SafeNet Authentication Manager
Integration Guide

SAM Using RADIUS Protocol for Citrix GoToMyPC
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 GoToMyPC as a RADIUS Client in IAS/NPS .................................................... 8
  SAM’s OTP Plug-in for Microsoft RADIUS Client Configuration ....................................... 10
Configuring Citrix GoToMyPC .................................................................................................. 10
  Configuring the GoToMyPC Administration Center for RADIUS Authentication ................. 10
  Configuring the GoToMyPC Client to Authenticate with RADIUS Protocol ....................... 13
Running the Solution ............................................................................................................... 16
Support Contacts ..................................................................................................................... 19
Third-Party Software Acknowledgement

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

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 GoToMyPC is a remote control software service that enables the user to operate their computer from another computer, over the Internet. The software allows a desktop view of a host computer to be manipulated from a client computer that is connected through a TCP/IP network. GoToMyPC extended that software model by using the Internet for connectivity, protecting transmissions with high-security encryption and multiple passwords. By combining a web-hosted subscription service with software installed on the host computer, transmissions could be passed through highly restrictive firewalls.

This document describes how to:

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

It is assumed that the Citrix GoToMyPC 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 GoToMyPC 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 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 GoToMyPC—Corporate Edition only
Audience

This document is targeted to system administrators who are familiar with Citrix GoToMyPC, 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 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 GoToMyPC.

1. A user attempts to log on to Citrix GoToMyPC using an OTP token.
2. Citrix GoToMyPC 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 GoToMyPC.
4. The user is granted or denied access to Citrix GoToMyPC based on the OTP value calculation results from SAM, and is connected to Citrix GoToMyPC.
RADIUS Prerequisites

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

- End users can authenticate from the Citrix GoToMyPC environment with a static password before configuring Citrix GoToMyPC to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix GoToMyPC.
- 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 GoToMyPC 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 GoToMyPC as a RADIUS Client in IAS/NPS, page 8
- SAM’s OTP Plug-in for Microsoft RADIUS Client Configuration, page 10

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 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 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 GoToMyPC.

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 personnel 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 GoToMyPC 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 GoToMyPC.

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 GoToMyPC.

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

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>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 name for the RADIUS client.</td>
</tr>
<tr>
<td>Address (IP or DNS)</td>
<td>Enter the Citrix GoToMyPC IP address or DNS.</td>
</tr>
<tr>
<td>Manual/Generate</td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td>Shared secret</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 GoToMyPC.</td>
</tr>
<tr>
<td>Confirm shared secret</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 GoToMyPC 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) 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 GoToMyPC

For this integration, configuring Citrix GoToMyPC requires the following:

- Configuring the GoToMyPC Administration Center for RADIUS Authentication., page Error! Bookmark not defined.
- Configuring the GoToMyPC Client to Authenticate with RADIUS Protocol, page 13

Configuring the GoToMyPC Administration Center for RADIUS Authentication.

1. Browse to the GoToMyPC Administration Center Secure Login page (https://www.gotomypc.com/members/login), and then log in.

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

3. Under **Groups and Subgroups**, select the group to add RADIUS authentication to.
4. Under **Group Settings**, click **Extended Authentication**.

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
5. Under **Extended Authentication**, in the **Host Authentication** section, click **RADIUS Configuration**.

6. Depending on your organization’s needs, select either **At each host PC** or **In Administration Center > RADIUS Domain**.

7. Click **Save Settings**.

### Configuring the GoToMyPC Client to Authenticate with RADIUS Protocol

Before proceeding, make sure that GoToMyPC Client is installed on the client machine.

1. Right-click the **GoToMyPC** icon in the system tray, and then select **Preferences**.

   (The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
2. On the **Preferences** window, click the **Authentication** tab.

![Preferences window]

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

3. Click **Configure RADIUS**.

4. On the **Configure RADIUS** window, enter the RADIUS server(s) (Primary and Secondary), and then enter the **Encryption key** (this is the shared secret configured on page 9, step 3).

![Configure RADIUS window]

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

5. To test the RADIUS authentication, you can add a user name with a valid token, click **Test Configuration**, enter the user's OTP, and then click **OK**.

![Test RADIUS Configuration window]

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
6. If the test passes, a successful message is displayed. Click **OK**.

![RADIUS Test Succeeded](image)

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

7. Click **OK** until all of the GoToMyPC windows are closed.
Running the Solution

Verify the integration solution after you have successfully configured Citrix GoToMyPC for SAM authentication.

1. Connect to your desktop via Citrix GoToMyPC. Browse to the Citrix GoToMyPC Secure Login page (https://www.gotomypc.com/users/login).

(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)
2. Choose the machine to connect to, and then click **Connect**.

![GoToMyPC](image1)

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

3. The **Opening GoToMyPC Launcher.exe** window is displayed. Save the file, and then launch the .exe.

![Opening GoToMyPC Launcher.exe](image2)

*(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)*
4. On the **Authentication** window, enter your unique password in the **Access Code** field, your OTP in the **RADIUS Credentials** field, and then click **OK**.

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

5. After successful authentication, the desktop is launched.

(The screen image above is from Windows®. Trademarks are the property of their respective owners.)
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></td>
<td></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><strong>Customer Portal</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td>Existing customers</td>
<td>with a Technical Support Customer Portal account can log</td>
</tr>
<tr>
<td></td>
<td>in to manage incidents, get the latest software upgrades,</td>
</tr>
<tr>
<td></td>
<td>and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>
