SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Microsoft RRAS
All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto N.V. and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Part Number**: 007-013390-001, Rev. A

**Release Date**: January 2016
Contents

Third-Party Software Acknowledgement .................................................................................4
Description .................................................................................................................................4
Applicability ...............................................................................................................................4
Environment .................................................................................................................................5
Audience .....................................................................................................................................5
RADIUS-based Authentication using SAS Cloud .......................................................................5
RADIUS-based Authentication using SAS-SPE and SAS-PCE ..................................................6
RADIUS Authentication Flow using SAS ....................................................................................6
Radius Authentication Flow using NPS Server with SAS ............................................................7
RADIUS Prerequisites ................................................................................................................7
Configuring SafeNet Authentication Service ............................................................................7
  Creating Users Stores in SAS .....................................................................................................8
  Assigning an Authenticator in SAS ...........................................................................................8
  Adding Microsoft RRAS as an Authentication Node in SAS ....................................................9
  Checking the SAS RADIUS Address ......................................................................................11
Configuring the Network Policy Server ....................................................................................12
  Configuring Connection Policies ..............................................................................................18
Enabling Microsoft RRAS .........................................................................................................25
Configuring Microsoft RRAS .....................................................................................................31
Creating a VPN Client ...............................................................................................................33
Configuring the VPN Client .......................................................................................................36
Running the Solution ..................................................................................................................39
Support Contacts .......................................................................................................................41
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Microsoft RRAS.

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.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

Microsoft Routing and Remote Access service (RRAS) supports IPv4 and IPv6 network routing, and remote user or site-to-site connectivity by using virtual private network (VPN) or dial-up connections.

The remote access feature provides VPN services so that users can access corporate networks securely over the Internet as if they were directly connected. Remote access also enables remote or mobile workers who use dial-up communication links to access corporate networks.

RRAS is a software router and an open platform for routing and networking. Its routing services can be used by organizations in local area network (LAN) and wide area network (WAN) environments or over the Internet by using secure VPN connections. Routing is used for multiprotocol LAN-to-LAN, LAN-to-WAN, VPN, and network address translation (NAT) routing services.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Microsoft RRAS using SafeNet one-time password (OTP) authenticators managed by SafeNet Authentication Service.
- Configure Microsoft RRAS to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Microsoft RRAS environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Microsoft RRAS can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A server version that is used to deploy the solution on-premises in the organization
Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service (SAS)**—SafeNet’s cloud-based authentication service
- **Microsoft RRAS**—Version 5.2.0000.0 (Windows 2008 R2 Enterprise Edition Service Pack 1)

Audience

This document is targeted to system administrators who are familiar with Microsoft RRAS, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service**—A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

  ![SAS Cloud Diagram](image)

- **Local RADIUS hosted on-premises**—A RADIUS agent that is implemented in the existing customer's RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

  ![Local RADIUS Diagram](image)

This document demonstrates the solution using the SAS cloud hosted RADIUS service.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to:

For more details on how to install and configure FreeRADIUS, refer to the SafeNet Authentication Service FreeRADIUS Agent Configuration Guide.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS)** or the legacy **Microsoft Internet Authentication Service (MS-IAS)**—SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
  
  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:  

- **FreeRADIUS**—The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.
  
  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the data flow of a multi-factor authentication transaction for Microsoft RRAS.

1. A user enters login credentials on the Microsoft VPN client to log on to Microsoft RRAS using an OTP authenticator.
2. The Microsoft VPN client sends an authentication request to the Windows VPN server running Microsoft RRAS.
3. Microsoft RRAS sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
4. The SAS authentication reply is sent back to Microsoft RRAS.
5. The user is granted or denied access to Microsoft RRAS based on the OTP value calculation results from SAS.
Radius Authentication Flow using NPS Server with SAS

The image below describes the dataflow of a multi-factor authentication transaction for Microsoft RRAS using the NPS server.

1. A user enters login credentials on the Microsoft VPN client to log on to Microsoft RRAS using an OTP authenticator.
2. The Microsoft VPN client sends an authentication request to the Windows VPN server running Microsoft RRAS.
3. Microsoft RRAS sends a RADIUS request with the user’s credentials to the NPS server.
4. The NPS server sends an authentication request to SafeNet Authentication Service for validation.
5. SAS authentication reply is sent back to the NPS server.
6. The NPS server in turn sends the reply back to Microsoft RRAS.
7. The user is granted or denied access to Microsoft RRAS based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Microsoft RRAS, ensure the following:

- End users can authenticate from the Microsoft RRAS environment with a static password before configuring the Microsoft RRAS to use RADIUS authentication.
- Ports 1812/1813 are open to and from Microsoft RRAS.
- A shared secret key has been selected. A shared secret key provides an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Microsoft RRAS using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 8
- Assigning an Authenticator in SAS, page 8
- Adding Microsoft RRAS as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Address, page 11
Creating Users Stores in SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time, using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent

For additional details on importing users to SafeNet Authentication Service, refer to “Creating Users” in the *SafeNet Authentication Service Subscriber Account Operator Guide*:


All SafeNet Authentication Service documentation can be found on the *Gemalto Knowledge Base* site.

Assigning an Authenticator in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through Microsoft RRAS.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SafeNet Gold
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning**—Assign an authenticator to users one at a time.
- **Provisioning rules**—The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change. An authenticator will be assigned automatically to the user.

Refer to “Provisioning Rules” in the *SafeNet Authentication Service Subscriber Account Operator Guide* to learn how to provision the different authentication methods to the users in the SAS user store.

Adding Microsoft RRAS as an Authentication Node in SAS

Add a RADIUS entry in the SAS Auth Nodes module to prepare it to receive RADIUS authentication requests from Microsoft RRAS. You will need the IP address of Microsoft RRAS and the shared secret to be used by both SAS and Microsoft RRAS.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.

3. In the Auth Nodes module, click the Auth Nodes link.
4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Node** section, complete the following fields, and then click **Save**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Description</td>
<td>Enter a host description.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enter the name of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Low IP Address In Range</td>
<td>Enter the IP address of the host that will authenticate with SAS.</td>
</tr>
<tr>
<td>Configure FreeRADIUS Synchronization</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Shared Secret</td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

![Add Auth Node dialog](image)

The authentication node is added to the system.
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Microsoft RRAS, check its IP address. The IP address will then be added to Microsoft RRAS as a RADIUS server at a later stage.

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select Auth Nodes.
3. In the **Auth Nodes** module, click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

![Auth Nodes screenshot](image)

### Configuring the Network Policy Server

Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for connection request authentication and connection request authorization.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. On the **Network Policy Server** window, in the left pane, expand **Radius Clients and Servers**, right-click **Radius Clients**, and then select **New**.

![Network Policy Server screenshot](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Enable this RADIUS client</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly Name</strong></td>
<td>Enter a name for the RADIUS client (for example, RRAS IP).</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the IP address of the Microsoft RRAS server.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret for the RADIUS client.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the **Network Policy Server** window, in the left pane, under **RADIUS Clients and Servers**, right-click **Remote RADIUS Server Groups**, and then select **New**.

![Network Policy Server Window](image1.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

5. On the **New Remote RADIUS Server Group** window, in the **Group name** field, enter a name for the RADIUS server group (for example, **Radius Server group**), and then click **Add**.

![New Remote RADIUS Server Group Window](image2.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
6. On the **Add RADIUS Server** window, in the **Server** field, enter the IP address of the RADIUS server, and then click **Verify**.

![Add RADIUS Server window](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
7. On the **Verify Address** window, click **Resolve**.

   ![Verify Address window]

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

8. The IP address is resolved and displayed in the **IP address** box. Click **OK**.

   ![Verify Address window]

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

9. On the **Add RADIUS Server** window, click the **Authentication/Accounting** tab.
10. Complete the following fields and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td><strong>Confirm Shared Secret</strong></td>
<td>Re-enter the shared secret key.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
11. On the **New Remote RADIUS Server Group** window, click **OK**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

### Configuring Connection Policies

Connection request policies are configured to designate RADIUS servers to be used for RADIUS accounting. It allows network administrators to designate RADIUS servers that perform the authentication and authorization of connection requests, so that the NPS server can communicate with RADIUS clients.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. On the **Network Policy Server** window, in the left pane, click **Policies > Connection Request Policies**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. In the right pane, in the **Policy Name** column, right-click **Use Windows authentication for all users**, and then select **Properties**.

![Policy Name](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. On the **Use Windows authentication for all users Properties** window, on the **Overview** tab, under **Policy State**, select **Policy enabled**.

![Policy State](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. Click the **Settings** tab. Then, in the left pane, under **Forwarding Connection Request**, select **Authentication**.

![Settings tab with Authentication selected](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

6. In the right pane, select **Forward requests to the following remote RADIUS server group for authentication**, select the RADIUS server group (for example, **Radius Server group**) that you created earlier in step 5 of “Configuring the Network Policy Server” on page 12, and then click **OK**.

![Settings tab with Radius Server group selected](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
7. On the **Network Policy Server** window, in the left pane, click **Policies > Network Policies**.

8. In the right page, in the **Policy Name** column, right click **Connections to Microsoft Routing and Remote Access server**, and then select **Properties**.
9. On the **Connections to Microsoft Routing and Remote Access server Properties** window, on the **Overview** tab, under **Access Permission**, select **Grant access**. Grant access if the connection request matches this policy.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

10. Click the **Constraints** tab. In the right pane, under **Less secure authentication methods**, ensure that **Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)** is selected, and then click **OK**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
11. On the **Network Policy Server** window, in the right pane, in the **Policy Name** column, right-click **Connections to other access servers**, and then select **Properties**.

![Network Policy Server](image1.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

12. On the **Connections to other access servers Properties** window, on the **Overview** tab, under **Access Permission**, select **Grant access**. **Grant access if the connection request matches this policy**.

![Connections to other access servers Properties](image2.png)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
13. Click the **Constraints** tab. In the right pane, under **Less secure authentication methods**, ensure that Microsoft Encrypted Authentication version 2 (MS-CHAP-v2) is selected, and then click **OK**.

14. Click **Start > Administrative Tools > Services**.

15. On the **Services** window, in the right pane, in the **Name** column, select **Network Policy Server**, and then click **Restart**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Enabling Microsoft RRAS

Enable Microsoft RRAS to configure it to provide virtual private network (VPN) services.

1. Click **Start > Administrative Tools > Routing and Remote Access**.

2. On the **Routing and Remote Access** window, in the left pane, under **Server Status**, right-click the hostname of the Windows VPN server (for example, **WIN-C4LH2418737 (local)**), and then select **Configure and Enable Routing and Remote Access**.

3. On the **Routing and Remote Access Server Setup Wizard** window, click **Next**.
4. Under **Configuration**, select **Virtual private network (VPN) access and NAT**, and then click **Next**.

5. Under **VPN Connection**, select the network interface that connects the Microsoft RRAS server to the Internet, and then click **Next**.
6. Under **IP Address Assignment**, select **From a specified range of addresses**, and then click **Next**.

7. Under **Address Range Assignment**, click **New**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. On the **New IPv4 Address Range** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start IP address</td>
<td>Enter the first address of the IP address range.</td>
</tr>
<tr>
<td>End IP address</td>
<td>Enter the last address of the IP address range.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

9. On the **Routing and Remote Access Server Setup Wizard** window, under **Address Range Assignment**, the newly assigned IP address range is listed. Click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
10. Under **Managing Multiple Remote Access Servers**, select **Yes, set up this server to work with a RADIUS server**, and then click **Next**.

![Routing and Remote Access Server Setup Wizard](image.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

11. Under **RADIUS Server Selection**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th><strong>Primary RADIUS server</strong></th>
<th>Enter the IP address of the primary RADIUS server or NPS server as per your configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret same as entered in step 5 of &quot;Adding Microsoft RRAS as an Authentication Node in SAS&quot;, on page 9.</td>
</tr>
</tbody>
</table>

![Routing and Remote Access Server Setup Wizard](image.png)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
12. Click **Finish**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

13. A message is displayed. Click **OK**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

On the **Routing and Remote Access** window, in the left pane, the icon of the hostname of the Windows VPN server (for example, **WIN-C4LH2418737 (local)**) turns green when the Routing and Remote Access service is initialized and started.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
Configuring Microsoft RRAS

1. Click **Start > Administrative Tools > Routing and Remote Access.**

2. On the **Routing and Remote Access** window, in the left pane, right-click the hostname of your Windows VPN server (for example, **WIN-C4LH2418737 (local)**), and then select **Properties.**

3. On the **WIN-C4LH2418737 (local) Properties** window, click the **Security** tab, and then click **Authentication Methods.**

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
4. On the **Authentication Methods** window, clear **Extensible authentication protocol (EAP)**, and then click **OK**.

![Authentication Methods window](image)

*The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.*

5. On the **WIN-C4LH2418737 (local) Properties** window, complete the following fields, and then click **OK**.

| Allow custom IPsec policy for L2TP connection | Select this option. |
| Preshared Key | Enter a preshared key to be used by the VPN connections. |

![WIN-C4LH2418737 (local) Properties window](image)

*The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.*
6. A message is displayed. Click Yes.

![Routing and Remote Access]

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

## Creating a VPN Client

Create a VPN client on a Windows workstation.

1. Click **Start > Control Panel > Network and Internet > Network and Sharing Center**.
2. Under **Network and Sharing Center** main window, in the right pane, click **Set up a new connection or network**.

![Network and Sharing Center]

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
3. On the **Setup up a Connection or Network** window, select **Connect to a workplace**, and then click **Next**.

4. On the **Connect to a Workplace** window, click **Use my Internet connection (VPN)**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. Under **Type the Internet address to connect to**, complete the following fields, and then click **Next**.

<table>
<thead>
<tr>
<th>Internet address</th>
<th>Enter the IP address of the Microsoft RRAS server.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Don’t connect now; just set it up so I can connect later</strong></td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

6. Under **Type your username and password**, click **Create**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
7. The VPN connection is ready to use. Click **Close**.

![Screen image of VPN connection ready](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

**Configuring the VPN Client**

Configure the VPN client created on the Windows workstation.

1. Click **Start > Control Panel > Network and Internet**.
2. Under **Network and Internet**, in the right pane, under **Network and Sharing Center**, click **Connect to a network**.

![Screen image of Network and Sharing Center](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
3. On the bottom right-hand corner, a list of network connection is displayed. Right-click **VPN Connection**, and then select **Properties**.

![VPN Connection Properties](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. On the **VPN Connection Properties** window, click the **Security** tab, and then perform the following steps:
   a. In the **Type of VPN** field, select **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**, and then click **Advanced settings**.

![VPN Connection Properties](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
b. On the **Advanced Properties** window, select **Use preshared key for authentication**. In the **Key** field, enter the preshared key same as entered in step 5 of “Configuring Microsoft RRAS” on page 31, and then click **OK**.

![Advanced Properties window](image)

(\textit{The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.})

c. In the **Data encryption** field, select **Optional encryption (connect even if no encryption)**.

d. Under **Authentication**, select **Allow these protocols**, and then select **Microsoft CHAP Version 2 (MS-CHAP v2)**.

e. Click **OK**.

![VPN Connection Properties](image)

(\textit{The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.})
Running the Solution

For this integration, SafeNet eToken PASS is configured for authentication with the SAS solution.

1. On the Windows workstation, on the bottom right-hand corner, click the icon.
2. A list of network connections is displayed. Under **VPN Connection**, click **Connect**.

![Current network connection](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

3. On the **Connect VPN Connection** window, complete the following fields, and then click **Connect**.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Enter your user name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Generate an OTP using the SafeNet eToken PASS token and then enter that OTP in this field.</td>
</tr>
</tbody>
</table>

![Connect VPN Connection](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
If the authentication is successful, the VPN connection is established, and the VPN connection status is changed to **Connected**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone 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>Gemalto, 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>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>