Symantec™ VIP

Enterprise Authentication Deployment Guide
Legal Notice

Copyright © 2011 - 2016 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Chapter 1 Introduction ................................................................. 6
About Symantec Cloud-Based Authentication Service ............... 6

Chapter 2 Choosing Your Credential ........................................ 7
About the Selection of Credentials .............................................. 7
VIP Access for Mobile ............................................................... 8
VIP Access Push ................................................................. 9
VIP Access Desktop ............................................................. 10
Security Code through SMS .................................................... 11
Security Code through Voice Call .......................................... 12
VIP Security Tokens ................................................................. 12
VIP Security Cards ............................................................... 13
VIP Trusted Device ............................................................... 14
Custom-embedded Credentials ............................................... 14

Chapter 3 VIP Deployment Overview ........................................ 16
Understanding Your Current Network Topography without VIP .......... 16
About Network Topography with VIP ........................................ 17
  About the VIP Enterprise Gateway ...................................... 19
  VIP Validation Service ......................................................... 21
  VIP Manager ................................................................. 22
  VIP Self Service Portal ....................................................... 22
  VIP Intelligent Authentication .............................................. 22
  VIP Login ......................................................................... 23
  About Authentication Levels .............................................. 24

Chapter 4 Creating a Test Deployment ........................................ 25
About the Test Deployment ..................................................... 25
Creating a Test User ............................................................. 26
Acquiring a VIP Credential .................................................... 26
Assigning the VIP Credential to a Test User in VIP Manager ........ 26
Installing VIP Enterprise Gateway .......................................... 27
Configuring VIP Enterprise Gateway ...................................... 27
Connecting VIP Enterprise Gateway to the Test User Store .......... 27
Chapter 8 Other Common Variations and Requirements 69
About LDAP Directory Synchronization 69
About Tunneling 70

Index 72
Introduction

This chapter includes the following topics:

- About Symantec Cloud-Based Authentication Service

About Symantec Cloud-Based Authentication Service

Symantec VIP is a cloud-based authentication service that enables enterprises to secure access and online transactions to meet compliance standards and to reduce fraud risk. VIP provides an additional layer of protection beyond standard user name and password through a wide variety of additional authentication capabilities including:

- Two-factor authentication - dynamic, one-time-use security codes generated by a user's VIP credential in the form of mobile apps, desktop software, security tokens, and security cards
- Out-of-band authentication - dynamic, one-time-use security codes delivered via phone call, SMS text message or email, or push notifications sent to a registered mobile device
- Risk-based authentication - real-time analysis of user and device characteristics including device IDs, device fingerprints and reputation, IP geolocation, and global network intelligence

VIP is based on OATH open standards, an industry-wide consortium working with other groups to promote widespread strong authentication. Because the service is hosted by Symantec, enterprises engage one solution to support multiple enterprise, partner, and customer-facing applications requiring strong authentication.

Intended for administrators, this guide explains how to prepare for VIP implementation by providing a comprehensive outline for planning, decision making, and task prioritization for a successful deployment.
Choosing Your Credential

This chapter includes the following topics:

- About the Selection of Credentials
- VIP Access for Mobile
- VIP Access Push
- VIP Access Desktop
- Security Code through SMS
- Security Code through Voice Call
- VIP Security Tokens
- VIP Security Cards
- VIP Trusted Device
- Custom-embedded Credentials

About the Selection of Credentials

Your organization provides users with credentials and all credentials generate security codes. Each time that users sign in to a participating web site, they must enter their user name, password, and a new security code to authenticate. Because users generate a security code only when they need to access their accounts. Unauthorized users cannot guess or otherwise discover the security code like they can with a traditional password. If a credential is lost or stolen, an unauthorized user still has to enter a user name and password for any registered member website before accessing a user’s accounts. Therefore it makes the credential useless for unauthorized access.

VIP supports the following types of credentials:
VIP Access for Mobile

VIP Access for Mobile is a free, online security credential that users can download to their mobile phones. It uses end user's current devices and eliminates the cost of hardware credential distribution, inventory management, and maintenance.

VIP Access for Mobile is available for all iPhone models, most Android, Windows, and BlackBerry devices; and other smart phones and feature phones from leading manufacturers.

For more information about VIP Access for Mobile, go to:

http://m.vip.symantec.com
VIP Access Push

VIP Access Push works with the VIP Access for Mobile credential to send a push notification to a user’s push enabled device. The user simply accepts the notification to complete the process of signing in. This functionality is a simple, convenient method for protecting web applications with a strong-authentication credential that does not require any additional devices.
VIP Access Desktop

The VIP Access Desktop credential is a stand-alone desktop client that enables two-factor authentication when downloaded to an end user's machine. This free credential eliminates the cost of hardware credential distribution, inventory management, and maintenance. At the click of a mouse, the user can copy and paste the current security code, as needed, into an application.

For desktops that ship with Intel chipsets containing Intel's Identity Protection Technology (IPT) firmware, the Intel security container (Intel ME) within the chipset secures the VIP credential and provides a hardware-based desktop credential. For those desktops that do not have Intel IPT chipsets, the credential is securely protected within the software of the device. VIP Access Desktop is available for Windows XP, Vista, and 7. For more information about VIP Access Desktop, visit:

https://idprotect.vip.symantec.com/desktop/
Security Code through SMS

VIP Authentication Service generates and delivers a security code to a user's mobile phone through the short message service (SMS). The user registers the phone number with VIP Authentication Service, which validates the security code. This functionality is ideal for protecting web applications with a convenient, strong-authentication credential that does not require any additional devices.
Security Code through Voice Call

VIP Authentication Service generates and delivers a security code to a user's phone through an automated phone call. The user registers the phone number with VIP Authentication Service that validates the security code. This functionality is ideal for protecting web applications with a convenient, strong authentication credential that does not require any additional devices.

VIP Security Tokens

VIP Security Tokens are based on proven one-time password technology. The inexpensive, robust, and easy-to-use token is ideal for large applications that need "platform neutral" devices—an important feature for deploying a widespread solution. The token does not require additional client software and is not dependent on a user's desktop configuration or operating system.

To obtain a security code, the user presses a button on the token to trigger the next security code value or waits for the display to change. The token displays the value on a small LCD. To authenticate to an application, the user enters this value, along with his or her traditional user name and password combination.
This token supports an event-based and time-based algorithm for security code generation.

VIP Security Cards

The VIP security card combines the convenience of a credit/client card with your enterprise branding specifications (logos, colors, and artwork). If you already issue bank or client cards and currently have an issuance and deployment process in place, you find this form factor most useful. Compared to hardware tokens, this slim, mail-worthy card saves you a significant amount in packaging and postage. The VIP security card also gives you a competitive edge by associating your enterprise brand with highly visible, leading security technology.

To obtain a security code, the user presses a button on the card to trigger the next security code value. The card displays the value on a small LCD. To authenticate to an application, the user enters this value, along with his or her traditional user name and password combination.
VIP Trusted Device

VIP Trusted Device is a form of device ID that provides security for your end users without requiring a traditional hardware or mobile credential. Symantec supports device IDs for computers and mobile devices using the VIP Service. By selecting Trusted Device within the Self Service Portal, end users register their laptops or PCs by downloading a plug-in which installs a security certificate. This certificate associates the device to a unique ID which becomes the assigned credential for that specific user’s laptop or PC and identifies the device when used for sign-in.

For mobile devices, VIP Mobile Software Development Kit (SDK) can be integrated into a mobile application. The SDK has an OATH library that enables the application to generate one-time dynamic security codes that are used to identify the mobile device. Using these solutions, the end user does not need to explicitly enter security codes or other information to authenticate. The VIP Service is able to identify the credential without requiring end-user action or knowledge of the additional authentication event.

See VIP Remembered Device Integration Guide for more information on Trusted Device.

If you currently use VIP Intelligent Authentication (IA) or are interested in this enhanced layer of security, you can combine Trusted Device and IA for a stronger mode of authentication for each device associated with an end user.

See VIP Intelligent Authentication Enterprise Integration Guide for more information on how to use Trusted Device in combination with VIP Intelligent Authentication.

Custom-embedded Credentials

The Symantec VIP Developer Toolkit enables enterprises to develop custom credentials, either as a stand-alone, one-time security code generator or as an
embedded component of an existing application. VIP members can therefore include strong authentication in client-side applications with little or no disruption to the user experience.

The API enables VIP members worldwide to successfully implement the full lifecycle functions for provisioning, management, and validation of credential deployment.

See “About Planning for Credential Deployments” on page 48.
VIP Deployment Overview

This chapter includes the following topics:

- Understanding Your Current Network Topography without VIP
- About Network Topography with VIP
- VIP Intelligent Authentication
- VIP Login

Understanding Your Current Network Topography without VIP

Before you start the deployment plan, you need to understand the current configuration of your network.

Figure 3-1 illustrates a sample VPN deployment in an enterprise network without VIP integration.
A VPN gateway is deployed in your enterprise’s perimeter network (DMZ) to enable remote users to access internal network resources. Remote users [A] sign in to the VPN [B] using their current Active Directory user name and password. The VPN gateway authenticates the user name and password by a call to the company's Active Directory [C]. If the user name and password are correct, the VPN gateway will authorize the user to connect to the corporate network to access protected resources [D]. If the user name and password are not correct, the VPN gateway denies a user's sign-in.

**About Network Topography with VIP**

After you deploy VIP features, the topography includes additional layers of security. Figure 3-2 provides an overview of the network topology with VIP.
Remote users [A] arrive at the sign-in page of an enterprise's VPN gateway [B]. They enter their enterprise user name, password, and security code. The VPN gateway will then forward the user name, password, and security code by RADIUS to VIP Enterprise Gateway [C]. VIP Enterprise Gateway authenticates the user's user name and password against your enterprise's Active Directory/LDAP [D]. Once authentication is successful, VIP Enterprise Gateway validates the user's security code against the VIP validation service in the cloud [E]. If the code is validated, Enterprise Gateway responds to the VPN gateway's RADIUS authentication request by indicating a successful authentication, allowing the user to sign in and access protected network resources [H].

Upon receiving a credential, a user needs to register it before signing in to the VPN to access internal network resources. The VIP Self Service Portal [G] enables the user to register and manage the user's credentials.

VIP Manager [F] allows your administrators to 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.

As illustrated in Figure 8, there are four main components in any VIP deployment:

- VIP Enterprise Gateway
- VIP Validation Service
VIP Manager
VIP Self Service

The following topics describe these components in more detail.

About the VIP Enterprise Gateway

VIP Enterprise Gateway integrates with your existing network infrastructure to strengthen and streamline your network security and help prevent unauthorized break-ins. VIP Enterprise Gateway acts as a bridge between the cloud-based VIP Service and your local network infrastructure, such as virtual private networks (VPN), Windows desktops, Linux servers, web-based email programs, routers, and firewalls using a single, integrated platform.

The VIP Enterprise Gateway Installation and Configuration Guide includes hardware and operating system requirements for successful deployment of VIP Enterprise Gateway — as well as the supported browsers that work with VIP Manager and the Self Service Portal. These system requirements are provided only as a guideline because components may vary among enterprises and according to implementation.

VIP Enterprise Gateway provides one or a combination of the following functions:

- Configuration Console
- Validation Server
- Identity Providers (IdPs)
- Self Service Portal Proxy
- Tunnel Forwarder and Receiver
- LDAP Synchronization
- Logging

Configuration Console

VIP Enterprise Gateway's Configuration Console enables administrators to sign in, configure, and manage Enterprise Gateway settings including the connection to your enterprise’s user store, such as an LDAP or Active Directory (AD) [D], and the connection to the VIP Service. The console also allows administrators to configure and manage other Enterprise Gateway features related to VIP validation:

See Figure 3-1 on page 17.

- Serving as an identity provider (IdP) for VIP Manager and Self Service Portal
- Tunneling UDP traffic through a TCP connection to accommodate certain restrictions
- Logging VIP transactions for auditing
- Synchronizing your enterprise's user store with the VIP user accounts

**Validation Server**

Enterprise Gateway's Validation server feature validates RADIUS authentication requests from applications such as a VPN gateway to ensure that only authenticated users have access to your applications and data files. The Validation server performs this function by first checking the user's name and password in the RADIUS request against your enterprise's user store such as an AD [D]. Once the server validates the user name and password, it extracts the security code in the same RADIUS request against the VIP Validation Service [E]. If both verifications are successful, the Validation server will inform the VPN gateway [B] through a RADIUS response to allow the user to access internal enterprise files and applications.

**Identity Providers**

An Identity Provider (IdP) is a web application that authenticates users for other web applications that require verification before providing services to those users. VIP Enterprise Gateway features an identity provider for the in-cloud VIP Manager and the in-cloud VIP Self Service Portal. The IdP authenticates a user against the local enterprise user store (AD or LDAP), and then securely re-directs the user to the Symantec-hosted VIP Manager or Self Service Portal with the proper permissions to access VIP Manager or Self Service Portal.

The cloud-based Self Service Portal uses VIP Enterprise Gateway Self Service IdP to authenticate users so they can register a credential or get a temporary security code when they do not have their credential.

While you can configure the IdP in VIP Enterprise Gateway to authenticate administrators for access to VIP Manager (in-cloud), you can also set up your own user name and password inside VIP Manager to authenticate administrators. For more information, see the online help in VIP Manager.

**Self Service Portal Proxy**

The Self Service Portal Proxy serves as a reverse proxy to the Self Service Portal IdP, suitable to be deployed in the perimeter network. Remote enterprise users access the Self Service Portal IdP in the back-end network through the Self Service IdP Proxy in the perimeter network, allowing users to register their own VIP credential even if they are not in the corporate network. The Self Service Portal Proxy is also used to facilitate out-of-band (OOB) security codes for end users when deploying VIP Intelligent Authentication.
Tunnel Forwarder and Receiver

The tunnel forwarder, an optional feature in Enterprise Gateway, provides a RADIUS package relay service over a TCP connection if your enterprise’s firewall policies prevent any UDP traffic (such as RADIUS authentication requests from a VPN gateway) to traverse from the perimeter network to Enterprise Gateway located in your enterprise's back-end network. The tunnel forwarder wraps the UDP request in a TCP connection and forwards it to the tunnel receiver located on the target Enterprise Gateway.

See “About Tunneling” on page 70.

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, sending the Validation server response back to the tunnel forwarder, again over TCP.

See “About Tunneling” on page 70.

LDAP Synchronization

LDAP Synchronization, an optional feature in Enterprise Gateway, periodically synchronizes your enterprise’s Active Directory or LDAP-based user store with user accounts located in the VIP Service. This service is useful to update user accounts that you have removed from your user store, such as when a user leaves your organization.

Logging

The Symantec VIP Logging Service records all significant events on a transaction-by-transaction basis.

See “About Logging and Reporting” on page 44.

VIP Validation Service

VIP Validation Service validates a user's second-factor VIP credential, usually the security code entered from the user's VIP credential (the value from VIP Access for Mobile or a VIP Security Token). After the VIP Validation server in Enterprise Gateway validates the user's user name and password (first-factor credential) against the local enterprise user store (an AD or LDAP), the Validation server sends the security code for the user's credential to the Validation Service. The Validation Service, hosted at Symantec, returns a success or failure to the Validation server. The Validation server decides if the user should be allowed access from a VIP-enabled application, such as a VPN gateway.

See Figure 3-2 on page 18.
VIP Manager

VIP Manager [F] provides authorized access to all functions including configuration, lifecycle management, and help desk. End-user administration functions includemanual credential assignment (early binding activation) and manual credential activation. Although the default credential distribution policy assumes that the credential is not activated (and therefore usable) until the user registers the credential, VIP Manager enables an administrator to manually register (or associate) a credential to a specific user and activate that credential on the user's behalf.

Other administrative functions include running reports, adding and removing help desk support personnel accounts, and setting up policies such as using aPIN instead of your enterprise's AD password for user authentication.

Administrators access VIP Manager either by signing in with their enterprise AD user name and password via VIP Enterprise Gateway's VIP Manager IdP or by using their email address, VIP Manager password, and a security code from a VIP credential.

See Figure 3-2 on page 18.

VIP Self Service Portal

The Self Service Portal [G] allows your end users to manage their VIP credentials, which includes registering, testing, or resetting credentials. End users can also remove credentials from their account if they are lost or stolen.

See Figure 3-2 on page 18.

To access the VIP Self Service Portal, users sign in with their enterprise user name and password through VIP Enterprise Gateway's VIP Self Service IdP Application.

VIP Intelligent Authentication

VIP Intelligent Authentication (IA) helps prevent malicious account sign-in from unknown sources. As an alternative to traditional hardware and mobile credentials, VIP IA provides layered security for your end users without asking them to install any special software applications.

The VIP IA security layer uses risk-based authentication to analyze various profile elements in addition to a typical user name and password for each user sign-in. VIP IA can assess the legitimacy of sign-in events by considering:

- End user behavior
- Browser and device attributes
- Device reputation and network intelligence
■ Device risk

The VIP IA policy must be enabled and configured within the VIP Manager tool before you can leverage IA for your users.

See the *VIP Intelligent Authentication Enterprise Integration Guide* for details on VIP IA.

If you currently use VIP Intelligent Authentication (IA) and are interested in enhancing it with another layer of security, you can combine IA with Trusted Device for a stronger mode of authentication for each device associated with an end user.

VIP Trusted Device is a form of device ID that provides security for your end users without requiring a traditional hardware or mobile credential. End users register their laptops or PCs through the Self Service Portal by downloading a plug-in that installs a security certificate. This certificate associates the device to a unique ID which becomes the assigned credential for that specific user’s laptop or PC.

See the *VIP Intelligent Authentication Enterprise Integration Guide* for more information on using Trusted Device in combination with VIP Intelligent Authentication.

**VIP Login**

If your login application supports SAML (Security Assertion Markup Language), you can use VIP Login to extend your login applications to support strong authentication. VIP Login provides strong authentication using the SAML protocol. SAML is a standard protocol for web-based authentication. Integrating SAML with your VIP service provides a flexible, standard means for securely authenticating users to common web applications that support SAML. Your users can log in using their VIP credential as a second factor. You act as the SAML service provider, and optionally, as the SAML identity provider, based on your configuration.

This feature is supported for physical credentials, mobile credentials, VIP Access Push, and out-of-band credentials (including SMS/Voice credentials).

In some cases, the user does not have access to a credential. 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 an email address or a different mobile device capable of receiving SMS or Voice messages. VIP automatically handles these out-of-band credentials if these credentials are registered with VIP. However, if you store your users’ out-of-band credentials in a local user store such as your HR database, you can configure VIP Login to request these out-of-band credentials from your enterprise IdP solution.

The IdP solution that you configure to return the out-of-band credential does not have to be the same solution that authenticates the user’s first factor.
See Symantec™ VIP Integrating VIP Login with your SAML Client for details on integrating VIP Login with your SAML clients.

About Authentication Levels

VIP Login also supports authentication levels. Authentication levels are groups of policy options that define what authentication method is available to a user when that user logs into a specific resource. Each level addresses a different security scenario. For example, for most of your users, you can define a level that allows them to authenticate with a security code generated by any credential. For users or groups with sensitive access, you can define a level that requires them to authenticate only with a security code received out-of-band through an SMS or voice message. For both or either of these authentication levels, you can restrict users from using temporary security codes when authenticating.

When users attempt to sign in to a resource, your website identifies the authentication method the users must use. VIP Login enforces that requirement, and users must sign in with that authentication method. If a user attempts to authenticate using a method that is not defined for the authentication level, authentication fails.

Typically, your organization’s regulatory or audit compliance requirements drive the levels you create.
Creating a Test Deployment

This chapter includes the following topics:

- About the Test Deployment
- Creating a Test User
- Acquiring a VIP Credential
- Assigning the VIP Credential to a Test User in VIP Manager
- Installing VIP Enterprise Gateway
- Configuring VIP Enterprise Gateway
- Connecting VIP Enterprise Gateway to the Test User Store
- Configuring VIP Enterprise Gateway for RADIUS Validation
- Connecting VPN Gateway to Enterprise Gateway Using RADIUS
- Performing End-to-end Testing of VIP Deployment

About the Test Deployment

Before you can roll out a full VIP solution to your enterprise, it is recommended that you run a test deployment to assess how VIP works from end to end. The test deployment helps you understand VIP technology and its various considerations before you perform a full test deployment.

Creating a test deployment includes the following general steps.

1. Creating a Test User
2. Acquiring a VIP Credential
3. Assigning the VIP Credential to a Test User in VIP Manager
Creating a Test User

If you want to complete a successful test, you need to create a user who uses a VIP credential to sign into the VPN gateway. You can create a user in your enterprise's existing user store (for example, your AD), or in a new user store that has been created exclusively for this test. Alternatively, the test can use an existing user in an existing user store.

See the product documentation for your user store for details on adding a user.

Acquiring a VIP Credential

The test user needs a VIP credential to sign in to the VIP-secured VPN application. The easiest way to acquire a VIP credential is to download a VIP Access for Mobile credential on a supported mobile phone or a VIP Access Desktop credential to a PC.

To acquire a VIP credential, go to:

http://m.vip.symantec.com

or

http://idprotect.vip.symantec.com/desktop/

Assigning the VIP Credential to a Test User in VIP Manager

You need to assign the VIP credential to a test user.

To assign the VIP credential to a test user in VIP Manager

1 Sign in to VIP Manager.
2 Add the test user's user name through the Manage VIP End Users section.
3 Assign the VIP credential ID to the user's account in VIP Manager.
Installing VIP Enterprise Gateway

To install VIP Enterprise Gateway, follow the steps in the *VIP Enterprise Gateway Installation and Configuration Guide* to download and install an instance of Enterprise Gateway. This document also provides the VIP Enterprise Gateway platform requirements.

Configuring VIP Enterprise Gateway

After you have successfully installed VIP Enterprise Gateway, you need to configure Enterprise Gateway to communicate with the VIP Authentication Service in the cloud to enable validation requests.

To configure VIP Enterprise Gateway

1. Access the Configuration Console and follow the steps to sign into the newly created instance of VIP Enterprise Gateway.
2. At the VIP Enterprise Gateway prompts, add a VIP Certificate to enable mutual authentication between the gateway and the VIP Service.
3. Add the VIP Certificate to secure communications with the VIP Authentication Service.

See *VIP Enterprise Gateway Installation and Configuration Guide* and the VIP Enterprise Gateway online help for information on configuring VIP Enterprise Gateway.

Connecting VIP Enterprise Gateway to the Test User Store

The VIP Enterprise Gateway manages validation of the user's user name and password, as well as the user's security code. It delegates the authentication of the user's name and password to the enterprise's locally-hosted user store.

Configure the user stores by following the steps in the *VIP Enterprise Gateway Installation and Configuration Guide.*
Configuring VIP Enterprise Gateway for RADIUS Validation

You configure VIP Enterprise Gateway for RADIUS validation when you add a Validation server. You add a Validation server in VIP Enterprise Gateway when you configure Validation Services. Before you can configure Enterprise Gateway for RADIUS validation, you must have the IP address of your VIP Gateway, as well as the port number and RADIUS shared secret as you specified on the Add Radius Validation Server page when you configured Validation Services.

Configure the VIP Enterprise Gateway for RADIUS validation by following the steps in the VIP Enterprise Gateway Installation and Configuration Guide.

Connecting VPN Gateway to Enterprise Gateway Using RADIUS

The VPN Gateway authenticates the user with two factors of authentication. The first factor, which is what the user knows, typically includes a user name and password. The second factor, which is what the user has, represents the security code that is derived from a user's VIP Credential.

If you want to enable strong authentication at the VPN gateway with VIP, you need to connect your VPN gateway to Enterprise Gateway via RADIUS.

To connect VPN to Enterprise Gateway using RADIUS

1. Follow your VPN Gateway's instructions to connect to the IP address and port of your Enterprise Gateway's RADIUS Validation Server.
2. Make sure that the RADIUS shared secret in the VPN Gateway is the same one that you have specified on the Add Radius Validation Server page.

Symantec provides integration guides for many common third-party applications. Refer to these guides (available on VIP Manager) for more information integrating third-party applications with the VIP Authentication Service and VIP Enterprise Gateway.

Performing End-to-end Testing of VIP Deployment

You are now ready to test VIP in the environment from end to end.

To perform end-to-end testing of VIP deployment

1. Sign into the VPN by entering the test user’s user name and password.
2. Append the security code from the VIP credential to the end of the password.
After a successful single-user end-to-end test, it is recommended that you roll out the deployment to a small set of users so that you can learn from the results to prepare for a full deployment.
VIP Deployment Planning

This chapter includes the following topics:

- About Corporate Policy Considerations
- About VIP Enterprise Gateway Deployment Considerations
- About Self Service Considerations
- VIP Manager Deployment Considerations
- About Planning for Application Integration

About Corporate Policy Considerations

Before you can roll out a full deployment, you need to consider the following high-level policy issues:

- How many credentials are allowed per user?
  VIP allows one user to register multiple credentials. Multiple credentials, especially in different form factors, provide additional convenience for user maintenance. You can set this policy in the VIP Policy Configuration section of VIP Manager.

- What is the password lock-out policy?
  If a user enters the security code incorrectly beyond the allowed attempts, the VIP system disables the credential. The user needs to either call the help desk or unlock the credential through the Self Service Portal. A lower number of allowable attempts increases the security of the system at the expense of additional administration and maintenance. Your enterprise must decide on this trade-off. You can set the number of allowed bad attempts in VIP Manager in the Credential Security Settings section.

- What temporary security code is allowed when a user forgets his or her credential?
If users forget their credentials, they can request a temporary security code from the Self Service Portal or from the help desk. VIP supports temporary security codes distributed via email, SMS, or a voice call. Your enterprise needs to decide which is the best mechanism to distribute this security code by taking into consideration the cost of SMS or voice call. The user’s account profile in the enterprise’s Active Directory provides the email addresses and phone numbers that are used to send temporary security codes. You can set this policy in the VIP Policy Configuration section of VIP Manager.

- Can you use PIN instead of password for the first factor?
  While we recommend using the user name and password found in your enterprise’s user store for first factor, some enterprises prefer to use user name, and a PIN. Go to VIP Managers Policy Configuration section to enable PIN-based authentication.

- How big should the VIP Validation window be?
  While a VIP credential changes its security code every 30 seconds, the VIP Validation Service considers the security code to be valid in a certain window that ranges from 64 seconds to 2048 seconds and defaults to 320 seconds. A low number increases security but could potentially cause more validation failures for users and thus increase lock-outs. A high number decreases lock-outs, but, at the same time, increases the validity window of a security code. You can configure this setting in the VIP Manager Credential Security Settings section.

- Who are the people involved in the VIP deployment?
  Since VIP deployment involves many people and roles in the organization, begin by engaging the cross-functional teams as you roll out the VIP solution. Some of the roles involved include the following:

  - IT Help Desk: The help desk receives support calls from VIP credential users.
  - Network Administrator: The network administrator is the point of contact for VIP Enterprise Gateway installations and application configurations such as VPN.
  - Network Security: This team may handle or create new firewall rules to enable the VIP solution. The team may also want to perform a security assessment of the deployment to understand how the deployment will meet current network security policies.
  - Fulfillment: The fulfilment team acquires new physical credentials or replaces broken credentials if the deployment requires hard credentials.
  - Employee Training Department: Depending on the complexity of your deployment or the nature of your relationship to the users who use VIP credentials, the training department provides users a higher-touch level of training on VIP usage.
Employees: Employees directly use the new VIP tools in your enterprise.

How do you configure VIP deployment to conform to your enterprise password security policy?
VIP deployment requires the creation of new accounts and passwords. Some enterprises have specific requirements for how passwords are stored and rotated. Below is a list of passwords created by VIP deployment:

Table 5-1 lists all available credentials in a VIP deployment

<table>
<thead>
<tr>
<th>Credential</th>
<th>Purpose</th>
<th>Credential Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP Enterprise Gateway Configuration Console Sign-in</td>
<td>The system administrator sign-in for VIP Enterprise Gateway</td>
<td>VIP Enterprise Gateway</td>
</tr>
<tr>
<td>VIP Manager Master Administrator</td>
<td>The first VIP Manager credential that will be responsible for creating other administrators for VIP Manager</td>
<td>VIP Manager in the cloud</td>
</tr>
<tr>
<td>VIP Manager Administrators</td>
<td>Administrator credentials for IT administrators and help desk personnel to perform help desk tasks, running reports, etc. If single sign-on for VIP Manager leveraging existing enterprise sign-in credentials is not deployed, then these accounts are created in VIP Manager in the cloud.</td>
<td>VIP Manager in the cloud</td>
</tr>
<tr>
<td>Shared RADIUS Passwords</td>
<td>The RADIUS password required between the client application (such as VPN) and VIP Enterprise Gateway’s Validation server</td>
<td>The client manages the password on the client. VIP Enterprise Gateway stores the password</td>
</tr>
</tbody>
</table>

About VIP Enterprise Gateway Deployment Considerations

Before you can deploy Enterprise Gateway in a production environment, you need to streamline your deployment process by considering the following preliminary questions:

- Where is the user store located?
What ports need to be opened and how are the firewalls impacted?
Which communication channels need to be secured?
How should Enterprise Gateway be physically secured?
Where will you store the logs?
What is the plan for failover and high availability?
Does your corporate policy require different VIP policies for different groups of users and administrators?

About the User Store

A user store contains information from your enterprise’s user accounts and is usually located on a LDAP or AD server. VIP Enterprise Gateway connects with a user store that requires an additional layer of security. Therefore users need to sign in to enterprise applications with VIP credentials.

VIP Enterprise Gateway employs the user store to verify a user name and password as the first factor during RADIUS authentication. If you enable out-of-band authentication, VIP Enterprise Gateway also uses email addresses or phone numbers from the user store. Additionally, if you configure Enterprise Gateway as an IdP to VIP Manager or the Self Service Portal, it authenticates the user through the user store before it allows access to VIP Manager or the Self Service Portal.

When choosing the user store for VIP Enterprise Gateway, you need to evaluate the location of the users in the subcomponent of the LDAP directory. Enterprise Gateway locates a user for authentication via an LDAP directory search, traversing the LDAP tree. Before choosing the user store, you need to specify the baseDN and the search filter for the LDAP traversal.

For more information on setting up the user store in Enterprise Gateway, see VIP Enterprise Gateway Installation and Configuration Guide.

About Multiple User Stores

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. These needs mainly arise from:

- Mergers and Acquisitions of organizations
- Partner relationship and trust across organizations
- Limited data sharing and information access to comply with geo-political regulations
In these situations, you may come across users having membership in multiple User Store trees or Active Directory (AD) domains/forests. VIP Enterprise Gateway is designed to address complex authentication use cases by providing flexibility in User Store configurations. While adding multiple user stores is fairly straightforward, the user management policies of the organization can lead to complex scenarios. Some of the well-known scenarios are described below.

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, which could be their possible User Principal Names in their respective AD domains.

Scenario 2:
When Acme Corporation was trying to set up its business applications, they decided to use best-of-breed applications from various vendors that suit their business needs. In doing so, they ended up having an Active Directory infrastructure for all normal employee directory service's needs. But, their file server still runs on Novell Open Enterprise Server, which uses Novell eDirectory as the backbone directory service. Now, John Smith, an employee working in Acme Corporation has two identities; one on the corporate AD forest (john_smith@acme.com) and the other on the corporate file server (ACMEFILETREE\john_smith). 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 3:
John Smith, an employee of Acme Corporation can sign into the corporate Active Directory networks as john_smith, ACME\john_smith, acme.com\john_smith, john_smith@acme.com. And 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.

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 4:
Acme Corporation has been convinced that Symantec VIP Services hosted in the Symantec cloud environment is absolutely secured, yet as 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 into the corporate AD environment as john_smith, in the Symantec VIP User Services, his employee id (U32461) is registered as his user name.

Enterprise data protection policies of certain organizations do not permit their employee's public cloud identities and their enterprise internal identities to be the same. In case of a data breach, the public cloud information of a user cannot be mapped to an enterprise user. This helps maintain data privacy in case of a data breach. In such cases organizations may want to use another attribute, like employee id, as a VIP user id stored in the cloud instead of the user name.

Distinguishing Users
Users are distinguished in VIP Services by their VIP User Names. The VIP User Name can be different than the users LDAP or login user name. When configuring a user store in VIP Enterprise Gateway, an administrator can provide which attribute from the LDAP user object can be used as the VIP User Name. As a result, all the scenarios described in Scenario 1 to 4 can be addressed by choosing the proper LDAP attribute for VIP User Name in the user store configuration.

Refer to VIP Enterprise Gateway Installation and Configuration Guide and the VIP Enterprise Gateway online help for the more information about configuring user stores.

Searching for Users across 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 Configuration page

- The user name provided as part of validation is replaced with the search filter 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 has domain information along with it (for example, domain\user name in case of Active Directory), the user name is only validated
against all of the user stores that serve the specific domain, in the order set on the User Store Configuration page.

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

---

**Note:** If a unique user is returned as part of a user search operation, the authentication request will be performed against that user. If the LDAP password fails for the user, it will be considered as an authentication failure and subsequent user stores will not be searched.

---

**Table 5-2**

<table>
<thead>
<tr>
<th>User Store Name</th>
<th>Domains</th>
<th>Users in User Store</th>
<th>User Search Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acme Financial</td>
<td>acme</td>
<td>■ cn=john_smith, ou=sales, dc=acme, dc=com&lt;br&gt;■ cn=john_smith, ou=eng, dc=acme, dc=com&lt;br&gt;■ cn=alice, ou=sales, dc=acme, dc=com</td>
<td>(cn=%s)</td>
</tr>
<tr>
<td>TrustedBank</td>
<td>trustedbank</td>
<td>■ cn=john_smith, cn=users, dc=trustedbank, dc=com&lt;br&gt;■ (sAMAccountName=john_smith)</td>
<td>(sAMAccountName=%s)</td>
</tr>
<tr>
<td>XYZBank</td>
<td>xyzbank</td>
<td>■ cn=bob, cn=users, dc=xyzbank,dc=com&lt;br&gt;■ (sAMAccountName=bob)</td>
<td>(sAMAccountName=%s)</td>
</tr>
</tbody>
</table>

---

**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 logs 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 log in.

**Scenario 3:**
In this scenario, the user logs 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.

---

**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 user record 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 occurs because of complex enterprise-level LDAP configurations:

- See “Use Case 1: Supporting Load-balancing and Failover” on page 38.
- See “Use Case 2: Synchronizing Disparate User Stores Independently from Different VIP Enterprise Gateway Servers” on page 39.

To resolve these use cases, you can configure LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers.

See “Configuring Multiple Instances of LDAP Directory Synchronization Service” on page 38.

---

**Note:** Symantec recommends you to follow these configurations only on such complex LDAP configurations 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. A maximum of 24 instances of LDAP Synchronization service from a VIP account are supported by the VIP Service.

**Note:** Do not continue with the configuration of multiple instances of LDAP Directory Synchronization Service if your User Store configuration that is associated with the VIP Enterprise Gateway servers do not conform to the one described in the following use cases. In such cases, Symantec recommends you to contact Symantec Support before you continue with this configuration.

Use Case 1 recommends that all User Stores be configured identically. Use Case 2 recommends that each group of user stores be configured with separate Synchronization Clusters.

**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 and arranged in the same order. To ensure identical User Store configuration on all the VIP Enterprise Gateway servers, 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 on the LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers, 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, which is part of the same Synchronization Cluster, can run within this window period.

- **Supporting Failover**
  To achieve failover on the LDAP Directory Synchronization Service on multiple VIP Enterprise Gateway servers, you must configure the synchronization schedules of these LDAP Directory Synchronization Services 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 the above 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 locational network visibility constraints that 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 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 of the Configuration of Multiple Instances of LDAP Directory Synchronization Service**

The following examples explains the configuration of multiple instances of LDAP Directory Synchronization Service:
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 whether an LDAP synchronization is in progress for the **Colossal** Synchronization Cluster or an LDAP.
Synchronization instance has started within the past three hours. When it recognizes that EG3 has started synchronization in the past three hours or EG3 is still synchronizing the user records for the *Colossal* Synchronization Cluster, EG4 aborts the scheduled LDAP synchronization and waits for the next interval.

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 the *Colossal* Synchronization 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.

**About Synchronizing 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 than assigning all administrators with the same level of privileges. The user groups and the administrator groups can be configured in VIP Manager.

However, 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 the users in LDAP/AD User Stores to one or more user groups or administrator groups in VIP Services, 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 that runs on VIP Enterprise Gateway can query the LDAP User Store for additions, deletions, and updates to the user and the administrator records for group membership. Then, the LDAP Synchronization service synchronizes the information to the VIP Services.

See the VIP Enterprise Gateway online help for detailed information on VIP User Group Mapping and VIP Administrator Group Mapping.

About Port and Firewall Considerations

Deploying VIP Enterprise Gateway may require changes to firewall rules, which need preparation beforehand.

View a list of ports used by VIP deployment in *VIP Enterprise Gateway Installation and Configuration Guide*.

About Planning for VIP Enterprise Gateway Communication Security

Before you deploy VIP Enterprise Gateway, you need to consider how to secure communications to and from the gateway.

Table 5-3 lists various communication channels and our recommendations to secure each channel.

<table>
<thead>
<tr>
<th>Direction</th>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>Administrator</td>
<td>VIP Manager Configuration Console</td>
<td>HTTP/HTTPS</td>
<td>Use SSL certificate for Configuration Console.</td>
</tr>
<tr>
<td>Inbound</td>
<td>User</td>
<td>Self Service Portal IdP</td>
<td>HTTP/HTTPS</td>
<td>Use SSL certificates for the IdP as passwords are entered at the IdP.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Administrator</td>
<td>VIP Manager IdP</td>
<td>HTTP/HTTPS</td>
<td>Use SSL certificates for the IdPs as passwords are entered at the IdP.</td>
</tr>
<tr>
<td>Inbound</td>
<td>Client App</td>
<td>VIP Enterprise Gateway</td>
<td>RADIUS</td>
<td>Protection through standard RADIUS shared secret; use strong shared secret and frequent password rotation.</td>
</tr>
</tbody>
</table>
### Table 5-3  Communication Channels and Security Recommendations (continued)

<table>
<thead>
<tr>
<th>Direction</th>
<th>From</th>
<th>To</th>
<th>Protocol</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outbound</td>
<td>VIP Enterprise Gateway</td>
<td>LDAP/AD</td>
<td>LDAP/LDAPS</td>
<td>Use LDAPS if the connection from Enterprise Gateway to AD traverses through multiple network segments. You may need to install a root certificate in Enterprise Gateway as most LDAPS configurations use a private certificate. See <em>VIP Enterprise Gateway Installation and Configuration Guide</em> for installation of root certificates.</td>
</tr>
<tr>
<td>Outbound</td>
<td>VIP Enterprise Gateway</td>
<td>VIP In-cloud Authentication Service</td>
<td>HTTPS</td>
<td>VIP Enterprise Gateway uses a client authorization certificate to secure communication. For multiple Enterprise Gateway instances, the enterprise needs to decide to use one certificate for all Enterprise Gateway instances, or to use one certificate for each machine.</td>
</tr>
</tbody>
</table>

---

### About Planning for Enterprise Gateway Physical Security

Enterprise Gateway is a critical security component of your enterprise network infrastructure. Therefore, it is recommended that you host it in the same location as other critical infrastructure components, such as your enterprise’s user store. Most likely, this location is your back-office network.

Sometimes, you may need to host an enterprise gateway outside your back-office network. For example, you can configure it as a tunnel forwarder in the perimeter network or as a Self Service IdP Proxy. Under these circumstances, it is
About Logging and Reporting

Symantec's VIP Service records all significant events on a transaction-by-transaction basis. The VIP solution creates audit trails for all security code transactions, including passed and failed validations, activations, and PIN resets. User-administration audit logs record functions executed by individual administrators.

VIP provides the following methods for storing logs:

- Enterprise Gateway local log file
- Syslog server

See *VIP Enterprise Gateway Installation and Configuration Guide* for more details on how to configure logging options that use the Configuration Console of Enterprise Gateway.

About Failover and High Availability

VIP Enterprise Gateway and its components are all stateless. Therefore your enterprise can achieve failover and redundancy by deploying the following VIP Enterprise Gateway instances.

- Failover and redundancy for client applications
  
  You need to prepare for failover and redundancy for client applications, such as VPN, by configuring the client(s) to connect to all VIP Enterprise Gateways in a round-robin fashion using RADIUS load balancing. For applications that use Symantec-provided integration plug-ins, you need to consult the specific VIP Application Integration Guide for your application's load balancing and failover information.

- Failover and redundancy for VIP Manager and Self Service Portal IdP
  
  Because the IdPs reside on VIP Enterprise Gateway represent web applications, it is recommended that you place a load balancer in front of each VIP Enterprise Gateway.

About Self Service Considerations

The Self Service Portal enables your end users to manage their VIP credentials including registration, testing, or resetting credentials, and removing credentials from their accounts if they are lost or stolen.
Users can connect to the VIP Self Service Portal by signing in with their enterprise AD/LDAP user name and password, which authenticates from VIP Enterprise Gateway through IdP functionality.

Considerations for deploying Self Service include the following:

- **From what location will users access the VIP EG IdP function?**
  If your enterprise decides that users can only access VIP EG from within your enterprise network, you can locate the VIP EG IdP in your back-office network, most likely on the same machine as VIP Enterprise Gateway. However, this decision means remote users are not be able to perform VIP Self Service tasks, such as registering their VIP credential, without being physically connected to your enterprise network or calling the IT help desk to complete these tasks.
  If your enterprise decides to enable remote users to access VIP Self Service from outside your enterprise network to perform tasks, such as registering their credential, you can set up an IdP Proxy in your enterprise’s perimeter network to proxy IdP requests to the VIP Self Service Portal IdP that is hosted inside your enterprise network.
  See the *VIP Intelligent Authentication Enterprise Integration Guide* on how to set up a Self Service Portal IdP Proxy,
  See Figure 7-2 on page 59.

- **Should users be required to verify their identity before registering a VIP credential?**
  If you allow remote users to register their VIP credentials from outside your enterprise network, you need to verify their identity before you can allow them to register their credentials. This consideration is especially important if, after registering credentials, users have a higher level of access to network resources than before.
  VIP provides the following Out-of-Band (OOB) capabilities to verify a user's identity:
    - Email
    - SMS to the user’s mobile phone
    - A call to the user’s registered phone number
  VIP uses the user’s email and phone numbers that are found in the corporate AD/LDAP to accomplish this task. Optionally, the phone numbers can be added to the user as Out-of_Band credentials. If you want to use SMS or voice call, you need to make sure that the phone numbers are current, accurate, and properly formatted with complete country code and area codes.
VIP Manager Deployment Considerations

Before you can deploy VIP Manager, you need to consider the following issues:

- Who has access to VIP Manager?
  In general, you need to give VIP Manager access to administrators who control VIP deployment policies, generate VIP reports, help VIP users troubleshoot their credentials, and manage VIP deployment in your enterprise.

- What roles does each person play in VIP Manager?
  You can view the roles that each person plays in VIP Manager in the FAQ list "Who are the people involved in the VIP deployment."
  See “About Corporate Policy Considerations” on page 30.

- Can you access VIP Manager directly or utilize Single Sign On (SSO)?
  VIP Manager allows users to sign in either via their enterprise AD user name and password or using separate accounts created inside VIP Manager.
  To allow users to sign in with AD credentials, you must configure Enterprise Gateway specifically for this purpose. To allow users to sign in through separately created accounts inside VIP Manager, you need to create these accounts initially from the Master Administration page in VIP Manager. Afterward, VIP Manager users with permission can to create new accounts.

- What roles in VIP Manager do not require a VIP credential?
  VIP Manager, by default, requires a user to sign in with a VIP credential. Enterprise administrators can decide to relax these requirements for some users that have certain roles inside VIP Manager and allow them to sign in using user name and password.

About Planning for Application Integration

When you plan for application integration with VIP, you need to determine the type of integration you need, and which application integration to use.

VIP supports a variety of applications, including Microsoft Outlook Web Access, Tivoli Access Manager, F5 BIG-IP, and Oracle Access Manager. For a complete list of applications, review the VIP Integration Guides that are available in VIP Manager. VIP continuously increases support for applications. Be sure to check this list frequently for updates.

If you cannot locate your application in VIP Integration Guides, VIP may still work with the application if it supports RADIUS authentication. This is true of most VPN gateways. In this case, it is recommended that you follow your application's configuration guide for RADIUS authentication and delegate that authentication to VIP Enterprise Gateway.
If you are unable to locate your application in the list, contact the Symantec VIP Support Team for additional options.

**About Authentication Modes**

Before you can set up VIP Enterprise Gateway for validation, you need to review the various authentication modes the server supports.

*Table 5-4* lists the authentication mode that are supported by servers.

<table>
<thead>
<tr>
<th><strong>Table 5-4</strong></th>
<th>Authentication Modes Supported by Server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What will be received by Validation Server</strong></td>
<td><strong>Who is responsible for authenticating UserID+Password</strong></td>
</tr>
<tr>
<td>UserID+LDAP Password + Security Code</td>
<td>VIP Enterprise Gateway, validating against the local user store</td>
</tr>
<tr>
<td>UserID+ LDAP Password + Security Code (RADIUS Access challenge mode)</td>
<td>VIP Enterprise Gateway, validating against the local user store</td>
</tr>
<tr>
<td>UserID + Security Code</td>
<td>The application, against its own user store</td>
</tr>
</tbody>
</table>

With multiple applications, you may need to set up multiple instances of the Validation server on separate ports in VIP Enterprise Gateway operating in different modes. For example, if you have a VPN application that forwards UserID+LDAP Password+Security Code to VIP Enterprise Gateway, and another application, such as OWA, that forwards only UserID+Security Code to VIP Enterprise Gateway, then you need two instances of the Validation server. One instance manages the UserID+LDAP Password+Security code validation for VPN, and the other instance handles UserID+Security Code validation for OWA.
Planning for Credential Deployment

This chapter includes the following topics:

- About Planning for Credential Deployments
- About Planning for Credential Acquisition
- Planning for Credential Registration
- Planning for Credential Management and Support
- About Planning for End-user Communication

About Planning for Credential Deployments

You need to familiarize yourself with the following distinct phases when you plan for credential deployment:

- Credential acquisition
  You need to decide on the type of credentials that are used by a certain set of users and how to deliver each type to your users

- Credential registration
  You need to decide on the method that your end users use to register their credentials and associate their user names with those credentials so VIP can identify the credentials that associated with the users

- Credential usage
  You need to decide on the users who use certain applications that are protected with the VIP credential

- Credential management
You need to decide about the best way to help your users to reduce interruptions when they encounter issues with their credentials.

### About Planning for Credential Acquisition

Your enterprise may design its own way of getting credentials to the user’s hands. As Chapter 2 mentioned, VIP credentials come in software and hardware versions. You can distribute software credentials by providing downloads to users through their mobile phones or notebook PCs. You can distribute hardware credentials by shipping to a user’s designated address or by making them available for pick-up at a known location, such as an IT manager’s desk at various sites.

Symantec recommends the following process for the distribution of VIP credentials:

- If a user has a corporate-issued mobile phone, have the user acquire a VIP mobile credential with a mobile download.
- If a user does not have a corporate-issued phone but has a personal phone, have the user acquire a VIP mobile credential, though there may be a cost associated with using the data plan to download and assign a credential.
- If a user does not have a corporate phone or personal phone, or does not wish to use a mobile credential, have the user download a VIP Access Desktop credential onto his or her corporate PC.
- If a user does not want to have either a mobile credential or a desktop PC credential, have the user obtain a VIP hardware credential (a key fob or a card). Your enterprise can either mail a credential to the user or have hardware credentials available at a known location for the user to pick up.

Since this process promotes software credentials and uses a self-service model for users to acquire their own credentials, your enterprise can maintain a low-cost for credentials and their distribution.

### Planning for Credential Registration

After credential distribution, users must register their credentials before use on an application like VPN. Credential registration associates a user’s name with the credential ID in his or her possession.

The following methods of credential registration are available:

- **Self Service Registration**
  - To register, the user Signs In to the VIP Self Service Portal which prompts him or her to enter the credential ID found on the credential and one security code generated from the credential.
Before you can use the self-service model for user registration, you need to determine if users need OOB authentication to access the VIP Self Service Portal. The user can request an OOB authentication credential via the Self Service Portal. The VIP Service then sends a one-time security code to the user by email, by SMS to the user's phone, or by a phone call to the user's registered phone number. The user needs to enter the security code on the registration page at the Self Service Portal before proceeding to register. OOB authentication prevents anyone who has stolen a corporate user's sign-in and password, and has downloaded a credential on his own phone, from posing as the real corporate user and registering a credential for VIP-enabled applications such as VPN.

If your enterprise decides to allow remote users outside the corporate network to access the Self Service Portal for self-service registration, we recommend enforcing OOB authentication. However, if your enterprise decides that only users who are on the corporate network can self-service register their credential, you do not need OOB authentication. You can configure OOB authentication in the VIP Policy Configuration section of VIP Manager.

- **IT Help Desk Registration**
  
  Your enterprise IT help desk can also register a user's credential for the user. VIP Manager provides a web interface for IT help desk personnel to sign in and search the user by name. Once the help desk finds a user's name, it can simply enter the user's credential ID to register the user. Help desk registration is useful when users cannot register for themselves. For example, if a user is not on the corporate network and cannot access the Self Service Portal, or if your enterprise mails hardware credentials to users, you can decide that the help desk will pre-register the credential for the user before the mailing. You may decide to use this option to provide the credential user a higher level of service.

### Planning for Credential Management and Support

After a successful roll-out, users may come across issues with their credentials when used at VIP-enabled applications. Some of the most common issues may include:

- **User does not have his or her credential, but needs to sign in immediately**
  
  When users do not have a credential handy, they cannot sign in to a VIP application, such as the VPN. If they want to have access to the application immediately, the user need to obtain a temporary code to enter in place of the security code from their credential.

  The following methods are available to obtain a temporary code:

  - The user can sign in to the VIP Self Service Portal with the usual enterprise user name and password and request a temporary code. The VIP Self Service Portal...
Portal sends the user a temporary code by email, SMS to the user's mobile phone in the corporate directory, or a voice call to the user's phone number in the directory.

- Alternatively, if the user cannot obtain a temporary security code via self service, the user can call the IT help desk to be issued a temporary security code offline.

The user can then sign in to the VIP application using the temporary code. The corporate administrator can set temporary security code policies by including length of code, and effective time duration, in VIP Manager's VIP Policy Configuration section.

- User lost his or her credential and needs to register a replacement
  As soon as the user obtains a new credential, the user may need to remove the old credential from his or her account. The user can remove a previously-registered credential on the Self Service Portal, and your enterprise IT department can set a policy in VIP Manager to control whether the user would need some kind of OOB authentication before removing a credential. Alternatively, if the user cannot perform self service to remove the previously registered credential, he or she can call the IT help desk to remove a credential through the VIP Manager tool.
  Registering a replacement credential follows the same process as registering a new credential.
  See “Planning for Credential Registration” on page 49.

- User's credential does not seem to work
  Sometimes the VIP Service may reject the security code entered by the user. Most often, this issue is caused by the credential's time clock not accurately reflecting the time. The user can simply re-synchronize the credential's clock in the ID Protection Center by entering the credential's Credential ID and security code.
  Alternatively, the user can call the IT help desk to synchronize the user's credential through VIP Manager.

About Planning for End-user Communication

End-user communication is a very important aspect of the VIP credential deployment process. The users need to know how to participate in the process. In general, end-user communication should cover the following information:

- What
  What is this initiative?

- Why
  Why are we doing this?
Who will be impacted by this deployment process?

How will users participate in the deployment process?

When will this process commence?

Where to go for more information?

About Planning for Token Fulfillment

Because these tokens are tangible items, they may get lost, broken, or stolen. If you plan to use physical tokens, you need to consider the following issues:

- How many tokens do you need?
  Beyond providing each user who needs a physical token with one, there are other considerations such as planning for broken and lost tokens. It is recommended that you plan for a reserve of 10% more tokens as replacements for broken or lost tokens.

- How long does it take to order a token?
  There is a lead time for ordering tokens. Therefore it is important to plan ahead and not wait until the last token is gone before ordering new ones.
VIP Deployment by Example

This chapter includes the following topics:

- About VIP Deployment Examples
- Basic Complexity: Enterprise 1
- Medium Complexity: Enterprise 2
- Non-VPN Application Integration: Enterprise 3

About VIP Deployment Examples

The following examples demonstrate various levels of complexity and describe common applications and deployment scenarios for VIP in an enterprise:

Basic Complexity: Enterprise 1

One of the most common applications for VIP in an enterprise is to add strong authentication to VPN access to ensure protection of enterprise network resources. The following topics illustrate this use-case for a fictional company, Enterprise 1.

Enterprise 1 Requirements Overview

Enterprise 1 Corporation has about 500 employees, 100 of which work remotely, or away from the main corporate office. Enterprise 1 is currently using two VPN gateways deployed in a perimeter network at the same physical location. Currently, a user authenticates to the VPN using an existing user name and password found in the corporate AD. The authentication is achieved by connecting the VPN gateways to a RADIUS Authentication Server that occasionally copies the user name/passwords from the corporate AD.
Enterprise 1 has decided to deploy VIP strong authentication for VPN users. Since most corporate users have company-issued mobile phones, Enterprise 1 decided to use VIP Mobile as the preferred credential. For those employees without corporate-issued mobile phones, Enterprise 1 will issue VIP hardware credentials.

Enterprise 1 also needs the VIP deployment to provide some kind of logging to conform to auditing requirements and high availability to ensure business continuity.

In terms of end-user support, the Enterprise 1 IT Department prefers the self-service model when users have trouble with their credentials while they are on the corporate network. However, for users with no access to corporate network—for example, when users are remote—the IT Department provides support over the phone.

Further, Enterprise 1 has decided to create new accounts for the help desk personnel to sign in to VIP Manager using its default account management features, rather than using their AD user name and passwords.

Enterprise 1 Solutions Overview

For basic VPN applications, we recommend configuring the VPNs to connect to VIP Enterprise Gateways via RADIUS to validate both the user's first-factor and the second-factor authentication. Deploy two Enterprise Gateways, along with a load balancer in front of them, to achieve high availability for access to the VIP Self Service Portal for both registration and troubleshooting.

VIP Deployment Network Diagram

Figure 7-1 illustrates components of the VIP deployment in Example 1.
Figure 7-1  Enterprise 1: VIP Deployment Diagram

Table 7-1 lists the name of the components for a VIP deployment in Example 1.

Table 7-1  Components of VIP Deployment in Example 1

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>User Access</td>
<td>Remote VPN users use VIP mobile credentials or VIP hardware credentials to access the two VPN gateways.</td>
</tr>
<tr>
<td>Listing</td>
<td>Name of Component</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>B</td>
<td>VPN gateways</td>
<td>Two VPN gateways enable employees to remotely access the corporate network. VIP is the authentication mechanism for each of these gateways. Each VPN gateway is configured to forward authentication requests via RADIUS to the two VIP Enterprise Gateways. Redundancy is achieved by configuring VPN 1 to forward RADIUS authentication to VIP EG 1 first, and then VIP EG 2; and configuring VPN 2 to forward RADIUS authentication to VIP EG 2 first, and then to VIP EG 1.</td>
</tr>
<tr>
<td>C</td>
<td>VIP Enterprise Gateways</td>
<td>Enterprise Gateways provide RADIUS validation services for two-factor authentication. They also act as identity providers for the in-cloud VIP Self Service Portal by connecting to the local LDAP database, providing authentication service of enterprise users before they are authorized any access to the VIP SSP in-cloud.</td>
</tr>
<tr>
<td>D</td>
<td>LDAP database</td>
<td>Each VIP Enterprise Gateway requires access to the LDAP user store hosted in close network proximity. The LDAP user store is used for end users authentication for both the VPN gateways and the VIP Self Service Portal.</td>
</tr>
<tr>
<td>E</td>
<td>Load Balancers</td>
<td>Load balancers ensure redundancy and failover for the two VIP Enterprise Gateways that act as Identity Providers for the in-cloud VIP Self Service Portal.</td>
</tr>
</tbody>
</table>
Table 7-1  Components of VIP Deployment in Example 1 (continued)

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| F       | Corporate Network / Back-office Users | - **Enterprise Configuration Administrator**  
The administrator configures and manages VIP Enterprise Gateways and VIP Manager. To manage VIP Enterprise Gateways, an administrator generally accesses directly with the IP address of the gateway servers. To manage VIP Manager, an administrator signs into the in-cloud VIP Manager portal.  
- **Help Desk**  
The help desk supports the end users with their access to the network when self service is not possible (for example, when a user is outside the corporate network). Help desk personnel sign in to the VIP Manager portal hosted in-cloud using accounts created for them by the Enterprise Configuration Administrator and stored in VIP Manager. Through this portal, they can manage a user’s credential—such as unlocking it once it is locked, registering a new credential, etc.  
- **Corporate VPN User**  
Users that require access to the corporate network. The users access VIP Enterprise Gateway through load balancers to authenticate themselves before being granted access to the VIP in-cloud Self Service Portal to perform self registration, as well as credential self service. |
| G       | VIP Authentication Service         | The VIP Authentication Service is a black-box service in the cloud provided by Symantec that primarily validates second-factor credentials, maintains credential and end-user management information, and provides end-user self-service functions. |
| H       | Logging                            | VIP Enterprise Gateway is configured to log access history in a local file store for this deployment.                                         |

**Medium Complexity: Enterprise 2**

A more complex use-case for the VPN application is when VPN gateways and the user store are in different physical locations. The deployment of VIP Enterprise...
Gateway has to adapt to the location issue while still supporting fault tolerance. Further, some enterprises may want to further reduce IT help desk cost by requiring users to perform self service for both credential registration and credential management, even when they are at a remote location, thus reducing phone calls to the corporate help desk personnel. Below is an example for such a deployment scenario.

Enterprise 2 Requirements Overview

Enterprise 2 is a 5000-employee company created through a merger of two different companies. The company has two main sites: one on the East coast and one on the West coast. Its main user database is an Active Directory hosted in both locations, kept in sync through AD replication. Its employees are also concentrated in these two main locations; however, each has its own mix of local and remote employees.

Enterprise 2 wants to deploy SSL VPN with strong authentication to enable employees to access corporate network resources. It has decided to deploy VIP Mobile as the preferred credential form factor for employees with enterprise-issued mobile phones and the VIP hardware credential as the back-up form factor. It wants to put one VPN gateway on each of the two physical locations.

Enterprise 2 also needs the VIP deployment to include failover support and logging to a central log server for audit and compliance, as well as to make the VIP Self Service Portal available to end users regardless whether they are on the corporate network or not.

In terms of help desk support, Enterprise 2 has decided that help desk personnel should authenticate to VIP Manager using their existing enterprise sign-in and password.

Enterprise 2 VIP Solution Overview

To support this deployment scenario, we recommend two instances of Enterprise Gateways, one at each physical location. The two VPN gateways are again connected to Enterprise Gateways through RADIUS, just as in the previous example, and each Enterprise Gateway is connected to the local AD user store. We recommend two load balancers, one at each site, deployed in front of each Enterprise Gateway to ensure high availability access to the Self Service Portal.

To ensure remote access to the Self Service Portal, it is recommended that Enterprise 2 deploy two instances of VIP Enterprise Gateways, one in each perimeter network of each physical location, configured as a Self Service Portal IdP Proxy. Further, to enable help desk personnel to authenticate to VIP Manager using their
existing enterprise sign-in and password, Enterprise Gateways needs to be configured as an IdP to the Symantec-hosted VIP Manager.

VIP Deployment Network Diagram

*Figure 7-2* illustrates components of the VIP deployment in Example 2.

*Figure 7-2*  Enterprise 2: VIP Deployment Diagram

> Table 7-2 lists the name of the components for a VIP deployment in Example 2.
Table 7-2 Components of VIP Deployment in Example 2

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>User Access</td>
<td>Remote VPN users use VIP Mobile or VIP hardware credentials to access the two VPN gateways. When these remote VPN users need to register their VIP credentials or need to perform self-service management of their credentials, they will be accessing the VIP Self Service Portal through the VIP Enterprise Gateway Self Service Portal IdP proxy.</td>
</tr>
<tr>
<td>B</td>
<td>VPN gateways</td>
<td>Two VPN gateways, one at each site, enable employees to remotely access the corporate network. VIP is the authentication mechanism for each of these gateways. Each VPN gateway is configured to forward authentication requests via RADIUS to the two VIP Enterprise Gateways. Redundancy is achieved by configuring VPN 1 to forward RADIUS authentication to VIP EG 1 first, and then VIP EG 2; and configuring VPN 2 to forward RADIUS authentication to VIP EG 2 first, and then to VIP EG 1.</td>
</tr>
<tr>
<td>C</td>
<td>VIP Enterprise Gateway SSP IdP Proxy</td>
<td>The SSP IdP Proxy is deployed to enable secure access to the VIP Enterprise Gateway's Self Service Portal IdP. VIP Enterprise Gateway needs to access to the enterprise's Active Directory. Locating VIP Enterprise Gateway in the perimeter network, while enabling remote users access to the SSP IdP for self-service tasks, will create a security concern as a firewall rule must be created to allow access from the perimeter network to the enterprise's Active Directory in the back-end network. The VIP EG IdP Proxy is an ideal solution to enable remote access to the Self Service Portal while ensuring network security.</td>
</tr>
</tbody>
</table>
Table 7-2 Components of VIP Deployment in Example 2 (continued)

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>VIP Enterprise Gateways</td>
<td>Provides RADIUS validation services for two-factor authentication. It also acts as an identity provider for the in-cloud VIP Self Service Portal, as well VIP Manager for help desk personnel, by connecting to the local LDAP database and providing authentication service of enterprise users before they are authorized any access to the VIP SSP and VIP Manager in-cloud. In this deployment scenario, one instance of the EG is deployed in each of the physical locations.</td>
</tr>
<tr>
<td>E</td>
<td>LDAP database</td>
<td>Each VIP Enterprise Gateway requires access to the LDAP user store hosted in close network proximity. The LDAP user store is used for end-users' authentication for the VPN gateways, as well as for VIP Self Service Portal. In this deployment scenario, each EG is connected to the local LDAP (AD) instance, and the two ADs at two physical locations are synced through AD sync.</td>
</tr>
<tr>
<td>F</td>
<td>Load Balancers</td>
<td>Two load balancers ensure redundancy and failover for the two VIP Enterprise Gateways acting as Identity Providers for the in-cloud VIP Self Service Portal and VIP Manager. One load balancer is deployed in each of the two physical locations.</td>
</tr>
<tr>
<td>Listing</td>
<td>Name of Component</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| G       | Corporate Network / Back-office Users     | Enterprise Configuration Administrator  
The administrator configures and manages VIP Enterprise Gateways and VIP Manager. To manage VIP Enterprise Gateways, an administrator generally accesses directly with the IP address of the gateway servers. To manage VIP Manager, an administrator signs into the in-cloud VIP Manager portal.  
Help Desk  
The help desk supports the end users with their access to the network when self service is not possible (for example, when a user is outside the corporate network). Help desk personnel sign in to the VIP Manager portal hosted in-cloud using accounts created for them by the Enterprise Configuration Administrator and stored in VIP Manager. Through this portal, they can manage a user's credential—such as unlocking it once it is locked, registering a new credential, etc.  
Corporate VPN User  
Users that require access to the corporate network. The users access VIP Enterprise Gateway through load balancers to authenticate themselves before being granted access to the VIP in-cloud Self Service Portal to perform self registration, as well as credential self service. |
| H       | VIP Authentication Service                | The VIP Authentication Service is a black-box service in the cloud provided by Symantec that primarily validates second-factor credentials, maintains credential and end-user management information, and provides end-user self-service functions. |
| I       | Logging                                  | The two VIP Enterprise Gateways are configured to send logs to a syslog service deployed at one of the two sites. |
Non-VPN Application Integration: Enterprise 3

VIP Enterprise Authentication supports other applications beyond just VPN. This example illustrates how VIP supports strong authentication to Microsoft Outlook Web Access (OWA).

Enterprise 3 Requirements Overview

Enterprise 3 is a 500-user company with about 100 remote users. The Enterprise 3 IT Department wants to enable VPN access to enterprise network resources, as well as enable remote users to access their Outlook exchange via OWA. But it wants to ensure that strong authentication is enforced for these two applications.

Enterprise 3 plans to deploy one VPN gateway, and one OWA server to start, hosted inside a perimeter network. It has decided to deploy VIP strong authentication for VPN and OWA users. Since most corporate users have company-issued mobile phones, it has decided to use VIP Mobile as the preferred form factor credential. For those employees without corporate-issued mobile phones, Enterprise 3 will issue VIP hardware credentials.

Enterprise 3 also needs the VIP deployment to include some kind of logging to conform to auditing requirements and high availability to ensure business continuity.

In terms of end-user support, the Enterprise 3 IT Department prefers the self-service model when users have trouble with their credentials while they are on the corporate network. However, for users having no access to corporate network—for example, when users are remote—the IT Department will provide support over the phone.

Further, Enterprise 3 has decided to create new accounts for the help desk personnel to sign in to VIP Manager using its default account management features, rather than using their AD user name and passwords.

Further, Enterprise 3 wants to turn on VIP Enterprise Gateway’s LDAP sync feature to ensure that, when a user leaves the organization, the VIP Self Service Portal will automatically remove that user’s account.

Enterprise 3 VIP Solution Overview

For basic VPN applications, we recommend configuring VPN to connect to VIP Enterprise Gateways via RADIUS to validate both the user’s first-factor and second-factor authentication. We recommend deploying two Enterprise Gateways, along with a load balancer in front of them, to achieve high availability for access to the VIP Self Service Portal for registration and troubleshooting.

For the OWA application, we recommend installing VIP’s integration module for OWA on the OWA IIS server. The OWA server will validate the user’s first-factor (user name and password) against the Exchange Server (which performs the
authentication against AD). Once the first-factor authentication is successful, VIP’s OWA module will take over to authentication the user’s second-factor (user name, security code) against VIP Enterprise Gateway.

VIP Deployment Network Diagram

Figure 7-3 illustrates the components of the VIP deployment in Example 3.

Table 7-3 lists the name of the components for a VIP deployment in Example 3.
<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>User Access</td>
<td>Remote VPN users use VIP Mobile or VIP hardware credentials to access the VPN gateway, as well as the OWA application.</td>
</tr>
<tr>
<td>B</td>
<td>VPN gateways</td>
<td>The VPN gateway enables employees to remotely access the corporate network. VIP is the authentication mechanism for the gateway. The VPN gateway is configured to forward authentication requests via RADIUS to two VIP Enterprise Gateways</td>
</tr>
<tr>
<td>C</td>
<td>OWA Server</td>
<td>The OWA Server enables remote employees to sign in to the exchange server via the web to access their Outlook email, etc. It is integrated with the VIP OWA module to enable strong authentication. The OWA Server validates the user's first-factor against the enterprise Exchange server just as before, when strong-authentication is not enabled. And the VIP OWA integration module validates the user's second-factor to enforce strong authentication by checking the user name and security code against VIP Enterprise Gateways via RADIUS.</td>
</tr>
<tr>
<td>D</td>
<td>VIP Enterprise Gateways</td>
<td>Provides a RADIUS validation services for two-factor authentication. It also acts as an identity provider for the in-cloud VIP Self Service Portal by connecting to the local LDAP database, providing authentication service of enterprise users before they are authorized any access to the VIP SSP in-cloud. Additionally, one VIP Enterprise Gateway is configured to perform periodic synchronization of local AD against the in-cloud VIP Self Service Portal to ensure the user accounts in-cloud match that in the local AD</td>
</tr>
<tr>
<td>E</td>
<td>The Exchange Server</td>
<td>The Exchange Server is the Microsoft Exchange Back-end Server to the OWA Server front end. It is connected to the AD for exchange server authentication and provides outlook data to the OWA server in the perimeter network.</td>
</tr>
</tbody>
</table>
Table 7-3  Components of VIP Deployment in Example 3 (continued)

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>LDAP database</td>
<td>Each VIP Enterprise Gateway, as well as the Exchange Server, requires access to the LDAP user store hosted in close network proximity. The LDAP user store is used for end-users authentication for both the VPN gateway and the VIP OWA Integration Module (user name only), as well as for VIP Self Service Portal.</td>
</tr>
<tr>
<td>G</td>
<td>Load Balancers</td>
<td>Load balancers ensure redundancy and failover for the two VIP Enterprise Gateways acting as Identity Providers for the in-cloud VIP Self Service Portal.</td>
</tr>
</tbody>
</table>
### Table 7-3 Components of VIP Deployment in Example 3 (continued)

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| H       | Corporate Network / Back-office Users    | - Enterprise Configuration Administrator  
  The administrator configures and manages VIP Enterprise Gateways and VIP Manager. To manage VIP Enterprise Gateways, an administrator generally accesses directly with the IP address of the gateway servers. To manage VIP Manager, an administrator signs into the in-cloud VIP Manager portal.  
  - Help Desk  
  The help desk supports the end users with their access to the network when self service is not possible (for example, when a user is outside the corporate network). Help desk personnel sign in to the VIP Manager portal hosted in-cloud using accounts created for them by the Enterprise Configuration Administrator and stored in VIP Manager. Through this portal, they can manage a user's credential—such as unlocking it once it is locked, registering a new credential, etc.  
  - Corporate VPN User  
  Users that require access to the corporate network. The users access VIP Enterprise Gateway through load balancers to authenticate themselves before being granted access to the VIP in-cloud Self Service Portal to perform self registration, as well as credential self service. The corporate policy can dictate specific credential types available to users, or to members within particular user groups. For example, one user group may be restricted to using only hardware credentials for VPN access, while both hardware and software credentials may be available to another user group for VPN access. |
| I       | VIP Authentication Service               | The VIP Authentication Service is a black-box service in the cloud provided by Symantec that primarily validates second-factor credentials, maintains credential and end-user management information, and provides end-user self-service functions. |
Table 7-3 Components of VIP Deployment in Example 3 (continued)

<table>
<thead>
<tr>
<th>Listing</th>
<th>Name of Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>J</td>
<td>Logging</td>
<td>VIP Enterprise Gateway is configured to log access history in a local file store for this deployment.</td>
</tr>
</tbody>
</table>
Other Common Variations and Requirements

This chapter includes the following topics:

- About LDAP Directory Synchronization
- About Tunneling

About LDAP Directory Synchronization

The LDAP Directory Synchronization Service enables you to automatically synchronize the user IDs in your LDAP directory with the user data in the VIP Authentication Service. This feature eliminates the need for manual editing of the user list in the VIP Authentication Service to keep it synchronized with the users in your LDAP.

Although VIP user and administrator groups can be created, modified, or removed in VIP Manager, VIP group members are mapped to each group through LDAP synchronization in VIP Enterprise Gateway:

- Administrator groups
  Both administrator groups and super administrator groups are added in VIP Manager. However, while administrator groups can be mapped in the VIP Enterprise Gateway configuration console, super administrator groups are system-generated by default and never mapped or synchronized in VIP Enterprise Gateway.

- User groups
  User groups are created in VIP Manager and then mapped in the VIP Enterprise Gateway configuration console. You need to synchronize the user groups in your LDAP directory with the user data in the VIP User Service.
About Tunneling

If your client applications, such as a VPN gateway, cannot access VIP Enterprise Gateway over UDP because of firewall rules or network policies, then you need to open a TCP port through your firewall and configure a tunnel forwarder and receiver pair using the Configuration Console in VIP Enterprise Gateway. The tunnel forwarder and receiver act together as a tunnel to carry UDP-based RADIUS validation requests from your client application to VIP Enterprise Gateway.

You set up a tunnel forwarder to forward validation requests from outside your network firewall to your VIP Enterprise Gateway. For example, if your VPN gateway resides in your perimeter network, you can set up a tunnel forwarder in the perimeter network to send validation requests to a tunnel receiver inside your firewall. Setting up a tunnel forwarder in this case means installing VIP Enterprise Gateway software on a machine, configuring this VIP Enterprise Gateway for Radius Validation, configuring it as a tunnel forwarder, and placing the machine inside your perimeter network. You also need to configure your VIP Enterprise Gateway inside your network to add a tunnel receiver.

Figure 8-1 illustrates the tunnel concept.
See the *VIP Enterprise Gateway Installation and Configuration Guide* for more information on how to set up tunnel forwarders and receivers,
Symbols
  tunnel forwarder and receiver 19

A
  Active Directory 17
  Administrator groups 69
  application integration
    planning for 46
  authentication 6
    first factor 28
    levels 24
    risk-based 22
    second factor 28

B
  Binary Runtime Environment for Wireless
    see BREW 8
  black-box service 57, 62, 67

C
  communication channels, security recommendations
    for 43
  configuration
    Enterprise Gateway for RADIUS validation 28
    VIP Validation Service 47
  credential
    acquisition of 26, 49
    assign 26
    deployment of 48
    management and support of 50
    manual activation of 22
    manual assignment of 22
    number allowed per user 30
    registration of 49
  credential type
    custom-embedded 15
    Security Code via SMS 11–12
    Security Code via Voice Call 12
    VIP Access Desktop 10
    VIP Access for Mobile 8
    credential type (continued)
      VIP Security Cards 13
      VIP Security Tokens 12
      VIP Trusted Device 14

D
  deployment
    end-to-end testing of 28
    Enterprise 1 basic complexity 53
    Enterprise 3 non-VPN complexity 63
    examples of 53
    overview 16
    people impacted during 31–32
    planning 30, 47
  DMZ
    see perimeter network 17

E
  Enterprise 1 basic complexity deployment
    network deployment diagram 55
    requirements 53
    solutions 54
  Enterprise 2 medium complexity deployment
    requirements 58
    solutions 59
  Enterprise 3 non-VPN complexity deployment
    requirements 63
    solutions 63
  Enterprise Gateway
    communication security for 42
    Configuration Console for 19
    deployment considerations of 32
    Identity Providers (IdPs) function of 19
    installing and configuring 27
    LDAP synchronization of 19
    logging function of 19
    physical security of 33, 43
    Self Service Portal 19
    tunnel forwarder and receiver 19
    Validation Server 19
example deployment
  basic (Enterprise 1) 53
  medium complexity (Enterprise 2) 58
  non-VPN (Enterprise 3) 63

F
failover and high availability 33
firewalls 33
first factor authentication 28

H
high availability and failover 33

I
IA. See Intelligent Authentication
Identity Providers (IdPs) 19
installing and configuring
  VIP Enterprise Gateway 27
Intelligent Authentication 22

L
LDAP directory synchronization 19, 21, 69
logging 19, 21, 33
  logging service 21
reporting and 44

M
manual credential
  activation 22
  assignment 22
Microsoft Outlook Web Access (OWA) 63

N
network deployment diagram
  basic complexity Enterprise 1 55
network topography
  with VIP 17
  without VIP 16

O
OATH open standards 6, 14
one-time password (OTP) 12
open standards
  OATH 6
OWA see Microsoft Outlook Web Access 63

P
password lock-out policy 30
perimeter network 17
physical security for Enterprise Gateway 43
PIN 22, 31
platform neutral devices 12
port and firewall considerations 42

R
RADIUS 18, 20, 28
  Validation 28
requirements
  basic complexity Enterprise 1 53
  medium complexity Enterprise 2 58
  non-VPN Enterprise 3 63
risk-based authentication 22

S
SAML
  identity provider 23
  service provider 23
  with VIP Login 23
second factor authentication 28
second-factor VIP credential 21
Security Assertion Markup Language. See SAML
Security Code via SMS 11–12
Security Code via Voice Call 12
self service considerations 44
Self Service Portal proxy 19–20
short message service
  see SMS 11
SMS 11
Software Development Kit (SDK) 14
Symantec VIP Developer Toolkit 15

T
temporary security code 31
test deployment 25, 29
token fulfillment 52
Trusted Device 14, 23
tunnel forwarder and receiver 21
tunneling 21, 70

U
User groups 69
user groups 67
user store 21, 32–33
V
Validation Server 19–20
VIP 6
deployment
  see deployment 30
Security Cards 13
Security Tokens 12
Validation window 31
VIP Access Desktop 10
VIP Access for Mobile 8
VIP Authentication Service 11
VIP EG
  see VIP Enterprise Gateway 18
VIP Enterprise Gateway 18
  installing and configuring 27
VIP Login 23
VIP Manager 19, 22
deployment considerations 46
IdP 22
VIP Self Service 19
  IdP application 22
Portal 18, 22
VIP Validation Service 18, 21
voice call, security code via 12
VPN gateway 17