Symantec™ Validation and ID Protection Service (VIP)

Integration Guide for Microsoft® Graphical Identification and Authentication
Symantec VIP Integration Guide for Microsoft® Graphical Identification and Authentication

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 April 15, 2014

Legal Notice

Copyright © 2011 - 2014 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. VeriSign, VeriSign Trust, and other related marks are the trademarks or registered trademarks of VeriSign, Inc. or its affiliates or subsidiaries in the U.S. and other countries and licensed to Symantec Corporation. 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
http://www.symauth.com/support/index.html
### Chapter 1  Introduction

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partner Information</td>
<td>1</td>
</tr>
<tr>
<td>Integration Overview</td>
<td>1</td>
</tr>
<tr>
<td>How VIP Module for GINA Works</td>
<td>1</td>
</tr>
</tbody>
</table>

### Chapter 2  Installation and Configuration

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration Summary</td>
<td>3</td>
</tr>
<tr>
<td>Test an End User</td>
<td>11</td>
</tr>
</tbody>
</table>
Introduction

This guide describes how to integrate Microsoft Graphical Identification and Authentication (GINA) with VIP Enterprise Gateway to allow the authentication methods listed in Table 1-2. This integration enables two-factor authentication for users who access your resources that GINA protects.

Two-factor authentication provides greater security for your protected resources, as it relies on something the user knows (a user name and a password) and something a user has (a security code generated by his or her VIP credential registered in the VIP Service) to validate the user.

Users generate a security code on their VIP credential that is registered in the VIP Service. Then, the users use that security code, along with their user name and access PIN or password, to gain access to the protected resources. The first factor is validated by Active Directory (AD), and the second factor is (user name and the security code) is validated by VIP Enterprise Gateway.

Partner Information

The following table lists partner and product details used to integrate GINA with VIP Enterprise Gateway:

Table 1-1 Partner Information

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>Microsoft®</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Name</td>
<td>Graphical Identification and Authentication (GINA)</td>
</tr>
</tbody>
</table>

Integration Overview

The following table provides a summary of GINA’s integration with VIP Enterprise Gateway:

Table 1-2 Integration Overview

<table>
<thead>
<tr>
<th>Authentication Methods Supported</th>
<th>User Name - Security Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Integration</td>
<td>VIP Enterprise Gateway (EG) 8.x or Higher</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>Microsoft Windows Server 2003 SP2 (x86)</td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server 2003 SP2 (x64)</td>
</tr>
</tbody>
</table>

How VIP Module for GINA Works

Figure 1-1 and the subsequent steps illustrate how VIP integration module for GINA integrates with VIP Enterprise Gateway using the User Name - Security Code authentication method.

After two-factor authentication is successfully enabled, users can access protected resources using their AD user name, password, and security code.
The user enters his or her user name, password, and security code.

As the first part of the two-factor authentication process, GINA authenticates the user name and password against the AD.

If the AD authenticates the user name and password, GINA asks for a security code, and then sends the user name and security code to the Validation Service for authentication. This is the second part of the two-factor authentication process.

The Validation Service authenticates the user name and security code with the VIP Authentication Service.

If the user name and security code are authenticated, the user is accepted for access.

Based on this response, the user is allowed to log in.
Integration Summary

The following summary of procedures describes how to install and configure the Symantec® GINA plug-in for two-factor authentication through VIP Enterprise Gateway.

- Task 1, "Install and Configure VIP Enterprise Gateway"
- Task 2, "Install and Configure the Symantec VIP GINA Plug-in"
- "Test an End User" on page 11

Task 1. Install and Configure VIP Enterprise Gateway

You must install and configure VIP Enterprise Gateway before you integrate Symantec VIP Module for GINA with VIP Enterprise Gateway. Configure VIP Enterprise Gateway Validation server in the **User Name – Security Code** mode. For more details, refer to the **VIP Enterprise Gateway Installation and Configuration Guide**.

After you configure the Validation server, you must modify your Validation Server settings as follows:

1. Navigate to the following folder:
   
   ```
   C:\<vipeg_install_folder>\Validation\servers\<validation_server_name>\conf
   ```
   
   Using a standard text editor, modify the `radserv.conf` file by changing
   ```
   StandardController.stripDomainName = true
   ```

2. Start the Validation Server (or restart it, if already running).

3. To test the Validation Server, download and run the `vsradiusclient_test` utility (available in `tools.zip` from the VIP Manager web site) on the GINA client host in verbose mode. Here is a sample command:
   ```
   C:\<tools_folder>\vsradiusclient_test.exe --server-host <your_server_ip> --server-port <your_server_port> --secret <your_server_password> --client-ip <your_client_ip> --user-name <username> --password <security_code> --verbose
   ```

   **Note**: Do not use the 32-bit `vsradiusclient_test` utility on 64-bit Windows.

Task 2. Install and Configure the Symantec VIP GINA Plug-in

Complete the procedures in this section to install and configure the Symantec VIP GINA Plug-in.

The following files are provided as part of the GINA integration module software package:

- **32 bit installer** - Microsoft\GINA\x86\VIP Enterprise Gateway GINA.msi
- **64 bit installer** - Microsoft\GINA\x86-64\VIP Enterprise Gateway GINA x86-64.msi

Software Requirements

- Microsoft Visual C++ 2010 x86 SP1 Redistributable (for 32 bit operating system)
- Microsoft Visual C++ 2010 x64 SP1 Redistributable (for 64 bit operating system)
Manual Installation

1. Download Microsoft_GINA.zip and Tools.zip from the VIP Manager web site and unzip both files.

2. Run the camouflage utility (available in the tools\windows folder), specifying your RADIUS shared secret on the command line. For 64-bit operating system, the camouflage utility is available at tools\windows_64.

   Usage:
   
   camouflage <password>

   Example:
   
   C:\<tools_folder>\camouflage password
   RNq6gi75hp0erLCbB7idaQ==

   Note: Do not use the 32-bit camouflage utility on 64-bit Windows.

3. Modify the entries in the C:\<microsoft_gina_setup_folder>\ginaconfig.txt file. Enter the correct RADIUS host IP, port number, and encrypted shared secret. For example, a line in the configuration file would read as follows:

   "Validation Server"="vipeg_server_ip:port:<camouflaged_password>"

   Where,
   
   - vipeg_server_ip:port is the IP address and port number of the validation service (RADIUS server) to which the Symantec GINA plug-in will connect.
   - <camouflaged_password> is the encrypted version of the RADIUS shared secret obtained in the previous step.

4. (Optional) To support failover to multiple RADIUS servers, add an additional parameter for the failover RADIUS server. For example:

   "Validation Server"="vipeg_server_ip_1:port:<camouflaged_password>,
vipeg_server_ip_2:port:<camouflaged_password>"

   Note: If two RADIUS servers are configured and both servers are up, the validation requests are load-balanced in round-robin sequence within a 20-second period. When one server is up, requests are sent to that active server.

5. (Optional) Increase the Validation Service response time out value, if required. By default, the Validation Service response time out value is set to 2 seconds.

6. Run C:\<microsoft_gina_setup_folder>\x86\VIP Enterprise Gateway GINA.msi (for 32 bit) or C:\<microsoft_gina_setup_folder>\x86-64\VIP Enterprise Gateway GINA x86-64.msi (for 64 bit). Browse for the location of the configured ginaconfig.txt file when the setup asks for it.

7. Restart the system after installation has completed.

Disable Two-Factor Authentication for Users without Credentials

All domain users must possess a security token. If they do not possess a security token, they will not be able to login.

For users without credentials, this behavior can be disabled with the following registry option:

HKEY_LOCAL_MACHINE\SOFTWARE\VeriSign\UAS\Options\Credential Bound User Only by setting to ‘0’
(By default, the value is ‘1’).

Note: This applies to both the users without credentials assigned to them and the users not added to VIP Authentication Service.
Sample ginaconfig.txt File

The following is an example of the ginaconfig.txt file:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\VeriSign\UAS\Client]
"Validation Server"="vipeg_server_ip_1:port:<camouflaged_password>,vipeg_server_ip_2:port:<camouflaged_password>"
[HKEY_LOCAL_MACHINE\SOFTWARE\VeriSign\UAS\Client]
"Time Out"="2"

Large Scale Deployment Using Microsoft Active Directory Group Policy

1. Follow steps 1-5 as described in the section "Manual Installation" on page 4.
2. Rename the ginaconfig.txt file to ginaconfig.reg.
3. Create MSI Transform (MST).

   Create an MSI Transform (MST) using installer tools such as InstallShield or Wise Installer Editor as explained below:

   **Note:** The screens provided in these procedures were captured from InstallShield 2011. Refer to the product documentation provided with your installer editor for specific screen captures and procedures.

   a. Start a new project using InstallShield.
   b. From the **All Types** tab, select the Transform template and provide your project name and location. Click OK.

   ![Figure 2-1 Selecting Transform Template](image)
installation and configuration
integration summary

c A wizard is displayed with a field for the Base MSI file name. Provide the path
C:\microsoft_gina_setup_folder\x86\VIP Enterprise Gateway GINA.msi (for 32 bit)
or C:\microsoft_gina_setup_folder\x86-64\VIP Enterprise Gateway GINA x86-64.msi (for 64 bit). Click Next.

d When the Additional Transforms screen displays, do not provide any Transform. Click Next.

e When the Create a Response Transform screen displays, do not select “Create response transform.” Click Finish.
From the Installation Designer tab, select Registry under System Configuration in the navigation pane. In the “Destination computer’s Registry view,” select HKEY_LOCAL_MACHINE.
Right-click on `HKEY_LOCAL_MACHINE`, and then click on Import REG File. From the Import Registry File screen, provide the path of the `ginaconfig.reg` file located in `<microsoft_gina_setup_folder>`. Click Next.
From the Import Conflict Options screen, select “Overwrite the registry data” and provide the log file path. Click **Import**.

After successful import, go to the **Client** folder in the “Destination computer’s Registry view” (HKEY_LOCAL_MACHINE\SOFTWARE\VeriSign\UAS\Client) and confirm that your Validation Server settings have been imported in this location.
4  Deploy Group Policy.

You can assign the C:\<microsoft_gina_setup_folder>\x86\VIP Enterprise Gateway GINA.msi (for 32 bit) or the C:\<microsoft_gina_setup_folder>\x86-64\VIP Enterprise Gateway GINA x86-64.msi (for 64 bit) package to the client machines. If the package is assigned, it will automatically be silently installed. In order to assign a package, follow these steps:

Note: Do not use the Browse button in the Open dialog to access the UNC location. Make sure that you type/paste the UNC path to the shared package whenever prompted within this process.

a  Click on the Start button, go to Programs, and then select Administrative Tools. Select Active Directory Users and Computers.
b  Right-click your domain name in the console tree, and select Properties.
c  Go to the Group Policy tab, select the object you want, and click Edit.
d  Expand Software Settings under User Configuration.
e  Right-click Software Installation, and select the New context menu. Click on Package.
f  In the Open dialog, type the full UNC path of the shared VIP Enterprise Gateway GINA.msi (for 32 bit) or VIP Enterprise Gateway GINA x86-64.msi (for 64 bit) package.
g  Click the Open button.
h  Click on Advanced, and then click OK.
i Go to Deployment tab, and select deployment type as Assigned. Click Install this application at logon.

j From the Modifications tab, click Add.

k In the Open dialog, type the full UNC path of the shared GINA Transform.mst file.

l Click OK (The VIP Enterprise Gateway GINA package will be added to the right pane of the "Group Policy" window).

m Close the Group Policy snap-in, click OK and exit the Active Directory Users and Computers snap-in.

n Run the following command to refresh Active Directory Group Policy settings:

```
C:\> gpupdate /force
```

5 When the client computers start, the VIP Enterprise Gateway GINA package will be installed automatically and restart the system after successful silent installation.

**Test an End User**

The end user will be guided through the following authentication sequence for online and offline modes, respectively.

**Client Authentication in Connected Mode (Online Mode)**

1 The user will see the normal Windows log on screen, and will need to provide his or her user name, password, and correct domain.

2 The user will be prompted for a security code.
Upon successful authentication, the user will be allowed to log on.

Client Authentication in Disconnected Mode (Offline Mode)
Symantec GINA does not support disconnected (offline) logon for credentials that do not have a USB Hybrid Token. Install GINA on a machine if the user either:

- Has a credential with a USB Hybrid Token and a valid device certificate.
- Only uses the machine in connected mode.

**Note:** Symantec GINA Plug-in does not support offline logon for 64-bit operating systems.

Prerequisites
- Client Authentication in Disconnected Mode (Offline Mode) is supported only with a USB Hybrid Token with a valid device certificate and Token Manager Client software (available with UA 4.x releases or contact customer support).
- Token Manager Client should be installed, and the token must be connected/used in the client system once before it is used in disconnected mode.
- Users must log on successfully at least once in connected mode before they can log on in disconnected mode.

1 The user will see the normal Windows log on screen as described in Step 1 of connected mode authentication.
2 The GINA plug-in will prompt the user to insert a USB hybrid token assigned to the user.
Upon successful retrieval of the valid device certificate from the USB Hybrid Token, the GINA plug-in may prompt the user to enter the Token PIN.

Upon successful authentication, the user will be allowed to log on.

Logging On Without GINA Plug-in

Local users and administrators can still access a workstation without logging on to a GINA-protected domain. However, the user has access only to the local or unprotected resources. This allows a user or administrator to log on to the local system to apply emergency patches related to the System/Symantec GINA plug-in module, if necessary.