SafeNet Authentication Manager

Integration Guide

Using RADIUS Protocol for Citrix NetScaler Gateway

gemalto
security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2016 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

Document Part Number: 007-013656-001, Rev. A

Release Date: November 2016

Contents

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

Third-Party Software Acknowledgement

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

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 Gateway is a secure application and data access solution that gives IT administrators a single point for managing access control and limit actions within sessions based on both user identity and the endpoint device. New threats, risks, and vulnerabilities, as well as evolving business requirements, underscore to 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 Gateway using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure Citrix NetScaler Gateway to work with SafeNet Authentication Manager in RADIUS mode.

It is assumed that the Citrix NetScaler Gateway 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 Gateway 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 8.2 HF 493—**A server version of SAM that is used to deploy the solution on-premises in the organization.
- **Citrix NetScaler Gateway—**Version 11.0

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

Audience

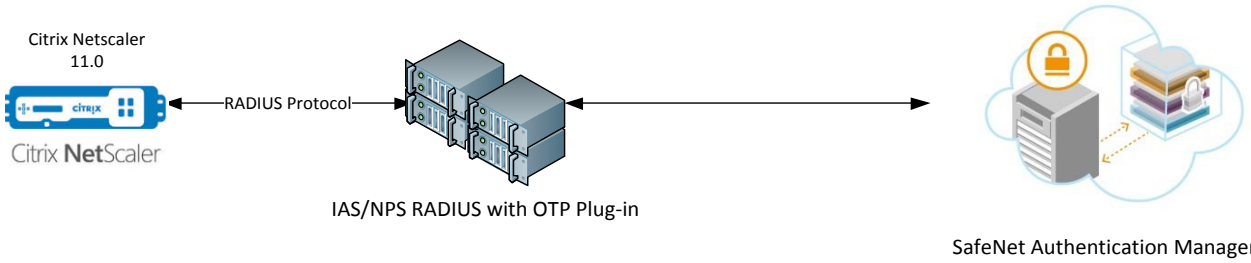
This document is targeted to system administrators who are familiar with Citrix NetScaler Gateway, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager (SAM).

RADIUS-based Authentication using SafeNet Authentication Manager

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 Manage (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.

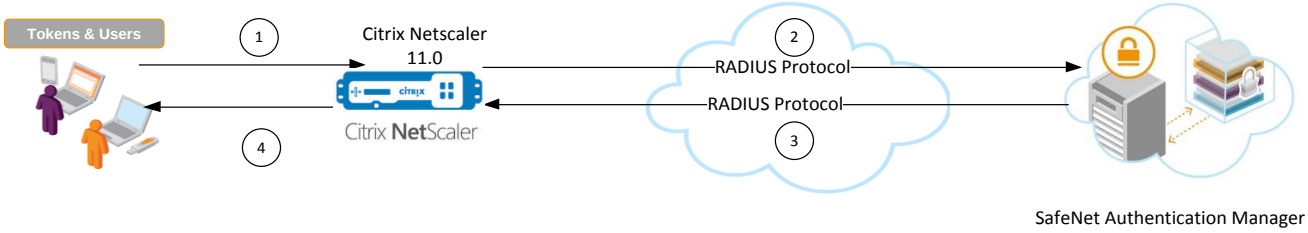


For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to the *SafeNet Authentication Manager 8.2 Administrator`s Guide*.

RADIUS Authentication Flow using SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) 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 Gateway.



1. A user attempts to log on to Citrix NetScaler Gateway using an OTP token.

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

2. Citrix NetScaler Gateway 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 Gateway.
4. The user is granted or denied access to Citrix NetScaler Gateway based on the OTP value calculation results from SAM and is connected to Citrix NetScaler Gateway.

RADIUS Prerequisites

To enable SafeNet Authentication Manager (SAM) to receive RADIUS requests from Citrix NetScaler Gateway, ensure the following:

- End users can authenticate from the Citrix NetScaler Gateway environment with a static password before configuring the Citrix NetScaler Gateway to use RADIUS authentication.
- Ports 1812/1813 are open to and from Citrix NetScaler Gateway.
- 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 Manager

The deployment of multi-factor authentication using SafeNet Authentication Manage (SAM) with Citrix NetScaler Gateway using the RADIUS protocol requires the following:

- Synchronizing Users Stores to SafeNet Authentication Manager, page 6
- Configuring SafeNet Authentication Manager's Connector for OTP Authentication, page 7
- Assigning a Token in SafeNet Authentication Manager , page 4
- Adding Citrix NetScaler Gateway as a RADIUS Client in IAS/NPS, page 8
- Configuring SafeNet Authentication Manager's OTP Plug-In for Microsoft RADIUS Client, page 10

Synchronizing Users Stores to SafeNet Authentication Manager

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 uses an internal ("stand-alone") user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory 2003, 2008, and 2008 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Configuring SafeNet Authentication Manager's Connector for OTP Authentication

SafeNet Authentication Manager (SAM) 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 Token Policy Object (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*.

Assigning a Token in SafeNet Authentication Manager

SafeNet Authentication Manager (SAM) supports a number of OTP authentication methods that can be used as a second authentication factor for users authenticating through Citrix NetScaler Gateway.

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

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

Tokens can be assigned to users as follows:

- **SAM Management Center**—Management site used by SAM administrators and helpdesk 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 NetScaler Gateway 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 Gateway.

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 Gateway.

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

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

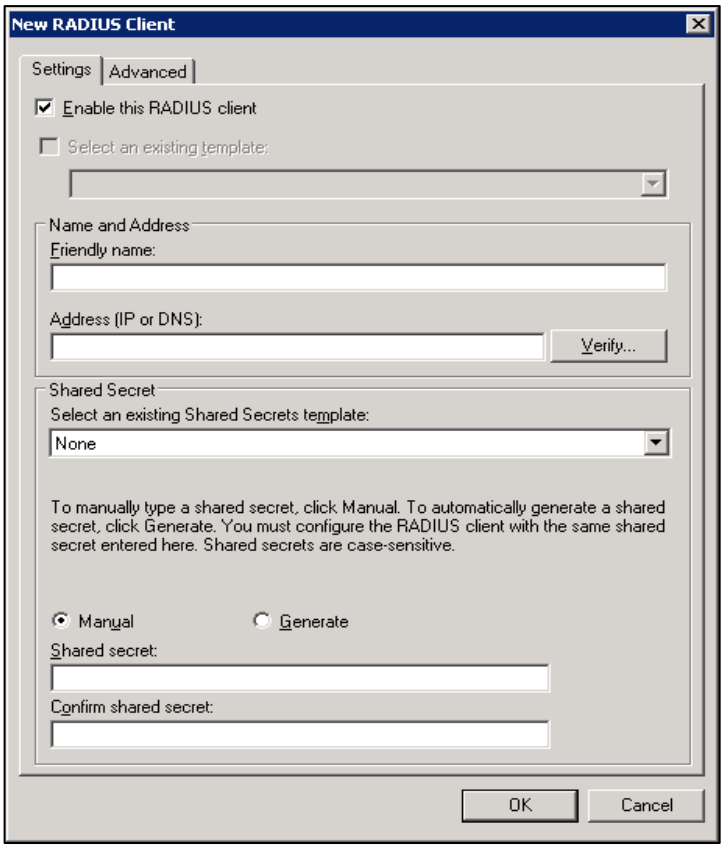
1. Click **Start > Administrative Tools > Network Policy Server**.
2. On the Network Policy Server web console, expand **RADIUS Clients and Servers**, right-click **RADIUS Clients** and then click **New**.

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

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

3. On the **New RADIUS Client** window, on the **Settings** tab, complete the following fields:

Enable this RADIUS client	Select this option.
Friendly name	Enter a RADIUS client name.
Address (IP or DNS)	Enter the Citrix NetScaler Gateway IP address or DNS.
Manual/Generate	Select **Manual**.
Shared secret	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 Gateway.
Confirm shared secret	Re-enter the shared secret to confirm it.



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

4. Click **OK**.

   Citrix NetScaler Gateway is added as a RADIUS client in NPS.

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

Configuring SafeNet Authentication Manager'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.

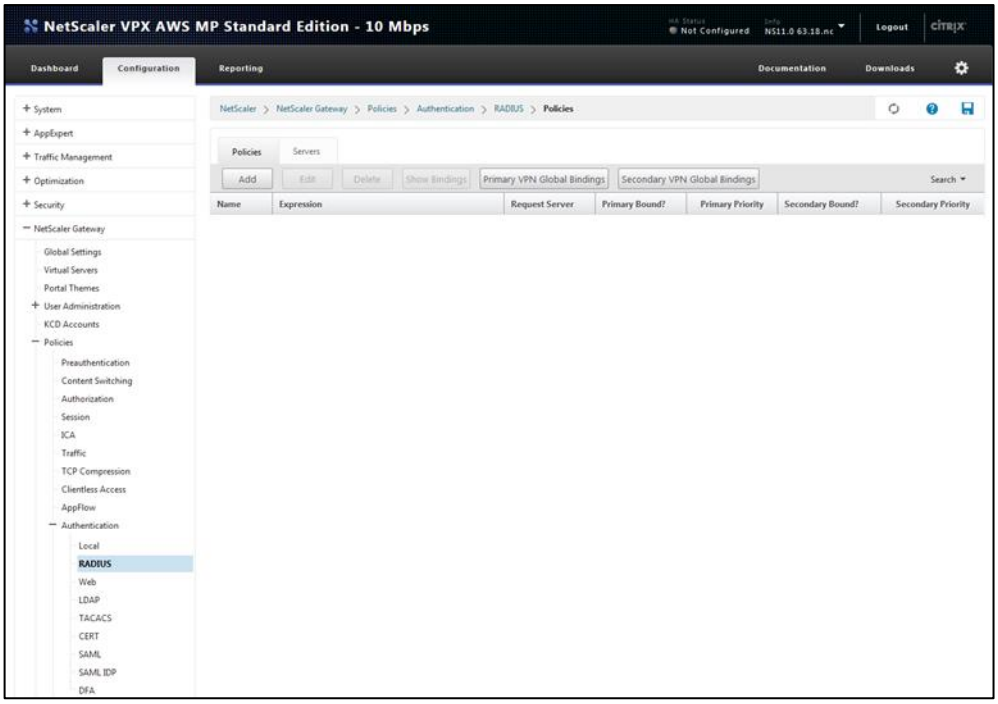
SafeNet Authentication Manager's OTP plug-in for Microsoft RADIUS Client works with Microsoft's IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated 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 Gateway

Configure the Citrix NetScaler Access Gateway to use RADIUS protocol as a secondary authentication method.

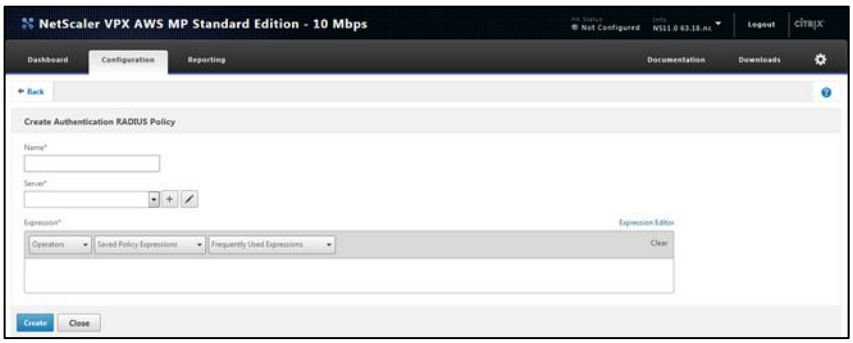
1. Log in to the Citrix NetScaler administrator console.
2. On the Citrix NetScaler administrator console, on the **Configuration** tab, perform the following steps:
   a. In the left pane, click **NetScaler Gateway** > **Policies** > **Authentication** > **RADIUS**.
   b. In the right pane, on the **Servers** tab, click **Add**.



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

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

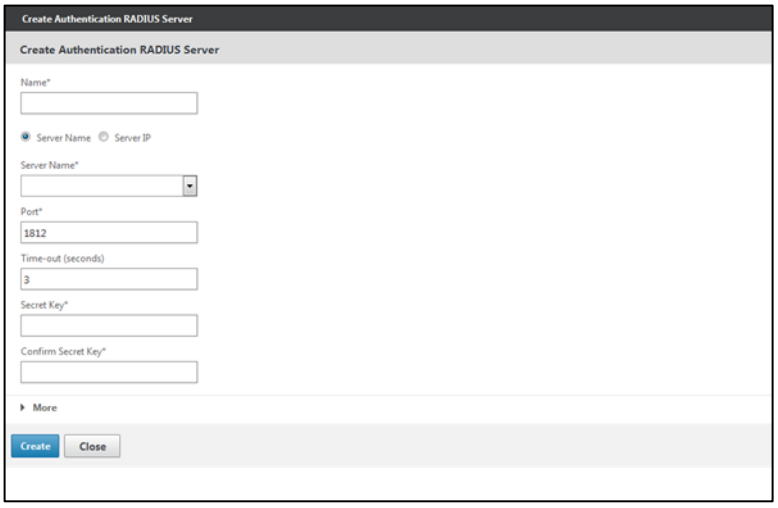
3. On the **Create Authentication RADIUS Policy** window, in the **Name** field, enter a name for the policy.



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

4. In the **Server** field, click the + icon.
5. On the **Create Authentication RADIUS Server** window, complete the following fields, and then click **Create**.

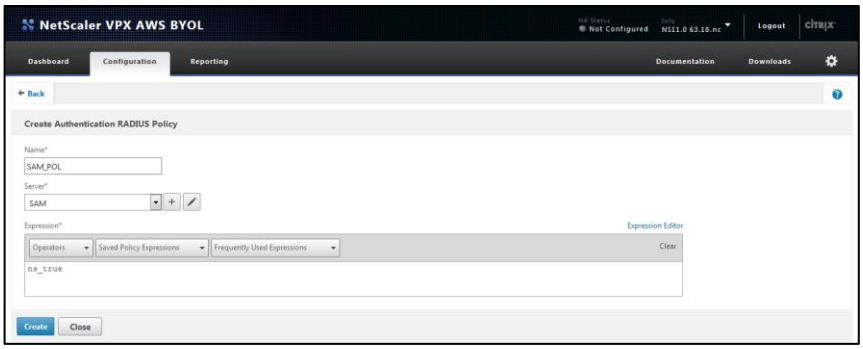
Name	Enter a name for the server.
Server Name/Server IP	Select an option, according to your preferred configuration.
Server Name	Enter the name or IP address of the server, depending on the option selected in the previous field.
Secret Key	Enter the shared secret.
Confirm Secret Key	Re-enter the shared secret.



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

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

6. On the **Create Authentication RADIUS Policy** window, under **Expression**, click **Saved Policy Expressions**, and then select **ns_true**.

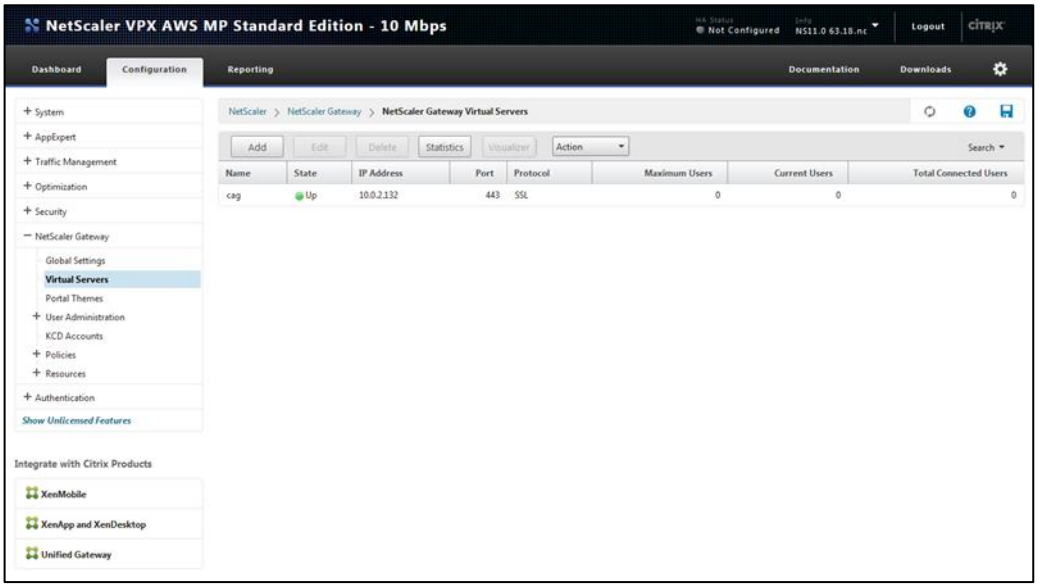


(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

7. Click **Create**.

Now you need to bind the RADIUS authentication to the virtual server.

8. On the **Configuration** tab, in the left pane, click **NetScaler Gateway** > **Virtual Servers**.

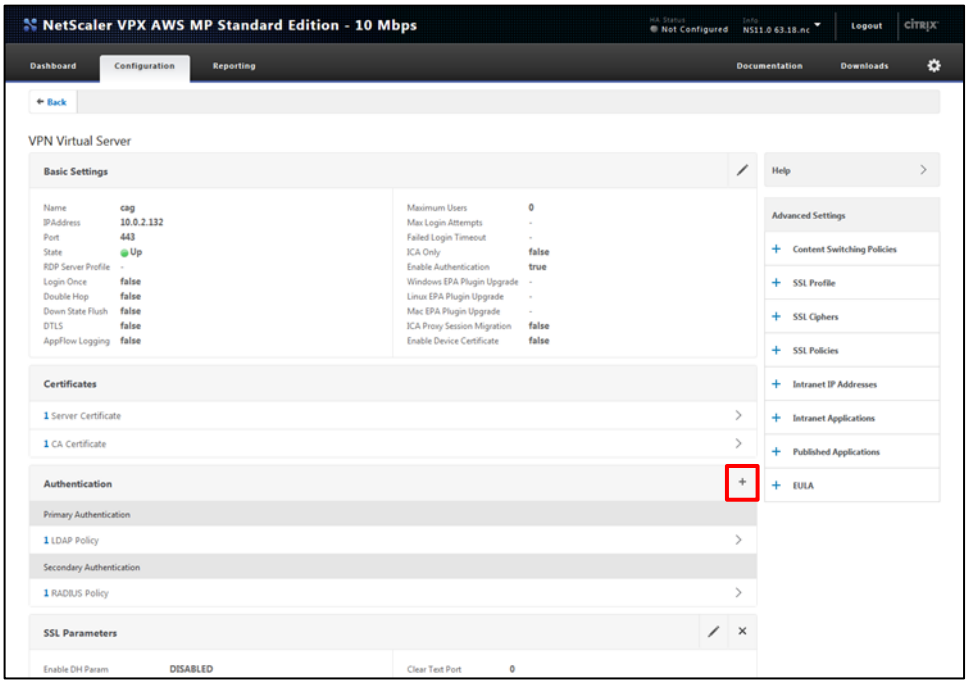


(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

9. In the right pane, select the gateway you created (for example, **cag**), and then click **Edit**.

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

10. On the **VPN Virtual Server** Window, under **Authentication**, click the + icon.



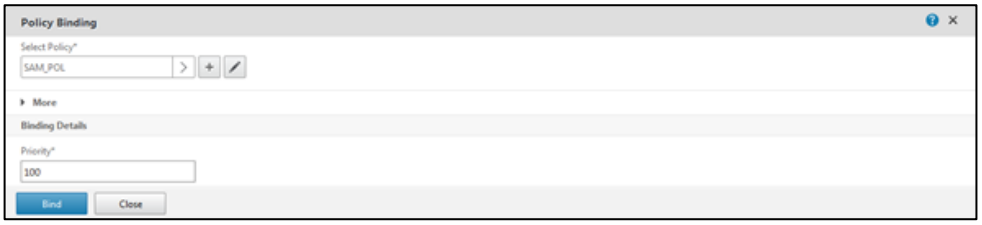
(The screen image above is from Citrix®. Trademarks are the property of their respective owners.)

11. On the **Choose Type** window, under **Policies**, complete the following fields, and then click **Continue**.

Choose Policy	Select **RADIUS**.
Choose Type	Select **Secondary**.

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

12. Under **Policy Binding**, in the **Select Policy** field, select the RADIUS policy that you created earlier in step 3, and then click **Bind**.



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

13. Click **Done**.

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

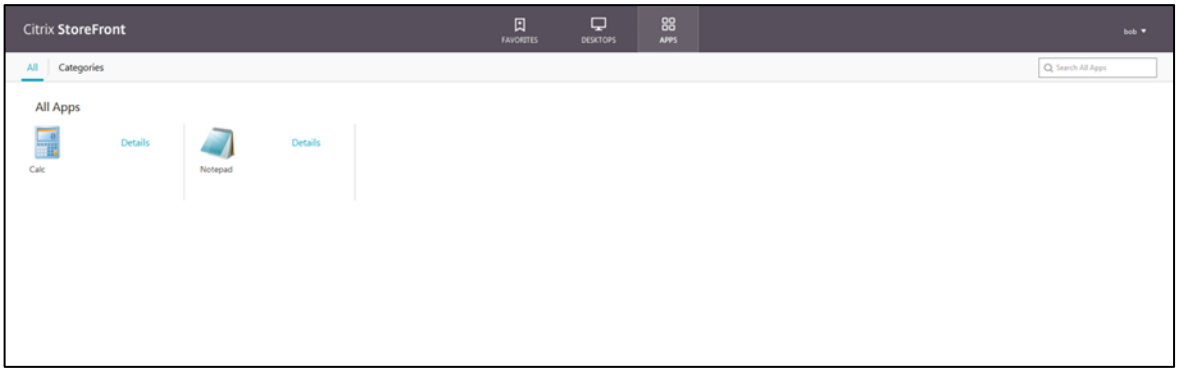
Running the Solution

After Citrix NetScaler Gateway is configured to use RADIUS with SafeNet Authentication Manager (SAM), you can log in to the NetScaler portal.

1. In a web browser, open the Citrix NetScaler Access Gateway login page.
2. On the Citrix NetScaler Access Gateway login page, enter your LDAP credentials and the OTP code, and then click **Log On**.

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

3. After a successful authentication, you will be redirected to access Citrix StoreFront.



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

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

Document PN: 007-013656-001, Rev. A, © Gemalto 2016. All rights reserved. Gemalto, the Gemalto logo, are trademarks and service marks of Gemalto and are registered in certain countries.