Symantec VIP Integration Guide for Microsoft Credential Provider

Table of Contents

About integrating Microsoft Credential Provider with Symantec VIP

The traditional user name and password authentication is no longer enough to meet today's evolving security threats and regulatory requirements. However, users demand an easy-to-use authentication solution. What is needed today is stronger and smarter authentication to secure corporate data and applications, while offering greater ease of use.

Symantec VIP is a cloud-based authentication service that enables enterprises to securely access online transactions, meet compliance standards, and reduce fraud risk. VIP provides an additional layer of protection beyond the 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 by phone call, by SMS text message or email, or by push notifications sent to a registered mobile device.

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 helps you prepare for VIP integration by providing a comprehensive outline for planning, decision making, and task prioritization for a successful deployment.

Users generate a security code on a VIP credential that they register with Symantec's VIP Service. They use that security code, along with their user name and password, to gain access to the resources protected by Credential Provider.

System requirements

The integration environment depicted in this document is based on using Microsoft Credential Provider with VIP Enterprise Gateway version 9.8.3 and later. Refer to the following for specific integration system requirements:

- Operating system requirements
- Hardware requirements
- Integration prerequisites

Operating system requirements

Online authentication

The Symantec VIP with Credential Provider for online authentication is available on the following platforms:

- Windows 7, Windows 8, Windows 8.1, Windows 10 (32-bit/64-bit)
- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 (64-bit), Windows Server 2019

Offline authentication

The Symantec VIP with Credential Provider for offline authentication is available only on the following platforms:

- Windows 10 (32-bit/64-bit)
- Windows 7 (32-bit/64-bit)

Offline authentication supports only one user per machine.

Hardware requirements

The Symantec VIP with Credential Provider for offline authentication is qualified on the following hardware:

- Symantec VIP Security Key
- Yubico Yubikey 4 Series
- Feitian U2F Security Key

Integration prerequisites

Online authentication

- Before you integrate Credential Provider with Symantec VIP for second-factor authentication, you must make sure that your first-factor authentication works.
- Install and configure VIP Enterprise Gateway. For configuration procedures, see the *Symantec VIP Enterprise Gateway Installation and Configuration Guide*, available on the Broadcom TechDocs portal.
- Visual C++ requirements:

Table 1: Visual C++ requirements for Symantec VIP with Credential Provider

Target operating system	System type	Software
Windows 7, Windows Server 2008, and Windows Server 2008 R2	32-bit	Visual C++ 2010 SP1 x86 Redistributable
	64-bit	Visual C++ 2010 SP1 x64 Redistributable
Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019	32-bit	Visual C++ 2012 x86 Update 4 Redistributable
	64-bit	Visual C++ 2012 x64 Update 4 Redistributable

Offline authentication

This is only applicable if you are planning to configure Symantec VIP with Credential Provider for offline authentication.

- Install Python 3.6.3 32-bit

  NOTE

  If you have 64-bit Windows operating system, you must still install the Python 32-bit application.

Contents of the integration package

The following files are provided as part of the Symantec VIP with Microsoft Credential Provider integration module software package.

Table 2: Contents of the integration package

Operating system	System type	Location
Windows Vista, Windows 7, Windows Server 2008	32-bit	Microsoft\Credential_Provider\Windows7\x86\VIP Enterprise Gateway Credential Provider.msi

Operating system	System type	Location
	64-bit	Microsoft\Credential_Provider\Windows7\x86_64\VIP Enterprise Gateway Credential Provider.msi
Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2012 R2, Windows Server 2016	32-bit	Microsoft\Credential_Provider\Windows8\x86\VIP Enterprise Gateway Credential Provider.msi
	64-bit	Microsoft\Credential_Provider\Windows8\x86_64\VIP Enterprise Gateway Credential Provider.msi

VIP supported features

lists the VIP Enterprise Gateway features that are supported with Credential Provider.

Table 3: VIP supported features

VIP feature	Support
First-factor authentication	
AD/LDAP password through VIP Enterprise Gateway	No
VIP PIN	Yes
Second-factor authentication	
VIP Push	Yes
SMS	Yes
Voice	Yes
Selective strong authentication	
End user-based	Yes
Risk-based	No
Target resource-based	No
General authentication	
Multi-domain	Yes
Anonymous user name	Yes
Allow Third-party Credential Providers along with Symantec Credential Provider	Yes
AD password reset	Yes
Integration method	
VIP JavaScript	No
VIP Login	No
SOAP Web Service APIs	No
Radius	Yes

Deployment considerations

Refer to the following considerations before integrating Symantec VIP with Microsoft Credential Provider.

Online authentication considerations

- Symantec VIP with Microsoft Credential Provider does not support second-factor authentication for folder sharing (UNC) and remote desktop connection (VNC).

The following limitations are specific to User ID–Access PIN– Security Code:

- An Active Directory password or a local password must be entered by the user for the first-factor authentication. The VIP Access PIN alone will not suffice for the first-factor authentication.
- An Access PIN cannot be reset if it is expired. It must be reset only through the VIP Self Service Portal.
- In Business Continuity (BC) mode, Push is not supported.

Offline authentication considerations

- Offline authentication does not support Remote Desktop, Virtual Machines, and Windows Server 2008/2012/2016/2019.

Authentication workflow

This section describes how the integration of Symantec VIP with Microsoft Credential Provider authenticates a user's access of protected resources. This workflow describes the integration for the **User ID–LDAP Password–Security Code** authentication method.

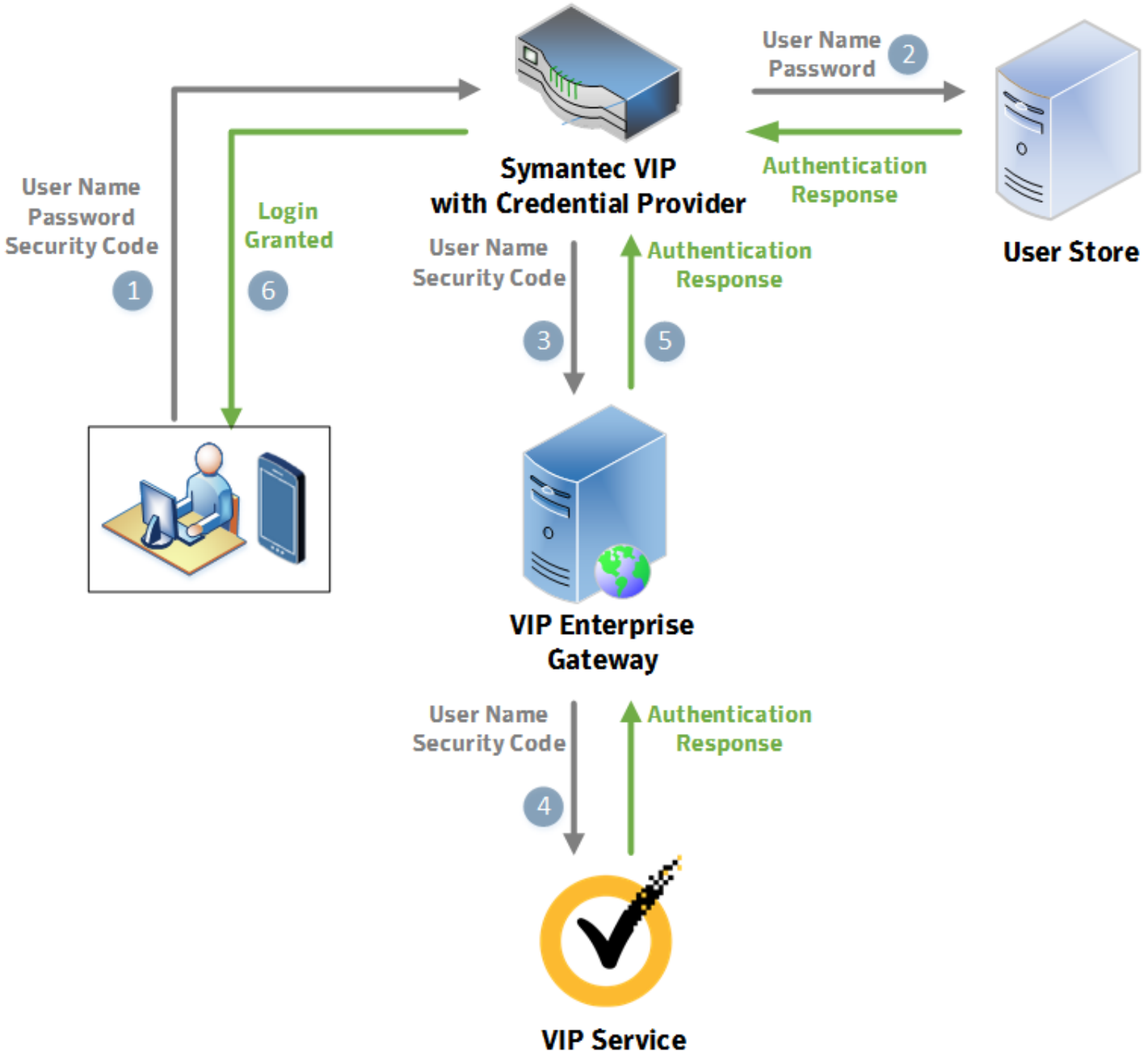

User Name
Password
2
Authentication
Response
User Store
Symantec VIP
with Credential Provider
User Name
Password
Security Code
1
Login
Granted
6
User Name
Security Code
3
Authentication
Response
5
VIP Enterprise
Gateway
User Name
Security Code
4
Authentication
Response
VIP Service

Table 4: Workflow description

Step	Description
1	The user enters an Active Directory (AD) user name and password to login page. If the user has a valid credential ID mapping, the user is prompted to enter the security code.
2	As the first part of the two-factor authentication process, Symantec VIP with Credential Provider sends the user name and the password to the User Store. For example, if AD/LDAP is the User Store, then Symantec VIP with Credential Provider sends the user name and password to your AD/LDAP server. If your User Store authenticates the user name and the password, the User Store returns the group permission details and the authentication response to Symantec VIP Credential Provider.
3	As the second part of the two-factor authentication process, Symantec VIP with Credential Provider sends the user name and the security code to VIP Enterprise Gateway for authentication.
4	The VIP Enterprise Gateway validation server authenticates the user name and the security code with VIP Service. VIP Service sends an authentication response to the VIP Enterprise Gateway validation server.
5	If VIP Service successfully authenticates the user name and the security code, VIP Enterprise Gateway returns an Access-Accept Authentication response to Symantec VIP with Credential Provider.
6	Based on the Access-Accept Authentication response, Symantec VIP with Credential Provider gives the user access to the protected resources.

This workflow describes the integration for the **User ID–Security Code** authentication mode.

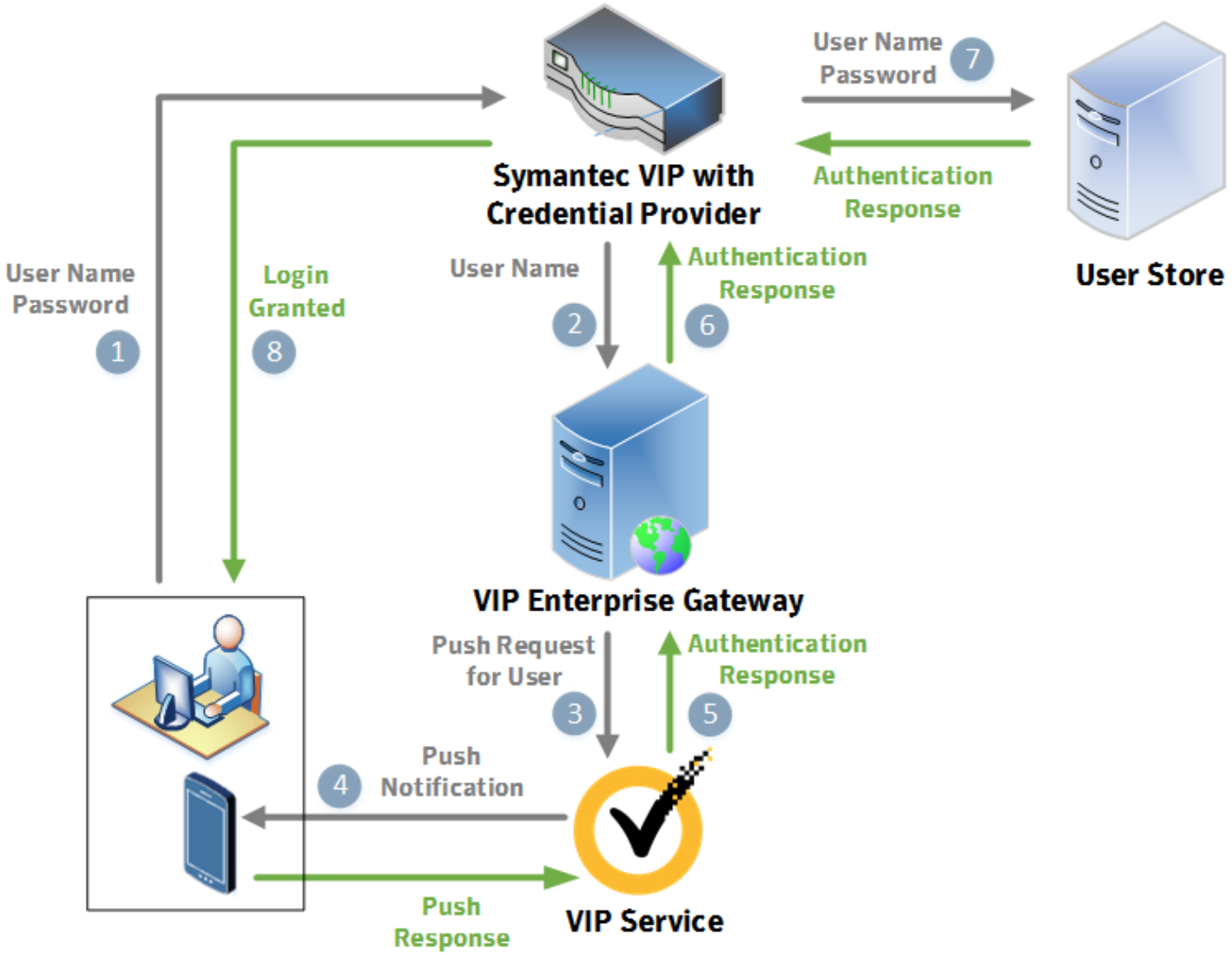


Table 5: Workflow description

Step	Description
1	The user enters an Active Directory (AD) user name and password to log in to the system.
2	As the first part of the two-factor authentication process, Symantec VIP with Credential Provider sends the user name and the Push key to VIP Enterprise Gateway.
3	The VIP Enterprise Gateway validation server instructs VIP Service to send a push to the credential associated with the user.
4	If the user has a VIP Access for Mobile credential that is enabled for VIP Access Push authentication, a push sign-in request is sent to the mobile device. The user taps Allow/Deny and the response is sent to VIP Service.
5	VIP Service sends the authentication response to the VIP Enterprise Gateway validation server.
6	Based on the response from VIP Service, the VIP Enterprise Gateway validation server sends an appropriate response to Symantec VIP with Credential Provider.

Step	Description
7	As the second part of the two-factor authentication process, Symantec VIP with Credential Provider sends the user name and the password to the user store (such as AD) to perform the domain authentication.
8	After the user name and the password are authenticated, users can log in.

Integrating Symantec VIP with Credential Provider

You can integrate Symantec VIP with Credential Provider in two ways:

- Integrate Symantec VIP with Credential Provider for online authentication.
  See Installing and configuring Symantec VIP with Credential Provider for online authentication.

  NOTE
  Once you have integrated VIP with Credential Provider for online authentication, you can perform advanced configurations. See Advanced configuration for online authentication
- Integrate Symantec VIP with Credential Provider for offline authentication.
  See Installing and configuring Symantec VIP with Credential Provider for offline authentication

Installing and configuring Symantec VIP with Credential Provider for online authentication

Complete the following general procedures to install and configure Symantec VIP with Microsoft Credential Provider for online authentication:

Table 6: Online authentication integration procedures

Step	Task
1	Ensure that you meet the minimum system requirements and prerequisites. See System requirements.
2	Add the User ID - Security Code Validation server. See Adding a User ID – Security code Validation server.
3	Add the User ID - Access PIN - Security Code Validation server. See Adding a User ID - Access PIN - Security Code Validation server.
4	Test the Validation servers. See Testing the Validation servers.
5	Manually install your Credential Provider. See Manually installing the Credential Provider.

Once you have installed and configured Symantec VIP with Credential Provider for offline authentication, test your integration.

See Testing the integration.

If you are an existing VIP Credential Provider user, you can also seamlessly upgrade your integration.

See Upgrading Symantec VIP with Credential Provider.

Adding a User ID – Security code Validation server

Complete the following steps to create a User ID – Security code Validation server:

1. Log in to VIP Enterprise Gateway and click the **Validation** tab.
2. Click **Add Server**. The Add RADIUS Validation server dialog box appears.
3. Configure the RADIUS validation parameters:

Field	Action
Vendor	Select **Microsoft** from the drop-down list.
Application Name	Select the vendor's application that you use, **Windows Credential Provider**.
Authentication Mode	Select the mode that you want to use for first and second-factor authentication. **User ID – Security code**: In this authentication mode, your User Store such as AD/LDAP validates the first-factor (user name and password). VIP Enterprise Gateway validates the second-factor (user name and security code) with VIP Service. Ensure that your first-factor validation works before selecting this authentication mode.

4. Click **Continue** to add the Validation server.

Adding a User ID - Access PIN - Security Code Validation server

Complete the following steps to add **User ID - Access PIN - Security Code** Validation server:

1. Log on to VIP Enterprise Gateway and click the **Validation** tab.
2. Click **Add Server**.
3. In Add RADIUS Validation server window, click custom configuration and do the following:
   - In the **Server Information** section, enter the details as per your requirement.
   - In the **RADIUS Access Challenge** section, select the **enable access challenge** check box and configure the **Challenge Timeout** as required. By default, the timeout value is 60 seconds.
   - In the First-Factor Authentication section, select the **Enable First Factor** check box and in the Authentication on field, select the **VIP Services** option.
   - Select the options in the User Store Configuration section based on your requirements.
4. Click **Submit**.

Testing the Validation servers

1. To test the Validation server, download and run the **vsradiusclient_test** utility. The utility is available in the **tools.zip** file from the VIP Manager website on the Symantec VIP Credential Provider client host, which you can access using verbose mode.
2. To test the User ID–Security Code authentication mode with security code, enter a command similar to the following. Use the appropriate values for your configuration.

```
C:\<tools_folder>\vsradiusclient_test.exe --server-host <your_server_ip> --server-port
<your_server_port> --secret <your_server_password> --client-ip <your_client_ip> --user-name
<username> --password <security_code> --verbose
```

3. To test the User ID–Security Code authentication mode with VIP Access Push-enabled, enter a command similar to the following. Use the appropriate values for your configuration.

```
C:\<tools_folder>\vsradiusclient_test.exe --server-host <your_server_ip> --server-port
<your_server_port> --secret <your_server_password> --client-ip <your_client_ip> --user-name
<username> --password <pushkey> --timeout <time_value> --verbose
```

NOTE

Enter `push` as the value for the **push** keyword.

4. To test the User ID–Access PIN–Security Code authentication mode, enter a command similar to the following. Use the appropriate values for your configuration.

```
C:\<tools_folder>\vsradiusclient_test.exe --server-host <your_server_ip> --server-port
<your_server_port> --secret <your_server_password> --client-ip <your_client_ip> --user-name
<username> --password <PIN+security_code> --verbose
```

Manually installing the Credential Provider

Complete the following procedures to install your Microsoft Credential Provider manually:

1. Install the version of Visual C++ appropriate to your operating system.

   See Integration prerequisites.

2. Download `Microsoft_Credential_Provider.zip` and `Tools.zip` from VIP Manager (**Account > Download Files > Third_Party_Integrations > Enterprise Gateway 9.8**).

3. Run the camouflage utility (available in the **tools** folder), specifying the password to encrypt on the command line. In these procedures, you must encrypt the following:

   - RADIUS shared secret
   - Proxy password if you are using a Windows proxy with basic authentication
   - Windows auto logon password, if you enable Windows auto logon

   The camouflage utility location is listed below:

Target operating system	System type	Folder location
Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2	32-bit	`tools\windows`
	64-bit	`tools\windows_64`
Windows 8, Windows 8.1, Windows 10, Windows Server 2012, and Windows Server 2012 R2, Windows server 2016, Windows Server 2019	32-bit	`tools\windows8`
	64-bit	`tools\windows_64`

4. For example, run:

```
camouflage <password>
```

   Where `<password>` is the password to encrypt. Do not use the following characters in the password, as this will lead to authentication failure: **& = "**

5. Using a standard text editor, modify `Microsoft_Credential_Provider\CPconfig.txt` to update the values as shown in the following table. A sample `CPconfig.txt` file is provided for your reference.

   See Sample file.

Option	Configuration details

Validation Server	Enter the correct RADIUS host IP address, port number, and the encrypted shared secret. For example, a line in the configuration file reads as follows:
	`Validation Server"="vipeg_server_ip:port:`
	`<camouflaged_password>`
	Where:
	• `vipeg_server_ip:port` is the IP address and the port number of the Validation Service (RADIUS server) to which Symantec VIP Credential Provider connects.
	• `<camouflaged_password>` is the encrypted version of the RADIUS shared secret obtained in the previous step.
	If you want to support failover to multiple RADIUS servers, add an additional parameter for the failover RADIUS server. For example,
	`"Validation Server"="vipeg_server_ip_1:port:`
	`<camouflaged_password>,vipeg_server_ip_2:port:`
	`<camouflaged_password>"`
	Use the same port number if you configure multiple VIP Enterprise Gateway servers for failover.
	Note: If more than one RADIUS server is configured and the servers are up, the validation requests are load-balanced in a round-robin sequence within a 20-second period.

Time Out	The default time-out value is set to 10 seconds. The retries define the number of attempts Symantec VIP Credential Provider makes based on the time-out configured before you decide that the Validation Service is not reachable.
Retries	The default value is set to 5.
Note: If you integrate out-of-band authentication (SMS, Voice, or Push), set the Time-out field to **20** seconds and the Retries field to **3** to avoid authentication failures. If the Retries field is unavailable, set the Time-out field to a minimum of **60** seconds.	
Allowed CP	When a third-party Credential Provider is replaced with Symantec VIP Credential Provider, there may be cases where all the users are not migrated to VIP yet and they need to be authenticated using the third-party Credential Provider. In such cases, the Allowed Credential Provider option can be used to enter the GUIDs of the other third-party Credential Providers that are allowed along with Symantec Credential Provider. The format for the flag is: {AllowedGUID1}:{AllowedGUID2} The default value of Allowed Credential Provider contains the GUIDs for Smartcard Pin Provider and WinBio Credential Provider. **Note:** Symantec recommends that you do not modify the Allowed CP default values. Modifying will result in two-factor authentication not working.
U2F Authentication	This setting indicates if authentication using VIP Security Keys (offline authentication) have been enabled. This setting defaults to 0, and is automatically updated. Do not change this setting. • If set to "0", offline authentication components have not been installed and U2F authentication is not enabled. • If set to "1", offline authentication components have been installed and U2F authentication is enabled.

Option	Configuration details
Offline Authentication	This setting indicates if security codes can be used for authentication if offline authentication is enabled but not available (VIP Security Key is unavailable and user is disconnected from the corporate network). This setting defaults to 0, and is automatically updated. Do not change this setting. • If set to "0", offline authentication components have not been installed and offline authentication is not enabled. • If set to "1", offline authentication components have been installed and offline authentication is enabled.
Offline Lease Period	Select the number of days (1 to 7) that users can continue to access the resource when the user is not connected to the corporate network and does not have access to a VIP Security Key. The counter resets once the user connects to the corporate network. This setting is optional, and should only be configured if you implement offline authentication.
Proxy Enabled	For offline authentication only: If your users access resources that reside behind a proxy, enable Windows proxy support to allow access through the proxy. For offline authentication only: Enable proxy support if your users access the VIP Service (to provision a credential) from behind a proxy. • If set to true, proxy support is enabled. • If set to false, proxies are not supported. If you enable proxy support, you must also configure the remaining proxy values.
Proxy Host	Enter the IP address of the proxy server.
Proxy Port	Enter the port number on which the proxy server listens.
Proxy Username	If the proxy server is configured for basic authentication, enter the Windows proxy username. Otherwise, leave this entry blank.
Proxy Password	If the proxy server is configured for basic authentication, enter the Windows proxy password in encrypted format. Otherwise, leave this entry blank. Use the camouflage tool to encrypt the password.

6. Run the `Microsoft_Credential_Provider\VIP Enterprise Gateway Credential Provider.msi` installer. Browse to and locate the `CPconfig.txt` file when the setup prompts for it.
7. After the installation is complete, restart the system.

Sample CPconfig.txt file

The following is an example of the `CPconfig.txt` file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP]
"Validation Server"="192.168.1.1:1812:vQa5KX9LJ5E0jdGkmm4mvatt5ss4cDcVrzH8T6Qk6WM=
,192.168.1.1:1813:vQa5KX9LJ5E0jdGkmm4mvatt5ss4cDcVrzH8T6Qk6WM=,192.168.1.1:1814:vQ
a5KX9LJ5E0jdGkmm4mvatt5ss4cDcVrzH8T6Qk6WM="
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP]
"Time Out"="10"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP]
"Retries"="5"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Allowed CP"="{94596c7e-3744-41ce-893e-bbf09122f76a}:{AC3AC249-E820-4343-A65B-377A
C634DC09}"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Enable U2F Authentication"="0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
```

```
"Enable Offline Authentication"="1"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Offline Lease Period"="7"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Proxy Enabled"="true"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Proxy Host"="192.186.1.1"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Proxy Port"="80"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Proxy Username"="external_web_proxy"
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options]
"Proxy Password"="e4c5rE5R8w"
```

Installing and configuring Symantec VIP with Credential Provider for offline authentication

Complete the following general procedures to install and configure Symantec VIP with Microsoft Credential Provider for offline authentication:

NOTE

Before you integrate Symantec VIP with Credential Provider for offline authentication using a VIP Security Key, you must install and configure the Symantec VIP with Credential Provider for online authentication.

See Installing and configuring Symantec VIP with Credential Provider for online authentication.

Table 7: Offline authentication integration procedures

Step	Task
1	Ensure that you meet the minimum system requirements and prerequisites. See System requirements.
2	Install Python. See Installing Python.
3	Install the offline authentication component. See Installing the offline authentication component.

Once you have installed and configured Symantec VIP with Credential Provider for offline authentication, test your integration.

See Testing the integration.

Installing Python

This section provides an overview of Windows-specific behavior while installing Python. Only complete these procedures if you integrate Symantec VIP with Credential Provider for offline authentication.

NOTE

You must install the 32-bit version of Python, even if you are running a 64-bit version of Windows.

1. Download the Python installer 3.6.3 32-bit package.
2. Run the installer and select the Customize installation option. This option allows you to select the features to install, define installation location, and other options. Select the **Add Python 3.6 to PATH** check box.
3. Select all the optional features and click **Next**.
4. On the Advanced Options page, select **Install for all users** and clear **Precompile standard library**.
5. Click **Install**.

Installing the offline authentication component

To install the Symantec VIP with Credential Provider for offline authentication, complete the following steps:

1. The offline authentication runs on port 8443 by default. Make sure this port is available during installation.

   You should not change this port and also make sure other existing applications do not use the port 8443. Else, the offline authentication functionality will not work.
2. From the VIP Credential Provider package, open the **VIP_Offline_Auth_U2F** folder.
3. As an administrator, open the command prompt and run the following command:

   ```
   $python VIPU2FInstaller.py
   ```

   By default, the offline package will be installed in the following paths:

   - `C:\Program Files\Symantec\VIP_U2F` (32-bit)
   - `C:\Program Files (x86)\Symantec\VIP_U2F` (64-bit)

Testing the integration

Complete the appropriate procedures to test the integration of Symantec VIP with Credential Provider in both online and offline modes:

- Testing the integration for online authentication
- Testing the integration for offline authentication

Testing the integration for online authentication

You can test for the User ID–Security Code (Security Code authentication), User ID–Security Code (Push/SMS/Voice authentication), and User ID–Access PIN–Security Code authentication methods that you use in your enterprise.

An authentication method can integrate the following verification mechanisms:

- **Hardware and VIP Access Credential**: In this method, the security code that you generate on your hardware or VIP Access credential is used besides the user name and password to access the protected resources.
  See Testing hardware and VIP Access credential authentication.
- **SMS/Voice**: If you have configured out-of-band (OOB) authentication in the VIP Enterprise Gateway validation server and in VIP Manager, then a security code is sent to your registered mobile device over SMS or Voice. You must use this security code besides the user name and password to access the protected resources.
  See Testing SMS/Voice authentication.
- **VIP Access Push**: For users who have installed VIP Access on their registered mobile devices, VIP Service sends a VIP Push notification message to the mobile device. The user must tap the Allow button on the device to perform the second-factor authentication and complete the sign-in.

See Testing VIP Access Push authentication.

- **Access PIN**: In this method, the security code that you generate on your hardware or VIP Access credential and Access PIN is used besides the user name and password to access the protected resources.
  See Testing Access PIN authentication.

Testing hardware and VIP Access credential authentication

If you are using the hardware or VIP Access credential authentication with the User ID – Security Code authentication method, then perform the following steps:

1. Access the VIP-protected computer directly or remotely using RDP.
2. In the Login prompt, enter your user name and password in the respective fields.
3. Click **Submit**. After successful authentication, the Confirm Your Identity window appears.
4. In the Enter Security Code field, enter the security code that you generate on your hardware or VIP Access credential and click **Submit**. After successful authentication, you can access the protected resources.

Testing SMS/Voice authentication

If you have integrated SMS or Voice authentication with the User ID – Security Code authentication method, then perform the following steps:

1. Access the VIP-protected computer directly or remotely using RDP.
2. In the Login prompt, enter your user name and password in the respective fields.
3. Click **Submit**. After successful authentication, the Confirm Your Identity window appears.
4. In the Enter Security Code field, enter Push or Send. (The key words Push and Send are not case-sensitive.)
5. Click **Submit**. If the credentials are correct, you will receive a security code over SMS or Voice on your registered mobile device and the Access Challenge page appears.
6. In the Access Challenge prompt, enter the security code that you received on your device and click **OK**. After successful authentication, you can access the protected resources.

Testing VIP Access Push authentication

If you have integrated Push authentication with the User ID – Security Code authentication method, then perform the following steps:

1. Access the VIP-protected computer directly or remotely using RDP.
2. In the Login prompt, enter your user name and password in the respective fields.
3. Click **Submit**. After successful authentication, the Symantec VIP Authentication window appears.
4. You will receive a Push notification on your registered mobile device.
5. Tap **Allow** on your device to complete the authentication. After successful authentication, you can access the protected resources.

Testing Access PIN authentication

If you are using the hardware or VIP Access credential authentication with the User ID – Access PIN – Security Code authentication method, then perform the following steps:

1. Access the VIP-protected computer directly or remotely using RDP.
2. In the Login prompt, enter your user name and password in the respective fields.
3. Click **Submit**. After successful authentication, the Confirm Your Identity window appears.
4. In the Enter Security Code field, enter the security code along with the Access PIN that you generate on your hardware or VIP Access credential and click **Submit**. After successful authentication, you can access the protected resources.

Testing the integration for offline authentication

Complete the following procedures to test the integration of Symantec VIP with Credential Provider for offline authentication using a VIP Security Key. These procedures also test the functionality of a VIP Security Key.

NOTE

You must have enabled offline authentication (in the CPconfig.txt file) before performing these tests.

See Manually installing the Credential Provider.

- See Registering the VIP Security Key.
- See Login using the VIP Security Key.
- See Re-register the VIP Security Key.
- See Disable the VIP Security Key.
- See Enable the VIP Security Key.

Registering the VIP Security Key

To register the VIP Security Key, follow these steps. For first-time registration, make sure you are connected to your enterprise network.

1. Lock or log out of your machine, and then log back on to the machine.
2. If you have enabled Push notification on your mobile device, the following prompt appears.
3. Alternatively, you can enter your security code if you have not enabled Push and click **Submit**.
4. Insert the VIP Security Key to start the enrollment process and click **Register**.
5. When your VIP Security Key flashes, tap it. A success message appears.

Login using the VIP Security Key

This section describes how to verify whether an end-user can log in to the protected resources using VIP Security Key.

1. Once you complete the VIP Security Key registration, lock or log out of your machine.
2. Log on to the machine again, and you will be prompted to tap the VIP Security Key when it flashes.
3. After successful authentication, you can access the machine.

Re-register the VIP Security Key

To re-register the VIP Security Key, follow these steps:

1. Remove the existing VIP Security Key. Lock or log out of your machine.
2. Log in to the machine again, and you will be prompted to enter your user name and password.
3. A prompt with Validate using VIP Security Key appears. You must not take any action and the prompt disappears after few seconds.
4. If you want to re-register your VIP Security Key, select **Click here to re-register your VIP Security Key**.
5. Click **OK** on the confirmation prompt.
6. If you have enabled Push notification on your mobile device, the following prompt appears.
7. Insert your VIP Security Key and click **Register**.
8. When your VIP Security Key flashes, tap it. A success message appears.

Disable the VIP Security Key

To disable a VIP Security Key for a new user, follow these steps:

1. Click **Do not show this message again** during registration.
2. Click **OK** to disable the VIP Security Key registration permanently.

   To disable a VIP Security Key for an existing user, follow these steps:
3. Log on to the machine without your VIP Security Key. The following prompt appears.
4. If you have enabled Push notification on your mobile device, the following prompt appears.
5. Select **Click here to re-register your VIP Security Key**. The Insert VIP Security Key prompt appears.
6. Click **Do not show this message again**.
7. Click **OK** to disable the VIP Security Key registration.

Enable the VIP Security Key

If you need to enable VIP Security Key authentication again, open the command prompt and navigate to the VIP Security Key package and run the following command:

```
$python VIPOptInForU2F.py <username>
```

For example, `$python VIPOptInForU2F.py test_user`

Uninstalling VIP Credential Provider for online authentication

To uninstall Symantec VIP with Credential Provider for online authentication, follow these steps:

1. Before you start the uninstallation, make sure that all active user connections are closed.
2. If you have enabled offline authentication, you must also uninstall the VIP Credential Provider for offline authentication.

   See Uninstalling VIP Credential Provider for offline authentication.
3. Go to **Control Panel > All Control Panel Items > Programs and Features > Uninstall VIP Enterprise Gateway Credential Provider**.

Uninstalling VIP Credential Provider for offline authentication

To uninstall Symantec VIP with Credential Provider for offline authentication, navigate to the VIP Security Key package location and run the following command:

```
$python VIPU2FUninstaller.py
```

The installation folder, registry keys, and VIP Security Key services are removed.

Advanced configurations for online authentication

You can add functionality to your Symantec VIP Credential Provider by performing some advanced configurations. The following advanced configurations are available for the online authentication mode:

Using qualified domain user names in Symantec VIP Credential Provider

While passing the user authentication information to the VIP Enterprise Gateway Validation server that is configured in the User Name–Security Code mode, Symantec VIP Credential Provider typically removes the domain qualification from the user name. For example, Symantec VIP Credential Provider sends acme\ john_doe as john_doe to the VIP Enterprise Gateway Validation server. The following Strip Domain registry settings controls this behavior. By default, the Strip Domain registry value is set to 1.

`[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options\Strip Domain]`

In multi-domain scenarios, the user can log-in using different user name formats. For example, the user John Doe can use any of the following user name formats to log-in, which are valid for a Microsoft Active Directory environment:

- acme\john_doe
- john_doe@acme.com
- acme.com\john_doe
- acme.com\john_doe@acme.com

All these user names represent the same user, John Doe. In such cases, you may consider setting the value of the `[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options\Strip Domain]` registry to 0. When the value is set to 0, Symantec VIP Credential Provider passes the domain-qualified user name, [domain]\[username], that the user enters (for example, acme\ john_doe or acme.com\ john_doe) on to the VIP Enterprise Gateway Validation server without any modification. However, if the user enters a non-qualified user name of the format sAMAccountName or uSerPrincipalName (for example, john_doe or john_doe@acme.com), Symantec VIP Credential Provider prefixes the computer's default DNS domain name to the user name as a domain qualification (for example, acme.com\john_doe or acme.com\ john_doe@acme.com) before sending it to VIP Enterprise Gateway Validation Server.

For this configuration to work, you must select the Use LDAP User Name for VIP Authentication Service Validation option in the VIP Enterprise Gateway Validation server configuration page.

NOTE

This applies to an Active Directory user store only. Also, you must install VIP Enterprise Gateway 9.8 or later to make this configuration work.

You cannot modify the Strip Domain registry value using the `CPconfig.txt` file during installation. You can modify the Strip Domain registry value by a separate registry operation through registry value push or MSI transform.

NOTE

If Strip Domain is disabled, the user will need to register the security key twice; once when logging into the system for the first time, and once when locking the system for the first time.

Allowing third-party Credential Providers along-with Symantec Credential Provider

Additional legacy authentication providers can be used along-with Symantec VIP credential provider. By default, the Symantec VIP with Credential Provider tile is available on the login screen. The other Credential Providers that are available by default are Smartcard Pin and WinBio Credential Providers.

In a migration scenario where all the users may not have migrated to VIP yet, the login screen must display additional tiles for the third-party Credential Providers to authenticate the users. To include additional tiles on the login screen, in the Allowed Credential Provider registry option, enter the colon-separated GUIDs of the third-party Credential Providers that can work along with the Symantec Credential Provider.

NOTE

If you want to allow a third-party Credential Provider to authenticate the users, the `HKLM/SOFTWARE/SYMANTEC/CP/OPTION/ShowConsoleRDP` flag must be set to 1. If the flag is set to 0, while connecting to the machine remotely using a Remote Desktop Protocol (RDP), the tile of the third-party Credential Provider will not appear on the console, and the credentials will be submitted against the default Symantec VIP Credential Provider.

Allow logon for selected users without two-factor authentication

To allow selected users to be authenticated without two-factor authentication:

1. Create a group named no2fa on your computer using **Local Users and Groups**.
2. Add the users to that group. The users can be local users or can belong to the domain.

Disable two-factor authentication for users without credentials

To log in to the system protected by Symantec VIP with Credential Provider, the domain users must possess a security credential. Two-factor authentication to access the resources protected by Symantec VIP with Credential Provider is a stronger security practice.

However, some organizations consider rolling out VIP credentials in phases. This type of implementation results in some early adopters who have VIP credentials and others who do not have associated VIP credentials. The following types of users will not have associated VIP credentials:

- The users not registered in VIP Services.
- The users without a credential bound to their account.
  You can disable two-factor authentication for users without an effective VIP credential by setting the following registry option to ‘1’ or ‘2’:
  `[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options\EnablePartial2FA]`
- If you set this registry value to ‘1’, all the users who do not have a VIP credential will be authenticated using their enterprise directory credentials only. The prompt for second-factor authentication will not be available.
- If you set this registry value to ‘2’, all the users that are not part of the VIP Enterprise Gateway User Store will be authenticated using the enterprise directory credentials, irrespective of them having the VIP credentials. However, if the users are located in the VIP Enterprise Gateway User Store, they will be prompted for the security code.

By default, the value for this option is 0. In this case, all the users will be challenged to enter a security code.

NOTE

You cannot modify the EnablePartial2FA registry value using the `CPconfig.txt` file during installation. You can modify this registry value by a separate registry operation through registry value push or MSI transform.

Selective two-factor authentication for a specific set of users in the LDAP directory

You can define distinct authentication or authorization policies in your corporate LDAP environments based on user distinguished names (DN) or group information. You can selectively provide highly secure two-factor authentication to a set of users. For example, a company can enable two-factor authentication for the system administrators who typically have higher privileges. The rest of the employees of the company may not have to use two-factor authentication. You can deploy this implementation using Symantec VIP Credential Provider:

1. In the VIP Enterprise Gateway User Store, configure only the users who are to be authenticated with two-factor authentication.
2. Configure a Validation server in the User Name–Security Code authentication mode.
3. Select the **Use LDAP User Name for VIP Authentication Service Validation** option while configuring the validation server.
4. Configure Symantec VIP Credential Provider as described in the Disable two-factor authentication for users without credential section.
5. Ensure that Symantec VIP Credential Provider can send RADIUS requests to the Validation server configured in step 2.

VIP Enterprise Gateway scenarios

While authenticating users, Symantec VIP with Credential Provider does the following:

- If the user is not located in the VIP Enterprise Gateway User Store, Symantec VIP with Credential Provider does not prompt for two-factor authentication. The user is authenticated using the user name and the LDAP password.
- If the user is located in the VIP Enterprise Gateway User Store:
  - If the user has a valid credential bound in VIP Services, the user is prompted for a security code.
  - If the user does not have an effective credential that is bound in the VIP Services, the following scenarios can occur:
    - Scenario 1: The EnablePartial2FA registry value is set to 1. Then, the user is not prompted for a security code. The user is authenticated using the user name and the LDAP password.
    - Scenario 2: The EnablePartial2FA registry value is set to 2. Then, the user is prompted for a security code.
  - If the VIP Enterprise Gateway server is in the Business Continuity mode, the user is not prompted for a security code. The user is authenticated using the user name and the LDAP password.
- If an error occurs in the communication among Symantec VIP with Credential Provider, VIP Enterprise Gateway, and VIP Services, Symantec VIP with Credential Provider terminates the authentication process and prompts the login page to the user to start the authentication process again.

Local user authentication with Symantec VIP Credential Provider

Local users and administrators can access a workstation that is protected by Symantec VIP Credential Provider without specifying a security code.

You can enter the user name using the [`hostname\user name`] format.

NOTE

In the case of local users, if the Validation Server is VIP User ID mapping-enabled, the skipLocalUsersForUserStoreSearch flag in the radserver.conf file must be set to **True**. When this flag is set to True, the Validation Server skips the user store search for local users.

Local users on domain joined machine and non-domain joined machine can be protected using VIP Credential Provider.

You can enable two-factor authentication for local users by setting the following registry to 1:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\CP\Options\ChallengeLocalUsers]
```

NOTE

You cannot modify the ChallengeLocalUsers registry value using the `CPconfig.txt` file during installation. You can modify this registry value by a separate registry operation through registry value push or MSI transform.

Resetting passwords

This section describes how to reset your password on the computer that is protected by Symantec VIP with Credential Provider. The users can reset the password in the following scenarios:

- If the users want to reset password after logging-in to the computer for the first time, they can do so through the change password screen.
- If the users want to reset password at anytime, they can press **Ctrl+Alt+Delete** and select **Change a password** from the options displayed.

Enter the security code and click **Submit**. You will be prompted to enter your security code multiple times. After changing the password successfully, the system displays the message that the password has been changed successfully.

Large-scale deployment

Large-scale deployments using Microsoft Active Directory group policy

You can use a group policy to deploy Symantec VIP Credential Providers to large groups of users in your Active Directory. Refer to the appropriate procedures:

- Large-scale deployment using Microsoft Active Directory group policy for online authentication
- Large-scale deployment of Credential Provider using group policy for offline authentication

Large-scale deployment using Microsoft Active Directory group policy for online authentication

Complete the following steps for to deploy the Symantec VIP Credential Provider for online authentication to large groups of users through a Microsoft Active Directory Group Policy.

Table 8: Deployment procedures

Step	Tasks
1	Follow steps 2 – 4 of the procedure for manually installing the Credential Provider. See Manually installing the Credential Provider.
2	Rename the `CPconfig.txt` file as `CPconfig.reg`.
3	Create the MSI transform (MST). See Create the MSI transform.
4	Deploy the Group Policy. See Assign a package.

When the client computers start, the Symantec VIP Credential Provider package is installed automatically. After successful silent installation, the system restarts.

Create the MSI transform

To create the MSI transform (MST) using InstallShield or Wise Installer Editor, complete the following steps:

NOTE

The screen shots provided in the following procedures are captured from InstallShield 2011. For specific screen shots and procedures, refer to the product documentation that is provided with your installer editor.

1. Launch the InstallShield and create a new project.
2. Under the **All Types** tab, select the **Transform** template. Then, provide your project name and location. Click **OK**. The Open Transform Wizard window appears.
3. In the **Base MSI File Name** field, provide the path for the **VIP Enterprise Gateway Credential Provider.msi** installer present in the microsoft_credential_provider_setup_folder, and click **Next**. The Open Transform Wizard - Additional Transforms window appears.
4. Do not provide any transform in this window. Click **Next**. The Open Transform Wizard - Create a Response Transform window appears.
5. Do not select the **Create response transform** check box. Click **Finish**.
6. Under the **Installation Designer** tab, on the left pane, under System Configuration, select Registry. In the Destination computer's Registry view, select the `HKEY_LOCAL_MACHINE` key.
7. Right-click the `HKEY_LOCAL_MACHINE` key and click **Import REG File** from the sub-menu. The Import REG File Wizard appears.
8. In the Registry File field, provide the path for the `CPconfig.reg` file present in **microsoft_credential_provider_setup_folder**. Click **Next**. The Import REG File - Import Conflict Options window appears.
9. Select **Overwrite the registry data**, select the **Log all registry conflicts and errors to a file** check box, and provide the log file path. Click **Import**.
10. After successful import, navigate to the CP key in the Destination computer's Registry view (`HKEY_LOCAL_MACHINE \SOFTWARE\Symantec\CP`) and confirm that your Validation Server settings are imported to this location. Save and close the project.

Assign a package

You can assign the `VIP Enterprise Gateway Credential Provider.msi` package to client computers. If you assign the package, it is installed automatically. To assign a package, follow these steps:

NOTE

Do not use the **Browse** button in the Open dialog to access the UNC location. Make sure that you type or paste the UNC path to the shared package whenever prompted within this process.

1. Select the respective Domain Group Policy that you want to use to assign the package and click **Edit**.
2. Under Computer Configuration, expand **Software Settings**.
3. Right-click **Software Installation** and then select **New > Package**.
4. In the Open dialog box, type the full UNC path of the shared **VIP Enterprise Gateway Credential Provider.msi** package and click **Open**.
5. In the Deploy Software dialog box, select **Advanced** and click **OK**.
6. Click the **Deployment** tab and select the deployment type as **Assigned**. Click **Install this application at logon**.
7. Click the **Modifications** tab and click **Add**.
8. In the Open dialog box, type the full UNC path of the shared **Credential Provider Transform.mst** file and click **OK**. The VIP Enterprise Gateway Credential Provider package appears in the right pane of the Group Policy window.
9. Close the Group Policy window, click **OK**, and exit the Active Directory Users and Computers window.
10. Run the following command to refresh the Active Directory Group Policy settings:

```
C:\> gpupdate /force
```

Large-scale deployment of Credential Provider using group policy for offline authentication

Complete the following steps for to deploy the Symantec VIP Credential Provider for offline authentication to large groups of users through a Microsoft Active Directory Group Policy.

You must have appropriate administrator permissions to execute the batch startup script. The startup script will be deployed on the end-user machine as a silent install and user will be prompted for a system restart. To perform the large scale deployment, follow these steps:

1. Extract **VIP_Offline_Auth_U2F.zip** from the VIP Credential Provider package and place it in a shared folder. This folder must be accessible by all end-user machines.
2. Edit the **VIPU2F_GPO_Installer.bat** file located under **VIP_Offline_Auth_U2F.zip** and update the following values:

Option	Configuration details
sourceSharedLoc	Update with the shared location from where you have extracted `VIP_Offline_Auth_U2F.zip`. For example, "\\192.186.1.1\cp\VIPU2F*"
localDestFolderLoc	Update with the local machine from where you need to copy the contents of `VIP_Offline_Auth_U2F.zip` from shared location. For example, `C:\temp\VIPU2F`
logFileLoc	Provide the path of the local machine where you want to save the log file. Once you make the changes, save the file with .bat extension. For example, `C:\startUpScriptLogFile.txt` **Note:** The log file that you specify must already exist.
u2fVersion	Update with the installer version of Symantec VIP for Credential Provider for off-line authentication. For example, `1.0`

3. Assign any startup scripts. Refer to the Microsoft documentation for details.
4. Test the large-scale deployment:
   - Verify if the VIP Security Key installation is successful. You can either view the batch script log file or the registry entries.
   - Lock or log out of your machine, and login to the machine again. See Registering the VIP Security Key to complete the registration process.

Upgrading Symantec VIP with Credential Provider

Prerequisites

The upgrade section is applicable for:

- Symantec VIP with Credential Provider for online authentication version 1.0 and later
- Symantec VIP with Credential Provider for offline authentication 1.0 and later

For version information, see the `version.txt` file packaged with the Symantec VIP with Microsoft Credential Provider integration module software package.

Note the following before upgrading:

- If you are using a Microsoft Credential Provider version lower than 1.0, you must uninstall the existing version and do a fresh installation of the latest version.
- Make sure end user machines can execute power-shell scrips.
- While performing the upgrade, you must first complete Symantec VIP with Credential Provider for online authentication followed by Symantec VIP with Credential Provider for offline authentication.
- If your machine is configured for both on line and off line authentication, you must upgrade both the modes.

Manual mode upgrade

Symantec VIP with Credential Provider for online authentication

To manually perform the upgrade for Symantec VIP with Credential Provider for online authentication:

1. Back up the Microsoft Credential Provider registry entry.
   - To do so, open the registry and navigate to **Start > Run > Regedit > HKEY_LOCAL_MACHINE-SOFTWARE > Symantec > CP**.
   - Right-click on the CP and export and save the file as **cpconfig_back.reg** in a temporary folder.
2. Open the `cpconfig_back.reg` file in a notepad and update the version value to the latest Credential Provider version and save it.
3. Download latest version of Microsoft Credential Provider from VIP Manager and install it. Now provide the `cpconfig_back.reg` file backed up in Step 1 as the Credential Provider configuration file and continue with the installation.
4. To verify if the installation is successful, navigate to **Control Panel > Add/Remove Program** and verify the latest version.

Symantec VIP with Credential Provider for offline authentication

To manually perform the upgrade for Symantec VIP with Credential Provider for offline authentication:

5. Download the latest version of the installer from VIP Manager and install the offline authentication components.

   See Installing the offline authentication component.
6. To verify if the installation is successful, see the version information in the registry file:
   - On 32-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\U2FServer`
   - On 64-bit: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\U2FServer`

Large-scale deployment upgrade

Symantec VIP with Credential Provider for online authentication

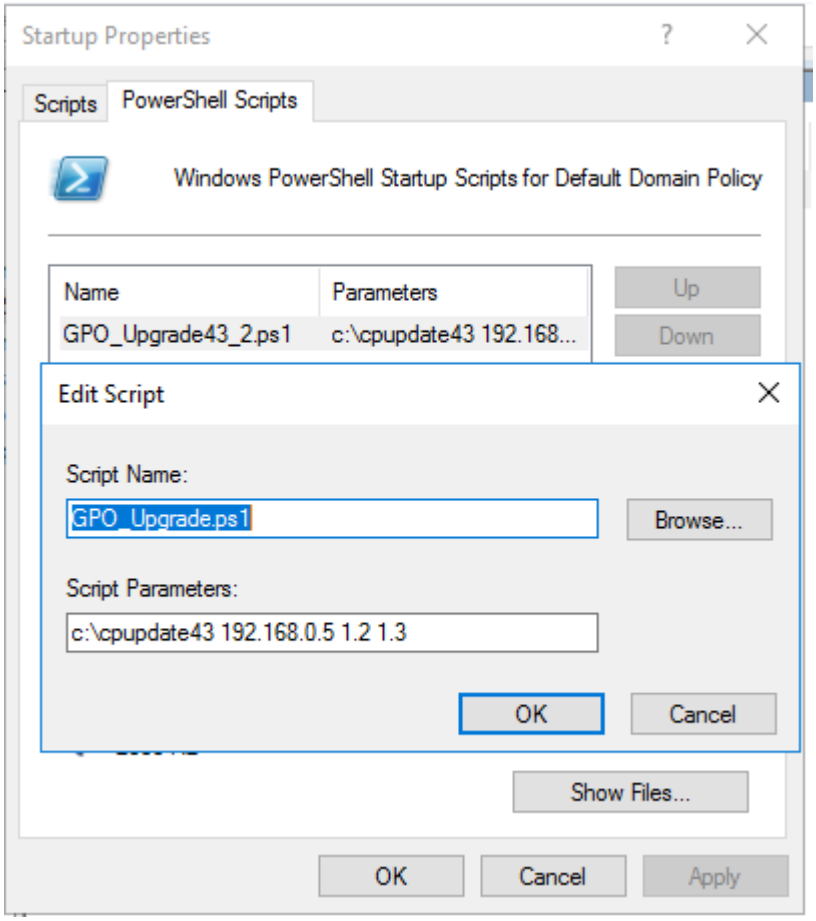
1. Download the latest version of VIP Credential Provider package from VIP Manager and extract it to a shared location. The shared location must have write permissions for domain computers.

   Make sure your shared location path looks exactly as follows. `\\<machine-ip>\Microsoft_Credential_Provider`.

   For example : `\\192.168.0.5\Microsoft_Credential_Provider`

2. Look for **GPO_Upgrade.ps1** and add this as a startup script in your domain controller group policy and edit the following parameters. See the figure for an example of the script parameters.

Parameter	Description
Destination location	Provide the path on your local machine where you want to copy the contents of the shared location (`C:\CPUpdate` in this example).
Shared location machine IP address	Provide the IP address of the machine where you have placed the VIP Credential Provider package you downloaded in the first step of these procedures (`192.168.0.5` in this example).
Existing CP version	Provide the existing version of the credential provider (`1.2` in this example).
New CP version	Provide the version of the credential provider to which you are upgrading (`1.3` in this example).



3. To assign startup scripts, see the Microsoft documentation.
4. In your end user machine, update your group policy using the command `gpupdate /force` and restart the machine. This process takes a few minutes to complete and your machine will restart multiple times.
5. To verify if the installation is successful, navigate to **Control Panel > Add/Remove Programs** and verify the latest version.

Symantec VIP with Credential Provider for offline authentication

To perform large-scale deployment upgrade for Symantec VIP with Credential Provider for offline authentication:

6. Complete the installation steps described in Large-scale deployment of Credential Provider using group policy for offline authentication.
7. Edit the `VIPU2F_GPO_Installer.bat` file and update the value of `u2fVersion` to the latest.

Troubleshooting

Issues and solutions

The following are some of the common issues that you may encounter during integration, along with typical solutions:

Table 9: Troubleshooting issues

Issues	Solutions
VIP Credential Provider issues	
In the VIP validation server log, the following message is displayed: *Incorrect LDAP static password. Enter the correct LDAP static password. Also, ensure that both the RADIUS server and the RADIUS client shares the same Shared Secret.*	You must have configured an incorrect validation server mode which is not supported by Credential Provider. You must configure validation server only in User ID–Security code mode.
In the VIP validation server log, the following message is displayed: *The security code does not meet policy requirements. Verify the security code you have entered. Also, ensure that both the RADIUS server and the RADIUS client shares the same Shared Secret, OTP length = 16*	You must reset the RADIUS shared secret in both Credential Provider plug-in and VIP validation server and restart the validation server.
Delay in receiving or not receiving the VIP Access Push notification.	Make sure your mobile device is connected to a network. Symantec recommends to have at least 3G or Wi-fi service to receive VIP Access Push notification.
In the VIP validation server log, the following message is displayed: *Push Trampled*	Make sure the time-out defined in Credential Provider plug-in and VIP Enterprise Gateway server are the same.
On Windows 7, remote desktop connection fails for local users if system is rebooted from Safe mode for the first time.	You must login to Credential Provider through Console once. Then, try to login through remote desktop connection.
The log file contains the error message, *Authentication failed with incorrect LDAP static password*.	Use any of the following solutions: • The password may be locked or it may have expired. Reset the password. • Make sure that the RADIUS shared secret set in the VIP Enterprise Gateway validation server and the application are the same.
Authentication fails even before you get the SMS/Voice security code or the Push notification on the registered mobile device.	Make sure that when configuring the RADIUS Server in the application, you set the Timeout field to 20 seconds and the Retries field to 3. (If the Retries field is unavailable, set the Timeout field to a minimum of 60 seconds.)
Offline Authentication issues	
Unable to get the VIP Security Key re-register prompt.	Do not insert your VIP Security Key. You must insert the VIP Security Key only after the re-register prompt appears.
VIP Security Key prompt goes blank if there is no action taken.	Make sure that your system screen save time is set for more than 180 seconds.
User getting the message, *Failed to register VIP Security Key* when they try to register.	Use the Symantec supported security key token.

Auto Logon Support for VIP Credential Provider

To enable Auto Logon support for VIP Credential Provider, complete the following tasks:

Task	Resource
Meet the operating system requirements	Operating system requirements
Enable Auto Logon	Enable Auto Logon
Test the configuration	Testing the Auto Logon configuration

Operating system requirements

The Auto Logon support for VIP Credential Provider is available on the following platforms:

- Windows 7 (32-bit/64-bit), Windows 10 (32-bit/64-bit)
- Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 (64-bit), Windows Server 2019

Enable Auto Logon

To enable auto logon, follow these steps:

1. Before you install Credential Provider, make sure the user selected for Auto Logon can log in to the system. Create a **no2FA** group using **Local Users and Groups** and add the Auto Logon user to this group.
2. Change the interactive logon settings.

   NOTE

   This step is applicable only for Windows 10, Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019. You can ignore this step if you are using Windows 7 or Windows Server 2008 R2

   - Launch Group Policy Editor (`gpedit.msc`)
   - Navigate to **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**
   - Set the value as **Enabled** in the one of the following setting. This option may be displayed based on your operating system.

     ```
     Interactive logon: Don't display last signed-in=Enabled
     Interactive logon: Do not display last user name=Enabled
     ```

3. Install Credential Provider. See Configuring Symantec VIP with Credential Provider.
4. Use the camouflage utility defined in Manually installing the Credential Provider section to convert the password of auto-logon user into camouflaged password.
5. From `regedit`, navigate to `HKLM\SOFTWARE\Symantec\CP\Options`. Create a new string value:
   - Value name: `WinAutoLogonPassword`
   - Value data: camouflaged auto-logon user password, which was generated earlier.

Testing the Auto Logon configuration

To test the auto logon configuration, follow these steps:

1. Restart the machine.
2. The Auto Logon user will be automatically logged into the machine without prompting for a security code.

   NOTE

   A security code prompt appears if you log in with any other user.

Copyright Statement


Symantec
A Division of Broadcom