

Symantec VIP Quick Start Guide

Windows Server authentication

Version 1.1

Author Maren Peasley



©2017 Symantec. All rights reserved.



Introduction	2
Design and topology considerations	3
Configuration Summary	. 5
Using PUSH to login to the server	5
Multifactor authentication for All Users	6
Multifactor authentication for All Active Directory Users	6
Multifactor authentication for All Active Directory Users, with some exceptions	.9
Multifactor authentication for All Active Directory users with a VIP credential	9
Multifactor authentication for only some users	10
Third party considerations	11
Troubleshooting tips	12
General reminders	12
Appendix A: Additional Resources and Guides	13



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 <u>Symantec VIP</u> <u>Integration Guide for Microsoft Credential Provider</u> 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:

ab Retries	REG_SZ	5
赴 Time Out	REG_SZ	60
ab Validation Server	REG_SZ	10.122.32.201:1814:AktluR

VIP Enterprise Gateway's Validation Server:

VIP Authentication			
*Remote Access Service Name/URL:	Remote Access Service Name	?	
*VIP Authentication Timeout	60 seconds 🥐		

VIP Manager showing the PUSH feature enabled:

	Mobile Push Au	uthentication
Enable Mobile Push:		Yes
Enable both 1st and 2nd factor authentication on mobile: Authenticate on a mobile device using a VIP Access Push (second factor) and a bio fingerprint or VIP PIN (first factor). Requires VIP Login.	nmetric	Yes

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.pashEndslebockoutFrotection fulse
182	SecondFactorModule.skipLocalUsersForUserStoreSearch = false
183	ScoondFasterMedule.pellingInterval = 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\c
onf\radserver.conf
```

See the "Local User Authentication with Symantec VIP Credential Provider" in the <u>Symantec VIP</u> 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)

Symantec VIP Quick Start Guide

Windows Server authentication



Registry: HKLM\SOFTWARE\Symantec\CP:

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

🚊 📲 Symantec	Name	Туре	Data
	赵 (Default)	REG_SZ	(value not set)
Options	30 LoginDomainFieldId	REG_DWORD	0×00000009 (9)
	ab Retries	REG_SZ	5
	赴 Time Out	REG_SZ	10
	赵 Validation Server	REG_SZ	10.122.32.201:1814:AktluRaCpwBkb4pf8grzLD+3KKIomEl3Ocp2yC6GprY=
🖭 🕌 Wow6432Node	_		

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

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

Windows Server authentication

🚊 📲 Symantec	Name	Туре	Data
ē 🎍 🕑	(Default)	REG_SZ	(value not set)
Options	Allowed CP	REG_SZ	{94596c7e-3744-41ce-893e-bbf09122f76a}:{AC3AC249-E820-4343-A65B-377AC6
InstalledApps	ab ChallengeLocalUsers	REG_SZ	0
	ab EnablePartial2FA	REG_SZ	0
	ab RDPShowConsole	REG_SZ	0
⊡]} Wow6432Node	ab Strip Domain	REG_SZ	1

VIP Enterprise Gateway setting: skipLocalUsersForUserStoreSearch: false

178	SecondFactorModule.pushChallengeTimeout = null
179	SecondFactorModule.pushChallengeMessage = null
180	SecondFactorModule.pushMessage = Remote Access Service Name
181	SecondFactorModule.pashEndblehockoutProtection fulse
182	SecondFactorModule.skipLocalUsersForUserStoreSearch = false
183	JevendFeaterMedule.pellingInterval = 2
184	<pre># End VIPEGPROXYSecondFactorModule section</pre>
105	

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

```
C:\Program Files
(x86)\Symantec\VIP_Enterprise_Gateway\Validation\servers\myValServer\c
onf\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.

🜆 lusrmar - [Local Users and Grou	ps (Local)\Groups]	📔 Active Directory Users and Com	puters			
Eile Action View Help						
 Could Serve and Groups (Local) Users Groups Groups 	Name Administrators Administrators Administrators Certificate Service DCO Cryptographic Operators Certificate Service DCO Cryptographic Operators Certificate Service DCO Comparison of the service D	Active Directory Users and Comput Borden Visers and Comput Borden Visers Saved Queries Boultin Computers Computers Computers Computers Users Description Vers Computers Vers Computers Vers Vers	Name Name Additional Constraints (Cert Publishers Cert Publishers Densid Rob Densid Admins Densid Const Densid Const Domain Const Domain Const Domain Const Domain Const Domain Guets Enterprise R Const Const Read-only D Schema Admins Schema Admins Const. Const Schema Admins Schema Admins	Type User Deserved Replication Security Group Security Group Itee	Built-in account for admini Group) ers in this group can Members in this group can Members in this group can DNS Administrators Group DNS clients who are permit Designated administrators All domain controllers in th All domain custs All domain users Designated administrators Members of this group can Built-in account for guest Designated administrators Members in this group can Built-in account for guest Designated administrators	I

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:

Chalongecocalosors	NEG_DE	
赴 EnablePartial2FA	REG_SZ	1
ahinneshawCancela	DEC 07	1

In this configuration, a user *without* a VIP credential will <u>not</u> 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.

	-	
赴 EnablePartial2FA	REG_SZ	2
ablasach	DEC 67	•

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

Example VIP Enterprise Gateway User Store configuration:

User Store

The following User Stores are available for use with VIP Enterprise Gateway. You can also adc

Add New

	Name	Туре
1111	JustHR	LDAP
44	JustENGR	LDAP
4444	AllUsers 🧟 📮	LDAP

🐼 VIP Administrator 🛛 🗔 Console Administrator

Example VIP Enterprise Gateway Validation Server configuration:

	User Store Configuration
	 User resides in user store (?) Enable User Store data for Out-of-Band (?)
User Store:	JustHR 🔹 🥐

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 <u>Integration Guide for</u> <u>Microsoft Credential Provider</u> covers interworking alongside other plugins in a section title "Allowing Third-party Credential Providers along-with Symantec Credential Provider" in the <u>Symantec VIP</u> <u>Integration Guide for Microsoft Credential Provider</u> 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

visit our website.

and contact numbers, please

Symantec World Headquarters 350 Ellis St.

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

1 (800) 721 3934

www.symantec.com

Copyright © 2015 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. 5/2015