



Symantec VIP Quick Start Guide

Helping your users

Version 1.0

Author

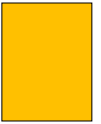
Maren Peasley





Table of Contents

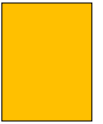
Introduction	2
Design and topology considerations.....	3
VIP Self-Service Portal: Internal only	4
VIP Self-Service Portal: External Allowed.....	5
Configuration Summary	6
VIP Self-Service Portal: Internal only	6
VIP Self-Service Portal: External Allowed.....	7
Important Processes	8
Forgotten Credential.....	8
Lost Credential	8
Stolen Credential.....	9
Troubleshooting tips	11
Appendix A: Additional Resources and Guides.....	12



Introduction

Let's face it: If users can find a way to get stuck in an unusual situation, they will. And it's our job to help them out of that situation (or keep them from going down that path in the first place). This is your guide to features meant specifically for the user, whether in a standard situation or an unusual situation and the emphasis is on easy self-help mechanisms.

Standard situations include how new users register and how they can keep their credentials updated through their own effort. Unusual situations include lost or forgotten credentials as well as stolen devices and what actions for the user and IT to take.



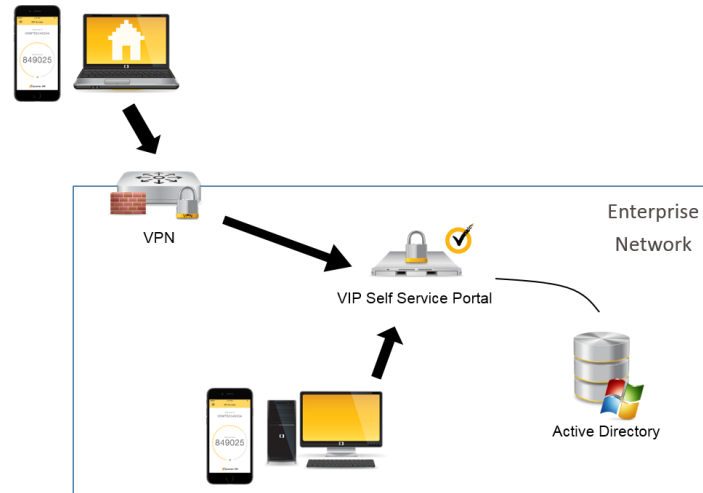
Design and topology considerations

Helping users in normal situations is relatively straightforward. There are two that we need chiefly be concerned with: getting new users registered and any credential updates that they may need to make over time. This latter situation is easily accommodated by providing a link to the VIP Self Service Portal on an internal help system and perhaps advertising this in email or an internal KB system. IT Helpdesk can also distribute this on a responsive basis as a reminder to users who get stuck.

There are two models for getting new users started via the Self Service Portal: internal-only registration and external registration. With internal-only registration, users need to either come in to the office or connect remotely in order to register. This presents a problem in that remote access services (such as VPN) typically need to be secured via multi-factor authentication which leads to a chicken-and-egg problem. With external registration, anyone from the Internet can discover the service and attempt to use it, leading to additional security requirements and technology considerations. Both are reviewed below.

VIP Self-Service Portal: Internal only

In this model, users first need to be on an internal network before they can access the Self Service Portal to register a new VIP credential. Users who cannot come into the office or gain remote access must contact IT Helpdesk to be provisioned or gain temporary access so they can do so themselves.



Ideally users register before the remote access method is changed. For large groups of users, a communication package is recommended in order to encourage action by the userbase and thereby reduce helpdesk calls after the remote access method requires two factor authentication (“go live”). In some instances, multiple VPN profiles can be active concurrently, reducing the urgency to change. In other instances it may be possible to send the user a security code out-of-band using a voice call, SMS message, or email. Normally, these are temporary until all users can register a VIP credential.

The user process looks something like this:

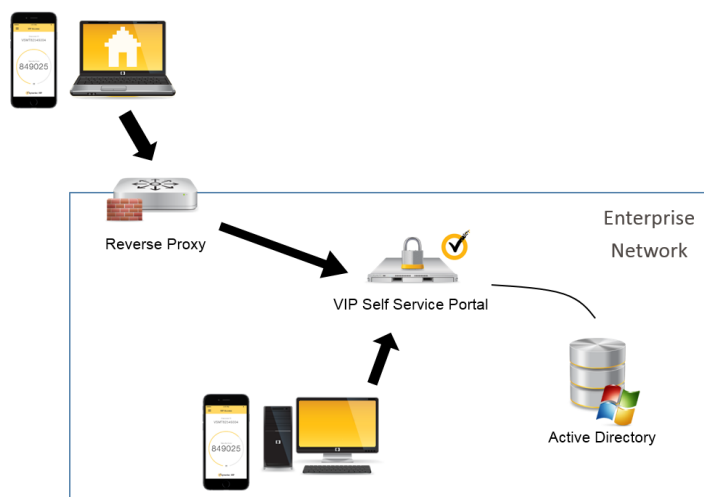


This link has a detailed view of this process:

<https://symantec.box.com/s/2aofmvljbkj1doat1f61hb3ucyfeasay>

VIP Self-Service Portal: External Allowed

In this model, internal users are sent directly to the Self Service Portal to register a new VIP credential and external users are directed to an external reverse proxy in the DMZ that internally contacts the VIP Self Service Portal on behalf of the user. It is strongly recommended to deploy additional automated verification checks of the user before allowing them to register a credential. This method uses VIP Enterprise Gateway's connection with the LDAP server to retrieve a phone or email attribute in order to send a security code to the user out-of-band. The user must be in possession of the phone number or email in order to proceed with registration.



The user process looks like this:



This link has a detailed view of this process:

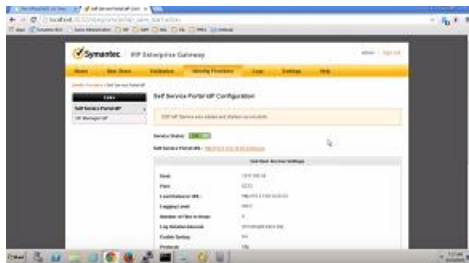
<https://symantec.box.com/s/5zf7ie70ff7yewj0o17xmvqccn0z115u>

Configuration Summary

[VIP Self-Service Portal: Internal only](#)

Enabling the VIP Self Service Portal for internal access only simply requires enabling the capability on one VIP Enterprise Gateway within the environment. Typically, only one Enterprise Gateway is required for registering users within any given environment.

A video of this process is available here:



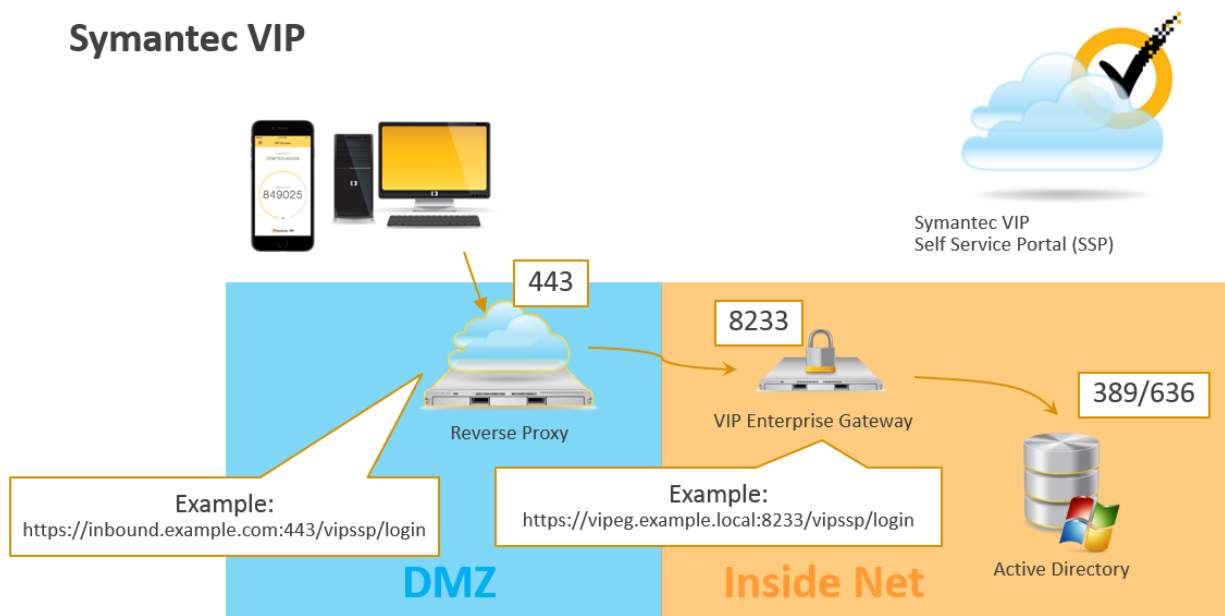
<https://youtu.be/Uzug6MM2dYo>

VIP Self-Service Portal: External Allowed

Enabling VIP Self Service Portal for external access requires:

- * The Self Service Portal is enabled in VIP Enterprise Gateway (as above),
- * A reverse proxy is mapping the external DNS name on tcp port 443 to the internal Self Service Portal URL on tcp port 8233
- * A secure, trusted digital certificate on the reverse proxy for the external DNS name
- * “Require second-factor authentication for first-time access” is configured in VIP Manager

For instructions on configuring your reverse proxy, see your proxy vendor’s documentation. The following diagram may be helpful:



Enabling “Require second-factor authentication for first-time access” in VIP Manager is done here:

VIP Manager > Policies > Components:

Require second-factor authentication for first-time access:

Yes No

Select one or more authentication method:

- Email
- SMS (Text Message)
- Voice Call

Important Processes

Now that the technology is setup, what remains is to give users an easy process and establish IT processes to handle these different situations. When the change is planned (such as when the user moves from one mobile device to another), IT can insert communication to improve the process: add the new VIP credential before removing the old one. Unexpected change usually happens when the user temporarily forgets their device with their VIP credential on it, loses their device, or where the device is actually stolen. These are each discussed, below.

Forgotten Credential

We've all done it: we show up at a remote location and don't have a required item. In this case, it's the user's 2nd factor credential sometimes referred to as the "VPN credential" due to its popularity with remote access services. While users can always call IT Helpdesk and get a one-time or temporary security code, you can provide "instant" or "middle-of-the-night" self-help through the Self Service Portal merely by enabling temporary security codes for the Self Service Portal.

Temporary Security Code enablement

- 1) Open [VIP Manager](#)
- 2) Select **Policies** from the top navigation
- 3) Select the **Components** subtab
- 4) Under **VIP Self Service Portal**, change "Enable temporary security codes" from No to Yes
- 5) Select distribution methods from **Email**, **SMS (Text Message)**, and **Voice Call**

The screenshot shows the configuration page for the VIP Self Service Portal. At the top right, there is a header with the text "VIP Self Service Portal" and a link "Reset to Default". Below this, the "Enable temporary security codes:" section has two radio buttons: "Yes" (which is selected) and "No". The "Select one or more distribution method:" section has three checkboxes, all of which are checked: "Email", "SMS (Text Message)", and "Voice Call".

Lost Credential



Occasionally, users will seamlessly shift from a "forgotten" credential to a "lost" credential, especially if they don't use it very often. Generally, it is easier for users to use their own VIP credential than to go through the several steps to obtain a temporary security code. However, users don't always want to go through the trouble of reporting a lost token and may feel embarrassed to do so. Operationally, this is a security concern if a user is no longer in possession of their security credentials.

IT should prepare for this situation in two ways: by proactively providing an easy method to report lost credentials (one additional aim of this is to reduce embarrassment in order to increase response from the users). IT can also proactively run an End User report in VIP Manager that clearly shows temporary

code activity across the entire account to look for users who might be using the temporary code feature as a replacement for their token.

Screening for lost tokens via VIP Manager reporting

- 1) Open [VIP Manager](#)
- 2) Select **Reporting** from the top navigation
- 3) Select the relevant period of time
- 4) Next to **Operation**, select “Set Temporary Password”
- 5) Click **Generate Report**
- 6) Optionally export the results to CSV for easier analysis

Reporting	
Report	Transaction Report ▼
Date Range	Last 90 Days ▼
Start Date:*	2017-Feb-17 
End Date:*	2017-May-18 
User ID	<input type="text"/>
Operation	Set Temporary Password ▼

Cancel

Generate Report

Confirmed (or strongly suspected) lost credentials should be marked as disabled for that user. As a reminder, the **disabled/inactive** states for a VIP credential are:

- Temporarily Unavailable
- Canceled
- Stolen
- Unspecified
- Lost
- Returned

Stolen Credential

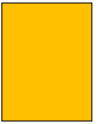
A stolen device is a major security event with multiple implications. In general, any accessibility through that device should be revoked. This includes credentials associated with that device as with VIP Access for Mobile, as well as any static application passwords associated with some applications. Further, the credential status should be changed by a VIP Administrator in VIP Manager from “Enabled” to “Disabled” -> “Stolen”:

Helping your users

The screenshot shows a form with the following fields:

- Credential Type:** VIP Access for Mobile
- Credential State:** Disabled ▼
- Reason:** A dropdown menu with the following options:
 - Select Reason ▼
 - Select Reason
 - Temporarily Unavailable
 - Canceled
 - Stolen (highlighted in blue)
 - Unspecified
 - Lost
 - Returned
- VIP Access Push:** (This field is currently empty)

Additional actions by the user or IT include contacting Law Enforcement, following an internal security process, contacting an internal security team, or more.



Troubleshooting tips

- Enable JavaScript debugging in your test browser
- Confirm components can communicate with each other

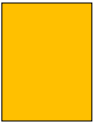
For further assistance, please contact:

Symantec Technical Support

<https://my.symantec.com>

Phone Support:

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

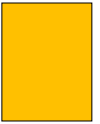


Appendix A: Additional Resources and Guides

[Quick Start Guide: Enabling Help Desk](#)

[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

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