SafeNet Authentication Service
Integration Guide

Protecting Microsoft Internet Security 2006 and Microsoft OWA 2007 with SAS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012646-001, Rev A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>Nov 2009</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
Contents

Introduction ................................................................................................................................. 4
  Third-Party Software Acknowledgement .............................................................................. 4
Overview ................................................................................................................................... 4
Applicability ............................................................................................................................... 5
Assumptions ................................................................................................................................. 5
Operation .................................................................................................................................... 5
Preparation and Prerequisites ................................................................................................. 5
Configuration .............................................................................................................................. 6
  Configuring ISA Server 2006 for Two-Factor Authentication ............................................... 6
Troubleshooting ....................................................................................................................... 19
  Logging .................................................................................................................................. 19
  Failed Logons ......................................................................................................................... 19
Support Contacts ...................................................................................................................... 20
Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft Internet Security 2006 and OWA 2007.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Overview

This documentation presents an overview and necessary steps to configure Internet Security and Acceleration (ISA) Server 2006. It is to be used in conjunction with Outlook Web Access (OWA) 2007 to view e-mail via web browser authenticating against SAS, using SafeNet tokens.

With SAS acting as the authentication server for an enabled resource, an authenticated connection sequence would be as follows:

2. The Username and Microsoft Password are sent to Active Directory for verification.
3. The Username and SafeNet Password are sent to SAS for verification.
4. User is presented to their Outlook Web Access 2007 email.
Applicability

<table>
<thead>
<tr>
<th>Security Partner Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Partner</td>
</tr>
<tr>
<td>Product Name and Version</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Unsupported authentication methods using ISA 2006 in RADIUS authentication mode</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Assumptions

- SAS has been installed and configured.
- A “Test” user account exists within SAS.

Operation

A RADIUS server is specified within the general server ISA 2006 configuration section. The VPN connections are then configured to send authentication requests to the SAS NPS/IAS RADIUS server. The SAS server then authenticates the provided credentials (User name and OTP), and either grants the user access or rejects the user access.

Preparation and Prerequisites

- SAS Agent for Microsoft Internet Authentication Service server (IAS) or Network Policy Server has been installed.
- The Microsoft ISA 2006 server must be a valid RADIUS client within the Microsoft Internet Authentication Service server (IAS) or Network Policy Server (NPS). This will allow RADIUS requests to be sent from Microsoft ISA 2006 to the RADIUS server.
Configuration

Configuring ISA Server 2006 for Two-Factor Authentication

1. On the ISA 2006 server, launch the ISA Server Management tool.

2. Select the **Firewall Policy (ISA)** section.

3. Enter a name for the new **Exchange Publishing** rule. Click **Next** to continue.
4. On the **Select Services** window, do the following:
   b. Select the **Outlook Web Access** option. Click **Next** to continue.

5. On the **Publishing Type** window, do the following
   a. Select **Publish a single Web site or load balancer**.
   b. Click **Next** to continue.
6. On the **Server Connection Server** window, do the following:
   a. Select **Use SSL to connect to the published Web server or server farm**.
   b. Click **Next** to continue.

7. On the **Internal Publishing Details** window, do the following:
   a. In the **Internal Site Name** section, enter the internal FQDN name of Exchange/OWA Server.
b. If ISA cannot resolve the FQDN name of the Exchange/OWA Server, select the option **Use a computer name or IP address to connect to the published server**, and then enter in the hostname or IP address of the Exchange/OWA Server.

c. In the **Public name** field, enter the URL that users externally can browse to for access to the OWA web page.

d. Click **Next** to continue.
8. A new Web Listener must be created. Click on the **New** button.
   
a. Enter in a name for the new Web Listener.

![New Web Listener Definition Wizard](image)

b. Click **Next** to continue.

c. On the **Client Connection Security** window, select **Require SSL secured connection with clients**. Click **Next** to continue.
d. Select a network the web listener will listen on.

   **Note:** For the purpose of testing, this documentation shows the internal interface has been chosen.

![New Web Listener Definition Wizard](image)

- **Listen for incoming Web requests on these networks:**
  - **External**: All IP addresses
  - **Internal**: All IP addresses
  - **Local Host**: All IP addresses
  - **Quarantined VPN Clients**: All IP addresses
  - **Others**: All IP addresses

- **Help about Web listener IP addresses**

![Select IP Addresses](image)

- **Select IP Addresses...**

9. The Web Listener now requires a valid certificate.
   a. Click **Select Certificate**.
   b. Click on a valid certificate in the list of available certificates, and then click **Select**.

![Select Certificate](image)
c. The new certificate is now displayed in the **Use a single certificate for this Web Listener** section. Click **Next** to continue.

d. Ensure that **HTML Form Authentication** is selected under **Select how clients will provide credentials to ISA Server**.
e. Select the option **Collect additional delegation credentials in the form.**

f. Select the **RADIUS OTP** option, and then click **Next.**

g. Clear the option **Enable SSO for Web sites published with this Web listener.** Click **Next** to continue.
10. An external RADIUS Server must now be added.
   a. Click the Add button.
   b. Enter the DNS or IP address of the RADIUS Server. This RADIUS Server will be the Microsoft NPS/IAS Server that has the SAS NPS IAS Agent installed.
   c. Adding a server description is optional but is helpful if there is more than one RADIUS Server configured.
   
   ![Add RADIUS Server](image)

   d. Click the Change button to set the shared secret.
   e. Click OK when finished.
   f. Click Next to continue, and then click Finish to complete the Web Listener Wizard.
11. The newly created Web Listener should automatically be selected after the Web Listener Wizard has been completed. The information entered in the Web Listener Wizard can be reviewed here. Click Next to continue.

12. On the Authentication Delegation window, under Select the method used by ISA Server to authenticate to the published Web server, select NTLM authentication. Click Next to continue.
13. A new User Set will need to be added to allow users to authenticate successfully via the ISA Published OWA page.
   a. Click the **Add** button. By default, the built-in User Set within ISA does not have any domain groups or users added.
   b. Create a new User Set and add the appropriate domain groups that will be allowed to authenticate via the **ISA Published OWA** page.
c. Once the User Set has been created, highlight it, and click **Add**. Close this window when finished.

d. The new user set has been added. Click **Next** to continue.

14. The Exchange Publishing Rule Wizard is now complete.

15. Before clicking **Finish**, it is recommended to click the **Test Rule** button to ensure the external web URL can connect to Exchange/OWA Server.
• If the test results succeed then the following will be displayed.

• If the test results fail, select the test that it failed on.

16. Browse to the external URL to access OWA webpage: https://External_URL_to_OWA/owa

17. Attempt to log in to the new web page. If authentication is successful, it will log into OWA, and display the authentication success in SAS.

If authentication is successful, it will log in to OWA and will display the authentication success in SAS.
## Troubleshooting

### Logging

By default, Microsoft ISA server 2006 has the ability to show live logging information from its reporting features. This should be used as a primary log source to determine authentication issues. Upon requiring more information, the SAS **Snapshot** tab should be used to determine authentication failure cause. The logging for the Microsoft Internet Authentication Service (IAS) or Network Policy Server (NPS) can be found in the Event Viewer. The SAS NPS/IAS agent logs can be found in the `\Program Files\CRYPTOCard\BlackShield ID\IAS Agent\Log` directory.

### Failed Logons

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Authentication request is rejected by Outlook Web Access.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indication</strong></td>
<td>11/19/20 User Authentication Failure 31221234 192.168.21.1 Invalid PIN 12:47:24 PM</td>
</tr>
<tr>
<td><strong>Possible Causes</strong></td>
<td>An incorrect server side PIN is being used.</td>
</tr>
<tr>
<td><strong>Solution</strong></td>
<td>Reset the server-side PIN within the SAS console.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Authentication request is rejected by Outlook Web Access.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Indication</strong></td>
<td>11/19/20 User Authentication Failure 31221234 192.168.21.1 Invalid authentication response 12:47:24 PM</td>
</tr>
<tr>
<td><strong>Possible Causes</strong></td>
<td>An invalid token code is being provided.</td>
</tr>
</tbody>
</table>
| **Solution** | • Verify the token code is being typed correctly.  
• Verify the token code is being typed with all correct CaSiNg applied to all characters.  
• The token could be out of sync. Resync the token from within the console manager. |
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>