Symantec™ Validation & ID Protection Service

Integration Guide for Apache® HTTP Server
Symantec VIP Integration Guide for Apache HTTP Server

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Last updated September 24, 2015

Legal Notice

Copyright © 2012 - 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. The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement. This document may describe features and/or functionality not present in your software or your service agreement. Contact your account representative to learn more about what is available with this Symantec* product.

Symantec Corporation
350 Ellis Street Mountain View, CA 94043

http://www.symantec.com
https://www.symantec.com/contactsupport
Chapter 1  Introduction .......................................................................................................................... 1
  Partner Information .............................................................................................................................. 1
  VIP Features Checklist .......................................................................................................................... 1
  Integration Summary ............................................................................................................................. 2
  Remote Access Integration Architecture ............................................................................................. 3
    Authentication Method: User Name - Security Code Using RADIUS (VIP Enterprise Gateway) .......... 4
    Authentication Method: User Name - Password - Security Code using RADIUS (VIP Enterprise Gateway) .................................................................................................................. 5
  Partner Product Requirements ............................................................................................................. 6
  Operating System Requirements .......................................................................................................... 6
  Software Requirements ......................................................................................................................... 7

Chapter 2  Installation and Configuration ............................................................................................. 9
  Integration Summary ............................................................................................................................. 9
  Installing and Configuring VIP Enterprise Gateway ........................................................................... 9
  Installing the VIP Integration Module for Apache HTTP Server ....................................................... 9
  Configuring the VIP Integration Module for Apache HTTP Server .................................................. 10

Chapter 3  VIP Intelligent Authentication Integration for Apache HTTP Server .................................. 19
  Prerequisites ......................................................................................................................................... 19
  Configure Intelligent Authentication with the VIP Components ....................................................... 19
  Generate Intelligent Authentication Code from VIP Manager ........................................................... 19
  Update the Login Page ......................................................................................................................... 19

Appendix A  Sample Login Pages and Configuration Files ............................................................... 21
This chapter includes the following topics:

- “Partner Information” on page 1
- “Integration Summary” on page 2
- “Remote Access Integration Architecture” on page 3
- “Partner Product Requirements” on page 6

The VIP Integration Guide for Apache HTTP Server describes how to integrate VIP integration module for Apache HTTP Server with VIP Enterprise Gateway to allow the User Name + Security Code authentication method. VIP integration module for Apache HTTP Server enables administrators to replace the standard login process with a two-factor, strong authentication login process. With the strong authentication process, the users must provide a security code along with the user name and the password to login to access a resource that is protected by Apache HTTP Server.

### Partner Information

<table>
<thead>
<tr>
<th>Table 1-1</th>
<th>Partner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Name</td>
<td>Apache®</td>
</tr>
<tr>
<td>Product Name</td>
<td>Apache® HTTP Server</td>
</tr>
<tr>
<td>Version</td>
<td>2.4.6 onwards</td>
</tr>
</tbody>
</table>

### VIP Features Checklist

Table 1-2 lists the VIP Enterprise Gateway features that are supported with Apache HTTP Server.

<table>
<thead>
<tr>
<th>Table 1-2</th>
<th>Supported Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>VIP Features</strong></td>
<td><strong>Support</strong></td>
</tr>
<tr>
<td>Multi-domain</td>
<td>Yes</td>
</tr>
<tr>
<td>Anonymous user name</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for AD/LDAP password via VIP Enterprise Gateway</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for VIP PIN authentication</td>
<td>No</td>
</tr>
<tr>
<td>Support for Push authentication</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for SMS authentication</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Integration Summary

#### Table 1-2 Supported Features

<table>
<thead>
<tr>
<th>VIP Features</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Voice authentication</td>
<td>Yes</td>
</tr>
<tr>
<td>End user-based for selective strong authentication</td>
<td>No</td>
</tr>
<tr>
<td>Risk-based for selective strong authentication</td>
<td>Yes</td>
</tr>
<tr>
<td>Legacy authentication provider</td>
<td>No</td>
</tr>
<tr>
<td>VIP JavaScript</td>
<td>Yes</td>
</tr>
<tr>
<td>VIP Login</td>
<td>No</td>
</tr>
</tbody>
</table>

#### Table 1-3 Integration Summary

<table>
<thead>
<tr>
<th>Authentication Methods Supported</th>
<th>User Name - Security Code</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>User Name - Password - Security Code</td>
</tr>
<tr>
<td></td>
<td>User Name - Access PIN - Security Code</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Integration</th>
<th>VIP Authentication Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RADIUS (VIP Enterprise Gateway 8.X or higher)</td>
</tr>
<tr>
<td></td>
<td>Intelligent Authentication (IA)</td>
</tr>
<tr>
<td></td>
<td>External Authentication Interface (You can configure Apache as EAI for IBM Tivoli Access Manager. For more information, see Symantec Validation and ID Protection Service Integration Guide for Tivoli Access Manager.)</td>
</tr>
</tbody>
</table>
Remote Access Integration Architecture

Authentication Method: User Name - Security Code Using VIP Authentication Service

The following flow diagram (Figure 1-1) illustrates the User Name - Security Code authentication method for Apache HTTP Server using the VIP Authentication Service.

1. The user enters a user name, password, and a security code in the Form Authentication login page.
2. As the first part of the two-factor authentication process, the VIP integration module for Apache HTTP Server sends the user name and the security code to VIP Authentication Service. The VIP Authentication Service authenticates the user name and the security code and returns an Access-Accept Authentication response to the VIP integration module for Apache HTTP Server.
3. As the second part of the two-factor authentication process, the user name and the password are sent to native authentication modules of Apache like File, LDAP, etc.
4. Based on this response, the user is allowed to access the resources protected by Apache HTTP Server.
Authentication Method: User Name - Security Code Using RADIUS (VIP Enterprise Gateway)

The following flow diagram (Figure 1-2) illustrates the User Name - Security Code authentication method for Apache HTTP Server using RADIUS (VIP Enterprise Gateway):

1. The user enters a user name, password, and security code in the Forms Authentication login page.
2. As the first part of the two-factor authentication process, the VIP integration module for Apache HTTP Server sends the user name and the security code to the Validation Service for authentication.
3. The Validation Service authenticates the user name and the security code with the VIP Authentication Service and returns an Access-Accept Authentication response to the VIP integration module for Apache HTTP Server.
4. As the second part of the two-factor authentication process, the user name and the password are sent to the native authentication modules of Apache like File, LDAP, etc.
5. Based on this response, the user is allowed to access the resources protected.
Authentication Method: User Name - Password - Security Code using RADIUS (VIP Enterprise Gateway)

The following diagram illustrates the User Name - Password - Security Code authentication method for Apache HTTP Server using RADIUS (VIP Enterprise Gateway):

1. The user enters a user name, password, and security code in the Forms Authentication login page.
2. As the first part of the two-factor authentication process, the VIP integration module for Apache HTTP Server sends the user name, password, and the security code to the Validation Server for authentication.
3. The Validation Server authenticates the user name and password with the user store.
4. The Validation server authenticates the user name and security code with the VIP Authentication Service and returns an Access-Accept Authentication response to the VIP integration module for Apache HTTP Server.
5. Based on this response, the user is allowed to access the resources protected.

The following diagram illustrates the User Name - Access PIN - Security Code authentication method for Apache HTTP Server using RADIUS (VIP Enterprise Gateway):

1. The user enters a user name, access pin, and security code in the Forms Authentication login page.
2. As the first part of the two-factor authentication process, the VIP integration module for Apache HTTP Server sends the user name, Access PIN, and the security code to the Validation Server for authentication.
3. The Validation server authenticates the user name, access pin, and security code with the VIP Authentication Service and returns an Access-Accept Authentication response to the VIP integration module for Apache HTTP Server.
4. Based on this response, the user is allowed to access the resources protected.
Partner Product Requirements

Operating System Requirements
- Red Hat Enterprise Linux 5.6 (64 Bit)
- Red Hat Enterprise Linux 6.2 (64 Bit)
- Red Hat Enterprise Linux 6.3 (64 Bit)
- Red Hat Enterprise Linux 6.4 (64 Bit)
- Red Hat Enterprise Linux 6.5 (64 Bit)

Software Requirements
- Apache HTTP Server 2.4.6
- Apache HTTP Server 2.4.7
- Apache HTTP Server 2.4.9
Introduction

Partner Product Requirements
Installation and Configuration

This chapter includes the following topic:

- **Integration Summary** on page 9

Integration Summary

The following summary of procedures describes how to configure the VIP integration module for Apache HTTP Server for two-factor authentication through RADIUS and VIP Authentication Service.

- **Step 1:** “Installing and Configuring VIP Enterprise Gateway” on page 9
- **Step 2:** “Installing the VIP Integration Module for Apache HTTP Server” on page 9
- **Step 3:** “Configuring the VIP Integration Module for Apache HTTP Server” on page 10

Installing and Configuring VIP Enterprise Gateway

1. Install and configure VIP Enterprise Gateway.
2. Add the validation server in one of the following modes:
   - User Name – Security Code
   - User Name – Access PIN – Security Code
   - User Name – Password – Security Code

**Note:** Ignore this step if you choose to integrate Apache with VIP Authentication Service.

Installing the VIP Integration Module for Apache HTTP Server

**Note:** In this document, **ApacheRoot** indicates the absolute path of the Apache root directory.

1. Copy the authentication module for Apache HTTP Server to the **modules** directory in the **ApacheRoot** directory.

   **Command Usage:**

   ```bash
   cp mod_authn_symc.so ApacheRoot/modules/mod_authn_symc.so
   ```

2. Copy the following libraries to the `/usr/lib64/` directory to resolve the run-time dependencies of the authentication module for Apache HTTP Server.
Command Usage:

- cp libvsauthotpclient.so /usr/lib64/
- cp libvsauthwsclientimpl.so /usr/lib64/
- cp libvsauthwsclient.so /usr/lib64/
- cp libvsradiusclientimpl.so /usr/lib64/
- cp libsymccar.so /usr/lib64/

3 Copy the following conf files to /opt/apache directory.
   cp symcAuth_radius.conf /opt/apache
   cp symcAuth_webservice.conf /opt/apache

4 Edit the Apache configuration file (ApacheRoot/conf/httpd.conf) to enable the authentication module for Apache HTTP Server by adding the following line in the LoadModule section:

   LoadModule authn_symc_module modules/mod_authn_symc.so

5 Enable the following modules:

   LoadModule auth_form_module modules/mod_auth_form.so
   LoadModule session_module modules/mod_session.so
   LoadModule request_module modules/mod_request.so
   LoadModule session_cookie_module modules/mod_session_cookie.so

6 Enable the first-factor authentication module, LDAP, or File.

Note: Ignore this step if you have already configured Apache with first-factor module. In this document, File based authentication is used as a first-factor authentication module for test purpose. You must enable the authentication module as per your configuration. Enabling the first-factor authentication module is not required if the VIP Enterprise Gateway Validation server is configured with User Name - Password - Security Code mode.

   LoadModule authn_file_module modules/mod_authn_file.so

Configuring the VIP Integration Module for Apache HTTP Server

You must complete the following procedures to configure the VIP integration module for Apache HTTP Server:

Note: The section Create a Web Resource to Test VIP Integration Module for Apache HTTP Server describes how to create a web resource and a login page. This section is included only to demonstrate how to configure the authentication module for Apache to protect a web resource. You can avoid the steps if you already have the web resource that you want to protect.

- Configure Authentication Methods
  - Configure VIP Authentication Service
  - Configure RADIUS Authentication
- Protect Apache Web Resource with VIP Integration Module
- Create a Web Resource to Test VIP Integration Module for Apache HTTP Server
- Update the User Login Page with Security Code Field
- Tivoli Access Manager (TAM) - External Authentication Interface (EAI) for Step-up Authentication
- Test Configuration Settings
- Restart Apache HTTP Server
Configure Authentication Methods

You can integrate the Apache web server with Symantec VIP using the following authentication methods:

- VIP Authentication Service
- RADIUS Authentication

You must choose the authentication method based on your requirement.

- For more information on configuring the VIP Authentication Service, see “Configure VIP Authentication Service” on page 11.
- For more information on configuring the RADIUS server, see “Configure RADIUS Authentication” on page 12.

Configure VIP Authentication Service

To configure the VIP Authentication Service, modify the following fields (Table 2-1) in the symcAuth_webservice.conf configuration file:

Table 2-1 Fields for configuring VIP Authentication Service

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VIP Authentication Service Settings</td>
<td></td>
</tr>
<tr>
<td>Module Name</td>
<td>Custom name for the VIP integration module. For example, Apache.</td>
</tr>
<tr>
<td>&lt;moduleName&gt;</td>
<td></td>
</tr>
<tr>
<td>Thread Pool Size</td>
<td>Number of synchronous threads created for serving the requests from client.</td>
</tr>
<tr>
<td>&lt;threadPoolSize&gt;</td>
<td></td>
</tr>
<tr>
<td>Authentication URL</td>
<td>VIP Authentication Service URL used to authenticate the user name and the security code:</td>
</tr>
<tr>
<td>&lt;validateUrl&gt;</td>
<td><a href="https://userservices-auth.vip.symantec.com/vipuserservices/AuthenticationService_1_1">https://userservices-auth.vip.symantec.com/vipuserservices/AuthenticationService_1_1</a></td>
</tr>
<tr>
<td>VIP Certificate</td>
<td>Specify the certificate file location currently on the local system.</td>
</tr>
<tr>
<td>&lt;keyStore&gt;</td>
<td></td>
</tr>
<tr>
<td>VIP Certificate Password</td>
<td>Enter the password of the VIP certificate file specified in the VIP Certificate field.</td>
</tr>
<tr>
<td>&lt;keyStorePassword&gt;</td>
<td></td>
</tr>
<tr>
<td>VIP Trust Store</td>
<td>Specify the trust certificate file location currently on the local system.</td>
</tr>
<tr>
<td>&lt;trustStore&gt;</td>
<td></td>
</tr>
<tr>
<td>Proxy Settings</td>
<td></td>
</tr>
<tr>
<td>Host IP</td>
<td>IP address of the proxy server.</td>
</tr>
<tr>
<td>&lt;proxyHost&gt;</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port number of the proxy server.</td>
</tr>
<tr>
<td>&lt;proxyPort&gt;</td>
<td></td>
</tr>
</tbody>
</table>
For a sample configuration file, which uses VIP Authentication Service as the authentication method, see Appendix A, "Sample Login Pages and Configuration Files."

**Configure RADIUS Authentication**

Modify the following fields in the `symcAuth_radius.conf` configuration file to configure the RADIUS authentication:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The optional user name for proxy basic authentication.</td>
</tr>
<tr>
<td>&lt;proxyUsername&gt;</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>The password for the optional user name for proxy basic authentication.</td>
</tr>
<tr>
<td>&lt;proxyPassword&gt;</td>
<td>If required, you can use the <code>camouflage</code> utility from the package to encrypt this password.</td>
</tr>
<tr>
<td>Usage: camouflage &lt;password&gt;</td>
<td>You can use the encrypted password in the following format:</td>
</tr>
<tr>
<td></td>
<td>::encrypted::&lt;encrypted_password&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>proxyPassword=::encrypted::&lt;encrypted_password&gt;</td>
</tr>
<tr>
<td>Business Continuity</td>
<td></td>
</tr>
<tr>
<td>Enable Business Continuity</td>
<td>Set to <code>true</code> to enable business continuity.</td>
</tr>
<tr>
<td>&lt;enableBusinessContinuity&gt;</td>
<td>Set to <code>false</code> to disable business continuity.</td>
</tr>
</tbody>
</table>

For a sample configuration file, which uses VIP Authentication Service as the authentication method, see Appendix A, "Sample Login Pages and Configuration Files."

**configure RADIUS Authentication**

Modify the following fields in the `symcAuth_radius.conf` configuration file to configure the RADIUS authentication:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Configuration</td>
<td></td>
</tr>
<tr>
<td>RADIUS Server Settings</td>
<td></td>
</tr>
<tr>
<td>Server IP</td>
<td>Specify your VIP Enterprise Gateway RADIUS server IP address.</td>
</tr>
<tr>
<td>&lt;serverIp&gt;</td>
<td></td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the RADIUS pre-shared secret.</td>
</tr>
<tr>
<td>&lt;serverSecret&gt;</td>
<td>If required, you can use the <code>camouflage</code> utility from the package to encrypt this password.</td>
</tr>
<tr>
<td>Usage: camouflage &lt;password&gt;</td>
<td>You can use the encrypted password in the following format:</td>
</tr>
<tr>
<td></td>
<td>::encrypted::&lt;encrypted_password&gt;</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>serverSecret=::encrypted::&lt;encrypted_password&gt;</td>
</tr>
<tr>
<td>Server Port</td>
<td>Enter the port number of the RADIUS server.</td>
</tr>
<tr>
<td>&lt;serverPort&gt;</td>
<td></td>
</tr>
<tr>
<td>RADIUS Common Settings</td>
<td></td>
</tr>
<tr>
<td>Context Pool</td>
<td>Enter the RADIUS server capacity.</td>
</tr>
<tr>
<td>&lt;contextPoolCapacity&gt;</td>
<td><strong>Note:</strong> This is the number of RADIUS server synchronous threads created for serving the requests from client. The default value is 16.</td>
</tr>
</tbody>
</table>
You can configure VIP integration module for Apache HTTP Server with multiple VIP Enterprise Gateway RADIUS servers for validation fail over. For this, you must define multiple VIP Enterprise Gateway RADIUS server instances each with a distinct server ID.

For example:

```
[RadiusServer#1]
# Radius server IP
serverIp=10.10.10.11
# Radius server port
serverPort=1812
# Radius shared secret
serverSecret=password1

[RadiusServer#2]
# Radius server IP
serverIp=10.10.10.12
# Radius server port
serverPort=1812
# Radius shared secret
serverSecret=password2
```

For a sample configuration file, which uses RADIUS Authentication as the authentication method, see Appendix A, "Sample Login Pages and Configuration Files."
Protect Apache Web Resource with VIP Integration Module

After the VIP integration module for Apache HTTP Server is loaded, you can protect a web resource deployed on the Apache HTTP Server using this module.

In the Apache HTTP configuration file (ApacheRoot/conf/httpd.conf), add or update the Directory section for the web resource that you want to protect as follows.


```html
<Directory "ApacheRoot/htdocs/symcTest">
    AuthFormProvider symc file
    AuthType form
    AuthName "VIP Authentication Protected Area"
    Session On
    SessionCookieName session path=/
    Require valid-user
    # This is the login page
    ErrorDocument 401 /login.html
    # This is the file containing users login data
    AuthUserFile ApacheRoot/auth/.htpasswd
    AuthSymcConf /opt/apache/symcAuth_radius.conf
    AuthSymcSplitPassword false
</Directory>
```

Username–Password–Security code

Note: If Apache web server is used as External Authentication Interface (EAI) for IBM Tivoli Access Manager (TAM), then make sure that in the SessionCookieName session path=/ is removed or commented.

```html
<Directory "ApacheRoot/htdocs/symcTest">
    AuthFormProvider symc
    AuthType form
    AuthName "VIP Authentication Protected Area"
    Session On
    SessionCookieName session path=/
    Require valid-user
    # This is the login page
    ErrorDocument 401 /login.html
    # This is the file containing users login data
    AuthUserFile ApacheRoot/auth/.htpasswd
    AuthSymcConf /opt/apache/symcAuth_radius.conf
    AuthSymcSplitPassword false
</Directory>
```

Note: Make sure that you update the highlighted part appropriately.
Create a Web Resource to Test VIP Integration Module for Apache HTTP Server

Create a directory called symcTest in the ApacheRoot/htdocs/ directory. Create a HTML file that you want to protect in the ApacheRoot/htdocs/symcTest directory.

Following is the sample HTML page (index.html). You must set the file permissions to 755.

```html
<html>
<head>
  <title>You are currently logged in using Symantec Authentication</title>
</head>
<body>
  <p>You are currently logged in using Symantec Authentication</p>
</body>
</html>
```
Update the User Login Page with Security Code Field

If you configure Apache in Username–Security code validation mode, then in the existing login page, add the below Security Code field under the Password field.

```html
<tr>
<td nowrap><label for="otp">Security Code:</label></td>
<td><input type="password" name="httpd_securitycode" value=""></td>
</tr>
```

If the Apache server is not configured with first-factor authentication, then you must perform the following step to configure the Apache server.

- Copy and paste the `login.html` and `login_error.html` to the `htdocs` folder. For a sample `login.html` and `login_error.html` file, see Appendix A, "Sample Login Pages and Configuration Files."

Tivoli Access Manager (TAM) - External Authentication Interface (EAI) for Step-up Authentication

IBM Tivoli Access Manager (TAM) server can rely on Apache HTTP Server as an External Authentication Interface (EAI) to perform only second-factor authentication, or both first and second-factor authentication.

If you have configured TAM with Step-up authentication (multi-level authentication) and if it uses the TAM Step-up login page, then you must configure the following sample login page as `stepup.html` login page in Apache.

Perform the following steps to configure the sample login page:

1. Create the login page as `stepup.html` and keep under the `htdocs` folder.

   ```html
   <html>
   <head>
   <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
   <title>Login page</title>
   </head>
   <body>
   <form method="POST" action="http://<Apache_FQDN/IP>/symcTest/">
   <table border="1">
   <tr>
   <td> User Name: <input type="text" name="httpd_username" readonly/></td>
   </tr>
   <tr>
   <td nowrap><label for="otp">Security Code: </label><input type="password" name="httpd_securitycode" value="" /></td>
   </tr>
   <br/>
   <input type="submit" name="login" value="Login" />
   </form>
   </body>
   </html>
   ```
Note:

1. You must update the highlighted text in the above code appropriately. SymcTest is the protected resource in Apache.

2. The POST action URL must end with "/". For example, `<form method="POST" action="http://<Apache_FQDN>/symcTest/>">

3. If Apache server is configured with https, then make sure that the POST Action URL is updated accordingly.

Set up the VIP Integration Module to protect a web resource and update the directory in the `httpd.conf` file as configured below:

```xml
<Directory "/usr/local/apache2/htdocs/symcTest">
    AuthFormProvider symc
    AuthType form
    AuthName "VIP Authentication Protected Area"
    Session On
    Require valid-user
    ErrorDocument 401 /stepup.html
    AuthSymcConf /home/vipadmin/Apache/2.4.2/linux_x86-64/symcAuth_radius.conf
    AuthSymcSplitPassword false
</Directory>
```

Ensure that the following entries are set appropriately in `symcAuth_radius.conf` for the step up authentication to work correctly:

- `validationMode=UO` or `UAO`
- `stepupAuthentication=true`
- `authenticationLevel=2`

Restart Apache HTTP Server.

Test Configuration Settings

You can use the `symc_test` utility for testing the configuration settings.

To test the VIP Authentication Service configuration, prepare the VIP Authentication Service configuration file (`<ApacheRoot>/webservice.conf`) and run the following command with a valid user name and a security code:

```bash
./symc_test -conf_file <ApacheRoot>/webservice.conf -username apache_user1 -securitycode 123456 -log_level SYMC_DEBUG -log_file /tmp/symcLogs
```

To test the RADIUS configuration, prepare the RADIUS configuration file (`ApacheRoot>/radius.conf`) and run the following command with a valid user name and a security code:

```bash
./symc_test -conf_file <ApacheRoot>/radius.conf -username apache_user1 -securitycode 123456 -log_level SYMC_DEBUG -log_file /tmp/symcLogs
```

Restart Apache HTTP Server

After the VIP integration module for Apache HTTP Server is setup properly, you must restart the Apache HTTP Server for the changes to take place.

To restart the Apache HTTP server, you can run the following command as root:

```bash
<ApacheRoot>/bin/apachectl restart
```

Note: Restart the Apache HTTP Server for the configuration changes to take effect.
VIP Intelligent Authentication Integration for Apache HTTP Server

This chapter describes how to integrate VIP Intelligent Authentication (IA) with Apache HTTP Server. To integrate VIP IA with Apache HTTP Server, you must perform the following steps:

- **Step 1**: “Configure Intelligent Authentication with the VIP Components” on page 19
- **Step 2**: “Generate Intelligent Authentication Code from VIP Manager” on page 19
- **Step 3**: “Update the Login Page” on page 19

Prerequisites

You must complete the steps in “Installation and Configuration” on page 9 before you configure Intelligent Authentication.

Configure Intelligent Authentication with the VIP Components

You must configure Intelligent Authentication (IA) with VIP Manager and VIP Enterprise Gateway (EG) before you update the login page of the integration module. For details, see *Symantec VIP Intelligent Authentication Enterprise Integration Guide* (IA_Enterprise_Integration.pdf), which you can download from the Intelligent_Authentication folder in VIP Manager.

Generate Intelligent Authentication Code from VIP Manager

You must select the Manual method and the User Name + Security Code authentication mode in VIP Manager to generate the VIP integration code.

Update the Login Page

1. Copy the VIP integration code that you have generated within VIP Manager and paste it between the `<head>` and the `</head>` tags of the Apache HTTP Server login page.
2. Hide the Security Code field by adding the following highlighted code in login page:

   ```html
   <td nowrap><label for="otp" style="display:none" >Security Code:</label> </td>
   <td> <input type="password" name="httpd_securitycode"  value="" style="display:none" />
   </td>
   
   <input type="hidden" name="httpd_securitycode" value="" />
   ```

   **Note:** This field will be filled automatically after the IA integration with the Apache HTTP Server module.

3. Save the changes.
Sample Login Pages and Configuration Files

This appendix provides samples of login pages and configuration files.

Note: The code provided in the following sections is a sample. The actual deployment code can be different, depending on your organization’s security policies.

Sample Login page

Note:

1. You must configure POST action if you use `login.html` and `login_error.html` page for TAM - EAI integration. For example, `<form method="POST" action="http://<Apache_FQDN>/symcTest/">` where SymcTest is the protected resource in Apache.

2. The POST action URL must end with "/". For example, `<form method="POST" action="http://<Apache_FQDN>/symcTest/">`

3. If Apache server is configured with https, then make sure that the POST Action URL is updated accordingly.

`login.html`

```html
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<title>Login page</title>
<style id="antiClickjack">body{display:none !important;}</style>
<script type="text/javascript">
if (self !== top) {
    var antiClickjack = document.getElementById("antiClickjack");
    antiClickjack.parentNode.removeChild(antiClickjack);
} else {
    top.location = self.location;
}
</script>
</head>
<body>
<form method="POST" action="" name="myForm">
```
<table border="1">
<tr>
<td>User Name: <input type="text" name="httpd_username" value="" /></td>
</tr>
<tr>
<td>Password: <input type="password" name="httpd_password" autocomplete="off" value="" /></td>
</tr>
<tr>
<td nowrap><label for="otp">Security Code: </label><input type="password" name="httpd_securitycode" autocomplete="off" value="" /></td>
</tr>
</table>
<br />
<input type="submit" name="login" value="Login" />
</form>
</body>
</html>

Sample Login Error page

login_error.html
<html>
<head>
<meta http-equiv="Content-Type" content= "text/html; charset=UTF-8">
<!-- Enter Page Title -->
title>Login Failed</title>
<style id="antiClickjack">body{display:none !important;}</style>
<script type="text/javascript">
if (self === top) {
    var antiClickjack = document.getElementById("antiClickjack");
    antiClickjack.parentNode.removeChild(antiClickjack);
} else {
    top.location = self.location;
}
</script>
</head>
<body>
<!-- Enter Message Header -->
<h1><font color="#FF0000">Login Failed</font></h1>
<p><!-- Enter Error Message -->
You must login with correct credentials before you can access the resource you have requested.
</p>
<form method="POST" action="" name="myForm">
<table border="1">
<tr>

Sample Login Pages and Configuration Files

<form>
<tr>
<td>User Name: <input type="text" name="httpd_username" value="" /></td>
</tr>
<tr>
<td>Password: <input type="password" name="httpd_password" autocomplete="off" value="" /></td>
</tr>
<tr>
<td>Security Code: <input type="password" name="httpd_securitycode" autocomplete="off" value="" /></td>
</tr>
</form>

<br/>

<input type="submit" name="login" value="Login" />

Sample Configuration file using VIP Authentication Service

The following is the sample configuration file which uses VIP Authentication Service as the authentication method:

```
# Authentication type <TYPE>
# <TYPE> takes the following values.
# radius : Radius authentication. (default)
# webservice : Direct to cloud.
authnType=webservice

# Webservice settings
[WebService]
# VIP Module Name
moduleName=Apache
# VIP Threadpool Size
threadPoolSize=10
# VIP Validation URL
validateUrl=https://userservices-auth.vip.symantec.com/vipuserservices/AuthenticationService_1_1
# VIP Truststores
trustStore=ApacheRoot/certs/root.pem
# VIP Keystores
keyStore= ApacheRoot /certs/KEYSTORE_extended_vip_cert.pem
keyStorePassword=password1
# VIP Business Continuity <true/false>
enableBusinessContinuity=
# VIP Proxy Info
proxyHost=
proxyPort=
proxyUsername=
proxyPassword=
```
Sample Configuration file using RADIUS Authentication

Following is the sample configuration file, which uses RADIUS Authentication as the authentication method:

```plaintext
# Authentication type <TYPE>
# radius: Radius authentication.
authnType=radius

# Radius common settings
[RadiusCommon]
# Radius retries
callAttempts=3
# Radius timeout
readTimeout=5
# Radius context pool capacity
contextPoolCapacity=10
# OTP size
otpSize=6
# Client IP (Local)
clientIp=10.10.10.10
# VIP Validation Server Mode <MODE>
# <MODE> takes the following values.
# UO : Here the validation server validates the Security Code for authentication.(default)
# ULO : Here the validation server validates the Password and Security Code for authenticaion.
# UAO : Here the validation server validates the Access Pin and Security Code for authenticaion.
validationMode=UO
# stepupAuthentication <value>
# <value> takes the following values.
# true : If apache is being used for TAM-EAI stepup authentication
# false : If apache is not being used for authenticationLevel TAM-EAI
stepupAuthentication=false
# authenticationLevel <value> needs to be set in header. Default is 2
authenticationLevel=2
# Radius server instance [RadiusServer#ID]
[RadiusServer#1]
# Radius server IP
serverIp=10.10.10.11
# Radius server port
serverPort=1812
# Radius shared secret
# Radius shared secret could be in plain text or encrypted value. Refer configuration guide for more details
serverSecret=password1

[RadiusServer#2]
# Radius server IP
serverIp=10.10.10.12
# Radius server port
serverPort=1812
# Radius shared secret
serverSecret=password2
```