CA Technologies API Management - SSL Certificate Management

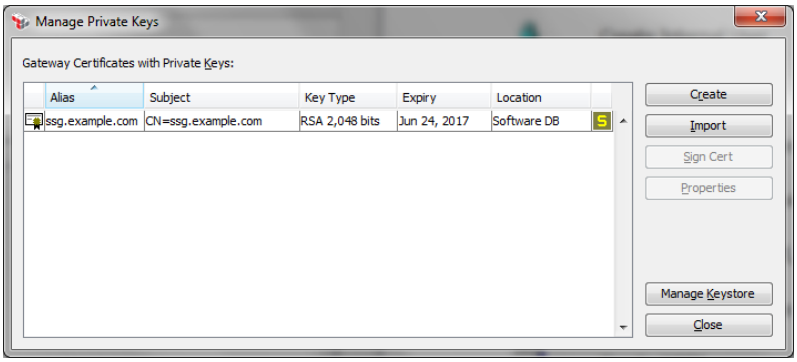
Table of Contents

Overview

Through the course of using the Layer 7 Product Suite, SSL Certificates will be utilized in a great number of areas from initial client connections to the Gateway, signing portions of the request message, through to outbound SSL connections to back-end systems. This document will focus on the Manage Private Keys and Manage Certificates options within the Policy Manager for generation and management of keys and certificates.

Manage Private Keys Interface

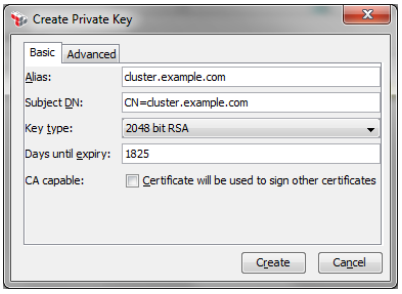
During the initial configuration of the Gateway through the ssgconfig menu, a default self-signed SSL key will be generated based on the name entered for the cluster hostname. Unless otherwise modified, this key will be used for all listen ports for inbound connections, HTTP routing assertions for the client certificate (if required), and signatures in the policy. Management of this key and others are handled through the Policy Manager -> Tasks - > Manage Private Keys interface.

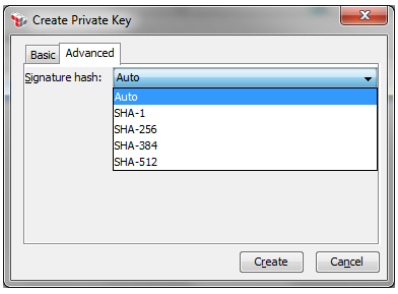


Generate a new self signed certificate

Additional keys or replacement of the default SSL may be required; the ability exists to generate new keys from within the Gateway. This is done by clicking on the Create button of the Manage Private Keys interface.

The Create Private Key window will appear and the main components that need to be filled in are the Alias and the Subject DN. Depending on the requirements of clients connecting or the back-ends that the Gateway is connect to, the Key type (Default: 2048 bit RSA) and on the Advanced tab the signature hash (Default: SHA-384) may need to be modified.





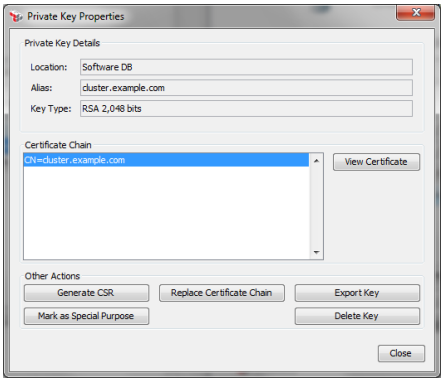
Process for Third-Party Certificate Authority Signing

When the requirement exists for a key to be signed by a Third-Party Certificate Authority either by an external CA such as Verisign, Geotrust, etc. or an Internal CA, the Policy Manager can be used to create a Certificate Signing Request (CSR) to be

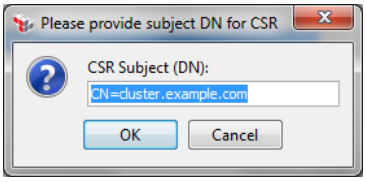
sent to the Certificate Authority. The following process outlines how to create a CSR, submit the file to the CA, and then replace the certificate chain within the Policy Manager.

Generate CSR File

1) Select the certificate from within the Manage Private Keys and click on the Properties button on the right.
2) From the Private Key Properties window, select Generate CSR button.



3) A window will prompt to enter in the Subject DN which will need to match the cluster hostname of the Gateways. Select the OK button to proceed to save the CSR file to a specific location.



4) Submit the CSR file to the CA.

Update Gateway with new certificate

After the CSR has been submitted and approved by the CA, the CA will provide a public key and a certificate chain for its signing authorities including intermediaries and Root CAs. In some instances, both the public key and the certificate chain will be included in one file that can be imported into the Gateway directly. Otherwise these files will need to be combined into one file manually (client/server cert >>> intermediate CA1 >>> intermediate CA2 >>> root CA). The following process outlines how to combine the files and import the key into the Gateway.

Note: If the file contains all keys/certificates, skip to step 5.

1) Download the public key and certificate chain files from the CA in PEM format. If the CA is unable to provide the files in PEM format, download them in DER format and import them into the Manage Certificates interface on the Tasks menu of the Policy Manager then export them out selecting PEM format.
2) Open each of the files in a text editor and select the following sections in the order outlined.
    a. Public key provided for the CSR submitted

-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIeyRBqnKDR5gwDQYJKoZIhvcNAQEMBQAwFzEVMBMGA1UEAxMMZXhhbXBs
ZWludGNhMB4XDTEyMDYyNTE4NDA0NloXDTE0MDYyNTE4NDA0NlowHjEcMBoGA1UEAxMTY2x1c3Rl
ci5leGFtcGxlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIouTRZX1P+fAysB
PqmS1cam2sbJHQ1B3MJ3iCjyfL534RuMlOdR8Eg0PUPQtVXWmnSAeDO3lrzVifWQ4JSbrDVuueB9
C70mgYq2v6AKcrCf2JRYNIKIs/cI27TI+/4O3UUfvebyUa1xX6qJ3IF/4EE7tyBJHNwKaZdDvAMP

V5bQVysftt7z16oV0vpIRUYlEn9Zjcc59QWzmgsYbv/0WMxQubhGII3SBs39BRimd4Exn2bP/TdU
qRdr4vgKZlrEo6mq/QDm1F0hDQsXtLx9I3Vj2woVemKJzfyNTrB7xRAm2jW2+0/CFApt/dorLmgU
JFOIVnf/SHq7KEn0ErO7JVECAwEAAaNgMF4wDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBeAw
HQYDVR0OBBYEFGSo+1rQrJjF2m9D7zW4g3lDqZxuMB8GA1UdIwQYMBaAFL1PqcEzC5hGgD/Ax2wP
hVMe3NnMMA0GCSqGSIb3DQEBDAUAA4IBAQA27ZW/98LI79XwlcU9opDbG69TpcKBfUPSkM6FrbV4
0+PEJQU3++nMfi1+it3NtbPUV2q3MOqUHvbAUuGAr4BNCNuA40J51WUq0YsmA4DOmMeayFE96PV8
JIQ3Cm/UcHlqzgP6R7FbTy9euI1zYiHk0uuV8i/ZDK4Gv7VAMf5MffIOV0dMNLwaFuFwVLepEvzU
BD8wauCpcu1mYIE3PfO/1TnvoQrN/lf46j2CizX5ojea6rxjYoqEdQWFVNvzHCLwOwc2wrN/LUi+
nYxNkmyyeZfRIjwmHri4p3UxWJLcAWvIeWa1gBdLoghBJhmZ5AShppTq+AOXXDzv56R88EZ2
-----END CERTIFICATE-----

b. Each Intermediary CA and the Root CA.
-----BEGIN CERTIFICATE-----
MIIDDTCCAfWgAwIBAgIIG+NhXrXD+7QwDQYJKoZIhvcNAQEMBQAwFDESMBAGA1UEAxMJZXhhbXBs
ZWNhMB4XDTEyMDYyNTE4MzkxOFoXDTE0MDYyNTE4MzkxOFowFzEVMBMGA1UEAxMMZXhhbXBsZWlu
dGNhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlCHJff2FseL9NPdDX5l7SecLlGwt
tIAo6+YioOe2oI/o8Ghbt0iZnYeP2fHhUu/T6xH5At411LIBPWdi6rzx4xsx8Y10okADOnVH7i4U
dVgb8uQRyHijKgcU71PUD73KAUK8G6lAYs4jmv3WhEZ6FU90Oiptq8ovfYHaUI87chX0osFtPKPl
z2yWzOvonfXIGS2FiSk+uXPuLa6hE0FG+/EgJnY+FjZzqsbCN5IqPd6+kJ4R2i2gV5hmwNTJaWGi
8dOFJgPjLEI6AKhAdmZz2WhnPcTmLw+zgdEFrcIVPMVl4NP4WMSdKtms8ElXLbdWQPn93pgajFFd
UX/g7OLAAwIDAQABo2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIF4DAdBgNVHQ4EFgQU
vU+pwTMLmEaAP8DHbA+FUx7c2cwwHwYDVR0jBBgwFoAUXB6Ea3nNNFNl2Dzn//3D5uIYi9IwDQYJ
KoZIhvcNAQEMBQADggEBAHCP30/6yDrugamzqDpzD2IbEm86yeGjzI5xZ5CO/Yeb3RJC3A9tBc2R
YiEIRo8RVQwxaFpDhqpKeLl6mWKejZ5ohFOYzT9QplYFxCyOmztM6JojaKpzbfvjW+pxjz/dfRY7
FYRnEJ+aEtmtGBugepcvpf66LB853r8Y2w1Q99tSfkPoMPDWcuRQyWM+H4OIm5jBj4NNIkQFsIXz
FM92LzyP+GBRwBB06wk8xwJUggEoZlgMAcvV0t5aHND3LKd7F5khUR0HToPXSnrgsOwSvqL/nb8o
lWaC4NoyRXFjT3AcbXC9zK5W/tj36auhaqzH2EBp/nzqEu6BbFls32801Dw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDETCCAfmgAwIBAgIJAL2efffStKM5MA0GCSqGSIb3DQEBDAUAMBQxEjAQBgNVBAMTCWV4YW1w
bGVjYTAeFw0xMjA2MjUxODM4MzJaFw0xNzA2MjQxODM4MzJaMBQxEjAQBgNVBAMTCWV4YW1wbGVj
YTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJlwjzAfTKD5BqtZiNZjbLNSfU3tg2zL
W4XUMqiYCFSPk4TP0cxWny6VKZk3FSi42xdr9drZkQUSQfMgn0US2krxwBRbJOZ/s7cHGUHxoZRZ
Rr0hsSTUGQOvNTC3SZ/m+OLurGvqRMqpZRVPBOBfirzo9QX9rtclfBVA3i/wfl4NXlpR87/rikIQ
mEa9KQXyM7t1w3N5tpkhUvfh3sqjMEDLwWj7RasUozAFdiM7hVr8E8tzeYFnEB0bj8MxLaE4Zyds
XenRi2+LRV1rmN8gqwZTlSmNfGgqkn3ndd4wSzD8OlQFoRJQcy2FuEkAXcpmNHMCVt8AcU8G5pz7
HUaJ58ECAwEAAaNmMGQwEgYDVR0TAQH/BAgwBgEB/wIBATAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0O
BBYEFFwehGt5zTRTZdg85//9w+biGIvSMB8GA1UdIwQYMBaAFFwehGt5zTRTZdg85//9w+biGIvS
MA0GCSqGSIb3DQEBDAUAA4IBAQAf0ONLnOTPdicecHK4fpzYtRwQvt9yOTzH+u1IXmm65JjkDtse
ZOa11Fg26Jh3vchmCvLJONVfxosKdjz6j/Ig0uaacKYeTR1IVcfY7yUswf9tRPmzK6dinWJhAXs4
Sv3PVXaMNJ+XcHflj4JconiPk5VY0Pjs9dDBPPGsut5XTdooIGrp1I0/E8kkPGFvZ44yl06KgyE0
FD7t316k9+eKWrdKwFC7BBoF4AusNBhfvdDlW0/uYEJ0WZc5rsxc1rJLIVAvCqWfc1mfPD48WcuG
hV7WgXBBPAYMiSgCPL+R09DQ0P7lzUrqkmIO237lSoih04Azm1Eo0qIPnWBKH+jA
-----END CERTIFICATE-----

3) Combine all keys/certificates into a new file
-----BEGIN CERTIFICATE-----
MIIDFzCCAf+gAwIBAgIIeyRBqnKDR5gwDQYJKoZIhvcNAQEMBQAwFzEVMBMGA1UEAxMMZXhhbXBs
ZWludGNhMB4XDTEyMDYyNTE4NDA0NloXDTE0MDYyNTE4NDA0NlowHjEcMBoGA1UEAxMTY2x1c3Rl
ci5leGFtcGxlLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIouTRZX1P+fAysB
PqmS1cam2sbJHQ1B3MJ3iCjyfL534RuMlOdR8Eg0PUPQtVXWmnSAeDO3lrzVifWQ4JSbrDVuueB9
C70mgYq2v6AKcrCf2JRYNIKIs/cI27TI+/4O3UUfvebyUa1xX6qJ3IF/4EE7tyBJHNwKaZdDvAMP

V5bQVysftt7z16oV0vpIRUYlEn9Zjcc59QWzmgsYbv/0WMxQubhGII3SBs39BRimd4Exn2bP/TdU
qRdr4vgKZlrEo6mq/QDm1F0hDQsXtLx9I3Vj2woVemKJzfyNTrB7xRAm2jW2+0/CFApt/dorLmgU
JFOIVnf/SHq7KEn0ErO7JVECAwEAAaNgMF4wDAYDVR0TAQH/BAIwADAOBgNVHQ8BAf8EBAMCBeAw
HQYDVR0OBBYEFGSo+1rQrJjF2m9D7zW4g3lDqZxuMB8GA1UdIwQYMBaAFL1PqcEzC5hGgD/Ax2wP
hVMe3NnMMA0GCSqGSIb3DQEBDAUAA4IBAQA27ZW/98LI79XwlcU9opDbG69TpcKBfUPSkM6FrbV4
0+PEJQU3++nMfi1+it3NtbPUV2q3MOqUHvbAUuGAr4BNCNuA40J51WUq0YsmA4DOmMeayFE96PV8
JIQ3Cm/UcHlqzgP6R7FbTy9euI1zYiHk0uuV8i/ZDK4Gv7VAMf5MffIOV0dMNLwaFuFwVLepEvzU
BD8wauCpcu1mYIE3PfO/1TnvoQrN/If46j2CizX5ojea6rxjYoqEdQWFVNvzHCLwOwc2wrN/LUi+
nYxNkmyyeZfRIjwmHri4p3UxWJLcAWvIeWa1gBdLoghBJhmZ5AShppTq+AOXXDzv56R88EZ2
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDDTCCAfWgAwIBAgIIG+NhXrXD+7QwDQYJKoZIhvcNAQEMBQAwFDESMBAGA1UEAxMJZXhhbXBs
ZWNhMB4XDTEyMDYyNTE4MzkxOFoXDTE0MDYyNTE4MzkxOFowFzEVMBMGA1UEAxMMZXhhbXBsZWlu
dGNhMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlCHJff2FseL9NPdDX5l7SecLlGwt
tIAo6+YioOe2oI/o8Ghbt0iZnYeP2fHhUu/T6xH5At411LIBPWdi6rzx4xsx8Y10okADOnVH7i4U
dVgb8uQRyHijKgcU71PUD73KAUK8G6lAYs4jmv3WhEZ6FU90Oiptq8ovfYHaUl87chX0osFtPKPl
z2yWzOvonfXIGS2FiSk+uXPuLa6hE0FG+/EgJnY+FjZzqsbCN5IqPd6+kJ4R2i2gV5hmwNTJaWGi
8dOFJgPjLEI6AKhAdmZz2WhnPcTmLw+zgdEFrcIVPMVl4NP4WMSdKtms8ElXLbdWQPn93pgajFFd
UX/g7OLAAwIDAQABo2AwXjAMBgNVHRMBAf8EAjAAMA4GA1UdDwEB/wQEAwIF4DAdBgNVHQ4EFgQU
vU+pwTMLmEaAP8DHbA+FUx7c2cwwHwYDVR0jBBgwFoAUXB6Ea3nNNFNl2Dzn//3D5uIYi9IwDQYJ
KoZIhvcNAQEMBQADggEBAHCP30/6yDrugamzqDpzD2IbEm86yeGjzI5xZ5CO/Yeb3RJC3A9tBc2R
YiEIRo8RVQwxaFpDhqpKeLl6mWKejZ5ohFOYzT9QplYFxCyOmztM6JojaKpzbfvjW+pxjz/dfRY7
FYRnEJ+aEtmtGBugepcvpf66LB853r8Y2w1Q99tSfkPoMPDWcuRQyWM+H4OIm5jBj4NNIkQFsIXz
FM92LzyP+GBRwBB06wk8xwJUggEoZlgMAcvV0t5aHND3LKd7F5khUR0HToPXSnrgsOwSvqL/nb8o
lWaC4NoyRXFjT3AcbXC9zK5W/tj36auhaqzH2EBp/nzqEu6BbFls32801Dw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDETCCAfmgAwIBAgIJAL2efffStKM5MA0GCSqGSIb3DQEBDAUAMBQxEjAQBgNVBAMTCWV4YW1w
bGVjYTAeFw0xMjA2MjUxODM4MzJaFw0xNzA2MjQxODM4MzJaMBQxEjAQBgNVBAMTCWV4YW1wbGVj
YTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJlwjzAfTKD5BqtZiNZjbLNSfU3tg2zL
W4XUMqiYCFSPk4TP0cxWny6VKZk3FSi42xdr9drZkQUSQfMgn0US2krxwBRbJOZ/s7cHGUHxoZRZ
Rr0hsSTUGQOvNTC3SZ/m+OLurGvqRMqpZRVPBOBfirzo9QX9rtclfBVA3i/wfl4NXlpR87/rikIQ
mEa9KQXyM7t1w3N5tpkhUvfh3sqjMEDLwWj7RasUozAFdiM7hVr8E8tzeYFnEB0bj8MxLaE4Zyds
XenRi2+LRV1rmN8gqwZTlSmNfGgqkn3ndd4wSzD8OlQFoRJQcy2FuEkAXcpmNHMCVt8AcU8G5pz7
HUaJ58ECAwEAAaNmMGQwEgYDVR0TAQH/BAgwBgEB/wIBATAOBgNVHQ8BAf8EBAMCAQYwHQYDVR0O
BBYEFFwehGt5zTRTZdg85//9w+biGIvSMB8GA1UdIwQYMBaAFFwehGt5zTRTZdg85//9w+biGIvS
MA0GCSqGSIb3DQEBDAUAA4IBAQAf0ONLnOTPdicecHK4fpzYtRwQvt9yOTzH+u1IXmm65JjkDtse
ZOa11Fg26Jh3vchmCvLJONVfxosKdjz6j/lg0uaacKYeTR1IVcfY7yUswf9tRPmzK6dinWJhAXs4
Sv3PVXaMNJ+XcHflj4JconiPk5VY0Pjs9dDBPPGsut5XTdooIGrp1I0/E8kkPGFvZ44yl06KgyE0
FD7t316k9+eKWrdKwFC7BBoF4AusNBhfvdDlW0/uYEJ0WZc5rsxc1rJLlVAvCqWfc1mfPD48WcuG
hV7WgXBBPAYMiSgCPL+R09DQ0P7lzUrqkmIO237lSoih04Azm1Eo0qIPnWBKH+jA
-----END CERTIFICATE-----

4) Validate the new certificate chain by running the following commands:
   - perl -n0777e 'map { print "---\n"; open(CMD, "| openssl x509 -noout -subject -issuer"); print CMD; close(CMD) } /^-----BEGIN.*?^-----END.*?\n/gsm' <new certificate file>.pem
     Sample Output:
     ---
     subject= /CN=cluster.example.com
     issuer= /CN=exampleintca
     ---
     subject= /CN=exampleintca
     issuer= /CN=exampleca
     ---
     subject= /CN=exampleca
     issuer= /CN=exampleca

- openssl verify <new certificate file>.pem
  Sample Output:
  <new certificate file>.pem: OK

5) Update the Gateway with the new combined certificate file by clicking on the Replace Certificate Chain from within the Private Key Properties' window and browse through to the new file. Once the certificate has been successfully imported into the Gateway, special purpose certificates such as default SSL will require that the Gateway is restarted to allow the new certificate to take effect.

Generate P12 File from a CA Signed Certificate

The process of generating a private key and subsequent CSR can be done from other toolsets outside of the Policy Manager which will require manual creation of a Public-Key Cryptography Standard #12 (PKCS#12) file. The standard tool that can be used to accomplish the creation of this file is OpenSSL. The following process outlines how to take the various components (private key, public key and certificate chain for the CAs) and combine them for import into the Gateway.

1) Collect the private key, CA signed certificate, and Intermediary and CA certificates. Ensure that each of these files is in PEM format.

   To convert a certificate from DER to PEM:
   openssl x509 –in input.crt –inform DER –out output.crt –outform PEM

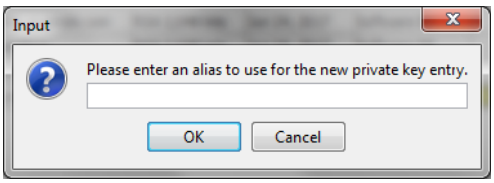
   To convert a key from DER to PEM:
   openssl rsa –in input.key –inform DER –out output.key –outform PEM

2) Combine the files by using the openssl command to read the PEM encoded certificate(s) and key and export to a single PKCS#12 file as follows. The root.crt is the PEM formatted root certificate and any other certificates in the chain concatenated into a single file (intermediate CA1 >>> intermediate CA2 >>> root CA)

   openssl pkcs12 -export -in input.crt -inkey input.key -certfile root.crt -out bundle.p12

   Note: By default, the key will be encrypted with Triple DES so you will be prompted for an export password (which may be blank).

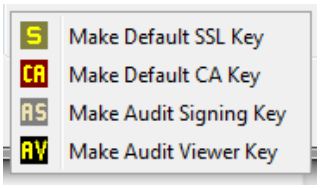
3) Import the newly created PKCS#12 file into the Gateway through the Policy Manager -> Tasks -> Manage Private keys. From the Manage Private keys interface select the Import button. The Import option will request that an alias is entered which is arbitrary name for the listing of keys.



4) Once the PKCS#12 file has been imported, it can be used immediately without the need to restart the Gateway. To assign a specific purpose to the key use the steps outlined in the following section.

Modification of a Key's Purpose within the Gateway

Private Keys both created within the Gateway and imported from another source can be slated for a primary purpose. This purpose change is modified through the Tasks -> Manage Private Keys interface by selecting a key and clicking on the Properties button. From the Private Keys Properties window, click on the Mark as Special Purpose button which will display the following options:



Breakdown of the Purposes:
Make Default SSL: Makes the selected key the default SSL private key for the cluster. This will be the key that all the listen ports, HTTP Routing Assertions and any other assertion requiring a private key by default.

Make Default CA: Makes the selected key the default CA private key for the cluster. This will allow the XML VPN Client to obtain certificates dynamically from the Gateway during initial configuration.

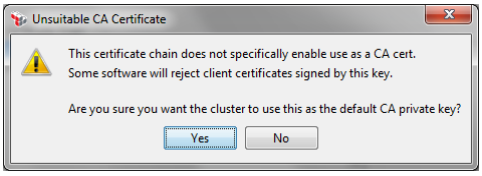
Make Audit Signing Key: Makes the selected key the default audit signing key. All internally-saved signed audit records will be signed with this key whenever internal audit signing is enabled. If an audit signing key is not assigned, the Gateway will use the default SSL key to sign audit records.

Make Audit Viewer Key: Makes the selected key the audit viewer key, to be used to decrypt encrypted audits in the Audit Viewer policy. The audit viewer key is required when an authorized user attempts to view encrypted audit information in the Policy Manager.

Change the Special Purpose for a key

Once the purpose for a key has been determined, the purpose will need to be selected from the listing outlined in the previous section. When the purpose has been selected a validation window will appear asking for additional confirmation. After selecting OK or Yes then the Gateway will need to be rebooted for the purpose to take effect.

Note: If the Default CA purpose is selected and the Gateway deems that there may be an issue with then the prompt shown below will appear. Please consider if this CA will be acceptable before proceeding.

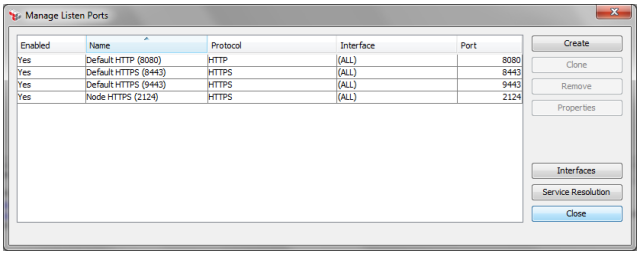


Private Key Usage within the Gateway

The private keys stored in the Gateway can be used in a variety of different areas of the product including Listen Ports and Policy Assertions.

Manage Listen Ports

Management of the ports available to the client is done through the Manage Listen Ports which can be accessed through the Policy Manager -> Tasks -> Manage Listen Ports menu option. All changes made to the ports through this interface will take effect immediately and will not require a restart of the Gateway.



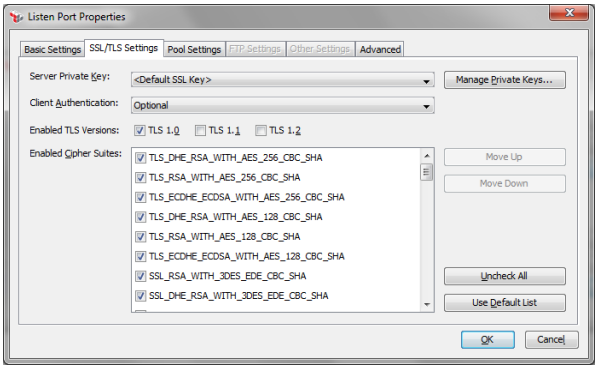
During the initial configuration of the Gateway, 4 ports will be configured:

- 8080 – Non-SSL port for request messages
- 8443 – SSL port with Client Mutual Authentication set to optional for both Policy Manager access and request messages.
- 9443 – SSL port with Client Mutual Authentication set to non for both Policy Manager access and request messages.
- 2124 – SSL port with Client Mutual Authentication set to optional for inter-node communication

Configuration of SSL Private Key

When a listen port has been set to use a protocol with SSL then the SSL/TLS Settings tab will become available for modification. Some of the settings on the page still may be grayed out based on the protocol selected on the Basic Settings tab.

Note: Modifications to the Listen Ports can only be done against ports that the Policy Manager is not currently connected to.



Server Private Key: By default, the Default SSL Key will be assigned to the port. Any existing Private Key can be assigned by clicking on the drop down arrow.

Client Authentication: By default when a port is created, None is set for this value. If Client Authentication is required in the policy, then the client must pass through a port with at the least Optional set for this value.

Enabled TLS Versions: Allows or limits the TLS versions that the inbound port will support.

Enabled Cipher Suites: The order of the Cipher Suites is important as the top most cipher in the list will be the one that the client and Gateway will attempt to use. If the client does not support the cipher suites listed, then the SSL handshake will fail.

Inbound SSL Handshake Issues

- Client requires Known Trusted CA listing before the client application will attempt to send through the client certificate

  Solutions:

  i) With TLS 1.1 / 1.2 enabled on the port, the Gateway will populate the accepted issuers list in the handshake based on the Trusted Certificates stored in the Manage Certificates with Signing Client Certificates usage option set.

  ii) With only TLS 1.0 enabled on the port, the Gateway can include an accepted issuers list in the handshake based on the Trusted Certificates stored in the Manage Certificates with Signing Client Certificates usage option set by setting the Listen Port Advanced property "acceptedIssuers" to "true". This can be found in the Policy Manager under Tasks -> Manage Listen Ports -> Properties -> Advanced tab.

  iii) To encompass all the listen ports, setting io.httpsAcceptedClientCa cluster property with the PEM formatted certificate for the CAs separated with commas (e.g.: -----BEGIN CERTIFICATE----- …. -----END CERTIFICATE-----, -----BEGIN CERTIFICATE----- …. -----END CERTIFICATE-----). This setting will require that the Gateway is restarted for the setting to take effect.

- Client fails to connect to Gateway over SSL

  Possible Reasons:

  i) Client does not support cipher suites set on the port. Ascertain supported cipher suites on client and adjust listen port settings.

  ii) Client certificate validation fails due to CA certificate not added to Manage Certificates and assigned correct usage.

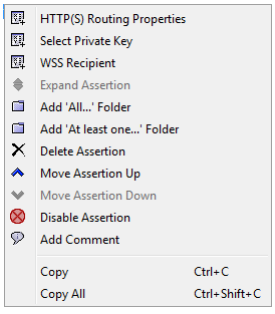
  iii) Client attempts to connect to the gateway using SSLv3. Default as of version 5.3, SSLv3 is no longer supported as default SSL protocol. Enabling this protocol can be done by setting the Listen Port Advanced property "overrideProtocols" to "SSLv2Hello,SSLv3,TLSv1". This can be found in the Policy Manager under Tasks -> Manage Listen Ports -> Properties -> Advanced tab.

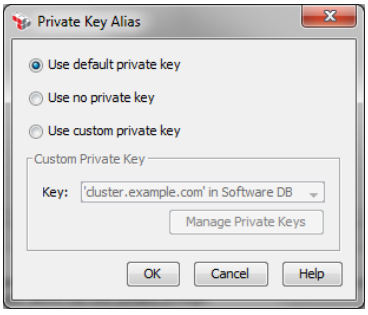
Policy Assertions

Several Assertions allow for configuration of the Private Key to be used. By default, the Default SSL Key will be used.

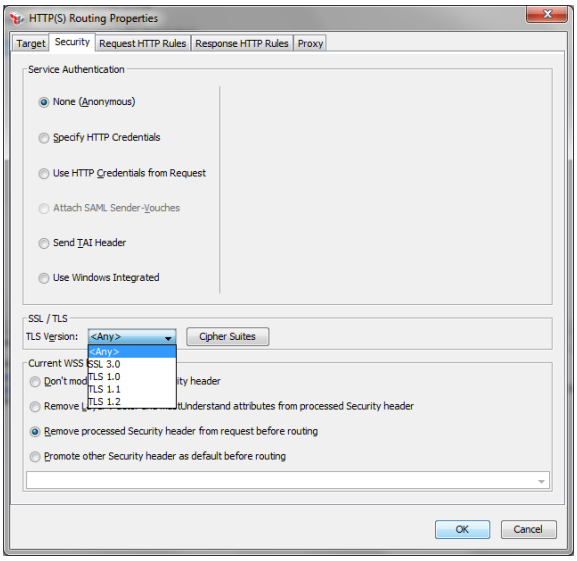
HTTP Routing Assertion

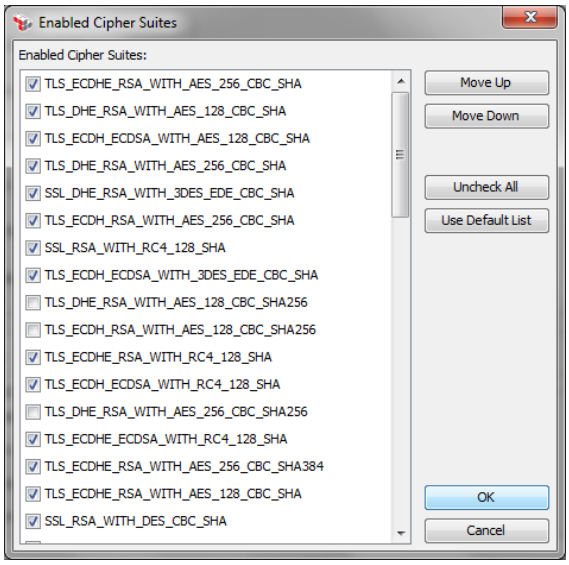
The HTTP Routing Assertion allows for the outbound Private Key to be modified by right clicking on the assertion in the policy window and clicking on Select Private Key. This option is only available if the URL in the HTTP Routing Assertion is https:// or a context variable is used in place of the URL. Once the Select Private Key is clicked the Private Key Alias window will be presented with the options to use the default private key, no private key, or select a specific private key.





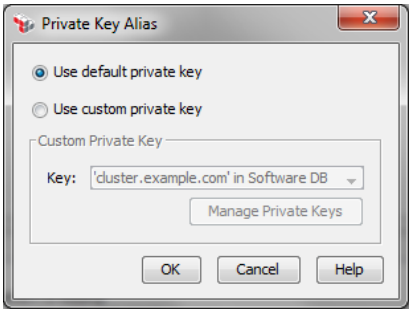
One other control mechanism of SSL handshake configuration within the HTTP Routing is on the Security tab of the Properties which allows specifying SSL/TLS protocols and Cipher Suites.





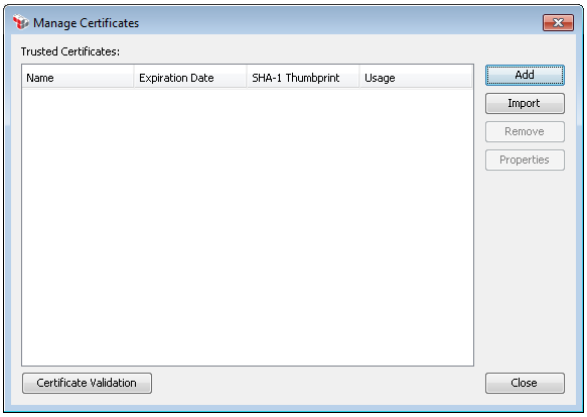
Add Security Token / (Non-SOAP) Sign XML Element / Create SAML Token / Sign Element Assertions

These assertions allow for the modification of which Private Key can be used. Private Key can be modified by right clicking on the assertion in the policy window and clicking on Select Private Key. Once the Select Private Key is clicked the Private Key Alias window will be presented with the options to use the default private key or select a specific private key.



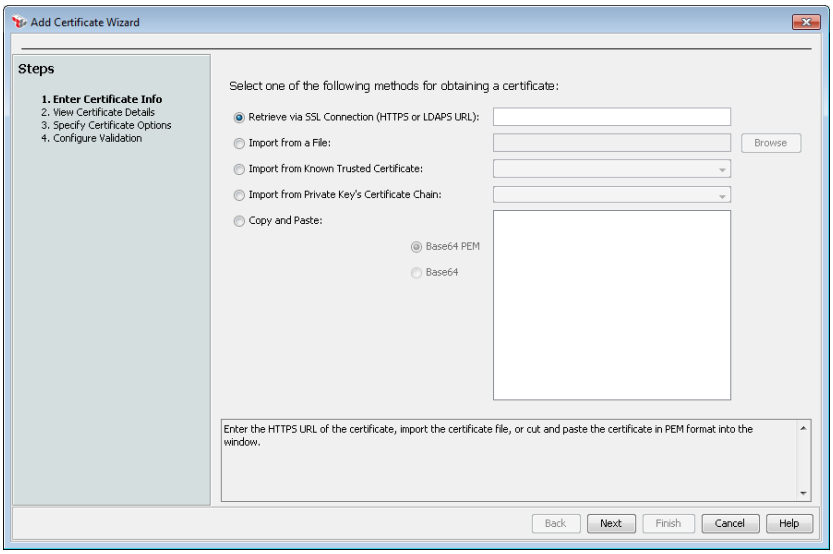
Manage Certificates Interface

The Layer 7 Gateway has been designed to not trust any certificates out of the box and will only trust certificates added through the Manage Certificate Interface. Management of these certificates is handled through the Policy Manager -> Tasks - > Manage Certificates interface.



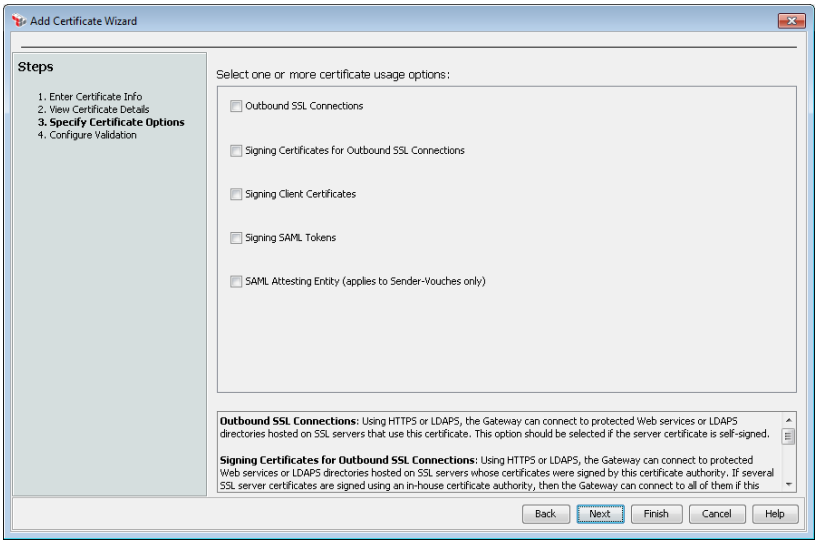
Add a Certificate

By clicking on the Add button of the Manage Certificates, the Add Certificate Wizard will be presented.

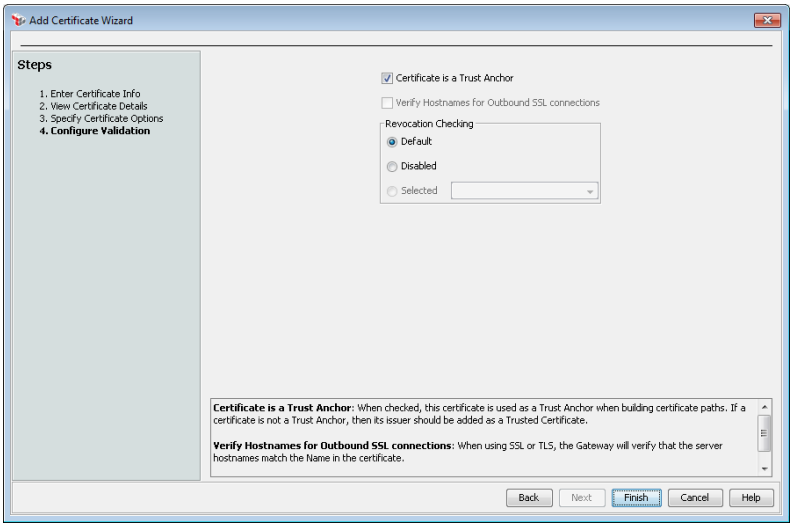


1) From this wizard multiple methods exist to add certificates to the list of trusted certificates including:
    a. Retrieving the certificate from a known end-point either over HTTPS or LDAPS. The connection to the end-point occurs from the Gateway so all firewall and routing must be in place prior to attempting to pull the certificate.
    b. Import a valid x.509 certificate from a share location or local hard disk.
    c. From the list of Known Trusted Certificates
    d. Import the certificate from the Gateway's Private Keys listing
    e. Copy and Paste either a Base64 PEM or Base64 certificate contents into the wizard window. *Base64 PEM:* The certificate must be surrounded by the PEM markers ('-----BEGIN CERTIFICATE-----' and '-----END CERTIFICATE-----'), with formatting that conforms to RFC3548. This is the default.
    Base64: The certificate can be imported regardless of formatting and does not require PEM markers.

2) Once the certificate has been selected, click on the Next button. To ensure that the certificate will be available for the right usages ensure to check off as many options as possible. For standard back-end connections, the first 3 options provide the best coverage and can also be used if the certificate is to be used in a Federated Identity Provider. The last 2 options are used for SAML specific Federated Identity Providers and general SAML validation.



3) At this point in the wizard the choice exists to either click Next or Finish.
4) If Next is selected, then
    a. Certificate Validation can be set to use the certificate as a Trust anchor to avoid following the certificate chain
    b. Verify Hostname for Outbound SSL connections so that the certificate used by the back-end must match the hostname. This option becomes available when either of the Outbound SSL usage options is checked.
    c. Revocation Checking can be set to use the Default policy which will vary based on type validation, Disable the validation, or use a predefined policy (OCSP or CRL).



Import a Certificate

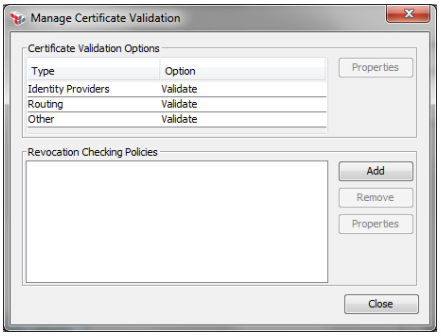
The other option to add certificates to the trusted list is by going straight to a file stored in a shared or local location by clicking on the Import button.

The types of files that the Gateway will accept are:
PEM/BASE64 x.509 Certificates
DER encoded x.509 Certificates
PKCS#12 key store

PKCS#7 empty envelope

Manage Certificate Validation / Revocation Checking

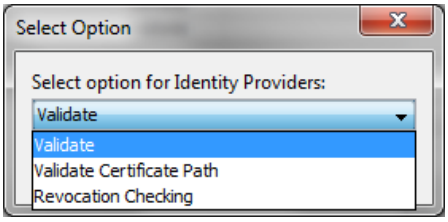
Validation and Revocation Checking of certificates being consumed and utilized by the Gateway is controlled through the Manage Certificate Validation window found on the Manage Certificates Interface.



From this window, the administrator is able to control how certificates used in Identity Providers, Routing Assertions and general usage is controlled by default. The individual components listed still have the ability to override the certificate validation defaults.

Change Certificate Validation Defaults

The defaults for the main components involving certificate can be modified by selecting the component and clicking on the Properties button. The Select Option window will prompt to select a new default option. Once this change has been made, the Gateway will begin to use the setting on subsequent requests without the need for a restart.



Options:
Validate: Ensure that the certificate is valid and trusted.

Validate Certificate Path: Ensure that the certificate path is valid to a trust anchor.

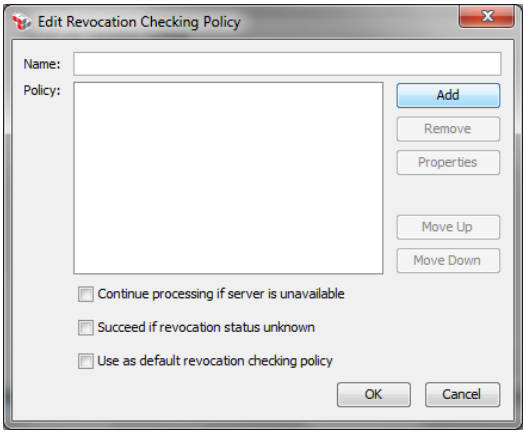
Revocation Checking: Validate the certificate path and perform revocation checking according to the revocation checking policies.

Managing the Revocation Checking Policies

By default, the Gateway is not set to check revocation against any source and requires policies to be established. Management of these policies can be done through the Revocation Checking Policies section of the Manage Certificate Validation window.

Add a New Policy

By clicking on the Add button next to the Revocation Checking Policies, the Edit Revocation Checking Policy window will appear. From within each main Revocation Checking Policy, individual policies can be established based on a variety of criteria including the signing authority certificate, URL from the certificate for CRL/OCSP based on URL Regex matching, and Static URL manually entered for CRL/OCSP.



Note: As with all certificate exchanges with the Gateway, the certificates for the destination LDAPS, HTTPS, and OCSP Signing Authority need to be imported and trusted by the Gateway for the revocation to function correctly. In addition, based on the protocol used, ensure that all firewall ports are opened.

Fields and Checkboxes:
Name: Unique identifier that will appear in drop down lists in several interfaces.

Policy: Revocation Policy specifying individual rules. Review Edit Certificate Revocation Checking Properties section below to change individual properties.

Continue processing if server is unavailable: This check box lets you control how the Gateway should respond if the CRL or OCSP responder is not available. Select this check box to check the cache for the CRL or OCSP response. If a cached value is found, that value is used. If a cached value is not found, then the certificate is permitted only if the [Succeed if revocation status unknown] check box is selected, otherwise it is revoked. Clear the check box to always revoke a certificate if the server is unavailable.

Succeed if revocation status unknown: This check box determines what will happen if all the steps in the policy are exhausted and the status are still undetermined:

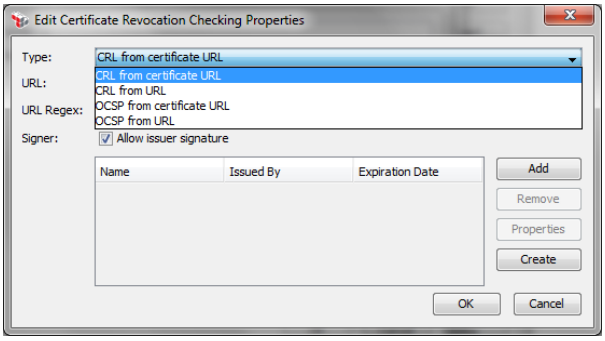
- Select this check box to permit use of the certificate even if its revocation status could not be determined.
- Clear this check box to prevent use of the certificate if its revocation status could not be determined.

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.

Use as default revocation checking policy: 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.
Select this check box to make the current policy the default. Clear the check box to remove the default status from the current policy. IMPORTANT: 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.

Edit Certificate Revocation Checking Properties

From the Edit Revocation Checking Policy window, click the Add button to configure an individual property for the overall policy.



Fields and Checkboxes:

Type: From the drop-down list, select how the certificate revocation status should be determined:

- CRL from certificate URL: Use the Certificate Revocation List (CRL) located at a URL that is extracted from the certificate. Use the URL Regex field to restrict the URL to a particular type or host.
- CRL from URL: Use the CRL located in the URL field.
- OCSP from certificate URL: Use the Online Certificate Status Protocol (OCSP) responder located at a URL that is extracted from the certificate. Use the URL Regex field to restrict the URL (perhaps to a particular host).
- OCSP from URL: Use the OCSP responder located at the URL.

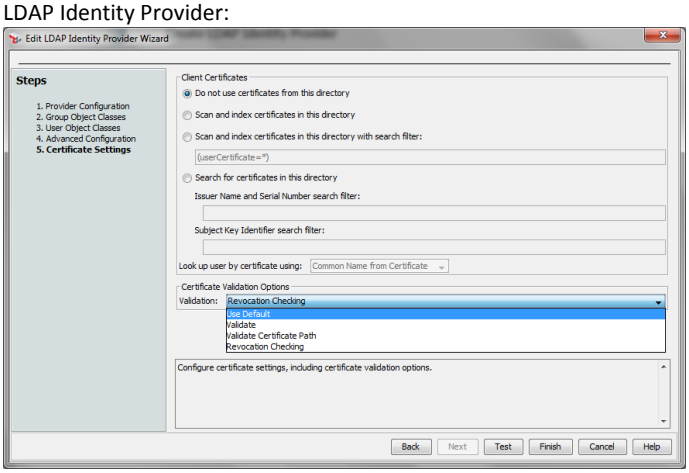
URL / URL Regex: Based on the type selected, these fields will become available and allow entry of the full URL to retrieve revocation information or a Regex value to pinpoint certain URLs for this property to act against. The default URL Regex ".*" will accept all URLs.

Signer: In this section, define the certificates that are permitted to sign the CRL or OCSP response:

- Allow issuer signature: 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.

Individual Component Overrides:

LDAP Identity Provider:



Federated Identity Provider: