SafeNet Authentication Manager
Integration Guide

Using SAM in RADIUS Mode 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>007-012659-001, Rev. A</td>
</tr>
<tr>
<td>Release Date</td>
<td>September 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>
<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

Third-Party Software Acknowledgement ................................................................. 4
Description .............................................................................................................. 4
Applicability ............................................................................................................ 4
Environment .......................................................................................................... 5
Audience .................................................................................................................. 5
RADIUS-based Authentication using SAM ............................................................ 5
RADIUS Authentication Flow using SAM ............................................................. 5
RADIUS Prerequisites .......................................................................................... 6
Configuring SafeNet Authentication Manager ....................................................... 7
  Synchronizing Users Stores to SafeNet Authentication Manager ....................... 7
  Configuring SAM’s Connector for OTP Authentication ...................................... 8
  Token Assignment in SAM ................................................................................. 8
Adding Cyberoam as a RADIUS Client in IAS/NPS ............................................. 9
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ....................... 11
Configuring Cyberoam .......................................................................................... 12
  Configuring Cyberoam to Use a RADIUS Server .......................................... 12
  Selecting RADIUS Server as the Primary Firewall Authentication Method .... 14
  Selecting RADIUS Server as the Primary SSL VPN Authentication Method .... 15
Running the Solution ............................................................................................ 17
  Using the Cyberoam Captive Portal ................................................................. 17
  Using the Cyberoam SSL VPN Web Portal ...................................................... 18
  Using the Cyberoam SSL VPN Client .............................................................. 19
Support Contacts .................................................................................................. 21
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

Cyberoam (UTMs and next-generation firewalls) offer enterprise-class network security with state-of-the-art firewall inspection, 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.

Remote access poses both a security and compliance challenge to IT organizations. The ability to positively identify users – often remote users – requesting access to resources is a critical consideration in achieving a secure solution.

Deploying a remote access solution without strong authentication is like putting your sensitive data in a vault (the data center) and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Cyberoam using SafeNet OTP tokens managed by SafeNet Authentication Manager 8.2.
- Configure Cyberoam to work with SafeNet Authentication Manager 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 Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager installation modes, refer to SafeNet Authentication Manager 8.2 Administrator's Guide.

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 Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manger** - A server version of SAM 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 Manager 8.2 HF 493**: A server version of SAM that is used to deploy the solution on-premises in the organization.
- **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 Manager.

RADIUS-based Authentication using SAM

SafeNet’s OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP Plug-In for Microsoft RADIUS Client, refer to *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

RADIUS Authentication Flow using SAM

SafeNet Authentication Manager 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 Cyberoam.

1. A user attempts to log on to Cyberoam using an OTP token.
2. Cyberoam sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Cyberoam.
4. The user is granted or denied access to Cyberoam based on the OTP value calculation results from SAM and is connected to the VPN.

**RADIUS Prerequisites**

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

- End users can authenticate from the Cyberoam environment with a static password before configuring 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 Manager

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

- Synchronizing Users Stores to SafeNet Authentication Manager, page 7
- Configuring SAM’s Connector for OTP Authentication, page 8
- Token Assignment in SAM, page 8
- Adding Cyberoam as a RADIUS Client in IAS/NPS, page 9
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration, page 11

Synchronizing Users Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM 8.2 uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server
Configuring SAM’s Connector for OTP Authentication

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The Simplified OTP-only configuration is as follows:

- Connectors - SAM Connector for OTP Authentication is installed
- SAM Backend Service - Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.

The SAM Connector for OTP Authentication is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

Token Assignment in SAM

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

The following tokens are supported:

- eToken PASS
- eToken NG-OTP
- SafeNet GOLD
- SMS tokens
- MobilePASS
- SafeNet eToken Virtual products
- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)
- SafeNet eToken 3400
- SafeNet eToken 3500

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self Service Center**: Self-service site used by end users for managing their tokens.
- **SAM Remote Service**: Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Adding Cyberoam as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Cyberoam.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Cyberoam.

Cyberoam must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Cyberoam for authentication.

NOTE: This document assumes that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

To add a RADIUS client:
2. From the NPS web console, in the left pane, expand RADIUS Clients and Servers, right-click RADIUS Clients and then click New.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable this RADIUS client</td>
<td>Select this option.</td>
</tr>
<tr>
<td>Friendly name</td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the IP address or DNS of Cyberoam.</td>
</tr>
<tr>
<td>Shared secret</td>
<td>Enter the shared secret for the RADIUS client. The value must be the same when configuring the RADIUS server in Cyberoam.</td>
</tr>
<tr>
<td>Confirm shared secret</td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

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

4. Click OK.

Cyberoam is added as a RADIUS client in NPS.
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) are Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM’s OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS Server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP Plug-in, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*. 
Configuring Cyberoam

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

This section includes the following:

- Configuring Cyberoam to Use a RADIUS Server, page 12
- Selecting RADIUS Server as the Primary Firewall Authentication Method, page 14
- Selecting RADIUS Server as the Primary SSL VPN Authentication Method, page 15

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, in the left pane, click Identity > Authentication.

3. In the right pane, on the Authentication Server tab, click Add.

(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><strong>Server Type</strong></td>
<td>Select <strong>RADIUS Server</strong>.</td>
</tr>
<tr>
<td><strong>Server Name</strong></td>
<td>Enter a name to identify the RADIUS server; for example, <strong>Cyberoam_RADIUS</strong>.</td>
</tr>
<tr>
<td><strong>Server IP</strong></td>
<td>Enter the IP address of the RADIUS server.</td>
</tr>
<tr>
<td><strong>Authentication Port</strong></td>
<td>Enter the port number through which the RADIUS server communicates. The default port number is 1812.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></td>
<td>Enter a shared secret used to encrypt information sent to Cyberoam.</td>
</tr>
<tr>
<td><strong>Integration Type</strong></td>
<td>Select <strong>Loose Integration</strong>. Select <strong>Tight Integration</strong> 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><strong>Group Name Attribute</strong></td>
<td>This field is available only when <strong>Tight Integration</strong> is selected for <strong>Integration Type</strong>. 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 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**.
Selecting RADIUS Server as the Primary Firewall Authentication Method

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

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

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.
4. Click **Apply**.

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

### Selecting RADIUS Server as the Primary SSL VPN Authentication Method

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

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

4. Click Apply.
Running the Solution

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

If you have an enrolled token, browse to the virtual server and enter the username and token code on the login window.

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

The sections below explain how to securely connect to Cyberoam:

- Using the Cyberoam Captive Portal, page 17
- Using the Cyberoam SSL VPN Web Portal, page 18
- Using the Cyberoam SSL VPN Client, page 19

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

(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.
If authentication is successful, all resources will be made available.

5. 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

   ![Welcome to the Cyberoam SSL VPN 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](image)

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.
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.

2. Enter your username in the Username filed.

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 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>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>