Symantec VIP Quick Start Guide

Push Authentication

Version 1.2

Author

Maren Peasley

Table of Contents

Introduction 2

Design and topology considerations 3

Configuration Summary 4

Third party considerations 5

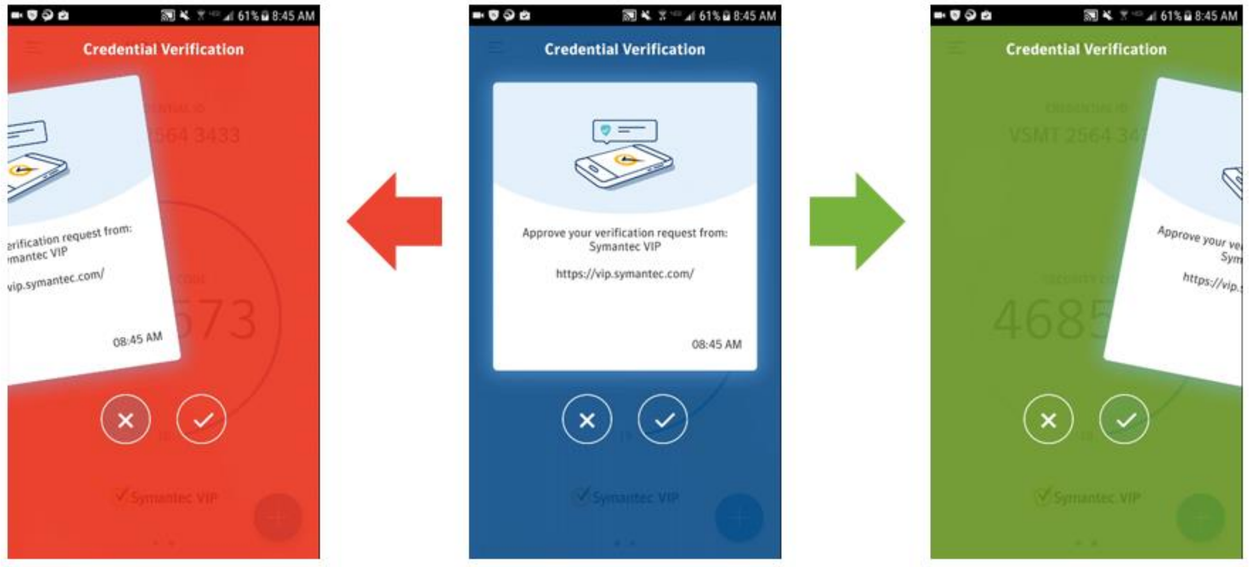
Troubleshooting tips 6

Appendix A: Additional Resources and Guides 7

Introduction

Symantec introduced the VIP PUSH feature in February, 2014. VIP Push saves users time by sending a real-time push verification to the registered mobile device upon sign-in, replacing the need for the user to manually enter a security code. With the touch of a button a user can approve the request, which is then verified by Symantec, a confirmation is instantly sent back to complete the sign-in. Ultimately, this one-tap system is a tremendous time-saver, doing away with all the hours wasted fumbling with six-digit verification codes.

Enabling VIP PUSH is done in two places – in **VIP Manager** and in the **application server** such as a VPN Gateway and typically takes only minutes to configure. VIP PUSH is available for the mobile platforms that support PUSH. Currently, this is available for Internet-connected Apple and Android devices.



Approve your verification request from:
Symantec VIP
https://vip.symantec.com/
08:45 AM

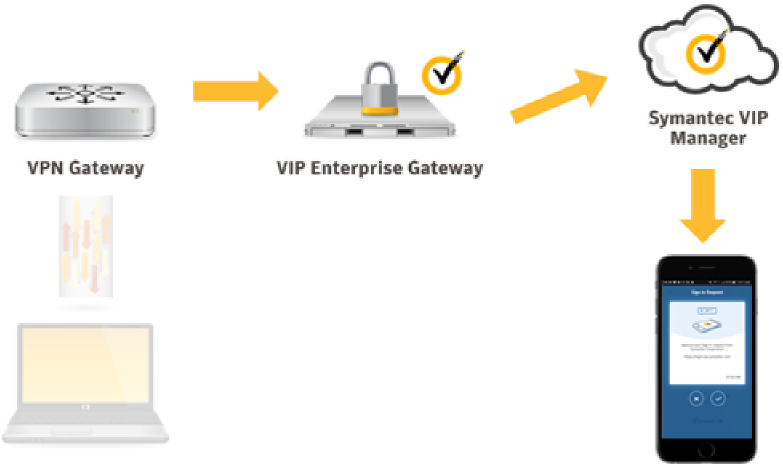
Design and topology considerations

Deploying VIP PUSH is done in three phases:

1. Enable the feature in **VIP Manager**
2. Enable the end application
3. Inform users of the new login experience

The biggest design and operational concept to be aware of is that the PUSH experience requires the application to "wait" longer for an authentication response. This is because not all authentication information was supplied at login, but a portion of this is waiting for the user to go to their device and approve the PUSH authentication. For this reason, a 5 second or 10 second timeout on the application needs to be increased.

General architecture of the VIP PUSH feature looks like this:



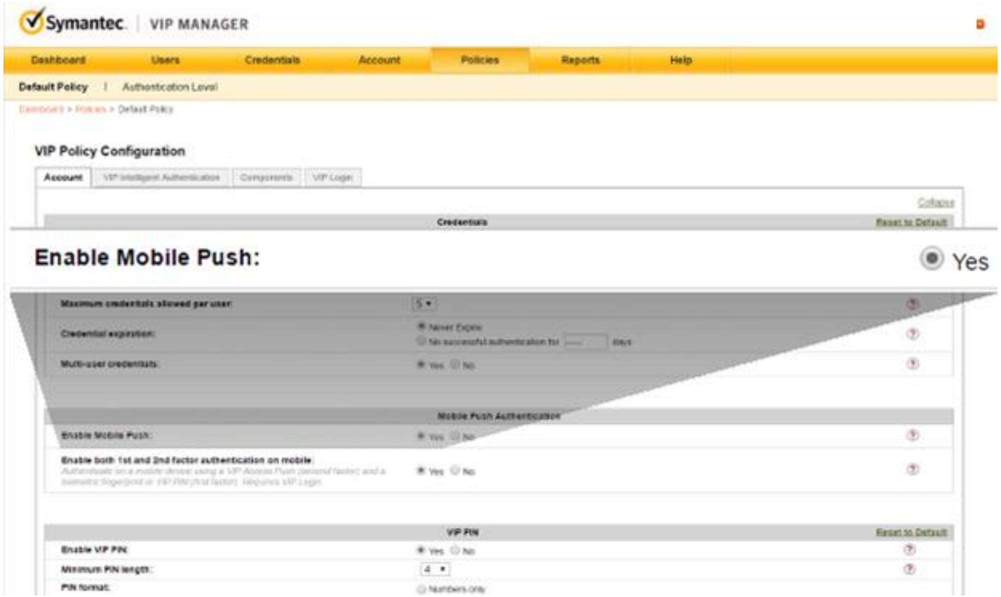
Additionally, VIP Enterprise Gateway tolerates a "classic experience" where the user supplies username, password, and security code together – and is authenticated. This allows smooth user experience transitions.

Configuration Summary

VIP PUSH feature enablement

To enable VIP PUSH in VIP Manager, do the following:

1) Open VIP Manager
2) Select **Policies** from the top navigation
3) On the **Account** subtab, select “Edit” from the right hand side
4) Under **Mobile Push Authentication**, change “Enable Mobile Push” from No to Yes



Enable Mobile Push: ● Yes

Maximum credentials allowed per user: 5

Credential expiration: ● Never Expire ○ No successful authentication for ____ days

Multi-user credentials: ● Yes ○ No

Enable Mobile Push: ● Yes ○ No

Enable both 1st and 2nd factor authentication on mobile: ● Yes ○ No
Authenticate on a mobile device using a VIP Access Push (second factor) and a biometric fingerprint or VIP PIN (first factor). Requires VIP Login.

Enable VIP PIN: ● Yes ○ No

Minimum PIN length: 4

PIN format: ○ Numbers only

Enabling the end application

Each application provider has different methods for configuring authentication servers such as VIP Enterprise Gateway. Key to the configuration is the ability to adjust the **timeout** of the “RADIUS Server”. Without this, authentication will likely be erratic for end users (can they beat the timeout or not). Typically, this will match the **Challenge Timeout** from VIP Enterprise Gateway.

Third party considerations

In general, the VPN or web application that is processing a PUSH login needs to wait for the downstream RADIUS server longer than it normally might. Changes from 5 seconds or 10 seconds (default application configuration) to 60 seconds (to support PUSH) are typical.

Specific recommendations about PUSH configuration settings are in the following integration guides:

Palo Alto Networks GlobalProtect VPN, see Chapter 3

Microsoft Active Directory Federation Services 3.0, see Chapter 4

Juniper Steel-Belted RADIUS, see Chapter 2

Cisco Secure Access Control Server (ACS), See Appendix A

Microsoft Credential Provider

Troubleshooting tips

If the timeout is not set correctly on the application server, it may retry. When it retries too fast (while VIP Enterprise Gateway is still awaiting the VIP service which is waiting on the VIP user to respond to the PUSH), then VIP Enterprise Gateway will log a “trample” message in that validation server’s logs.

The message below is an excerpt from a log where this happened:

```
“text=Access DENIED PUSH Trampled. ,reason=29; PUSH Trampled.”
```

If you see this message, identify the log that this is coming from and the associated application server. Then, review the application server’s authentication settings and be sure to configure the timeout value correctly (generally: increase it).

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 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