Symantec™ Validation and ID Protection Service (VIP)

Enterprise Gateway Installation and Configuration Guide

Symantec

Symantec™ VIP Enterprise Gateway Installation and Configuration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated July 11, 2016

Legal Notice

Symantec Corporation

350 Ellis Street Mountain View, CA 94043

http://www.symantec.com

https://www.symantec.com/contactsupport

Contents

Chapter 1 Introduction 1

Preinstallation Steps 1
About This Guide 2

Chapter 2 Hardware and Software Requirements 5

Installation Prerequisites 5
Password and User Information 5
Hardware and Software Requirements 6
VIP Enterprise Gateway Host 6
User Store 8
Configuring Syslog 8
Client Applications 8

Chapter 3 Installing VIP Enterprise Gateway 9

Before You Start 9
Activate Your Account 9
Review Platform Considerations 9
Special Considerations 10
Installing VIP Enterprise Gateway on Windows 10
Linux sudoers File Settings for VIP Enterprise Gateway 14
Installing VIP Enterprise Gateway on Linux 14
Starting and Stopping VIP Enterprise Gateway 15
Configuring Services for Autostart on Reboot 16

Chapter 4 Getting Started 17

Accessing the Configuration Console 17
Signing-in to the Configuration Console 17
Securing Communications with the VIP Authentication Service 19
Configuring SSL Certificates in VIP Enterprise Gateway 20
Restricting Transport Layer Security (TLS) Protocols and Weak Ciphers 22
Trusted CA Certificates 22
Initial Settings for Configuration Console 23
Configuring Console Settings 23
Configuring HTTP Proxy Settings 23
Viewing Configuration Summary 24
Notification Settings 25
Configuring Automatic Business Continuity 25

Chapter 5 Configuring User Stores 27

Multiple User Stores Configured with VIP Enterprise Gateway 27

Searching for Users in VIP Enterprise Gateway Configured with Multiple User Stores 28
Adding a User Store 30
Advanced User Store Configurations 32
Managing Connections 32
Modifying Search Criteria 33
Configuring Optional Attributes 34
Using User Groups and Administrator Groups in VIP Enterprise Gateway 35
Resetting the Expired Active Directory Password 36

Chapter 6 Configuring Validation Services 39

Prerequisites 39
Support for Out-of-Band Authentication 39
Authentication Modes 40
Authenticating Users Using VIP Access Push 42
Adding a Validation Server 44
Adding Custom RADIUS Attributes for the LDAP to RADIUS Mapping 48
Tunnel Forwarders and Receivers 48
Tunnel Forwarders 49
Tunnel Receivers 50
Starting and Stopping a Tunnel Forwarder or Tunnel Receiver 52
Health Monitor for Validation Server 52

Chapter 7 Configuring VIP Administrator Authentication 53

Administrators in VIP Enterprise Gateway 53
Configuring VIP Administrators 54
Authenticating Console Administrators to Sign In Using Their Enterprise Credentials 56

Chapter 8 Configuring Identity Providers 59

Self Service Portal Configuration 59
Configuring Self Service Portal IdP 59
Configuring Out-of-Band Authentication 60
Supported Languages 61
Password Management Support for Self Service Portal 61
Alternative IdP to Access Self Service Portal and VIP Manager 62
Testing Self Service Portal 62
Troubleshooting Self Service Portal 62
Self Service IdP Proxy 63
Publishing Self Service IdP as Reverse Proxy 63
Trusted Service Access Settings 63
VIP Manager IdP Configuration 65

Chapter 9 Configuring LDAP Directory Synchronization Service....67

Using LDAP Directory Synchronization Service to Synchronize User Stores to the VIP Service 67
Configuring Multiple Instances of LDAP Directory Synchronization Service 68

Use Case 1: Supporting Load-balancing and Failover 68
Use Case 2: Synchronizing Disparate User Stores Independently from Different VIP Enterprise Gateway Servers 68
Use Case 3: Synchronizing Users Created Through Third-party Identity Provider for Self Service Portals 69
An Example that Explains the Configuration of Multiple Instances of LDAP Directory Synchronization Service 69
Configuring LDAP Synchronization Service from the Configuration Console 71
LDAP Directory Synchronization - Best Practices that Symantec Recommends 71

Chapter 10 Testing the Installation 73

Verifying Component Installation 73
Verifying the RADIUS Client 73
Verifying Overall Operation 75

Chapter 11 Upgrading VIP Enterprise Gateway 77

Checking for the Upgrades and Patches 77
Installing VIP Enterprise Gateway Upgrades and Patches 79

Chapter 12 Logging of VIP Enterprise Gateway Components 83

Log File Components 83
Messages 84
Logging Detail Levels 84
Logging Options 86
Logs Tab 87
VIP Enterprise Gateway Components 87
Validation Server Logging 87
Configuration Console 88
IdP Service 90
LDAP Directory Synchronization 90
Syslog Logging 91
Configuring Syslog 91

Chapter 13 Exporting and Importing Configuration Settings 93

Exporting Configuration Settings 93
Importing Configuration Settings 94
Limitations of Importing the Configuration Settings 94

Appendix A Upgrading to VIP Enterprise Gateway Version 9.8 97

Upgrading to VIP Enterprise Gateway Version 9.8 97
Applying VIP Enterprise Gateway Updates Manually 98

Appendix B Uninstalling VIP Enterprise Gateway 99

Uninstalling VIP Enterprise Gateway Version 9.8 99
Uninstalling on Windows 99

Uninstalling on Linux 99
Restoring the Previous Version of VIP Enterprise Gateway 100

Appendix C Default Ports and Protocols 101

List of Default Ports and Protocols 101
Restricted Ports 102

Appendix D VIP Enterprise Gateway Utilities 103

Using the packTrustCA Utility 103
Using the vipdiagnostic Utility 104

Appendix E Troubleshooting 105

List of Error Codes 105

Index 109

Chapter 1

Introduction

This chapter includes the following topics:

- "Preinstallation Steps" on page 1
- "About This Guide" on page 2

VIP Authentication Service lets you authenticate any user on any network through a two-factor authentication process. In today's security-conscious environment, traditional user name and password approaches are increasingly recognized as insufficient to address the needs of enterprises. With VIP Authentication Service, users can access secured resources through a two-factor authentication process. This method of accessing resources eliminates the security problems that are associated with the use of passwords alone.

While seemingly free, passwords impose hidden costs of insecurity and management. The users may forget or compromise their passwords easily. Passwords can be compromised in a number of ways. The passwords can be sniffed on the network or recorded by keystroke loggers. They can be discovered as jotted on a notepad, or extracted from unwary employees through social engineering scams or phishing email campaigns.

Symantec Validation and ID Protection (VIP) Enterprise Gateway enables your organization's employees and associates to use the strong authentication capabilities that Symantec VIP Services provides, along with their enterprise directory authentication credentials.

VIP Enterprise Gateway provides RADIUS-based authentication server. You can use this authentication server with most of the enterprise-level network infrastructures that provide Remote Access Services such as VPN, Firewall, and application reverse proxy. Additionally, VIP Enterprise Gateway provides the plug-in options that you can use to integrate your enterprise-level applications and access management software with VIP Authentication framework.

VIP Enterprise Gateway provides Identity Providers (IdPs) for Self Service Portal (SSP) and VIP Manager Portal that Symantec's VIP Services host. VIP Manager Portal IdP enables your organization's IT Administrators to authenticate to VIP Manager using their LDAP user name and password and manage the VIP Account. The SSP IdP enables employees and associates to register or un-register their VIP credentials by authenticating with their enterprise directory authentication credentials.

Once VIP Enterprise Gateway is installed, you use the Configuration Console to configure VIP Enterprise Gateway and its components, and the Validation server.

Note: For more information on VIP implementation, refer to *Symantec™ VIP Enterprise Authentication Deployment Guide*.

Preinstallation Steps

To ensure a smooth installation of the VIP Enterprise Gateway, complete these preinstallation steps:

Step 1 Confirm your VIP Authentication Service account information

After your representative sets up an account for you, your designated Technical Contact receives a VIP Authentication Service account activation email. This email is to confirm that your contact information is correct. If you are unsure who your technical contact is, contact Customer Support.

After your purchase is processed, access VIP Manager to obtain the VIP Enterprise Gateway software and VIP certificate.

Step 2: Acquire and install hardware and software

Acquire the hardware and associated software you need to work with VIP Enterprise Gateway. Ensure that your system meets the minimum hardware and software requirements.

See “Hardware and Software Requirements” on page 6.

Step 3: Before you install and configure VIP Enterprise Gateway and its components, Symantec recommends you to read *Symantec VIP Enterprise Authentication Deployment Guide*. This guide helps you understand Symantec VIP authentication service.

To access the *Symantec VIP Enterprise Authentication Deployment Guide* in VIP Manager, complete the following steps:

1. Sign in to VIP Manager.
2. Click the **Accounts** tab. On the right side, under **Links**, click **Download Files**.
3. In the Download Files page, in the **File List** table, click **General Documentation**.
4. In the list of PDF files, locate the VIP_Enterprise_Authentication_Deployment_Guide.pdf file. Click the file to open the *Symantec VIP Enterprise Authentication Deployment Guide* or save the file to the hard drive of your computer.

About This Guide

This guide is meant for anyone responsible for installing and configuring VIP Enterprise Gateway Configuration Console, such as Information Technology (IT) administrators and database administrators (DBAs).

The following is the summary of chapters in this guide:

- Chapter 2, "Hardware and Software Requirements," describes the minimum hardware and software requirements for VIP Enterprise Gateway installation.
- Chapter 3, "Installing VIP Enterprise Gateway," describes how to install the VIP Enterprise Gateway software.
- Chapter 4, "Getting Started," describes how to get started with VIP Enterprise Gateway.
- Chapter 5, "Configuring User Stores," describes how to configure one or more User Stores for user authentication. User Stores are the directory services that typically contain the user information that is related to authentication.
- Chapter 6, "Configuring Validation Services," describes how to configure Validation service with VIP Enterprise Gateway. Validation service is a RADIUS server that processes requests to authenticate user credentials. Validation service validates users against your chosen authentication factors (such as security codes and LDAP passwords).
- Chapter 7, "Configuring VIP Administrator Authentication," describes the two portals - Configuration Console and VIP Manager Identity Provider (IdP) - that VIP Enterprise Gateway provides for administrative functions. Also, this chapter describes the administrators - Local administrator, VIP administrators, and Console administrators - in VIP Enterprise Gateway.
- Chapter 8, "Configuring Identity Providers," describes how to configure secure access to Self Service Portal IdP and VIP Manager IdP from VIP Enterprise Gateway. The Self Service Portal IdP provides secure access to the SSP. The VIP Manager IdP provides secure access to the VIP Manager.
- Chapter 9, "Configuring LDAP Directory Synchronization Service," describes how to configure LDAP Directory Synchronization Service. This service automatically synchronizes the users and the administrators in your LDAP directory with the user data in the VIP Service.
- Chapter 10, "Testing the Installation," describes how to test your installation of VIP Enterprise Gateway. This testing verifies the correct installation of the individual components of VIP Enterprise Gateway and verifies its overall operation. This testing ensures that your deployment is ready to support users in a production environment.
- Chapter 11, "Upgrading VIP Enterprise Gateway," describes how to use the Update Settings feature to check for product updates, download them, and install them.

- Chapter 12, "Logging of VIP Enterprise Gateway Components," describes how the log files are created, configured, and viewed in VIP Enterprise Gateway.
- Chapter 13, "Exporting and Importing Configuration Settings," describes how to export the various configuration settings that are saved as a .zip file to the VIP Enterprise Gateway server. The import section describes how to reuse the configuration settings among the same version and cross-version of VIP Enterprise Gateway server.
- Appendix A, "Upgrading to VIP Enterprise Gateway Version 9.8," describes how to upgrade your VIP Enterprise Gateway instance to the latest version.
- Appendix B, "Uninstalling VIP Enterprise Gateway," describes how to uninstall your current VIP Enterprise Gateway instance and restore its previous version.
- Appendix C, "Default Ports and Protocols," describes the default ports and the protocols that VIP Enterprise Gateway use.
- Appendix D, "VIP Enterprise Gateway Utilities," provides an overview of the VIP Enterprise Gateway utilities.
- Appendix E, "Troubleshooting," describes the reason codes that you may encounter in VIP Enterprise Gateway, and provides some solutions.

Chapter 2

Hardware and Software Requirements

This chapter includes the following topics:

- "Installation Prerequisites" on page 5 lists the items you need to acquire, and the tasks you need to complete, to prepare the hardware and software you use for your VIP Enterprise Gateway installation.
- "Hardware and Software Requirements" on page 6 lists the hardware and the software that are required for your VIP Enterprise Gateway components.
- "Client Applications" on page 8 discusses the integration modules you can use to integrate VIP Enterprise Gateway with your client applications.

This chapter describes the hardware and software you need to deploy the VIP Enterprise Gateway components on dedicated hosts for Windows and Linux platforms.

Installation Prerequisites

Before you begin the installation of VIP Enterprise Gateway, you need to have or to complete the following:

- VIP Enterprise Gateway installation `.zip` (Windows) or `.tar` (Linux) file. This file is available from VIP Manager.
- Configuration Console administrator passwords and appropriate user rights. See "Password and User Information" on page 5.
- Hardware and software, which meet the requirements. See "Hardware and Software Requirements" on page 6.
- Domain Naming System (DNS) that properly functions. This requirement is essential to configure Active Directory as User Store with VIP Enterprise Gateway.

Password and User Information

You need the following to complete the installation process:

- **Sign in information for the administrator who does theVIP Enterprise Gateway configuration**. Your administrator will need a user name and password to access the VIP Enterprise Gateway Configuration Console.

- **User rights**. You need to have users with the rights to access the VIP Enterprise Gateway components described in Table 2-1.

Table 2-1 Users and Rights

Component	User/Right
User Store	■ For AD-based User Stores, the user must have domain user privileges. ■ For LDAP-based User Stores, the user must have search privileges on the sub tree for the given search base.
VIP Enterprise Gateway host	Root access on Linux and Local computer Administrator group access on Windows.

Hardware and Software Requirements

This section lists the VIP Enterprise Gateway hardware and software requirements by component type.

You need to install the following on your servers:

- "VIP Enterprise Gateway Host" on page 6
- "User Store" on page 8

VIP Enterprise Gateway Host

See Table 2-2 and Table 2-3 for lists of the hardware and software you need to install VIP Enterprise Gateway. These requirements also apply if you install VIP Enterprise Gateway in a virtual environment.

Note: Symantec recommends to run only the VIP Enterprise Gateway processes or servers on this host.

Windows Platform

Table 2-2 Requirements for VIP Enterprise Gateway on Windows

Minimum Hardware Requirements	Software Requirements
■ Intel or Intel-compatible 64-bit architecture ■ 4 GB RAM ■ 40 GB disk space	One of the following operating systems: ■ Windows 2012 R2 x64 ■ Windows 2012 x64 ■ Windows 2008 R2 x64 (Service Pack 1)

Linux Platform

Table 2-3 Requirements for VIP Enterprise Gateway on Linux

Minimum Hardware Requirements	Software Requirements
■ Intel or Intel-compatible 64-bit architecture ■ 4 GB RAM ■ 40 GB disk space	One of the following operating systems: ■ RHEL 7.2 (64 bit) ■ RHEL 7.1 (64 bit) ■ RHEL 6.8 (64 bit) ■ RHEL 6.7 (64 bit) Install the following supported GNU C (glibc) 32 bit libraries: ■ RHEL 7.x - glibc 2.17 or higher ■ RHEL 6.x - glibc 2.16 or higher **Note:** The glibc versions mentioned in this table are examples only. For more information on the supported glibc versions, refer to the Product Documentation of the respective RHEL version.

Installing the Dependencies Required for VIP Enterprise Gateway on Red Hat Linux EL 6.x, and 7.x (64-bit)

1. Mount the RHEL <*version*> CD/DVD.
2. Navigate to `/mnt/Packages` on the drive where you have mounted the CD.
3. From the `Packages` folder, run the following command:

```
rpm -ivh libgcc-4.4.6-4.el6.i686.rpm libstdc++-4.4.6-4.el6.i686.rpm glibc-2.12-
.80.el6.i686.rpm nss-softokn-freebl-3.12.9-11.el6.i686.rpm libidn-1.18-2.el6.i686.rpm
```

Note: The versions that are displayed in bold in this command may differ based on the RHEL versions you use. You must ensure that you use the correct RHEL version to install the dependencies.

Browser Requirements

The following are the supported browsers that can be used to access the Configuration Console:

- Microsoft Internet Explorer versions 10.0, 11.0, and Edge
- Firefox versions 47
- Chrome version 51

Note: If you want to use Internet Explorer to access VIP Enterprise Gateway Configuration Console, you must disable **Internet Explorer Enhanced Security Configuration (IE ESC)**.

User Store

VIP Enterprise Gateway supports LDAP User Stores. You may use one or more LDAP directories as User Stores, but they must be one of the following:

- Windows Active Directory 2003
- Windows Active Directory 2008
- Windows Active Directory 2008 R2
- Windows Active Directory 2012
- Windows Active Directory 2012 R2
- Novell eDirectory 8.8 Service Pack 8
- Open LDAP 2.4.44
- Oracle Directory Server Enterprise Edition 11.1.1.7.0

Configuring Syslog

By default, VIP Enterprise Gateway writes logs to standard log files ("Logging of VIP Enterprise Gateway Components" on page 83). You can also configure VIP Enterprise Gateway to use syslog to write logs to the syslog server ("Configuring Syslog" on page 91).

Client Applications

VIP Enterprise Gateway is compatible with the client application integration modules. For more information on these modules, refer to the VIP third-party integration guides.

To download these guides from VIP Manager, do the following:

1. Access VIP Manager (https://manager.vip.symantec.com).
2. Click **Accounts** tab.
3. On the right side, under **Links**, click **Download Files**.
4. In the **File List** table, under the **Name** column, click to open the `Third_Party_Integrations` folder and download the VIP third-party integration guides.

Chapter 3

Installing VIP Enterprise Gateway

This chapter includes the following topics:

- "Before You Start" on page 9
- "Installing VIP Enterprise Gateway on Windows" on page 10
- "Installing VIP Enterprise Gateway on Linux" on page 14
- "Starting and Stopping VIP Enterprise Gateway" on page 15
- "Configuring Services for Autostart on Reboot" on page 16

This chapter describes how to install VIP Enterprise Gateway.

Before You Start

Before you begin this installation, refer to the *VIP Enterprise Gateway Release Notes*. Review the text carefully, as it may include corrections to the instructions that you read in this chapter.

Activate Your Account

You received an activation email from VIP Manager. Complete the instructions in that email to activate your account.

Review Platform Considerations

Review the following platform-specific considerations before you begin the installation.

Windows

On Windows, you must always install VIP Enterprise Gateway as a user with administrator privileges.

Linux

Note the following for Linux:

- Do not install in a directory that contains a space in its name. If you do so, later steps in the installation procedure fail.
- The user name should not contain a space.
- Ensure that the host name is set correctly in the `/etc/hosts` file for the computer on which you plan to install VIP Enterprise Gateway.

Special Considerations

After installing VIP Enterprise Gateway or before upgrading to a newer version of VIP Enterprise Gateway, ensure that the VIP Enterprise Gateway server can access the following URLs:

- https://ssp.vip.symantec.com/
- https://manager.vip.symantec.com
- https://userservices.vip.symantec.com/
- http://liveupdate.symantecliveupdate.com
- http://liveupdate.symantec.com
- https://userservices-auth.vip.symantec.com
- http://www.symantec.com
- https://knowledge.symantec.com

Installing VIP Enterprise Gateway on Windows

Complete the following steps to install VIP Enterprise Gateway on Windows:

1 Download the VIP Enterprise Gateway installation `.zip` file from VIP Manager.

2 Extract the `.zip` file to a temporary directory on the computer where you want to host the Configuration Console.

3 Open the **windows** folder. Run `setup.exe` to start the installation.

The Welcome page displays (Figure 3-1).

Figure 3-1 Welcome dialog box

4 Click **Next**.

The Symantec Software License Agreement page displays (Figure 3-2).

Figure 3-2 License Agreement dialog box

5 In the License Agreement page, read the agreement, and then click **Next**.

The Configuration Console Access page displays (Figure 3-3).

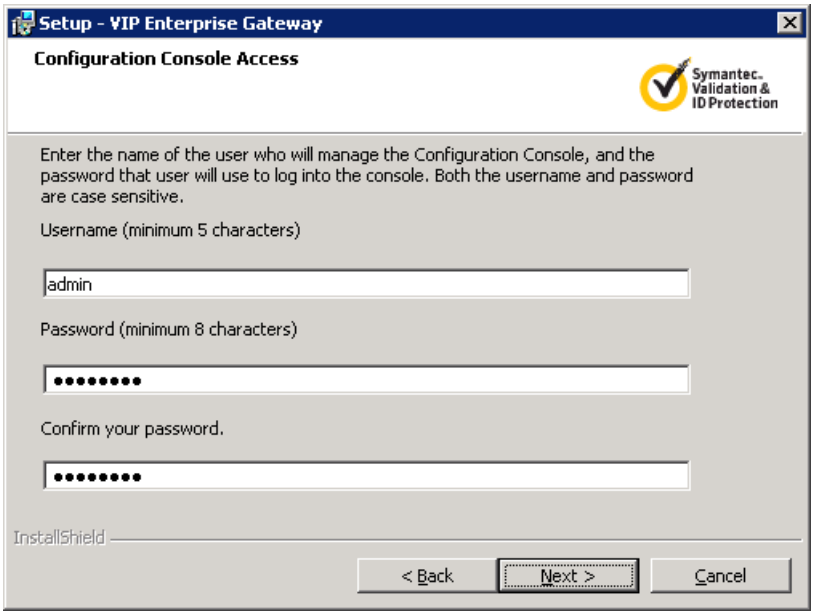

Figure 3-3 Configuration Console Access page

6 In the Configuration Console Access page, type a user name and password for the administrator who accesses Configuration Console.

- Type a user name that contains at least five characters, but not more than 40 characters.

- Type a password that contains at least eight characters, but not more than 40 characters.

7 Click **Next**.

The Destination Folder page displays (Figure 3-4).

a The Change Current Destination Folder page displays. By default, the files are installed in:

On Windows 2008 and later (64 bit): `C:\Program Files (x86)\Symantec\VIP_Enterprise_Gateway`
If you choose to install files to a different location, click **Browse** to locate the directory where you want to install VIP Enterprise Gateway.

b If the disk space is low, the Disk space Requirements page displays. Click **Space** to verify that you have enough disk space to install the selected features, or click **Next** to set the installation directory.

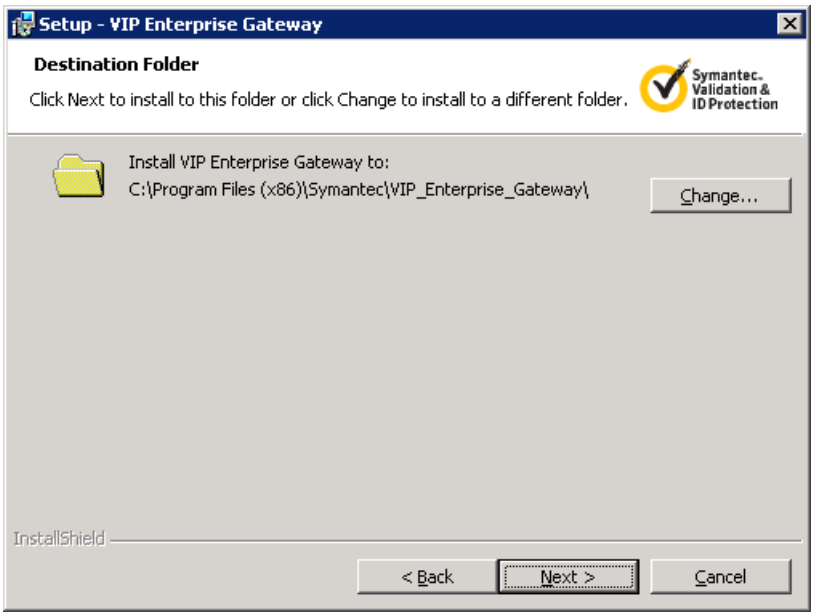

Figure 3-4 Destination Folder page

8 Click **Next**.

The Ready to Install VIP Enterprise Gateway page displays (Figure 3-5).

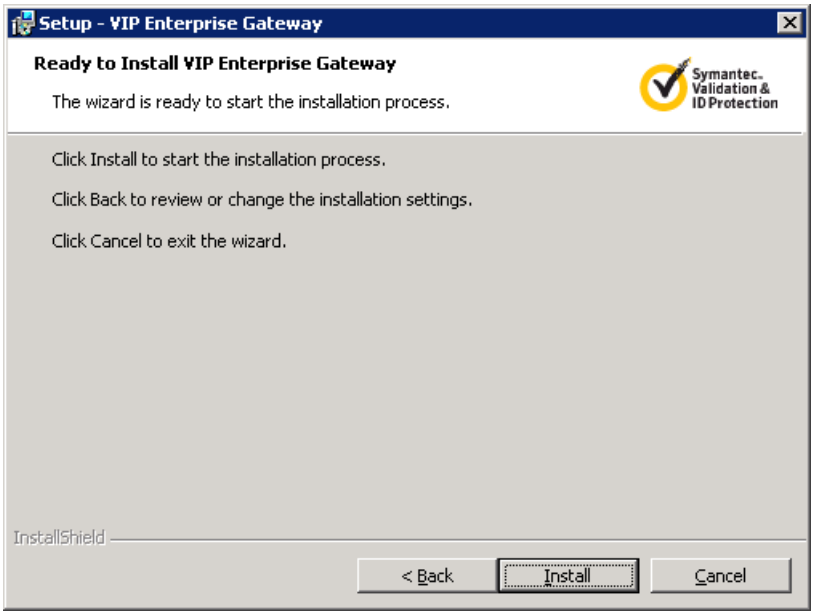

Figure 3-5 Ready to Install VIP Enterprise Gateway page

9 The installer now has enough information to begin installing VIP Enterprise Gateway. Click **Install** to begin the installation.

10 When the installation is complete, the Success page displays (Figure 3-6).

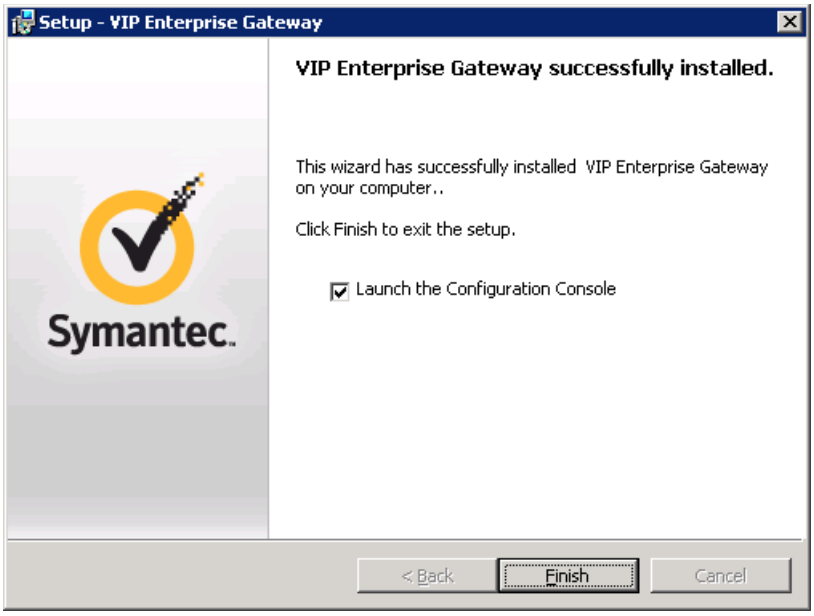

Figure 3-6 InstallShield Wizard Completed page

You can open the Configuration Console immediately after exiting the installer by keeping the **Launch the Configuration Console** check box selected.

11 Click **Finish** to exit the installer.

Next

You must configure VIP Enterprise Gateway in the Configuration Console before you can begin using it.

You can use the following URL to access the Configuration Console:

http://<hostname of the VIP Enterprise Gateway machine>:8232

Linux sudoers File Settings for VIP Enterprise Gateway

The `sudoers` file is located at `/etc` on all Linux-based operating systems (for example, RHEL). This file contains a list of users and their sudo permission levels.

To install VIP Enterprise Gateway on a Linux-based operating system, the users require to be part of the `sudoers` list.

The `sudoers` file is composed of two types of entries – aliases (basically variables) and user specifications (specifying the user's permissions).

The examples of the sudoers file entries are:

```
user1     ALL=(ALL)
```

That is, `user1` has full permissions, but needs a password. Operating system prompts for a password whenever `user1` tries to perform a task.

```
user2    ALL=(ALL)    NOPASSWD: ALL
```

That is, `user2` can perform all tasks without a password. The operating system no longer prompts for a password.

Note: To install VIP Enterprise Gateway version 9.7, the user must have permission levels equivalent to `user2` that is described in this example.

For more information on sudoers, refer to Linux documentation.

The super user of the system needs to add the following information to the `/etc/sudoers` file to enable you to install VIP Enterprise Gateway as a normal user:

Note: The user with administrator privileges that will install the VIP Enterprise Gateway must have access to the path locations mentioned in the sudoers list.

```
Cmnd_Alias EG_FOLDERS = <VRSN_MAUTH_HOME >/server/bin/ , /root/LiveUpdate, /bin/rm, /usr/bin/
vim, /bin/bash, <VRSN_MAUTH_HOME>/server/work/, <VRSN_MAUTH_HOME >/_uninst/, /opt/Symantec/
LiveUpdate, /bin/chmod, <Extracted PATH of installer>/linux/setup.bin

<VIPUser> ALL= NOPASSWD:EG_FOLDERS
```

If you want to install VIP Enterprise Gateway as a super user, you do not need to make this change.

Installing VIP Enterprise Gateway on Linux

To install VIP Enterprise Gateway on Linux, follow these steps:

Task 1. Prepare the installation files.

1. Download the VIP Enterprise Gateway installation tar file from VIP Manager.
2. Extract the `.tar` file to a temporary directory on the computer where you want to host the Configuration Console.
3. Open a terminal window.

Task 2. Run the installation script

1. From the temporary directory where you copied the installation files (in Task 1), execute **.**`/setup.sh`. The user that executes this installation script is the user that starts the VIP Enterprise Gateway server process.

Note: Run the `setup.sh` file as a sudo user who does not require a password for the sudo operations. For more information on how to add a user to `/etc/sudoers`, refer to the Linux documentation.
For more information on the `sudoers` file, see "Linux sudoers File Settings for VIP Enterprise Gateway" on page 14.

2. The script displays a *Welcome* message. Press **Enter** to continue with the installation.
3. Symantec Software License Agreement displays. Press **Enter** to read the agreement. Type **1** to accept the terms of the license agreement with Symantec and press **Enter** again to continue with the installation.
4. Enter the user name and the password that are used to access Configuration Console.

Note: Both the user name and password are case-sensitive.

   a. Enter a user name that is at least 5 characters, but not more than 40 characters.
   b. Enter a password that is at least 8 characters long, but not more than 40 characters.
   c. Re-enter your password to confirm it.
   d. Press **Enter** to continue with the installation.
5. The default directory where VIP Enterprise Gateway files are installed is displayed.
   To change the location, enter the new location, and then press **Enter**.
6. Review the installation summary, then press **y** to install VIP Enterprise Gateway.

   The installer begins installing VIP Enterprise Gateway.
7. Run `<VRSN_MAUTH_HOME>/server/bin/startup.sh` to start the server that hosts the Configuration Console, where `<VRSN_MAUTH_HOME>` is the directory where the VIP Enterprise Gateway is installed. You can run the `startup.sh` script from any location.

Step 3: Configure VIP Enterprise Gateway

You must configure VIP Enterprise Gateway in the Configuration Console before you can begin using it. Access the Configuration Console at http://<hostname of the VIP Enterprise Gateway machine>:8232.

Starting and Stopping VIP Enterprise Gateway

Some procedures that are discussed in this document require that you stop the VIP Enterprise Gateway service before you make some change. You must start this service again after you make the changes.

After you have completed the installation, VIP Enterprise Gateway runs as a service on the computer on Windows. Either the administrator who installed VIP Enterprise Gateway (or an administrator for that computer) or the console administrator can start, stop, or modify the VIP Enterprise Gateway Service.

See "Authenticating Console Administrators to Sign In Using Their Enterprise Credentials" on page 56.

To start or stop the VIP Enterprise Gateway service:

- **Windows**: Go to **Start** → **Administrative Tools** → **Services** → **VIP Enterprise Gateway** and manage it as a standard Windows service application.
- **Linux**: To start the service, run:
  `<VRSN_MAUTH_HOME>/server/bin/startup.sh`

  To stop the service, run `<VRSN_MAUTH_HOME>/server/bin/shutdown.sh`.

Configuring Services for Autostart on Reboot

If you are running VIP Enterprise Gateway on Linux, you can configure various services to autostart on reboot. Follow these steps to set up the autostart for required services:

Note: You must have super user privilege to execute this procedure.

1. Copy the .rc file of the following components and place it in `/etc/init.d`:
   - For VIP Enterprise Gateway, copy vipegconsole.rc from:
     `<VRSN_MAUTH_HOME>/server/bin`
   - For SSP IDP, copy SSP.rc from:
     `<VRSN_MAUTH_HOME>/IDP/services/SSP/logs`
   - For VIP Manager, copy VIPMGR.rc from:
     `<VRSN_MAUTH_HOME>/IDP/services/VIPMGR/logs`
   - For LDAP Synchronization Service, copy ldapService.rc
     `<VRSN_MAUTH_HOME>/LdapSync/services/ldapSync/logs`
   - For Validation servers, copy <valServer>.rc from:
     `<VRSN_MAUTH_HOME>/Validation/servers/<valServer>/logs`
2. Make the script executable by using the following command:

   ```
   chmod +x /etc/init.d/<name of the rc file(s)>
   ```

   (This is optional, as the rc files have execute permissions by default when created.)
3. Create a start script symlink in the run level rc directory for the required services' .rc files. For VIP Enterprise Gateway:

   `/etc/init.d/vipegconsole.rc.`

   For example:

   ```
   $ ln -s /etc/init.d/vipegconsole.rc /etc/rc.d/rc5.d/S999vipegconsole
   ```

   The run level of the Linux machine should be checked using the following command:

   ```
   who –r
   ```

   Then place the start script symlink in that particular run level rc directory.
4. Test start/stop of the service manually by calling the corresponding functions. For example:

   ```
   /etc/init.d/vipegconsole.rc start
   ```

   or

   ```
   /etc/init.d/vipegconsole.rc stop
   ```

If the manual tests succeed, the configuration for autostart of services on reboot is considered complete.

Note: On RHEL 7.x, autostart on reboot does not automatically start all the components with .rc files. Refer the Knowledge Center to customize the .rc files for RHEL 7.x to autostart services.

Chapter 4

Getting Started

This chapter helps you get started with VIP Enterprise Gateway. This chapter describes the following:

- "Accessing the Configuration Console" on page 17
- "Securing Communications with the VIP Authentication Service" on page 19
- "Configuring SSL Certificates in VIP Enterprise Gateway" on page 20
- "Restricting Transport Layer Security (TLS) Protocols and Weak Ciphers" on page 22
- "Trusted CA Certificates" on page 22
- "Initial Settings for Configuration Console" on page 23
- "Viewing Configuration Summary" on page 24
- "Notification Settings" on page 25

Accessing the Configuration Console

The Configuration Console allows you to configure the VIP Enterprise Gateway settings.

Use the same user name and password that you provided during the installation of the VIP Enterprise Gateway to login to the Configuration Console. Contact your IT administrator for any support regarding your user credentials.

Use the Password tool to add new users who can access Configuration Console, delete users from Configuration Console, or reset your user name and password. The Password tool is a command line tool. To run the Password tool, go to the <VRSN_MAUTH_HOME>/server/bin directory, and run `passwordTool.bat` (Windows) or `passwordTool.sh` (Linux).

Signing-in to the Configuration Console

You can sign in to the Configuration Console as a local administrator. Use the user credentials that you provided during the installation of the VIP Enterprise Gateway to sign in to the Configuration Console.

Note: You can also sign in to the Configuration Console using the enterprise directory credentials (AD or LDAP). Refer to "Authenticating Console Administrators to Sign In Using Their Enterprise Credentials" on page 56 for more information.

To sign in to the Configuration Console:

1 Go to **Start** → **Programs** → **Symantec** → **VIP Enterprise Gateway**→ **Configuration Console** (Windows)

or

Use a browser to access the following URL:

http(s)://<hostname/FQDN of the VIP Enterprise Gateway Machine>:8232

If you have signed in as a local administrator, the Sign In page is displayed as shown in Figure 4-1.

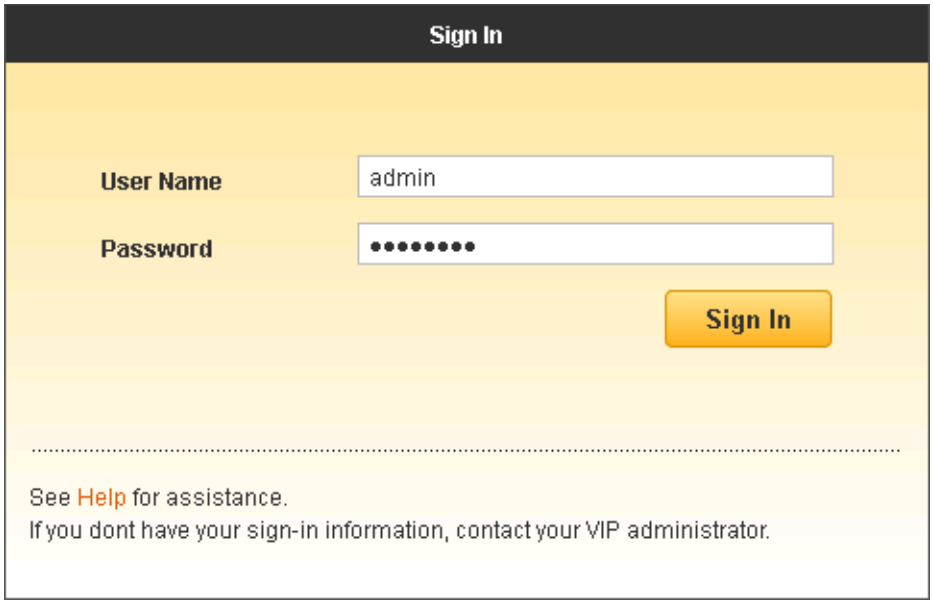

Figure 4-1 Configuration Console Sign In page

2 Enter your user name and password, and then click **Sign In**.

The Configuration Console will display a Confirm Sign In message if another user has already logged in. Click **No** if you want to cancel the sign in attempt and return to the Sign In page. Click **Yes** if you want to continue to sign into the Configuration Console. After you sign in, the first user is redirected to the Sign In page at the subsequent click of an active tab, button, or a link.

On the Home page, a brief description of the VIP Enterprise Gateway is provided. You must first add a VIP Certificate to start using VIP Enterprise Gateway. This certificate is required for VIP Enterprise Gateway to authenticate itself to the VIP Authentication service in the cloud.

Click **Add VIP Certificates** to obtain the certificate from VIP Manager and import it to VIP Enterprise Gateway. Refer to "Securing Communications with the VIP Authentication Service" on page 19 for more information.

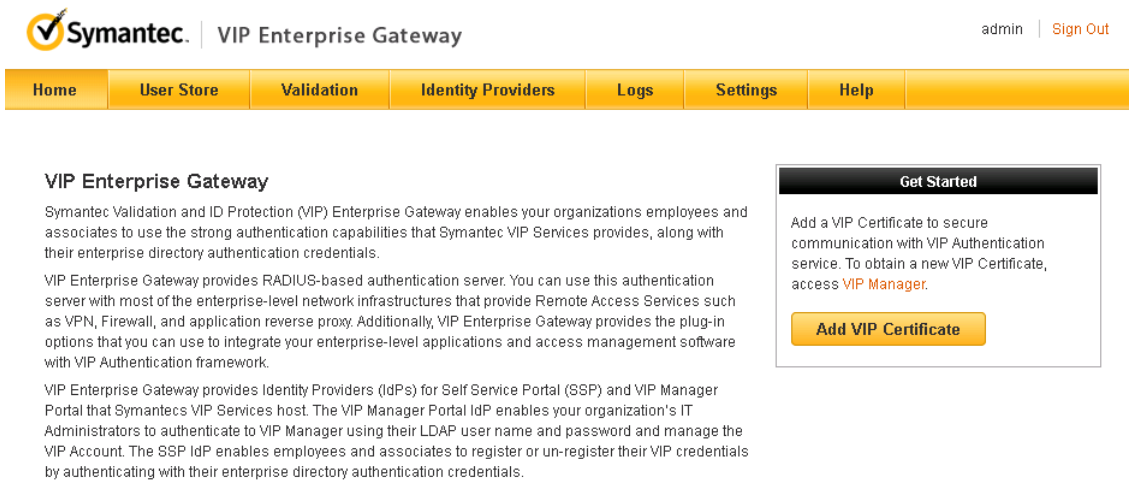

Figure 4-2 Home page

Securing Communications with the VIP Authentication Service

VIP Enterprise Gateway uses a digital certificate to authenticate itself to the VIP Authentication Service.

To import the VIP certificate to VIP Enterprise Gateway:

1. Do one of the following:
   - From the Home page, click **Add VIP Certificates**.
   - Navigate to **Settings > VIP Certificate** and click **Add VIP Certificates**.
2. Click **Browse** to locate and select the certificate in the PKCS#12 format.
3. Enter the password that you specified while obtaining the certificate from VIP Manager.
4. Enter an alias name for the certificate. The alias name can only contain alphanumeric characters, and hyphens, spaces, or underscores.
5. Click **Submit**.

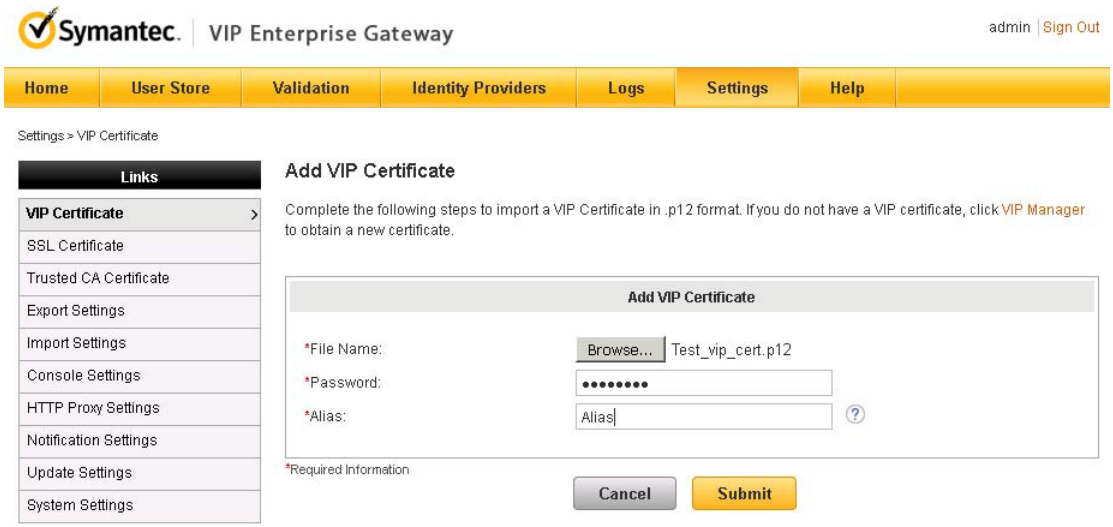

Figure 4-3 Add VIP Certificate page

The VIP certificates that are imported to VIP Enterprise Gateway are listed as shown in Figure 4-4.

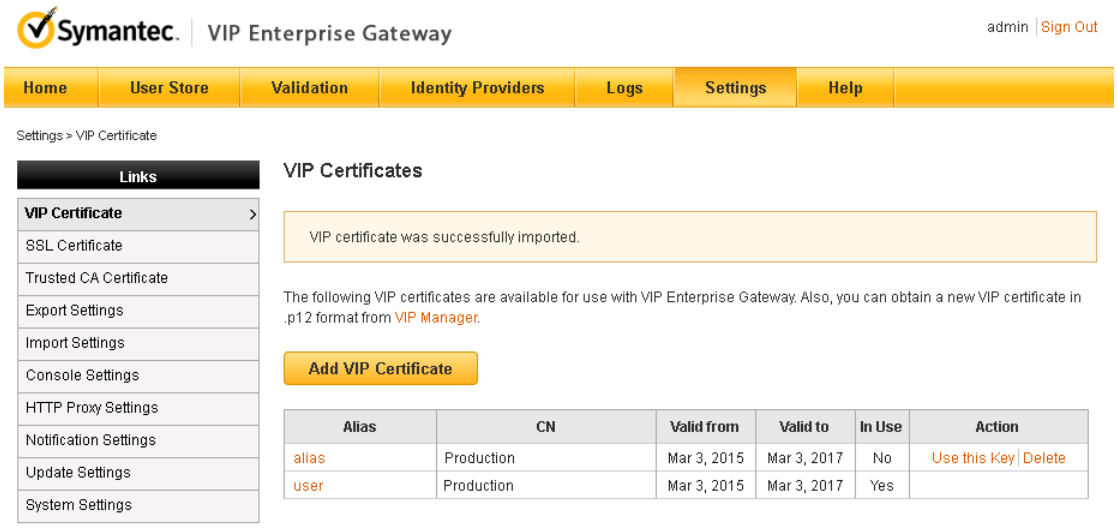

Figure 4-4 VIP Certificates List Page

Note: You can delete the VIP certificates that are not in use or are expired. Click the **Delete** link in the Action column on the VIP Certificates page to delete the certificate.

Configuring SSL Certificates in VIP Enterprise Gateway

To establish a HTTPS communication on your server, you need to apply for an SSL certificate, and install that certificate on your server. You can use Configuration Console to complete the following general steps. Refer to the *VIP Enterprise Gateway online help* for detailed procedures:

1. Generate a certificate key pair and a Certificate Signing Request (CSR) using the information about your organization and your server computer.
2. Submit the CSR to Symantec to obtain a Symantec CA certified Server Certificate.
3. Install the SSL certificate that you receive over an email.
4. Enable the SSL key for the certificate that you have installed on the VIP Enterprise Gateway server.
5. Optionally, if the SSL certificate is not issued by a public CA, import the CA chain into your trusted CA keystore. Refer to "Trusted CA Certificates" on page 22 for more information on trusted CA chains.
6. You can also import a certificate in the PKCS#12 format.

   To import the SSL Certificate, do the following:

   a. Navigate to **Settings** > **SSL Certificate.**
   b. In the SSL Certificates page**,** click **Add SSL Certificate.**
   c. In the Add SSL Certificate page, select **Import SSL Certificate** (Figure 4-5).
   d. Click **Browse** to locate and select a certificate in the PKCS#12 format.
   e. Enter the password for the certificate that you have selected to import.
   f. Enter an alias name for the certificate. The alias name can only contain alphanumeric characters, and hyphens, spaces, or underscores.
   g. Click **Add**.

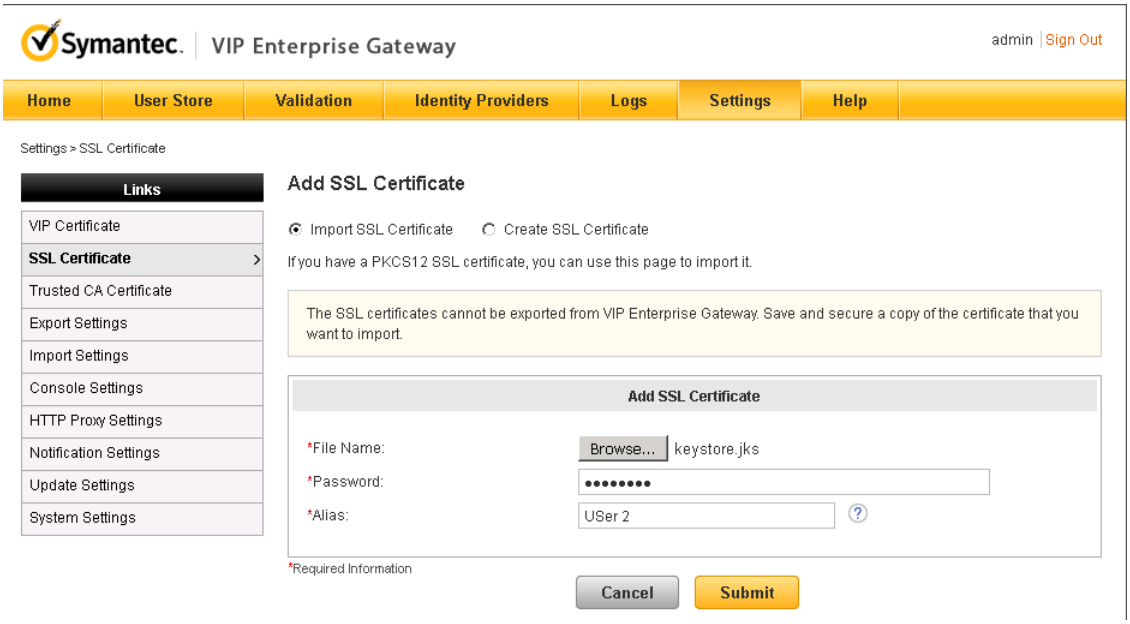

Figure 4-5 Import PKCS12 SSL Certificate

Note: The SSL certificates cannot be exported from VIP Enterprise Gateway. Store and secure the certificate in the organization certificate vault to reuse or recover it in the future. Select the **Import SSL certificate** option to reuse the stored certificate.

The SSL certificates that are created or imported are listed in the SSL Certificates page (Figure 4-6).

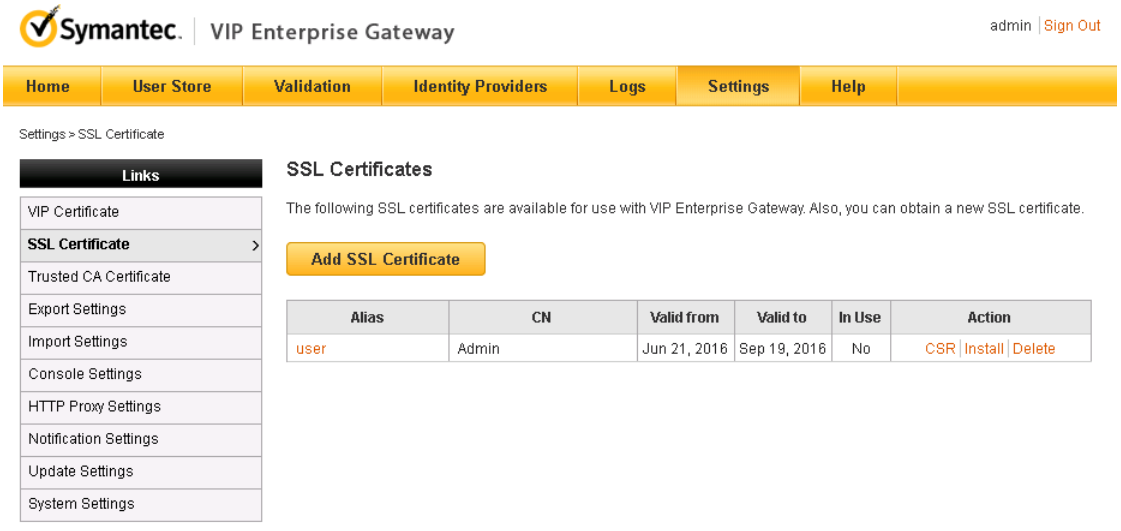

Figure 4-6 SSL Certificates page

You can delete the SSL certificate if it is not used by SSP IdP, VIP Manager IdP, Enterprise Gateway Configuration Console, or a Tunnel Receiver. To delete the SSL certificate, click the **Delete** link under Action column.

Restricting Transport Layer Security (TLS) Protocols and Weak Ciphers

By default, SSL protocol versions 2.0 and 3.0 are considered weak and are listed in the `BlacklistedProtocols.properties` file. The weak ciphers, that is the ciphers with key length lesser than 128 bits are restricted and are listed in the `weakciphers.properties` file.

You can modify the `BlacklistedProtocols.properties`, or `weakciphers.properties` files to restrict any TLS protocol such as SSL or weak cipher such as RC4 when potential vulnerabilities are detected.

Trusted CA Certificates

To manage your Trusted CA store, navigate to **Settings > Trusted CA Certificates** (Figure 4-7).

You may also need to add a CA to the Trusted CA Store, if your SSL certificate is not issued from a public Issuing Authority.

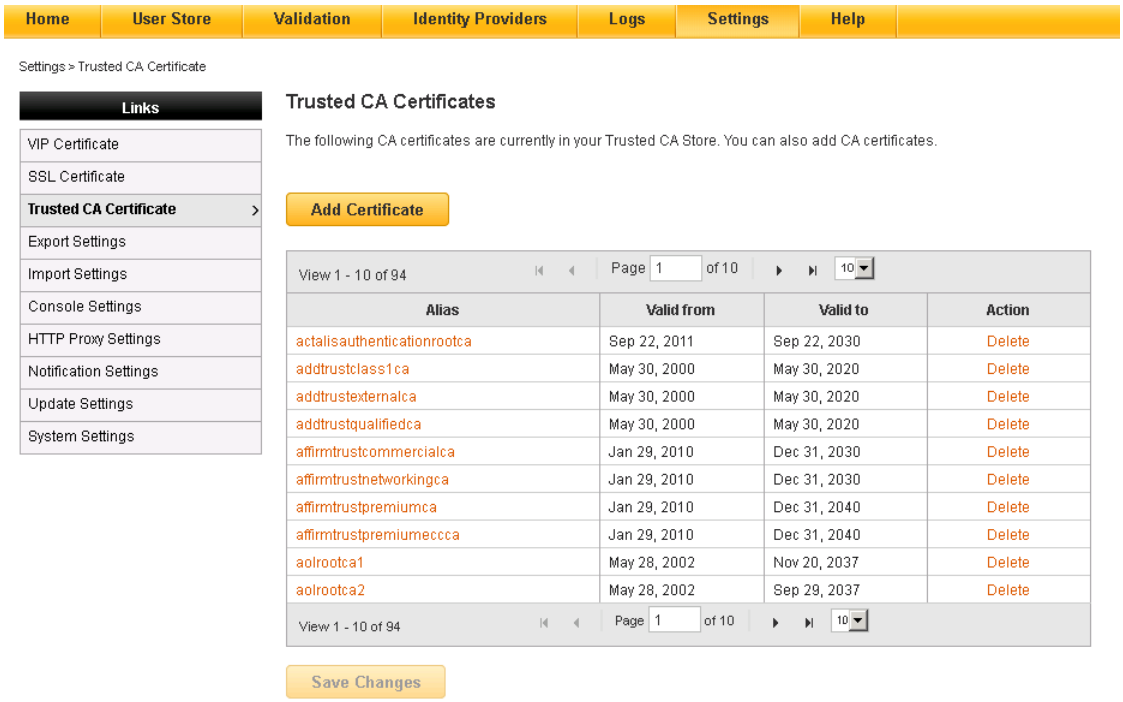

Figure 4-7 Trusted CA Certificates page

Initial Settings for Configuration Console

After you add the VIP certificate, Symantec recommends you to do the following settings on the Configuration Console:

Configuring Console Settings

To set the port, protocol (HTTP or HTTPS), logging level, or syslog option from Configuration Console, navigate to **Settings > Console Settings**.

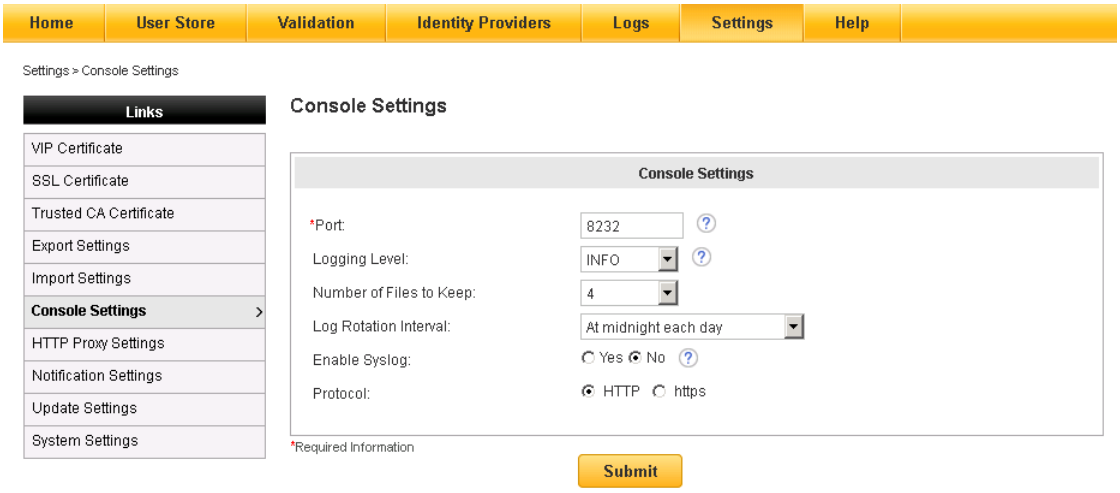

Figure 4-8 Console Settings page

Configuring HTTP Proxy Settings

VIP Enterprise Gateway supports proxy servers using Anonymous or Basic Authentication.

To configure HTTP proxy settings, navigate to **Settings > HTTP Proxy Settings**.

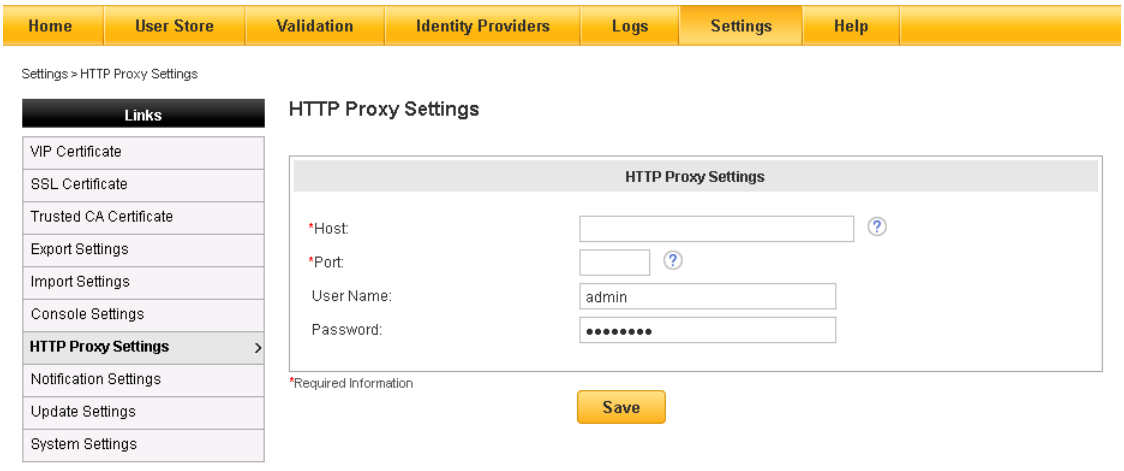

Figure 4-9 HTTP Proxy Settings page

Viewing Configuration Summary

The Configuration Summary page displays the configuration settings of all the components as described in Table 4-1.

Table 4-1 Configuration Summary of VIP Enterprise Gateway components

Component	Description
VIP Certificate	You can view the name of the VIP certificate and its validity. Also, you can see a notification indicating the days remaining for the expiration of the active VIP certificate.
User Store	You can view the names of the User Stores, their IP addresses, and whether SSL is enabled on them for communication.
LDAP Directory Synchronization	You can view the User Synchronization and the Administrator Synchronization settings. Also, you can start or stop the LDAP Directory Synchronization service from this page.
RADIUS Validation Server	You can view the names of the RADIUS Validation servers and their IP addresses. Also, you can start or stop the RADIUS Validation service from this page.
Tunnel Server	You can view the names of the Tunnel Receivers and Forwarders, their IP addresses and whether SSL is enabled on them. Also, you can start or stop the Tunnel Service from this page.
Self Service Portal IdP	You can view the Self Service Portal IdP URL and whether SSL is enabled for this URL. Also, you can start or stop the Self Service Portal IdP Service from this page.
VIP Manager IdP	You can view the VIP Manager IdP URL and whether SSL is enabled for this URL. Also, you can start or stop the VIP Manager IdP Service from this page.

Notification Settings

Notification settings allows you to define and configure email notifications for network connectivity issues and switching to business continuity mode. To configure email notification, navigate to **Settings > Notification Settings**.

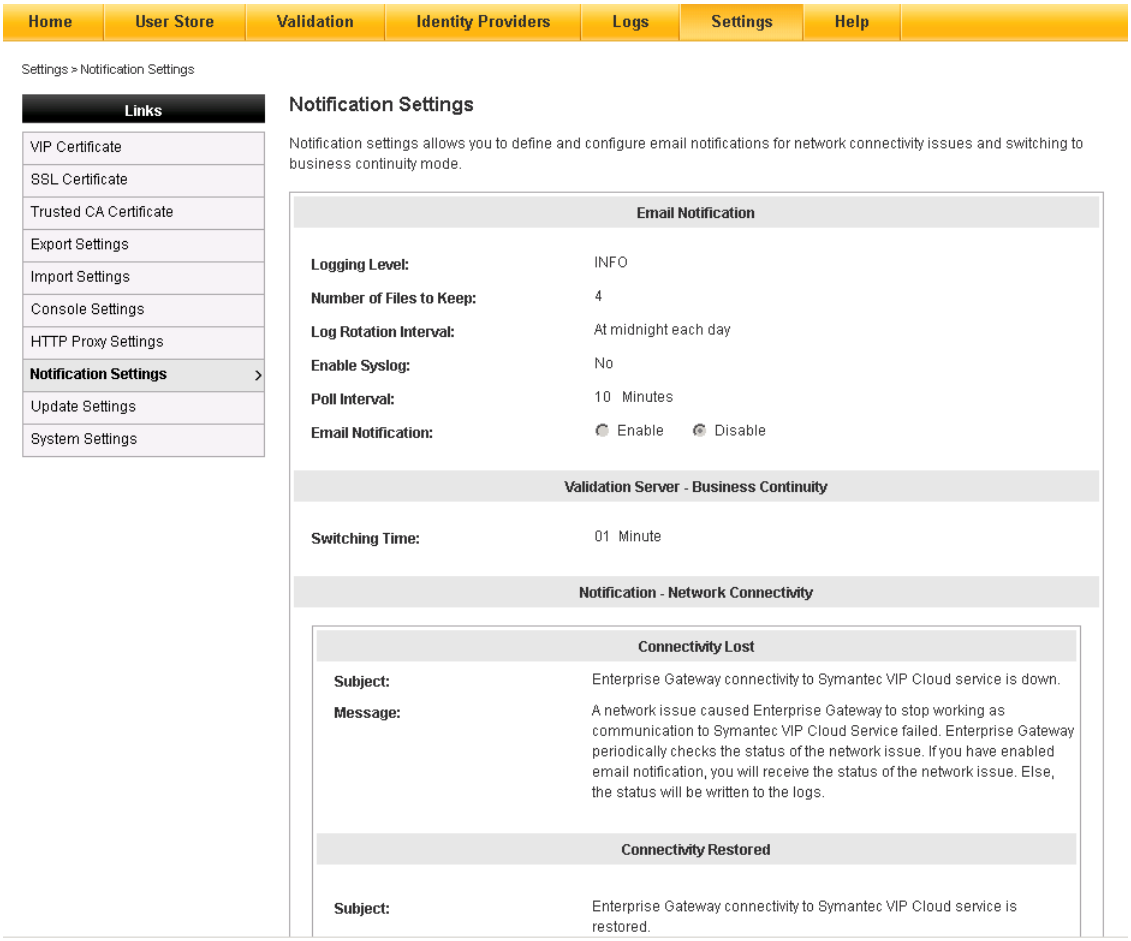

Figure 4-10 Notification Settings page

Configuring Automatic Business Continuity

In an environment that VIP protects, connectivity is crucial for the communication between the enterprise applications and VIP Authentication Service. Any disruption in this communication affects the ability to perform two-factor authentication.

The Automatic Business Continuity feature enables Validation servers to detect loss of connectivity to VIP Authentication Service and switch to the Business Continuity mode automatically. In the Business Continuity mode, Validation servers use only first factor authentication. After the connectivity is restored, Validation servers switch back to two-factor authentication without human intervention.

The following are some of the typical connectivity issues that the Business Continuity feature in the Automatic mode detects:

- Unreachable VIP User Web services host or port.
- Problems to access Enterprise HTTP proxy.
- Expired VIP certificate.

Warning: If the VIP Enterprise Gateway host is connected to the VIP User Service through an HTTP proxy server, a delay can occur in detecting the connectivity issues. This delay may affect the timely switching between the normal and the Business Continuity modes.

As an administrator, you can control this switching time in the Automatic Business Continuity configuration file (`VRSN_HOME/conf/autobc.properties`) as follows:

```
autobc.proxy.timeoutinseconds=<seconds>
```

You must restart all the Validation servers to make this change take effect.

The Business Continuity feature does not detect the connectivity issues between:

- VIP Enterprise Gateway and a User Store
- Enterprise applications such as VPN and VIP Enterprise Gateway

To enable Automatic Business Continuity for a Validation server that you configured, edit the Validation server settings and then select **Automatic** in the **Business Continuity** field.

For more information on configuring Automatic Business Continuity, refer to the online help associated with VIP Enterprise Gateway.

Chapter 5

Configuring User Stores

User Stores are the directory services that typically contain the user information that is related to authentication and authorization. LDAP is the widely used protocol to access such directories. VIP Enterprise Gateway lets you configure one or more LDAP User Stores for user authentication. You can configure User Stores of completely different types, vendors, and that are separate in their operations. For example, you can configure one LDAP directory that runs on Active Directory and the other LDAP directory that runs on Oracle Directory Server.

Until you configure a User Store, you cannot configure Self Service Portal or VIP Manager, or configure the LDAP Directory Synchronization Service. Also, you can configure Validation servers only in the User ID – Security Code and the User ID – Access PIN – Security Code validation modes.

Multiple User Stores Configured with VIP Enterprise Gateway

You can configure VIP Enterprise Gateway with multiple disparate User Stores, which can provide two-factor authentication to various enterprise services. Many organizations face complex User Store configurations when they try to address structural needs of the organization. Such needs can arise out of:

- Mergers and acquisitions of organizations
- Partnership relationship and trust across organizations.
- Limited data sharing and information access to comply with geo-political regulations

In these scenarios, you may come across users with membership in multiple User Store trees or Active Directory (AD) domains or forests. By design, VIP Enterprise Gateway provides flexibility in the User Store configurations to address complex authentication use cases.

Scenario 1:

When **Acme Corporation** acquired **TrustedBank**, both companies had two users with the same user name in their independent Active Directory domains. For example, both organizations had an employee by the name John Smith (log in ID: `john_smith`). However, they can be distinguished as `john_smith@acme.com` and `john_smith@trustedbank.acme.com`.

Similarly, enterprise applications enforce the usage of specific directory services. For example, Oracle applications need Oracle Directory Server, Novell applications need Novell eDirectory, and Microsoft applications need Active Directory to operate. In such scenario, a user may end up having multiple accounts for the same applications.

Scenario 2:

When **Acme Corporation** sets up its business applications, they decided to use best–of–breed applications from various vendors, which suit their business needs. In doing so, they ended up with an Active Directory infrastructure for all normal employee directory service's needs. But, their file server was configured on Novell Open Enterprise Server, which used Novell eDirectory as the backbone directory service.

John Smith, an employee working in **Acme Corporation**, now has two identities; one on the corporate AD forest (`john_smith@acme.com`) and the other on the corporate file server (`ACMEFILETREE\john_smith`).

While LDAP provides a flexible scheme for user searches, the search can be initiated with any of the user attributes making the user name representation complex. Even in well-defined user search environments like Windows logon many different formats for user name exists for the same user.

Scenario 3:

John Smith, an employee of **Acme Corporation** can sign in to the corporate Active Directory network as `john_smith`, `ACME\john_smith`, `acme.com\john_smith`, `john_smith@acme.com`. If the Distinguished Name (DN) based user names are permitted, John Smith can use `CN=john_smith, CN=Users, DC=acme, DC=com` as a user name.

Enterprise data protection policies of certain organizations do not permit their employee's public cloud identities and their enterprise internal identities be the same. In case of a data breech, the public cloud information of a user cannot be mapped to an enterprise user. This method helps maintain data privacy in case of data breech. In such cases, organizations can use another attribute such as employee ID as a VIP user ID that is stored in the cloud.

Scenario 4:

Acme Corporation has been convinced that Symantec VIP Services that is hosted in the Symantec cloud environment is secured. However, their internal enterprise data protection policy does not allow them to use the same user name for the cloud services and their internal systems. John Smith can sign in to the corporate AD environment as `john_smith`. In the Symantec VIP User Services, John Smith's employee ID (U32461) is registered as the user name.

Searching for Users in VIP Enterprise Gateway Configured with Multiple User Stores

VIP Enterprise Gateway searches for a user in the User Stores based on the following rules:

- To search for a user in the User Stores, VIP Enterprise Gateway follows the order in which the User Stores appear in the User Stores page. If you want to change the order of search, you can re-order the User Stores in the User Stores page.
- The user name that is provided as part of validation is replaced with the search filter that is provided in the User Store configuration. If the search query returns exactly one record, the user bind is attempted with the password provided. If no records are found or more than one user records are returned, the user search on that User Store is skipped. VIP Enterprise Gateway continues the search for the user on the next User Store.
- If the user name record contains domain information, the user name is only validated against the User Store that serves the specific domain. For example, `domain\user name` in case of Active Directory.

The following scenarios explain how VIP Enterprise Gateway searches for the users in the User Stores:

Table 5-1 Details of the scenarios

User Store Name	Domains	Users in User Store	User Search Filter
Acme Financial	acme	■ `cn=john_smith, ou=sales, dc=acme, dc=com` ■ `cn=john_smith, ou=eng, dc=acme, dc = com` ■ `cn=alice, ou=sales, dc=acme, dc=com`	`(cn=%s)`

Table 5-1 Details of the scenarios

User Store Name	Domains	Users in User Store	User Search Filter
TrustedBank	trustedbank	■ `cn=john_smith, cn=users, dc=trustedbank, dc=com` ■ `(sAMAccountName=john_smith)`	`(sAMAccountName=%s)`
XYZBank	xyzbank	■ `cn=bob, cn=users, dc=xyzbank,dc=com` ■ `(sAMAccountName=bob)`	`(sAMAccountName=%s)`

Scenario 1:

In this scenario, the user logs in as `bob`. VIP Enterprise Gateway does not find the user name match in the User Stores **Acme Financial** and **Trusted Bank**. So, the search fails in these User Stores. However, VIP Enterprise Gateway finds the user `bob` in the User Store **XYZBank**.

Scenario 2:

In this scenario, the user signs in using the user name `john_smith`. VIP Enterprise Gateway finds two instances of the user name `john_smith` in the **Acme Financial** User Store. Because the user `john_smith` is not uniquely identified, VIP Enterprise Gateway skips the **Acme Financial** User Store. Then, VIP Enterprise Gateway searches the **TrustedBank** User Store for the user `john_smith`. Because the user `john_smith` is uniquely identified in the **TrustedBank** User Store, the user `john_smith` is allowed to sign in.

Scenario 3:

In this scenario, the user signs in as `xyzbank\bob`. In this case, VIP Enterprise Gateway identifies `xyzbank` as the domain and **XYZBank** as the User Store that serves the domain. So, VIP Enterprise Gateway searches for the user `bob` only in the **XYZBank** User Store.

Adding a User Store

To configure a User Store, click the **User Store** tab in the Configuration Console. In the User Store page, click **Add New**.

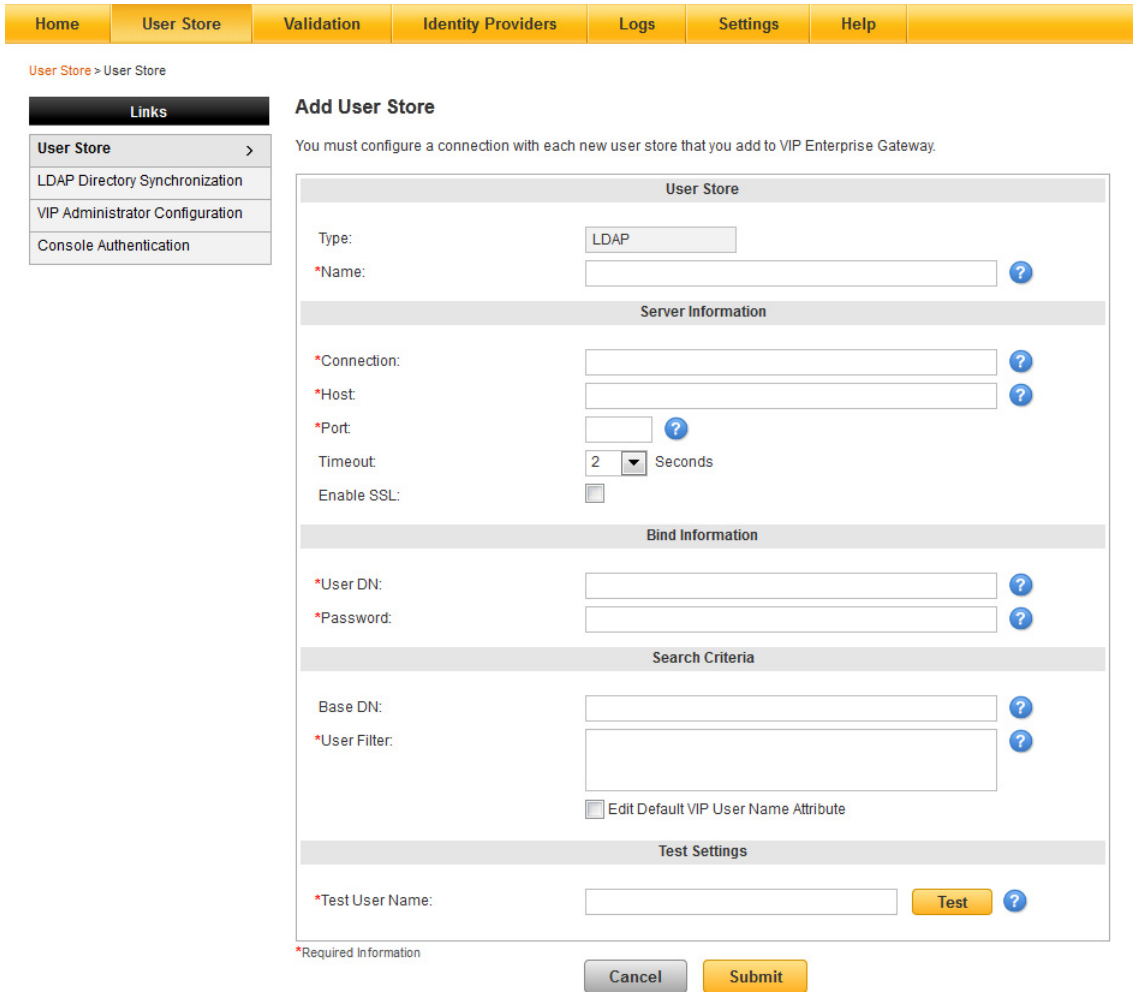

Figure 5-1 Add User Store Page

If you want to edit the LDAP attribute value that is used as VIP user name in VIP Authentication Service, select **Edit Default VIP User Name Attribute**. The LDAP attribute value that you specify in the **VIP User Name Attribute** field uses as VIP user name in VIP Authentication Service (Figure 5-2).

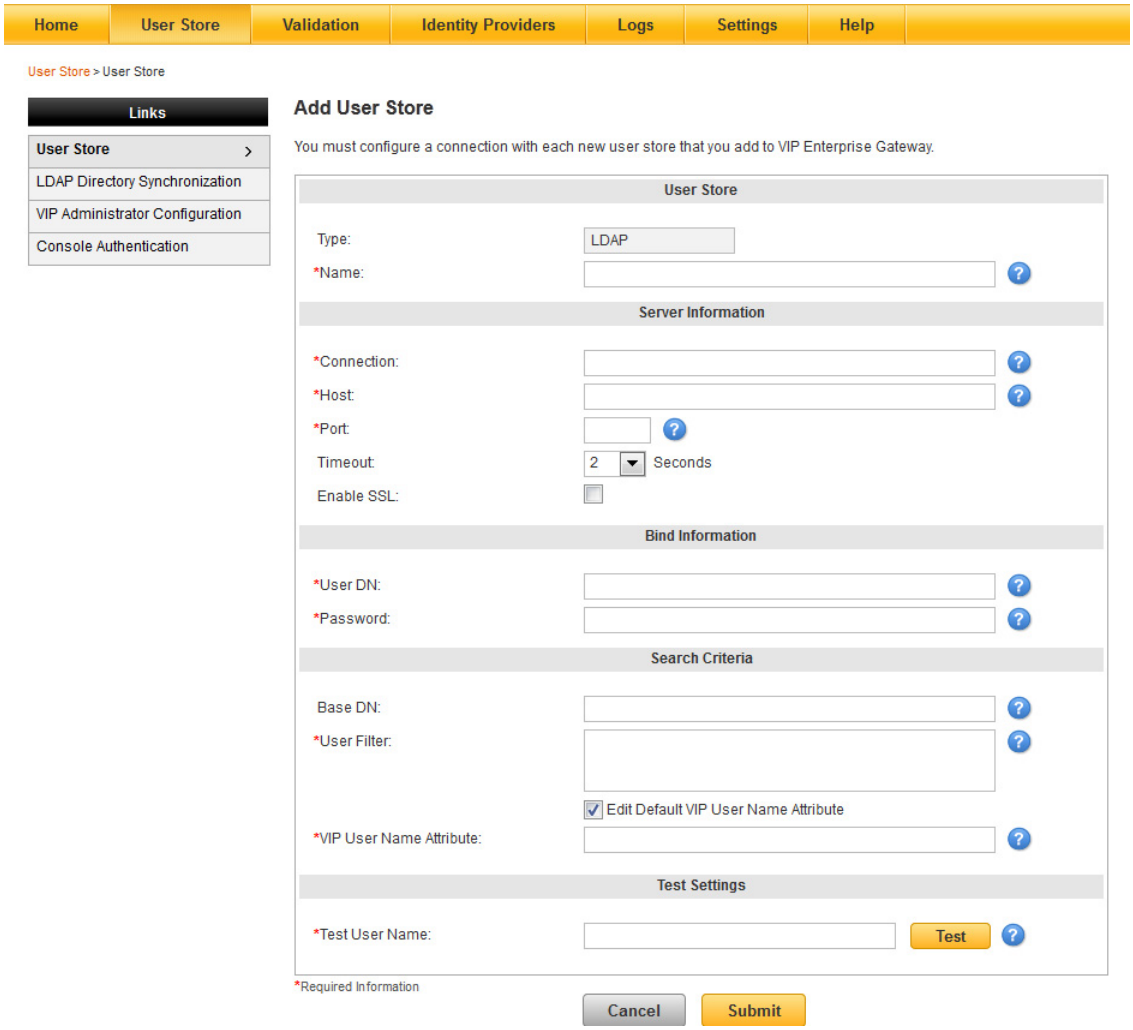

Figure 5-2 Add User Store – Edit VIP User Name Attribute

If the LDAP server is configured with SSL and if you have selected the Enable SSL option, you must ensure the following:

- Import the root and the intermediate certificates that are associated with the SSL certificate that the LDAP server uses, to VIP Enterprise Gateway Trusted CA Store.
- Adding the root and the intermediate certificates make LDAP Server connection from Configuration Console, Self Service Portal, VIP Manager, IdPs, and LDAP Sync successful.
- As the Validation Server uses Windows native LDAP client, you must add the root and the intermediate certificates to the Windows certificate store. To do this configuration, navigate to **MMC -> Add/Remove Snap-in -> Certificates** and import the root and the intermediate certificates that are associated with LDAP.
- Subject Name in the LDAP SSL certificate must have the Fully Qualified Domain Name (FQDN), including the host name of the LDAP server.
- Restart all the Validation servers after these changes have been completed.

In the versions before VIP Enterprise Gateway 9.2, the search user attribute and the user name that is created in the VIP Service are not differentiated. The VIP user name that is created in the VIP Service was the search attribute that matches the input user name parameter in the User Store configuration. However, users were able to use different user names for various applications. For example, to sign into the Windows Logon

sequence, the user, John Smith, can use various formats such as `domain\john_smith`, `john_smith@domain.com`, or `john_smith`. All these user name formats are accepted for the user John Smith.

From the version 9.2 onwards, VIP Enterprise Gateway differentiates the search user attribute from the user name that is created in the VIP Service. By default, the attribute that is used for searching the user is used to create the user in the VIP Service. However, the VIP User Name Attribute can be configured to another LDAP attributes as well.

For example, in an AD configuration you can configure the user search attribute as: `(|(sAMAccountName=%s)(uSERPrincipalName=%s))` and configure the VIP user name attribute to `sAMAccountName`. Thus, even when the user signs in as `john_smith@domain.com`, the user is logged into the VIP Service with the user name `john_smith`.

The VIP User Name Attribute can be used to address the additional use cases that result from the usage of disparate User Stores in the enterprises. Some organizations may use various applications, which limit their choice of directory services. For example, an organization with a file system on Novell Netware systems requires a Novell eDirectory server as a User Store. However, the same users are also available on Active Directory with Microsoft Exchange as the email application. John Smith, the employee in the organization using both systems with same VIP tokens, must have the same user name populated in the VIP Service database. So, the identity administrator must ensure that the VIP User Name Attribute synchronized from both the Active Directory and the Novell eDirectory has the same value. The identity administrator realized that email is unique per user in an organization and also available in both the directories. The identity administrator configures Active Directory with ‘mail’ attribute and Novell eDirectory with ‘email’ attribute as the VIP User Name Attribute.

Note: Directory attributes stated here are indicative and do not represent the exact defaults that the directory vendors state.

As VIP User Name Attribute is different from the user’s sign-in attribute, an identity administrator can configure another unique attribute to a user inside the enterprise. For example, the employee ID of the user can be used as a VIP User Name Attribute. User’s enterprise user name does not register in the VIP Service. So, the identity administrators can use this feature to keep their employee information in the VIP Service relatively anonymous.

For the procedure on adding a User Store to your VIP Enterprise Gateway server, refer to the *VIP Enterprise Gateway online help*.

Advanced User Store Configurations

In the Edit User Store page, you can do the following User Store configurations:

- Manage connections.
- Modify the search criteria.
- Configure optional attributes.
- Map users to one or more VIP User Groups available in the VIP service.
- Reset the expired Active Directory password.

Managing Connections

You can configure additional connections or LDAP server replicas with the User Store to ensure failover. You add a connection to a User Store when you configure the User Store for the first time. Later, you can navigate to the Edit User Store page to add new connections to the User Store or to edit the existing connections.

If a User Store has more than one connection associated with it, VIP Enterprise Gateway uses the first one in the list of connections by default. The remaining connections in the list act as failover servers. If the first connection server is unavailable, VIP Enterprise Gateway searches for the next connection servers to make it the active connection.

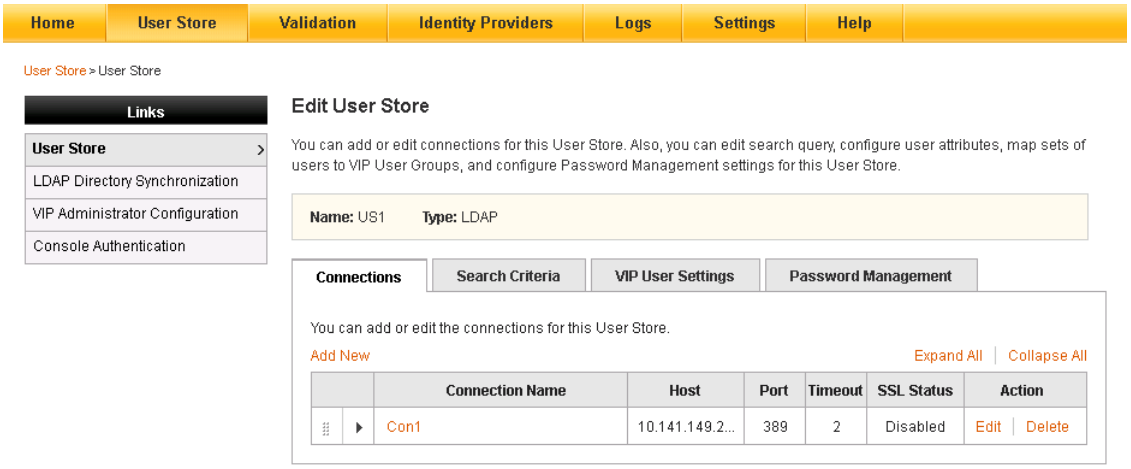

Figure 5-3 Edit Connections

Modifying Search Criteria

As part of editing the configuration of a User Store, you can modify the user search query that is configured for the User Store. The user search query that you define for a User Store applies to all the connections that are associated with the User Store.

In a multi-domain Microsoft Active Directory environment, when a user store is configured with a Global Catalog port, you can additionally configure the DNS and NetBIOS names. Therefore, users can authenticate by logging in with the domain qualified username formats used in Windows. Examples of such usernames are `colossal\john_smith` and `colossal.com\john_smith`.

In case of a Global Catalog search, you do not need to necessarily specify a domain name. That is, the Base DN name can be any value including a NULL. For more information on modifying the search criteria, refer to VIP Enterprise Gateway online help.

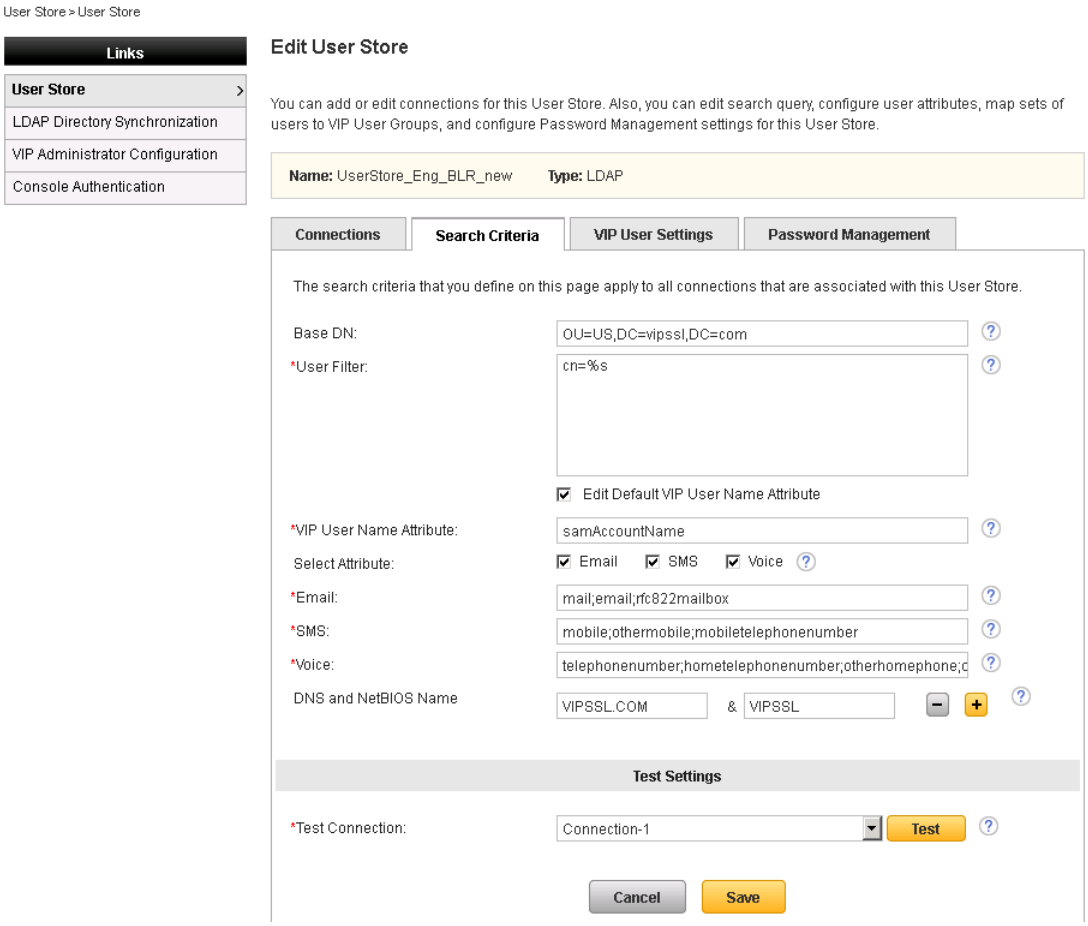

Figure 5-4 Edit Search Criteria

Configuring Optional Attributes

VIP User Attributes that you configure in the Edit User Store page help administrators search and identify the users in VIP Manager. You can configure the following VIP User Attributes:

- First Name
- Last Name
- Email Address
- Employee ID
- Department

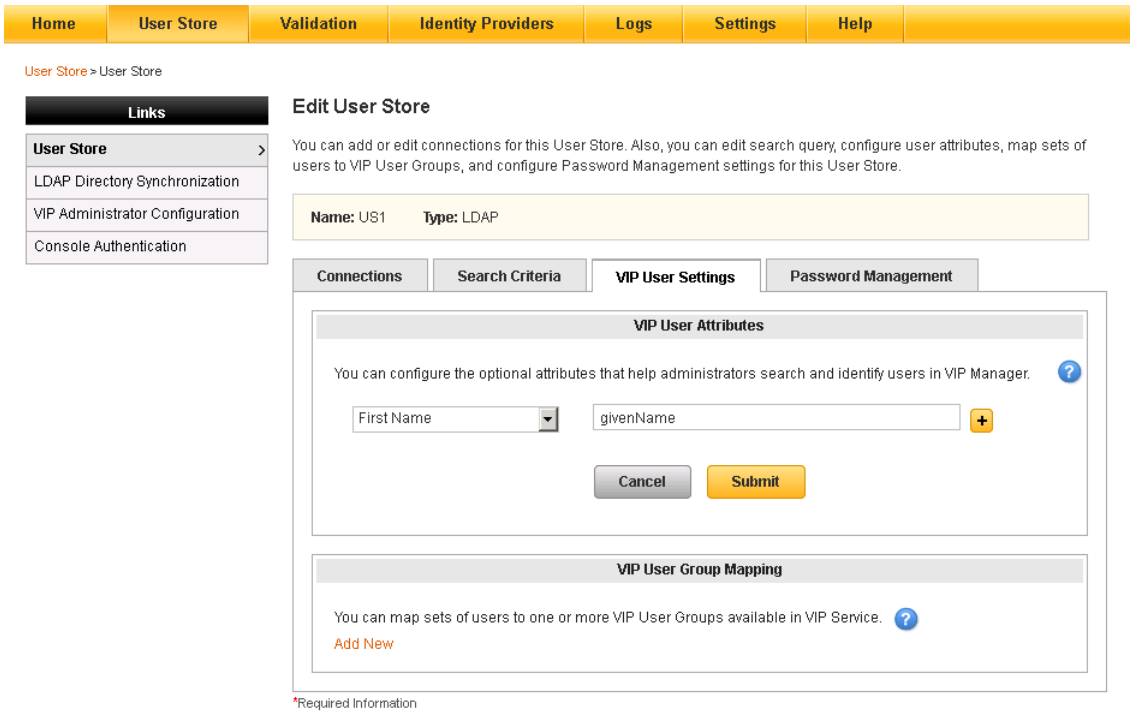

Figure 5-5 Optional attributes

Using User Groups and Administrator Groups in VIP Enterprise Gateway

An organization can configure multiple user groups for easier security policy management. Also, the organization can create groups of administrators and provide selective rights to them rather than assigning all administrators with the same level of privileges. The user groups and the administrator groups can be configured in VIP Manager. For detailed information on setting up User Group, refer to the *VIP Enterprise Gateway Online Help*.

Manually updating the user groups and the administrator groups for user and administrator memberships in VIP Manager is a cumbersome task. VIP Enterprise Gateway enables you to map users in LDAP/AD User Stores to one or more user groups or administrator groups in the VIP Service. These mappings occur based on the following:

- Distinguished Name.
- Membership of the users in LDAP/AD groups.
- Value of one of the attributes of LDAP user object.

LDAP Synchronization service can query the LDAP User Store to add, delete, and update the user and the administrator records for group membership. Then, the LDAP Synchronization service synchronizes the information to the VIP Services.

For detailed information on VIP User Group Mapping and VIP Administrator Group Mapping, refer to the *VIP Enterprise Gateway online help*.

Mapping Users to VIP User Groups

For the procedure on mapping users to VIP User Groups, refer to *VIP Enterprise Gateway online help*.

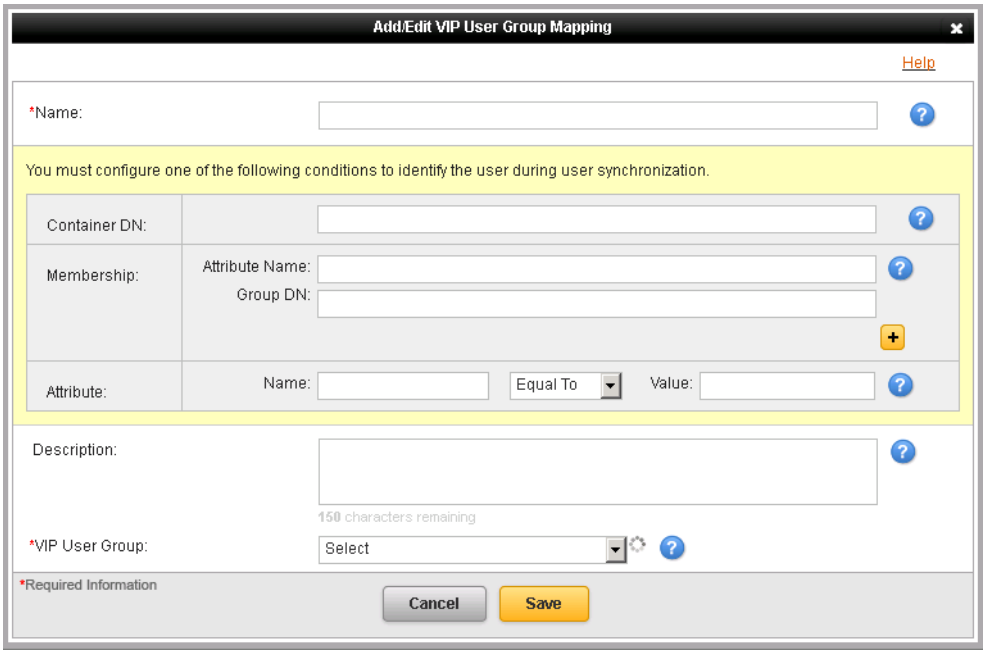

Figure 5-6 VIP User Group Mapping

Resetting the Expired Active Directory Password

VIP Enterprise Gateway enables the administrators to configure the Password Management feature that enables users to reset their expired Active Directory password. You can enable the Password Management feature only if Active Directory is configured as User Store with VIP Enterprise Gateway. VIP Enterprise Gateway uses the Active Directory password for the first-factor authentication of the user. The Password Management feature enables the administrators to configure the labels for the fields that are displayed to the users to reset their Active Directory password.

For detailed information on resetting the expired Active Directory password, refer to the *VIP Enterprise Gateway online help*.

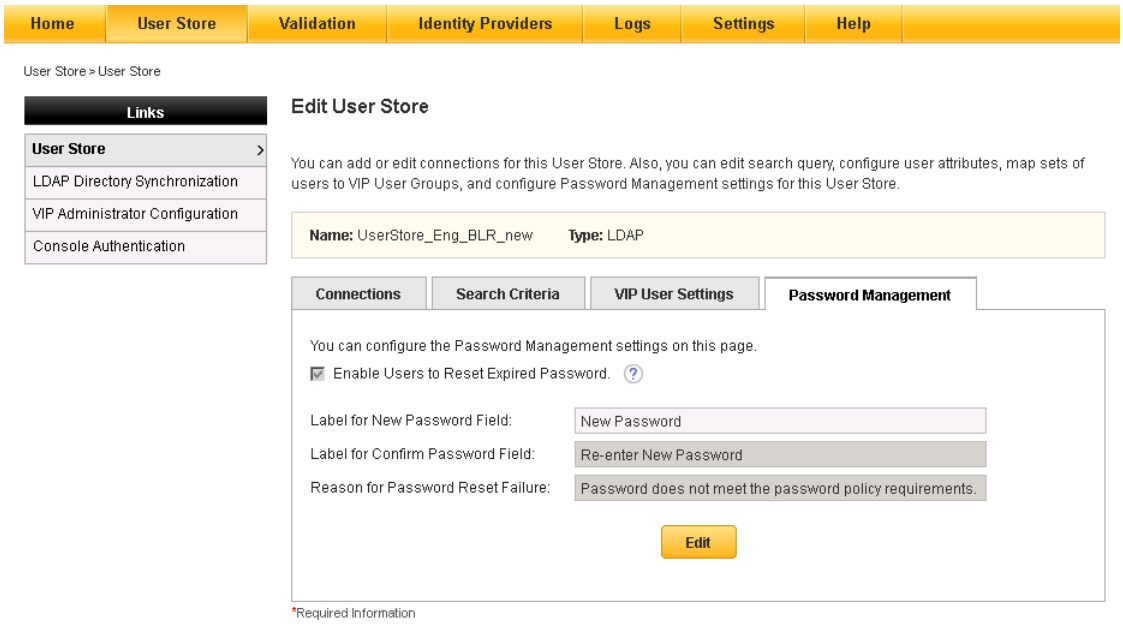

Figure 5-7 Password Management

Chapter 6

Configuring Validation Services

The VIP Enterprise Gateway Validation server is a RADIUS-based authentication service for interfacing with the enterprise network infrastructure. VIP Enterprise Gateway uses RADIUS Password Authentication Protocol (PAP) as the authentication protocol.

The VIP Enterprise Gateway Validation server supports Request for Comments (RFC) 2865.

The VIP Enterprise Gateway Validation server supports popular vendors such as Microsoft, Cisco, Juniper, Citrix, to name a few. For the list of available integrations and their supported modes, refer to https://knowledge.symantec.com/support/ua-support/index?page=content&id=AR3816

Prerequisites

Before you install VIP Enterprise Gateway, you need to consider the following about the Validation Service:

- The Validation Service connects to the VIP Authentication Service through the Internet over outbound port 443. You must open your firewall or prepare a proxy server accordingly.

  See "Default Ports and Protocols" on page 101

- Your client applications (such as a VPN Gateway) must be able to access the Validation Service over UDP. If not, you need to open a UDP or a TCP port through your firewall. If opening a TCP port, you also need to configure a tunnel forwarder and receiver using Configuration Console.
- Decide the application you need to use. For example, for VPN gateway, PAM, and Outlook Web Access, you can use the appropriate validation mode that the application supports.

  For the list of available third party applications and configuration instructions, refer to the Integration Guides on VIP Manager.

If you want to implement multiple applications that require different validation modes, you need to configure separate Validation servers for each.

Support for Out-of-Band Authentication

VIP Enterprise Gateway validation supports Out-of-Band authentication (OOB) across different channels such as VIP Access Push, SMS, and Voice across all authentication modes. The selection of OOB channel would be based on the credential type of the user assigned in VIP Manager. Administrators can also configure to use user's Mobile, Phone, or Email values as OOB channel from their Enterprise Directory.

Out-of-band (OOB) authentication channels like Push, SMS, or Voice credentials is supported across all the modes.

The following explains the typical authentication flow:

1. The user enters the user name and the LDAP password for the Validation server to validate.
2. On successful validation of first-factor, the user is sent an OOB push, security code over SMS/Voice.
3. If the user has a push enabled Mobile Credential, then the push is sent to the user and he has to approve the request.
4. If the user has a phone without a push credential, a SMS/Voice is sent to the phone, and user is also presented a challenge with a form field to enter the security code.

5 The user enters the security code in the form field, which the Validation server validates.

6 On successful validation, the user is provided access to the resource.

The Validation server has the following characteristics:

- At least one User Store must be configured in VIP Enterprise Gateway to use the Validation server to support Out-of-Band authentication (OOB)
- In the Business Continuity mode, though the user is challenged to enter a security code, the Access-Accept is granted without validating the security code with the VIP Service.
- Some applications may not support RADIUS Access-Challenge. You must ensure that the application that you integrate with the Validation server configured with Challenge is capable of supporting RADIUS Access-Challenge messages.

The OOB sequence is triggered in the following order.

1 The push is triggered, if the user has a push enabled Mobile credential.

2 The SMS/Voice is triggered, if the user does not have a push enabled Mobile Credential.

Authentication Modes

VIP Enterprise Gateway supports the following validation modes with various vendor and application configuration.

- "User ID - Security Code" on page 40
- "User ID - Access PIN - Security Code" on page 41
- "User ID - LDAP Password - Security Code" on page 41

User ID - Security Code

The third party application integrations validates the first-factor authentication and User ID - Security Code validates the second-factor authentication.

Typically, the User Interface of the application provides a separate field to enter the second-factor validation code. The following are some of the scenarios where you can use this validation mode:

- Many enterprise applications implement stacked authentication schemes. In such schemes, the authentication that is validated with one authentication provider is passed on to the next authentication scheme for additional factor validation.
- Many applications have integrated a primary authentication scheme to their session management. For example, many Microsoft applications provide session access only after a successful Active Directory validation.
- The enterprise application may not be authenticating to an LDAP server, so you cannot configure any other validation mode that VIP Enterprise Gateway supports. In such cases, the security code validation must be carried out independent of the first factor authentication.

However, this kind of authentication requires the following:

- An understanding of the application authentication stack.
- An understanding of how the user name and the security code fields are extracted and passed on to the Validation server.

Note: If this mode of integration is supported in VIP third party application integration plug-ins, the plug-in typically takes care of the extraction of the user name and the security code from the original RADIUS authentication request.

The following are the characteristics of the Validation server that is configured in the User ID – Security Code mode:

- This Validation server must be used for the second factor authentication only. The application must carry out the first-factor authentication separately.

- During the Business Continuity mode, this Validation server accepts any security code without validating it. If the Business Continuity mode is used in isolation, it can lead to a significant security compromise.
- This Validation server can be used without configuring a User Store. However, when you authenticate to an LDAP system for first factor authentication, you may use a different authentication user name than the one registered with VIP. For example, Microsoft applications. In such cases, you may use the **Use LDAP User Name for VIP Authentication Service Validation** option, which mandates the configuration of at least one LDAP User Store.
- If the Validation server is configured with VIP Access Push, the third-party applications must use **push** as the keyword instead of a security code to initiate a Push request.

User ID - Access PIN - Security Code

This validation mode is similar to the User ID - LDAP Password - Security Code mode used with the following remote access scenarios:

- Organization wants to implement another first-factor credential for VPN than the LDAP/AD password.
- Some of the users of the organization's services may not have an entry in the organization's LDAP.

In this validation mode, the concatenated Access PIN and the security code are sent to the VIP Enterprise Gateway server. The VIP Enterprise Gateway server forwards the Access PIN and the security code to the VIP Service for validation. On a successful validation in the VIP Service, the user is provided access to the resources.

- This Validation server can be configured without configuring an LDAP User Store with VIP Enterprise Gateway.
- The user cannot be authenticated using an enterprise LDAP user name.
- The Business Continuity mode is not supported for this Validation server.

User ID - LDAP Password - Security Code

Typically you use this mode where first-factor password and second-factor security code are entered in the same field because of the interface restrictions. Also, this configuration is an example where the application allows only one RADIUS authentication server to be configured without any stacked authentication. On receiving the RADIUS request, the Validation server separates the LDAP password and the security code. It validates the LDAP password with the User Store and the security code with VIP Authentication Service. A User Store must be configured for this kind of integration. Most organizations with VPNs use this mode of authentication.

Note: If you have configured User Name - LDAP Password - Security Code (ULO) validation server, and if you enter wrong credentials, your LDAP account will be locked based on the configuration in AD password lockout policy.

To prevent an AD user from getting locked out with first-factor along with a wrong security code, make sure to enable user lockout policy in VIP Manager. Also, ensure AD password lockout count to be higher than the user lockout count in VIP Manager. This will lock the user in VIP Manager and prevents AD user from getting locked out from the enterprise.

User ID – LDAP Password – Security Code (RADIUS Access Challenge Mode)

This mode is now deprecated and displayed as User Name - LDAP Password - Security Code in the Validation Server configuration page.

Validation Servers configured in User Name - LDAP Password - Security Code (RADIUS Access Challenge Mode) in the previous releases, will be automatically migrated to User Name - LDAP Password - Security Code. The Validation Server functionality remains the same and will continue to function normally.

Authenticating Users Using VIP Access Push

VIP Enterprise Gateway supports authentication using VIP Access Push verification. When users sign in to your enterprise using their first-factor authentication, the VIP Service sends a VIP Access Push verification message to their registered mobile devices. The users can tap the **Allow** button on the verification message to perform second-factor authentication and complete their sign in. This ensures enhanced usability for users to perform second-factor authentication.

If the user has multiple registered mobile devices, the VIP Service sends the push verification message to all these devices. However, the user only needs to approve a push verification once.

VIP Access Push is an alternative for security code. Users can always use a security code for second-factor authentication if VIP Access Push is unavailable.

If Business Continuity is ON, then the push notification will not be sent to any device and the user is challenged to enter security code. The user is challenged only if they enter user name and password. Users with security code enabled is not challenged. For more information on configuring your application with Access Challenge Mode, refer to the appropriate VIP third-party integration guides.

Push feature is supported across all the authentication modes.

The following figure illustrates how a user accesses the account using VIP Access Push.

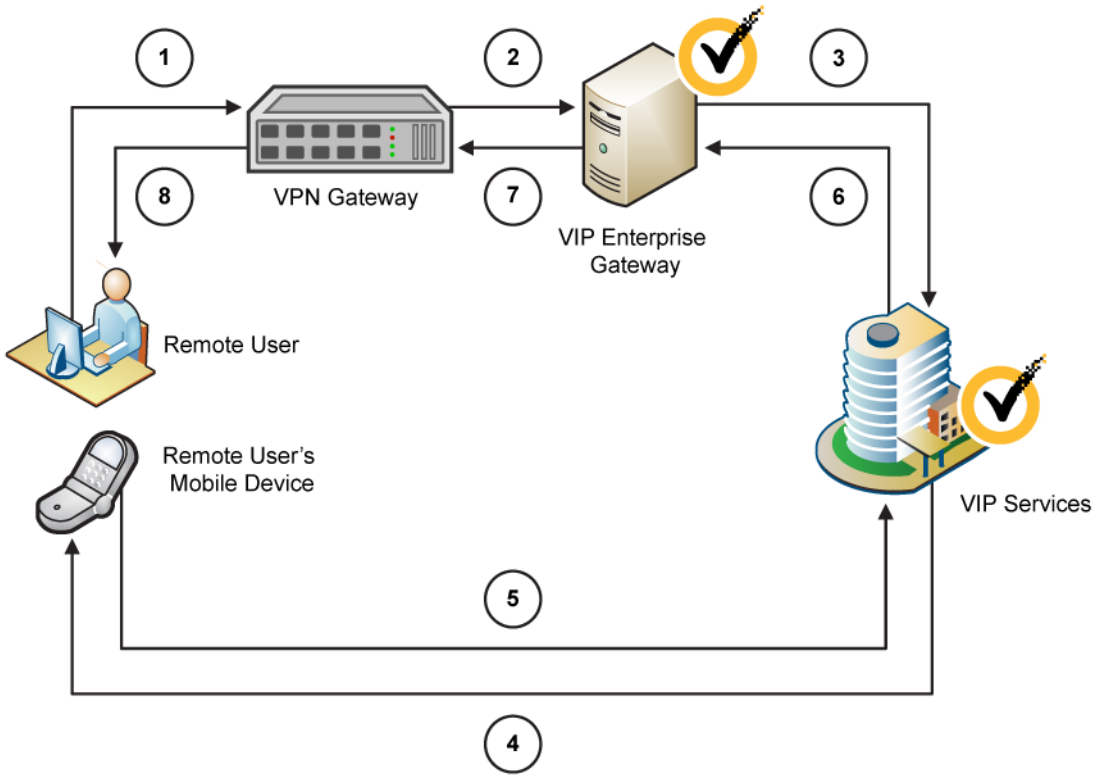

Figure 6-1 VIP Access Push flow

As an administrator, you can configure VIP Access Push authentication on a VIP Enterprise Gateway Validation server that is configured in the User Name - Security Code mode or the User Name - LDAP Password - Security Code mode.

1 The user enters the user name and password to sign-in to the application.

2 The VPN gateway forwards the user name and password to VIP Enterprise Gateway using the RADIUS protocol.

3 VIP Enterprise Gateway communicates with the VIP Service to authenticate the user using VIP Access Push. In case of the User Name - LDAP Password - Security Code mode, the VIP Enterprise Gateway also authenticates the user name and the password against the User Store configured with it.

4 The VIP Service sends a push verification message to the VIP Access client on the user's registered mobile device.

5 The user approves the push verification.

6 The VIP service confirms the second-factor authentication by the user to VIP Enterprise Gateway.

7 VIP Enterprise Gateway sends the Access Accept Authentication response to the VPN gateway or the VIP Plug-in.

8 The VPN gateway or the VIP Plug-in allows the user to sign-in to the enterprise.

You can configure the following in VIP Enterprise Gateway:

- Maximum time that is allowed to complete the second-factor authentication. This value must be between 30 and 300 seconds.
- Name or URL for the remote access service (such as the web server, application server, VPN, or similar) where you want to use VIP Access Push to authenticate your users.

The default value for the VIP Access Push timeout is 60 seconds.

The remote access service such as a VPN can attempt to authenticate with VIP Enterprise Gateway multiple times within the specified VIP Access Push timeout. That is, the VPN timeout multiplied by the VPN attempts made to the VIP Enterprise Gateway must be equal to the specified VIP Access Push timeout.

*VPN timeout * Number of VPN attempts made to authenticate with VIP EG = VIP Access Push timeout*

For example, consider the VIP Access Push timeout is set to 60 seconds and the VPN timeout is set to 15 seconds. In this case, the VPN can attempt to authenticate with the VIP EG four times before the VIP Access Push timeout is elapsed.

*15 * 4 (first attempt + three retries) = 60*

If you have configured User Name - LDAP Password - Security Code (ULO) validation server with push, and if you enter wrong credentials, your LDAP account will be locked based on the configuration in AD password lockout policy.

If the user receives a push notification on their device and if they deny or no action is performed for five push requests, their push service will be locked for one hour to minimize repeated notifications to the user. User can still be authenticated using the LDAP Password and Security Code.

Note: The PUSH feature is supported only for Android and iOS devices.

SMS/Voice workflow is similar to the VIP Access Push flow.

Adding a Validation Server

You add Validation servers from the Add RADIUS Validation Server page. To access this page, click the **Add Server** button under the Validation tab.

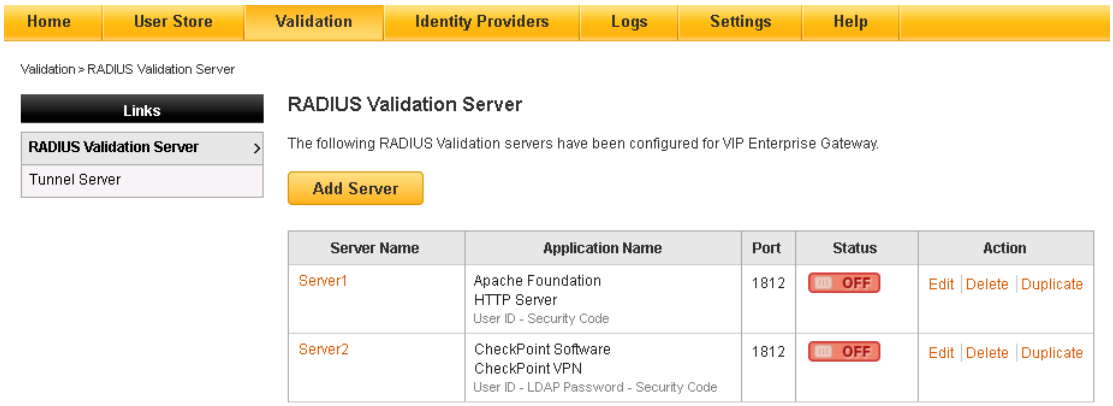

Figure 6-2 RADIUS Validation Server

You can choose one of the following options to create a Validation Server:

- **Application configuration** – Administrators can select a pre-defined configuration template for the available applications from the Validation server page. The vendors, application details, and supported authentication modes are pre-defined. Symantec recommends to use this method to configure your Validation server.
- **Custom configuration** – If your vendor or application is not available in the pre-defined list, then you can use this mode and customize your two-factor authentication configuration.

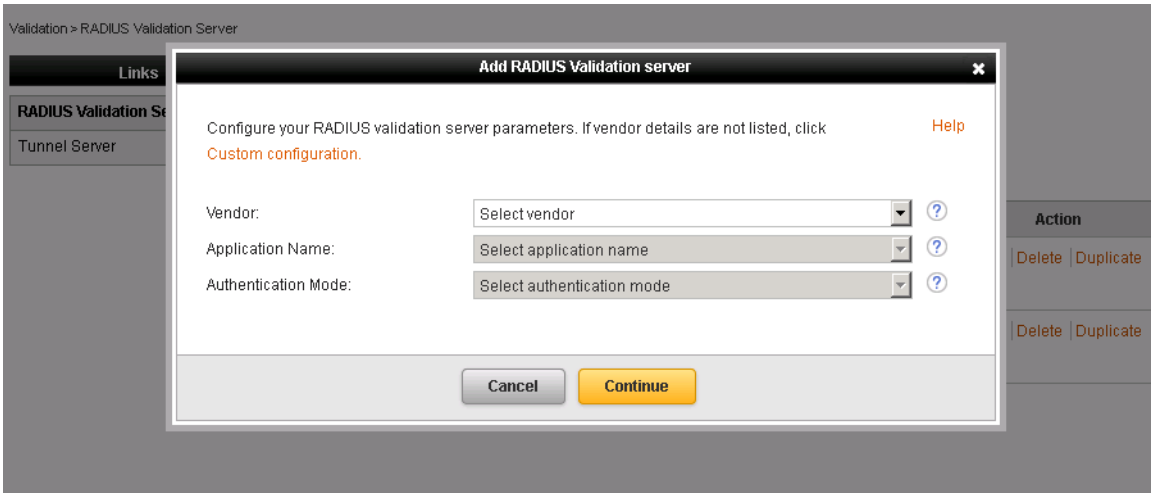

Figure 6-3 Add RADIUS Validation Server

To create a Validation Server using Application Server settings:

1 Click **Add Server**. The Add RADIUS Validation Server page is displayed.

2 Do the following:

- Select the Vendor details from the drop-down.
- Select the Application Name. The applications are listed based on the selected vendor.
- Select the Authentication Mode. The authentication mode listed are displayed based on the applications that you selected.

3 Click **Continue**.

If you want to enable additional configuration, complete Task 1 to Task 6 to create your Application server.

To create an Application Server using custom configuration settings:

1 Click **Custom configuration** from the Add RADIUS Validation Server page.

2 Complete Task 1 to Task 6 to configure an Application server based on your organization's requirement.

Task 1. Configure the Application Server with basic settings

1 Enter values for the server name, IP address, and port number.

2 Enter the format in which the password is encoded. The validation service will use the same format to decode the client password information.

- On Windows, you can select UTF-8 or Default as the password encoding formats. Default represents the default platform encoding value.
- On Linux, you can select UTF-8 or any other value that iconv-l function returns. To support the Extended ASCII characters as part of the password on a Linux platform, you must modify the radserv.conf file located in the install directory. For more information, refer to "Changing the Password Encoding Format on Linux Platform" on page 48".

3 Click **Submit**. The Application Server is created with basic settings.

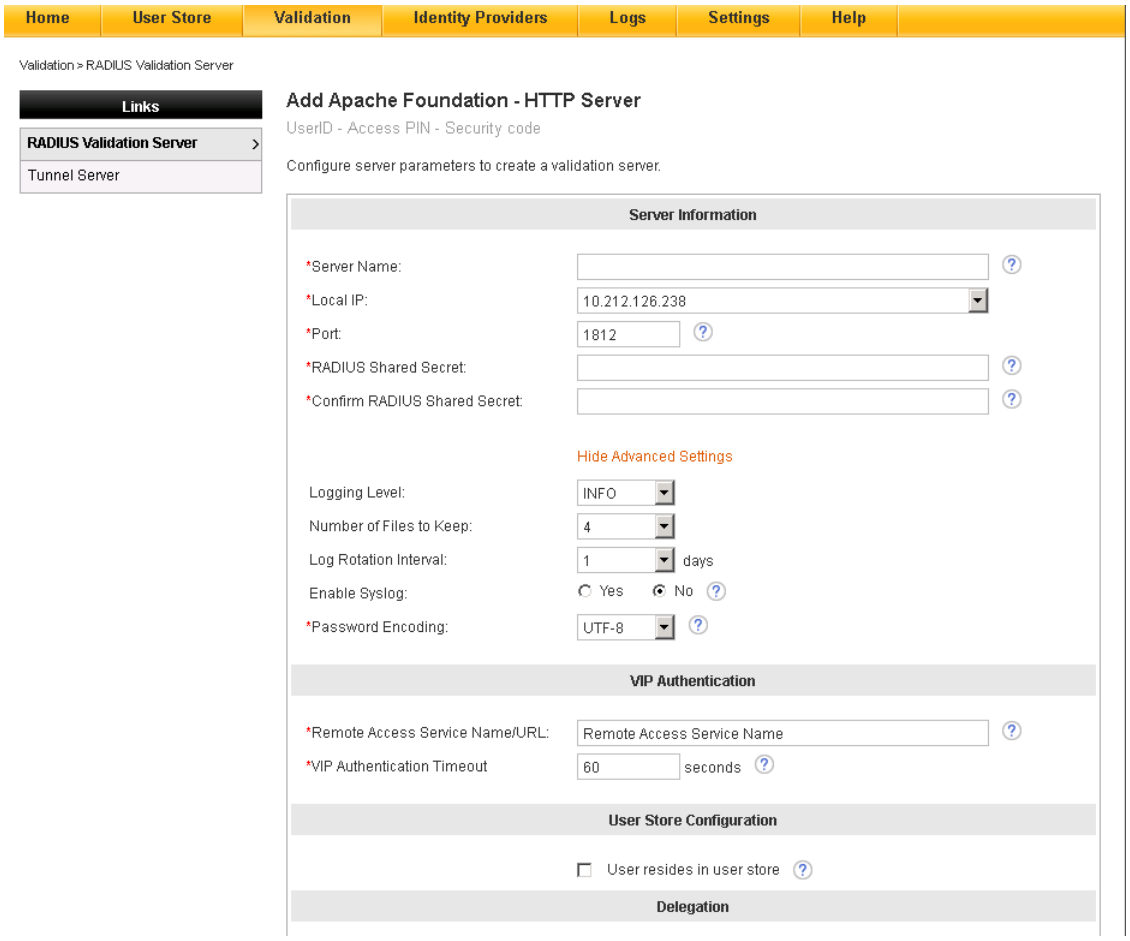

Figure 6-4 Application Server settings

Task 2. Configure the Validation Server with advanced settings

1. Enter values for logging level, number of files to keep, log rotation interval, enable syslog, and password encoding.
2. Enter remote access service name/url. The name you enter here will display to users in VIP Access Push notification that they receive on their mobile device.
3. Enter a VIP authentication timeout.
4. Select **User resides in user store** check box and select the user that you configured from the User Store drop-down.

Task 3. Enable Business Continuity

1. Enable Business Continuity on the Validation servers.
2. Select one of the following options:
   - Automatic – To enable the Business Continuity automatically.
   - Enabled – To enable the Business Continuity manually.
   - Disabled – To disable Business Continuity.

In the Business Continuity mode, Validation servers use only first factor authentication. This mode enables the Validation servers to authenticate the users in the absence of the communication between the enterprise applications and VIP Authentication Service. For more information to configure Business Continuity, refer

"Configuring Automatic Business Continuity" on page 25.

Note: Business Continuity is not supported for the User ID - Access PIN - Security Code validation mode. You must ensure that the users that need to be delegated are not part of the User Stores that you configured in VIP Enterprise Gateway if: you use User ID – Security Code or User ID – LDAP Password – Security Code validation modes, configure delegation server with Business Continuity, enable Automatic Business Continuity. Alternatively, you can configure the users to be delegated in a different group and exclude this group in the VIP Enterprise Gateway User Store search filter.

Task 4. Setting the Delegation server (if you choose to use one)

1 Select Enable Delegation check box.

2 Enter values for retries and timeout.

3 Enter IP address, port number, host name, and RADIUS Shared Secret.

Task 5. LDAP to RADIUS mapping

1 Select **Configure LDAP to RADIUS mapping** check box.

2 Enter values for RADIUS mapping attribute and data type.

3 Click **Add New**. Enter the required data to complete LDAP to RADIUS mapping.

If you use a VPN device (for example, a Cisco ASA 5500 series), and configured an LDAP User Store, you can configure LDAP to RADIUS mapping to add VPN group information for users in the authentication RADIUS response. For example, if you typically authenticate a user with the user name and password combination, you can use this option to include the user's group associations being returned in the authentication response from LDAP.

4 Click **Submit**. The RADIUS Validation page displays the Application servers that are added. To change the parameters, click the server name, and edit the settings.

Task 6. Start the Application Server

After completing the configuration of an Application server, you can also start or stop the Application server, copy the Application server settings, or delete it, by clicking the appropriate link in the **Actions** column.

Duplicating the Application Server Settings

Use the Duplicate Application server settings feature if you want to add a Application server that has a similar configuration of an existing server in VIP Enterprise Gateway.

This feature retains the values of the parameters that can be common between the servers, and provides a dialog box to enter the differential values such as port number, shared secret key, and so on.

Complete the following procedure to copy the Application Server settings of an existing configuration:

1 In the Configuration Console, click the **Validation** tab.

2 On the RADIUS Validation Server page, identify the Application server that you want to copy the settings from. In the Actions column, click **Duplicate**.

3 In the Duplicate Settings popup, enter the Name, Port Number, and the Radius Shared Secret of the new Application Server (refer to Figure 6-5).

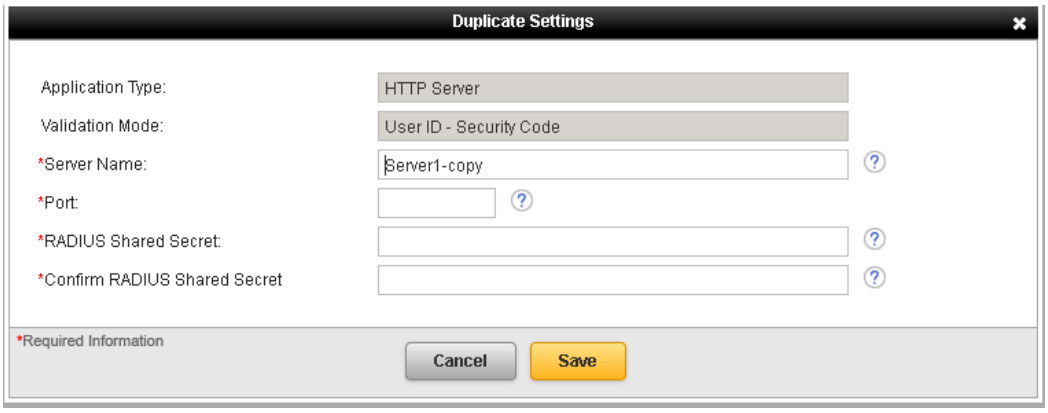

Figure 6-5 Duplicate Validation Server Settings

4 Click **Save** to save the changes.

Changing the Password Encoding Format on Linux Platform

The default password encoding format is UTF-8. However, if the LDAP password contains Extended ASCII characters such as Ñ, ñ, you need to modify the password encoding field in the `radserv.conf` file located in the install directory.

Perform the following steps to modify the `radserv.conf` file:

1 Stop the Validation server.

2 Delete `radserv.conf.working` file located in the `<INSTALL_DIR>/Validation/servers/<server_name>/conf` folder.

3 Open the `radserv.conf` and change server.encoding to **ISO-8859-1** and save the file.

4 Start the Validation server.

The ISO-8859-1 encoding format is listed as another option in the Password Encoding drop-down, and you can select it if the LDAP password contains Extended ASCII characters.

Adding Custom RADIUS Attributes for the LDAP to RADIUS Mapping

Complete the following procedure to add the custom attributes for the LDAP to RADIUS mapping:

1 Stop the Validation servers.

2 Add the RADIUS attribute to the `<INSTALL_DIR>\conf\radius-attributes.conf` file (for example, Framed-Pool, 88, string, 0).

3 Select the newly added attribute in the **RADIUS Mapping Attribute** drop-down.

4 Select the appropriate LDAP attribute.

5 Select the **Test** button to make sure that the RADIUS to LDAP mapping returns the proper result.

6 Start Validation servers.

Tunnel Forwarders and Receivers

Tunnels carry UDP messages over a TCP connection. A tunnel forwarder accepts UDP requests to send data over a TCP connection to a tunnel receiver. A tunnel receiver receives TCP data from a tunnel forwarder and sends it over UDP to the Validation server for processing. Then, the tunnel receiver sends the Validation server response back to the tunnel forwarder over TCP. Tunnels are optional, advanced configurations.

UDP is a connectionless protocol. So, the reliability of packet delivery is not guaranteed. You can use UDP tunneling over TCP as an alternate to support the following scenarios:

- Enterprise network does not have a network reliability issue.
- UDP packets are generally not accepted in the network.

You can set up a tunnel forwarder (and at least one associated tunnel receiver) to send and verify validation requests. You set up a tunnel forwarder to forward validation requests from outside your network firewall to your Validation Service. For example, if your VPN gateway resides in your DMZ, you can set up a tunnel forwarder in the DMZ to send validation requests to a tunnel receiver inside your firewall. Configure the tunnel receiver to forward validation requests to your Validation Service.

You add tunnel forwarders and receivers from the Add Tunnel page. Access this page by clicking the **Add Tunnel** button from the **Validation** tab. You need to choose whether to add a tunnel forwarder or tunnel receiver.

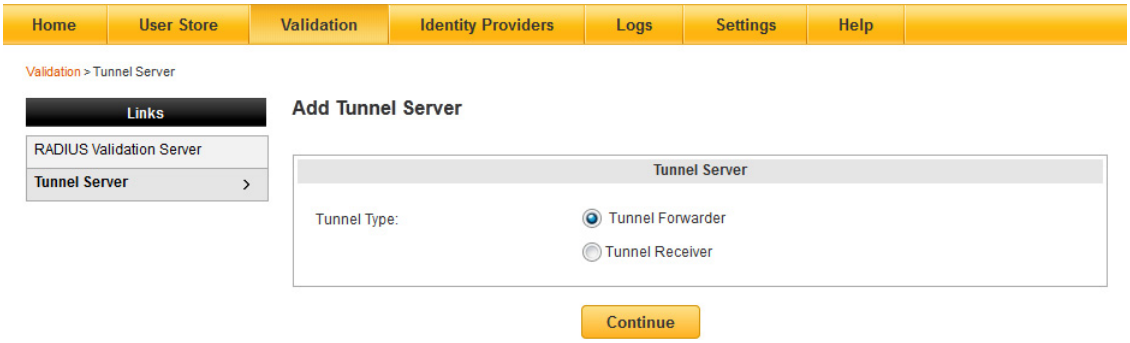

Figure 6-6 Add Tunnel Server

Note: A VIP certificate is not required to add a tunnel forwarder or tunnel receiver.

Tunnel Forwarders

You can configure a tunnel forwarder to connect in one of two ways:

- **Tunnel Forwarder** (direct connection). Configure a tunnel forwarder to route validation requests directly from a VPN gateway in your DMZ to a tunnel receiver inside your firewall.
- **Tunnel through a proxy web server**. Add a proxy web server between the tunnel forwarder and tunnel receiver. VIP Enterprise Gateway only supports proxy servers using Anonymous or Basic Authentication.

When you set up and use a tunnel forwarder with your configuration, you must ensure the following:

- Set up a tunnel receiver that is associated with the tunnel forwarder.
- The parameters you set for your tunnel receiver must match the parameters you enter on the Add Tunnel Receiver page.

When a tunnel receiver accepts TCP data from a tunnel forwarder, it completes the transmission by sending the data over UDP to the Validation server. When it gets the server's response, the receiver initiates another TCP transmission, and sends the Validation server response back to the tunnel forwarder, again over TCP.

After you add a new tunnel forwarder, it shows in the Validation page. To change parameters, click the tunnel name. You can also start or stop the tunnel, or delete it by clicking the appropriate link in the **Actions** column.

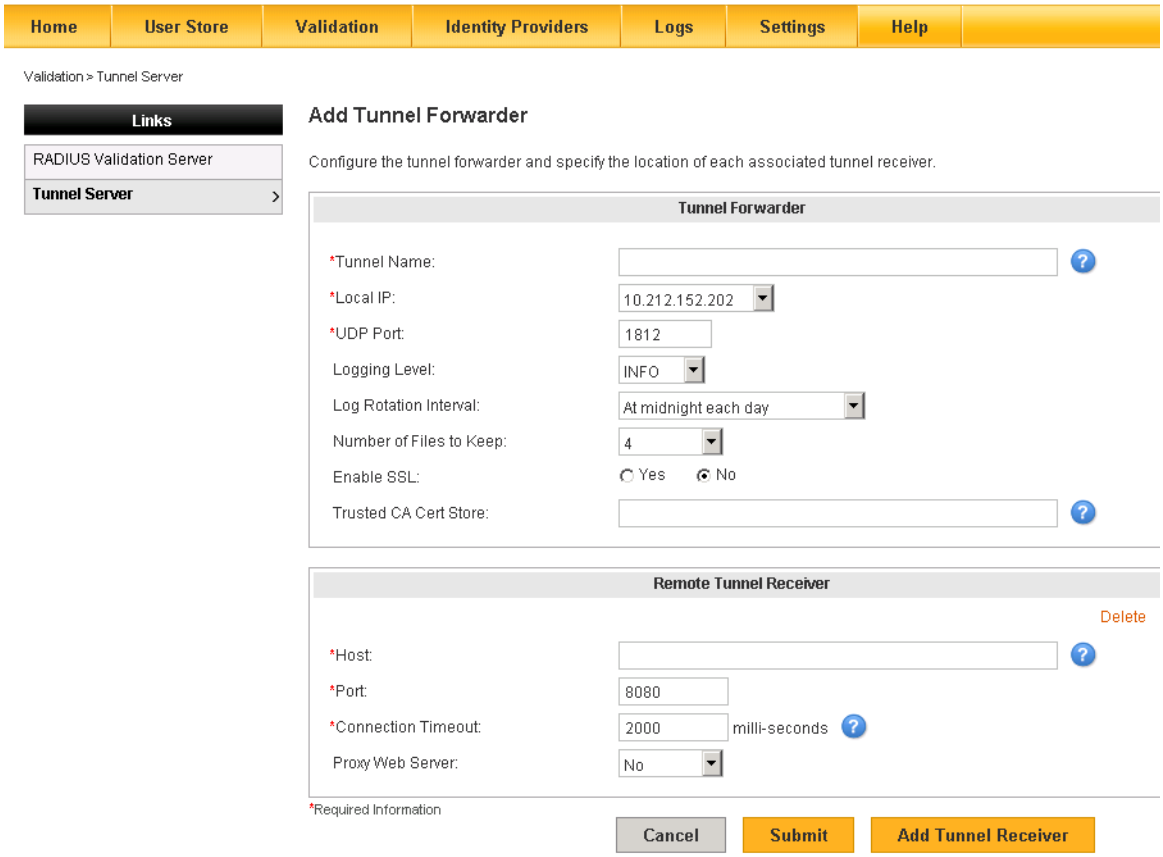

Figure 6-7 Add Tunnel Forwarder

Tunnel Receivers

When a tunnel receiver accepts TCP data from a tunnel forwarder, it completes the transmission by sending the data over UDP to the Validation server. When it gets the server's response, the receiver initiates another TCP transmission, and sends the Validation server response back to the tunnel forwarder, again over TCP.

If you set up a tunnel forwarder, you must configure at least one tunnel receiver for that forwarder.

Note: You can configure multiple receivers for a single forwarder (for example, for failover). However, each forwarder must have at least one distinct receiver.

You cannot start a tunnel receiver if you have a pending SSL certificate in your keystore. After you install or remove the pending certificate, you can start the tunnel receiver.

See "Configuring Console Settings" on page 23.

After you add a new tunnel receiver, it shows in the Validation page. To change parameters, click the tunnel name. You can also start or stop the tunnel, or delete it by clicking the appropriate link in the **Actions** column.

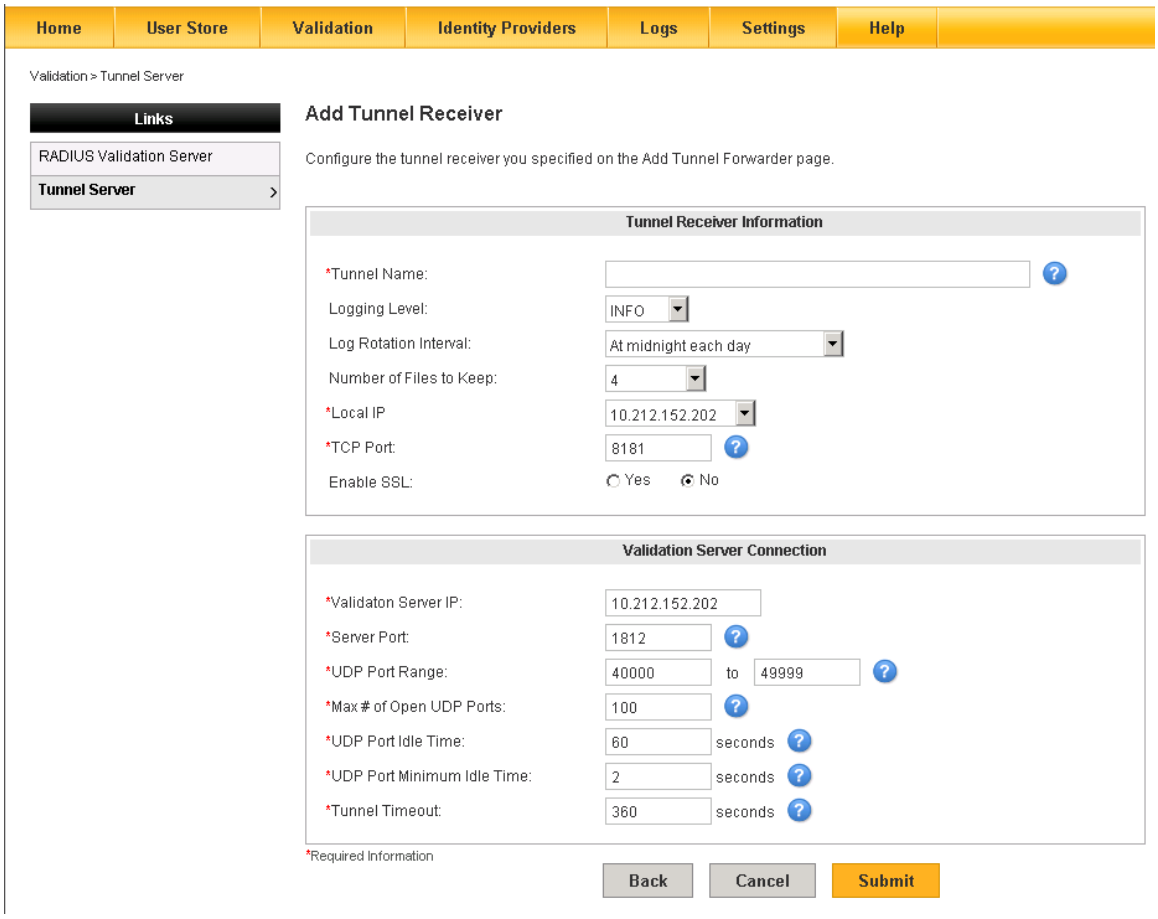

Figure 6-8 Add Tunnel Receiver

Starting and Stopping a Tunnel Forwarder or Tunnel Receiver

When you reboot the host machine, the Validation server does not automatically restart. You can start the server from the Validation page. The **Status** column on the Validation page shows you the current run status (started or stopped) of a server or tunnel. A server or tunnel must be running before you can use it for validation.

- Start a server or tunnel manually whenever you add it to your validation configuration, or after you edit it. To start a server or tunnel manually, click **Start** in the **Action** column for that server or tunnel. The status (in the **Status** column) changes from **Stopped** to **Started**.
- Stop a server or tunnel manually to do system maintenance or make configuration changes. To stop a server or tunnel manually, click **Stop** in the **Action** column for that server or tunnel. The status (in the **Status** column) changes from **Started** to **Stopped**.

You can also configure the Configuration Console to automatically start your Validation Service when you reboot your machine. To set up automatic restart:

- For Windows:
  a. Go to **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Services**.
  b. Locate the service associated with the server: `Validation Authentication Service <server name>`.
  c. Right-click the service name and from the sub-menu, select **Properties**.
  d. Change the Startup type to **Automatic**.
- For Linux:

  Add the following entry to your server inittab:

  ```
  <install dir>/Validation/bin/vsauthstartserver -servicename <server name> inittab
  ```

You may also need to manually start or stop a server or tunnel.

Health Monitor for Validation Server

A health check is performed to examine the current status of the nodes in your network. VIP Enterprise Gateway offers health check feature to monitor the Validation servers when configured using a NAS/VPN. After you configure monitoring in NAS, the load balancer periodically checks the health of each Validation Servers. NAS sends an authentication RADIUS request to the Validation Server with pre-defined values such as user name. The Validation Server provides an Access-Reject response to the request. There will be no processing of request through the Authentication Stack. Once the response is received, Validation Server will not write to logs in INFO mode.

By default, Health check feature is enabled across all modes of the Validation Server. The default user name for doing a health check request is `SASMonitor`.

You can edit the following flags in the **radserv.conf** file located in the install directory to modify the user name for monitoring health:

```
server.monitor.enabled = true
server.monitor.username = <username>
```

Chapter 7

Configuring VIP Administrator Authentication

This chapter includes the following topics:

- "Administrators in VIP Enterprise Gateway" on page 53
- "Configuring VIP Administrators" on page 54
- "Authenticating Console Administrators to Sign In Using Their Enterprise Credentials" on page 56

Administrators in VIP Enterprise Gateway

To configure the VIP Enterprise Gateway settings, one or more Enterprise Gateway Console Administrators may be needed. The first such Console Administrator is configured during the installation of VIP Enterprise Gateway. Additional console administrators can be locally created for each VIP Enterprise Gateway instance by using a command Line tool: `passwordTool.bat`. Alternatively, you can configure an LDAP User Store for VIP Enterprise Gateway console administration.

Console Administrators in VIP Enterprise Gateway do not have any differentiated access control. They have the same level of privilege of a Local Administrator. For more information on Console Administrator configuration, See "Authenticating Console Administrators to Sign In Using Their Enterprise Credentials" on page 56.

VIP Enterprise Gateway provides an Identity Provider (IdP) to Symantec-hosted VIP Manager. The VIP Administrators can use this IdP to sign in to VIP Manager using their enterprise LDAP user name and password. VIP Administrators can configure various policies in VIP Manager to manage VIP accounts and users. VIP Administrators have granular access control in VIP Manager. They can be aggregated in groups. LDAP Directory Synchronization Service uses the information from the LDAP User Store to synchronize VIP Administrators and their membership details in various VIP Administrator Groups.

Configuring VIP Administrators

To configure VIP Administrators, you can navigate to **User Store > VIP Administrator Configuration**.

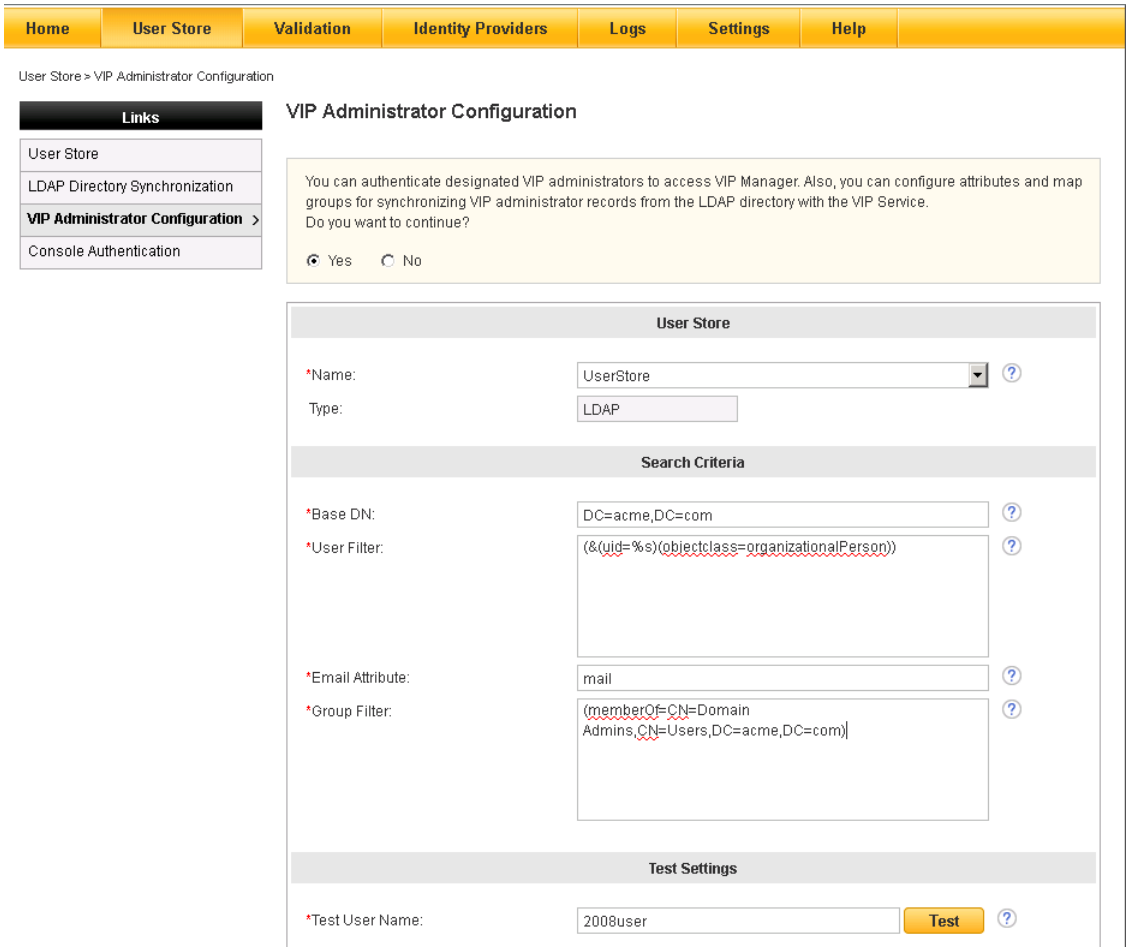

Figure 7-1 VIP Administrator Configuration

You can edit the VIP Administrator settings that you configured to do the following:

- Under **Authentication**, modify the VIP Administrator settings.
- Under **Synchronization**, configure the settings for synchronizing administrators from the LDAP User Store to the VIP Service.

Under **Synchronization**, you must specify the attribute values that store the first name and the last name of the administrators in the LDAP User Store. Also, you must map the administrators to at least one of the VIP Administrator Groups available in the VIP Service. The VIP Administrator Group that the administrators are mapped to determines the roles that are assigned to them.

If the administrator synchronization is enabled, the information that you configure under **Synchronization** is synchronized to the VIP Service during the next LDAP Directory Synchronization.

To know how to map the administrators to VIP Administrator Groups, refer to he online help associated with VIP Enterprise Gateway.

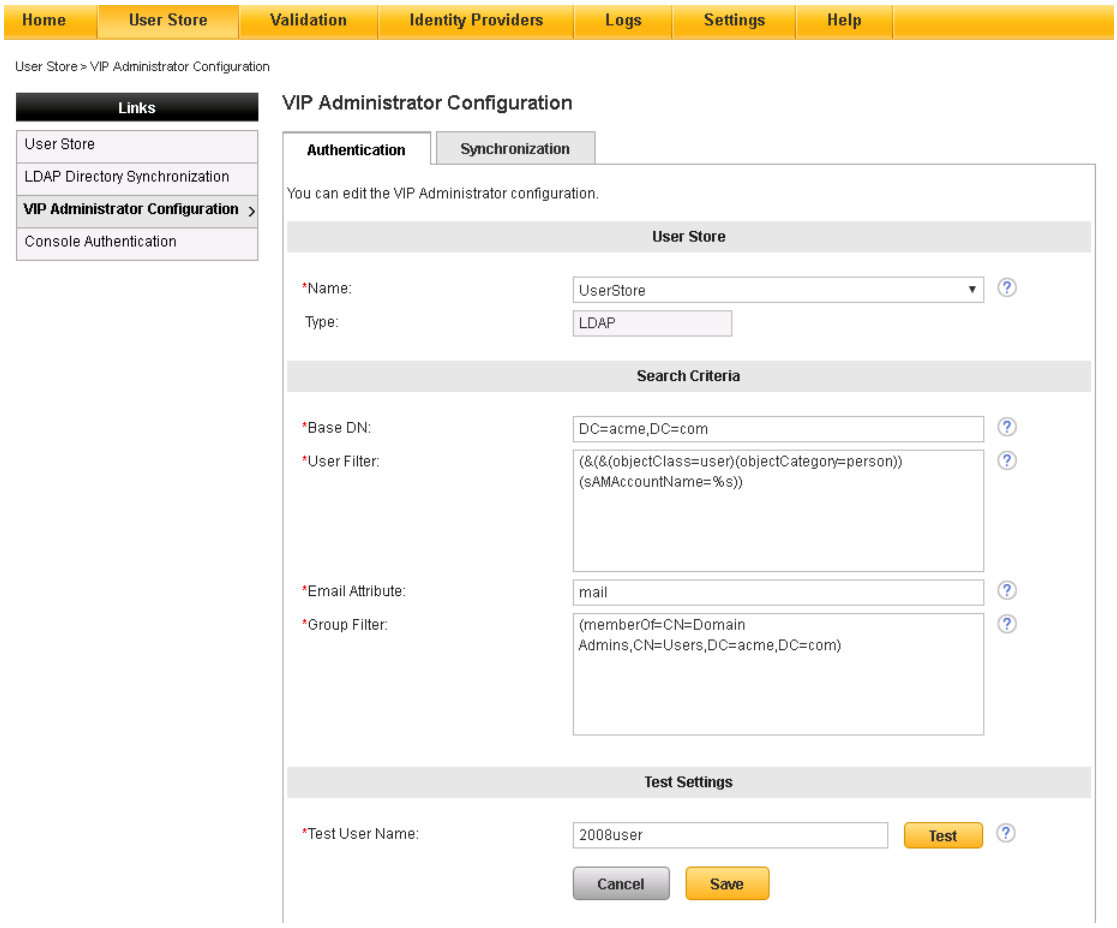

Figure 7-2 Edit VIP Administrator Configuration - Authentication

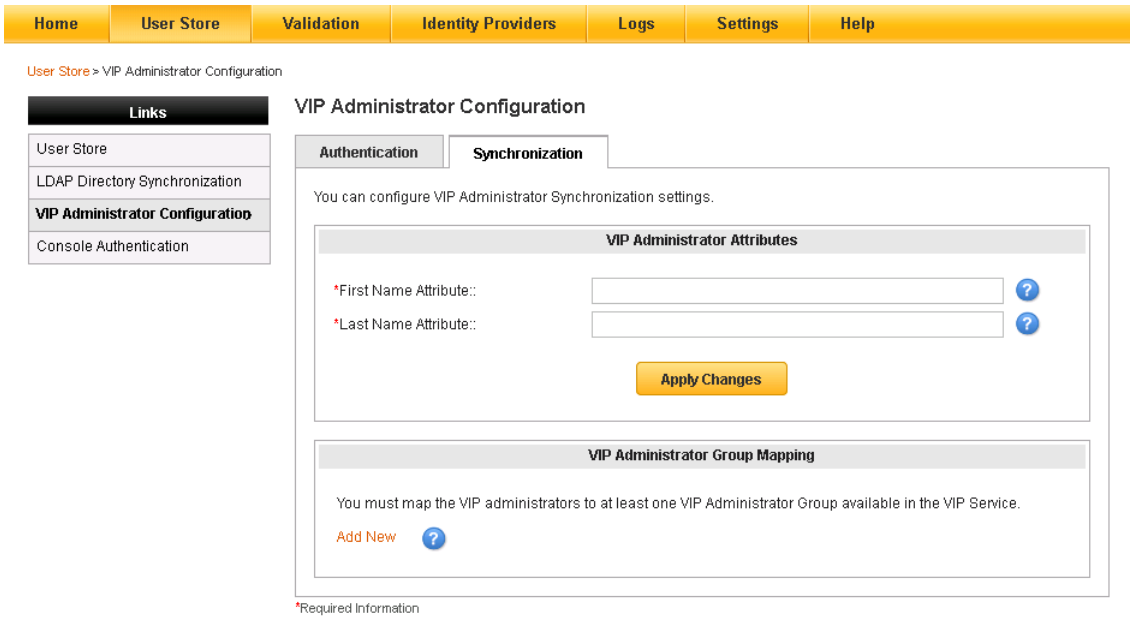

Figure 7-3 Edit VIP Administrator Configuration - Synchronization

Authenticating Console Administrators to Sign In Using Their Enterprise Credentials

To configure Console Authentication of Console administrators, you can navigate to **User Store > Console Authentication**.

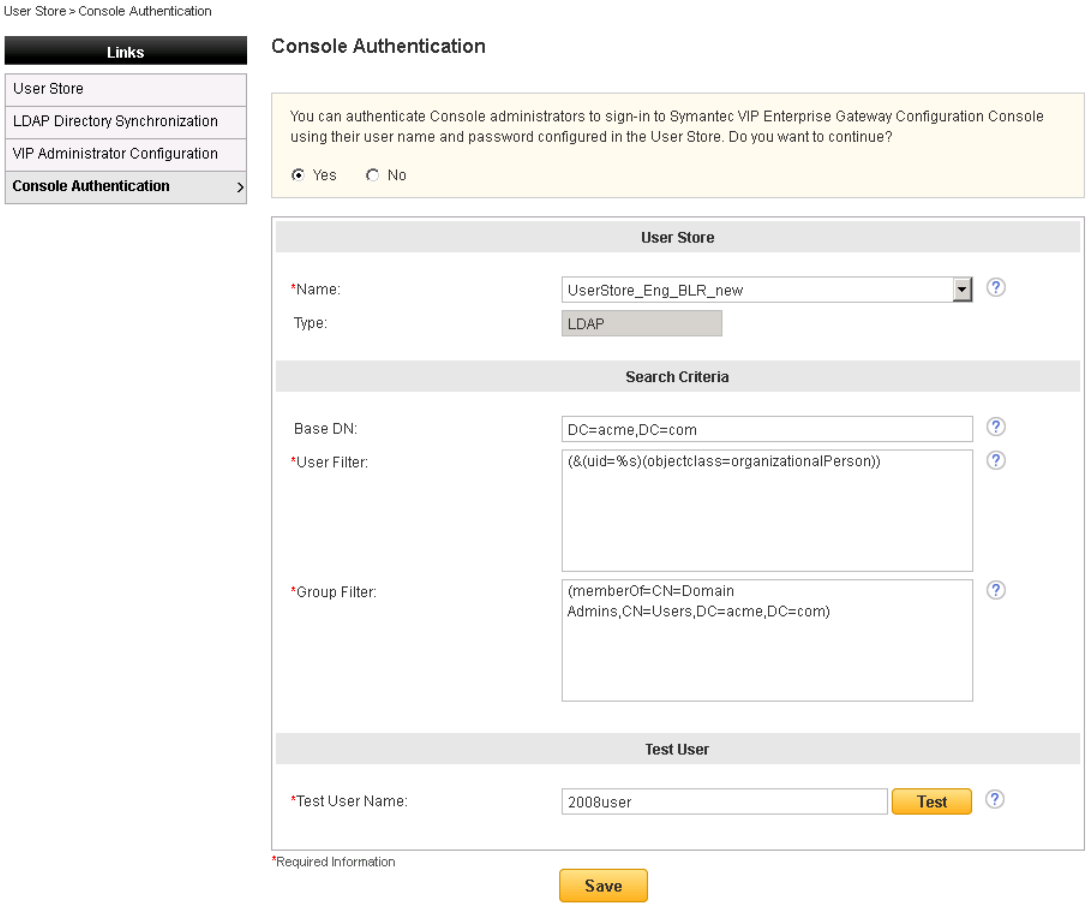

Figure 7-4 Console authentication

1. Select **Yes** in the message to allow the administrators to authenticate using the credentials configured in the User Store.
2. Select a User Store from the **Name** drop-down list.
3. Enter the **Base DN**, **User Filter**, and **Group Filter** information for the Search Criteria.
4. Enter a user name and click **Test** to check if the user is configured in the selected User Store.
5. Click **Save** to save the configuration.

After the configuration is saved, the VIP administrators can sign into the configuration console using their enterprise directory (AD or LDAP) credentials. The Sign In page will include a drop-down field as shown in the Figure 7-5.

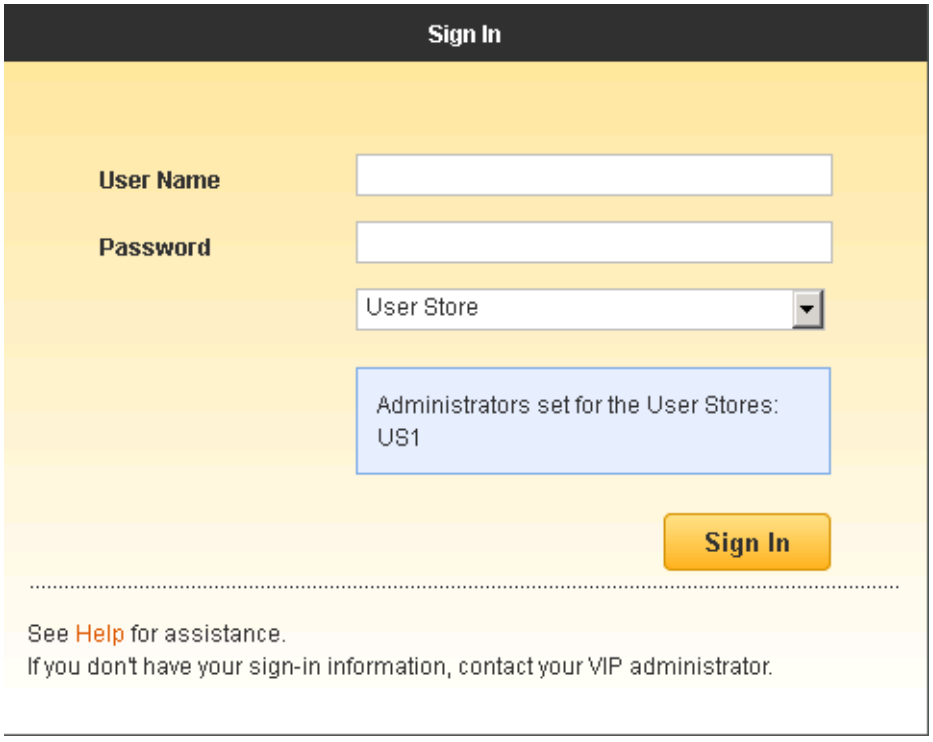

Figure 7-5 Configuration Console Sign in page for console administrators

Select **User Store** from the drop-down list below the Password field and then click **Sign In**.

Note: If you have signed in as a console administrator, all actions that you perform are logged under your name, making the auditing of VIP Enterprise Gateway operations easier.

Chapter 8

Configuring Identity Providers

This chapter describes how you can configure Self Service Portal Identity Provider (IdP) and VIP Manager IdP with VIP Enterprise Gateway.

Self Service Portal Configuration

The Self Service Portal is a cloud-based web application. Your end users can use this application to register, test, reset, or remove credentials from their accounts.

You can configure VIP Enterprise Gateway to provide secure access for your end users to the Self Service Portal, and for your administrators to VIP Manager.

Note: Optionally, your administrators can use VIP Manager's native authentication method (email address, password, and security code) to access VIP Manager. You must configure secure access to the Self Service Portal, either using VIP Enterprise Gateway or a third-party solution.

Configuring Self Service Portal IdP

You configure how end users access the Self Service Portal as well as how logs are handled from the **Self Service Portal IdP** tab. You can also configure whether users are prompted for a security code the first time they register a credential.

This tab also displays the Service Status and the Self Service Portal URL:

- **Service Status**: After you configure end-user access to Self Service Portal, the service runs by default. You can click **Stop Service** to stop the service at any time. Once the service is stopped, you can click **Start Service** to start it. However, each time you modify configuration settings and click **Apply Changes**, the service is stopped and restarted automatically.
- **Self Service Portal URL**: Your end users can use this URL to access Self Service Portal. It is generated dynamically, based on your configuration settings on this page. You need to provide this URL to your end users.
- **JavaScript Integration**: If you are planning to use the Self Service Portal IdP for JavaScript integration, then use the following URL to generate the VIP Integration Code: https://<Your_SSP_IdP_URL>/vipssp/login

The first time you access the Self Service Portal tab, you are prompted to configure access. After you configure access, the page appears in view-only mode. To re-configure end-user access to Self Service Portal, click **Edit**.

If there are more than one User Store configured, Self Service Portal searches for the user in these User Stores until it uniquely identifies the user. SSP displays the name of the User Store where the user belongs and the attributes that are configured for the user. To search for a user in the User Stores, Self Service Portal follows the order in which the User Stores are added to VIP Enterprise Gateway.

See "Searching for Users in VIP Enterprise Gateway Configured with Multiple User Stores" on page 28.

Along with Symantec's branding, your organization can also brand VIP Self Service Portal (SSP) with your organization's logo. To do this branding, you must sign in to VIP Manager and do the following in the VIP Policy Configuration page:

- Enable the cobranding feature.

- Upload your organization's logo.
- Select the applications where you want to display your organization's logo.

For more information, refer to the VIP Manager documentation.

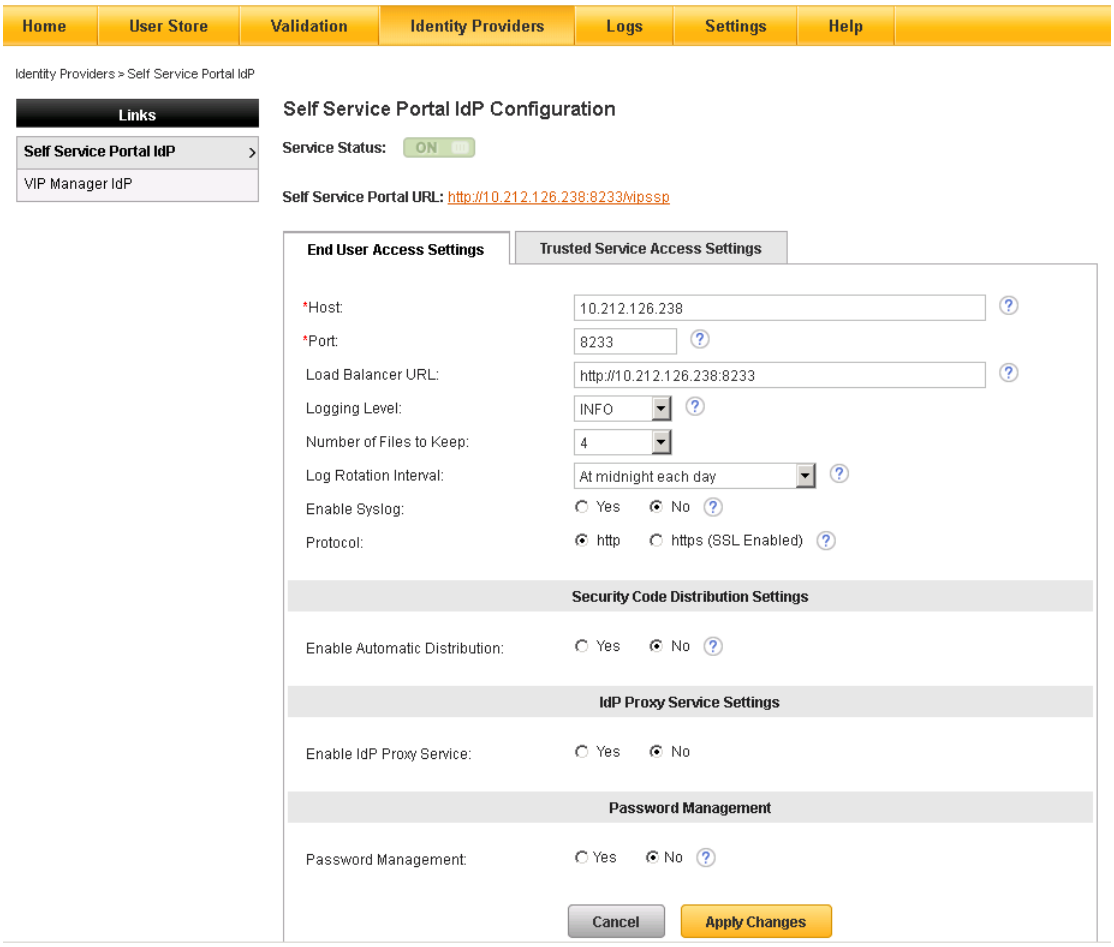

Figure 8-1 Self Service Portal

Configuring Out-of-Band Authentication

Use the Out-of-Band Authentication Settings to configure how users will receive out-of-band authentication requests. In some cases, a user does not have access to a credential when authenticating with a second factor. In this case, the user may need to request that a temporary passcode be sent through an out-of-band channel. This channel may be by email (the default), or by a mobile device capable of receiving SMS or Voice messages.

Out-of-Band Prerequisites

- Enable Automatic Distribution option should be selected
- In User Store, you must configure out-of-band authentication attributes such as Email, Voice, or SMS

After the prerequisites are defined, a request is initiated to fetch the OOB attributes. The server then checks if time difference between the current time and request time is more than the allowed delta time.

Supported Languages

VIP Self Service Portal IdP supports the following languages for localization:

Note: VIP Self Service Portal IdP accepts the default language that is set to the browser that you use to access it.

- English (US)
- Spanish (Castilian)
- French
- German
- Italian
- Portuguese (Brazilian)
- Japanese
- Korean
- Greek
- Chinese (Traditional)
- Chinese (Simplified)

Password Management Support for Self Service Portal

Password management feature available in SSP IdP enables you to manage and change your expired passwords. You must ensure you have met few simple prerequisites before you change your password.

Password Management Prerequisites

Before you enable and use the self-service password reset, you must complete the following prerequisites in Enterprise Gateway:

- Enable password management option in User Store
- Https (SSL Enabled) protocol must be selected in Self Service Portal IdP Configuration

Once these changes are done and submitted, the following additional configuration is done on VIP Manager:

- **Policies > Account tab > Application domain names** - add domain names for SSP IdP or Load Balancer. SSP IdP server host name should be a fully qualified domain name.
- **Policies > VIP Intelligent Authentication** - Enable VIP Intelligent Authentication.

Out-of-Band Authentication for Password Management

You can use out-of-band authentication for password management. Make sure to select the prerequisites to enable out-of-band.

Out-of-Band Prerequisites

- Enable Automatic Distribution option should be selected
- In User Store, you must configure out-of-band authentication attributes such as Email, Voice, or SMS

After the prerequisites are defined, a request is initiated to fetch the OOB attributes. The server then checks if time difference between the current time and request time is more than the allowed delta time.

By default, the maximum time difference must not be more than five minutes. If administrator wants to change the delta time, then modify the configuration property value in the **ssp.conf** file and should restart the SSP service.

```
samlidp.timestamp.delta
```

Reset your Expired Password

If your password is expired, you will be prompted to enter your security code. On successful authentication, you need to enter your new password and confirm.

By default, the retry attempt is 10. You can configure this value in the User Store property file

Note: The password that you enter should be in accordance with the password policy of the respective User Store.

Alternative IdP to Access Self Service Portal and VIP Manager

You can use enterprise IdP to access Self Service Portal or VIP Manager. For configuration details and supported IdPs, refer to *VIP Third-party Integration Guides* available in the **Download > Third Party Integration**.

Alternatively, you can develop your own Web service clients to manage Self Service Portal or VIP Manager web applications. Refer to the following documents for more information about using Web services for these operations:

- For end-user credential operations, refer to *Symantec VIP User Services Developer's Guide.*
- For operations on credentials, refer to *Symantec VIP Web Services Developer's Guide.*

Testing Self Service Portal

1. Access the link `<http://<sspidphost>:8233/vipssp>`
2. Enter your LDAP user name and password and click **Submit**.
3. You will be redirected to Self Service Portal. Enter the security code to access the portal.

If your password is expired, you will be challenged to enter the security code.

Troubleshooting Self Service Portal

The following are the troubleshooting issues for Self Service Portal:

Table 8-1 Troubleshooting

Issue	Solution
Unable to start the service. Check the Time zone and the time is set accurately on the VIP Enterprise Gateway Server.	You may encounter this message when you start these services. Start the Self Service Portal or the VIP Manager IdP portal, you must ensure that the clock on the computer where you have installed VIP Enterprise Gateway displays the time according to your time zone. Then, you must restart the VIP Enterprise Gateway service
We've Encountered an Unexpected Problem.	You must ensure that the clock on the computer where you have installed VIP Enterprise Gateway displays the time according to your time zone. Then, you must restart the VIP Enterprise Gateway services, SSP service, and the IdP service to resolve this problem. The VIP Enterprise Gateway portal displays this error even if there is a difference of a few minutes with the local time. You can also synchronize the VIP Enterprise Gateway servers with a network-synchronized clock by using NTP or any other standards that the platform supports.

Self Service IdP Proxy

Self Service Proxy (IdP Proxy) has been discontinued from VIP Enterprise Gateway 9.8 release. As an alternative to SSP IdP Proxy, you must use reverse proxy applications such as Web Application Proxy (Windows) or Squid (Linux). However, SSP IdP Proxy 9.7 will still work with VIP Enterprise Gateway 9.8 with limited features.

Publishing Self Service IdP as Reverse Proxy

If you are publishing Self Service IdP as a reverse proxy, then use the following URL to publish the Self Service IdP: https://<SSP_IdP_FQDN>/vipssp/

Once you publish the Self Service IdP, if you are integrating with JavaScript, then use the following URL to generate the VIP Integration Code: https://<Reverse_Proxy_FQDN>/vipssp/login

Trusted Service Access Settings

Trusted Service Access Settings is introduced for third-party application to use Self Service Portal IdP in JavaScript integration. In order to get the out-of-band attributes such as Email, SMS, Voice, the Self Service Portal IdP requires the LDAP password. Since few of the third-party applications do not provide password in their login page (such as step up and multi step authentication), configuring out-of-band becomes difficult.

This issue can be addressed using the Trusted Service Access Settings. This service uses VIP certificate to authenticate LDAP user to receive out-of-band attributes.

Symantec recommend to use this feature only if VIP third-party integration supports Trusted Access Settings. Refer *VIP third-party Integration Guides* to learn more about the supported information.

To use this feature, you must configure Self Service Portal IdP with https.

Trusted Access Settings allows you to fetch the attributes from LDAP. For example, Email, Phone Number. You must add a valid VIP certificate which is used in third-party applications such as Active Directory Federation Service.

In the Trusted Service Access Settings, you must add the VIP certificate that is used in the third-party application such as AD FS.

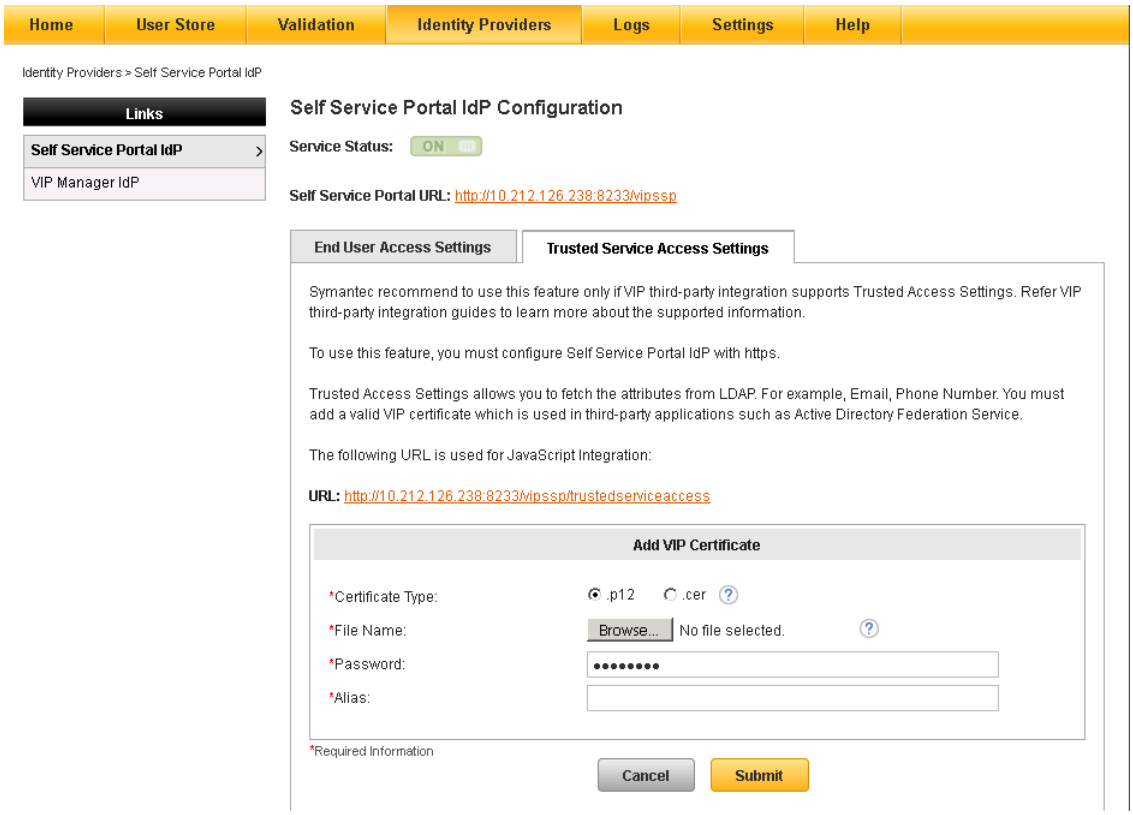

Figure 8-2 Trusted Service Access Settings

VIP Manager IdP Configuration

VIP Manager is a cloud-based web application your administrators use to manage VIP credentials for your end users.

VIP Manager is where your administrators manage VIP credentials for your end users. Normally, administrators access VIP Manager using their email address, VIP Manager password, and a security code from a VIP credential. Using VIP Enterprise Gateway, you can allow your administrators or help desk personnel to access VIP Manager. You can authenticate them using their user name and password from your User Store.

You configure how administrators access VIP Manager, as well as how logs are handled, from the **VIP Manager** IdP Configuration page. This page also displays the Service Status and the VIP Manager URL.

- Service Status: After you configure administrator access to VIP Manager, the service runs by default. You can click **Stop Service** to stop the service at any time. Once the service is stopped, you can click **Start Service** to start it. However, each time you modify configuration settings and click **Apply Changes**, the service is stopped and restarted automatically.
- VIP Manager URL: Your administrators use this URL to access VIP Manager. It is generated dynamically, based on your configuration settings on this page. You need to provide this URL to your administrators.

The first time you access the **VIP Manager** tab, you are prompted to configure access. After the access is configured, the page appears in view-only mode. To re-configure end-user access to VIP Manager, click **Edit**.

VIP Manager authenticates the user present in the User Store that you have selected in the **User Store** field.

Figure 8-3 shows the **VIP Manager IdP Configuration** page.

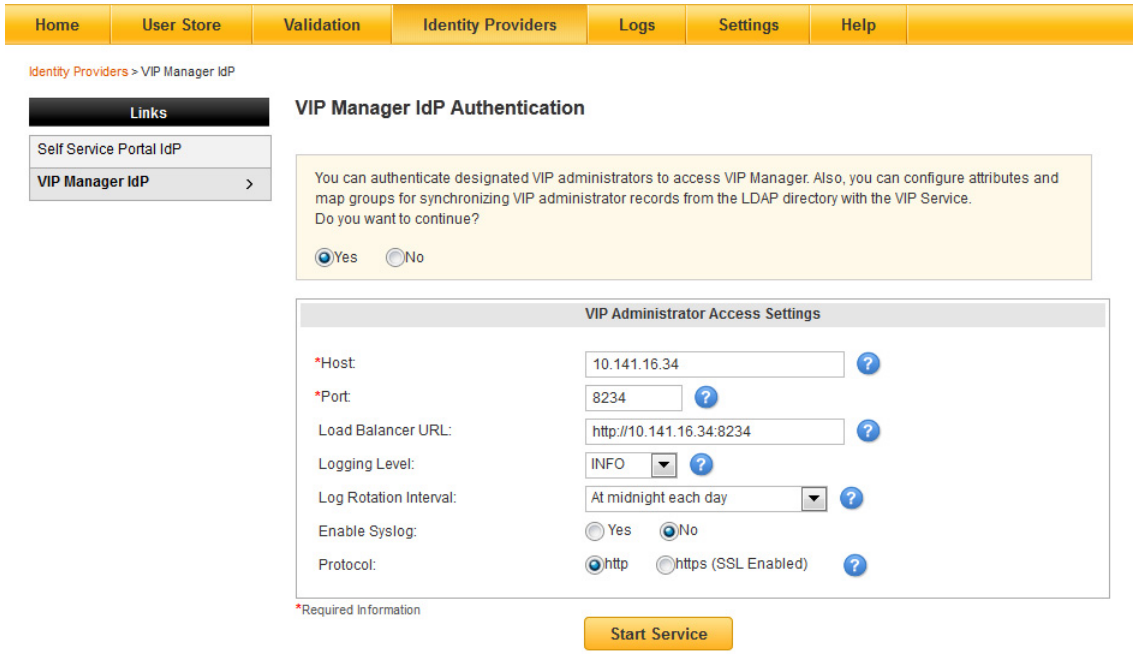

Figure 8-3 VIP Manager tab in editable mode

Chapter 9

Configuring LDAP Directory Synchronization Service

The LDAP Directory Synchronization Service lets you automatically synchronize the users and the administrators in your LDAP directory with the user data in the VIP Service.

To enable LDAP Directory Synchronization Service:

- You must configure at least one User Store.

  LDAP Directory Synchronization Service synchronizes the VIP attribute IDs in all User Stores to VIP User Service.
- The LDAP Directory Synchronization connects to the VIP Service through the Internet over outbound port 443.

If you add, modify or delete entries in your LDAP directory, LDAP Directory Synchronization service automatically adds, modifies, or deletes these entries in the VIP Service.

You have the option of running the synchronization operation in a simulation mode. This mode lets you see the changes that are made to the VIP User Service without performing any synchronization.

Using LDAP Directory Synchronization Service to Synchronize User Stores to the VIP Service

LDAP Directory Synchronization Service adds, updates, or deletes users and administrators to the VIP Service based on the membership of the users in the enterprise User Store. In a simple LDAP Directory Synchronization configuration, all User Stores are configured with a single VIP Enterprise Gateway server. In such a configuration, the LDAP Directory Synchronization Service can access all the user records and synchronize them to the VIP Service. The LDAP Directory Synchronization Service synchronizes user data to the VIP Service once a day. This synchronization usually occurs when the load on VIP Enterprise Gateway server is not high.

However, Symantec has identified the following additional use cases that occur because of complex enterprise-level LDAP configurations:

- "Use Case 1: Supporting Load-balancing and Failover" on page 68
- "Use Case 2: Synchronizing Disparate User Stores Independently from Different VIP Enterprise Gateway Servers" on page 68
- "Use Case 3: Synchronizing Users Created Through Third-party Identity Provider for Self Service Portals" on page 69

To resolve these use cases, you can configure LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers. For more information, See "Configuring Multiple Instances of LDAP Directory Synchronization Service" on page 68.

Note: Symantec recommends you to follow these configurations only on such complex LDAP configurations, which are listed in this section.

Configuring Multiple Instances of LDAP Directory Synchronization Service

You can configure LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers. The VIP Service supports a maximum of 24 instances of LDAP Synchronization service from a VIP account.

Note: Check whether your User Store configuration that is associated with the VIP Enterprise Gateway servers conform to the one described in the following use cases (User Case 1 or Use Case 2). If not, do not continue with the configuration of multiple instances of LDAP Directory Synchronization Service. In such cases, Symantec recommends you to contact Symantec Support before you continue with this configuration.

Use Case 1 recommends that the User Stores must be configured identically. **Use Case 2** recommends that separate Synchronization Clusters must be configured for each group of User Stores.

Use Case 1: Supporting Load-balancing and Failover

Before you configure LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers, you must ensure that the User Stores for these servers are configured identically. Also, the User Stores on all the VIP Enterprise Gateway servers must be arranged in the same order. Ideally, you can configure the User Stores on a VIP Enterprise Gateway server, export its configuration settings, and import them on the other servers.

Supporting Load-balancing

To achieve load-balancing, you must ensure that the synchronization schedules of these VIP Enterprise Gateway servers are distinct and at least three hours apart. Three hours is the window period for a synchronization schedule beyond which a synchronization task will not last. No other instance can run within this window period if that instance is part of the same Synchronization Cluster.

Supporting Failover

To achieve failover, you must configure the synchronization schedules of the LDAP Directory Synchronization Service instances within the window period of three hours.

In such cases, only one instance of LDAP Directory Synchronization service can synchronize the users. At the beginning of its synchronization schedule, the other instances of LDAP Directory Synchronization service verify the following:

- Whether an LDAP synchronization is in progress.
- Whether an LDAP Synchronization instance has started within the past three hours.

If either of these conditions are met, the LDAP Synchronization Service aborts the scheduled LDAP synchronization and waits for the next interval. If these conditions are not met, the LDAP Synchronization Service starts synchronizing the users.

Use Case 2: Synchronizing Disparate User Stores Independently from Different VIP Enterprise Gateway Servers

Enterprise LDAP directories may have the location network visibility constraint. This constraint leads to an issue in synchronizing all LDAP servers from the same VIP Enterprise Gateway server. In such cases, you can configure a Synchronization Cluster for each group of LDAP servers visible in the network. The VIP Enterprise Gateway servers in each Synchronization Cluster can synchronize the users that are part of that Synchronization Cluster. They cannot synchronize the users that are part of another Synchronization Cluster. You must ensure that overlapping user sets do not exist across the Synchronization Clusters in your environment.

To configure Synchronization Cluster, you can navigate to **Settings > System Settings** in the Configuration Console. By default the VIP Enterprise Gateway displays the name of the Synchronization Cluster as VIP_EG.

Use Case 3: Synchronizing Users Created Through Third-party Identity Provider for Self Service Portals

Organizations may already have a third-party Identity Provider (IdP) configured in their enterprise. They can reuse this IdP to access VIP Self Service Portal (SSP). If a user does not exist in the VIP Service, VIP SSP on receipt of a valid SAML assertion creates the user in the VIP Service. To use a specific LDAP Directory Synchronization Service for synchronizing the users thus created, the user assertion must contain an attribute named GUID. The value of this attribute is the name that you configure for the Synchronization Cluster.

An Example that Explains the Configuration of Multiple Instances of LDAP Directory Synchronization Service

The following example explains the configuration of multiple instances of LDAP Directory Synchronization Service:

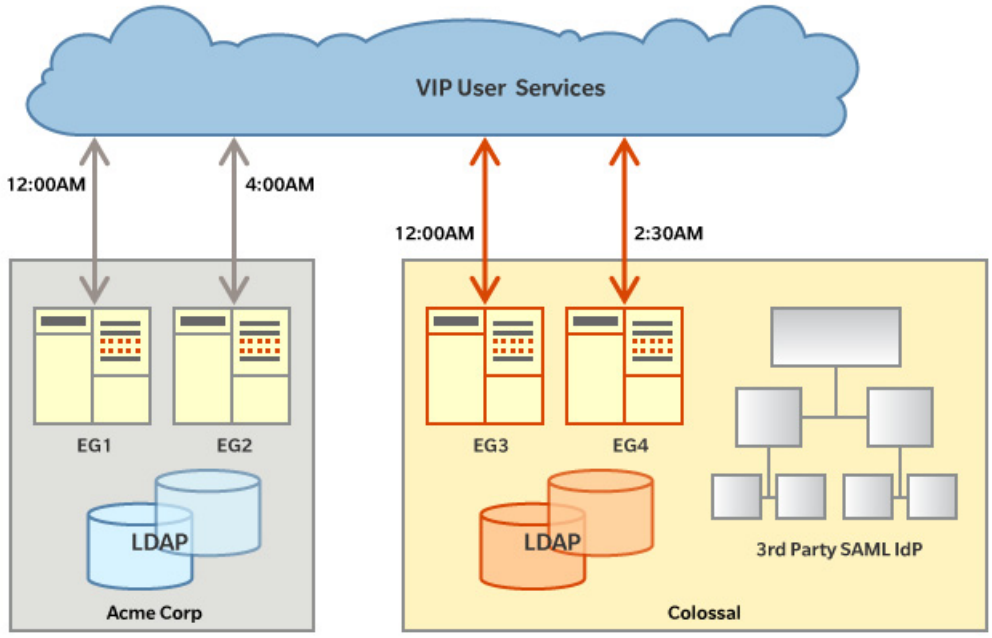

Figure 9-1 ACME Corporation - LDAP Synchronization Configuration

ACME Corporation uses two Synchronization Clusters - **Acme Corp** and **Colossal** - for LDAP synchronization. The user stores EG1 and EG2 are part of the **Acme Corp** Synchronization Cluster and EG3 and EG4 are part of the **Colossal** Synchronization Cluster. The LDAP Synchronization service instances that run on these servers synchronize the user and the administrator records that are available in ACME Corporation's user stores.

EG1 and EG2 are part of the **Acme Corp** Synchronization Cluster. These servers synchronize the user records that are available in the User Stores, which are part of the **Acme Corp** Synchronization Cluster. The user stores that are associated with EG1 and EG2 must have identical configuration. Ideally, you should export the user store configuration from EG1 and import it to EG2.

EG3 and EG4 are part of the **Colossal** Synchronization Cluster. These servers synchronize the user records that are available in the User Stores, which are part of the **Colossal** Synchronization Cluster. Also, the user stores that are associated with EG3 and EG4 that are part of the **Colossal** Synchronization Cluster must have identical configuration.

EG1 start synchronizing the user records at 12 midnight. No synchronization service runs for the next three hours, which is the window period for synchronization. Then, EG2 start synchronizing the user records at 4:00 A.M. Before EG2 start synchronizing the records, it ensures that no other LDAP synchronization is in progress for the **Acme Corp** Synchronization Cluster.

For **Colossal** synchronization cluster, EG3 is scheduled to synchronize the user records at 12 midnight. EG4 is scheduled to synchronize the user records at 2:30 A.M. Before EG4 start synchronizing the records, it verifies the following:

- Whether an LDAP synchronization is in progress for the **Colossal** Synchronization Cluster.
- Whether an LDAP Synchronization instance has started within the past three hours.

EG4 aborts the scheduled LDAP synchronization and waits for the next schedule when it recognizes one of the following conditions:

- EG3 has started synchronization in the past three hours for the **Colossal** Synchronization Cluster.
- EG3 is in the process of synchronizing the user records for the **Colossal** Synchronization Cluster.

The user stores configured for the **Acme Corp** Synchronization Cluster and the **Colossal** Synchronization Cluster must not overlap. The user IDs that an Enterprise Gateway server synchronizes with the VIP Service carries the name of its Synchronization Cluster as attribute GUID. For example, the user `John_Smith` that EG1 synchronizes carries an attribute GUID **Acme Corp**. If `John_Smith` is also part of the **Colossal** Synchronization Cluster, the LDAP synchronization operation for that cluster checks the GUID of `John_Smith` in the VIP Service. If it finds GUID **Acme Corp** with `John_Smith`, the LDAP synchronization service for the **Colossal** Synchronization Cluster does not synchronize the user `John_Smith`. That is, only EG1 and EG2 that are dedicated to the **Acme Corp** Synchronization Cluster can synchronize the user record `John_Smith`.

A Synchronization Cluster can now synchronize a user record that a third-party Identity Provider (IdP) creates. In this example, the **Colossal** Synchronization Cluster synchronizes a user that the **3rd Party SAML IdP** creates. To synchronize a user that **3rd Party SAML IdP** creates, the user assertion must contain an attribute named GUID. The value of this attribute is the name that you configure for the Synchronization Cluster. In this case the value of GUID attribute is **Colossal** because the user is synchronized from the **Colossal** Synchronization Cluster.

Configuring LDAP Synchronization Service from the Configuration Console

You configure the LDAP Directory Synchronization from the **LDAP Directory Synchronization** page.

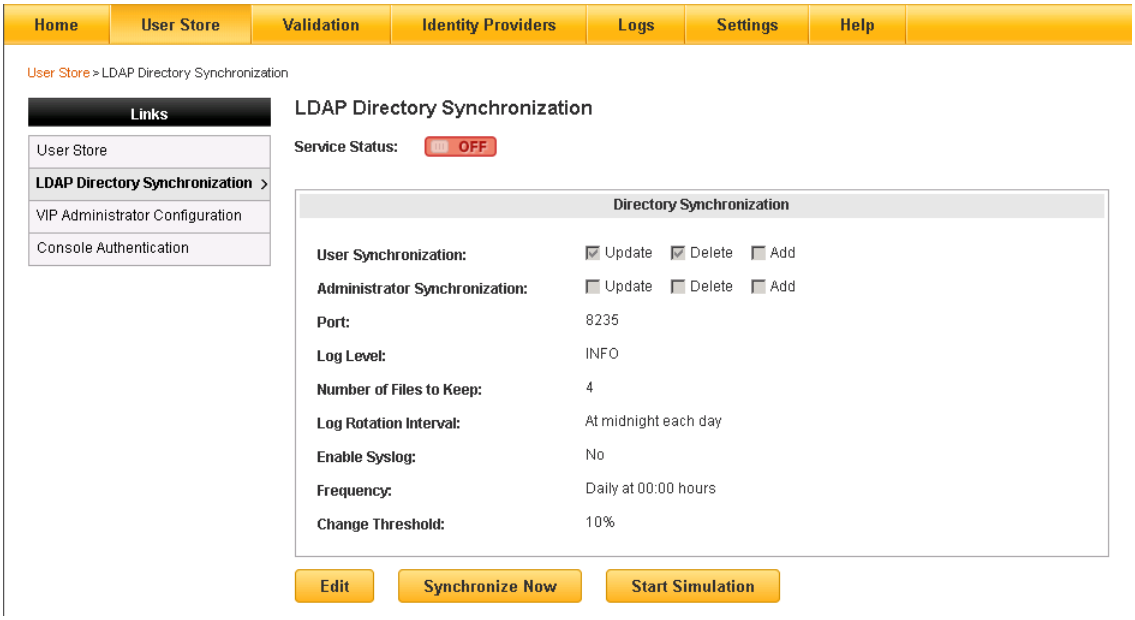

Figure 9-2 Directory Synchronization page

You configure the LDAP Directory Synchronization Service through the Configuration Console. For the procedure on configuring LDAP Directory Synchronization service, refer to the online help associated with VIP Enterprise Gateway.

LDAP Directory Synchronization - Best Practices that Symantec Recommends

- Symantec recommends you to use only one approach for adding, updating, and editing user information.
- Adding Users – The SSP IdP portal that you configure is the preferred approach to add users.
- Editing or Deleting Users – If LDAP synchronization is configured to edit or delete user information, the administrators must not modify user names, or delete users from VIP Manager.
- Before LDAP Directory Synchronization Service compares user information with VIP Authentication Service, it queries for all the users in the User Stores that it can validate. A large user search scope returns a large amount of redundant user information from the LDAP sources. Ideally, the query must return only the users who use the VIP authentication. To enhance the performance of the user query, you can create specific group membership for the users in the LDAP source.
- Before you start the LDAP Directory Synchronization Service, Symantec recommends that you run the simulation. After you run the simulation, check the simulation logs to find the user accounts that may be affected.
- Use **Run Once** to immediately synchronize all the changes from the User Store to the user services.
- If you do not want to synchronize users with status `disabled` or `locked` in an Active Directory User Store, use the following filters with your User Store filters:

- For excluding the users with the status `disabled` in the User Store - **(&(<Your Filter>)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))**
- For excluding the users with the status `locked` in the User Store - **(&(<Your Filter>)(!(userAccountControl:1.2.840.113556.1.4.803:=16)))**

The LDAP Directory Synchronization Service does not synchronize (add, update, or delete) these users. For example, the status of the user in the User Store changes from `enabled` to `disabled` or `locked` in two consecutive LDAP Synchronization operations. Then, the LDAP Directory Synchronization Service considers that user as deleted from the User Store. The service removes the user's account from the VIP Service.

Chapter 10

Testing the Installation

This chapter includes the following topics:

- "Verifying Component Installation" on page 73
- "Verifying Overall Operation" on page 75

This chapter describes how to test the installation of VIP Enterprise Gateway. Testing requires the verification of the correct installation of individual components, followed by verification of overall operation.

Verifying Component Installation

Complete the following steps to verify that your VIP Enterprise Gateway implementation has been installed and configured correctly.

- Verify that all of VIP Enterprise Gateway components are accessible:
  - Log in to the Configuration Console (http://<hostname of the VIP Enterprise Gateway machine>:8232).
  - In the Configuration Console, select the **Validation** tab and verify that all the servers and tunnels are started and running as expected.
  - In Configuration Console, select the **Identity Providers** tab. Verify that the **Service Status** field of **Self Service Portal** and **VIP Manager** are set to **On** if these IdPs are configured. Also, access the service URLs for Self Service Portal and VIP Manager and verify that they function as expected. Then, navigate to **User Store > LDAP Directory Synchronization** and verify that the **Service Status** field is set to **On**.

    If any problems or error conditions are found, check the logs for the specific component under the **Logs** tab.

Verifying the RADIUS Client

Use the `<VIP_MAUTH_HOME>/tools/vsradiuseclient_test` tool to test that your RADIUS client functions properly. This tool sends an authentication request to the VIP Validation Service. The credential that is used in this test must already be bound to a user.

Usage:

```
./vsradiusclient_test --server-host <server name/ip address> --server-port <server port> --
client-ip <ip address> --secret <radius shared secret> --user-name <username> --password <OTP>
--verbose --attempts 3 --timeout <60>
```

Table 10-1 vsradiusclient_test parameters

Parameter	Required?	Definition
server-host	Y	The IP address or host name of the Validation server.

Table 10-1 vsradiusclient_test parameters

Parameter	Required?	Definition
server-port	N	The port number for the Validation server. This port must match the port number that set in Configuration Console. If not provided, the tool uses port 1812.
client-ip	Y	The IP address for the RADIUS client.
secret	Y	The RADIUS shared secret for the RADIUS client. This value must match the shared secret set in Configuration Console.
user-name	Y	A user ID for the authentication request.
password	Y	<security code> for User ID - Security Code mode. <LDAP password><security code> for User ID - LDAP Password - Security Code mode.
verbose	N	Gives more information about the request including radius mapping attributes from the server.
attempts	N	Number of times the authentication request will be retried before timing out.
timeout (in seconds)	N	Select the amount of time (in seconds). RADIUS client should wait for the Validation server to respond to each retry.

Example Commands

The following sample command uses the `vsradiusclient_test` tool to verify functionality of the RADIUS client in the **User ID - Security Code** validation mode. In this example, the password is a security code.

```
./vsradiusclient_test --server-host 10.10.0.10 --server-port 1812 --client-ip 10.10.0.12 --
secret myradiussecret --user-name user1 --password 940682
```

The following sample command uses the `vsradiusclient_test` tool to verify functionality of the RADIUS client in the **User ID - LDAP Password - Security Code** validation mode. In this example, the password is a combination of the user's LDAP password and the security code.

```
./vsradiusclient_test --server-host 10.10.0.10 --server-port 1812 --client-ip 10.10.0.12 --
secret myradiussecret --user-name user1 --password user1password940682
```

The following sample command uses the `vsradiusclient_test` tool to verify functionality of the RADIUS client in the **User ID - Access PIN - Security Code** validation mode. In this example, the password is a combination of the user's Access PIN and the security code.

```
./vsradiusclient_test --server-host 10.10.0.10 --server-port 1812 --client-ip 10.10.0.12 --
secret myradiussecret --user-name user1 --password user1apin940682
```

The following sample uses the `vsradiusclient_test` tool to verify functionality of the RADIUS client in the **User ID - LDAP Password - Security Code (RADIUS Access Challenge)** validation mode. In this example, the password is user's LDAP password.

```
./vsradiusclient_test --server-host 10.10.0.10 --server-port 1812 --client-ip 10.10.0.12 --
secret myradiussecret --user-name user1 –password user1password
```

When you enter this command, you are prompted for the security code that you receive on your registered phone.

Verifying Overall Operation

When you have verified the correct installation of all components, the next step is to verify overall operation.

This step requires:

- If access to the Self Service Portal or VIP Manager are not configured, integrate your custom application with the VIP Enterprise Gateway Web Services. For more information, refer to *VIP Web Services Developer's Guide* or *VIP User Services Developer's Guide*.
- Set up an active user account through which users log in and test security code validation.

Chapter 11

Upgrading VIP Enterprise Gateway

This chapter includes the following topics:

- "Checking for the Upgrades and Patches" on page 77
- "Installing VIP Enterprise Gateway Upgrades and Patches" on page 79

Note: The screen shots that are used in this chapter are for illustrative purpose only.

You can upgrade VIP Enterprise Gateway either through LiveUpdate server or by installing the package that you downloaded from VIP Manager.

Though you can customize the path to install VIP Enterprise Gateway, the LiveUpdate server is installed in the following path : `C:\Program Files (x86)\Common Files\Symantec Shared\Java LiveUpdate` (Windows) or `/opt/Symantec/LiveUpdate` (Linux).

Checking for the Upgrades and Patches

Automatic Mode

When you set Update Settings to Automatic mode, VIP Enterprise Gateway communicates with the LiveUpdate server to check for product updates automatically.

1 If new updates are available for installation, you will see the following options when you sign into VIP Manager:

- View, download, and install updates
- Remind me on next login
- Switch to manual mode

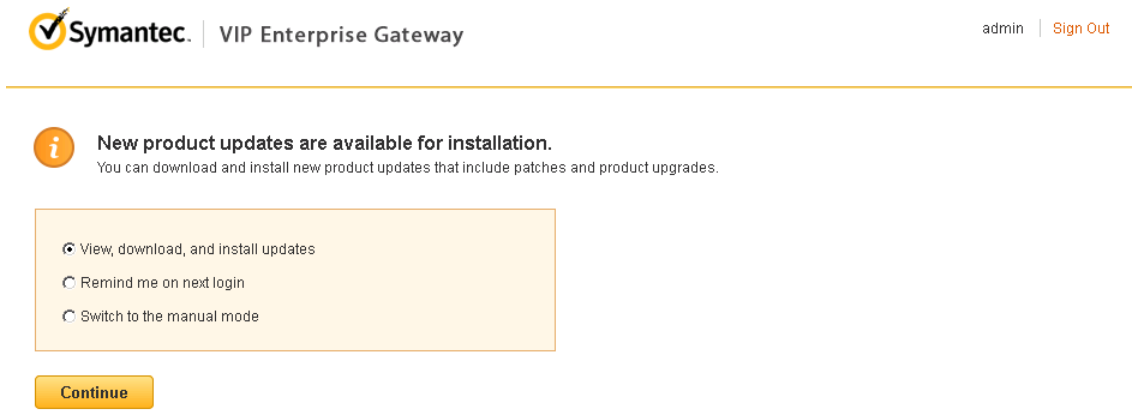

Figure 11-1 New updates available screen in Automatic mode

2 Select **View, download, and install updates** and click **Continue**.

The Update page appears listing all the product upgrades and patches that are available for installation.

Manual Mode

In Manual mode, you must initiate the check for the product updates.

1 On the Update Settings page, click **Check for updates**.

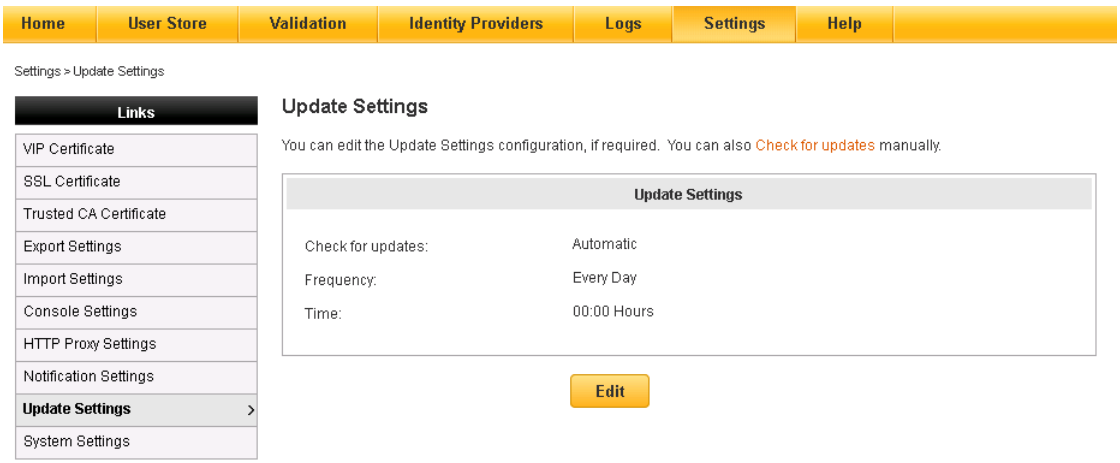

Figure 11-2 Manual Mode – check for updates

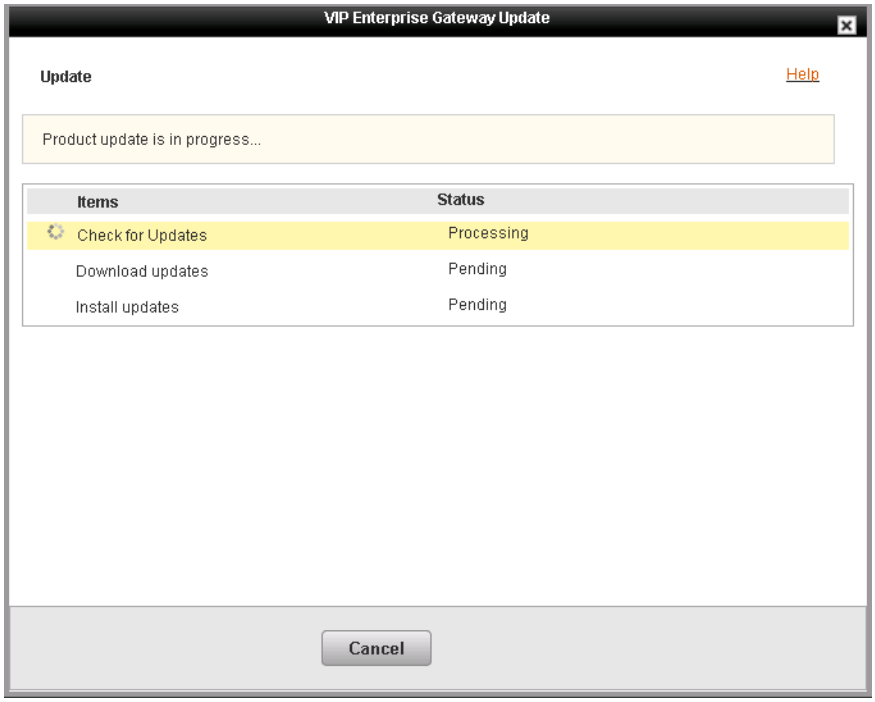

Figure 11-3 Check for Updates – Status

Installing VIP Enterprise Gateway Upgrades and Patches

The Update page lists all the product upgrades and patches that are available for your installed version of VIP Enterprise Gateway. By default, all the product updates appear selected. Deselect product updates that you do not want to install.

Note: VIP Enterprise Gateway takes backup of the existing configuration during the product update. If an update fails, you can use the restore script to manually reinstate the previous version.

See "Restoring the Previous Version of VIP Enterprise Gateway" on page 100.

1 After you select the updates to install, click **Download**.

In the Update page, view the status of the **Download Updates** item as **Processing**. After all the selected updates are downloaded, the status of the **Download Updates** item changes to **Completed**.

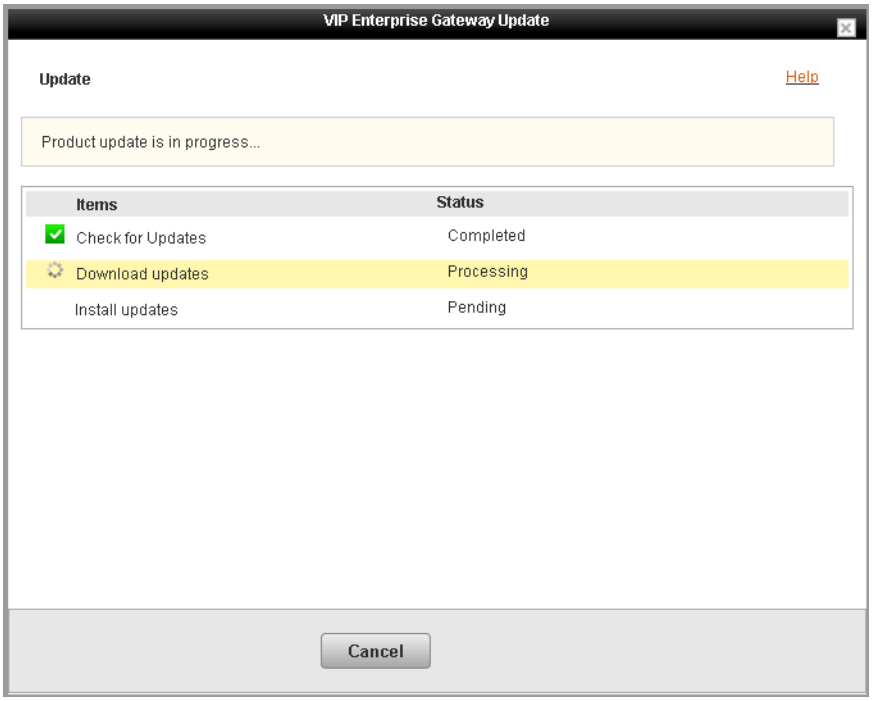

Figure 11-4 Download Updates – Processing

2 In the message box: Warning: Service Update, click **Proceed**.

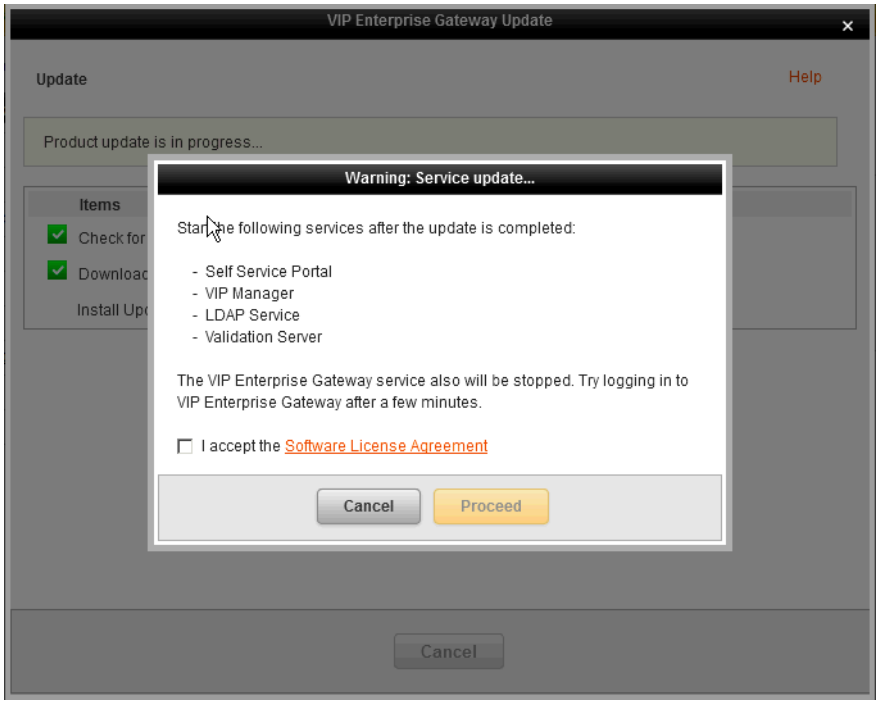

Figure 11-5 Warning – Service Update

3 After the upgrade starts, the following screen appears for a few seconds (Figure 11-6). Subsequently, the VIP Enterprise Gateway log-in page displays (Figure 11-7).

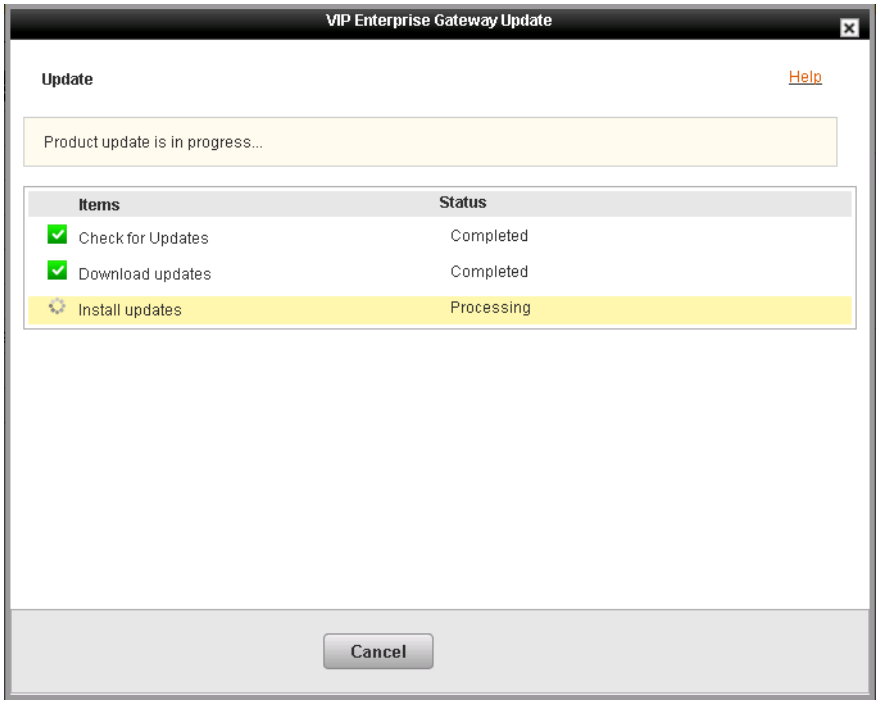

Figure 11-6 Install Updates – Status

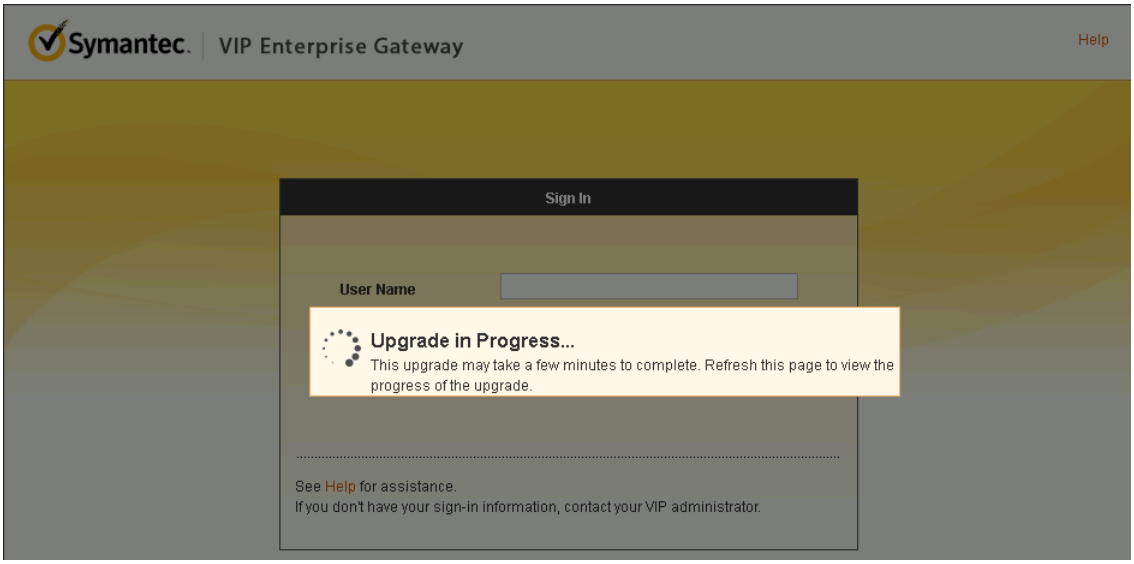

Figure 11-7 VIP Enterprise Gateway log-in page

4 To display the upgrade status, refresh the log-in page after a few minutes.

The **Upgrade in Progress** page appears.

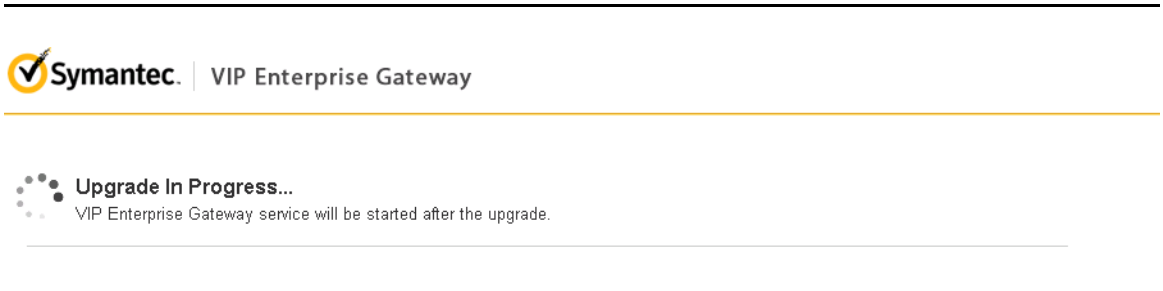

Figure 11-8 VIP Enterprise Gateway - Upgrade in Progress

5 After the upgrade is completed, the following page displays

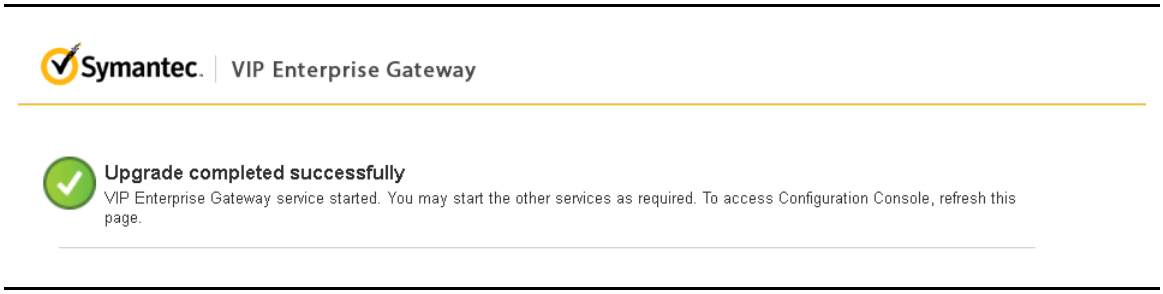

Figure 11-9 VIP Enterprise Gateway - Successful upgrade

6 Refresh the page to display the VIP Enterprise Gateway Sign In page.

Chapter 12

Logging of VIP Enterprise Gateway Components

You have considerable flexibility in creating, configuring, and viewing the log files in VIP Enterprise Gateway. VIP Enterprise Gateway logs share a common format that is explained in this chapter. This format supports the use of automated tools, both for report generation and for troubleshooting.

If you want to be alerted when there are errors, instead of searching for errors in log files, you can use a third-party log monitoring program.

Reporting tools should generally parse the logging data to extract audit type transactions, normally one line per operation. Then, they can extract major event components such as time stamp, client IP and message. They can also parse operation-specific name-value pairs in messages to gain operation-specific data.

Log File Components

The components shown in the log file are tab-delimited and can be customized.

The `vipegconsole` and the server logs use the following format for their entries:

```
LogLevel DateTime ClientIP Component [SessionID] TransactionID ErrorCode \ Message [ThreadID]
[SourceClassName]
```

The message component has the following format:

```
"[actor=who,][text=some message,][op=x,][tid=y,][user=user1,]\[nameX=valueX]"
```

Table 12-1 Log line components

Component	Meaning
LogLevel	One of DEBUG, INFO, ERROR, AUDIT, WARN
DateTime	Double-quoted string in the following format: "yyyy-MM-dd HH:mm:ss.SSS 'GMT'Z"
ClientIP	Numeric client IP address of the original request. It shouldn't be a host name. If there is no client involved for some logging, the application should set the value to 0.0.0.0.
Component	The name of the software module that creates the logging. For example: Validation Server.
Session ID	A numerical string that uniquely represents the session at which the log is created. This is optional and applies only to the `vipegconsole` log.
TransactionID	An identifier for an operation that may involve multiple logging events. It is optional. If it doesn't apply to the application, it should set the value to '0'.
ErrorCode	Decimal error code.

Component	Meaning
Message	Comma delimited name-value pairs with predefined names. Each name-value pair is optional, but there must be at least one name-value pair.

Messages

The message component has the following general format:

```
"[text=message,][actor=who,][op=x,][tid=y,][user=user1,]"
```

A message consists of comma-delimited name-value pairs with predefined names. Each name-value pair is optional, but at least one name-value pair must be present. The message component is always double quoted. It uses the reserved names that are listed in Table 12-6.

Table 12-2 Message names

Name	Value
text	Log message.
actor	The ID of the user who has requested the operation. The provisioning administrative module uses this parameter most.
op	An operation name. Operation names are published for parsers to use.
user	The ID of the end user on whom the requested operation acts.
clientip	IP address of client host.
component	Application making the request.
error	Error code.

Additional name-value pairs can be used for operation-specific reporting.

Certain characters must be treated specially in the log file format:

- Logging line components are separated using spaces.
- Inside the message component, the delimiter for the name-value pairs is a comma, which can appear with or without a following space.
- A message component that contains a space (such as the date and time) must be placed in ASCII double quotes. Quoting a component that does not contain a space makes no difference to the value.
- Double-quote characters, commas, and backslashes that appear in message text or values must be escaped with a backslash as “\"”, “\,”, and “\\” so that log file utilities can easily determine the extent of the message fields.

In the following example, the message section contains two double quotes (one in the text value and one in the incorrect tid value) and a comma. All are escaped inside the regular double quotes.

```
INFO  "2013-07-03 19:32:40.855 GMT+0530" 127.0.0.1 vipegconsole 6db5dabc55093f8f 0
"actor=admin,text=VCAddServerAction1\, validationType = USERID-LDAPPASSWORD-USERID-OTP\,
tokenType = IN-CLOUD"
```

Logging Detail Levels

Table 12-3 describes the logging levels that are provided in VIP Enterprise Gateway

Table 12-3 VIP Enterprise Gateway logging levels

Setting	Action
DEBUG	The log captures all possible transaction details, including stack traces of all exception events.

Table 12-3 VIP Enterprise Gateway logging levels

Setting	Action
INFO	The log captures the general details that are needed to track how the server functions.
WARN	The log captures details of potentially harmful events: rejected transactions and exception events, which affect the server.
ERROR	The log captures details on the events that hinder the server or transaction, but allow the server to function (the exception events that affect the server).
AUDIT	The log captures details of each and every transaction performed by the administrator such as authentication success and failure, configuration changes.

The default logging level is 'INFO' for all the modules. Each module has the configuration setting that can override this default logging level.

Table 12-4 lists the type of log files and describes their content:

Table 12-4 Log file types and contents

Type	Content	Log File Location
`startup`	Events and errors during startup of servers.	<VRSN_MAUTH_HOME>\logs
`vipegconsole`	Configuration and deployment events and errors in the Configuration Console.	<VRSN_MAUTH_HOME>\logs
`server`	Server transactions and errors.	<VRSN_MAUTH_HOME>\Validation\servers\<server_name>\logs
`service`	Events and errors from the `ssp`, `vipmgr`, and `ldapsync` configurations.	For IdP, <VRSN_MAUTH_HOME>\IdP\services\<service_name>\logs where, <service_name> can be SSP or VIPMGR. For LDAP Synchronization, <VRSN_MAUTH_HOME>\LdapSync\services\ldapSync\logs
`jettyServer`	All the logs that the Jetty server produces.	<VRSN_MAUTH_HOME>\logs
`notification`	Notification verifies the connectivity with various VIP User Services.	<VRSN_MAUTH_HOME>\logs

Here are some examples of the kinds of events in each log:

Table 12-5 Log events example

Type	Log Item Example
`startup`	`DEBUG "2016-06-01 11:52:17.940 GMT+0530" ServerCtr "Main :Servers started"`
`vipegconsole`	`AUDIT "2016-06-01 11:53:23.998 GMT+0530" 169.254.1.75 vipegconsole 1965844761 3767425574202839 0 "actor=admin,text=User Successfully Logged In.,op=logon"`

Table 12-5 Log events example

Type	Log Item Example
server	INFO "2014-02-12 17:07:44.875 GMT+0530" 0.0.0.0 ValidationServer 0 0 "text=VSValidationServer._workerThread() -- Started" Thread-3576 VSValidationServer.cpp
service	INFO "2014-02-11 18:52:06.187 GMT+0530" 10.141.18.140 SSP 0 0 0 "actor=SSP,text=Trying in userstore - 1\, total stores configured: 7,op=Authentication"
jettyServer	INFO "2013-06-29 09:58:35.522 GMT+0530" JettyServer "[UserGroupServiceStub.getAllUserGroups] requestId:EG_IP_10_141_149_66_SID_0"

Logging Options

The logging component collects logging information from each VIP Enterprise Gateway component. The level of detail is configurable for each component. The Logging component logs events to text files. You can view the log data from the **Logs** tab. You can specify how your server logs are rotated and the level of the logs to be produced.

Make sure that there is sufficient disk space at all times on your components. If space runs out, VIP Enterprise Gateway is unable to write to the log file. Records of all events during this period are lost.

You can specify how you want your server logs to be rotated, and the level of the logs you want the system to produce. The settings that you can select are listed in Table 12-6.

Table 12-6 Logging parameters

Parameter	Description
Log Rotation Interval	Select an option from the drop-down menu to configure the frequency of your log rotation. For example, if you rotate logs at midnight of each day, your log files for the previous day are archived, and new log files are created. Administrators should take care to archive their own logs.
Default Logging Level	The level of logs you want the system to produce. This logging level is the default for all the Configuration Console components. You can override the default logging level for an individual component by editing its settings and specifying a different logging level. The default logging level is **Info**.
Syslog enable	You can configure Syslog daemon/server as a Syslog Logging server to collect and store most of the VIP Enterprise Gateway logs to that Syslog facility. Before you make this selection, ensure that the Syslog settings have been configured. If not, navigate to Logs > Syslog Settings to configure Syslog settings.
Number of files to keep	Select the number of old log files that the Enterprise Gateway serivce keeps. To determine how many days' logs the server keeps, multiply the Number of files to Keep by the Log File Rotation Interval.

You also have the option to configure each VIP Enterprise Gateway component to a particular logging level.

Higher logging levels require more disk space. You should regularly review and back up your log files to manage disk space and to maintain audit trails.

Logs Tab

This tab enables you to view and download logs of service events. In the VIP Enterprise Gateway configuration console, click **Gateway > Logs**. A list appears, including the current and date-stamped older versions of the following:

- `vipegconsole.log`
- `server.log`
- `service.log`
- `startup.log`
- `jettyServer.log`
- `notification.log`

From this page you can:

- View the file name, size, and last modified date of all available logs. All the logs in the <logdir> directory, the current log, and all old log files are listed on the page.
- View the full text of a specific log. Click **View** in the **Actions** column next to the log you want to view to open the log in the same window. Click Refresh to update the log immediately.

Download a specific log. Click **Download** in the Actions column next to the log you want to download. The log file is saved such that each entry starts with a new line.

VIP Enterprise Gateway Components

The following sections describe the log files for the various VIP Enterprise Gateway components.

Validation Server Logging

The **server.log** collects all the server related activities performed on the validation server. Validation servers logs are written to: `<VRSN_MAUTH_HOME>/Validation/servers/<server-name>/logs`.

Separate logs are written to subdirectories for each Validation server you create.

- The default Log Rotation Interval is one day. When a new log file is generated, the authentication server archives the existing log file.
- To set the number of old log files that the Validation server archives, enter a number for the parameter, Number of Files to Keep.
- To determine the number of days' logs that the server keeps, multiply the Number of Files to Keep by the Log Rotation Interval.

  For example, to keep the logs for 28 days, select 7 for the Log File Rotation Interval. Then, select 4 for Number of Files to Keep. Or 1 for Log File Rotation Interval and 28 for Number of Files to Keep. After 28 days, the server overwrites the oldest archived files.
- The component has server name along with the port number. From the below example, `UO-apache-foundation-http-serv:1812` is the server name and port number.

Note: When the Validation server is configured with all the components in the INFO mode, the size of the log message is typically 3 KB for every Validation Server request.

Example

```
INFO "2016-06-01 13:46:55.369 GMT+0530"  0.0.0.0 UO-apache-foundation-http-serv:1812 0 0
"text=VSValidationServer._initialize() -- Initializing protocol handler" Thread-16032
VSValidationServer.cpp
```

Configuration Console

The **vipegconsole.log** collects all the activities that an administrator performs.

Examples

Example 1: Error logging by vipegconsole module

```
ERROR "2015-01-06 15:16:07.755 GMT+0530" 172.16.156.44 vipegconsole 500830242
d6bee767a54f3dad 18476  "actor=admin,text=Could not bind to the directory server.
```

Example 2: Informational General logging by vipegconsole module

```
INFO  "2015-01-06 15:28:39.794 GMT+0530" 172.16.156.44 vipegconsole 500830242
1a8bb013ca860bf7 0  "actor=admin,text=Update Settings have been changed successfully."
```

Example 3: Information Verbose logging by vipegconsole module

```
DEBUG "2015-01-06 15:27:13.335 GMT+0530" 172.16.156.44 vipegconsole 500830242
d2b64af3f58aaf92 0  "actor=admin,text=Checking status for = SSP. Status: running"
```

Example 4: Warning Log message by SSP module

```
WARN  "2015-01-06 15:48:24.891 GMT+0530" 10.141.18.180 SSP 0 0 0  "text=Invalid polling
interval. Resetting to default 5 minutes.,op=Authentication"
```

Example 5: Audit Logging by vipegconsole module

```
AUDIT "2015-01-06 15:27:13.336 GMT+0530" 172.16.156.44 vipegconsole 500830242
d2b64af3f58aaf92 0  "actor=admin,text=Self Service Portal service has been added and
started."
```

AUDIT Log Format to Capture Configuration Changes

In VIP Enterprise Gateway, the configurations of most of the components are performed in the Configuration Console. VIP Enterprise Gateway creates a log message for such a configuration change.

The format of the Configuration Console log (vipegconsole) has been enhanced to capture the AUDIT log for specific configuration changes. **Session ID,** a unique identifier that is created for every user sign-in, tracks the user sign-in session responsible for the changes. However, this identifier must not be confused with the web application session ID that is used for the HTTP(S) sessions.

The following logging format has been defined for capturing the entire configuration changes in the `TEXT` part of the AUDIT logs:

```
text=TYPE<blank>ATTRIBUTES<blank>OPERATION_VALUES
```

Following are the log format productions rules in the Extended Backus-Naur Form (EBNF) notation:

```
Blank= +U-0020
text=TYPE<Blank>ATTRIBUTES<Blank>OPERATION_VALUES
TYPE = CONF
OPERATION_VALUES = ADD_VALUES | EDIT_VALUES | DEL_VALUES
ADD_VALUES = ADD<blank>VALUE
EDIT_VALUES = EDIT<blank>VALUE<blank>VALUE
DEL_VALUES = DELETE<blank>VALUE
VALUE = <alpha numeric>+
ATTRIBUTES = CLASSES [.]PROPERTIES
CLASSES = CLASS | CLASS(INSTANCE) | CLASSES.CLASS(INSTANCE)
CLASS = <alphanumeric>+
INSTANCE = <alphanumeric>*
PROPERTIES = PROPERTY_NAME | PROPERTY(PROPERTY_NAME)
PROPERTY_INSTANCE = <alphanumeric>+
PROPERTY = property
PROPERTY_NAME = <alphanumeric>*
```

These production rules support the following three types of configuration changes:

- ADD - On adding a configuration, each line of addition is logged as an ADD operation in the following format:

  ```
  TYPE<BLANK>ATTRIBUTES<BLANK>ADD<BLANK><NEWVALUE>
  ```

  For example, configuring the user search filter as %s as part of configuring the first user store

  ```
  CONF uerstoreIndex(0).connectionIndex(0).property(ldap.userFilterFormat) ADD cn=%s"
  ```

- EDIT - On editing a configuration, each line of modification is logged as an EDIT operation in the following format:

  ```
  TYPE<BLANK>ATTRIBUTES<BLANK>EDIT<BLANK>NEWVALUE<BLANK>OLDVALUE
  ```

  For example, modifying the user search filter as samAccountName=%s

  ```
  CONF uerstoreIndex(0).connectionIndex(0).property(ldap.userFilterFormat) EDIT
  samAccountName=%s cn=%s"
  ```

- DELETE - On deleting a configuration, each line of deletion is logged as a DELETE operation in the following format:

  ```
  TYPE<BLANK>ATTRIBUTES<BLANK>DELETE<BLANK>OLDVALUE
  ```

  For example, deleting the user search filter: samAccountName=%s

  ```
  CONF uerstoreIndex(0).connectionIndex(0).property(ldap.userFilterFormat) DELETE
  samAccountName=%s"
  ```

The following scenario explains how the configuration changes are logged in the `TEXT` part of the AUDIT logs:

An administrator has been assigned with installing and configuring VIP Enterprise Gateway for **Colossal Corporation**. After you install VIP Enterprise Gateway, the administrator signs in as `admin`. The administrator performs all the initial configurations and then proceeds to configure the User Store US_1. When you add a new User Store, all the configurations are logged as ADD operations. The following table lists the AUDIT log files that are created for configuring the user store US_1:

Note: The Session ID and the Transaction ID are highlighted in the first row of the AUDIT log file for reference purposes.

Table 12-7 Add User Store - AUDIT logs for ADD operation

```
AUDIT "2014-01-27 16:28:00.206 GMT+0530" 10.141.16.34 vipegconsole 30000826 b962ffedc1cfcd42
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(dnsName) ADD
COLOSSAL.COM"
AUDIT "2014-01-27 16:28:00.206 GMT+0530" 10.141.16.34 vipegconsole 30000826 b962ffedc1cfcd42
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(ldap.baseDN) ADD
cn=users\,dc=colossal\,dc=com"
AUDIT "2014-01-27 16:28:00.207 GMT+0530" 10.141.16.34 vipegconsole 30000826 b962ffedc1cfcd42
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(ldap.cloudAttribute)
ADD cn"
.......
.......
AUDIT "2014-01-27 16:28:00.212 GMT+0530" 10.141.16.34 vipegconsole 30000826 b962ffedc1cfcd42
0  "actor=admin,text=CONF
userstoreIndex(0).connectionIndex(0).property(ldap.userFilterFormat) ADD cn=%s
```

After a month, **Colossal Corporation** decided to change the group filter that is part of the search criteria. The administrator modified the User Filter to `samaccountname=%s`. and the AUDIT log files are now logged as EDIT operations. The log files created for this modification are described as follows:

Table 12-8 Edit User Store Configuration - AUDIT logs for EDIT operation

```
AUDIT "2014-02-27 16:29:36.191 GMT+0530" 10.141.16.34 vipegconsole 30000826 4a55375e1318a8c8
0  "actor=admin,text=CONF
userstoreIndex(0).connectionIndex(0).property(ldap.userFilterFormat) EDIT samaccountname=%s
cn=%s"
```

After a year, **Colossal Corporation** decided to decommission the User Store US_1. The AUDIT log files that are created for these operations are logged as DELETE operations described as follows:

Table 12-9 Delete User Store - AUDIT logs for DELETE operation

```
AUDIT "2015-01-27 16:30:38.633 GMT+0530" 10.141.16.34 vipegconsole 30000826 2b850bbb5fbc3989
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(dnsName) DELETE
COLOSSAL.COM"

AUDIT "2015-01-27 16:30:38.633 GMT+0530" 10.141.16.34 vipegconsole 30000826 2b850bbb5fbc3989
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(ldap.baseDN) DELETE
cn=users\,dc=colossal\,dc=com"

.....

.....

AUDIT "2015-01-27 16:30:38.640 GMT+0530" 10.141.16.34 vipegconsole 30000826 2b850bbb5fbc3989
0  "actor=admin,text=CONF userstoreIndex(0).connectionIndex(0).property(netbiosName) DELETE
COLOSSAL"
```

IdP Service

The **service.log** captures the events recorded in Self Service Portal (SSP IdP) and VIP Manager (VIPMGR). The following are the location of the service.log files under different components:

- For SSP IdP - `<VRSN_MAUTH_HOME>/IDP/services/SSP/logs`
- For VIP Manager - `<VRSN_MAUTH_HOME>/IDP/services/VIPMGR/logs`

You can also refer the **service.out** log for details on starting and stopping the IdP service.

Example

Example 1: SSP IdP

```
INFO  "2016-04-14 15:27:28.661 GMT+0530" 192.168.7.165 SSP 0 0 0 1423299933
"actor=SSP,text=Authenticating user - 2k3sanuser,op=Authentication"
```

Example 2: VIP Manager

```
INFO  "2016-04-14 14:31:47.380 GMT+0530" 192.168.7.165 VIPMGR 0 0 0 11560079 4
"actor=VIPMGR,text=Server started on port 8234,op=Authentication"
```

LDAP Directory Synchronization

The **service.log** captures the events recorded in LDAP Directory Synchronization logs are written to: `<VRSN_MAUTH_HOME>/LdapSync/services/ldapSync/logs`

The following are three types of log files:

- service.log - Captures the details of the LDAP directory synchronization
- service.out - Captures the start and stop services
- simulation.log - Captures the details of the LDAP directory synchronization under simulation

Syslog Logging

Although VIP Enterprise Gateway log files can be viewed from Configuration Console, this may not be a practical way of monitoring what happens in the system. You can configure the syslog server as a syslog logging server to collect and store most of the VIP Enterprise Gateway logs. The logs are still stored in files.

By default, VIP Enterprise Gateway uses the LOG_LOCAL0 facility for syslog. In the default configuration, all syslogs for the LOG_LOCAL0 facility go to /var/log/messages. To configure a different location for syslogs, update the `/etc/syslog.conf` file as described:

Note: The log levels you configure for the VIP Enterprise Gateway in Configuration Console override the log levels you set here.

---

1 Set the syslog facility level to the same as what is set in VIP Enterprise Gateway Configuration Console. For example:

```
local0.*  /var/log/vipeg_9_8.log
```

Where * indicates the levels of logging.

Refer to the `syslog.conf` main page for more details on customized configurations.

2 Send a SIGHUP signal to the syslog process.

You can use the following filters in the syslog server to categorize the logs according to VIP Enterprise Gateway components:

Table 12-10 VIP Enterprise Gateway log filters

Filters	Description
vipegconsole	To filter the logs that are related to VIP Enterprise Gateway console.
SSP	To filter the logs that are related to VIP Enterprise Gateway Self Service Portal.
VIPMGR	To filter the logs that are related to VIP Enterprise Gateway VIP Manager IdP.
LDAP Sync	To filter the logs that are related to VIP Enterprise Gateway LDAP Directory synchronization.
ValidationServer	To filter the logs that are related to VIP Enterprise Gateway Validation server.
JettyServer	To filter the logs that are related to VIP Enterprise Gateway Jetty Server logs.

If you want to get all the logs related to VIP Enterprise Gateway components, use all the filters described in Table 12-10.

Syslog supports large messages without any message truncations. You can view a unique sequence number with each individual line of syslog. This sequence number acts as the identifier for the line of log. If the message is larger than 1024 Bytes, VIP Enterprise Gateway splits the message in the application-level and introduces tags to identify the continuity.

Configuring Syslog

You can configure VIP Enterprise Gateway to send log messages to your syslog daemon.

To configure the syslog settings:

1 Navigate to **Logs > Syslog Configuration** to access the Syslog Configuration page.

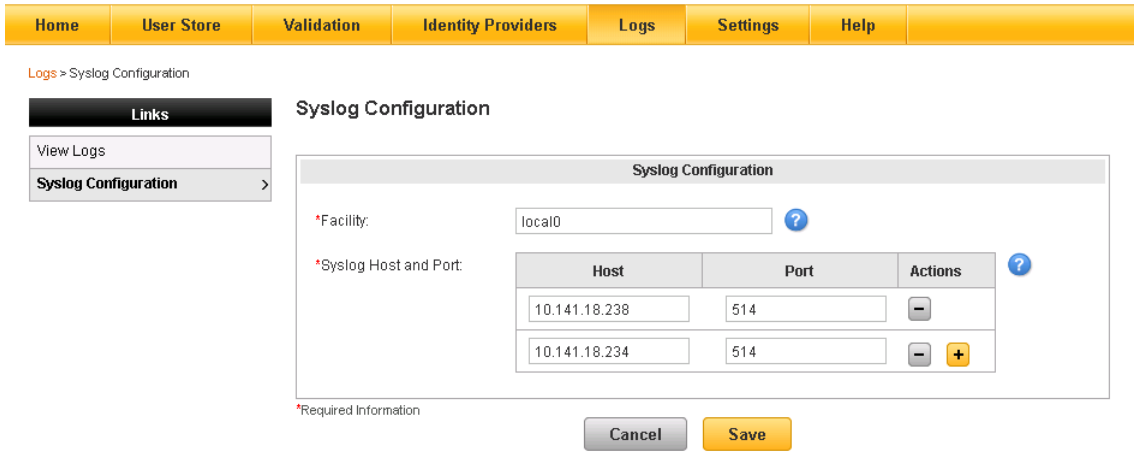

Figure 12-1 Syslog Configuration page

2 Set the appropriate facility level for logging, for example local0.

3 Enter the host name or the IP address of the system that runs the syslog daemon.

4 Enter the port number to which the service will listen to. The default port number is 514.

5 Click **Save** to save the configuration settings.

You can configure VIP Enterprise Gateway to send the log messages to multiple syslog servers simultaneously. By configuring multiple servers, the log messages are not lost if one of the servers is not accessible for a certain duration.

To add another syslog server to the existing configuration:

1 Click the plus icon in the Actions column against the primary syslog server entry.

2 Enter the host name and the port number, and then click **Save** to save the new configuration settings.

Handling Larger Messages

If the log message is larger than 1024 bytes, VIP Enterprise Gateway splits the message into multiple log messages. While receiving these logs, you can identify these messages using the tags and unique ID.

```
<unique_ID> <total_number_of_messages>_<current_message_number>
```

For example, `571620528 15_0`.

where, `571620528` is the unique ID and large messages are split into 15 smaller messages starting with `15_0`.

Example

```
Apr 20 07:55:16 192.168.7.1  ERROR "2016-04-20 20:25:16.753 GMT+0530" 169.254.1.75
vipegconsole 1803174971 6721700995016865 18478 571620528  15_0 "actor=admin,text=R "2016-04-20
20:2      5:16.753 GMT+0530" 169.254.1.75 vipegconsole 1803174971 6721700995016865 18478
571620528 "actor=admin,text=Could not bind to the directory server.^M VsException
[error=18478] [javax.      naming.AuthenticationException: [LDAP: error code 49 - 80090308:
LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1

....

....

Apr 20 07:55:17 192.168.7.1  ERROR "2016-04-20 20:25:16.758 GMT+0530" 169.254.1.75
vipegconsole 1803174971 6721700995016865 18478 571620528 15_14 "actor=admin,text=
com.verisign.ldap.BaseLdapClient.getConnectio     n(BaseLdapClient.java:74)      ... 109 more
"
```

Chapter 13

Exporting and Importing Configuration Settings

In VIP Enterprise Gateway, you can use the Export and the Import features to transfer the configuration settings from one instance of VIP Enterprise gateway to another. Typically, this feature helps you maintain identical configuration settings on all VIP Enterprise Gateway instances in your environment.

Exporting Configuration Settings

You can use the **Export** option to export the configuration settings to the VIP Enterprise Gateway server. The exported configuration settings are saved as a `.zip` file. VIP Enterprise Gateway provides you the option to encrypt this `.zip` file using a password, if required.

VIP Enterprise Gateway exports the following configuration settings:

- User Store Settings
- Proxy Settings
- Syslog Settings
- Self Service Portal IdP
- VIP Manager IdP

Note: If the VIP Enterprise Gateway server is configured with HTTPS, you cannot export the SSL certificates for the Console, VIP Manager, and SSP IdP.

- LDAP Synchronization
- Automatic Business Continuity
- LiveUpdate Settings
- Validation servers

Note: This includes Tunnel Forwarders, Tunnel Receivers, and all the modes of Validation servers.

The VIP Enterprise Gateway Console Settings are not exported. You must configure the Console Settings in the VIP Enterprise Gateway host where you import the configuration settings. For the procedure on exporting configuration settings, refer to *Symantec VIP Enterprise Gateway Online Help*.

Importing Configuration Settings

VIP Enterprise Gateway allows you to reuse the configuration settings among the same version and cross-version from 9.1 onwards. You can export the configuration settings from one VIP Enterprise Gateway instance and import the settings to the other instances.

To import the configuration settings to a VIP Enterprise Gateway instance:

1. Navigate to **Settings** > **Import Settings**.
2. Click **Import**.
3. Browse and select the file to be imported.
4. Select the configuration settings to be imported.
   - Same version import - You cannot import the settings that are already existing in the VIP Enterprise Gateway instance. These settings will be displayed as read-only on the Import Configuration panel during an import.
   - Cross-version import - After you configure a new instance of VIP Enterprise Gateway, you can import the configuration settings from an existing instance of VIP Enterprise Gateway. VIP Enterprise Gateway 9.8 supports cross-version import from 9.1 onwards.

     If you already have CA certificates on the existing instance of VIP Enterprise Gateway, these CA certificates will be overwritten during the import. However, you cannot restore any components configured in Enterprise Gateway 9.8 after performing the cross-version import. All the existing settings will be replaced after the import.
5. Click **Finish** to complete the import of the configuration settings.

Refer to the *VIP Enterprise Gateway online help* for more information on importing a configuration settings file.

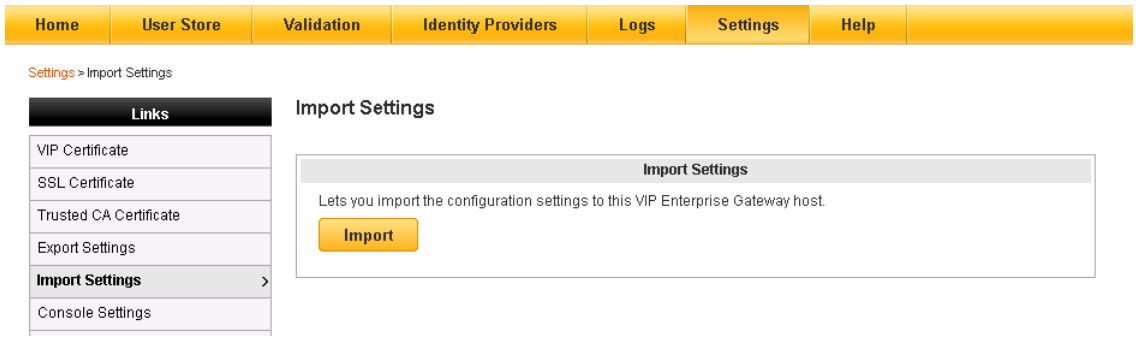

Figure 13-1 Import settings

Limitations of Importing the Configuration Settings

This section provides a list of the limitations of importing the configuration settings:

- During the import, administrators created using Password tool (`passwordtool.bat`) from the previous version of Enterprise Gateway will not be imported. You have to recreate the administrators in the new instance of Enterprise Gateway.
- If LDAP is communicated over SSL channel (LDAPS), and cross-version import is performed on a new system, then CA certificate needs to be added in Windows Cryptographic Application Programming Interface (CAPI). (Windows only).

Same version limitation

The following are the limitations if Enterprise Gateway has two instances running the same version.

- The following settings cannot be imported on the VIP Enterprise Gateway instance that is configured with a User Store:

- Self Service Portal IdP
- VIP Manager IdP
- LDAP Directory Synchronization

- If the Validation server that you want to import and the Validation server that is already available in your VIP Enterprise Gateway have the same name, the Validation server that you import is added as a new one to VIP Enterprise Gateway. The string *_imported* is appended to the new server name.

Cross version limitation

- If you are importing VIP Enterprise Gateway 9.1 onwards to the latest version, all the existing settings available on your latest Enterprise Gateway will be replaced. You cannot restore any components configured in the latest version of Enterprise Gateway after performing the cross-version import.

General Import Configuration Settings

- The VIP Enterprise Gateway servers must use the same platform type to enable exporting and importing of the configuration settings.
- If the VIP Enterprise Gateway server from which you export the configuration settings is configured with HTTPS, you cannot import the SSL certificates configured for VIP Manager and SSP IdP. As the VIP Enterprise Gateway administrator, you must configure new certificates on the target VIP Enterprise Gateway server to configure it to use HTTPS.
- If you are importing SSP IdP components with password reset enabled, you need to select https (SSL Enabled) in the Protocol field, add domain names for SSP IdP and Load Balancer in VIP Manager.

Once the import process is complete, Symantec recommends you to run the vipdiagnostic tool to collect the diagnostic data when there is an unexpected connectivity issue in VIP Enterprise Gateway. See “Using the vipdiagnostic Utility” on page 104.

Appendix A

Upgrading to VIP Enterprise Gateway Version 9.8

This appendix includes the following topics:

- "Upgrading to VIP Enterprise Gateway Version 9.8" on page 97
- "Applying VIP Enterprise Gateway Updates Manually" on page 98

If you are running a previous version of VIP Enterprise Gateway, you can upgrade your configuration to VIP Enterprise Gateway version 9.8. When you upgrade to VIP Enterprise Gateway version 9.8, you do not have to meet the prerequisites or do many of the configurations required for a new installation. The VIP Enterprise Gateway version 9.8 retains your existing configurations.

Upgrading to VIP Enterprise Gateway Version 9.8

You can upgrade VIP Enterprise Gateway through the LiveUpdate server or you can download the updates from VIP Manager and perform the upgrade operation manually.

Note: On Linux, the user who upgrades VIP Enterprise Gateway to version 9.8 must be the same user who installed the previous version of VIP Enterprise Gateway.

See "Upgrading VIP Enterprise Gateway" on page 77.

You can upgrade to VIP Enterprise Gateway version 9.8 on the following Linux and Windows platforms:

Table 14-1 Platforms that support upgrade

Linux: ■ RHEL 5.9 (64 bit) ■ RHEL 5.10 (64 bit) ■ RHEL 5.11 (64 bit) ■ RHEL 6.4 (64 bit) ■ RHEL 6.5 (64 bit) ■ RHEL 6.6 (64 bit) ■ RHEL 7.0 (64 bit) ■ RHEL 7.1 (64 bit)
Windows: ■ Windows 2012 R2 x64 ■ Windows 2012 x64 ■ Windows 2008 x64 (Service Pack 2) ■ Windows 2008 R2 x64 (Service Pack 1)

Applying VIP Enterprise Gateway Updates Manually

This topic describes how to apply the VIP Enterprise Gateway updates manually. The `<VRSN_MAUTH_HOME>` directory in the following procedures refers to the directory where VIP Enterprise Gateway is installed.

Note: On Windows, you must always run the command prompt as a user with administrator privileges to apply the updates manually.

On Linux, you must run the following commands as a root user to apply the updates manually. Also, on Linux, run the `setup.sh` file as a sudo user who does not require a password for the sudo operations. For more information on how to add a user to `/etc/sudoers`, refer to the Linux documentation.

See "Linux sudoers File Settings for VIP Enterprise Gateway" on page 14.

---

1. From VIP Manager, download the `VIP_Windows_Package_9_8_0.zip` file (for Windows) or the `VIP_Linux_Package_9_8_0.tar` file (for Linux) that contains the VIP Enterprise Gateway update you want to apply.
2. Unzip the file and extract the contents to a temporary location.

   For example:

   - On **Windows:** C:\temp\,
   - On **Linux:** /tmp/).
3. Back up the `<VRSN_MAUTH_HOME>\tools\actionScript.jar` file.
4. Copy the `actionScript.jar` file from the extracted folder to the `<VRSN_MAUTH_HOME>/tools` directory.

   For example:

   - On **Windows:** copy from `C:\temp\VIP_Windows_Package_9_8_0` to the `<VRSN_MAUTH_HOME>\tools` directory
   - On **Linux:** copy from /`tmp`/`VIP_Linux_Package_9_8_0` to the `<VRSN_MAUTH_HOME>/tools` directory.
5. Open the Command Line Interface, and navigate to `<VRSN_MAUTH_HOME>/tools` directory.
6. Do the following:

   - On Windows, run the `actionScript.bat` script.
   - On Linux, run the `actionScript.sh` script.

   Usage on Windows: `actionScript.bat <Location of the extracted package> <Version of the update>`
   For example, `actionscript.bat "C:\temp\VIP_Windows_Package_9_8_0\" 9.8.0`

   Usage on Linux: `actionScript.sh <Location of the extracted package> <Version of the update>`

   For example, `actionscript.sh "/tmp/VIP_Linux_Package_9_8_0" 9.8.0`
7. After successful update, start all the required services.

   Note: On Linux, you must start the VIP Enterprise Gateway service manually.

Appendix B

Uninstalling VIP Enterprise Gateway

This chapter includes the following topics:

- "Uninstalling VIP Enterprise Gateway Version 9.8" on page 99
- "Restoring the Previous Version of VIP Enterprise Gateway" on page 100
- "All components that you configured previously are now restored. However, you need to restart them." on page 100

This appendix describes how to uninstall VIP Enterprise Gateway version 9.8 and how to restore the previous version of VIP Enterprise Gateway.

Uninstalling VIP Enterprise Gateway Version 9.8

Complete the following procedures to uninstall VIP Enterprise Gateway version 9.8. On Windows, you must have administrator access to the computer to uninstall these components. On Linux, you must be the same user who installed VIP Enterprise Gateway.

After you have uninstalled VIP Enterprise Gateway version 9.8, you can restore your previous version of VIP Enterprise Gateway.

See "Restoring the Previous Version of VIP Enterprise Gateway" on page 100.

Uninstalling on Windows

Before you start, ensure that you have not opened any command prompts, file browsers, or file dialog boxes to the directory where VIP Enterprise Gateway components are installed. Windows does not allow directories to be removed when they are open anywhere in the system.

To uninstall, go to **Control Panel** > **Add or Remove Programs** > **VIP Enterprise Gateway**.

Uninstalling on Linux

For Linux, run the appropriate command on your VIP Enterprise Gateway machine to uninstall VIP Enterprise Gateway version 9.8.

If you have performed a fresh installation of VIP Enterprise Gateway version 9.8 or upgraded from 9.7, then navigate to the `<install_dir>` directory and run the `./uninstall` command as a sudo or a root user. The `<install_dir>` is the directory where you installed VIP Enterprise Gateway version 9.8. For example,

```
[root@colossal-rhel62-166 VIP_Enterprise_Gateway]# ./uninstall
```

Restoring the Previous Version of VIP Enterprise Gateway

Note: When you upgrade VIP Enterprise Gateway to version 9.8, the restore script (`restoreVIPEG97.vbs` (for Windows) and `restoreVIPEG97.sh` (for Linux)) is copied to the backup directory. For example, on the Windows platform, you can find the `restoreVIPEG97.vbs file` at:
`C:\....\Symantec\VIP_Enterprise_Gateway9.7.bak\tools\restoreVIPEG97.vbs`

After you uninstall VIP Enterprise Gateway version 9.8, complete the following procedures to restore VIP Enterprise Gateway 9.7:

To restore VIP Enterprise Gateway 9.7, you require the following:

- Installation scripts and documentation for VIP Enterprise Gateway 9.7.
- Installation `.zip` (Windows) or `.tar` (Linux) files for VIP Enterprise Gateway 9.7
- The path to the backup directory that was created when you upgraded to VIP Enterprise Gateway version 9.8. Typically, this path is `C:\Program Files\Symantec\VIP_Enterprise_Gateway9.7.bak` (Windows) or `/opt/Symantec/VIP_Enterprise_Gateway9.7.bak` (Linux).

1. Reinstall VIP Enterprise Gateway version 9.7 using the appropriate installation scripts. You must reinstall in the same directory in which it was originally installed.
2. After you install VIP Enterprise Gateway 9.7, stop the VIP Enterprise Gateway service.
3. Navigate to the `VIP_Enterprise_Gateway9.7.bak\tools` directory and run the restore script based on the platform on which you have installed VIP Enterprise Gateway:
   - On Windows, run `restoreVIPEG97.vbs`
   - On Linux, run `restoreVIPEG97.sh`

   You are prompted for the following:
   - Path to the backup directory that was created when you installed VIP Enterprise Gateway version 9.8.
   - Path where you installed VIP Enterprise Gateway 9.7.
4. Restart the VIP Enterprise Gateway service.
5. All components that you configured previously are now restored. However, you need to restart them.

Appendix C

Default Ports and Protocols

This chapter includes the following topics:

- "List of Default Ports and Protocols" on page 101
- "Restricted Ports" on page 102

This appendix lists the default ports and protocols VIP Enterprise Gateway expects. You can change these ports using the Configuration Console. To avoid conflicts on the listed ports, make sure that no other services you have installed listen on these ports. Otherwise, change the default in the Configuration Console.

List of Default Ports and Protocols

Table 16-1 lists the default ports and protocols in VIP Enterprise Gateway. The URL spaces for RADIUS components are left blank because the users can determine these.

Table 16-1 Default ports and protocols in VIP Enterprise Gateway

Component	Protocol	Direction	URL	Port No.
Secure access to VIP Self Service Portal by end users	http/https	Inbound	http://<host_name_or_IP>:8233/vipssp	8233
Secure access to VIP Manager by administrators	http/https	Inbound	http://<host_name_or_IP>:8234/vipmgr	8234
Access to VIP Enterprise Gateway Configuration Console by administrators	http/https	Inbound	http://<host_name_or_IP>:8232/vipegconsole	8232
LDAP Directory Synchronization Service	http (service management)	Internal only	http://localhost:8235	8235
SSP IdP Proxy Service	http/https	Internal only	http://<host_name_or_IP>:8236/vipsspdmz	8236
LDAP communication from VIP Enterprise Gateway	LDAP LDAP (SSL)	Outbound		389 636 (SSL) 3268 3269 (SSL)
VIP Enterprise Gateway communicating with VIP Authentication Service	https	Outbound	■ https://userservices-auth.vip.symantec.com ■ https://userservices.vip.symantec.com	443
User access to Symantec VIP Self Service Portal	https	Outbound	https://ssp.vip.symantec.com	443

Table 16-1 Default ports and protocols in VIP Enterprise Gateway

Component	Protocol	Direction	URL	Port No.
Administrator access to Symantec VIP Manager	https	Outbound	https://manager.vip.symantec.com	443
VIP Enterprise Gateway communicating with Symantec LiveUpdate service	http	Outbound	liveupdate.symanteclive update.com	80
Syslog	UDP	Outbound		514
Validation Service listening for requests from client applications	RADIUS	Inbound		1812 **Note:** This port is the default for all RADIUS servers. If you have any other RADIUS servers running on this computer (such as IIS), do not use this default port for the Validation Service.
SMTP Server	SMTP	Outbound		25
More information on Symantec LiveUpdate service	https	Outbound	https://knowledge.symantec.com	443
Access to Symantec pages	http	Outbound	http://www.symantec.com	443

Restricted Ports

Applications use the following ports. You must not configure them for use with VIP Enterprise Gateway components.

Table 16-2 Restricted Ports

Application	Restricted Port
Firefox browser	601

Appendix D

VIP Enterprise Gateway Utilities

This chapter includes the following topics:

- Using the packTrustCA utility
- Using the vipdiagnostic utility

This appendix provides an overview and the procedure for using the VIP Enterprise Gateway utilities.

Using the packTrustCA Utility

To make the process of replicating the trust of CAs across multiple instances of VIP Enterprise Gateway easier, the `packTrustCA` utility is included. For example, use this utility to copy the trusted CAs from your Configuration Console host to all Enterprise Gateway servers you may have installed on separate computers.

Note: The `packTrustCA` tool replicates VIP Enterprise Gateway-related CAs only. If you have loaded CAs to your system outside the VIP Enterprise Gateway system such as Microsoft Windows CAPI, these CAs are not replicated. You must manually add these CAs to your system.

Complete the following procedures to run this utility:

1. From a command prompt on the computer where you have installed and trusted the CAs, access the `<VRSN_MAUTH_HOME>/tools` directory.
2. Run the appropriate utility:
   - packTrustCAs.bat (Windows)
   - packTrustCAs.sh (Linux)

   The utility creates the `TrustedCAs.pak` file and displays a checksum. You may choose to make a note of the checksum value for confirmation when replicating the trusted CAs.

   Note: If a previous version of `TrustedCAs.pak` exists in the `tools` directory, the new version overwrites it.

   ---
3. Copy the `TrustedCAs.pak` file to the `<VRSN_MAUTH_HOME>/tools` directory on the other computer.
4. From a command prompt, run the appropriate utility:
   - `unpackTrustCAs.bat` (Windows)
   - `unpackTrustCAs.sh` (Linux)

   After you run the utility, a checksum is displayed. You can compare it to the checksum that is obtained in Step 2.
5. Restart VIP Enterprise Gateway.

   Navigate to **Settings** > **Trusted CA Certificate** to verify that the trusted CA certificates were updated.

Repeat Step 3 through Step 5 for each separate installation.

Using the vipdiagnostic Utility

Run the vipdiagnostic utility to collect the diagnostic data when there is an unexpected connectivity issue in VIP Enterprise Gateway. The diagnostic data is collected in the log file, which can be used to analyze the issue in detail.

To run the utility:

1. Go to the Tools folder in the VIP Enterprise Gateway install directory.
2. Run the following command:

   For Windows, `vipdiagnostic.bat [option] [--LogFile file] [--LogLevel level]`

   For Linux, `vipdiagnostic.sh [option] [--LogFile file] [--LogLevel level]`

   where:

   <*option*> can take the following values:

--All	Run all the tests except the loop test. This is the default option.
--LDAP	Run all the LDAP connectivity tests.
--Cloud	Run all the Cloud connectivity tests.
--Misc	Run all the miscellaneous tests excluding LDAP and Cloud connectivity tests.
--Loop [--LoopCount count]	Run the Cloud and LDAP connectivity tests in a loop. ■ The loop count can be given using LoopCount switch. The default value is 10. ■ Example: vipdiagnostic.bat --Loop --LoopCount 5 ■ This will help in finding intermittent connectivity issues.

   <*LogLevel*> can be INFO, DEBUG, WARN, or ERROR. INFO is the default log level.

   <*LogFile*> by default, is <VRSN_MAUTH_HOME>/logs/vipDiagnostic.log.

Appendix E

Troubleshooting

This chapter includes the following topics:

- "List of Error Codes" on page 105

If your users experience issues with VIP Enterprise Gateway, refer to the VIP Enterprise Gateway log files.

List of Error Codes

Table 18-1 lists the reason codes you may encounter in the Validation server log, and provides some solutions. Set the logging level to DEBUG to view these reason codes.

Table 18-1 Validation server reason codes

Error Code	Cause	Solution
0	Success.	As stated.
1	No token is assigned to the user.	Assign a credential to the user or select another user.
3	The first-factor validation failed. This problem is typically due to an incorrect user name or password value.	Correct the user name and/or password or select another user.
6	The user store is not accessible.	Verify that the user store is accessible.
7	The user was not found in the user store.	Add the user or select another user.
8	The password is incorrect.	Enter a valid user password.
11	The user does not have an enabled credential.	Assign a credential to the user, or select another user.
12	If the Validation Server is configured in the User ID - Access PIN - Security Code mode, this error could be because of an incorrect Access PIN or security code. If the Validation Server is configured in any of the other modes, this error is due to an incorrect security code.	Enter a valid Access PIN or security code.
14	The credential state is new. Credentials must be assigned to a user and in the enabled state to be used for validation.	Register and activate the credential before the user can use it for authentication.
15	The credential is disabled. Credentials must be assigned to a user and in the enabled state to be used for validation.	Enable the credential or choose one that is already enabled.
16	The credential is Locked. Credentials must be assigned to a user and in the enabled state to be used for validation.	Unlock the credential or choose one that is already unlocked.

Table 18-1 Validation server reason codes

Error Code	Cause	Solution
17	The credential is Inactive. Credentials must be assigned to a user and in the enabled state to be used for validation.	Activate the credential or choose one that is already active.
18	The credential(s) are in mixed states, but none are enabled. Credentials must be assigned to a user and in the enabled state to be used for validation.	Enable a credential or choose one that is already enabled.
20	This account or administrator does not have the correct permissions to perform this operation.	Retry the operation with the correct permissions.
22	The credential operation you requested is not valid for this credential type.	Select an operation that is valid for this credential type.
23	The user you selected does not exist in the VIP Authentication Service.	Select a valid user or add the user to the VIP Authentication Service (using the VIP Manager or VIP Web Service).
24	Access PIN validation failed. This problem is typically due to an incorrect Access PIN.	Enter a valid Access PIN.
25	Sending Push to device failed.	Verify whether VIP Access Push is enabled on the user accounts and the devices. Also, verify whether the push-enabled VIP credentials are registered with the VIP Service.
26	Push request timed out.	Retry and press **Allow** or **Deny** on the push message within the time interval specified for completing the second-factor authentication.
27	Push request approved.	As stated.
28	Push request denied.	As stated.
29	Push request changed (overwritten by another request).	Submit another VIP Access Push request only after the first request is Timed out, approved, or denied.
32	Access PIN expired.	Select the **Enable Users to Reset Expired PIN** check box in the Validation Server.
33	User PIN is not enabled for this account.	Enable the **End user PIN** option in the VIP account.
34	Schema validation failed.	Retry the operation with the correct value.
40	Invalid access challenge. Credentials must be used when they are in enabled state for validation. In this case, the credentials were disabled in the validation server due to a timeout,	Use the credential when it is in active state.
41	Error fetching RADIUS authoring attributes. This error may indicate that attribute was not able to fetch LDAP to RADIUS mapping	Active Directory administrator should verify the attribute defined.
42	Automatic Business Continuity second factor. During Business continuity, if you enter an invalid security code, it fails to authenticate.	Enter a valid second factor code and try again.

Table 18-1 Validation server reason codes

Error Code	Cause	Solution
43	Automatic Business Continuity password expired. The Active Directory password expired and must be changed.	Reset your Active Directory password.
44	Failed password mismatch. The problem is due to an incorrect password entered in the confirm password field and password is not matching,	Retry the operating with the correct password.
45	PasswordExpiredAccessChallengeDisabled.	Change the password and configure Validation server to enable access challenge.
46	Access Challenge Timeout User has not entered the security code within the configured access challenge timeout period	Users must be trained and informed to enter security code when prompted. If this problem is recurring for your users, increase the Access-Challenge time out period in the Validation server configuration
47	Invalid input. This error may indicate that an incorrect PIN or security code was entered. It can also be due to the invalid length of PIN or security code.	Enter a valid PIN or security code as input.
48	Connectivity to service is failed.	Verify the network connectivity and try again.
49	InfoCallFailedBizModeOn. Business continuity mode is enabled and info call failed.	Resolve your connectivity issues.
50	PIN does not meet policy. This problem is due to an invalid PIN length while resetting it.	Enter a valid Access PIN.
100	The credential type you selected is not supported for this account.	Select a valid credential type.
101	An internal error occurred. This error may indicate that the VIP account you selected is not valid.	Verify that you access the correct VIP account. If this error persists, contact Technical Support.
150	Access Challenge Timeout. User has not entered the security code within the configured access challenge timeout period.	Educate your users to enter the security code when prompted. If this problem is recurring for your users, increase the Access-Challenge time out period in the Validation server configuration.
151	Access-Challenge buffer full. Many pending responses to the Access-challenge that is thrown to the user.	Increase the watermark level or decrease the Access-Challenge time out period in the Validation server configuration.
152	Access Challenge User Limit exceeded. The user has sent multiple requests with valid user name and LDAP password, but has not responded to the access challenge.	Educate your users to enter the security code when prompted. If this problem is a recurring for your users, increase the number of requests that is allowed per user in the configuration file.

Index

A

accessing the Configuration Console 11, 15
activate your account 9
Add User Store 30
adding
    new Configuration Console administrators 17
    tunnel forwarders 49
    tunnel receivers 50
administrator
    adding 17
    changing the password for 17
    configuring access to VIP Manager for 63
    credential operations 62
    username and password for 5, 11
Administrators in VIP Enterprise Gateway 53
Anonymous Authentication 49
AUDIT log
    configuration changes 88
Automatic Business Continuity
    Configuring 48
autostarting
    tunnel forwarders and receivers 52

B

Basic Authentication 49

C

Certificate Signing Request 20
changing installation directory
    Windows 12
changing the administrator password 17
client application 62
    hardware/software requirements for 8
component testing 73
Configuration Console 39
    accessing 11, 15
    editing settings 23
    overview 1
    password 11, 15
    URL for accessing 17
Configuration Console administrator
    see administrator
Configuration Console host
    testing 73
    user rights 6
Configuration Summary 24
configure
    LDAP Directory Synchronization Service 71
    Self Service Portal IdP 59
    SSP IdP 59
    VIP Manager IdP 65
Configuring
    Automatic Business Continuity 48
configuring
    administrator access to VIP Manager 63
    Configuration Console settings 23
    third-party IDP service 61
    User Stores 27
    Validation service ??-44
considerations for installation 9
    Linux 9
console administrators 56
    using the enterprise credentials to sign-in 56
credential operations using Web services 62
CSR
    see Certificate Signing Request

D

default installation location
    Windows 12
default protocols 101
DMZ 49

E

editing Configuration Console settings 23
end-user credential operations 62
error codes 105
Export configuration settings 93

F

files for installation 5, 10

G

GUI, installation 97-98

H

hardware/software requirements 6
    client application 8
    Linux 7
    User Store 8
    VIP Enterprise Gateway host 6
    Windows 6
HTTP proxy 39, 49

I

Identity Provider 59

IdP 59
Importing Configuration Settings 94
Initial configurations 23
installation considerations
  Linux 9
installation files 5, 10
installation pre-requisites 5
installation testing 73
installing
  using the GUI 97-98
  VIP Enterprise Gateway 9-16
  wizard 97-98
installing on Linux 14
installing on Windows 10-13
  changing the directory 12
installing using wizard 10-13, 14
Internet 39
Issuing Authority 22

L

LDAP directory
  hardware/software requirements 8
LDAP Directory Synchronization
  configure 71
  disparate User Stores 68
  Load-balancing and Failover 68
  Third-party Identity Provider 69
LDAP Directory Synchronization Service 67
  multiple instances 68
license agreement 10
Linux
  Configuration Console host requirements 7
  configuring tunnels to autostart on 52
  hardware/software requirements 7
  installation considerations 9
  installation file for 5
  installing on 14
  Password tool 17
  requirements for Configuration Console on 6, 7
  starting and stopping VIP Enterprise Gateway on 15
  trusted CA replication tool 103
  uninstalling VIP Enterprise Gateway on 99
logging 83

M

manual upgrade 98
Multiple User Stores 27

N

non-public SSL certificates for tunnel forwarder 22

O

outbound port 39
overall operation, testing 75
overview
  Configuration Console 1
  Self Service Portal 59
  tunnel forwarders 49
  tunnel receiver 50
  VIP Enterprise Gateway 1
  VIP Manager 65

P

packTrustCA utility 103
packTrustCAs.bat 103
packTrustCAs.sh 103
password
  administrator 5, 11
  Configuration Console 11, 15
  login information 5
  restrictions 12
password management 36
Password tool, adding new administrator with 17
passwordTool.bat 17
passwordTool.sh 17
platform considerations 9
port, outbound 39
pre-installation steps 1
pre-requisites for installation 5
Product updates
  Checking 77
  Installing 79
proxy server 39, 49
public Issuing Authority 22

R

reboot
  configuring tunnels to autostart after 52
replicating trusted CA certificates 22
requirements
  client application 8
  hardware and software 6
  LDAP directory 8
  User Store 8
  VIP Enterprise Gateway host 6
reset LDAP password 36
restrictions
  password 12

S

Searching User Stores 28
secure access 59
  VIP Manager 65
securing communications with VIP Authentication Service 19
security code validation, testing 75
Self Service Center Portal
  URL 59
Self Service Portal
  configuring third-party IDP service for 61
  overview 59
  secure access to 59
  Service Status 59
  testing the 73
Service Status
  Self Service Portal 59

VIP Manager 65
setup.exe 10
shutdown.sh 15
Sign-in as local administrator 17
software requirements 6
client application 8
Configuration Console 7
User Store 8
SSL certificates 22
configure 20
non-public for tunnel forwarder 22
SSL key 20
starting
tunnel forwarders 52
tunnel receiver 52
VIP Enterprise Gateway 15
startup.sh 15
stopping
tunnel forwarders 52
tunnel receivers 52
VIP Enterprise Gateway 15
Synchronization Cluster 68
syslog 91

T

tar file for installation 5
TCP 39, 49, 50
Technical Contact 1
testing
component installation 73
Configuration Console host 73
installation 73
overall operation 75
security code validation 75
Self Service Portal 73
Validation service 73
VIP Manager 73
troubleshooting 105
trusted CA certificates
replicating 22
Trusted CA Store 22
TrustedCAs.pak 103
tunnel forwarder
adding 49
configuring autostart for 52
direct 49
overview 49
starting and stopping 52
through proxy 49
tunnel receiver
adding 50
configuring autostart for 52
overview 50
starting and stopping 52

U

UDP 39, 49, 50
uninstall 99
on Linux 99
on Windows 99
uninstalling VIP Enterprise Gateway 99
unpackTrustCAs.bat 103
unpackTrustCAs.sh 103
Update
VIP Enterprise Gateway 77
Update Settings
Checking 77
Installing 79
upgrade 97
Upgrading
Apply patches manually 98
upgrading
VIP Enterprise Gateway 97-98
URL
Self Service Portal 59
VIP Manager 65
user rights 6
User Store
advanced configuration 32
configuring 22, 27
hardware/software requirements 8
optional attributes 34
search criteria 33
user rights 6
username, administrator 5, 11

V

Validation mode
User ID - Access PIN - Security Code 41
User ID - LDAP Password - Security Code 41
User ID – LDAP Password – Security Code (RADIUS Access Challenge Mode) 41
User ID - Security Code 40
Validation server
Automatic Business Continuity 25
duplicating 47
Validation service
configuring ??-44
testing 73
Validation tab 49
VIP Access Push 42
VIP Administrator Authentication 53
VIP Administrator Groups 35
VIP Administrators 54
VIP Authentication Service 1, 19, 39
securing 19
VIP certificate 1
VIP Enterprise Gateway 83
default ports 101
error codes 105
export configuration settings 93
installation zip file 10
installing 9-16
installing on Linux 14
installing on Windows 10-13
overview 1
restoring 100

starting and stopping 15
synchronization cluster 68
troubleshooting 105
uninstall 99
uninstalling 99
upgrade 97
upgrading 97-98
VIP Enterprise Gateway host
hardware/software requirements 6
VIP Enterprise Gateway logging
levels 84
options
Validation server 87
VIP Enterprise Gateway logs 83
VIP Manager 1
configuring 63
configuring secure access to 65
configuring third-party IDP service for 61
overview 65
secure access to 59
Service Status 65
testing 73
URL 65
VIP User Groups 35
virtual private network 39, 49
vsradiusclient_test 73

W

Web Services 62
Windows
changing the installation directory on 12
Configuration Console host requirements 6
configuring tunnels to autostart 52
default installation location for 12
hardware/software requirements 6
installation file for 5, 10
installing on 10-13
Password tool 17
requirements for Configuration Console on 6
starting and stopping VIP Enterprise Gateway on 15
trusted CA replication tool 103
uninstalling on VIP Enterprise Gateway 99
wizard
for installing VIP Enterprise Gateway on Linux 14
for installing VIP Enterprise Gateway on Windows 10-13
for upgrading to VIP Authentication Service 97-98

Z

zip file for installation 5, 10