SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with Cyberoam
Document Information

<table>
<thead>
<tr>
<th>Product Version</th>
<th>1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document Part Number</td>
<td>007-012658-001, Rev. A</td>
</tr>
<tr>
<td>Release Date</td>
<td>August 2014</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>
</table>
| Mail | SafeNet, Inc.  
4690 Millennium Drive  
Belcamp, Maryland 21017, USA |
| Email | TechPubs@safenet-inc.com |
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>4</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS Cloud</td>
<td>5</td>
</tr>
<tr>
<td>RADIUS-based Authentication using SAS-SPE and SAS-PCE</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Authentication Flow using SAS</td>
<td>6</td>
</tr>
<tr>
<td>RADIUS Prerequisites</td>
<td>7</td>
</tr>
<tr>
<td>Configuring SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Synchronizing Users Stores to SafeNet Authentication Service</td>
<td>7</td>
</tr>
<tr>
<td>Authenticator Assignment in SAS</td>
<td>8</td>
</tr>
<tr>
<td>Adding Cyberoam as an Authentication Node in SAS</td>
<td>9</td>
</tr>
<tr>
<td>Checking the SAS RADIUS Address</td>
<td>11</td>
</tr>
<tr>
<td>Configuring Cyberoam</td>
<td>13</td>
</tr>
<tr>
<td>Configuring Cyberoam to use a RADIUS Server</td>
<td>13</td>
</tr>
<tr>
<td>Selecting RADIUS Server as the Primary Authentication Method on Firewall</td>
<td>15</td>
</tr>
<tr>
<td>Selecting RADIUS Server as the Primary Authentication Method on SSL VPN</td>
<td>16</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>18</td>
</tr>
<tr>
<td>Using the Cyberoam Captive Portal</td>
<td>18</td>
</tr>
<tr>
<td>Using the Cyberoam SSL VPN Web Portal</td>
<td>19</td>
</tr>
<tr>
<td>Using the Cyberoam SSL VPN Client</td>
<td>21</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>22</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

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

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.

Cyberoam network security appliances (UTMs and next-generation firewalls) offer enterprise-class network security with state-of-the-art inspection firewall, VPN, and IPS. It offers Layer 8 identity-based controls, and Layer 7 application visibility and controls. Cyberoam ensures high levels of network security, network connectivity, continuous availability, and secure remote access with controlled network access to road warriors, telecommuters, partners, and customers.

With granular controls and advanced networking features, Cyberoam appliances offer enterprise-class security and high flexibility with protection against blended threats, malware, Trojans, DoS, DDoS, IP spoofing attacks, spam, intrusions, and data leakage.

This document describes how to:

- Configure Cyberoam to work with SafeNet Authentication Service in RADIUS mode.

This document assumes that the Cyberoam environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Cyberoam 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** – SafeNet’s cloud-based authentication service.
- **Cyberoam** - CRIV-TR firmware 10.6.1

Audience

This document is targeted to system administrators who are familiar with Cyberoam 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.

![Diagram of SAS cloud hosted RADIUS service]

- **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.

![Diagram of Local RADIUS hosted on-premises]

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
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 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 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 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 dataflow of a multi-factor authentication transaction for Cyberoam.

1. A user attempts to log on to Cyberoam using an OTP authenticator.
2. Cyberoam 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 Cyberoam.
4. The user is granted or denied access to the Cyberoam based on the OTP value calculation results from SAS and gets connected to the VPN.
RADIUS Prerequisites

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

- End users can authenticate through from the Cyberoam environment with a static password before configuring the Cyberoam to use RADIUS authentication.
- Ports 1812/1813 are open to and from Cyberoam.
- 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 signature purposes.

Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SAS
- Authenticator assignment in SAS
- Adding Cyberoam as an Authentication Node in SAS
- Checking the SAS RADIUS IP address

Synchronizing Users Stores to SafeNet Authentication Service

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

All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.
Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users authenticating through Cyberoam.

The following authenticators are supported:

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

Authenticators can be assigned to users in two ways:

- **Manually provision** – Assign an authenticator to users one by one.
- **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 the sections on Provisioning Rules in the *SafeNet Authentication Service - Subscriber Account Operator Guide* to learn how to provision the different authentication methods to users in the SAS User Store.

Adding Cyberoam as an Authentication Node in SAS

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

To add an Authentication Node in SAS:

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

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

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

![Add Auth Nodes](image)

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 entered above to confirm it.</td>
</tr>
</tbody>
</table>

![Add Auth Node](image)

The Auth Node is added to the system.
Checking the SAS RADIUS Address

Before adding SafeNet Authentication Service as a RADIUS server in Cyberoam, check the IP address of the SAS RADIUS server. The IP address will then be added to Cyberoam as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

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

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

3. Click the Auth Nodes link.
The SAS RADIUS server details are displayed.
**Configuring Cyberoam**

This section covers how to configure Cyberoam to use RADIUS server for user authentication on SSL VPN and for Captive portal. Configuration is performed via the Web Admin Console with an Administrator profile.

Configuring Cyberoam includes the following:

- Configure Cyberoam to use a RADIUS Server
- Select RADIUS Server as the Primary Authentication Method on Firewall
- Select RADIUS Server as the Primary Authentication Method on SSL VPN

**Configuring Cyberoam to use a RADIUS Server**

1. Log in to the Cyberoam Web console: `http://<IPAddress of Cyberoam>/`. The default username/password combination is admin/admin.

2. From the Cyberoam web console window, in the left pane, click **Identity > Authentication**.

3. In the right pane, the Authentication Server tab is displayed. Click Add.

![Cyberoam Web Console](image-url)  
*(The screen image above is from Cyberoam® software. Trademarks are the property of their respective owners.)*
4. On the Add External Server window, complete the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Type</td>
<td>Select RADIUS Server.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter a name to identify the RADIUS Server; for example, Cyberoam_RADIUS.</td>
</tr>
<tr>
<td>Server IP</td>
<td>Enter the IP address of the SAS RADIUS Server.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the port number through which the SAS RADIUS Server communicates.</td>
</tr>
<tr>
<td></td>
<td>The default port number is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter a shared secret used to encrypt information sent to the appliance.</td>
</tr>
<tr>
<td>Integration Type</td>
<td>Select Loose Integration.</td>
</tr>
<tr>
<td></td>
<td>Select Tight Integration only if you want to use the vendor-specific attribute for setting the user group membership and specifying a group name attribute.</td>
</tr>
<tr>
<td>Group Name Attribute</td>
<td>This field is available only when Tight Integration is selected for Integration Type. Specify the vendor-specific value for this field.</td>
</tr>
</tbody>
</table>

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

5. Confirm that the Cyberoam is able to connect to the RADIUS Server by clicking Test Connection on the Add External Server window.

6. From the Test Connection window, enter the administrator’s name in the User Name field and OTP passcode in the Password field, and then click Test Connection.

(The screen image above is from Cyberoam® software. Trademarks are the property of their respective owners.)
7. If the connection is successful, on the Add External Server window click OK to save. A row with the newly added server details appears under Authentication Server.

![Image of Add External Server window]

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

Selecting RADIUS Server as the Primary Authentication Method on Firewall

The firewall is accessed by the Captive Portal. Specify RADIUS server as the primary authentication method for the firewall.

1. From the Cyberoam Web console, click Identity > Authentication on the left pane.

![Image of Cyberoam Web console]

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

2. In the right pane, select the Firewall tab.

3. Under Authentication Methods, in the Authentication Server List, select an authentication server (for example, Cyberoam_RADIUS). The selected server is added to the Selected Authentication Server list.
NOTE: For multiple servers, authentication requests are sent according to the Selected Authentication Server column.

4. Click **Apply**.

The firewall can now be accessed through the Captive Portal at `http://<ipaddress of cyberoam>:8090` using SAS via RADIUS.

**Selecting RADIUS Server as the Primary Authentication Method on SSL VPN**

1. From the Cyberoam Web console, in the left pane, click **Identity > Authentication**.
2. In the right pane, select the **VPN** tab.
3. Under **SSL VPN Authentication Methods**, in the **Authentication Server List**, select an authentication server (for example, **Cyberoam_RADIUS**). The selected server is added to the **Selected Authentication Server** list.

![Image](image_url)

**NOTE:** For multiple servers, authentication requests are sent according to the **Selected Authentication Server** column.

4. Click **Apply**.
Running the Solution

Before running the RADIUS server integration solution, the Cyberoam must be configured with an appropriate firewall and SSL VPN policy.

If you have an enrolled token (OTP, GridSure, SMS, MobilePASS, etc.), browse to the virtual server and enter the username and token code on the login window.

A user can be assigned several types of SAS-supported tokens. For this integration test, the SafeNet MobilePASS token for Windows is configured for authentication with the SAS solution.

The sections below explain how to securely connect to the Cyberoam appliances:

- Using the Cyberoam Captive Portal
- Using the Cyberoam SSL VPN Web Portal
- Using the Cyberoam SSL VPN Client

Using the Cyberoam Captive Portal

The Cyberoam Captive Portal authenticates users for Internet access. When a user attempts to access the Internet, a default Captive Portal is presented for authentication.

1. Open a web browser and go to: http://<Cyberoam LAN IP>:8090

   ![Cyberoam Captive Portal](image)

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

2. In the **Username** field, enter your username.
3. Click **Generate Token Code** on the MobilePASS application to generate a one-time password (OTP).

![Token Generation](image)

4. On the login page, enter the OTP in the **Password** field and then click **Login**.
   
   If authentication is successful, all resources will be made available.

5. To check successful authentication logs with the RADIUS server, click the **Snapshot** tab in SAS cloud.

6. If logged in successfully, the username is displayed on the Cyberoam Web Admin Console under **Identity > Live Users**.

**Using the Cyberoam SSL VPN Web Portal**

For remote users to access resources (for example, web and intranet servers) on the company’s internal network, configure SSL VPN in Cyberoam. Refer to the following Cyberoam Knowledge Base article: http://kb.cyberoam.com/default.asp?id=2270&Lang=1&SID=

1. Open a web browser and go to: https://<WAN IP address of Cyberoam>:8443

![SSL VPN Login](image)

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

2. In the **Username** field, enter your username.
3. Click **Generate Token Code** on the MobilePASS application to generate a one-time password (OTP).

4. On the login page, enter the OTP in the **Password** field and then click **Login**.

   On successful login, the user is directed to the main page, which displays the **Tunnel, Web, or Application Access Mode** section according to applied user policies.

   (The screen image above is from Cyberoam® software. Trademarks are the property of their respective owners.)
Using the Cyberoam SSL VPN Client

To download and install Cyberoam SSL VPN client, refer to the following Cyberoam KB article: http://kb.cyberoam.com/default.asp?id=2270

1. Open **Cyberoam SSL VPN Client**.

   ![Cyberoam SSL VPN Client](image)

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

2. Enter your username in the **Username** filed.

3. Click **Generate Token Code** on the MobilePASS application to generate a one-time password (OTP).

   ![Generate Token Code](image)

4. On the login page, enter the OTP in the **Password** field, and then click **Login**.

   On successful authentication, the user can access the company’s internal network through SSL VPN.
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></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support</strong></td>
<td></td>
</tr>
<tr>
<td>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 SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>