SafeNet Authentication Service
Integration Guide

Using RADIUS Protocol for Citrix GoToMyPC
Contents

Third-Party Software Acknowledgement .............................................................................................................. 4
Description .................................................................................................................................................................. 4
Applicability ................................................................................................................................................................. 4
Environment .................................................................................................................................................................. 5
Audience ....................................................................................................................................................................... 5
RADIUS-based Authentication using SAS Cloud ...................................................................................................... 5
RADIUS-based Authentication using SAS-SPE and SAS-PCE ............................................................................ 6
RADIUS Authentication Dataflow using SAS ........................................................................................................ 6
RADIUS Prerequisites .................................................................................................................................................. 7
Configuring SafeNet Authentication Service ........................................................................................................... 7
  Synchronizing Users Stores to SAS .......................................................................................................................... 7
  Assigning an Authenticator in SAS .......................................................................................................................... 8
  Adding Citrix GoToMyPC as an Authentication Node in SAS .............................................................................. 9
  Checking the SAS RADIUS Address .................................................................................................................. 11
Configuring Citrix GoToMyPC ..................................................................................................................................... 12
  Configuring the GoToMyPC Administration Center for RADIUS Authentication .............................................. 12
  Configuring the GoToMyPC Client to Authenticate with RADIUS Protocol .................................................. 15
Running the Solution .................................................................................................................................................. 17
Support Contacts .......................................................................................................................................................... 20
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 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.

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) authenticators managed by SafeNet Authentication Service.
- Configure Citrix GoToMyPC to work with SafeNet Authentication Service 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 Service.

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 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 – Private Cloud Edition (SAS-PCE)**—Version 3.3.3
- **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 Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

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

![SAS Cloud RADIUS Service](image)

- **Local RADIUS hosted on-premises**—A RADIUS agent is implemented in the customer’s existing 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.

![Local RADIUS on-premises](image)

This document demonstrates the solution using the SAS cloud-hosted RADIUS service.


For more details on how to install and configure FreeRADIUS, refer to the **SafeNet Authentication Service FreeRADIUS Agent Configuration Guide**.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

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 Dataflow 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 Citrix GoToMyPC.

1. A user attempts to log on to a desktop via Citrix GoToMyPC using an OTP authenticator.
2. Citrix GoToMyPC sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS 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 SAS.
RADIUS Prerequisites

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

- End users can authenticate through 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 RADIUS client for encryption, decryption, and digital signatures.

Configuring SafeNet Authentication Service

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

- Synchronizing Users Stores to SAS, page 7
- Assigning an Authenticator in SAS, page 8
- Adding Citrix GoToMyPC as an Authentication Node in SAS, page 9
- Checking the SAS RADIUS Address, page 11

Synchronizing Users Stores to SAS

Before SAS can authenticate any user in your organization, you need to create a user store in SAS that reflects the users who 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” in the SafeNet Authentication Service Subscriber Account Operator Guide:


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

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

The following authenticators are supported:

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

Authenticators can be assigned to users in two ways:

- Manual provisioning—Assign an authenticator to users one at a time.
- 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” in the SafeNet Authentication Service - Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SafeNet Authentication Service User Store.

Adding Citrix GoToMyPC as an Authentication Node in SAS

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

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

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

3. In the Auth Nodes module, click the Auth Nodes link.
4. Under **Auth Nodes**, click **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 (in this case, a range of IP addresses is being used).</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 (in this case, a range of IP addresses is being used).</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.</td>
</tr>
</tbody>
</table>

The authentication node is added to the system.
Checking the SAS RADIUS Address

Before adding SAS as a RADIUS server in Citrix GoToMyPC, check the IP address of the SAS RADIUS server. The IP address will then be added to Citrix GoToMyPC as a RADIUS server later in this document.

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

![SAS RADIUS Address](image)

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

![Auth Nodes](image)

3. In the Auth Nodes module, click the Auth Nodes link.
The SAS RADIUS server details are displayed.

### Configuring Citrix GoToMyPC

For this integration, configuring Citrix GoToMyPC requires the following:

- Configuring the GoToMyPC Administration Center for RADIUS Authentication, page 12
- Configuring the GoToMyPC Client to Authenticate with RADIUS Protocol, page 15

#### Configuring the GoToMyPC Administration Center for RADIUS Authentication

1. Browse to the Citrix GoToMyPC Administration Center (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 **Manage Groups**.

![GoToMyPC Corporate](image1.png)

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

3. Under **Groups and Subgroups**, select the group to add RADIUS authentication to.

![GoToMyPC Corporate](image2.png)

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

![Preference Window](image1.png)

*(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, add the RADIUS server(s) (Primary and Secondary), and then enter the **Encryption key** (this is the shared secret configured in SAS on page 11, step 5).

![Configure RADIUS](image2.png)

*(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 Configuration](image3.png)

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

(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 SAS authentication.

1. Browse to the Citrix GoToMyPC Secure Login page (https://www.gotomypc.com/users/login) and log in.

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

![GoToMyPC Authentication Window](image1.png)

*(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.png)

*(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**.

![Authentication - GoToMyPC](image3.png)

*(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>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>