SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Juniper Web Portal
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.

© 2015 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:** 007-013039-001, Rev. B

**Release Date:** November 2015
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 Prerequisites ............................................................................................ 7
Configuring SafeNet Authentication Service ......................................................... 7
  Creating Users Stores in SAS .................................................................................. 7
  Assigning an Authenticator in SAS ...................................................................... 8
  Adding Juniper Web Portal as an Authentication Node in SAS ......................... 9
  Checking the SAS RADIUS Address .................................................................. 11
Configuring the Juniper Web Portal ..................................................................... 12
  Adding a RADIUS Authentication Server .......................................................... 12
  Attaching an Authentication Server to the User Realm ..................................... 14
Configuring Kerberos Constrained Delegation (KCD) .......................................... 16
  Defining the Delegated Authentication Services .............................................. 17
  Configuring Juniper SA for KCD ..................................................................... 20
Configuring the Exchange Server ...................................................................... 27
  Configuring the SSO Profile .............................................................................. 27
Running the Solution - OTP .................................................................................. 31
Configuring GrIDsure Support .......................................................................... 32
  Modifying the Sample.zip File ......................................................................... 32
  Configuring the SSO Profile ............................................................................. 32
  Assigning the GrIDsure Sign-in Pages to the User Realm ............................... 34
Running the Solution - GrIDsure ......................................................................... 36
Support Contacts .................................................................................................... 38
Third-Party Software Acknowledgement

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

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.

The Juniper Networks SSL VPN appliances meet the needs of companies of all sizes. The Junos Pulse Gateway MAG series appliances use SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for pre-installed client software, changes to internal servers, and costly ongoing maintenance and desktop support. The SA Series also offers sophisticated partner/customer extranet features that enable controlled access to differentiated users and groups without requiring infrastructure changes, demilitarized zone (DMZ) deployments, or software agents.

This document describes how to:

- Configure Juniper Web Portal to work with SafeNet Authentication Service in RADIUS mode.

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

Juniper Web Portal 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 – Private Cloud Edition (SAS-PCE)**—only when using this version. For Cloud not necessary to fill in version number.
- **Juniper MAG2600 Junos Pulse Gateway** – Version 7.2R2

Audience

This document is targeted to system administrators who are familiar with Juniper Web Portal, 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.

- **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.

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:
http://www2.gemalto.com/cryptocard/implementation-guides/Microsoft/Blackshield Agent Implementation Guide for Microsoft IAS, NPS.pdf

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 Juniper Web Portal.

1. A user attempts to log on to Juniper Web Portal using an OTP authenticator.
2. Juniper Web Portal sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to the Juniper Web Portal.
4. The user is granted or denied access to the Juniper Web Portal based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Juniper Web Portal, ensure the following:

- End users can authenticate from the Juniper Web Portal environment with a static password before configuring the Juniper Web Portal to use RADIUS authentication.
- Ports 1812/1813 are open to and from Juniper Web Portal.
- 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 Juniper Web Portal using RADIUS protocol requires the following:

- Creating Users Stores in SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Juniper Web Portal as an Authentication Node in SAS, page 8
- 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 SafeNet 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 Juniper Web Portal.

The following authenticators are supported:

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

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 Juniper Web Portal 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 Juniper Web Portal. You will need the IP address of Juniper Web Portal and the shared secret to be used by both SAS and Juniper Web Portal.

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.

![Auth Nodes module](image)

4. Under **Auth Nodes**, click **Add**.

5. In the **Add Auth Nodes** 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 or the lowest IP address in a range of addresses that will authenticate with SAS.</td>
</tr>
<tr>
<td>High IP Address In Range</td>
<td>Enter the highest IP address in a range of IP addresses 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>
The authentication node is added to the system.

Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Juniper Web Portal, check its IP address. The IP address will then be added to Juniper Web Portal 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.
Configuring the Juniper Web Portal

Configuring the Juniper Web Portal requires the following:

- Adding a RADIUS Authentication Server, page 12
- Attaching an Authentication Server to the User Realm, page 14

Adding a RADIUS Authentication Server

The authentication server that you create in this section will be configured with RADIUS support.

1. Log in to the Juniper administrator console.
2. Click Authentication, and then click Auth. Servers. The Authentication Servers window is displayed.

3. In the New menu, select Radius Server, and then click New Server.
4. Complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this server.</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>Enter a name for the device.</td>
</tr>
<tr>
<td>Radius Server</td>
<td>Enter the SAS RADIUS IP address.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the RADIUS authentication port number.</td>
</tr>
<tr>
<td></td>
<td>The default is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret configured for RADIUS.</td>
</tr>
</tbody>
</table>

Do not change any default values.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
Attaching an Authentication Server to the User Realm

To use SAS RADIUS authentication, attach the authentication server that you created in the previous section to the user realm.

1. Log in to the Juniper administrator console.
2. Click **User**, and then click **User Realms**.

![User Authentication Realms](image)

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

3. Under **Authentication Realms**, click **Users**.
4. Click the **General** tab.

---

SafeNet Authentication Service: Integration Guide
Using RADIUS Protocol for Juniper Web Portal
Document PN: 007-013039-001, Rev. B, Copyright © 2015 Gemalto, Inc., All rights reserved.
5. Complete the following fields under the **Servers** section, and then click **Save Changes**:

<table>
<thead>
<tr>
<th><strong>Authentication</strong></th>
<th>Select the authentication server that was created.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directory/Attribute</strong></td>
<td>Select <strong>Same as above</strong>.</td>
</tr>
</tbody>
</table>

Do not change any other default values.

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

6. Click the **Role Mapping** tab.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
7. Click **New Rule**, complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th>Rule based on</th>
<th>Select <strong>Username</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>Rule: If username...</strong></td>
<td>Select a user or a list of users who are allowed to authenticate to the realm.</td>
</tr>
<tr>
<td><strong>...then assign these roles</strong></td>
<td>Select the role to assign to these users from the <strong>Available Roles</strong> list, and then click <strong>Add</strong> to move it to the <strong>Selected Roles</strong> list.</td>
</tr>
</tbody>
</table>

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

**Configuring Kerberos Constrained Delegation (KCD)**

Juniper SA is often used to protect web application resources, such as Outlook Web Access (OWA) and SharePoint, which are based on Windows authentication. KCD enables single sign-on (SSO) for the application resource, so that users are only required to log on once per session—the user logs on to SA, and then is not required to authenticate again when accessing Microsoft applications. This section describes the steps used to authenticate a user to a web application.

Setting up KCD with SA requires the following:

- Defining the Delegated Authentication Services, page 17
- Configuring Juniper SA for KCD, page 20
Defining the Delegated Authentication Services

KCD requires an Active Directory user account that has protocol transition and delegation rights. This user account has rights to request a Kerberos ticket on behalf of a user signing in to SA. This section describes how to define the OWA delegated authentication services for a user (in this example, the user is Bob). First, you will need to configure the user account for web application access, and then define the Delegated Authentication Services for the user.

1. Use the `setspn` command to enable the Delegation tab in the new user account’s Properties window in Active Directory Users and Computers. From the command line, type:

   ```bash
   setspn -A HTTP/<user_account> <domain>/<user_account>
   ```

   where:
   - `<user_account>` is the User Logon Name of the user that will authenticate using KCD
   - `<domain>` is your domain

2. Define the Delegated Authentication Services for the user.
   a. From the Windows Start menu, navigate to and open Active Directory Users and Computers.
   b. Click Users, and then right-click on the defined user. The user’s Properties window is displayed.

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

![Delegation tab](image)

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

d. Select the following options to enable the user to be trusted for delegation to all authentication protocols.

- **Trust this user for delegation to specified services only**
- **Use any authentication protocol**

e. Click **Add**. The **Add Services** window is displayed.

![Add Services window](image)

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
f. Click **Users or Computers**. The **Select Users or Computers** window is displayed.

g. Enter the name of the protected service’s server in the domain that the user will be trusted to delegate for, and then click **OK**. (In this example, the OWA service is the protected service’s server, and it is hosted on the same server as the Active Directory Domain Controller.)

![Select Users or Computers window](image1)

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

The **Add Services** window is displayed again.

h. Select the appropriate **Service Type**, and then click **OK**.

![Add Services window](image2)

*(The screen image above is from Microsoft®, Trademarks are the property of their respective owners.)*
i. Click **Apply**, and then click **OK**. Active Directory is now configured for KCD.

![Bob Properties](image)

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

### Configuring Juniper SA for KCD

Configuring the Juniper SA with Constrained Delegation for users who are connecting to an application via the Juniper Web Portal involves the following steps:

- Configuring the Web SSO, page 21
- Configuring the Constrained Delegation Service List, page 22
- Configuring the SSO Policies, page 24
- Configuring the SSO Profile, page 25

In this example, users will connect to the OWA application.
Configuring the Web SSO

In this procedure, you will add the Kerberos realm to the Juniper SA’s Kerberos SSO settings.

1. In the SA Administrator console, select Users > Resource Policies > SSO > General. The WebPolicySSOGeneric window is displayed.

2. Click Kerberos SSO Settings to view additional settings.

3. Click Enable Kerberos SSO.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
4. Under **Realm Definition**, add the Kerberos realm as follows, then click **Add**:

<table>
<thead>
<tr>
<th>Realm</th>
<th>Enter the DNS domain name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern List</td>
<td>Enter the DNS domain name.</td>
</tr>
<tr>
<td>KDC</td>
<td>Enter the FQDN of the Active Directory server.</td>
</tr>
</tbody>
</table>

5. Click **Save Changes**.

### Configuring the Constrained Delegation Service List

In this procedure, you will create a text file, and then upload it to create a constrained delegation service list.

6. Open Notepad or any other text editor.
7. Create a file containing the DC server name.

8. Save the file.
10. Click **Kerberos SSO Settings** to view additional settings.

11. Under **Constrained Delegation**, click **Edit**. The constrained delegation service list window opens.

12. Click **New Service List**. A new line will be added to the window:

   ![Constrained Delegation Service Lists](Image)

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

13. In the **Name** field enter a name for the new entry.

14. Click **Choose File**, and then select the text file that was created in step 2.

15. An upload window is displayed. When the upload is complete, click **Close**.

16. Under **Constrained Delegation**, complete the following fields, and then click **Add**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Label</strong></td>
<td>Enter a name for the rule.</td>
</tr>
<tr>
<td><strong>Realm</strong></td>
<td>Select the Kerberos realm defined in the previous step.</td>
</tr>
<tr>
<td><strong>Principal Account</strong></td>
<td>Enter the user logon name that was configured for KCD in “Defining the Delegated Authentication Services” on page 17.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Enter the user’s domain password.</td>
</tr>
<tr>
<td><strong>Service List</strong></td>
<td>Select the service list name.</td>
</tr>
</tbody>
</table>

   ![Constrained Delegation](Image)

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

17. Click **Save Changes**.
Configuring the SSO Policies

In this procedure, you will define the roles and resources for which constrained delegation will be performed.


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

2. Click New Policy. The New Policy window is displayed.

3. Complete the following fields, and then click Save Changes:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a policy name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resources</td>
<td>Enter the exact FQDN.</td>
</tr>
<tr>
<td>Roles</td>
<td></td>
</tr>
<tr>
<td>Action</td>
<td>Select Constrained Delegation.</td>
</tr>
<tr>
<td>Credential</td>
<td>Select the credentials defined in &quot;Configuring the Constrained Delegation Service List&quot; on page 22.</td>
</tr>
</tbody>
</table>
Configuring the SSO Profile

1. In the SA Administrator console, select Users > Resource Policies > Web.

2. Click New Profile. The New Profile window is displayed.
3. Complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th>Type</th>
<th>Select Microsoft OWA 2010. The OWA configuration window will expand.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the policy name.</td>
</tr>
<tr>
<td>Base URL</td>
<td>Enter the OWA URL.</td>
</tr>
</tbody>
</table>

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

4. Select **Autopolicy: Web Compression**. Verify that it contains the OWA URL, and that the assigned **Action** is **Compress**.

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

5. Select **Autopolicy: Single Sign-on**.
6. Complete the following fields, and then click **Save Changes**:

<table>
<thead>
<tr>
<th><strong>Constrained Delegation</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Resource</strong></td>
<td>Enter the web server (OWA) FQDN.</td>
</tr>
<tr>
<td><strong>Credential</strong></td>
<td>Select the constrained delegation label defined in “Configuring the Constrained Delegation Service List” on page 22.</td>
</tr>
</tbody>
</table>

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

### Configuring the Exchange Server

In the following section, you will configure the OWA for KCD authentication.

#### Configuring the SSO Profile

To configure OWA and Exchange Control Panel (ECP):

1. Open the Microsoft Exchange Management Console.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)
2. In the left pane, select **Server Configuration > Client Access**.

3. In the center pane under **Client Access**, select your exchange server.

4. In the center pane under the selected server section, click the **Outlook Web App** tab.

5. Right-click **owa (Default Web Site)**, and then select **Properties**. The **owa (Default Web Site) Properties** window is displayed.
6. Click the **Authentication** tab.

   ![Authentication tab screenshot]

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

7. Complete the following, and then click **OK**:

   | Use one or more standard authentication methods | Select this option. |
   | Integrated Windows authentication | Select this option. |

8. In the center pane under the selected server section, click the **Exchange Control Panel** tab.

   ![Exchange Control Panel screenshot]

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

9. Right-click on **ecp (Default Web Site)**, and then select **Properties**. The **ecp (Default Web Site) Properties** window is displayed.

10. Click the **Authentication** tab.
11. Complete the following, and then click **OK:**

<table>
<thead>
<tr>
<th>Use one or more standard authentication methods</th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrated Windows authentication</td>
<td>Select this option.</td>
</tr>
</tbody>
</table>

![ECP Properties](image)

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

12. Restart the IIS service—open a terminal, and then enter the command `iisreset`. 
Running the Solution - OTP

Verify the integration solution after you have successfully configured the Juniper Web Portal for SAS authentication. The following example illustrates authenticating to the Juniper SA Web Portal using SAS RADIUS, and KCD authentication to SSO to Outlook Web Access.

13. Browse to the Juniper Web Portal and log in with your username and OTP. After successful authentication, you will be logged in to the Juniper Web Portal.

14. Click the OWA KCD bookmarked link to authenticate using KCD SSO to Outlook Web Access.

After successful authentication, you will be logged in to Outlook Web Access.
Configuring GrIDsure Support

Configuring GrIDsure support requires the following:

- Modifying the Sample.zip File, page 32
- Configuring the SSO Profile, page 32
- Assigning the GrIDsure Sign-in Pages to the User Realm, page 34

Modifying the Sample.zip File

1. Download the sample.zip file that contains the supported files from the following location (DOW3564 in Inquira): http://bel1web002:9876/Files/b638c2d558c54af7a0bbd0cd041bace7
2. Extract the sample.zip file.
3. Open Notepad or any other text editor, and edit the gridsure.js file as follows:
   a. Search for the string, `<URL of the BlackShield ID Self Service page>.
   b. Replace the string with the SafeNet SAS self-service URL + ?getChallengedImage=true&userName=.
      For example:
4. Save the changes to the gridsure.js file.

Configuring the SSO Profile

To support GrIDsure authentication, the following Juniper login pages must be updated:

- loginPage.html—default login page
- loginPage-ipad.thtml—iPad login page
- loginPage-mobile-webkit.thtml—default mobile login page
- gridsure.js—contains several js functions that support the GrID authentication

These files can be found in the sample.zip file that was downloaded in the previous section.
1. Log in to the Juniper administrator console.
2. Select Authentication > Signing In.
3. Click the **Sign-in Pages** tab.

4. Click **Upload Custom Pages**.

5. In the far-right pane, under **Sample Templates Files**, click **Sample**. The file sample.zip will be downloaded.

6. Extract the sample.zip file and copy the following files into the extracted folder (replace the existing files):
   - `loginPage.html`
   - `loginPage-ipad.html`
7. Compress the files in the folders to a zip file.
8. On the **Upload Custom Sign-In Pages** window, under **Sign-in Pages**, complete the following:

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the sign-in method.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Template Files</strong></td>
<td></td>
</tr>
<tr>
<td>• Select <strong>Choose file</strong>.</td>
<td></td>
</tr>
<tr>
<td>• Select the new zip file you created, and then click <strong>Upload Custom Pages</strong>.</td>
<td></td>
</tr>
</tbody>
</table>

**Assigning the GrIDsure Sign-in Pages to the User Realm**

1. Log in to the Juniper administrator console.
2. Select **Authentication > Signing In**.

3. Select a specific **User URL** or click **New URL**.

---

*(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)*
4. In the Sign-in page menu, select the login policy name that you created in step 8 in “Configuring the SSO Profile” on page 34, and then click Save Changes.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
Running the Solution - GrIDsure

Verify the integration solution after you have successfully configured the Juniper Web Portal for SAS authentication with GrIDsure. The following example illustrates authenticating with GrIDsure token to the Juniper SA Web Portal using SAS RADIUS, and KCD authentication to SSO to Outlook Web Access.

1. Browse to the Juniper Web Portal.

   ![Juniper Web Portal](image1)

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

2. Enter your username, and then click **GetGrID**. The challenge grid is displayed.

   ![Challenge Grid](image2)

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

3. In the **Password** field, enter the characters from the grid that correspond to your PIP (personal identification pattern), and then click **Sign In**.

   ![Password Entry](image3)
4. After successful authentication, you will be logged in to the Juniper Web Portal. Click the OWA **KCD** link.

![Image of Juniper Web Portal]

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

You are now authenticated using KCD SSO and logged into OWA.

![Image of Microsoft Outlook Web App]

*(The screen image above is from Microsoft®. 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>Address</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>Phone</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>Technical Support</td>
<td></td>
</tr>
<tr>
<td>Customer Portal</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 Gemalto Knowledge Base.</td>
</tr>
</tbody>
</table>