Symantec VIP Quick Start Guide

Windows Server authentication

Version 1.1

Author

Maren Peasley

Symantec

Table of Contents

Introduction

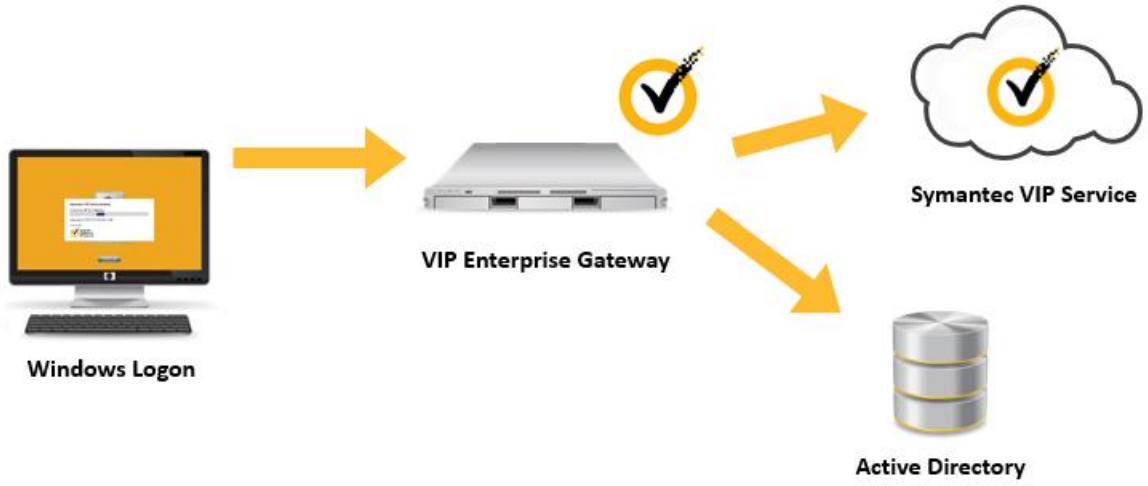
Symantec's VIP authentication offers multi-factor authentication to a variety of applications including the Windows logon screen for Windows servers and other fixed Windows systems. Whether logging on directly at the console or across the network via Remote Desktop, Symantec VIP can secure session access with multi-factor authentication.

Symantec's integration flexibly offers security for a variety of situations: for all users, for those with credentials, for those in a particular group, and more. This quick start guide summarizes the options available to you.

Design and topology considerations

The Symantec VIP plugin for Microsoft Credential Provider was designed to protect only *internal* resources. The plugin is not designed for logging in to Windows workstations and laptops across the Internet or other untrusted networks.

Below is a typical architecture:



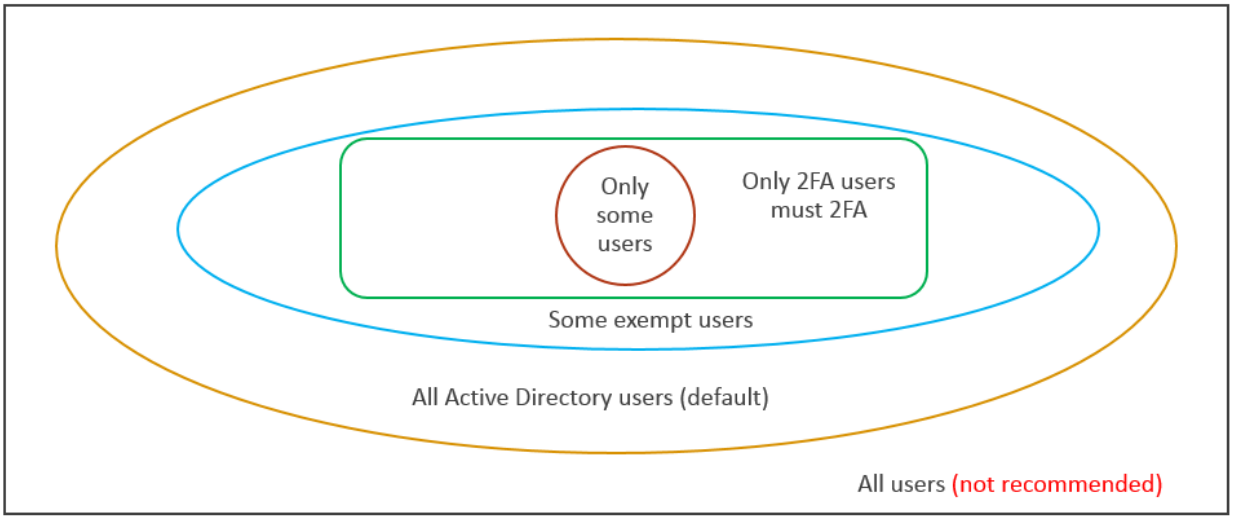
The Windows system needs to be able to contact VIP Enterprise Gateway across the local network. From there, communication to Active Directory is required for some configurations. For all configurations, VIP Enterprise Gateway must be able to contact the Symantec VIP service.

The Symantec VIP plugin for Microsoft Credential Provider utilizes three parameters to control different levels of protection. These are:

- ChallengeLocalUser
- no2fa
- EnablePartial2FA

Together, these can describe multiple protection levels, five of which are outlined below:

- All users (not recommended)
- All Active Directory users (default and recommended)
- All Active Directory users, with some manual exceptions
- Only Active Directory users with a VIP credential
- Only some Active Directory users



The above five protection levels will be described in this quick start guide, though other combinations are possible.

Configuration Summary

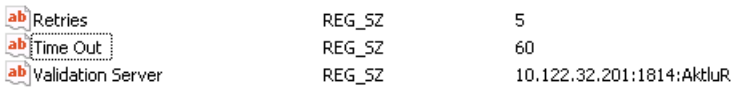
The below configuration descriptions rely upon an initial installation and configuration on the target server and then a subsequent modification of the Windows Registry to customize the configuration. For full details around each setting and general deployment considerations, see the Symantec VIP Integration Guide for Microsoft Credential Provider for details.

Using PUSH to login to the server

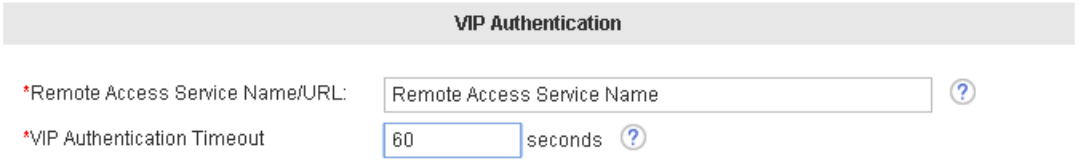
The Symantec VIP plugin for Microsoft Credential Provider supports a PUSH login experience when logging in to the target server. In order for the plugin to work correctly, it needs to wait an appropriate amount of time for the PUSH request to reach the user and then for the user to take action. This change is made in two places: the target server's Time Out registry setting and VIP Enterprise Gateway's validation server Timeout configuration. The initial suggested value for PUSH timers is 60 seconds – these are depicted below.

Note that `CPConfig.txt` can also be used to set these values at initial installation on the target server.

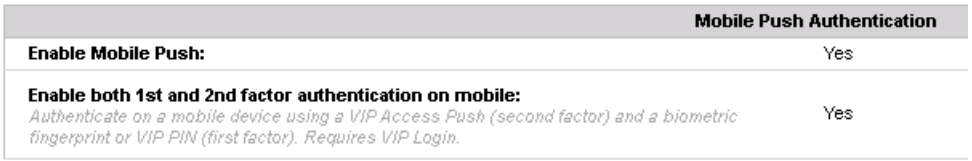
Target server's registry:



VIP Enterprise Gateway's Validation Server:



VIP Manager showing the PUSH feature enabled:



Multifactor authentication for All Users

DANGER: It is possible to lock yourself out of a server using this method!

For this configuration, each target server must have the registry key ChallengeLocalUser set to 1, as in:

`HKLM\Software\Symantec\CP\Options\ChallengeLocalUser`

If the associated VIP Enterprise Gateway validation server also checks for users against Active Directory, then the following Enterprise Gateway flag must be additionally set (in `radserver.conf`):

`skipLocalUsersForUserStoreSearch`

This value is normally set to "False" and must be changed to "True".

```
178  SecondFactorModule.pushChallengeTimeout = null
179  SecondFactorModule.pushChallengeMessage = null
180  SecondFactorModule.pushMessage = Remote Access Service Name
181  SecondFactorModule.pushEnableLockoutProtection = false
182  SecondFactorModule.skipLocalUsersForUserStoreSearch = false
183  SecondFactorModule.pollingInterval = 2
184  # End VIPEGPROXYSecondFactorModule section
```

radserver.conf is typically located here on VIP Enterprise Gateway running on Windows:

`C:\Program Files (x86)\Symantec\VIP_Enterprise_Gateway\Validation\servers\myValServer\conf\radserver.conf`

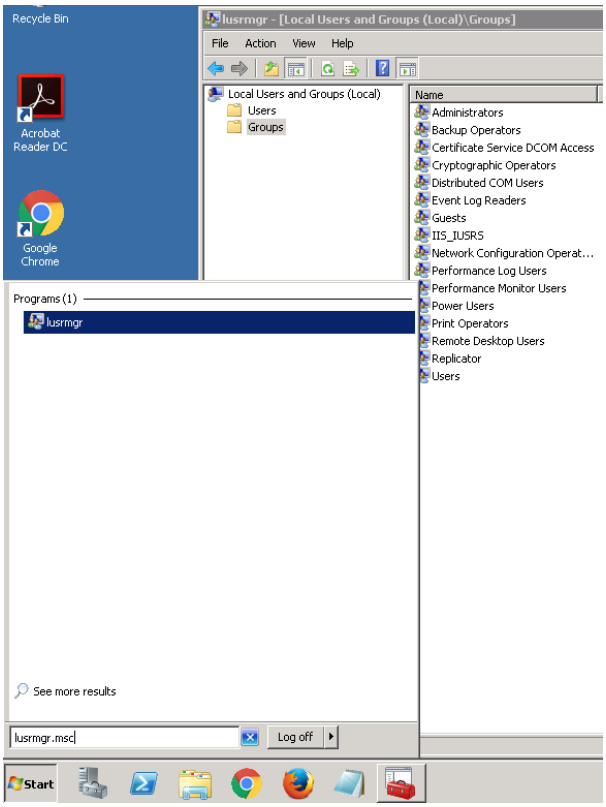
See the "Local User Authentication with Symantec VIP Credential Provider" in the Symantec VIP Integration Guide for Microsoft Credential Provider.

In this configuration, it may be beneficial to configure some local users in the "no2fa" local group in order to continue to allow access to this server. Without this, in a lockout scenario remotely editing the registry of this server or performing local maintenance in order to remove or modify that registry value would be required.

Multifactor authentication for All Active Directory Users

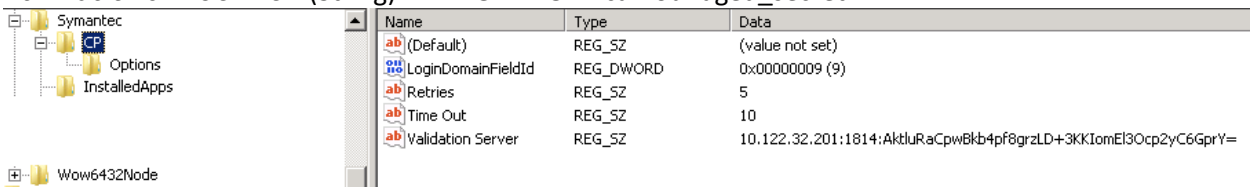
No special configuration is needed. The default values are listed below, for reference:

Group "no2fa": does not exist or empty (either as a local group or an Active Directory group)



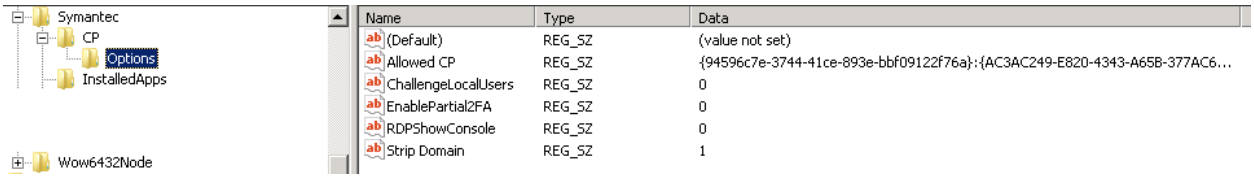
Registry: `HKLM\SOFTWARE\Symantec\CP`:

`LoginDomainFieldId` (DWORD): 9
`Retries` (String): 5
`Time Out` (String): 10
`Validation Server` (String): VIP-EG-IP:PORT:camouflaged_secret



Registry: `HKLM\SOFTWARE\Symantec\CP\Options`:

`AllowedCP` (String): {GUID}:{GUID}
`ChallengeLocalUsers` (String): 0
`EnablePartial2FA` (String): 0
`RDPShowConsole` (String): 0
`Strip Domain` (String): 1



VIP Enterprise Gateway setting: `skipLocalUsersForUserStoreSearch`: false

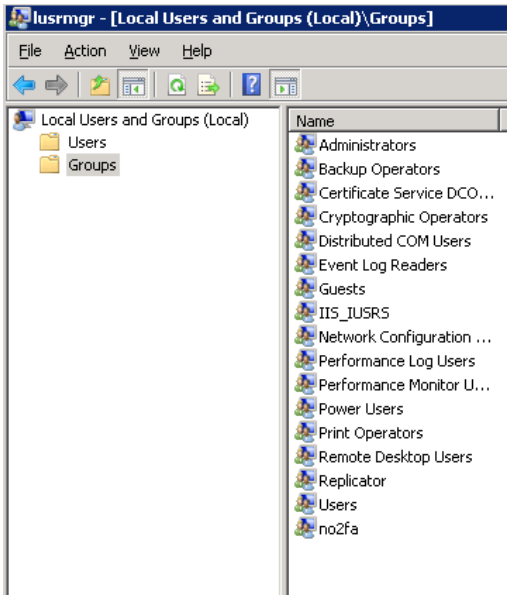
```
178  SecondFactorModule.pushChallengeTimeout = null
179  SecondFactorModule.pushChallengeMessage = null
180  SecondFactorModule.pushMessage = Remote Access Service Name
181  SecondFactorModule.pushEnableLockoutProtection = false
182  SecondFactorModule.skipLocalUsersForUserStoreSearch = false
183  SecondFactorModule.pollingInterval = 2
184  # End VIPEGPROXYSecondFactorModule section
```

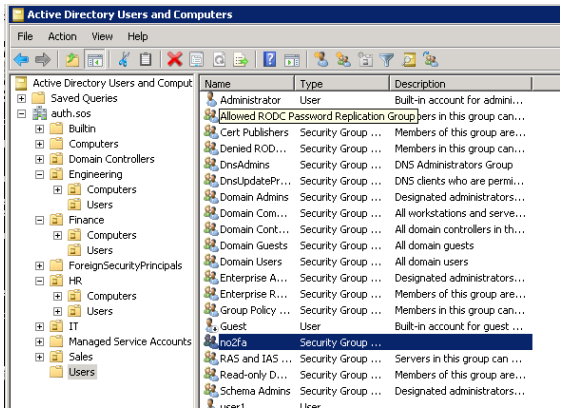
radserver.conf is typically located here on VIP Enterprise Gateway running on Windows:

`C:\Program Files (x86)\Symantec\VIP_Enterprise_Gateway\Validation\servers\myValServer\conf\radserver.conf`

Multifactor authentication for All Active Directory Users, with some exceptions

For this configuration, each target server must have a group created called “no2fa”. Each Active Directory user that bypasses Symantec VIP to logon to this server should be added to this group. Note that this can either be a local group or a group in Active Directory. In either case, changes made to the group affect the logon behavior instantly (the target server does not need to be rebooted). In the case of an Active Directory group, this presumes that the particular domain controller queries has received any appropriate synchronization.





Multifactor authentication for All Active Directory users with a VIP credential

For this configuration, each target server must have a registry key added called “`EnablePartial2FA`”. It is added at this location in the Windows Registry:

`HKLM\Software\Symantec\CP\Options\EnablePartial2FA`

`EnablePartial2FA` is of type String with a value of 1:

In this configuration, a user *without* a VIP credential will *not* be prompted for two factor authentication: username and password will be sufficient to login (provided that user has permission to logon to this server).

Multifactor authentication for only some users

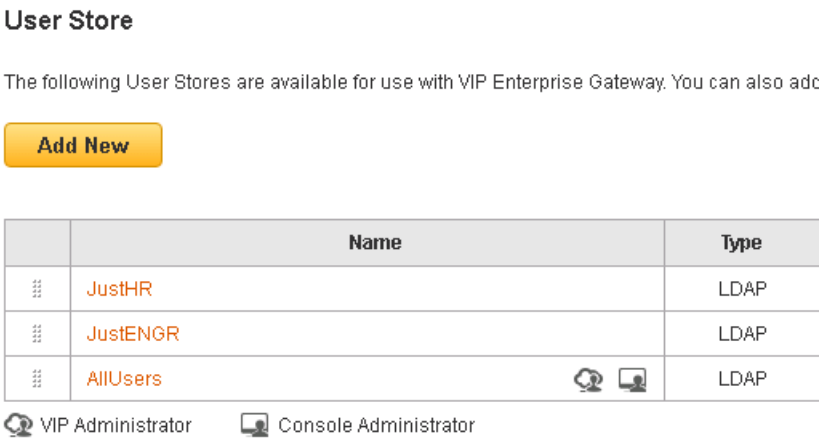
For this configuration, each target server must have a registry key added called “EnablePartial2FA”. It is added at this location in the Windows Registry on the target server:

`HKLM\Software\Symantec\CP\Options\EnablePartial2FA`

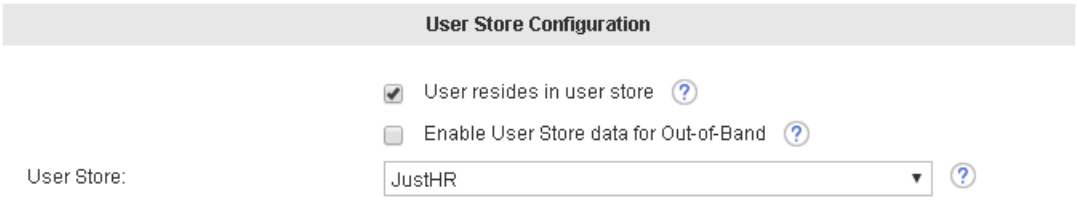
`EnablePartial2FA` is of type String with a value of 2.

Additionally, this requires configuration on VIP Enterprise Gateway’s User Store and Validation Server.

Example VIP Enterprise Gateway User Store configuration:



Example VIP Enterprise Gateway Validation Server configuration:



The User Store must select the users that require 2FA. For best practice, restrict logon to the target server to these users so that:

1) Only the select users may logon to that server, and
2) All approved users require 2FA in order to logon.
3) Any exceptions to this are carefully documented and secured.

Third party considerations

Microsoft Credential Provider is utilized during local login, remote desktop login, and unlocking an existing session. Microsoft Credential Provider is not utilized for remote file share access, permissions escalation in Windows, or authenticating via Integrated Windows Authentication (IWA), so VIP cannot secure those resources.

The Credential Provider architecture offers a flexible and extensible method to add authentication to Windows. Some systems make use of other Credential Provider plugins and it is necessary for VIP to interwork with them properly – especially in technology transition scenarios. The Integration Guide for Microsoft Credential Provider covers interworking alongside other plugins in a section title "Allowing Third-party Credential Providers along-with Symantec Credential Provider" in the Symantec VIP Integration Guide for Microsoft Credential Provider guide.

Troubleshooting tips

The Symantec VIP plugin for Microsoft Credential Provider has a number of settings that need to be coordinated on the target server in concert with Windows permissions, the VIP Enterprise Gateway, and more. Occasionally, issues may surface while initially working on this integration. This section offers some general reminders only.

General reminders

- VIP Enterprise Gateway requires that the Validation Server operate in "UserID – Security code" mode.
- A camouflaged password is inserted into CPConfig.txt and the actual password is typed in to VIP Enterprise Gateway.
- After initial installation and any registry key change, a reboot is necessary for the settings to "sink in"
- It takes humans a certain amount of time to respond to a PUSH

For further assistance, please contact:

Symantec Technical Support

https://my.symantec.com

Phone Support:

https://support.symantec.com/en_US/contact-support.html

Appendix A: Additional Resources and Guides

Symantec VIP Quick Start Guides

Symantec VIP Quick Start Guide: PUSH

Symantec VIP Documentation

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters 350 Ellis St.

Mountain View, CA 94043
USA+1 (650) 527 8000

1 (800) 721 3934

www.symantec.com