SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with CA SiteMinder
SafeNet Authentication Service: Integration Guide SAS Using RADIUS Protocol with CA SiteMinder

Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012792-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>October 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

<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>4</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 CA SiteMinder 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 CA SiteMinder</td>
<td>13</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>25</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>26</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 CA SiteMinder.

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. It provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

The CA SiteMinder solution is a web access management system that provides secure single sign-on and flexible access management to applications and web services either on-premises, in the cloud, from a mobile device, or at a partner’s site.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in CA SiteMinder using SafeNet OTP authenticators managed by SafeNet Authentication Service.
- Configure CA SiteMinder to work with SafeNet Authentication Service in RADIUS mode.

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

CA SiteMinder 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 used in this document is based on the following software versions:

- **SafeNet Authentication Service** – Cloud-based authentication service
- **CA SiteMinder** 12.5.1
Audience

This document is targeted to system administrators who are familiar with CA SiteMinder and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS-mode topologies:

- **SAS cloud hosted RADIUS service** – A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises** - A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a FreeRADIUS server only.

For more details on how to install and configure FreeRADIUS, refer to the *SAS FreeRADIUS Agent Configuration Guide*.

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 solution that serves as a local RADIUS server:

- **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 dataflow of a multi-factor authentication transaction for CA SiteMinder is as follows:

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

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

- End users can authenticate in the CA SiteMinder environment with a static password before configuring CA SiteMinder to use RADIUS authentication.
- Ports 1812/1813 are open to and from the CA SiteMinder Policy Server.
- 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 CA SiteMinder using the RADIUS protocol requires:

- Synchronizing users stores to SAS
- Authenticator assignment in SAS
- Adding CA SiteMinder 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 the SafeNet Authentication Service Subscriber Account Operator Guide:


All SafeNet Authentication Service documentation can be found on the SafeNet Implementation Guide web page.
Authenticator Assignment in SAS

SAS supports a number of authentication methods that can be used as a second authentication factor for users who are authenticating through CA SiteMinder.

The following authenticators are supported:

- eToken PASS
- RB-1 Keypad Token
- KT-4 Token
- SMS Token
- MP-1 Software Token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning** – 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 “provisioning” and “provisioning rules” in the SafeNet Authentication Service - Subscriber Account Operator Guide to learn how to provision the different authentication methods to users in the SafeNet Authentication Service User Store.

Adding CA SiteMinder 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 CA SiteMinder. You will need the IP address of CA SiteMinder and the shared secret to be used by both SAS and CA SiteMinder.

To add an Authentication Node in SAS:

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

2. Click the COMMS tab.

3. Select the Auth Nodes module. The Auth Nodes pane is displayed.
4. Click the **Auth Nodes** link. The SAS RADIUS server details are displayed.

   ![Auth Nodes](image1)

   **Auth Nodes**

   Using the RADIUS protocol over the internet provides limited security of the traffic between the organization's data center and the authentication service. For improved security and for alternatives to RADIUS traffic, please refer to the recommendations included in the SafeNet Authentication Service Administrator guide.

   **Add** **Change Log** **Cancel**

   Primary RADIUS Server IP: 109.73.126.149:1812
   Primary SafeNet Authentication Service Agent DNS: agent1.safenet-inc.com:443
   Max. Auth Nodes: 10

   No Records

5. Click **Add**. The **Add Auth Node** pane opens.

   ![Add Auth Node](image2)

6. Complete the following fields, and then click **Save**:

   **Agent Description**
   Enter a host description.

   **Host Name**
   Enter the name of the host that will authenticate with SAS.

   **Low IP Address In Range**
   Enter the IP address of the host or the lowest IP address in a range of addresses that will authenticate with SAS.

   **High IP Address In Range**
   Enter the highest IP address in a range of IP addresses that will authenticate with SAS.

   **Configure FreeRADIUS Synchronization**
   Select this option.

   **Shared Secret**
   Enter the shared secret key.

   **Confirm Shared Secret**
   Re-enter the shared secret key to confirm.
The Auth Node is added to the system.

Checking the SAS RADIUS Address

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

3. Select the Auth Nodes module. The Auth Nodes pane is displayed.

4. Click the Auth Nodes link. The SAS RADIUS server details are displayed.
Configuring CA SiteMinder

To configure RADIUS authentication on a CA SiteMinder Policy Server:
1. Create an Authentication Scheme
2. Create a RADIUS-protected Realm
3. Create a Domain Policy

Creating an Authentication Scheme

In this section, the Authentication Scheme creation will be shown, where SAS RADIUS is configured on the CA SiteMinder Policy Server.

1. Log in to the SiteMinder Administrative UI.

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

The SiteMinder Administrative UI window is displayed.

2. Click the Infrastructure tab.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
3. In the lower tab row, click Authentication. In the left pane, click Authentication Schemes. The Authentication Schemes window is displayed.

4. In the right pane, click Create Authentication Scheme. The Create Authentication Scheme window is displayed.
5. Select **Create a new object of type Authentication Scheme** and then click **OK**. The **Create Authentication Scheme** window is displayed.

6. Fill in the required fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the scheme (for example, RADIUS Login).</td>
</tr>
<tr>
<td>Authentication Scheme Type</td>
<td>Select <strong>RADIUS Server Template</strong>.</td>
</tr>
<tr>
<td>Protection Level</td>
<td>Leave this setting at 5 (default).</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the SAS RADIUS server IP address.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter 1812.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared secret key.</td>
</tr>
<tr>
<td>Confirm Secret</td>
<td>Re-enter the shared secret key to confirm it.</td>
</tr>
</tbody>
</table>
7. Click **Submit**.

The new Authentication Scheme is added and is displayed in the list of schemes.

![Image](image.png)

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

8. Click **Close**.

### Configuring a RADIUS-protected Realm

This section describes the RADIUS-protected Realm configuration, where the resource to be protected by RADIUS authentication is configured.

1. Log in to the SiteMinder Administrative UI.

![Image](image.png)

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
2. In the **SiteMinder Administrative UI** window, in the upper tab row, click **Policies**.

   ![SiteMinder Administrative UI](image1)

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

3. In the lower tab row, click **Domain**, and then, in the left pane, click **Domains**.

   ![SiteMinder Administrative UI](image2)

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

4. To modify your domain, under **User Directories**, click the pencil icon next to the domain’s name.

   ![SiteMinder Administrative UI](image3)

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

5. In the lower tab row, click **Realms**.
6. In the left pane, click **Create Realm**.

   ![Screen capture of SiteMinder Administrative UI](image)

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

7. Complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the realm (for example, RADIUS_realm).</td>
</tr>
<tr>
<td>Agent</td>
<td>Select a web agent (if the agent doesn’t exist, you need to create one by clicking <strong>Create Agent</strong> in the <strong>Lookup Agent/Agent Group</strong> window).</td>
</tr>
<tr>
<td>Resource Filter</td>
<td>Select the virtual directory you want to secure using this realm (for example, /RADIUS/).</td>
</tr>
<tr>
<td>Authentication Scheme</td>
<td>Select the authentication scheme you created previously in the Creating an Authentication Scheme section, page 13.</td>
</tr>
</tbody>
</table>
8. In the **Rules** section, click **Create**.

9. In the **Create Rule** window, complete the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter a name for the rule (for example, <code>protect_all</code>).</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter a description for the rule.</td>
</tr>
<tr>
<td><strong>Resource</strong></td>
<td>Select a resource (you may leave the default value of <code>*</code>).</td>
</tr>
<tr>
<td><strong>Allow/Deny and Enable/Disable</strong></td>
<td>Leave the default value.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Select <strong>Web Agent actions</strong>. In the <strong>Actions</strong> list, select <strong>Get</strong> and <strong>Post</strong>.</td>
</tr>
</tbody>
</table>

10. Click **OK** to save the rule.

11. Click **OK** to save the new realm.

   The new realm is now added to the list of realms in your domain.
12. Click **Submit** to submit the changes to the Policy Server.

**Create a Domain Policy**

In this section, the Domain Policy creation is shown, where the RADIUS authentication policy is being assigned to users in the domain.

1. Log in to the SiteMinder Administrative UI:

   Click **Submit** to submit the changes to the Policy Server.
The **SiteMinder Administrative UI** window is displayed.

2. Click the **Policies** tab.

3. In the lower row, click **Domain** and then, in the left pane, click **Domains**.

4. Click the pencil icon next to the domain’s name to modify your domain.
5. In the lower tab row, click the Policies tab and then click the Create button.

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

6. Click the General tab. In the Name field, enter a name for the policy.

(The screen image above is from CA Technologies. Trademarks are the property of their respective owners.)
7. On the lower tab row, click the **Users** tab and then select the users to whom you want to apply the policy (either by clicking **Add Members** and choosing specific users, or by clicking **Add All**, which will add all users).

8. On the lower tab row, select the **Rules** tab and then, in the **Rules** section, click **Add Rule**.
9. In the **Available Rules** section, select the RADIUS rule created in the Configuring a RADIUS-protected Realm section, page 16, and then click **OK**.

10. Click **OK** again to save the changes.

11. Click **Submit** to submit the changes to the Policy Server.

The resource is now protected by CA SiteMinder and SAS RADIUS authentication.
Running the Solution

The following demonstrates how to authenticate to a website protected by CA SiteMinder using a SAS OTP authenticator.

1. Bob opens an Internet browser and browses to a configured website/web Application protected by CA SiteMinder. A login window is displayed.

   ![Login window]

2. Bob enters his user name and then uses his OTP authenticator to generate an OTP, which he will enter into the Password field.

3. After successful authentication, Bob will be redirected to the requested website/web application.
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>Address</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>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Customer Portal</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>