SafeNet Authentication Manager
Integration Guide

Using RADIUS Protocol for Citrix NetScaler 10.5
Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-013238-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>July 2015</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 .......................................................................................................................................................4
Audience............................................................................................................................................................5
RADIUS-based Authentication using SAM ..........................................................................................................5
RADIUS Authentication Flow using SAM ...........................................................................................................5
RADIUS Prerequisites........................................................................................................................................6
Configuring SafeNet Authentication Manager ................................................................................................6
  Synchronizing Users Stores to SAM..................................................................................................................6
  Configuring SAM’s Connector for OTP Authentication....................................................................................7
  Assigning a Token in SAM................................................................................................................................7
  Adding Citrix NetScaler 10.5 as a RADIUS Client in IAS/NPS.........................................................................8
  Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client ....................................................................10
Configuring Citrix NetScaler 10.5 for RADIUS Authentication........................................................................10
Running the Solution..........................................................................................................................................15
Customizing the Citrix NetScaler Logon Page....................................................................................................16
Support Contacts................................................................................................................................................17
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Citrix NetScaler 10.5.

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.

Citrix NetScaler Access Gateway is a secure application and data access solution that provides IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities, and evolving business requirements emphasize the need for a strong authentication approach based on multi-factor authentication.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Citrix NetScaler 10.5 using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure Citrix NetScaler 10.5 to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Citrix NetScaler 10.5 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 the SafeNet Authentication Manager 8.2 Administrator’s Guide.

Citrix NetScaler 10.5 can be configured to support multi-factor authentication in several modes. RADIUS protocol will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- SafeNet Authentication Manager—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—Version 8.2 (HF 493)
- Citrix NetScaler 10.5
Audience

This document is targeted to system administrators who are familiar with Citrix NetScaler 10.5, 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 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 the 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 dataflow of a multi-factor authentication transaction for Citrix NetScaler 10.5.

1. A user attempts to log on to Citrix NetScaler 10.5 using an OTP token.
2. Citrix NetScaler 10.5 sends a RADIUS request with the user’s credentials to SafeNet Authentication Manager for validation.
3. The SAM authentication reply is sent back to Citrix NetScaler 10.5.
4. The user is granted or denied access to Citrix NetScaler 10.5 based on the OTP value calculation results from SAM.
RADIUS Prerequisites

To enable SafeNet Authentication Manager to receive RADIUS requests from Citrix NetScaler 10.5, ensure the following:

- End users can authenticate from the Citrix NetScaler 10.5 environment with a static password before configuring Citrix NetScaler 10.5 to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix NetScaler 10.5.
- 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 the RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Manager

The deployment of multi-factor authentication using SAM with Citrix NetScaler 10.5 using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SAM, page 6
- Configuring SAM’s Connector for OTP Authentication, page 7
- Assigning a Token in SAM, page 7
- Adding Citrix NetScaler 10.5 as a RADIUS Client in IAS/NPS, page 8
Synchronizing Users Stores to SAM

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OSTP, 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 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 the 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 Back-end 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 (Token Policy Object) 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*.

Assigning a Token in SAM

SAM supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Citrix NetScaler 10.5.

The following tokens are supported:

- eToken PASS
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 Citrix NetScaler 10.5 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 Citrix NetScaler 10.5.

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 Citrix NetScaler 10.5.

Citrix NetScaler 10.5 must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Citrix NetScaler 10.5 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.

1. Click **Start > Administrative Tools > Network Policy Server**.
2. From the NPS web console, 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><strong>Enable this RADIUS client</strong></th>
<th>Select this option.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a name for the RADIUS client.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the Citrix NetScaler 10.5 IP address or DNS.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. This entry must match the shared secret that was used when the RADIUS server was configured in Citrix NetScaler 10.5.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret.</td>
</tr>
</tbody>
</table>

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

4. Click **OK**. Citrix NetScaler 10.5 is added as a RADIUS client in NPS.
Configuring SAM’s OTP Plug-In for Microsoft RADIUS Client

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) as 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 Citrix NetScaler 10.5 for RADIUS Authentication

1. Log in to the Citrix NetScaler administrator console.
2. Click the Configuration tab.
3. In the left pane, select NetScaler Gateway > Policies > Authentication > RADIUS.

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
4. Click **Add**. The **Create Authentication RADIUS Policy** window is displayed.

![Create Authentication RADIUS Policy](image_url)

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

5. In the **Name** field, enter a name for the RADIUS policy.

6. Click **+** adjacent to the **Server** field. The **Create Authentication RADIUS Server** window is displayed.

![Create Authentication RADIUS Server](image_url)

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

7. Complete the following fields, and then click **Create**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the RADIUS server.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the RADIUS server name or IP address.</td>
</tr>
<tr>
<td>Secret Key</td>
<td>Enter the RADIUS shared secret.</td>
</tr>
<tr>
<td>Confirm Secret Key</td>
<td>Re-enter the RADIUS shared secret.</td>
</tr>
</tbody>
</table>
8. On the **Create Authentication RADIUS Policy** window, in the **Expression** table, click the **Saved Policy Expressions** menu, and then select **ns_true**.

![Create Authentication RADIUS Policy window](image)

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

9. Click **Create**.

10. On the **Configuration** tab, in the left pane, select **NetScaler Gateway > Virtual Servers**.

![Configuration tab](image)

*(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
11. In the center pane, select the gateway that you created, and then click **Edit**. The **VPN Virtual Server** window is displayed.

![VPN Virtual Server window](image)

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

12. Under **Authentication**, click `+`. The **Choose Type** window is displayed.

![Choose Type window](image)

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

13. Complete the following fields, and then click **Continue**.

<table>
<thead>
<tr>
<th>Choose Policy</th>
<th>Select RADIUS.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Type</td>
<td>Select Secondary.</td>
</tr>
</tbody>
</table>
14. Under **Policy Binding**, from the **Select Policy** menu, select the RADIUS policy that you created in step 4, and then click **Bind**.

![NetScaler VPX (10) Configuration Screen](image)

(\textit{The screen image above is from Citrix®. Trademarks are the property of their respective owners.})

15. Click **Done**.
Running the Solution

Verify the integration solution after you have successfully configured the Citrix NetScaler 10.5 for SAM authentication. In the following solution, the user is enrolled with a MobilePASS token. Additionally, the **Password 1** and **Password 2** fields on the Citrix Access Gateway logon page have been customized. For customization details, see “Customizing the Citrix NetScaler Logon Page” on page 16.

1. From a web browser, browse to the Citrix NetScaler VPX logon page.

   ![Citrix Access Gateway Logon Page](image1)

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

2. Complete the following fields, and then click **Log On**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User name</strong></td>
<td>Enter your user name.</td>
</tr>
<tr>
<td><strong>Windows Password</strong></td>
<td>Enter your Windows password.</td>
</tr>
<tr>
<td><strong>SafeNet Passcode</strong></td>
<td>Generate an OTP using the MobilePASS token, and then enter the OTP in this field.</td>
</tr>
</tbody>
</table>

   ![Citrix Desktop](image2)

   After successful authentication, you are logged in to the Citrix application.
Customizing the Citrix NetScaler Logon Page

When multi-factor authentication is configured on the Citrix Access Gateway Enterprise Edition, the user is prompted for a User name, Password 1, and Password 2 on the logon page. These password field names can be customized as needed. For example, these fields were changed to Windows Password and SafeNet Passcode in “Running the Solution” on page 15.

The following procedure explains how to modify the fields in English (en.xml). For other languages, choose the appropriate xml file for the desired language in step 3, and follow the same procedure.

1. Use SSH to log in to the Citrix NetScaler computer.
2. Navigate to /netscaler/ns_gui/vpn/resources.
3. In the resources folder, locate the en.xml file.
5. Open the en.xml file using a text editor.
6. Search for the Password string, and then replace it with the desired text (for example, Windows Password).

```xml
<Property id="Enter user name" property="title">Enter user name</Property>
<String id="Password">Password</String>
<String id="Password2">Password 2</String>
<String id="Enter password">Enter password</String>
```

7. Search for the Password2 string, and then replace it with the desired text (for example, SafeNet Passcode).
8. Save the xml file.
10. Backup the file login.js.
11. Open the login.js file using a text editor.
12. Search for the following line:
   ```javascript
   if ( pwc == 2 ) { document.write('&nbsp;1'); }
   ```
13. Delete the 1 character, and then save the js file.

The changes to the logon page are shown below.

![Before Customization](image1.png) ![After Customization](image2.png)
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>