.                               |
| 4035 | WARNING | Downstream service returned status ({0}) with non-XML payload.   |
| 4036 | WARNING | Ignoring invalid cookie header '{0}'   |
| 4037 | INFO    | Protected service requires authentication  |
| 4038 | INFO    | Downstream service returned status ({0}). This is considered a failure case.                                 |

|      |         |   |
|------|---------|---|
| 4039 | INFO    | Downstream service returned an empty response but still included a content-type of ({0}). |
| 4041 | WARNING | Remote network connection timed out.  |
| 4042 | WARNING | Problem routing to {0}. Error msg: {1}  |
| 4049 | INFO    | Downstream service response did not include a content type header, using default.         |
| 4050 | WARNING | Invalid HTTP configuration '{0}'  |
| 4100 | INFO    | Authentication required   |
| 4114 | INFO    | Found client certificate for {0}  |
| 4115 | FINE    | Ignoring empty cookie with the name: {0}  |
| 4150 | INFO    | Service resolution has already been performed for this request                            |
| 4151 | INFO    | Request has already been assigned to a service  |
| 4152 | INFO    | No service matched the specified parameters   |
| 4153 | INFO    | More than one service matched the specified parameters                                    |
| 4154 | WARNING | Service resolution failed: {0}  |
| 4155 | INFO    | Resolved to service ID: {0}   |
| 4200 | WARNING | Request is authenticated but request has no login credentials!                            |
| 4201 | WARNING | No credentials found!   |
| 4202 | FINEST  | Request already authenticated   |
| 4203 | WARNING | Cannot call checkRequest() when no valid identity provider ID has been set!               |
| 4204 | WARNING | Could not find identity provider!   |
| 4205 | WARNING | Identity assertion refers to a non-existent identity provider                             |
| 4206 | FINE    | Authentication success {0}  |
| 4207 | INFO    | Invalid client certificate for {0}  |
| 4208 | INFO    | Authentication failed for {0}   |
| 4209 | WARNING | Assertion not configured properly: both login and UID are null                            |
| 4210 | FINE    | Authentication failed because ID of provider did not match ({0} instead of {1}).          |
| 4211 | FINE    | Authentication failed because the user ID did not match                                   |
| 4212 | FINE    | Authentication failed because the login did not match                                     |
| 4213 | WARNING | Assertions refer to a nonexistent group; policy may be corrupted                          |
| 4214 | FINE    | User not member of group  |
| 4215 | FINE    | Reusing cached group membership failure   |
| 4216 | WARNING | {0} message is authenticated but has no login credentials!                                |
| 4217 | FINE    | Credentials failed for {0} due to '{1}'   |
| 4300 | FINE    | Intended for another recipient; nothing to validate                                       |
| 4301 | INFO    | Request not SOAP; cannot verify WS-Security contents                                      |
| 4302 | INFO    | Request did not contain any WSS level security  |
| 4304 | WARNING | Assertion configuration error: {0}  |
| 4305 | WARNING | {0} message not soap; {1}<br>(where: 0 is the message target and 1 are more details)      |
| 4306 | WARNING | {0} message has no part {1}   |
| 4307 | WARNING | {0} message has not initialized   |
| 4330 | WARNING | Invalid target message, variable {0}: {1}   |
| 4331 | WARNING | {0} message not XML. {1}  |
| 4400 | INFO    | Request not SOAP; cannot validate attachments   |
| 4401 | INFO    | The request does not contain attachment or is not a multipart message                     |
| 4402 | FINEST  | Operation not found in the request; XPath expression is: {0}                              |
| 4403 | INFO    | Same operation appears more than once in the request; XPath expression is: {0}            |
| 4404 | INFO    | XPath pattern {0} found non-element node '{1}'  |
| 4405 | INFO    | XPath pattern {0}/{1} found non-element node '{2}'  |

|      |         |   |
|------|---------|---|
| 4406 | FINEST  | The operation {0} is found in the request   |
| 4407 | FINE    | MIME part not found in the request; xpath expression is: {0}/{1}}   |
| 4408 | FINE    | Same MIME part appears more than once in the request; xpath expression is: {0}/{1}  |
| 4409 | FINEST  | Parameter {0} is found in the request   |
| 4410 | INFO    | The reference (href) of the {0} is found in the request   |
| 4411 | FINEST  | The href of the parameter {0} is found in the request, value={1}  |
| 4412 | INFO    | Invalid Content-ID URL {0}  |
| 4413 | INFO    | The content type of the attachment {0} must be one of the types: {1}  |
| 4414 | INFO    | The content type of the attachment {0} must be: {1}   |
| 4415 | INFO    | The parameter [{0}] has {1} attachments; the total length exceeds the limit: {2} K bytes                                      |
| 4416 | INFO    | The length of the attachment {0} exceeds the limit: {1} K bytes   |
| 4417 | INFO    | The required attachment {0} is not found in the request   |
| 4418 | INFO    | Unexpected attachment {0} found in the request  |
| 4419 | INFO    | The operation specified in the request is invalid   |
| 4420 | WARNING | Error parsing request, detail is '{0}'.   |
| 4421 | INFO    | Passing extra attachment {0}.   |
| 4422 | INFO    | Maximum length of extra attachments exceeds the limit {0} K bytes.  |
| 4423 | INFO    | Dropping extra attachment {0}.  |
| 4424 | WARNING | Missing required signature for part '{0}', for attachment with Content-ID URL '[1]'   |
| 4500 | INFO    | Request was not received via TCP; cannot validate remote IP address   |
| 4501 | INFO    | The remote address {0} is null or not in expected format  |
| 4502 | FINE    | ST Requestor address {0} is accepted  |
| 4503 | INFO    | Requestor address {0} is not allowed  |
| 4504 | WARNING | Could not resolve a remote IP address from the context variable {0}.  |
| 4505 | WARNING | Invalid IP range configured   |
| 4600 | INFO    | Request not SOAP; unable to check for WS-SecureConversation token   |
| 4601 | INFO    | This request did not contain any WSS level security   |
| 4602 | FINE    | Ignoring SecurityContextToken with no proof-of-possession   |
| 4603 | WARNING | Request referred to a SecureConversation token unrecognized on this server; possible expired session - returning AUTH_FAILED. |
| 4604 | FINE    | Secure Conversation session recognized for user {0}   |
| 4605 | INFO    | This request did not seem to refer to a Secure Conversation token   |
| 4606 | WARNING | Response not SOAP; unable to attach WS-SecureConversation token   |
| 4700 | WARNING | Request not XML; cannot evaluate XPath expression   |
| 4701 | WARNING | Response not XML; cannot evaluate XPath expression  |
| 4702 | WARNING | Assertion has failed because the XPath pattern is null or empty.  |
| 4703 | INFO    | Assertion has failed because the XPath pattern did not match request  |
| 4704 | INFO    | Assertion has failed because the XPath pattern did not match response   |
| 4705 | FINE    | XPath pattern returned true   |
| 4706 | INFO    | XPath pattern returned false  |
| 4707 | FINE    | XPath pattern found a text node   |
| 4708 | FINE    | XPath pattern found an element  |
| 4709 | FINE    | XPath pattern found some other node   |
| 4710 | FINE    | XPath pattern matched request; assertion succeeds   |
| 4711 | FINE    | XPath pattern matched response; assertion succeeds  |
| 4712 | FINE    | XPath pattern found {0} results; .result variable will contain first value  |
| 4713 | FINE    | XPath result #{0}: \  |
| 4714 | WARNING | Cannot evaluate XPath expression: XPath pattern is invalid '{0}'.   |
| 4715 | INFO    | XPath pattern didn't match request; assertion therefore fails; XPath is '{0}'.  |
| 4716 | INFO    | XPath pattern didn't match response; assertion therefore fails; XPath is '{0}'.   |

|      |         |  |
|------|---------|--|
| 4717 | FINE    | Multiple result elements expected, using non-accelerated XPath.  |
| 4719 | WARNING | {0} not XML; cannot evaluate XPath expression  |
| 4720 | WARNING | Cannot resolve namespace prefix {0}  |
| 4750 | INFO    | Hardware acceleration not available; falling back to software XPath processing                           |
| 4751 | INFO    | Hardware acceleration not available for this XPath expression; falling back to software XPath processing |
| 4752 | FINE    | Message has no hardware acceleration context; falling back to software XPath processing                  |
| 4800 | FINE    | This is intended for another recipient; there is nothing to validate                                     |
| 4801 | INFO    | Request not SOAP; unable to check for WS-Security signature  |
| 4802 | INFO    | Request did not contain any WSS level security   |
| 4803 | INFO    | No tokens were processed from this request; returning AUTH_REQUIRED                                      |
| 4804 | WARNING | Request presented more than one valid signature from more than one client certificate                    |
| 4805 | FINE    | Certificate loaded as principal credential for CN:{0}  |
| 4806 | INFO    | This assertion did not find a proven X509 certificate to use as credentials - returning AUTH_REQUIRED    |
| 4807 | INFO    | {0} not SOAP; unable to check for WS-Security signature  |
| 4808 | INFO    | {0} did not contain any WSS level security   |
| 4809 | INFO    | No tokens were processed from {0}; returning {1}   |
| 4810 | WARNING | {0} presented more than one valid signature.   |
| 4811 | WARNING | {0} presented more than one valid signature for {1}.   |
| 4812 | INFO    | No proven {0} X.509 certificate to use as credentials - returning {1}                                    |
| 4870 | FINEST  | Sophos AV detected a virus name ( {0} ), type ( {1} ), location ( {2} ), disinfectable ( {3} )           |
| 4871 | FINER   | Sophos AV detected a virus name ( {0} ), type ( {1} ), location ( {2} ), disinfectable ( {3} )           |
| 4872 | FINE    | Sophos AV detected a virus name ( {0} ), type ( {1} ), location ( {2} ), disinfectable ( {3} )           |
| 4873 | INFO    | Sophos AV detected a virus name ( {0} ), type ( {1} ), location ( {2} ), disinfectable ( {3} )           |
| 4874 | WARNING | Sophos AV detected a virus name ( {0} ), type ( {1} ), location ( {2} ), disinfectable ( {3} )           |
| 4900 | INFO    | Request not SOAP; cannot check for replayed signed WS-Security message                                   |
| 4901 | INFO    | This request did not contain any WSS level security  |
| 4902 | INFO    | Assertion has failed because no timestamp present in request   |
| 4903 | INFO    | Assertion has failed because no signed timestamp present in request                                      |
| 4904 | INFO    | Timestamp in request has no Created element  |
| 4905 | INFO    | Timestamp in request has no Expires element; assuming expiry {0}ms after creation                        |
| 4906 | FINE    | Clock skew: message creation time is in the future: {0}; continuing anyway                               |
| 4907 | FINER   | Timestamp was signed with an X.509 certificate   |
| 4908 | FINER   | Timestamp was signed with a SAML holder-of-key assertion   |
| 4909 | FINER   | Timestamp was signed with a WS-SecureConversation derived key  |
| 4910 | FINEST  | Message ID {0} has not been seen before unique; assertion does not fail                                  |
| 4911 | FINER   | Timestamp was signed with an EncryptedKey  |
| 4912 | WARNING | Message ID {0} is a replay   |
| 4913 | WARNING | Request timestamp contained stale Expires date   |
| 4914 | WARNING | Request timestamp contained Created older than the maximum message age hard cap                          |
| 4915 | WARNING | Unable to generate replay-protection ID; a SKI cannot be derived from signing cert ''{0}''               |
| 4916 | WARNING | Unable to generate replay-protection ID for timestamp -- it was  |

|      |         |   |
|------|---------|---|
|      |         | signed, but with the unsupported token type {0}   |
| 4917 | WARNING | Found multiple eligible sender identity tokens; unable to proceed   |
| 4918 | WARNING | Found multiple signed wsa:MessageID values; unable to proceed   |
| 4919 | FINE    | Found signed wsa:MessageID {0}  |
| 4920 | FINE    | No signed wsa:MessageID was present in the request; using Timestamp instead   |
| 4922 | FINER   | Timestamp in {0} was signed with a kerberos token   |
| 4923 | FINE    | {0} replay protection using scope {1} and identifier {2}  |
| 4924 | WARNING | Error processing variables for {0} {1}; unable to proceed   |
| 4925 | WARNING | {0} replay message identifier is empty; unable to proceed   |
| 5000 | FINE    | Service:{0}, custom assertion: {1}, principal:{2}   |
| 5001 | WARNING | Invalid custom assertion descriptor detected for {0}; policy element is misconfigured and will cause the policy to fail |
| 5100 | INFO    | Request not HTTP; unable to extract HTTP credentials  |
| 5200 | FINE    | This is intended for another recipient; nothing to validate   |
| 5201 | INFO    | Request not SOAP; cannot check for WS-Security UsernameToken  |
| 5202 | INFO    | Request did not include WSS Basic credentials   |
| 5203 | INFO    | Cannot find credentials   |
| 5204 | INFO    | Request did not include an encrypted UsernameToken  |
| 5205 | WARNING | Response not SOAP; unable to use WS-Security EncryptedUsernameToken   |
| 5206 | INFO    | {0} message is not SOAP; cannot check for WS-Security UsernameToken   |
| 5207 | INFO    | {0} message did not include WSS Basic credentials   |
| 5208 | INFO    | {0} message did not include an encrypted UsernameToken  |
| 5300 | FINE    | SSL required and present  |
| 5301 | INFO    | SSL required but not present  |
| 5302 | INFO    | SSL forbidden but present   |
| 5303 | FINE    | SSL forbidden and not present   |
| 5304 | FINE    | SSL optional and present  |
| 5305 | FINE    | SSL optional and not present  |
| 5400 | INFO    | Request not SOAP; unable to check for WS-Security encrypted elements  |
| 5401 | INFO    | Request did not contain any WSS level security  |
| 5402 | WARNING | Request included more than one X509 security token whose key ownership was proven                                       |
| 5403 | WARNING | Unable to encrypt response; request did not include X509 token or SecureConversation                                    |
| 5404 | WARNING | Response not SOAP; unable to encrypt response elements  |
| 5405 | FINE    | No matching elements to encrypt in response; returning success  |
| 5406 | FINEST  | Designated {0} response elements for encryption   |
| 5407 | WARNING | {0} message not SOAP; unable to encrypt message elements  |
| 5408 | INFO    | No matching elements to encrypt in {0} message: Assertion therefore fails   |
| 5409 | FINEST  | Schema validation success   |
| 5410 | INFO    | Request did not include a token suitable for response encryption.   |
| 5500 | INFO    | Request not SOAP; cannot sign response.   |
| 5501 | WARNING | Response not SOAP; cannot apply WS-Security signature   |
| 5502 | FINE    | No matching elements to sign in response; returning success   |
| 5503 | FINE    | Designated {0} response elements for signing  |
| 5504 | WARNING | {0} message not SOAP; cannot apply WS-Security signature  |
| 5505 | INFO    | No matching elements to sign in {0} message: Assertion therefore fails  |
| 5506 | FINE    | Designated {1} {0} message elements for signing   |
| 5550 | FINE    | Response not SOAP; cannot return SignatureConfirmation  |
| 5551 | WARNING | Request has multiple signers; failing   |
| 5604 | WARNING | Assertion failure: {0}  |
| 5605 | FINEST  | Schema validation success   |
| 5606 | FINE    | Nothing to validate because the body is empty   |

|      |         |   |
|------|---------|---|
| 5607 | INFO    | Schema cannot be hardware accelerated   |
| 5608 | INFO    | Hardware-accelerated schema validation failed; falling back to software                             |
| 5609 | INFO    | Message was valid but payload was in an unexpected namespace  |
| 5610 | WARNING | Cannot validate schema because the global schema named {0} cannot be retrieved                      |
| 5611 | INFO    | {0} is not well-formed XML; cannot validate   |
| 5612 | FINEST  | Validating {0}  |
| 5613 | WARNING | Cannot validate schema because schema information cannot be retrieved: {0}                          |
| 5700 | FINEST  | Nothing to check  |
| 5701 | INFO    | Failed because day of week outside allowed range  |
| 5702 | INFO    | Failed because time of day outside allowed range  |
| 5703 | FINEST  | Request is within time range.   |
| 5800 | WARNING | Unknown assertion invoked; details: {0}   |
| 5900 | INFO    | Message not XML; cannot perform XSL transformation  |
| 5901 | FINEST  | Transforming request  |
| 5902 | INFO    | Response not XML; cannot perform XSL transformation   |
| 5903 | FINEST  | Transforming response   |
| 5904 | WARNING | Assertion does not specify whether transformation applies to request or response; returning failure |
| 5905 | WARNING | Assertion refers to nonexistent MIME part {0}   |
| 5906 | WARNING | Document contained multiple <xml-stylesheet> processing instructions; not currently supported       |
| 5907 | WARNING | Could not retrieve linked XSL stylesheet at {0}: {1}  |
| 5908 | WARNING | Unable to parse external XSL at {0}: {1}  |
| 5909 | WARNING | Unable to parse XSL: {0}  |
| 5910 | WARNING | No <xml-stylesheet> processing instruction was found in the message                                 |
| 5911 | WARNING | Stylesheet URL {0} did not match any configured regular expression                                  |
| 5912 | WARNING | Could not retrieve linked XSL stylesheet at {0}: {1}; continuing using previous version             |
| 5913 | INFO    | XSL-T Warning '{0}'   |
| 5914 | INFO    | XSL-T Error '{0}'   |
| 5915 | INFO    | No <xml-stylesheet> processing instruction was found in the message; assertion succeeds             |
| 5916 | FINEST  | Transforming message '{0}'  |
| 6000 | INFO    | Failed to establish JMS connection on try #{0}; will retry after {1}ms                              |
| 6001 | FINE    | Inbound request queue is not temporary; using selector to filter responses to our message           |
| 6002 | WARNING | Topics not supported!   |
| 6003 | FINER   | Routing request to protected service  |
| 6004 | FINEST  | Getting response from protected service   |
| 6005 | WARNING | Did not receive a routing reply within the timeout of {0} ms; empty response being returned         |
| 6006 | FINER   | Received routing reply  |
| 6007 | WARNING | Received JMS reply with unsupported message type {0}  |
| 6008 | INFO    | No response expected from protected service   |
| 6009 | FINER   | Deleting temporary queue  |
| 6010 | FINER   | Returning NO_REPLY (null) for {0}   |
| 6011 | FINER   | Returning AUTOMATIC {0} for {1}   |
| 6012 | FINER   | Returning REPLY_TO_OTHER {0} for {1}  |
| 6013 | WARNING | Unknown JmsReplyType {0}  |
| 6014 | WARNING | Request and reply endpoints must belong to the same connection                                      |
| 6015 | FINER   | Creating request as TextMessage   |
| 6016 | FINER   | Creating request as BytesMessage  |



|      |         |  |
|------|---------|--|
| 6017 | FINE    | As routed request endpoint specified NO_REPLY, JMSReplyTo and JMSCorrelationID will not be set   |
| 6018 | FINE    | Setting JMSReplyTo and JMSCorrelationID  |
| 6019 | WARNING | JMS Routing Assertion contains a reference to nonexistent JmsEndpoint #{0}                       |
| 6020 | WARNING | JMS Routing Assertion cannot access SAML signing information                                     |
| 6021 | WARNING | Failed to establish JMS connection on try #{0}. Will retry after {1}ms.                          |
| 6022 | WARNING | Tried {0} times to establish JMS connection and failed.  |
| 6024 | WARNING | Request message too large  |
| 6025 | WARNING | Error processing JMS outbound template '#{0}'.   |
| 6026 | WARNING | JMS Destination/Session type mismatch  |
| 6027 | WARNING | Sent message had no message ID. Unable to correlate  |
| 6028 | WARNING | Invalid JMS configuration '#{0}'   |
| 6030 | WARNING | Cannot set JMS Property X to value Y on IBM MQ JMS Provider                                      |
| 6031 | WARNING | JMS message format error while constructing JMS message to route                                 |
| 6054 | WARNING | No user name found for passing through to FTP server   |
| 6055 | WARNING | No FTP command specified   |
| 6056 | WARNING | FTP command '#{0}' is not supported  |
| 6057 | INFO    | FTP routing succeeded; transient negative completion reply code returned for command '#{0}': {1} |
| 6058 | INFO    | FTP routing succeeded; permanent negative completion reply code returned for command '#{0}': {1} |
| 6059 | WARNING | FTP routing failed; transient negative completion reply code returned for command '#{0}': {1}    |
| 6060 | WARNING | FTP routing failed; permanent negative completion reply code returned for command '#{0}': {1}    |
| 6061 | WARNING | FTP routing failed; no reply returned for command '#{0}': {1}                                    |
| 6062 | WARNING | FTP routing failed; invalid or unsupported reply code returned for command '#{0}': {1}           |
| 6063 | FINE    | FTP routing succeeded  |
| 6064 | WARNING | FTP routing error: {0}   |
| 6065 | WARNING | FTP routing failed; connection error: {0}  |
| 6066 | WARNING | Unable to find stored gateway account password: {0}  |
|      |         |  |
| 6100 | FINE    | ST Request not SOAP; cannot validate SAML statement  |
| 6101 | INFO    | No tokens were processed from this request; returning AUTH_REQUIRED                              |
| 6102 | WARNING | Request contained more than one SAML assertion   |
| 6103 | INFO    | Assertion did not find an acceptable SAML assertion to use as credentials                        |
| 6104 | WARNING | SAML assertion validation errors: {0}  |
| 6105 | FINE    | {0} message not SOAP; cannot validate SAML statement   |
| 6106 | INFO    | No tokens were processed from {0} message: Returning AUTH_REQUIRED                               |
| 6107 | WARNING | {0} message contained more than one SAML assertion   |
| 6108 | WARNING | SAML token is expired when constrained to maximum allowed lifetime                               |
| 6109 | INFO    | SAML token name identifier contained an invalid DN value for X509SubjectName format displayed    |
|      |         |  |
| 6200 | INFO    | The current request did not contain credentials of any supported type                            |
| 6201 | WARNING | WS-Trust response did not contain a security token of a supported type                           |
| 6202 | WARNING | WS-Trust response had non-200 status   |
| 6203 | INFO    | Cannot replace security token in a non-XML message   |
| 6204 | WARNING | Unable to replace security token   |
| 6205 | INFO    | Original security token was not XML; cannot remove from request                                  |
| 6206 | WARNING | Multiple exchangeable Security Tokens found in request   |
| 6207 | WARNING | HTTP failure talking to WS-Trust server  |
| 6208 | WARNING | Unsupported WS-Trust namespace: {0}  |

|      |         |   |
|------|---------|---|
| 6300 | WARNING | Assertion has failed because regex pattern ''{0}'' compile error: {1}                         |
| 6301 | WARNING | Regular expression cannot be evaluated; content is too large (>= + 1024 * 512 + bytes)        |
| 6302 | WARNING | A replace was requested, but no replacement string was specified (null).                      |
| 6303 | WARNING | Cannot search or replace in nonexistent part #{0}   |
| 6304 | INFO    | Character encoding not specified; will use default {0}  |
| 6305 | FINE    | Using overridden character encoding {0}   |
| 6306 | INFO    | Failing because expression was not matched {0}  |
| 6307 | INFO    | Failing because expression was matched {0}  |
| 6308 | WARNING | Failing because replacement expression was not valid {0}                                      |
| 6400 | WARNING | HTTP GET for login form resulted in non-200 status  |
| 6401 | WARNING | HTTP GET for login form resulted in non-HTML response   |
| 6402 | WARNING | Could not read login form HTML  |
| 6403 | WARNING | Unable to parse login form HTML   |
| 6404 | WARNING | Unable to find login and/or password field(s) in login form HTML                              |
| 6405 | WARNING | Login form contained multiple username or password fields                                     |
| 6406 | WARNING | Multiple login forms found  |
| 6407 | WARNING | No matching login form found  |
| 6408 | WARNING | Login form method was not POST  |
| 6409 | WARNING | Login form is not valid   |
| 6410 | WARNING | Invalid redirect after FORM login   |
| 6420 | WARNING | Request does not contain any credentials  |
| 6421 | WARNING | Request credentials do not include a password   |
| 6500 | WARNING | HTTP GET for login resulted in non-302 status   |
| 6501 | WARNING | Redirect from login contained no query string   |
| 6502 | WARNING | Redirect from query string could not be parsed  |
| 6503 | WARNING | Could not find SAML artifact in redirect query string   |
| 6504 | WARNING | Could not login   |
| 6582 | WARNING | A required Form field is missing in the request. (name={0})                                   |
| 6589 | INFO    | A required Form field is empty. (name={0})  |
| 6600 | WARNING | Request not valid XML   |
| 6601 | INFO    | Login XPath evaluation failed   |
| 6602 | INFO    | Login XPath evaluation failed to find any result  |
| 6603 | WARNING | Login XPath evaluation found multiple results   |
| 6604 | WARNING | Login XPath evaluation found content of an unsupported type                                   |
| 6605 | WARNING | Cannot remove login element; parent is not an Element   |
| 6611 | WARNING | Password XPath evaluation failed  |
| 6612 | WARNING | Password XPath evaluation failed to find any result   |
| 6613 | WARNING | Login XPath evaluation found multiple results   |
| 6614 | WARNING | Password XPath evaluation found content of an unsupported type                                |
| 6615 | WARNING | Cannot remove password element; parent is not an Element                                      |
| 6700 | INFO    | Email message sent  |
| 6701 | WARNING | Bad destination email address(es)   |
| 6702 | WARNING | Bad source email address  |
| 6703 | WARNING | The OID ending with zero is reserved for the message field; using .1 for the trap OID instead |
| 6704 | WARNING | Authentication failure, message not sent  |
| 6705 | WARNING | SSL connection failure, message not sent  |
| 6706 | WARNING | Connection failure, message not sent  |
| 6707 | WARNING | Bad smtp port set, message not sent   |
| 6708 | WARNING | Bad smtp host set or not set at all, message not sent   |
| 6709 | WARNING | Bad smtp user name set or not set at all, message not sent                                    |
| 6710 | WARNING | Bad smtp password set or not set at all, message not sent                                     |

|      |         |  |
|------|---------|--|
| 6711 | WARNING | Invalid OID (value={0}). Using .1 for the trap OID instead   |
| 6712 | WARNING | Bad smtp host set or not set at all (value={0})  |
| 6800 | WARNING | Request does not appear to be an HTTP form submission ({0})  |
| 6801 | WARNING | Request was not received via HTTP  |
| 6802 | WARNING | Field {0} had multiple values; skipping  |
| 6803 | WARNING | Field {0} could not be found   |
| 6804 | WARNING | No MIME parts were found   |
| 6805 | WARNING | Unable to write new MIME message   |
| 6806 | WARNING | Field {0} is too large ( $\geq 512 * 1024$ bytes)  |
| 6850 | INFO    | Request is not HTTP  |
| 6851 | INFO    | HTTP POST does not contain HTML Form data. (content type= {0})   |
| 6852 | INFO    | HTTP request method not allowed: {0}   |
| 6853 | INFO    | A required Form field is missing in the request. (name={0})  |
| 6854 | FINE    | Unspecified Form field encountered but allowed through. (name={0})   |
| 6855 | INFO    | Form field value has wrong data type. (name={0}, value={1}, data type allowed={2})   |
| 6856 | INFO    | Form field occurrences < min allowed. (name={0}, occurs={1}, min occurs allowed={2})   |
| 6857 | INFO    | Form field occurrences > max allowed. (name={0}, occurs={1}, max occurs allowed={2})   |
| 6858 | INFO    | Form field is found in location not allowed. (name={0}, location not allowed={1})  |
| 6900 | WARNING | Quota exceeded on counter {0}. Assertion limit is {1} current counter value is {2}   |
| 6901 | INFO    | Quota already exceeded on counter {0}  |
| 6902 | WARNING | Invalid Quota Counter ID: {0}  |
| 6903 | WARNING | Configured max quota value {0} is too large. The max value allowed is {1}<br>(where: {0} is the value found at runtime and {1} is the maximum allowed value) |
| 6950 | INFO    | Rate limit exceeded on rate limiter {0}  |
| 6951 | INFO    | Unable to further delay request for rate limiter {0}, because maximum delay has been reached   |
| 6952 | INFO    | Unable to delay request for rate limiter {0}, because queued thread limit has been reached   |
| 6953 | INFO    | Concurrency exceeded on rate limiter {0}.  |
| 6954 | INFO    | Rate limit of {0} exceeds maximum rate limit of {1}. Setting maximum limit to {2}  |
| 7001 | WARNING | Message has no part #{0}   |
| 7002 | WARNING | Part #{0} is too large ( $\geq 512 * 1024$ bytes)  |
| 7025 | FINE    | Pattern not matched: {0}   |
| 7026 | INFO    | No patterns were matched   |
| 7027 | INFO    | Pattern matched: {0}   |
| 7050 | INFO    | Request cannot be echoed because it is not XML (Content-Type {0})  |
| 7051 | INFO    | Requests cannot be echoed because it has no Content-Type   |
| 7100 | INFO    | Comparison matched   |
| 7101 | INFO    | Comparison did not match: {0}  |
| 7102 | WARNING | Unsupported operator: {0}  |
| 7103 | WARNING | At least one comparison value was null   |
| 7104 | FINE    | Converting {0}! value into {1}   |
| 7105 | INFO    | Value of type {0} cannot be converted to {1}   |
| 7106 | INFO    | {0} value for binary predicate '{1}' is not Comparable; using value.toString() instead   |
| 7107 | INFO    | Right value of null is not supported by comparison '{0}'<br>(where '0' is the name of the comparison operator)   |
| 7150 | FINE    | Target message is not HTTP   |

|      |         |   |
|------|---------|---|
| 7151 | FINE    | No response body to check because request has not been routed yet.  |
| 7152 | WARNING | Cannot parse Request message body as XML  |
| 7153 | WARNING | {3} detected in {0} parameter \"{1}\": {2}  |
| 7154 | WARNING | {2} detected in {0}: {1}  |
| 7155 | WARNING | Message is not HTTP, cannot parse content type '{0}'  |
| 7156 | FINE    | Scanning request URL query string   |
| 7163 | WARNING | Unable to protect against code injection attacks - the request has already been routed                            |
| 7164 | FINE    | Scanning {0} message body as application/json   |
| 7165 | FINE    | Scanning request URL path   |
| 7166 | WARNING | {3} detected in {0} path \"{1}\": {2}   |
| 7200 | WARNING | Unrecognized protection name: {0}. Assertion will always fail.  |
| 7201 | WARNING | Request was flagged by SQL attack protection assertion  |
| 7203 | WARNING | Unable to protect against SQL attacks - the request has already been routed                                       |
| 7204 | WARNING | {0} was flagged by Protect Against SQL Attacks Assertion  |
| 7205 | FINE    | No response body to check because request has not been routed yet.  |
| 7210 | FINE    | Target message is not HTTP  |
| 7211 | FINE    | Scanning request URL query string   |
| 7212 | FINE    | Scanning {0} message body as text.  |
| 7213 | WARNING | Cannot parse {0} as {1}   |
| 7214 | WARNING | {3} detected in {0} parameter \"{1}\":{2}   |
| 7215 | WARNING | {2} detected in {0}: {1}  |
| 7216 | FINE    | Scanning request URL path   |
| 7217 | WARNING | {3} detected in {0} path \"{1}\": {2}   |
| 7220 | WARNING | Request body size exceeds configured limit  |
| 7221 | WARNING | Request first part size exceeds configured limit  |
| 7222 | WARNING | {0} body size exceeds configured limit  |
| 7223 | WARNING | {0} first part size exceeds configured limit  |
| 7224 | WARNING | {0} content type is syntactically invalid: {1}  |
| 7225 | WARNING | {0} message has already been buffered   |
| 7230 | WARNING | Unable to protect against document structure threats -- the request has already been routed                       |
| 7231 | WARNING | Request includes an oversized text node or attribute value  |
| 7232 | WARNING | Request XML nesting depth exceeds the policy limit  |
| 7233 | WARNING | Request message SOAP Body has too many children   |
| 7234 | WARNING | Request message does not have a valid SOAP Envelope   |
| 7235 | WARNING | Request message is not well-formed XML  |
| 7238 | WARNING | {0} includes an oversized text node or attribute value  |
| 7239 | WARNING | {0} XML nesting depth exceeds the policy limit  |
| 7240 | WARNING | {0} message SOAP Body has too many children   |
| 7241 | WARNING | {0} message does not have a valid SOAP Envelope   |
| 7242 | WARNING | {0} is not XML.   |
| 7243 | FINE    | No response body to check because request has not been routed yet.  |
| 7244 | WARNING | Message variable {0} does not contain well-formed XML   |
| 7245 | INFO    | Message variable {0} does not contain XML   |
| 7248 | WARNING | Message variable {0} does not contain XML<br>(where: {0} is the variable name, which may or may not have a value) |
| 7300 | INFO    | The current request did not contain credentials of any supported type   |
| 7301 | WARNING | WS-Federation response did not contain a security token of a supported type                                       |
| 7302 | WARNING | WS-Federation response had non-200 status   |
| 7303 | INFO    | Cannot replace security token in non-XML message  |
| 7304 | WARNING | Unable to replace security token  |
| 7305 | INFO    | Original security token was not XML; cannot remove from request   |
| 7306 | WARNING | Multiple security tokens found in request   |

|      |         |  |
|------|---------|--|
| 7307 | WARNING | HTTP failure while communicating with WS-Federation server   |
| 7308 | WARNING | Unknown encoding from WS-Federation server   |
| 7309 | WARNING | Cannot parse HTML from WS-Federation server  |
| 7310 | WARNING | Invalid IP/STS URL in policy configuration   |
| 7311 | WARNING | Authentication with service failed   |
| 7312 | WARNING | Not authorized to access this service  |
| 7401 | INFO    | Request not SOAP; unable to check for WS-Security Binary Security Token                                      |
| 7402 | INFO    | Request did not contain any WSS level security   |
| 7403 | INFO    | No tokens were processed from this request; returning AUTH_REQUIRED  |
| 7404 | INFO    | This assertion did not find a Kerberos Binary Security Token to use as credentials. Returning AUTH_REQUIRED. |
| 7405 | FINE    | Kerberos ticket processed, principal is:{0}  |
| 7406 | FINE    | Kerberos session processed, principal is:{0}   |
| 7407 | WARNING | Either the Kerberos server configuration is invalid or the KDC is unreachable                                |
| 7408 | WARNING | Could not process Kerberos ticket (not for this service?)  |
| 7500 | WARNING | No identity mapping for provider #{0} found in attribute #{1}  |
| 7501 | WARNING | No security token mapping for provider #{0} found in attribute #{1}  |
| 7502 | WARNING | No suitable value could be found in any security token   |
| 7503 | WARNING | No matching identities could be found  |
| 7504 | WARNING | No value could be found from any matching identity   |
| 7600 | INFO    | Request not SOAP; unable to check for WS-I Basic Security Profile compliance                                 |
| 7601 | INFO    | Response not SOAP; unable to check for WS-I Basic Security Profile compliance                                |
| 7602 | WARNING | WS-I BSP rule broken in request ({0}): {1}   |
| 7603 | WARNING | WS-I BSP rule broken in response ({0}): {1}  |
| 7604 | INFO    | Failing non WS-I BSP compliant request   |
| 7605 | INFO    | Failing non WS-I BSP compliant response  |
| 7606 | WARNING | Server WS-I BSP rules are incorrect  |
| 7700 | INFO    | Request not SOAP; unable to check for WS-I SAML Token Profile compliance                                     |
| 7701 | INFO    | Response not SOAP; unable to check for WS-I SAML Token Profile compliance                                    |
| 7702 | WARNING | WS-I SAML Token Profile rule broken in request ({0}): {1}  |
| 7703 | WARNING | WS-I SAML Token Profile rule broken in response ({0}): {1}   |
| 7704 | INFO    | Failing non WS-I SAML Token Profile compliant request  |
| 7705 | INFO    | Failing non WS-I SAML Token Profile compliant response   |
| 7706 | WARNING | Server WS-I SAML Token Profile rules are incorrect.  |
| 7800 | INFO    | The assertion is not applicable because the request is either not XML or not SOAP                            |
| 7801 | INFO    | No Timestamp found in the request  |
| 7802 | WARNING | Timestamp found in the request, but was not signed   |
| 7803 | WARNING | Timestamp found in the request, but Created time was too far in the future                                   |
| 7804 | WARNING | Timestamp found in the request, but expired too long ago   |
| 7805 | WARNING | Timestamp found in the request, but has no Expires time  |
| 7806 | WARNING | Timestamp found in the request and is not expired, but lifetime exceeds configured maximum                   |
| 7807 | WARNING | Timestamp found in the request, but has no Created time  |
| 7809 | WARNING | Timestamp found in the request, but is expired when constrained to maximum allowed lifetime                  |
| 7900 | WARNING | Unsupported security token type: {0}   |

|      |         |  |
|------|---------|--|
| 7901 | WARNING | No credentials were available from the request   |
| 7902 | WARNING | Credentials were available, but no username could be found   |
| 7903 | WARNING | Password inclusion was requested, but no password could be found   |
| 7904 | WARNING | Specified context variable exists but does not contain a WS-SecureConversation session   |
| 7905 | WARNING | SAML assertion variable did not contain a valid SAML assertion: {0}  |
| 7906 | INFO    | Unable to identify the encryption recipient because we are decorating a response to a request with multiple eligible tokens. Encryption recipient must be specified explicitly.                                  |
| 7907 | WARNING | The SAML assertion uses a secret key for subject confirmation, but the Gateway does not already possess this key, and is unable to unwrap it from the EncryptedKey   |
| 7908 | WARNING | The SAML assertion uses a secret key for subject confirmation, but but the Gateway does not already possess this key, and is unable to unwrap it from the EncryptedKey: {0}<br>(where: {0} is the encrypted key) |
| 8000 | INFO    | Assertion '{0}'; {1}   |
| 8001 | WARNING | Assertion '{0}'; {1}   |
| 8100 | INFO    | Could not match WSDL operation ({0} instead of {1})  |
| 8101 | INFO    | Cannot identify any WSDL operation from request  |
| 8200 | WARNING | Could not process Kerberos token (Negotiate) error is '{0}'  |
| 8300 | INFO    | Request not FTP; unable to extract FTP credentials   |
| 8301 | FINE    | Not authenticated  |
| 8302 | FINE    | Found credentials for user {0}   |
| 8400 | FINE    | Issued SAML Authentication statement   |
| 8401 | FINE    | Issued SAML Attribute statement  |
| 8402 | FINE    | Issued SAML Authorization Decision statement   |
| 8403 | FINE    | Adding attribute {0} = {1}   |
| 8404 | WARNING | NameIdentifier configured as "From Authenticated User", but no user has been authenticated   |
| 8405 | WARNING | Message is not XML   |
| 8406 | WARNING | Message is not SOAP  |
| 8407 | WARNING | Message appeared to be SOAP but is not valid   |
| 8408 | WARNING | WS-Security decoration failed  |
| 8409 | WARNING | Specified NameIdentifier chosen, but no value specified; using default   |
| 8410 | FINE    | One or more configured Attributes are missing: {0}   |
| 8411 | WARNING | Ignoring invalid filter Attribute / AttributeDesignator value: {0}   |
| 8412 | FINE    | Attribute filter contained one or more unknown Attribute / AttributeDesignator elements: {0}   |
| 8413 | WARNING | Attribute filter values contained duplicate Attribute / AttributeDesignator elements: {0}  |
| 8414 | FINE    | No Attributes were available after SAML Attribute filter was applied   |
| 8415 | FINE    | Attribute filter AttributeValue excluded some Attributes: {0}  |
| 8416 | FINE    | Attribute filter filtered some Attributes: {0}   |
| 8417 | WARNING | Error parsing the {0} for expected SOAP Message: {1}<br>(where {0} is 'request' or 'response' and {1} are the details of the error)  |
| 8418 | WARNING | Message appeared to be SOAP but is not valid: {0}  |
| 8419 | FINE    | Resolved value for Attribute '{0}' was filtered as its value '{1}' was not included in the corresponding filter Attribute's AttributeValue   |
| 8420 | WARNING | Problem processing Attribute Statement: {0}  |
| 8421 | FINE    | Filter expression '{0}' yielded no values  |

|      |         |  |
|------|---------|--|
| 8450 | INFO    | No user from the expected identity provider has yet been authenticated                         |
| 8451 | INFO    | Multiple users from the expected identity provider have been authenticated; choosing the first |
| 8500 | WARNING | Included policy was updated, and is now invalid: {0}   |
| 8501 | WARNING | Included policy #{0} ({1}) could not be located  |
| 8502 | WARNING | Included policy failure: {0}   |
| 8550 | WARNING | Required WS-Addressing headers not present   |
| 8551 | WARNING | Required signed WS-Addressing headers not present  |
| 8552 | FINE    | WS-Addressing headers present  |
| 8553 | FINE    | No WS-Addressing headers found   |
| 8554 | FINE    | No signed WS-Addressing headers found  |
| 8555 | FINE    | Found WS-Addressing headers for namespace {0}  |
| 8556 | FINE    | Found signed WS-Addressing headers for namespace {0}   |
| 8600 | FINE    | Sending response early   |
| 8601 | WARNING | Unable to send early response for non HTTP messages  |
| 8602 | WARNING | Invalid response status: {0}   |
| 8604 | INFO    | Found {0} results for field {1}. Only the first value will be used                             |
| 8650 | WARNING | Unable to decorate message: Message not SOAP   |
| 8651 | WARNING | Unable to decorate message: Parse failure: {0}   |
| 8652 | WARNING | Unable to decorate message: No credentials have been collected                                 |
| 8653 | WARNING | Unable to decorate message: Invalid Document Format: {0}                                       |
| 8654 | WARNING | Unable to decorate message: {0}  |
| 8700 | WARNING | {0} variable has not been set; unable to proceed   |
| 8701 | WARNING | {0} parse failure: {1}   |
| 8702 | WARNING | {0} is not SOAP  |
| 8703 | WARNING | {0} did not contain a signed SAML assertion  |
| 8704 | WARNING | {0} did not contain a signed wsu:Timestamp   |
| 8705 | WARNING | {0} did not contain a signed wsa:MessageID   |
| 8706 | WARNING | {0} SOAP Body was not signed   |
| 8707 | WARNING | {0} contained the expected elements, but they were covered by different Signatures             |
| 8780 | INFO    | Request is not HTTP; could not get domain ID injection header                                  |
| 8781 | INFO    | Requestor did not attempt to include domain ID information                                     |
| 8782 | WARNING | Invalid format for {0}: {1}  |
| 8783 | WARNING | Requestor attempted to gather domain ID information but encountered an error                   |
| 8784 | INFO    | Requestor explicitly declines to provide domain ID information                                 |
| 8785 | WARNING | Requestor provided incomplete domain ID information  |
| 8786 | WARNING | Requestor did not include required identifier: {0}   |
| 8800 | WARNING | Message is not XML.  |
| 8801 | WARNING | Unable to insert element because no existing element was found                                 |
| 8802 | WARNING | Unable to insert element because more than one existing element was found                      |
| 8803 | WARNING | Unable to insert element because the new element was not a well-formed XML fragment            |
| 8850 | WARNING | Message is not SOAP.   |
| 8851 | WARNING | Unable to decorate {0}: {1}  |
| 8852 | WARNING | Could not find trusted certificate {0}   |
| 8853 | WARNING | Error when finding trusted certificate {0}: {1}8900  |
| 8854 | INFO    | Error checking certificate expiry for {0}  |
| 8900 | WARNING | Error generating request: {0}  |
| 8901 | INFO    | A value for {0} was not found. Cannot add <Attribute> element to the {1} element               |
| 8902 | INFO    | Assertion failed: a value for {0} was not found  |

|      |         |  |
|------|---------|--|
| 8903 | WARNING | XML attribute name {0} with value {1} are not valid for an XML attribute   |
| 8905 | INFO    | Incorrect xpath result type {0} found for field {1}. Cannot add <Attribute> element to the {2} element   |
| 8906 | INFO    | Xpath base expression {0} found no results   |
| 8907 | INFO    | Invalid value for issue instant: {0} IssueInstant, if supplied, must be a valid datetime with a format "yyyy-MM-dd'T'HH:mm:ss[Z]"  |
| 8908 | INFO    | Not all values from {0} were used as {1} also part of iteration and had less values  |
| 8909 | INFO    | Only {0} values from all referenced context variables will be used. The largest referenced variable has {1} values.  |
| 8910 | INFO    | Namespace prefix {0} with incorrect namespace URI may cause XPath base pattern to match no results   |
| 8911 | INFO    | Unsupported type of mixed content found for Attributevalue: {0}  |
| 8912 | WARNING | Cannot import XML element into XACML request document: {0}   |
| 8930 | WARNING | Error processing XACML request: {0}  |
| 8931 | WARNING | XACML request is not SOAP encapsulated   |
| 8932 | WARNING | XACML request namespace is not recognized: {0}   |
| 8960 | WARNING | Error encoding MTOM message: {0}   |
| 8961 | INFO    | Not encoding MTOM message, no elements found to encode.  |
| 8962 | WARNING | Invalid XPath expression for MTOM encoding {0}   |
| 8963 | WARNING | XPath expression did not match.  |
| 8964 | WARNING | Error decoding MTOM message: {0}   |
| 8965 | WARNING | Error validating MTOM message: {0}   |
| 9002 | INFO    | Message context mapping overridden {0}   |
| 9003 | WARNING | Message context mapping dropped {0}  |
| 9004 | WARNING | Message context mapping value truncated {0}  |
| 9050 | WARNING | Error processing management request {0}  |
| 9100 | WARNING | JDBC Connection Pooling cannot start due to: {0}   |
| 9101 | WARNING | Cannot configure a pool associated with a JDBC connection {0} due to: {1}  |
| 9102 | WARNING | Cannot delete a pool associated with a JDBC connection {0} due to: {1}   |
| 9103 | WARNING | The Gateway would not configure a disabled JDBC connection {0}   |
| 9104 | WARNING | "Perform JDBC Query" assertion failed due to: {0}  |
| 9105 | WARNING | "Perform JDBC Query" assertion failed due to no query results via a connection {0}   |
| 9105 | INFO    | "Perform JDBC Query" assertion failed due to no query results via a connection {0}<br>(The INFO version of code is returned when the "Perform JDBC Query Assertion" is configured to "Fail if no results returned by query") |
| 9130 | INFO    | JSON Schema validation failure: {0}  |
| 9131 | INFO    | {0} is not well-formed JSON  |
| 9132 | FINEST  | Validating {0} against JSON schema   |
| 9133 | FINEST  | JSON Schema validation success   |
| 9134 | WARNING | Cannot validate JSON schema because JSON schema information cannot be retrieved: {0} (This is caused when resource is unavailable or JSON data is invalid.)  |
| 9160 | WARNING | Error encoding or decoding: {0}  |
| 9161 | WARNING | Strict processing failed   |
| 9162 | WARNING | Variable of type [0] could not be created from decoded data: [1]   |
| 9163 | WARNING | Variable of type {0} cannot be accessed as {1} for encoding or decoding  |
| 9164 | WARNING | Error accessing variable of type {0}: {1}<br>(This is caused when the source cannot be processed (e.g., text required and Message is not a text content type)  |
| 9190 | WARNING | Cannot {0} SAML Protocol Response: {1}   |



|      |         |   |
|------|---------|---|
| 9230 | WARNING | SAML 2.0 web SSO profile rule violation: {0}  |
| 9231 | WARNING | Cannot access AuthnRequest for binding '{0}': '{1}'   |
| 9232 | WARNING | Cannot Invalid AuthnRequest: '{0}'  |
| 9233 | WARNING | Cannot Signature validation failure: '{0}'  |
| 9234 | WARNING | SAML 1.1 Web SSO profile rule violation: {0}  |
| 9260 | WARNING | Target message has no associated SOAPAction. Cannot automatically add the Action element.   |
| 9261 | WARNING | Action is a required WS-Addressing messaging property. No value found at runtime.   |
| 9262 | WARNING | Action extension element not found in the WSDL.   |
| 9263 | INFO    | Invalid URI value {0} for WS-Addressing {1} property.<br>(where: 0 is the invalid value, 1 is the property which had this invalid value)              |
| 9264 | WARNING | Invalid URI value {0} for required WS-Addressing {1} property.<br>(where: 0 is the invalid value, 1 is the property which had this invalid value)     |
| 9265 | WARNING | Invalid namespace: {0}. {1}.<br>(where 0 is the invalid namespace, 1 is the reason it is invalid)   |
| 9290 | WARNING | Invalid RST SOAP Request: {0}   |
| 9291 | WARNING | Invalid Security Token: {0}   |
| 9292 | WARNING | Expired Secure Conversation Session: {0}  |
| 9293 | WARNING | Authentication Failure: {0}   |
| 9294 | WARNING | Authorization Failure: {0}  |
| 9295 | WARNING | Unable to issue token: {0}  |
| 9330 | WARNING | Error building RST: {0}   |
| 9331 | WARNING | Unable to create RST message variable {0}   |
| 9350 | WARNING | {0} is not SOAP   |
| 9351 | WARNING | {0} parse failure: {1}  |
| 9352 | WARNING | Invalid response: {0}   |
| 9353 | WARNING | Error processing encrypted key: {0}   |
| 9354 | WARNING | Expected token of type {0}, but found: {1}  |
| 9380 | WARNING | Session Lookup Failure: {0}   |
| 9381 | WARNING | Outbound Secure Conversation Establishment Failure: {0}   |
| 9400 | WARNING | The request was not an HTTP request, failing assertion.   |
| 9401 | WARNING | Multiple cookie values were detected, failing assertion.  |
| 9402 | WARNING | The expected cookie value was not found, failing assertion.   |
| 9403 | WARNING | Looking for a {0} parameter, but the request was not a {0} request, failing assertion.<br>(where: 0 is the request type (GET, POST, or GET and POST)) |
| 9404 | WARNING | The expected parameter was not found, failing assertion.  |
| 9405 | WARNING | The parameter had more than one value, failing assertion.   |
| 9406 | WARNING | The parameter did not match the cookie value, failing assertion.  |
| 9407 | WARNING | The HTTP-Referer header was not provided but it is required, failing assertion.   |
| 9408 | WARNING | The HTTP-Referer header was provided multiple times, failing assertion.   |
| 9409 | WARNING | The HTTP-Referer header value '{0}' was not valid, failing assertion.<br>(where: {0} is the invalid HTTP Referer value)                               |
| 9420 | WARNING | Failed to perform transformation  |
| 9430 | INFO    | Request not SSH; unable to extract SSH credentials  |
| 9431 | FINE    | Not authenticated   |
| 9432 | FINE    | Found credentials for user <user_login>   |
| 9433 | WARNING | No user name found for passing through to SSH server  |
| 9434 | WARNING | SSH routing error: {0}  |
| 9435 | FINE    | SSH routing: Finished sending file: {0} in Session: {1}<br>SSH routing: Finished retrieving file: {0} in Session: {1}                                 |

|      |         |   |
|------|---------|---|
| 9445 | WARNING | Invalid timeout value from timeout ({0}). Timeout value must be a valid integer with range 1 to 3600 inclusive. |
| 9446 | WARNING | Invalid port specified, port must be between 1 and 63353: {0}.  |
| 9447 | WARNING | Invalid ICAP URI: {0}   |
| 9448 | WARNING | Unable to connect to the specified server: {0}  |
| 9449 | WARNING | I/O error occurred while scanning message {0}   |
| 9450 | WARNING | Error reading MIME content from {0} : {1}   |
| 9451 | WARNING | Error occurred while scanning content {0} : {1}   |
| 9452 | WARNING | Service not available {0}   |
| 9453 | WARNING | No valid ICAP server entries found  |
| 9454 | WARNING | Virus detected in {0} ({1})   |
| 9455 | WARNING | ICAP Status: ({0}: {1})   |
| 9456 | WARNING | {0}   |
| 9457 | WARNING | No ICAP response received   |
| 9458 | WARNING | Unsupported encoding: {0}   |
| 9500 | INFO    | Invalid AttributeQuery: {0}   |
| 9501 | INFO    | AttributeQuery request is not SOAP encapsulated   |
| 9502 | INFO    | Unsupported value found for {0} in AttributeQuery. Found {1} expected one of {2}                                |
| 9503 | INFO    | Unexpected results after decrypting encrypted name identifier: {0}  |
| 9504 | FINE    | EncryptedID element found but not decrypted. Context variables related to Subject will have no values           |
| 9550 | FINE    | Looking up certificate for name {0}   |
| 9551 | WARNING | Certificate not found for name {0}  |
| 9552 | WARNING | Multiple certificates found for name {0}  |
| 9553 | WARNING | Error looking up certificate {0}  |
| 9554 | FINE    | Looking up certificate for {0}{1}   |
| 9555 | WARNING | Certificate not found for {0}{1}  |
| 9556 | WARNING | Multiple certificates found for {0}{1}  |
| 9557 | WARNING | Error looking up certificate for {0}{1}   |
| 9580 | WARNING | Invalid URI value found for {0}: {1}  |
| 9581 | WARNING | Failed to build SAML Protocol Request: {0}  |
| 9610 | FINER   | Routing request to protected service  |
| 9611 | WARNING | Did not receive a routing reply within the timeout period of {0} ms; empty response being returned              |
| 9612 | FINER   | Received routing reply  |
| 9613 | INFO    | No response expected from protected service   |
| 9614 | FINE    | Outbound request endpoint {0} specifies NO_REPLY  |
| 9615 | FINE    | Outbound request endpoint {0} specifies REPLY_TO_OTHER, setting replyToQueueName to {1}                         |
| 9616 | WARNING | Failed to establish MQ connection on try #{0}. will retry after {1}ms   |
| 9617 | WARNING | Tried {0} times to establish MQ connection and failed   |
| 9618 | FINE    | Outbound request endpoint {0} specifies AUTOMATIC, using temporary queue  |
| 9619 | WARNING | Request message too large   |
| 9620 | WARNING | Response message too large  |
| 9621 | WARNING | Invalid MQ configuration {0}  |
| 9622 | WARNING | Error processing MQ outbound template {0}   |
| 9623 | FINER   | Ignoring invalid response timeout: {0}  |
| 9624 | FINER   | Using response timeout {0}ms  |
| 9625 | WARNING | Ignoring invalid response size limit: {0}   |
| 9626 | FINER   | Using response size limit {0} (bytes)   |
| 9630 | WARNING | Routing completed with warning status. Reason code: {0}'  |
| 9635 | WARNING | '{0}' is not set  |
| 9636 | WARNING | Unsupported Algorithm: '{0}'  |
| 9637 | WARNING | Invalid key: '{0}'  |
| 9638 | WARNING | Error generating hash signature   |

|      |         |   |
|------|---------|---|
| 9645 | WARNING | Source is not a valid JSON  |
| 9646 | WARNING | Invalid JSON Path expression '{0}'  |
| 9647 | WARNING | Invalid Evaluator: {0}  |
| 9648 | WARNING | Error occurred evaluating JSON Path: {0}  |
| 9649 | WARNING | Could not find any matching results; assertion therefore fails; Expression is {0}   |
| 9655 | INFO    | Context variable {0} is not found.  |
| 9656 | WARNING | Source variable is not set.   |
| 9657 | WARNING | Target output variable is not set.  |
| 9658 | WARNING | Invalid variable syntax: {0}  |
| 9659 | WARNING | {0} is not a supported data type.   |
| 9660 | WARNING | Target data type is {0} but found {1}.  |
| 9670 | WARNING | Found duplicate oauth parameter: x  |
| 9671 | WARNING | Invalid request url: invalidurl   |
| 9672 | WARNING | Http method is empty  |
| 9673 | INFO    | OAuth parameters found: [(oauth_consumer_key, asdf), (oauth_callback, foobar)]  |
| 9674 | WARNING | Required oauth parameter is missing or empty: x   |
| 9721 | WARNING | Service route failed, feedback: {0}   |
| 9722 | WARNING | Strategy {0} returned no route.   |
| 9723 | WARNING | {0} variable not found in policy enforcement context  |
| 9724 | WARNING | {0} variable is not the right type.   |
| 9725 | WARNING | Create Routing Strategy Assertion has no routes!  |
| 9670 | WARNING | Found duplicate oauth parameter: x  |
| 9671 | WARNING | Invalid request url: invalidurl   |
| 9672 | WARNING | Http method is empty  |
| 9673 | INFO    | OAuth parameters found: [(oauth_consumer_key, asdf), (oauth_callback, foobar)]  |
| 9674 | WARNING | Required oauth parameter is missing or empty: x   |
| 9701 | WARNING | Protocol Transition option does not support kerberos credentials<br>(where the delegation method is "Protocol Transition")  |
| 9701 | WARNING | Constrained Proxy option does not support non-kerberos credentials<br>(where the delegation method is "Constrained Proxy")  |
| 9702 | WARNING | Unable to obtain Kerberos Service Ticket: {0}   |
| 9703 | WARNING | Unable to find stored gateway account password: {0}   |
| 9704 | WARNING | Unable to obtain kerberos service ticket for service principal: {0}   |
| 9705 | WARNING | Unable to find login credentials  |
| 9706 | FINE    | Added Kerberos Credentials to Authentication Context.<br>Service Principal  |
| 9707 | WARNING | Unable to handle Realm: {0}   |
| 9708 | WARNING | Error message returned from KDC: {0}  |
| 9721 | WARNING | Service route failed, feedback: {0}   |
| 9722 | WARNING | Strategy {0} returned no route  |
| 9723 | WARNING | {0} variable not found in policy enforcement context  |
| 9724 | WARNING | {0} variable is not the right type!   |
| 9725 | WARNING | Create Routing Strategy Assertion has no routes!  |
| 9800 | WARNING | Resolved maximum acceptable cache age value is invalid<br>'{0}'. Value must be in seconds between '{1}' and '{2}' inclusive |
| 9801 | FINE    | Retrieved from cache: '{0}'   |
| 9802 | FINE    | Cache miss with key: '{0}'  |
| 9900 | WARNING | Invalid configuration value: {0}  |
| 9920 | WARNING | OTK Installation Problem: {0}   |

|       |         |  |
|-------|---------|--|
| 9921  | INFO    | Component {0} conflicts for {1}: {2}<br>where: {0} is the name of the OTK component e.g. 'OAuth 2.0', {1} is either Services, Policies or JDBC Connections and {2} is the name of the conflict   |
| 10000 | WARNING | No certificate found for variable:foo  |
| 10001 | WARNING | Certificate CN=foo validation(valType)failed with status:status  |
| 10002 | WARNING | Certificate CN=foo validation(valType)failed: message  |
| 10020 | WARNING | The custom logger name uses non-existing context variables: {0}.<br>The custom logger name now falls back to the default package name, {1}<br>(where: {0} is the invalid context variable name(s) and {1} is "com.17tech.server.policy.assertion.ServerAuditDetailAssertion")                  |
| 10021 | WARNING | The custom logger name contains invalid package name derived from context variable(s): {0}. The custom logger name now falls back to the default package name, {1}.<br>(where: {0} is the context variable name(s) and {1} is "com.17tech.server.policy.assertion.ServerAuditDetailAssertion") |
| 10100 | WARNING | "{0} assertion: SiteMinder Policy Server Error: {1}"   |
| 10101 | FINE    | SiteMinder {0} assertion: {1}  |
| 10102 | WARNING | SiteMinder {0} assertion: {1}  |
| 10200 | WARNING | Radius Server Error: {0}   |
| 10201 | INFO    | No credentials found!  |
| 10202 | FINE    | Authentication Against Radius Server failed for credentials: {0}   |
| 10350 | FINE    | Added header/property with name {0} and value {1}  |
| 10351 | FINE    | Removed header/property with name {0}  |
| 10352 | FINE    | Removed header/property with name {0} and value {1}  |
| 10353 | WARNING | Header/property name is empty  |
| 10400 | WARNING | Cookie max age is invalid: {0}   |
| 10401 | WARNING | Cookie name is null or empty   |
| 10402 | FINE    | No cookies matched   |
| 10403 | WARNING | A cookie with name {0}, domain {1} and path {2} already exists   |
| 10404 | FINE    | Added cookie with name {0} and value {1}   |
| 10405 | FINE    | Removed cookie with name {0} and value {1}   |
| 10406 | WARNING | Cookie version is invalid: {0}   |
| 10407 | WARNING | Cookie {0} is null or empty<br>(where: {0} is the attribute name; occurs when a context variable resolves to empty at runtime)   |
| 10450 | WARNING | Text to search is empty<br>(NOTE: Audit 10450 will cause the Replace Tag Content Assertion to fail at run time, as the context variables were resolved to empty.)  |
| 10451 | WARNING | Tags to search is empty<br>(NOTE: Audit 10451 will cause the Replace Tag Content Assertion to fail at run time, as the context variables were resolved to empty.)  |
| 10452 | WARNING | Ignoring empty tag   |
| 10453 | FINE    | Tag not found: {0}   |
| 10454 | FINE    | No replacements performed  |
| 10500 | INFO    | {0} is not JSON  |
| 10501 | WARNING | {0} is not well-formed JSON  |
| 10502 | WARNING | Container depth constraint violated at line {0}  |
| 10503 | WARNING | Object entry count constraint violated at line {0}   |
| 10504 | WARNING | Array entry count constraint violated at line {0}  |
| 10505 | WARNING | Entry name length constraint violated at line {0}  |
| 10506 | WARNING | String value length constraint violated at line {0}  |

```

10600  WARNING  The specified Service Metadata Document is invalid: {0}
10601  WARNING  Could not parse OData resource path: {0}
10602  WARNING  {0} payload could not be parsed: {1}
10603  WARNING  Request for Service Metadata Document attempted
10604  WARNING  Request for raw value attempted: {0}
10605  WARNING  OData request attempted using forbidden operation '{0}'
10606  WARNING  Unable to parse {0} expression: {1}
10607  WARNING  {0} is not an HTTP request; cannot automatically determine HTTP
method
10608  WARNING  Invalid OData HTTP method: '{0}'
10609  WARNING  HTTP method is null or empty

```

## Customizing the Audit Format for Logging

You can customize the format of audit messages that are recorded to a file or Syslog. There are three types of audit messages generated by the Gateway:

- Administrative actions
- System events
- Message processing events

These message types are described in greater detail in Message Auditing.

For the purposes of customizing the audit format, the three message types are grouped into the following two categories:

- **Service-related:** These are the *message processing* events
- **Other:** These are the *administrative* actions and *system* events

The following terms are used to describe the parts of the audit information that can be customized:

- *header*: This is the first log message related to processing of a message.
- *details*: This is the detail log message for each audit detail.
- *footer*: This is the final log message and relates to the audit record.

For service-related events, you can customize the header, footer, and details using these cluster properties:

Table 189: Cluster properties to customize audit format

|          | Cluster Property                      | Description   | Default                                    |
|----------|---------------------------------------|---|--|
| <b>1</b> | <i>audit.log.service.headerFormat</i> | Format for the first log message of a service audit | <i>Processing request for service: {3}</i> |
| <b>2</b> | <i>audit.log.service.footerFormat</i> | Format for the final (summary)                      | <i>{1}</i>                                 |

|          | Cluster Property                      | Description                                       | Default        |
|----------|---------------------------------------|---|----------------|
|          |                                       | log message of a service audit                    |                |
| <b>3</b> | <i>audit.log.service.detailFormat</i> | Format for details related to a service audit     | <i>{0}:{1}</i> |
| <b>4</b> | <i>audit.log.other.format</i>         | Format used for other (non-service) audit logs    | <i>{1}</i>     |
| <b>5</b> | <i>audit.log.other.detailFormat</i>   | Format used for other (non-service) audit details | <i>{0}:{1}</i> |

The following table describes in greater detail the variables that can be used in each cluster property.

Table 190: Validity of variables for audit format cluster properties

| Variable | Description         | Example                            | Available for: |     |     |     |     |
|----------|---------------------|------------------------------------|----------------|-----|-----|-----|-----|
|          |                     |                                    | 1              | 2   | 3   | 4   | 5   |
| {0}      | Audit message ID    | 1234                               | Yes            | No  | No  | Yes | No  |
| {1}      | Audit message       | Authentication required            | Yes            | No  | Yes | Yes | Yes |
| {2}      | Service entity ID   | a1g38fj352da                       | Yes            | Yes | Yes | No  | No  |
| {3}      | Service description | Warehouse or Warehouse [warehouse] | Yes            | Yes | Yes | No  | No  |

For even greater flexibility, you can add a context variable before the *{x}* placeholder variables for service-related events. This will insert the contents of the specified context variable when the audit is logged. For example:

```
audit.log.service.headerFormat = ${requestId}: processing message.
audit.log.service.footerFormat = ${requestId}: {1}
audit.log.service.detailFormat = ${requestId}: {0}: {1}
```

---

**Note:** When using context variables, the maximum length permitted per variable is 1000 characters. The overall message size is limited to 10000 characters, subject to any limitations of the sink (for example, syslog size limits).

---

## Appendix G: Key Usage Enforcement Policy

A key usage enforcement policy is XML code that dictates how an X.509 Certificate may be used by the Gateway. This policy is in effect by default, but is ignored if key usage is overridden to provide more lenient usage.

The default enforcement policy delivered with the Gateway should be adequate for most scenarios, but you can override it with a customized version if you have specific enforcement needs.

---

**Note:** Creating a key usage enforcement policy is intended for advanced users. Please consult CA Technical Support if you are not familiar with the process or to determine whether overriding the default policy is necessary.

---

➤ To use a customized key usage enforcement policy:

1. Access the [Manage Cluster-Wide Properties](#) task.
2. Add the new key usage enforcement policy to the [pkix.keyUsagePolicy](#) cluster property. A sample template is given below to help you get started.
3. Restart the Gateway.

## Recognized Action Names

The following key usage activity names are recognized by the Gateway:

Table 191: Recognized key usage actions

| Action                  | Description                                     | Notes  |
|-------------------------|---|--|
| <b>verifyXml</b>        | Verifies signed XML using public key            |  |
| <b>encryptXml</b>       | Encrypts XML with public key, for private key   |  |
| <b>sslServerRemote</b>  | Allows handshake with remote server certificate | The client performs this check during an outgoing SSL connection |
| <b>sslClientRemote</b>  | Allows handshake with remote client certificate | The server performs this check during an incoming SSL connection |
| <b>verifyClientCert</b> | Verifies certificates signed                    | Check performed during certificate chain                         |

| Action            | Description   | Notes  |
|-------------------|---|--|
|                   | by this certificate   | verification   |
| <b>verifyCrl</b>  | Verifies the Certificate Revocation List signed by this certificate   | Check performed by Gateway's CertValidationProcessor during authentication and during outbound SSL |
| <b>decryptXml</b> | Decrypts XML with public key that was encrypted using the private key | This action is highly unusual. The Gateway will never attempt to do this in normal use.            |
| <b>signXml</b>    | Signs XML using public key  | This action is highly unusual. The Gateway will never attempt to do this in normal use.            |

## Sample Enforcement Policy Template

You can use the following sample template to help you get started. Refer to the embedded comments for more details. The actions are highlighted.

```
<keyusagepolicy xmlns="http://www.layer7tech.com/ws/keyusage">
<!-- A permit rule without an action applies to every action -->
<permit><req>anyExtendedKeyUsage</req></permit>
<!-- A permit rule without requirements always succeeds -->
<permit action="signXml"/> <permit action="decryptXml"/>
<!-- Multiple permit rules may be specified for an activity.
At least one permit rule must succeed. -->
<permit action="verifyXml"><req>digitalSignature</req></permit>
<permit action="verifyXml"><req>nonRepudiation</req></permit>
<!-- Multiple requirements may be specified for a permit rule.
All requirements must match for that permit rule to succeed. -->
<permit action="sslClientRemote"><re-
q>digitalSignature</req><req>keyEncipherment</req></permit>
<permit action="sslClientRemote"><re-
q>nonRepudiation</req><req>keyEncipherment</req></permit>
<!-- An ext. key usage requirement may use a dotted-decimal OID. -->
<permit action="sslClientRemote"><req>1.3.6.1.5.5.7.3.2</req></permit>
<permit action="encryptXml"><req>keyEncipherment</req></permit>
<permit action="sslServerRemote"><req>keyEncipherment</req></permit>
<permit action="sslServerRemote"><req>keyAgreement</req></permit>
<permit action="sslServerRemote"><req>id-kp-serverAuth</req></permit>
<permit action="verifyClientCert"><req>keyCertSign</req></permit>
<permit action="verifyCrl"><req>CRLSign</req></permit>
</keyusagepolicy>
```

To create an "Or" logic permission within an action, use this syntax:

```
<!-- key_usage_value_1 or key_usage_value_2 is required for permission of action_value -
->
<permit action="action_value"><req>key_usage_value_1</req></permit>
<permit action="action_value"><req>key_usage_value_2</req></permit>
```

To create an "And" logic permission within an action, use this syntax:

```
<!-- both key_usage_value_1 and key_usage_value_2 are required for permission of action_
value -->
```



```
<permit action="action_value"><req>key_usage_value_1</req><req>key_usage_value_2</req></permit>
```

### Notes from sample template:

- The enforcer may do zero, one, or two passes through the policy depending on what critical extensions are present:
  - If there is neither a critical KeyUsage nor a critical ExtKeyUsage in the certificate, the enforcer always permits the activity.
  - If there is a critical KeyUsage, the enforcer will scan the policy from top to bottom for a matching KeyUsage permit rule. If it reaches the end of the policy without finding one, the policy is denied. A permit rule pertains to the KeyUsage if it is a blanket permit, or if it contains a requirements for one of the standard KeyUsage bit names:

```
cRLSign
dataEncipherment
decipherOnly
digitalSignature
encipherOnly
keyAgreement
keyCertSign
keyEncipherment
nonRepudiation
```

- If there is a critical ExtKeyUsage, the enforcer will scan the policy from top to bottom for a matching ExtKeyUsage permit rules. If it reaches the end of the policy without finding one, the activity is denied. A permit rule pertains to the ExtKeyUsage if it is a blanket permit, or if it contains a requirement for a dotted-decimal OID string, or a requirement for one of the recognized ExtKeyUsage names:

```
any
anyExtendedKeyUsage
id-kp-clientAuth
id-kp-codeSigning
id-kp-emailProtection
id-kp-ipsecEndSystem
id-kp-ipsecTunnel
id-kp-ipsecUser
id-kp-OCSPSigning
id-kp-serverAuth
id-kp-smartcardlogon
id-kp-timeStamping
id-pkix-ocsp-nocheck
```

- A permit rule for an activity that contains no requirements is a blanket permit for that activity.
- A KeyUsage matches a permit rule if every requirement in the permit rule has the corresponding bit set in the KeyUsage.
- An ExtKeyUsage matches a permit rule if every requirement in the permit rule has the corresponding OID present in the ExtKeyUsage.
- A single permit rule that mixes KeyUsage and ExtKeyUsage requirements inside the same <permit> element can never be matched, since no possible KeyUsage or ExtKeyUsage will be capable of matching all its requirements. A rule such as this is likely an error.

## Appendix H: Actional Integration

The Gateway can be configured to be managed as a node by an Actional® Looking Glass™ server. When this configuration is in effect, the Gateway will capture message information at the following points during message processing:

- **message receipt** (after service resolution, but prior to policy enforcement)
- **pre-HTTP routing** (immediately before routing to the downstream/protected service)
- **post-HTTP routing** (immediately after receiving the associated response from the downstream/protected service)
- **message processing complete** (after any post-routing policy has been executed, but prior to forwarding the response back to the client)

The captured information is sent to the Actional Agent (configured externally), which then relays it to the Looking Glass server. For instructions on configuring the Agent, refer to the document *Installing the Actional Agent*. Please [contact](#) CA Technical Support to obtain this document.

---

**Note:** If the Actional Agent is not running, the Actional Integration will buffer messages until the buffer is filled. At this point, the oldest data will be discarded and a warning message will be logged.

---

The Actional Integration feature is licensed separately and requires that the Progress® Actional® for SOA Operations is correctly installed and configured.

### Configuring the Actional Integration

To enable the Actional Integration, set the cluster property *interceptor.enable* to "true" (see Table 192 below). Note that it may take up to two minutes for the integration to be fully enabled after changing the cluster property.

Once the integration is enabled, you can configure it using the following cluster properties:

Table 192: Actional Integration cluster properties

| Property                                    | Description  |
|---|--|
| <b>interceptor.enable</b>                   | Enables/disables the Actional Integration. This value is checked every 2 minutes. Value is a Boolean.<br><br>Default: <b>false</b>   |
| <b>interceptor.configDir</b>                | The configuration directory that is common to both the Actional Integration and the Actional Agent. This setting must be configured to the same location as the Agent. Value is a String.<br><br>Default: <b>/opt/SecureSpan/Actional/LG.Interceptor</b><br><br><b>IMPORTANT:</b> Do not change this path for appliance Gateways. Requires a Gateway restart for changes to take effect. |
| <b>interceptor.enableOutboundHttpHeader</b> | Determines whether the Gateway interceptor adds a manifest HTTP header to the outbound request.<br><br>Default: <b>true</b>  |
| <b>interceptor.enforceInboundTrustZone</b>  | Determines whether the Gateway interceptor enforces Trust Zones on inbound messages. Value is a Boolean.<br><br>Default: <b>false</b>  |
| <b>interceptor.inboundHttpHeaderName</b>    | The HTTP header name used when processing the manifest HTTP header from the inbound request message.<br><br>Default: <b>LG_Header</b>  |
| <b>interceptor.outboundHttpHeaderName</b>   | The HTTP header name used when a manifest HTTP header is added to outbound request messages.<br><br>Default: <b>LG_Header</b>  |
| <b>interceptor.transmitConsumerPayload</b>  | Determines whether XML payloads are captured and forwarded by the Actional Integration along with statistical information when processing outgoing request messages. Value is a Boolean.<br><br>Default: <b>false</b><br><br><b>Note:</b> Transmitting the payload can be resource intensive. Changes to this property may take up to 120 seconds to take effect.                        |
| <b>interceptor.transmitProviderPayload</b>  | Determines whether XML payloads are captured and forwarded by the Actional Integration along with statistical information when processing incoming request messages. Value is a Boolean.<br><br>Default: <b>false</b><br><br><b>Note:</b> Transmitting the payload can be resource intensive. Changes to this property may take up to 120 seconds to take effect.                        |

For more information on using cluster properties, see "Managing Cluster-Wide Properties" on page 40.

## Configuring the Routing Assertion

When the Actional Integration is configured to add a header to the routed message (default "LG\_Header"), then the header can be passed to the protected service by doing the following:

1. Access the Route via HTTP(S) Assertion.
2. Choose the [Headers] tab within the properties.
3. Clear the **[Pass through only certain request headers]** check box to pass through all headers. If you do not wish to pass through all headers, define the Looking Glass headers as follows:
  - a. Ensure **[Customize headers to pass through]** is selected.
  - b. Click **[Add]**. The Custom Header Setting dialog appears.
  - c. For the **Header Name**, enter **LG\_Header**.
  - d. Ensure **[Pass original value]** is selected, then click **[OK]**.

After routing, you can access the value of the header using this variable:

```
${<target>.http.header.<headername>}
```

Where "<target>" is either **request** or a message context variable that has been set in the policy. **Note:** The Actional Integration does not support adding HTTP headers to the response message.

For example:

```
${request.http.header.lg_header}
```

The names of the inbound and outbound HTTP headers can be configured using the cluster properties:

```
interceptor.inboundHttpHeaderName
interceptor.outboundHttpHeaderName
```

See Table 192 above for details.

---

**Tip:** context variables and HTTP headers are not case sensitive, so "lg\_header" and "LG\_Header" are interchangeable.

---

## Enabling Debugging

You can enable interceptor debugging by the Gateway by setting the following system property:

**`com.actional.lg.interceptor.debug=true`**

---

**Note:** Debugging mode is used only for troubleshooting purposes. You should enable debugging only when directed by CA Technical Support.

---

# Appendix I: Stylesheet for Transforming XML to JSON

The following stylesheet can be used to transform an existing XML message into a JSON structure.

For more information on working with JSON structures on the CA API Gateway, see "Working with JSON" on page 213.

```
<xsl:stylesheet version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/Transform">
  <xsl:output encoding="UTF-8" indent="no" media-type="text/x-json" method="text" omit-xml-declara-
tion="yes"/>
  <xsl:strip-space elements="*" />
  <!--contant-->
  <xsl:variable name="d">0123456789</xsl:variable>

  <!-- ignore document text -->
  <xsl:template match="text() [preceding-sibling::node() or following-sibling::node()]" />

  <!-- string -->
  <xsl:template match="text()" >
    <xsl:call-template name="escape-string">
      <xsl:with-param name="s" select="."/>
    </xsl:call-template>
  </xsl:template>

  <!-- Main template for escaping strings; used by above template and for object-properties
  Responsibilities: placed quotes around string, and chain up to next filter, escape-bs-string -->
  <xsl:template name="escape-string">
    <xsl:param name="s" />
    <xsl:text>"</xsl:text>
    <xsl:call-template name="escape-bs-string">
      <xsl:with-param name="s" select="$s" />
    </xsl:call-template>
    <xsl:text>"</xsl:text>
  </xsl:template>

  <!-- Escape the backslash (\) before everything else. -->
  <xsl:template name="escape-bs-string">
    <xsl:param name="s" />
    <xsl:choose>
      <xsl:when test="contains($s, '\\')">
        <xsl:call-template name="escape-quot-string">
          <xsl:with-param name="s" select="concat(substring-before($s, '\\'), '\\\\')"/>
        </xsl:call-template>
        <xsl:call-template name="escape-bs-string">
          <xsl:with-param name="s" select="substring-after($s, '\\')"/>
        </xsl:call-template>
      </xsl:when>
      <xsl:otherwise>
        <xsl:call-template name="escape-quot-string">
          <xsl:with-param name="s" select="$s" />
        </xsl:call-template>
      </xsl:otherwise>
    </xsl:choose>
  </xsl:template>
```

```

</xsl:template>

<!-- Escape the double quote ("). -->
<xsl:template name="escape-quot-string">
  <xsl:param name="s"/>
  <xsl:choose>
    <xsl:when test="contains($s,'&quot;')">
      <xsl:call-template name="encode-string">
        <xsl:with-param name="s" select="concat(substring-before($s,'&quot;'),'&quot;')"/>
      </xsl:call-template>
      <xsl:call-template name="escape-quot-string">
        <xsl:with-param name="s" select="substring-after($s,'&quot;')"/>
      </xsl:call-template>
    </xsl:when>
    <xsl:otherwise>
      <xsl:call-template name="encode-string">
        <xsl:with-param name="s" select="$s"/>
      </xsl:call-template>
    </xsl:otherwise>
  </xsl:choose>
</xsl:template>

<!-- Replace tab, line feed and/or carriage return by its matching escape code. Can't escape back-
slash
or double quote here, because they don't replace characters (&#x0; becomes \t), but they prefix
characters (\ becomes \\). Besides, backslash should be separate anyway, because it should be
processed first. This function can't do that. -->
<xsl:template name="encode-string">
  <xsl:param name="s"/>
  <xsl:choose>
    <!-- tab -->
    <xsl:when test="contains($s,'&#x9;')">
      <xsl:call-template name="encode-string">
        <xsl:with-param name="s" select="concat(substring-before($s,'&#x9;'),'&#x9;',substring-
after($s,'&#x9;'))"/>
      </xsl:call-template>
    </xsl:when>
    <!-- line feed -->
    <xsl:when test="contains($s,'&#xa;')">
      <xsl:call-template name="encode-string">
        <xsl:with-param name="s" select="concat(substring-before($s,'&#xa;'),'&#xa;',substring-
after($s,'&#xa;'))"/>
      </xsl:call-template>
    </xsl:when>
    <!-- carriage return -->
    <xsl:when test="contains($s,'&#xd;')">
      <xsl:call-template name="encode-string">
        <xsl:with-param name="s" select="concat(substring-before($s,'&#xd;'),'&#xd;',substring-
after($s,'&#xd;'))"/>
      </xsl:call-template>
    </xsl:when>
    <xsl:otherwise><xsl:value-of select="$s"/></xsl:otherwise>
  </xsl:choose>
</xsl:template>

<!-- number (no support for javascript mantise) -->
<xsl:template match="text()[not(string(number())='NaN')]">
  <xsl:text><xsl:value-of select="."/></xsl:text></xsl:template>

<!-- boolean, case-insensitive -->
<xsl:template match="text()[translate(.,'TRUE','true')='true']">true</xsl:template>
<xsl:template match="text()[translate(.,'FALSE','false')='false']">false</xsl:template>

<!-- item:null -->
<xsl:template match="*[count(child::node())=0 and not(attribute::node())]">
  <xsl:call-template name="escape-string">

```



```

        <xsl:with-param name="s" select="local-name()" />
      </xsl:call-template>
      <xsl:text>:null</xsl:text>
      <xsl:if test="following-sibling::*">,</xsl:if>
    </xsl:template>

<!-- object -->
<xsl:template match="*" name="base">
  <!-- <xsl:if test="not(preceding-sibling:*)" "></xsl:if> -->
  <xsl:call-template name="escape-string">
    <xsl:with-param name="s" select="name()" />
  </xsl:call-template>
  <xsl:text>:</xsl:text>
  <xsl:choose>
    <xsl:when test="attribute::node() and child::node()">
      <xsl:if test="attribute::node() or child::node()">
        <xsl:text>
{</xsl:text>
      <xsl:call-template name="handleAttributes">
        <xsl:with-param name="attrib" select="attribute::*" />
      </xsl:call-template>
      <xsl:if test="attribute::* and child::node()"><xsl:text>,</xsl:text></xsl:if>
      <xsl:apply-templates select="child::*" />
      <xsl:if test="text()">
        <xsl:text>"$" :</xsl:text><xsl:apply-templates select="text()" />
      </xsl:if>
      <xsl:text>}
</xsl:text>
    </xsl:if>
  </xsl:when>

  <xsl:when test="not(attribute::node()) and child::node()">
    <xsl:if test="child::*"></xsl:if>
    <xsl:apply-templates select="child::*" />
    <xsl:if test="text() and child::*">
      <xsl:text>"$" :</xsl:text>
    </xsl:if>
    <xsl:apply-templates select="text()" />
    <xsl:if test="child::*"></xsl:if>
  </xsl:when>
  <xsl:when test="attribute::node()">
    <xsl:text>
{</xsl:text>
    <xsl:call-template name="handleAttributes">
      <xsl:with-param name="attrib" select="attribute::*" />
    </xsl:call-template>
    <xsl:text>}
</xsl:text>
  </xsl:when>
  <xsl:otherwise>
    <xsl:apply-templates select="text()" />
  </xsl:otherwise>
</xsl:choose>
  <xsl:if test="following-sibling::*">,</xsl:if>
  <!-- <xsl:if test="not(following-sibling:*)" "></xsl:if> -->
</xsl:template>

<!-- array -->
<!-- <xsl:template match="*[count(../*[name(../*)=name(../*)]=count(../*) and count(../*)>1]"> -->
<xsl:template match="*[name(preceding-sibling::*[1]) = name(.) or name(following-sibling::*[1]) =
name(.)]">
  <xsl:if test="name(.) != name(preceding-sibling::*[1])">
    <xsl:text>"</xsl:text><xsl:value-of select="name(.)"></xsl:text>": [</xsl:text>
  </xsl:if>
  <xsl:choose>
    <xsl:when test="not(child::node()) and not(attribute:*)">
      <xsl:text>null</xsl:text>
    </xsl:when>

```

```

        <xsl:otherwise>
            <xsl:text>
{</xsl:text>
        <xsl:call-template name="handleAttributes">
            <xsl:with-param name="attrib" select="attribute::*"/>
        </xsl:call-template>
        <xsl:if test="attribute::* and (text() or child::node())"><xsl:text>, </xsl:-
text></xsl:if>
        <xsl:apply-templates select="child::*"/>
        <xsl:if test="text()">
            <xsl:text>"$" :</xsl:text><xsl:apply-templates select="text()"/>
        </xsl:if>
        <xsl:text>}
</xsl:text>
    </xsl:otherwise>
</xsl:choose>
<xsl:if test="name(.) != name(following-sibling::*[1]) or not(following-sibling:*)"></xsl:if>
<xsl:if test="following-sibling:*)"></xsl:if>
</xsl:template>

<xsl:template name="handleAttributes">
    <xsl:param name="attrib"/>
    <xsl:param name="count" select="count($attrib)"/>

    <xsl:for-each select="$attrib">
        <xsl:text>"@</xsl:text><xsl:value-of select="name()"/><xsl:text>": </xsl:text>
        <xsl:choose>
            <xsl:when test=".">
                <xsl:text>"</xsl:text><xsl:value-of select="."/><xsl:text>"</xsl:text>
            </xsl:when>
            <xsl:otherwise>
                <xsl:text>"</xsl:text>
            </xsl:otherwise>
        </xsl:choose>
        <xsl:if test="position() &lt; $count">
            <xsl:text>, </xsl:text>
        </xsl:if>
    </xsl:for-each>
</xsl:template>

<!-- convert root element to an anonymous container -->
<xsl:template match="/">
    <xsl:text>{</xsl:text><xsl:apply-templates select="node()"/><xsl:text>}
</xsl:template>
</xsl:stylesheet>

```

## Appendix J:

# SiteMinder Failure Reasons

The following table lists the failure values that can be returned during CA SiteMinder authentication or authorization. The failure reason value is stored in the `${<prefix>.smcontext.attributes.SESS_DEF_REASON}` context variable.

**Notes:** (1) The CA SiteMinder Policy Server must be configured to support SM session failure reason codes, otherwise failure reason "0" will always be returned. (2) Not all failures result in a specific code being returned. For example, errors such as incorrect user credentials will result in code "0" being returned.

Table 193: CA SiteMinder authentication/authorization failure reasons

| Value | Reason                       | Value | Reason                     |
|-------|------------------------------|-------|----------------------------|
| 0     | None                         | 26    | NoRedirectConfigured       |
| 1     | PwMustChange                 | 27    | ErrorMessagelsRedirect     |
| 2     | InvalidSession               | 28    | Next_Tokencode             |
| 3     | RevokedSession               | 29    | New_PIN_Select             |
| 4     | ExpiredSession               | 30    | New_PIN_Sys_Tokencode      |
| 5     | AuthLevelTooLow              | 31    | New_User_PIN_Tokencode     |
| 6     | UnknownUser                  | 32    | New_PIN_Accepted           |
| 7     | UserDisabled                 | 33    | Guest                      |
| 8     | InvalidSessionId             | 34    | PWSelfChange               |
| 9     | InvalidSessionIp             | 35    | ServerException            |
| 10    | CertificateRevoked           | 36    | UnknownScheme              |
| 11    | CRLOutOfDate                 | 37    | UnsupportedScheme          |
| 12    | CertRevokedKeyCompromised    | 38    | Misconfigured              |
| 13    | CertRevokedAffiliationChange | 39    | BufferOverflow             |
| 14    | CertOnHold                   | 40    | SetPersistentSessionFailed |
| 15    | TokenCardChallenge           | 41    | UserLogout                 |
| 16    | ImpersonatedUserNotInDir     | 42    | IdleSession                |

Table 193: CA SiteMinder authentication/authorization failure reasons

| Value | Reason                       | Value | Reason                      |
|-------|------------------------------|-------|-----------------------------|
| 17    | Anonymous                    | 43    | PolicyServerEnforcedTimeout |
| 18    | PwWillExpire                 | 44    | PolicyServerEnforcedIdle    |
| 19    | PwExpired                    | 45    | ImpersonationNotAllowed     |
| 20    | ImmedPWChangeRequired        | 46    | ImpersonationNotAllowedUser |
| 21    | PWChangeFailed               | 47    | FederationNoLoginID         |
| 22    | BadPWChange                  | 48    | FederationUserNotInDir      |
| 23    | PWChangeAccepted             | 49    | FederationInvalidMessage    |
| 24    | ExcessiveFailedLoginAttempts | 50    | FederationUnacceptedMessage |
| 25    | AccountInactivity            |       |                             |

# Index

## A

|  |              |
|--|--------------|
| Access control                             | 132          |
| Account information                        | 34           |
| Active Policy Assertions command           | 15           |
| Add  |              |
| certificates                               | 239-240      |
| cluster-wide property                      | 41           |
| federated identity provider                | 441          |
| federated identity provider groups         | 451          |
| federated identity provider users          | 446          |
| federated virtual groups                   | 452          |
| internal identity provider groups          | 294          |
| internal identity provider users           | 286          |
| LDAP identity providers                    | 304          |
| listen port                                | 56, 80       |
| revocation checking policy                 | 254          |
| sample messages                            | 387          |
| Simple LDAP identity provider              | 304          |
| user or group to role                      | 152          |
| Add Certificate Wizard                     | 240          |
| Add Permissions to Role Wizard             | 142          |
| Adding a New Certificate                   | 239          |
| Adding a Sample Message                    | 386          |
| Adding a User or Group to a Role           | 152          |
| Adding an HTTP Option                      | 190          |
| Alerts                                     | 28           |
| Analyze Gateway Performance                | 401          |
| API Proxy Gateway                          | 509          |
| Applet version                             | 6            |
| Archiver                                   | 413          |
| Assertion                                  |              |
| finding                                    | 31           |
| info                                       | 32           |
| line numbers                               | 24, 30       |
| selecting a private key                    | 275          |
| View Info                                  | 32           |
| Assertion Information                      | 32           |
| Assertion Numbering                        | 21, 30       |
| Assertion Status Codes                     | 625          |
| Assertions tab                             | 14, 25       |
| Assertions Tool Bar                        | 23           |
| Assigning Security Zones                   | 160          |
| Audit archive                              | 413          |
| cluster properties                         | 623          |
| Audit cluster properties                   | 569          |
| Audit context variables                    | 524          |
| Audit events                               | 415, 426-427 |
| alerts                                     | 28           |
| certificate expiration                     | 237          |
| deleting                                   | 424          |
| downloading                                | 424          |
| saving                                     | 424          |
| severity levels                            | 166          |
| Audit format, customizing                  | 651          |
| Audit Lookup context variables             | 524          |
| Audit lookup policy                        |              |
| deleting                                   | 183          |
| Audit Message Codes                        | 627          |
| Audit records                              |              |
| decrypting                                 | 424          |
| searching                                  | 418          |
| Audit Sink context variables               | 528          |
| Audit sink policy                          | 175, 178     |
| custom                                     | 180          |
| deleting                                   | 180          |
| JDBC                                       | 181          |
| troubleshooting                            | 179          |
| Audit Sink Properties                      | 175          |
| Audit viewer                               | 415, 580     |
| Audit Viewer policy                        | 424          |
| Auditing                                   | 28, 415      |
| gateway cluster properties                 | 569          |
| overriding severity                        | 427          |
| Authentication context variables           | 531          |
| Authentication domain                      | 433          |
| <b>B</b>                                   |              |
| Bridging identity                          | 429          |
| Browser client                             | 6, 11        |
| <b>C</b>                                   |              |
| CA private key                             | 274          |
| Cache                                      |              |
| credentials                                |              |
| cluster properties                         | 577          |
| Certificate attributes context variables   | 533          |
| Certificate Properties                     | 246          |
| Certificate Revocation Checking Properties | 257          |
| Certificate Signing Request                | 267          |
| Certificate validation                     | 251          |
| cluster properties                         | 574          |
| Certificates                               | 237, 437     |
| adding                                     | 239          |
| deleting                                   | 247          |
| editing                                    | 247          |
| expiration                                 | 237          |
| exporting                                  | 248          |
| importing                                  | 248          |
| recipient                                  | 250          |
| revocation checking properties             | 257          |
| revoking                                   | 285          |
| signing                                    | 268          |
| Change                                     |              |
| password                                   | 44           |
| resolution path                            | 371          |
| Changing a Password                        | 44           |
| Changing the Resolution Path for a Service | 371          |
| Character sets                             | 2            |
| Check existence of variables               | 520          |

|  |          |   |          |
|--|----------|---|----------|
| Cipher suites .....                                    | 194      | Connecting to the Gateway .....                   | 8        |
| supported .....  | 194      | Contact Information .....                         | 507      |
| Clone .....  |          | Context Variables .....                           | 517, 560 |
| email listener .....                                   | 127, 200 | audit .....                                       | 524      |
| JDBC connection .....                                  | 83       | audit lookup .....                                | 524      |
| LDAP identity provider .....                           | 305      | audit sink .....                                  | 528      |
| LDAP identity providers .....                          | 305      | authentication .....                              | 531      |
| listen port .....                                      | 56, 80   | certificate attributes .....                      | 533      |
| log sink .....   | 165      | credential certificates .....                     | 537      |
| Salesforce connection .....                            | 504      | data types .....                                  | 519      |
| Simple LDAP identity provider .....                    | 305      | date/time .....                                   | 539      |
| Cloning an LDAP or Simple LDAP Identity Provider ..... | 305      | existence of .....                                | 520      |
| Cluster properties .....                               | 40, 567  | general .....                                     | 522      |
| _adding .....  | 41       | message layer .....                               | 540, 544 |
| _editing .....   | 41       | message routing .....                             | 547      |
| _removing .....  | 42       | multi-value .....                                 | 558      |
| Administrative Account .....                           | 567      | naming .....                                      | 518      |
| Audit (incl. Sink & Lookup) .....                      | 569      | predefined .....                                  | 521      |
| Audit Archiver .....                                   | 568      | service/policy .....                              | 549      |
| Email Properties .....                                 | 580      | SiteMinder .....                                  | 562      |
| Enterprise Service Manager Properties .....            | 580      | system .....                                      | 549      |
| Fault Level Properties .....                           | 581      | transport layer .....                             | 550      |
| FTP Properties .....                                   | 582      | validating .....                                  | 520      |
| Global Cluster Properties .....                        | 583      | viewing .....                                     | 32       |
| Input/Output Properties .....                          | 584      | Context Variables for SiteMinder .....            | 562      |
| JDBC .....   | 595      | Context Variables for XPathS .....                | 560      |
| Kerberos .....   | 597      | Copy .....  |          |
| LDAP Properties .....                                  | 598      | Simple LDAP identity provider .....               | 305      |
| Messge Validation Properties .....                     | 599      | Copy All command .....                            | 17       |
| Miscellaneous Properties .....                         | 613      | Copy command .....                                | 16       |
| Rate Limit Properties .....                            | 602      | Create .....                                      |          |
| SAML Properties .....                                  | 602      | email listener .....                              | 126, 200 |
| Service Properties .....                               | 603      | federated group .....                             | 451      |
| Traffic Logger Properties .....                        | 605      | federated identity provider .....                 | 441      |
| UDDI Properties .....                                  | 606      | federated user .....                              | 446      |
| WS-Security Properties .....                           | 607      | federated virtual group .....                     | 452      |
| XML Security Properties .....                          | 610      | interface .....                                   | 77       |
| Cluster settings .....                                 | 583      | internal group .....                              | 294      |
| Cluster Status window .....                            | 406      | internal user .....                               | 286      |
| Command line window .....                              | 233      | JDBC connection .....                             | 83       |
| Compare Policy command .....                           | 16       | LDAP identity provider .....                      | 304      |
| Configure .....  |          | log sink .....                                    | 164      |
| email listen port .....                                | 126      | Salesforce connection .....                       | 504      |
| FIP groups .....                                       | 451      | Simple LDAP identity provider .....               | 304      |
| FIP users .....  | 446      | WSDL .....  | 337      |
| IIP groups .....                                       | 294      | Create Federated Identity Provider Wizard .....   | 442      |
| IIP users .....  | 286      | Create LDAP Identity Provider Wizard .....        | 306      |
| listen port .....                                      | 54       | Create Simple LDAP Identity Provider Wizard ..... | 319      |
| log sink .....   | 164      | Create WSDL Wizard .....                          | 337      |
| preferences .....                                      | 210      | Creating a Custom Roles .....                     | 149      |
| SAML policies .....                                    | 462      | Creating a Federated Group .....                  | 451      |
| SFTP polling listen port .....                         | 199      | Creating a Federated Identity Provider .....      | 441      |
| Configure Recipient Certificate Wizard .....           | 250      | Creating a Federated User .....                   | 446      |
| Configuring a Reverse Web Proxy .....                  | 392      | Creating a Federated Virtual Group .....          | 452      |
| Configuring Encryption Settings .....                  | 235      | Creating a Log Sink .....                         | 166      |
| Configuring Preferences .....                          | 210      | Creating a Policy-Backed Identity Provider .....  | 326      |
| Configuring SAML Policies for Identity Bridging .....  | 462      | Creating a Private Key .....                      | 262      |
| Connect command .....                                  | 16       | Creating an Internal Group .....                  | 294      |

|   |          |  |                       |
|---|----------|--|-----------------------|
| Creating an Internal User .....                         | 286      | Disabling a Service .....                              | 367                   |
| Creating an LDAP or Simple LDAP Identity Provider ..... | 304      | Disconnect command .....                               | 16                    |
| Credential caching cluster properties .....             | 577      | Dynamic Routing .....                                  | 214                   |
| Credential certificates context variables .....         | 537      |  |                       |
| Credentials .....                                       |          | <b>E</b>   |                       |
| SAML .....  | 430      | Edit .....   |                       |
| X.509 .....   | 431      | certificates .....                                     | 246-247               |
| CSR .....   | 267      | cluster-wide property .....                            | 41                    |
| Custom audit sink .....                                 | 180      | federated identity providers .....                     | 441                   |
| Customizing MQ Messages .....                           | 122      | internal identity providers .....                      | 299, 458              |
| Customizing the Audit Format for Logging .....          | 651      | JDBC connection .....                                  | 83                    |
|   |          | LDAP identity providers .....                          | 305                   |
| <b>D</b>  |          | listen port .....                                      | 57, 80                |
| Dashboard .....   |          | log sink .....   | 165                   |
| analyzing performance .....                             | 401      | revocation checking policy .....                       | 254                   |
| cluster status .....                                    | 406      | Salesforce connection .....                            | 504                   |
| filters .....   | 403      | sample messages .....                                  | 388                   |
| interval summary .....                                  | 405      | Simple LDAP identity providers .....                   | 305                   |
| message rates .....                                     | 404      | Edit Federated Identity Provider Wizard .....          | 442                   |
| notification bar .....                                  | 404      | Edit HTTP Options .....                                |                       |
| response times .....                                    | 404      | General tab .....                                      | 191                   |
| service metrics .....                                   | 402      | Proxy tab .....  | 193                   |
| zooming time intervals .....                            | 406      | Edit Simple LDAP Identity Provider Wizard .....        | 319                   |
| Dashboard command .....                                 | 21       | Edit WSDL Wizard .....                                 | 337                   |
| Data types for context variables .....                  | 519      | Editing a Certificate .....                            | 247                   |
| Date context variables .....                            | 539      | Editing a Custom Role .....                            | 150                   |
| Date/time context variables .....                       | 539      | Editing a Federated Identity Provider .....            | 441                   |
| Debug log .....   | 185      | Editing a Policy-Backed Identity Provider .....        | 327                   |
| Decrypting auditing details .....                       | 424      | Editing a Revocation Checking Policy .....             | 254                   |
| Default gateway .....                                   | 336, 360 | Editing a Sample Message .....                         | 388                   |
| Default private keys .....                              | 274      | Editing an LDAP or Simple LDAP Identity Provider ..... | 305                   |
| Delete .....  |          | Editing or Deleting a User or Group .....              | 299, 458              |
| audit sink policy .....                                 | 180, 183 | Email .....  | 507                   |
| certificates .....                                      | 247      | Email cluster properties .....                         | 580                   |
| federated identity providers .....                      | 442      | Email listener .....                                   | 126-127               |
| folders .....   | 27       | cloning .....  | 127, 200              |
| interface .....   | 77       | creating .....   | 126, 200              |
| internal identity providers .....                       | 299, 458 | removing .....   | 127, 200              |
| LDAP identity providers .....                           | 306      | viewing .....  | 127, 200              |
| multiple items .....                                    | 27       | Email Listener Properties .....                        | 127                   |
| private key .....                                       | 266      | Enabling .....   |                       |
| sample messages .....                                   | 388      | service .....  | 357, 368              |
| services .....  | 369      | Enabling a Service .....                               | 368                   |
| Simple LDAP identity providers .....                    | 306      | Encoding .....   | 2                     |
| Delete Service command .....                            | 16       | Encryption settings .....                              | 235                   |
| Deleting a Certificate .....                            | 247      | Enforcement policy, key usage .....                    | 653                   |
| Deleting a Custom Role .....                            | 151      | Enterprise Service Manager Settings .....              | 580                   |
| Deleting a Federated Identity Provider .....            | 442      | ESM .....  |                       |
| Deleting a Policy-Backed Identity Provider .....        | 327      | listener .....   | 230                   |
| Deleting a Private Key .....                            | 266      | subscription .....                                     | See WSDM subscription |
| Deleting a Published Service .....                      | 369      | trusted .....  | 186                   |
| Deleting a Sample Message .....                         | 388      | user mappings .....                                    | 186                   |
| Deleting an LDAP or Simple LDAP Identity Provider ..... | 306      | Events .....   | 426                   |
| Desktop client .....                                    | 5        | Exit command .....                                     | 16                    |
| Destroying a private key .....                          | 266      | Expiration of certificates .....                       | 237                   |
| Disable .....   |          | Explicit SSL .....                                     | 414                   |
| service .....   | 367      |  |                       |

|  |                    |
|--|--------------------|
| Export                                 |                    |
| certificates                           | 248                |
| private key                            | 266                |
| Export Policy command                  | 15                 |
| Exporting a Certificate                | 248                |
| Exporting a Private Key                | 266                |
| <b>F</b>                               |                    |
| Fault Level cluster properties         | 581                |
| Features by Product                    | 509                |
| Federated                              |                    |
| groups                                 | 299, 445, 451, 458 |
| identity providers                     | 440                |
| users                                  | 299, 445, 447, 458 |
| virtual groups                         | 445, 453           |
| virtual users                          | 446                |
| Federated group                        |                    |
| properties                             | 295, 454           |
| Federated Identity Provider Wizard     | 442                |
| Federated Identity Providers           | 440                |
| adding                                 | 441                |
| adding group                           | 451                |
| adding user                            | 446                |
| adding virtual group                   | 453                |
| deleting                               | 299, 442, 458      |
| editing                                | 299, 441, 458      |
| searching                              | 280, 459           |
| users and groups                       | 445                |
| Federated User Properties              | 448                |
| Filter Service and Policy Tree command | 22                 |
| Filters for log sinks                  | 169                |
| Find command                           | 18                 |
| Find Next command                      | 18                 |
| Find Previous command                  | 18                 |
| Finding assertions                     | 31                 |
| FIP                                    | 440                |
| FIPS 140-2                             | 265                |
| Firewall rule                          |                    |
| adding                                 | 80                 |
| cloning                                | 80                 |
| editing                                | 80                 |
| properties                             | 81                 |
| removing                               | 80                 |
| Firewall Rule                          |                    |
| properties                             | 81                 |
| Force password reset                   | 53                 |
| FTP Audit Archiver                     | 413                |
| FTP cluster properties                 | 582                |
| FTP Requests                           | 389                |
| configuring policy                     | 390                |
| considerations                         | 391                |
| context variables                      | 391                |
| setting up server                      | 390                |
| Fully dynamic XPath expressions        | 561                |

## G

|  |          |
|--|----------|
| Gateway                                  |          |
| as HTTP proxy                            | 232      |
| audit events                             | 415      |
| certificates                             | 237      |
| license                                  | 37       |
| management service                       | 371      |
| REST management service                  | 372      |
| Gateway (Cluster) Properties             | 40       |
| Actional Integration                     | 657      |
| Administrative Account settings          | 567      |
| Audit Archiver settings                  | 568      |
| Audit settings                           | 569      |
| Certificate Validation settings          | 574      |
| Cluster settings                         | 583      |
| Credential Caching settings              | 577      |
| Email properties                         | 580      |
| Fault Levels settings                    | 581      |
| FTPP settings                            | 582      |
| Input/Output settings                    | 584      |
| Kerberos settings                        | 597      |
| LDAP settings                            | 598      |
| Message Validation settings              | 599      |
| Miscellaneous settings                   | 613      |
| Rate Limit settings                      | 602      |
| SAML Properties                          | 602      |
| Service settings                         | 603      |
| Time Units                               | 567      |
| Traffic Logger settings                  | 580, 605 |
| UDDI settings                            | 606      |
| WS-Security settings                     | 607      |
| XML Security settings                    | 610      |
| Gateway (Cluster) Status                 | 406      |
| Gateway Audit Events                     | 415      |
| actions                                  | 424      |
| analyzing performance                    | 401      |
| Associated Logs Search Parameters        | 420      |
| audit events panel                       | 421      |
| Audit Record Search Parameters           | 418      |
| control panel                            | 418      |
| Entity Type Search Parameters            | 420      |
| event details panel                      | 422      |
| invoking Audit Viewer policy             | 424      |
| Message Operation Search Parameter       | 420      |
| show/hide panels                         | 417      |
| Source panel                             | 417      |
| validate signatures                      | 420      |
| Gateway Cluster Properties               | 567      |
| Gateway Management Service               | 371      |
| Gateway REST Management Service          | 372      |
| Gateway status                           | 407      |
| Gateway URL                              | 8        |
| default resolution URI                   | 336      |
| editing resolution URI                   | 360      |
| General Workflow                         | 36       |
| Generating a Certificate Signing Request | 267      |
| Generic Identify Management Service      | 372, 382 |



|  |              |  |                    |
|--|--------------|--|--------------------|
| Generic LDAP .....                           | 303          | IP address .....   | 77                 |
| Go to Assertion command .....                | 18           | Policy Development Window .....                            | 28                 |
| Group .....                                  |              | tagging .....  | 76                 |
| properties .....                             | 295, 454     | Internal .....   |                    |
| Group Properties .....                       | 295, 454     | groups .....   | 286, 294, 299, 458 |
| Groups .....                                 | 286, 445     | users .....  | 286, 299, 458      |
| adding to role .....                         | 152          | Internal group .....                                       |                    |
| creating .....                               | 294, 451-452 | properties .....   | 295, 454           |
| deleting .....                               | 299, 458     | Internal Identity Provider .....                           | 286                |
| editing .....                                | 299, 458     | adding groups .....  | 294                |
| removing from role .....                     | 152          | adding users .....   | 286                |
| virtual .....                                | 445          | deleting .....   | 299, 458           |
|  |              | searching .....  | 280, 459           |
| <b>H</b>                                     |              | wizard .....   | 300                |
| Hide assertion numbers .....                 | 24, 30       | Internal Services .....                                    | 371, 374           |
| Hide Assertion Numbers command .....         | 21           | Gateway Management .....                                   | 371-372            |
| Home page .....                              | 13, 27       | Generic Identity Management .....                          | 372                |
| Hostnames .....                              |              | publish .....  | 375                |
| verifying .....                              | 434          | Security Token .....                                       | 372                |
| wildcard matching .....                      | 234          | UDDI Notification .....                                    | 373                |
| How to .....                                 |              | WSDM QosMetrics .....                                      | 373                |
| Configure Listener for ESM .....             | 230          | WSDM Subscription .....                                    | 373                |
| Establish Outbound Secure Conversation ..... | 227          | Internal user .....  | 286                |
| How to Integrate the Gateway with WCF .....  | 228          | Internal User Properties .....                             | 288                |
| How to Use the Gateway as HTTP Proxy .....   | 232          | Internationalization .....                                 | 2                  |
| HTTP options .....                           |              | IO cluster properties .....                                | 584                |
| adding .....                                 | 190          | IPv6 .....   | 10, 307, 319       |
| managing .....                               | 188          | ISO-8859 .....   | 2                  |
| properties .....                             | 190          |  |                    |
| HTTP proxies .....                           | 188, 190     | <b>J</b>   |                    |
| using Gateway as .....                       | 232          | JDBC audit sink .....                                      | 181                |
|  |              | JDBC Cluster Properties .....                              | 595                |
| <b>I</b>                                     |              | JDBC connection .....                                      | 82                 |
| Identify management service .....            | 372, 382     | cloning .....  | 83                 |
| Identity bridging .....                      | 429, 466     | creating .....   | 83                 |
| requirements .....                           | 433          | deleting .....   | 83                 |
| SAML source .....                            | 430          | editing .....  | 83                 |
| X.509 source .....                           | 431          | properties .....   | 83                 |
| Identity Provider .....                      | 279-280, 459 | JMS destinations .....                                     | 89                 |
| federated .....                              | 440          | JMS message size .....                                     | 92                 |
| internal .....                               | 286          | JMS requests .....   | 357                |
| LDAP .....                                   | 303          | JMS topics .....   | 89                 |
| on interface .....                           | 13, 25       | JSON .....   |                    |
| policy-backed .....                          | 325          | working with .....   | 213                |
| Identity Tags .....                          | 283          |  |                    |
| IIP .....                                    | 286          | <b>K</b>   |                    |
| Implicit SSL .....                           | 414          | Kerberos cluster properties .....                          | 597                |
| Import Policy command .....                  | 15           | Kerberos Ticket Authorization Info context variables ..... | 540                |
| Importing a Private Key .....                | 265          | Key Usage Enforcement Policy .....                         | 653                |
| Importing Certificates .....                 | 248          | recognized action names .....                              | 653                |
| Inactivity timeout .....                     | 210          | Keys, private .....  | 260, 271, 274      |
| Input/Output cluster properties .....        | 584          | Keystore .....   |                    |
| Installing a License File .....              | 37-38        | default .....  | 208                |
| Interface .....                              | 13           |  |                    |
| creating .....                               | 77           |  |                    |
| deleting .....                               | 77           |  |                    |

## L

|                                |                                |
|--------------------------------|--------------------------------|
| Layer 7 Product Overview ..... | 1                              |
| Layer 7 Technologies .....     | 507                            |
| LDAP cluster properties .....  | 598                            |
| LDAP Identity Providers .....  | 303                            |
| adding .....                   | 304                            |
| cloning .....                  | 305                            |
| deleting .....                 | 306                            |
| editing .....                  | 305                            |
| searching .....                | 280, 459                       |
| simple .....                   | 304                            |
| wizard .....                   | 306                            |
| LDAP User Properties .....     | 321                            |
| Licenses .....                 |                                |
| installing .....               | 38                             |
| removing .....                 | 39                             |
| viewing .....                  | 37                             |
| Limits .....                   |                                |
| cluster properties .....       | 602                            |
| Line numbers .....             | 30                             |
| Listen port .....              | 76, 126, 199                   |
| adding .....                   | 56                             |
| cloning .....                  | 56                             |
| editing .....                  | 57                             |
| properties .....               | 57                             |
| removing .....                 | 57                             |
| Listener .....                 | 54, 57, 126-127, 199, 201, 230 |
| Log events .....               | 407                            |
| saving .....                   | 412                            |
| severity levels .....          | 166                            |
| viewing .....                  | 412                            |
| Log sink .....                 | 185                            |
| cloning .....                  | 165                            |
| creating .....                 | 164, 166                       |
| editing .....                  | 165                            |
| filters .....                  | 169                            |
| managing .....                 | 164                            |
| properties .....               | 167                            |
| removing .....                 | 165                            |
| Log, traffic .....             |                                |
| cluster properties .....       | 605                            |
| Login .....                    |                                |
| form .....                     | 8                              |
| saving .....                   | 210                            |
| Logs .....                     |                                |
| viewing .....                  | 409                            |
| Luna HSM .....                 | 208                            |

## M

|   |        |
|---|--------|
| Main menu .....                                   | 13, 15 |
| Main tool bar .....                               | 13, 22 |
| Manage Cluster-Wide Properties .....              | 567    |
| Management Service, Gateway .....                 | 371    |
| Managing Administrative User Account Policy ..... | 301    |
| Managing Certificate Validation .....             | 251    |
| Managing Certificates .....                       | 237    |

|   |              |
|---|--------------|
| Managing Cluster-Wide Properties .....      | 40           |
| Managing Email Listeners .....              | 126          |
| Managing ESM User Mappings .....            | 186          |
| Managing Firewall Rules .....               | 78           |
| Managing FTP Requests .....                 |              |
| configuring policy .....                    | 390          |
| considerations .....                        | 391          |
| context variables .....                     | 391          |
| setting up server .....                     | 390          |
| Managing Gateway Licenses .....             | 37           |
| installing .....                            | 38           |
| removing .....                              | 39           |
| Managing HTTP Options .....                 | 188          |
| Managing Interfaces .....                   | 76           |
| Managing JDBC Connections .....             | 82           |
| Managing JMS Queues .....                   | 89           |
| Managing Keystore .....                     | 208          |
| Managing Listen Ports .....                 | 54           |
| Managing Log Sinks .....                    | 164          |
| Managing MQ Native Queues .....             | 110          |
| Managing Private Keys .....                 | 260          |
| Managing Roles .....                        | 48, 130, 301 |
| Managing Salesforce Connections .....       | 503          |
| Managing Security Zones .....               | 153          |
| Managing Service Resolution .....           | 196          |
| Managing SFTP Polling Listeners .....       | 199          |
| Managing SiteMinder Configurations .....    | 220          |
| Managing SOAP Web Services .....            | 331          |
| creating WSDL .....                         | 337          |
| publishing service .....                    | 333          |
| Managing Stored Passwords .....             | 42           |
| Managing the Audit Sink .....               | 175          |
| Managing XML Applications .....             | 346          |
| publishing .....                            | 346          |
| Mappings .....                              |              |
| ESM .....                                   | 186          |
| Message codes .....                         | 627          |
| Message layer context variables .....       | 544          |
| Message processing rate .....               | 402          |
| Message routing context variables .....     | 547          |
| Message Validation cluster properties ..... | 599          |
| Messages .....                              |              |
| audit .....                                 | 415          |
| sample .....                                | 386          |
| Metrics .....                               | 401-402      |
| Migrate Namespaces command .....            | 18           |
| MIME multipart messages .....               | 391          |
| Miscellaneous cluster properties .....      | 613          |
| MQ Messages .....                           |              |
| customizing .....                           | 122          |
| MQ Native .....                             |              |
| configuration .....                         | 110          |
| managing connections .....                  | 110          |
| message size .....                          | 110          |
| properties .....                            | 114          |
| MQ Native Queue Properties .....            | 114          |
| MS DOS window .....                         | 233          |
| MSAD .....                                  | 303          |

|  |          |   |                        |
|--|----------|---|------------------------|
| Multivalued Context Variables .....          | 558      | desktop client .....                    | 5                      |
| concatenation .....                          | 558      | identity bridging .....                 | 429                    |
| converting to XML .....                      | 558      | starting .....                          | 5                      |
| indexing .....                               | 559      | troubleshooting mode .....              | 233                    |
| number of .....                              | 559      | Policy Messages command .....           | 21                     |
| My Account .....                             | 34       | Policy Search Bar .....                 | 31                     |
| <b>N</b>                                     |          | Policy Tool Bar .....                   | 14, 24                 |
| Naming context variables .....               | 518      | Policy Validation Messages Window ..... | 14, 28                 |
| nCipher .....                                | 265      | Predefined context variables .....      | 521                    |
| Node   |          | Predefined Roles and Permissions .....  | 130, 132               |
| deleting .....                               | 408      | Preferences .....                       | 210                    |
| log information .....                        | 408      | Preferences command .....               | 16                     |
| renaming .....                               | 408      | Private key                             |                        |
| Non-SOAP applications .....                  | 346      | creating .....                          | 262                    |
| Notification service for UDDI .....          | 373      | default SSLor CA .....                  | 274                    |
| NTLM .....                                   | 192, 552 | deleting .....                          | 266                    |
| <b>O</b>                                     |          | exporting .....                         | 266                    |
| Oracle Internet Directory .....              | 303      | generating CSR .....                    | 267                    |
| Other permission .....                       | 139      | importing .....                         | 265                    |
| Outbound secure conversation .....           | 227      | locations .....                         | 274                    |
| Overriding the Audit Level .....             | 427      | managing .....                          | 260                    |
| Overview .....                               | 1        | properties .....                        | 271                    |
| <b>P</b>                                     |          | selecting custom .....                  | 275                    |
| Passive listeners .....                      | 54, 57   | Private Key Properties .....            | 271                    |
| Password .....                               | 53       | Private Service Policy .....            | 145                    |
| changing .....                               | 34, 44   | Private thread pool .....               | 63                     |
| cluster properties .....                     | 623      | Publish Internal Service Wizard .....   | 375                    |
| creating .....                               | 286      | Publish REST Service Proxy Wizard ..... | 352                    |
| resetting .....                              | 290      | Publish Reverse Web Proxy Wizard .....  | 392, 395               |
| secure .....                                 | 42       | Publish SOAP Web Service Wizard .....   | 333                    |
| stored .....                                 | 42, 46   | Publish to UDDI command .....           | 16                     |
| Paste command .....                          | 17       | Publish Web API Wizard .....            | 346                    |
| Performance .....                            | 401-402  | Published Service Properties .....      | See Service Properties |
| Permission Group Properties .....            | 150      | Publishing                              |                        |
| Permissions .....                            | 130, 132 | Internal Service .....                  | 374                    |
| add to role .....                            | 142      | Non-SOAP Application .....              | 346                    |
| understanding .....                          | 137      | Other Services .....                    | 346                    |
| Policy                                       |          | SOAP Web Service .....                  | 331                    |
| error .....                                  | 14       | Web API .....                           | 346                    |
| private service .....                        | 145      | XML Application .....                   | 346                    |
| searching .....                              | 31       | <b>Q</b>                                |                        |
| violations (viewing) .....                   | 14, 402  | QosMetrics Service .....                | 373                    |
| window .....                                 | 14       | Queue                                   |                        |
| Policy-Backed Identity Provider Wizard ..... | 327      | JMS .....                               | 89                     |
| Policy-Backed Identity Providers .....       | 325      | <b>R</b>                                |                        |
| creating .....                               | 326      | Rate limit                              |                        |
| deleting .....                               | 327      | cluster properties .....                | 623                    |
| editing .....                                | 327      | RBAC .....                              | 132                    |
| Policy context variables .....               | 549      | Recipient certificate .....             | 235, 250               |
| Policy Development Window .....              | 13, 28   | Refresh command .....                   | 21                     |
| Policy Manager .....                         | 4        | Remember user name .....                | 210                    |
| browser client .....                         | 6, 11    | Remove                                  |                        |
|  |          | cluster-wide property .....             | 42                     |
|  |          | email listener .....                    | 127, 200               |

|  |                   |   |                    |
|--|-------------------|---|--------------------|
| JDBC connection .....                      | 83                | deleting .....                                | 388                |
| listen port .....                          | 57, 80            | editing .....                                 | 388                |
| log sink .....                             | 165               | Save and Activate command .....               | 15                 |
| Salesforce connection .....                | 504               | Save command .....                            | 15                 |
| user or group from role .....              | 152               | Save user name .....                          | 210                |
| Removing a User or Group from a Role ..... | 152               | Saved events .....                            | 426                |
| Renaming .....                             |                   | Saved Events command .....                    | 22                 |
| node .....                                 | 408               | SCP messages .....                            | 206                |
| service .....                              | 357, 368          | Searching .....                               |                    |
| Renaming a Service .....                   | 368               | audits .....                                  | 417                |
| Request identifier .....                   | 419, 523          | identity providers .....                      | 280, 459           |
| Reset password .....                       | 290               | policy .....                                  | 31                 |
| Resetting WSDL for a Service .....         | 370               | trusted certificates .....                    | 259                |
| Resolution path .....                      | 367, 371          | Secure passwords .....                        | 42                 |
| Resolution URI .....                       | 360, 371          | SecureSpan Manager .....                      | See Policy Manager |
| Response times .....                       | 402               | SecureSpan XML VPN Client .....               | 3                  |
| REST API .....                             | 372               | identity bridging .....                       | 429, 466           |
| REST Services .....                        | 349               | Security configuration .....                  | 48, 130, 132, 301  |
| Publish REST Service Proxy Wizard .....    | 352               | Security Token Service .....                  | 372, 377           |
| Reverse web proxy .....                    | 392, 395          | Security Zone Properties .....                | 159                |
| Revocation checking .....                  |                   | Security zones .....                          |                    |
| certificate validation .....               | 251               | assigning .....                               | 160                |
| policy .....                               | 254               | managing .....                                | 153                |
| properties .....                           | 257               | properties .....                              | 159                |
| Revoking User Certificates .....           | 285               | unavailable .....                             | 158                |
| Roles .....                                | 48, 130, 132, 301 | understanding .....                           | 156                |
| adding permissions .....                   | 142               | Selecting .....                               |                    |
| adding to .....                            | 152               | private key .....                             | 275                |
| creating custom .....                      | 149               | Selecting Cipher Suites .....                 | 194                |
| deleting custom .....                      | 151               | Service .....                                 |                    |
| editing .....                              | 152               | cluster properties .....                      | 623                |
| editing custom .....                       | 150               | deleting .....                                | 369                |
| removing from .....                        | 152               | disabling .....                               | 367                |
| understanding permissions .....            | 137               | disabling/enabling .....                      | 357                |
| viewing .....                              | 34                | enabling .....                                | 368                |
| Route to JMS queue .....                   | 89                | renaming .....                                | 357, 368           |
| Routing .....                              |                   | resolution path .....                         | 371                |
| dynamic .....                              | 214               | statistics .....                              | 406, 409           |
| failures (viewing) .....                   | 402               | WSDL .....                                    | 369-370            |
| URI .....                                  | 357               | Service context variables .....               | 549                |
|  |                   | Service Metrics window .....                  | 402                |
| <b>S</b> .....                             |                   | Service Properties .....                      | 357                |
| SafeNet Luna .....                         | 208               | HTTP/FTP .....                                | 360                |
| Salesforce connection .....                | 503               | UDDI .....                                    | 364                |
| cloning .....                              | 504               | WSDL .....                                    | 362                |
| creating .....                             | 504               | Service Properties command .....              | 15                 |
| deleting .....                             | 504               | Service resolution .....                      | 78, 196            |
| editing .....                              | 504               | Service usage records .....                   | 141                |
| properties .....                           | 504               | Services .....                                | 331                |
| Salesforce Connection Properties .....     | 504               | internal .....                                | 371, 374-375       |
| SAML .....                                 |                   | tab .....                                     | 13                 |
| policies .....                             | 462               | Services and Policies .....                   | 25                 |
| workflow .....                             | 436               | Setting a Default SSL or CA Private Key ..... | 274                |
| SAML cluster properties .....              | 602               | Severity levels .....                         | 166, 418           |
| SAML Constraints Wizard .....              | 463               | overriding .....                              | 427                |
| Sample Messages .....                      | 386               | SFTP Listener .....                           | 201                |
| adding .....                               | 386               | SFTP messages .....                           | 206                |
|  |                   | SFTP Polling listener .....                   | 199                |

|  |          |  |          |
|--|----------|--|----------|
| SFTP Polling Listener Properties .....     | 201      | Time units for cluster properties .....            | 567      |
| Shared thread pool .....                   | 63       | Timeout setting .....                              | 210      |
| Show assertion numbers .....               | 24, 30   | TivoliLDAP .....                                   | 303      |
| Show Assertion Numbers command .....       | 21       | Token Service .....                                | 377      |
| Signing a Certificate .....                | 268      | Tool bar .....                                     | 13       |
| Simple LDAP Identity Providers .....       | 304      | Assertions .....                                   | 23       |
| adding .....                               | 304      | Main .....   | 22       |
| cloning .....                              | 305      | Policy .....                                       | 24       |
| deleting .....                             | 306      | Traffic Logger cluster properties .....            | 605      |
| editing .....                              | 305      | Transport layer context variables .....            | 550      |
| wizard .....                               | 319      | Troubleshooting Mode .....                         | 233      |
| SiteMinder .....                           |          | Trust anchors .....                                | 252      |
| attributes .....                           | 564      | Trusted Certificates .....                         | 237      |
| configuration properties .....             | 222      | searching .....                                    | 259      |
| configurations .....                       | 220      | Trusted ESMs .....                                 | 186      |
| context variables .....                    | 562      | Trusted mode .....                                 | 11       |
| working with .....                         | 216      |  |          |
| SiteMinder Configuration Properties .....  | 222      | <b>U</b>   |          |
| SOA Gateway .....                          | 509      | UDDI cluster properties .....                      | 606      |
| SOAP fault .....                           |          | UDDI Notification Service .....                    | 373      |
| gateway cluster properties .....           | 581      | UDDI registry .....                                |          |
| SOAP operation .....                       |          | configuring .....                                  | 364      |
| searching by .....                         | 420      | Understanding Role Permissions .....               | 137      |
| SOAP web services .....                    | 332      | Understanding Security Zones .....                 | 156      |
| publishing .....                           | 331      | User certificates .....                            |          |
| publishing from WSDL .....                 | 337      | revoking .....                                     | 285      |
| wizard .....                               | 333      | User Name .....                                    | 9        |
| Sort Service and Policy Tree command ..... | 22       | saving .....                                       | 210      |
| ssg logs .....                             | 164, 409 | User properties .....                              |          |
| SSH support .....                          | 206      | federated .....                                    | 448      |
| SSL private key .....                      | 274      | internal .....                                     | 288      |
| sspc logs .....                            | 164, 409 | LDAP .....   | 321      |
| Starting the Policy Manager .....          | 5        | Users .....  | 286      |
| Statistics .....                           | 402, 409 | adding to role .....                               | 152      |
| Status bar .....                           | 13, 28   | creating .....                                     | 286, 446 |
| Status Bar command .....                   | 21       | deleting .....                                     | 299, 458 |
| Status codes .....                         | 625, 627 | editing .....                                      | 299, 458 |
| Stored passwords .....                     | 42, 45   | removing from role .....                           | 152      |
| Subscription notification .....            |          | tagging .....                                      | 283      |
| ESM .....                                  | 371      | template .....                                     | 282, 461 |
| UDDI .....                                 | 371      | virtual .....                                      | 446      |
| Subscription Service .....                 |          | Using the SecureSpan XVC for Identity Bridging ... | 466      |
| UDDI .....                                 | 373      |  |          |
| WSDM .....                                 | 373      | <b>V</b>   |          |
| Support .....                              | 507      | Validate .....                                     |          |
| Syslog .....                               | 167      | certificate .....                                  | 251      |
| System context variables .....             | 549      | context variables .....                            | 520      |
|  |          | Validate command .....                             | 15       |
| <b>T</b>                                   |          | Variable prefix .....                              |          |
| Tagging authenticated users .....          | 283      | validating .....                                   | 520      |
| TCP port listen .....                      | 54, 57   | Variables .....                                    | 517      |
| Technical support .....                    | 507      | Verifying Hostnames for Outbound Connections ...   | 434      |
| Template outbound queues .....             | 93, 111  | View .....   |          |
| template user .....                        | 282, 461 | logs .....   | 409      |
| Thales nCipher .....                       | 265      | WSDL .....   | 369      |
| Thread pool .....                          | 63       | View Assertion Info .....                          | 32       |
| Time context variables .....               | 539      |  |          |

|  |          |
|--|----------|
| View Logs command .....                        | 22       |
| Viewing Context Variables for Assertions ..... | 32       |
| Viewing Logs .....                             | 409      |
| Virtual groups .....                           | 445, 453 |
| Virtual users .....                            | 446      |

|                          |     |
|--------------------------|-----|
| XML Security             |     |
| cluster properties ..... | 610 |
| XPath                    |     |
| context variables .....  | 560 |
| fully dynamic .....      | 561 |

## W

|  |  |
|--|--|
| WCF .....  | 228  |
| Web API .....  | 346  |
| Web client .....   | 11   |
| Web proxy .....  | 392, 395   |
| Web service .....  | 1, 331   |
| publication .....  | 331  |
| RESTful .....  | 349  |
| wizard .....   | 333, 337   |
| WebLogic JMS .....   | 98, 588  |
| Wildcard Matching of Hostnames .....                       | 234  |
| Wildcards .....  | 361  |
| Wizards .....  | 14, 142, 177, 300, 306, 333, 337, 346, 352, 395, 442 |
| Configure Recipient Certificate .....                      | 250  |
| Policy-Backed Identity Provider .....                      | 327  |
| Workflow .....   | 36   |
| SAML .....   | 436  |
| X.509 Certificate .....                                    | 437  |
| Working FTP Requests .....                                 | 389  |
| Working with Dynamic Routing .....                         | 214  |
| Working with Internal Services .....                       | 371  |
| Working with JSON .....                                    | 213  |
| Working with Log Sinks and Debug Logs .....                | 185  |
| Working with Multi-Value Context Variables .....           | 558  |
| Working with RESTful Web Services .....                    | 349  |
| Working with SCP/SFTP Messages .....                       | 206  |
| Working with SiteMinder .....                              | 216  |
| Working with SOAP Web Services .....                       | 331  |
| Working with the Audit Sink Policy .....                   | 178  |
| Working with the Generic Identity Management Service ..... | 382  |
| Working with the Security Token Service .....              | 377  |
| WSDL   |  |
| reset for service .....                                    | 370  |
| view for service .....                                     | 369  |
| wizard .....   | 337  |
| WSDM QosMetrics Service .....                              | 373  |
| WSDM subscription .....                                    | 373  |
| WSDM Subscription Service .....                            | 373  |

## X

|                               |          |
|-------------------------------|----------|
| X.509 certificate             |          |
| workflow .....                | 437      |
| X.509 credential source ..... | 433, 437 |
| XML Application               |          |
| routing URI .....             | 360      |
| wizard .....                  | 346      |
| XML Firewall Gateway .....    | 509      |
| XML Networking Gateway .....  | 509      |