SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with Juniper Steel-Belted Radius
## Contents

- Third-Party Software Acknowledgement ................................................................. 4
- Description .................................................................................................................. 4
  - SafeNet Authentication Service .............................................................................. 4
  - MAG2600 Junos Pulse Gateway ........................................................................... 4
  - Steel-Belted Radius Enterprise ............................................................................ 4
- Applicability .............................................................................................................. 5
- 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 ................................................................. 7
- RADIUS Prerequisites ............................................................................................. 7
- Configuring SafeNet Authentication Service ........................................................... 8
  - Synchronizing User Stores with SAS ................................................................. 8
  - Assigning an Authenticator in SAS ..................................................................... 8
  - Adding Juniper Steel-Belted Radius as an Authentication Node in SAS ............ 9
- Configuring Juniper MAG2600 Junos Pulse Gateway ............................................. 12
  - Adding an Authentication Server ..................................................................... 12
  - Attaching Authentication Servers to User Realms .............................................. 14
- Configuring Steel-Belted Radius .............................................................................. 15
  - Configuring RADIUS Clients .......................................................................... 15
  - Configuring Proxy Targets ............................................................................... 18
  - Configuring Authentication Methods ............................................................... 19
- Running the Solution ............................................................................................... 21
- Support Contacts ..................................................................................................... 23
Third-Party Software Acknowledgement

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

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

SafeNet Authentication Service (SAS) 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.

MAG2600 Junos Pulse Gateway

The Juniper MAG2600 Junos Pulse Gateway provides SSL/VPN, network access control (NAC) with Unified Access Control (UAC), or guest access capabilities to small and midsize businesses (SMBs), and small and medium enterprises.

Junos Pulse software enables dynamic SSL VPN connectivity, network access control (NAC), mobile security, and collaboration, through a simple end-user interface. It simplifies and optimizes connectivity to end users at the same time it checks their device type and security state, location, identity, and adherence to corporate access control policies.

Steel-Belted Radius Enterprise

Steel-Belted Radius (SBR) Series Servers deliver scalable authentication control, robust access policy management, and centralized configuration management with the performance needed to tackle tens of thousands of concurrent users.

SBR Enterprise Edition is the market-leading AAA/RADIUS server for small to mid-sized enterprises.

This document describes how to:

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

It is assumed that the Juniper Steel-Belted Radius and MAG2600 Junos Pulse Gateway environment is already configured, and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Juniper Steel-Belted Radius 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)**—An on-premises version that is used by service providers to deploy instances of SafeNet Authentication Service
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—An on-premises 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**—SafeNet’s cloud-based authentication service
- **Juniper Steel-Belted Radius**—Version 6.1.0
- **Juniper MAG2600 Junos Pulse Gateway**
- **Juniper Junos Pulse**—Version 3.0

Audience

This document is targeted to system administrators who are familiar with Juniper Steel-Belted Radius 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**—A RADIUS service 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 is implemented in the customer’s existing 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 FreeRADIUS, refer to the *SafeNet Authentication Service FreeRADIUS Agent Configuration Guide*.

**RADIUS-based Authentication using SAS-SPE and SAS-PCE**

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

• **SafeNet Authentication Service – Service Provider Edition (SPE)**—An on-premises version of SafeNet Authentication Service that is targeted at service providers interested in hosting SAS in their data center.

• **SafeNet Authentication Service – Private Cloud Edition (PCE)**—An on-premises version of SafeNet Authentication Service that is targeted at organizations interested in hosting SAS in their private cloud environment.

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: [http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf](http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf)

• **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](http://www2.safenet-inc.com).
RADIUS Authentication Flow using SAS

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

The following diagram describes the data flow of a multi-factor authentication transaction for Juniper Steel-Belted Radius.

1. A user attempts to log on to Junos Pulse Gateway using a one-time password (OTP) authenticator.
2. Junos Pulse Gateway sends a RADIUS request with the user’s credentials to Juniper Steel-Belted Radius.
3. Juniper Steel-Belted Radius sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
4. The SAS authentication reply is sent back to the Juniper Steel-Belted Radius.
5. Juniper Steel-Belted Radius forwards the authentication reply to Junos Pulse Gateway.
6. The user is granted or denied access to Junos Pulse Gateway based on the OTP value calculation results from SAS.

RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Juniper Steel-Belted Radius, ensure the following:

- End users can authenticate through the Juniper Steel-Belted Radius and MAG2600 Junos Pulse Gateway environment with a static password, before configuring the Juniper Steel-Belted Radius to use RADIUS authentication.
- Ports 1812/1813 are open to and from Juniper Steel-Belted Radius.
- A shared secret key has been selected. A shared secret key provides an added layer of security between the RADIUS server and RADIUS client for encryption, decryption, and digital signatures.
- Junos Pulse client software is installed on the client machine.
- SafeNet eToken PASS is already enrolled as an OTP token in SAS.
Configuring SafeNet Authentication Service

Deploying multi-factor authentication using SAS with Juniper Steel-Belted Radius and RADIUS protocol requires the following:

- Synchronizing User Stores with SAS, page 8
- Assigning an Authenticator in SAS, page 8
- Adding Juniper Steel-Belted Radius as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Server’s IP Address, page 11

Synchronizing User Stores with SAS

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users who 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 authenticating through Juniper Steel-Belted Radius.

The following authenticators are supported:

- eToken PASS
- MobilePASS
- SMS Tokens

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 Steel-Belted Radius 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 Steel-Belted Radius. You will need the IP address of Juniper Steel-Belted Radius and the shared secret that will be used by SAS and Juniper Steel-Belted Radius.

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 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 Server’s IP Address

Before adding SAS as a RADIUS server in Juniper Steel-Belted Radius, check its IP address. The IP address will be added to Juniper Steel-Belted Radius as a RADIUS server later in this document.

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 Juniper MAG2600 Junos Pulse Gateway

Configuring Juniper MAG2600 Junos Pulse Gateway with Steel-Belted Radius requires the following:

- Adding an Authentication Server, page 12
- Attaching Authentication Servers to User Realms, page 14

Adding an Authentication Server

The authentication server that you create in this section will be configured with RADIUS support. Later, the authentication server will be set as the main authentication server of Juniper Secure Access (SA). This enables Juniper SA to be accessed with RADIUS authentication using SafeNet SAS through Steel-Belted Radius.

1. Open the Juniper MAG2600 web console.
2. Click **Authentication**, and then click **Auth. Servers**.

3. In the New field, select **Radius Server**, and then click **New Server**.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
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>Radius Server</td>
<td>Enter the Steel-Belted Radius IP address.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret configured for Steel-Belted 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 Authentication Servers to User Realms

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

1. Open the Juniper MAG2600 web console.
2. Click **Users**, and then click **User Realms**.

3. Under **Authentication Realms**, click the user realm to edit.
4. Click the **General** tab.

5. Under **Servers**, click the **Authentication** menu, and then select the authentication server that you created in the previous section.
6. Click **Save Changes**.
Configuring Steel-Belted Radius

Configuring Juniper Steel-Belted Radius with SAS and MAG2600 Junos Pulse Gateway requires the following:

- Configuring RADIUS Clients, page 15
- Configuring Proxy Targets, page 18
- Configuring Authentication Methods, page 19

Configuring RADIUS Clients

A RADIUS client is a network device or software application that contacts Steel-Belted Radius to authenticate a user. In this integration, Juniper MAG2600 will be the RADIUS client for Steel-Belted Radius.

1. Open the Steel-Belted Radius console using the following format: \texttt{http://< IP address of SBR>:1812}
2. Click \textit{Launch}.

(The screen image above is from Juniper Networks\textsuperscript{®}. Trademarks are the property of their respective owners.)
3. On the **Login** window, enter the appropriate user credentials, and then click **Login**.

4. Click **Steel-Belted Radius**, and then click **RADIUS Clients**.

5. Click **Add**.
6. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the RADIUS client.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Enter the IP address of the RADIUS client.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter the authentication shared secret for the RADIUS client.</td>
</tr>
<tr>
<td><strong>Make or model</strong></td>
<td>Select <strong>Standard Radius</strong>.</td>
</tr>
</tbody>
</table>

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

The Radius client is added.

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

Steel-Belted Radius will be configured as the proxy server for this integration. In this section, you will set up proxy forwarding from the Steel-Belted Radius server (the proxy) to another RADIUS server (the target).

1. In the Steel-Belted Radius console, select **Proxy Targets**, and then click **Add**.

2. Complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the proxy target.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the proxy target.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the authentication shared secret for the proxy target.</td>
</tr>
<tr>
<td>Non-default Ports &gt; Authentication</td>
<td>Verify this option is selected, and that the value is 1812.</td>
</tr>
<tr>
<td>Make available as an authentication method</td>
<td>Verify this option is selected.</td>
</tr>
</tbody>
</table>

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

![Steel-Belted Radius console](image)

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

## Configuring Authentication Methods

Each time an Access-Request message reaches the server, an authentication transaction begins. During this transaction, the server attempts to authenticate the request by sequentially trying its configured and enabled authentication methods. The server consults its list of authentication methods to determine which methods to try, and in which order to try them. In this section, you will set up the appropriate authentication method.

1. In the Steel-Belted Radius console, select **Authentication Policies**, and then click **Order of Methods**.

![Steel-Belted Radius console](image)

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
2. Under Inactive **Authentication Methods**, select the appropriate method, (for example, proxy: SAS), and then click the add icon to move the selection to **Active Authentication Methods**.

3. Click **Apply**. The authentication method is configured.
Running the Solution

After configuring Juniper Steel-Belted Radius for RADIUS authentication with SAS, a user can securely access the corporate network using the Junos Pulse client software. Check the configured solution of SAS RADIUS authentication using the Junos Pulse.

1. From the Windows Start menu, select All Programs > Juniper Networks > Junos Pulse > Junos Pulse.
2. In the Junos Pulse client interface, click Connections, and then click to add a new connection.

3. Complete the following fields, and then click Add.

<table>
<thead>
<tr>
<th>Type</th>
<th>Select UAC or SSL-VPN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the connection name (for example, JUNOSclient).</td>
</tr>
<tr>
<td>Server URL</td>
<td>Enter the URL of the JUNOS server.</td>
</tr>
</tbody>
</table>

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

4. Select the connection (for example, JUNOSclient), and then click Connect.
5. Enter the user credentials in Username and Password fields, and then click Connect.

(The screen image above is from Juniper Networks®. Trademarks are the property of their respective owners.)
6. After successful authentication, the user can access the company’s internal network through the VPN connection.

(The screen image above is from Juniper Networks®. 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 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 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>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>