SafeNet Authentication Service
Integration Guide

Juniper SA Configuration for SAML Authentication with SAS
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012619-001, Rev A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>April 2013</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
  - About This Guide ................................................................................................................ 4
  - Intended Audience ............................................................................................................. 4
  - Additional Information ...................................................................................................... 4
- **Software Requirements** .................................................................................................. 4
- **Overview** ......................................................................................................................... 5
  - Security Assertion Markup Language ............................................................................... 5
  - SAML Authentication Flow ............................................................................................... 6
- **Pre-Configuration** ............................................................................................................ 6
  - Preparing the SA Entity Id ................................................................................................. 6
- **SA Configuration as a Service Provider** ........................................................................ 7
  - Viewing SAS’s SAML Settings .......................................................................................... 7
  - Creating an Authentication Server .................................................................................... 8
  - Setting the User Authentication Realm ............................................................................ 9
- **SAML Authentication Configuration in SAS** ................................................................ 10
  - Configuring the SAML Service Provider ......................................................................... 10
  - Configuring SAML Services .............................................................................................. 12
  - Manually Enabling User Authentication ......................................................................... 12
  - Using SAML Provisioning Rules to Enable User Authentication .................................... 14
- **KCD Configuration** ......................................................................................................... 15
  - Configuring the User Account .......................................................................................... 16
  - Defining the Delegated Authentication Services ............................................................. 17
  - Configuring the Exchange Server ..................................................................................... 20
  - Configuring SA .................................................................................................................. 22
  - Configuring Web SSO ....................................................................................................... 22
  - Configuring the Constrained Delegation Service List ..................................................... 23
  - Configuring SSO Policies .................................................................................................. 26
- **Running the Solution** ..................................................................................................... 28
  - User Authentication Scenario .......................................................................................... 28
- **Troubleshooting** ............................................................................................................. 30
- **Support Contacts** ........................................................................................................... 30
Introduction

Third-Party Software Acknowledgement

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

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.

About This Guide

The goal of this document is to provide guidance for setting up and managing the SafeNet Authentication Service (SAS) authentication solution in a Juniper Networks’ Junos Pulse Secure Access Service (SA) environment based on SAML 2.0.

The information in this guide includes the following:
- Solution requirement outline, and deployment scenarios for SafeNet’s authentication solution
- Step-by-step instructions for implementing Juniper Networks’ Junos Pulse Secure Access Service in a SAML solution

Intended Audience

The guide is intended for Information Technology professionals responsible for the organization’s network security.

Additional Information

For a detailed explanation of SafeNet Authentication Service (SAS) 3.2 and the other infrastructure components involved in the solution, or any other SafeNet products mentioned in this guide, refer to SafeNet’s product documentation.

For additional information on Microsoft or Juniper Networks software and hardware components mentioned in this guide, refer to the relevant manufacturers’ documentation.

Software Requirements

For this scenario, the working environment must include the following software:
- Juniper Networks Junos Pulse Secure Access Service Version 7.1 R5 or later
- Microsoft Active Directory
- SafeNet Authentication Service (SAS) 3.2 or later
Overview

Security Assertion Markup Language

Security Assertion Markup Language (SAML) 2.0 is a standard for exchanging authentication and authorization data between security domains.

SAML 2.0 is an XML-based protocol that uses security tokens (information packets) containing assertions to pass information about a principal (usually an end-user) between an identity provider (IdP) and a web service. SAML 2.0 enables web-based scenarios including single sign-on (SSO) authentication.

SAML 2.0 is supported by Juniper Networks’ Junos Pulse Secure Access Service (SA), enhancing the SSL VPN’s ability to securely integrate single sign-on authentication and authorization with external applications, such as cloud application providers.

In this SAML scenario, SA is the service provider, and SafeNet Authentication Service (SAS) is the Identity Provider. SA implements the authentication result determined by SAS.
SAML Authentication Flow

The following describes the SafeNet authentication process using SAML.

1. The user connects to Juniper SA using a web browser.
2. SA redirects the user to the SafeNet Authentication Service (SAS) authentication webpage.
3. The authentication webpage requests the user’s authenticating credentials, such as user name and password.
4. The user enters her authenticating credentials.
5. SAS verifies the user’s credentials.
6. SAS sends the SAML token to SA which redirects the user to the SA SSO website.
7. The user selects a secure site, such as Outlook Web Access (OWA).
8. Juniper SA uses Kerberos Constrained Delegation (Microsoft-based SSO) to automatically authenticate the user to the secure site.

Pre-Configuration

This solution requires information from the SA administrator’s console for the “Preparing the SA Entity Id” process.

Preparing the SA Entity Id

Before configuring SA, use the SA administrator’s console to update the SA’s Entity Ids.

To update the SA’s Entity Ids:

1. In the SA administrator’s console, go to System > Configuration > SAML > Settings.

2. In the Host FQDN for SAML field, enter the host name for SA when using SAML.
3. Click Save Changes.
4. Click Update Entity Ids. The Confirm Update Entity Ids message is displayed.
5. Click **Update Entity Ids**.

**Note**
It is very important that the timezone and time be set correctly in Juniper. Incorrect setting of the time or timezone may result in authentication failure.

**SA Configuration as a Service Provider**

**Viewing SAS’s SAML Settings**

Display the SAS data that will be needed for SA configuration in “Creating an Authentication Server” on page 8.

To access the SAS SAML settings required for Juniper configuration:

1. In your SAS console, select the Virtual Server > COMMS.

2. In the **SAML Service Providers** area, click **SAML 2.0 Settings**. The **SAML 2.0 Settings** are displayed. The following is an example of the settings.
Creating an Authentication Server

Use the SAS SAML settings to configure SA so that it is recognized by SAS as a SAML service provider. See “Viewing SAS’s SAML Settings” on page 7 to view the SAS SAML settings.

To create an authentication server:

1. In the SA administrator’s console, go to **Authentication > Auth. Servers**.
2. From the **New** list, select **SAML Server**, and then click **New Server**.

3. The **New SAML Server** window opens.

   - **SA Entity Id**: The value that was updated in “Preparing the SA Entity Id” on page 6.
   - **Server Name**: Any value. You will need this value for step 3 of “Setting the User Authentication Realm” on page 10.

The **SA Entity ID** field contains the value that was updated in “Preparing the SA Entity Id” on page 6.

4. Set the **Server Name** to any value. You will need this value for step 3 of “Setting the User Authentication Realm” on page 10.
5. In the **Settings** area, do the following:
   a. In the **Identity Provider Entity Id** field, enter the **Entity ID** displayed in the SAS console.
   b. In the **Identity Provider Single Sign On Service URL** field, enter the **Identity Provider HTTP-Redirect login URL** displayed in the SAS console.

6. In the **SSO Method** area, do the following:
   a. Download the certificate whose link appears in the SAS console as **Download URL for Identity Provider Certificate**.
   b. In the **Upload Certificate** area, click **Choose File** and upload the downloaded certificate.

7. In the **Service Provider Metadata Settings > Metadata Validity** field, enter the number of days for which the metadata will be valid.

8. Click **Save Changes**.

9. In the **Service Provider Metadata Settings** area, click **Download Metadata**, and download and save the metadata xml file. You will need this file for step 6 of “Configuring the SAML Service Provider” on page 11.

### Setting the User Authentication Realm

To set the user authentication realm:

1. In the SA administrator’s console, click **Users > User Realms**.

![User Authentication Realms](image-url)
2. Select the appropriate authentication realm. In this example, the realm is **Users**. The realm’s properties are displayed.

3. On the **General** tab in the **Servers > Authentication** list, select the authentication server that was created in step 4 of “Creating an Authentication Server” on page 8.

4. Click **Save Changes**.

**SAML Authentication Configuration in SAS**

The following steps are used to configure SAML authentication in SAS:

- Configuring the SAML Service Provider, see page 10.
- Configuring SAML Services, see page 12.

**Configuring the SAML Service Provider**

Configure the virtual server to process authentication requests received from a specific SAML service provider.

To configure the virtual server:

1. In your SAS console, select the **Virtual Server > COMMS**.
2. In the **SAML Service Providers** area, click **SAML 2.0 Settings**. The **SAML 2.0 Settings** are displayed. The following is an example of the settings.

3. Click **Add** to add a new service provider. The **Add SAML 2.0 Settings** fields are displayed.

4. In the **Friendly Name** field, enter a name for the Juniper SA service provider. You will need this value for **Configuring SAML Services**, beginning on page 12. In this example, the value is **Juniper SA**.

5. Select **Upload Existing Metadata File**, and click **Choose File**.

6. Select the metadata file saved in step 9 of “Creating an Authentication Server” on page 9, and then click **Open**.

7. Click **Apply**. The new service provider is displayed in the **Entity ID** list.
Configuring SAML Services

Enable or disable SAML authentication services for individual users or user groups. SAML services are enabled and disabled in either of the following ways:

- Manually Enabling User Authentication, see page 12.
- Using SAML Provisioning Rules to Enable User Authentication, see page 14.

Manually Enabling User Authentication

Enable an individual user to authenticate against the Juniper SA service provider defined in “Configuring SAML Services”.

To manually enable authentication for a user:

1. In your SAS console, select the Virtual Server > ASSIGNMENT.
2. Search for the user for whom to enable SAML authentication, and click its User ID. The user options opens.

3. Select SAML Services. The SAML Services options are displayed.

4. Click Add. More options are displayed.

5. From the Service list of configured SAML service providers, select the Juniper SA service provider’s Friendly Name created in step 4 of “Configuring the SAML Service Provider” on page 11. In this example, it is Juniper SA.

6. For SAML Login ID, select User ID.

7. Click Add. The service’s name is displayed as the user’s SAML service provider. In this example, it is Juniper SA.
Using SAML Provisioning Rules to Enable User Authentication

Use SAML Provisioning Rules to automatically enable or disable user authentication to SAML service providers. The Provisioning Rules can be used instead of, or in addition to, manual authentication configuration.

To set SAML Provisioning Rules for users:

1. In your SAS console, select the Virtual Server > POLICY.

2. Select Automation Policies > SAML Provisioning tools.

3. Click New Rule. The Add SAML Auto-create Role options are displayed.

4. In the Rule Name field, enter a name for the new rule.

5. In the Virtual Server groups list, select the group to be authenticated against Juniper SA, and click the right arrow to move the group to the Used by rule list.

6. In the Relying Parties list, select the Juniper SA service provider’s Friendly Name created in step 4 of “Configuring the SAML Service Provider” on page 11, and click the right arrow to move the service provider to the Rule Parties list. In this example, the value is Juniper SA.
7. For **SAML Login ID**, select **User ID**.

8. Click **Add**. The new rule is displayed in the list of **SAML Provisioning Rules**.

---

**KCD Configuration**

Juniper SA is often used to protect Web application resources, such as Outlook Web Access (OWA) and SharePoint, which are based on Windows authentication.

Kerberos Constrained Delegation (KCD) enables single sign-on for the application resource, so that users are required to log on only once per session. The user logs on to SA, and then is not required to authenticate again when accessing Microsoft applications.

The following steps are used to authenticate a user to a Web application:

1. SA verifies the user’s identity using SAML authentication.
2. SA then impersonates the user and obtains a Kerberos service ticket.
3. The Web application resource uses the Kerberos ticket as proof of authentication, and the user is logged on.

The following steps are used to configure KCD with SA:

- Configuring the User Account, see page 16.
- Configuring the Exchange Server, see page 20.
- Configuring SA, see page 22.
Configuring the User Account

Creating a KCD User Account in Active Directory

KCD requires an Active Directory user account that has Protocol Transition and Delegation rights. This account has rights to request a Kerberos ticket on behalf of a user signing in to SA.

To create a new user in Active Directory:


2. In the left pane, expand your domain name, and right-click Users.

4. Add the new user's information. This account will be used to access Web application resources, such as OWA. You will need the **User logon name** value for the following steps:
   - Step 1 of “Defining the Delegated Authentication” on page 17
   - Step 11c of “Configuring the Constrained Delegation Service List” on page 25

   In this example, the **User logon name** of the new account to provide Constrained Delegation is **samservice**.

### Defining the Delegated Authentication Services

To configure the new account for Web application access, do the following:

1. Use the `setspn` command to enable the **Delegation** tab in the new user account's **Properties** window.

   ![User Properties Window](image)

   - Use the `setspn` command to enable the Delegation tab in the new user account's Properties window.
   - Open the Command Prompt window, and enter the command:

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

     where:
     - `<user_account>` is the **User logon name** created in step 4 of *Creating a KCD User Account in Active Directory* on page 17
     - `<domain>` is your domain

     In the following example, **sfnt** is the domain, and **samservice** is the user account's **User logon name**.
2. In the **Active Directory Users and Computers** window, right-click the new user. The user’s **Properties** window opens.

3. Select the **Delegation** tab.

4. Select the following options:
   - Trust this user for delegation to specified services only
   - Use any authentication protocol

    **Note**
    Do not select **Use Kerberos only** because that option is not compatible with Protocol Transition and Constrained Delegation.
5. Click **Add**. The **Add Services** window opens.

6. To select the computer hosting the constrained services, click **Users or Computers**. The **Select Users or Computers** window opens.

7. Enter the name of the protected service's server in the domain.

   **Note**
   In this example, the OWA service is hosted on the same server as Active Directory Domain Controller, so **DC** is selected.

8. In the **Add Services** window, the services available on the selected server are displayed.

9. Select the appropriate service type, and click **OK**.
Note
In this example, Constrained Delegation must be configured for OWA. Select http to configure for OWA and for any other Web-based applications running on this server, such as SharePoint.

10. In the user’s Properties window, the delegated services are displayed.

11. Click Apply, and then click OK.
Active Directory is now configured for this solution.

Configuring the Exchange Server

Configure the server hosting the web application.

Note
This solution can be configured for any web application hosted on any server within the domain.
In this example, the selected web application is OWA, and it is hosted on the same server as the Active Directory Domain Controller.

To configure OWA and ECP:
1. Open the Microsoft Exchange console.
2. In the left pane, go to Server Configuration > Client Access.
3. In the middle pane’s Client Access area, select your Exchange server.
4. In the server area, select the Outlook Web App tab.
5. Right-click **owa (Default Web Site)**, and select **Properties**.

6. Select the **Authentication** tab, and do the following:
   a. Select **Use one or more standard authentication methods**.
   b. Select **Integrated Windows Authentication**.
   c. Click **OK**.

7. In the Microsoft Exchange console, select the Exchange Control Panel tab.

8. Right click **ecp (Default Web Site)**, and select **Properties**. The **ecp (Default Web Site) Properties** window opens.
9. Select the **Authentication** tab, and do the following:
   a. Select **Use one or more standard authentication methods**.
   b. Select **Integrated Windows Authentication**.
   c. Click **OK**.

10. To restart IIS so that the configurations take effect, open a terminal and enter `iisreset`.

### Configuring SA

Configure SA with Constrained Delegation for users connecting via SA to a selected application. This involves the following steps:

- Configuring Web SSO, see page 22.
- Configuring the Constrained Delegation Service List, see page 23.
- Configuring SSO Policies, see page 26.

In this example, **OWA** is the application to which users connect.

### Configuring Web SSO

Add the Kerberos realm to SA’s Kerberos SSO Settings.

1. In the SA administrator’s console, go to **Users > Resource Policies > Web > SSO (Single Sign-on) > General**.
The WebPolicySSOGeneral window opens.

2. Select the SSO tab.
3. Select Enable Kerberos SSO.
4. In the Realm Definition area, add the Kerberos realm. You will need this value for step 11b of "Configuring the Constrained Delegation Service List" on page 25. In this example, the added realm is sfnt.com.

**Note**
The Kerberos realm is typically the DNS domain.

5. Click Add.
6. Click Save Changes.

**Note**
The Site Name field can be used only if your Active Directory is set up with Sites.

Configuring the Constrained Delegation Service List

Upload a text file to create a Constrained Delegation Service List.

To configure the Constrained Delegation Service List:

1. Open Notepad or similar text application, and create a file containing the DC server name.
2. Save the file. You will need it for step 8 of this procedure.
3. In the SA administrator's console, go to Users > Resource Policies > Web > SSO (Single Sign-on) > General.

4. Select the SSO tab.

5. In the Constrained Delegation area, click Edit. The Constrained Delegation Service Lists window opens.

6. Click New Service List.

7. In the Name field, enter any value. You will need it for step 11e of this procedure.

8. Click Choose File, and browse to the text file saved in step 2 of this procedure.

9. Click OK. The Upload Status window opens.
10. When the upload is complete, click **Close**.

11. In the **Constrained Delegation** area, do the following:
   a. In the **Label** field, enter any value.
      You will need this value for step 10c of “Configuring SSO Policies” on page 27.
      In this example, the value is **sfnt**.
   b. In the **Realm** list, select the Kerberos realm defined in step 4 of "Configuring Web SSO" on page 23.
   c. In the **Principal Account** field, enter the **User logon name** created in step 4 of “Creating a KCD User Account in Active Directory” on page 17.
      
      **Note**
      In the example, we enter the samservice account created in Active Directory for Constrained Delegation.
   d. In the **Password** field, enter the user’s domain password.
      
      **Note**
      Ensure that the password is entered exactly as defined in the Active Directory.
   e. In the **Service List** list, select the service list **Name** defined in step 7 of this procedure.
   f. Click **Add**. The realm is displayed in the **Constrained Delegation** area.
Configuring SSO Policies

Define the roles and resources for which Constrained Delegation will be performed.

To configure SSO policies for OWA:

1. In the SA administrator's console, go to Users > Resource Policies > Web > Kerberos/NTLM/Basic Auth.

3. In the Type list, select Microsoft OWA 2010. The OWA 2010 window opens.
4. Select the Resource tab.
5. In the **Name** field, enter any value for the policy name.

6. In the **Base URL** field, enter the OWA site’s base URL.

7. Select **Autopolicy: Web Compression**.

8. In the **Autopolicy: Web Compression** area, do the following:
   a. In the **Resource** column, enter the OWA site.
   b. In the **Action** column list, select **Compress**.
   c. Click **Add**. The resource is displayed on a new line.

9. Select **Autopolicy: Single Sign-on**.

10. In the **Autopolicy: Single Sign-on** area, do the following:
   a. Select **Constrained Delegation**.
   b. In the **Resource** field, enter the host FQDN of the web server.
   c. In the **Credential** list, select the Constrained Delegation’s Label defined in “Configuring the Constrained Delegation Service List” on page 25.

11. Click **Save Changes**.
Running the Solution

User Authentication Scenario

In this example, a user named Walter authenticates to SA in the following environment:
Walter has already enrolled an OTP GrIDsure token. Each time Walter wants to sign in, he authenticates using a grid.

How Walter authenticates to OWA:

1. Walter opens a web browser and browses to SA.
   In this example, the SA site is https://Juniper.sfnt.com
   SA automatically redirects the authentication request to the SAS Authentication Portal.
   The Authentication Portal’s Login window opens.

2. Walter enters his User Name, and clicks Login.
   The login grid is displayed.
3. In the **Password** field, Walter enters his OTP based on his PIP (personal identification pattern), and clicks **Login**. Walter is redirected to the SA portal.

4. Walter clicks the **OWA 2010** link. Walter is automatically authenticated to his OWA account.
Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Cause</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The SAS Authentication Portal does not open</td>
<td>The user entered an incorrect URL.</td>
<td>Ensure that the URL entered is correct.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Identity Provider Single Sign On Service URL</strong> is not correct.</td>
<td>In the SA configuration, ensure that the <strong>Identity Provider Single Sign On Service URL</strong> is correct.</td>
</tr>
<tr>
<td>An error message is displayed: “Verification cert not available, Signature has no X509Cert”</td>
<td>The <strong>Response Signing Certificate</strong> in the authentication server is incorrect or missing.</td>
<td>Download the signing certificate from SAS, and import it again in the SA configuration’s <strong>Authentication Server page</strong>.</td>
</tr>
<tr>
<td>An error message is displayed: “Unknown issuer value in response”</td>
<td>The <strong>Identity Provider Entity Id</strong> and the <strong>SAS Entity ID</strong> do not match.</td>
<td>Ensure that the <strong>Identity Provider Entity Id</strong> in the SA configuration’s <strong>Authentication Server page</strong>, and the <strong>Entity ID</strong> of SAS are identical.</td>
</tr>
<tr>
<td>After logon, an error message is displayed: “The page you requested could not be found”</td>
<td>The service provider’s <strong>Location</strong> in the SAML settings in SAS is incorrect.</td>
<td>Enter the correct Juniper SA login URL as the <strong>Location</strong> in the SAML settings.</td>
</tr>
</tbody>
</table>

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>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><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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>