SafeNet Authentication Service

Implementation Guide

Citrix Web Interface 5.x

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012523-001, Rev A
Release Date	September 2014

Trademarks

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.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Overview

By default, Citrix Web Interface requires that a user provide a correct user name and password to successfully log on. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password (OTP) generated by a SafeNet token during user authentication.

Applicability

This integration guide is applicable to:

Security Partner Information	
Security Partner	Citrix
Product Name and Version	Citrix Web Interface 5.0, 5.1, 5.2, 5.3
Protection Category	Remote Access

SAS Server	
Authentication Server	SAS Server 2.4 or higher
Network	TCP Port 80 or 443
RADIUS Server	• Microsoft Internet Authentication Server (IAS) Microsoft Network Policy Server (NPS) • Juniper Steel Belted RADIUS Server
Unsupported Token Types	GrIDsure

Prerequisites

- Ensure end users can authenticate through the Citrix Web Interface with a static password before configuring the Citrix to use RADIUS authentication.
- Ensure the SAS server is installed and a user account has been assigned with a SafeNet token.
- SAS Agent for Internet Authentication Service (IAS), Network Policy Server (NPS) or Juniper Steel Belted RADIUS is installed
- Ensure that TCP port 80 or 443 is open between the SAS Agent for Internet Authentication Service (IAS), Network Policy Server (NPS) or Juniper Steel Belted RADIUS, and the SAS Server.
- UDP Port 1812 and 1813 network traffic must be permitted from Citrix Web Interface to the RADIUS server used by SAS.

Configuration

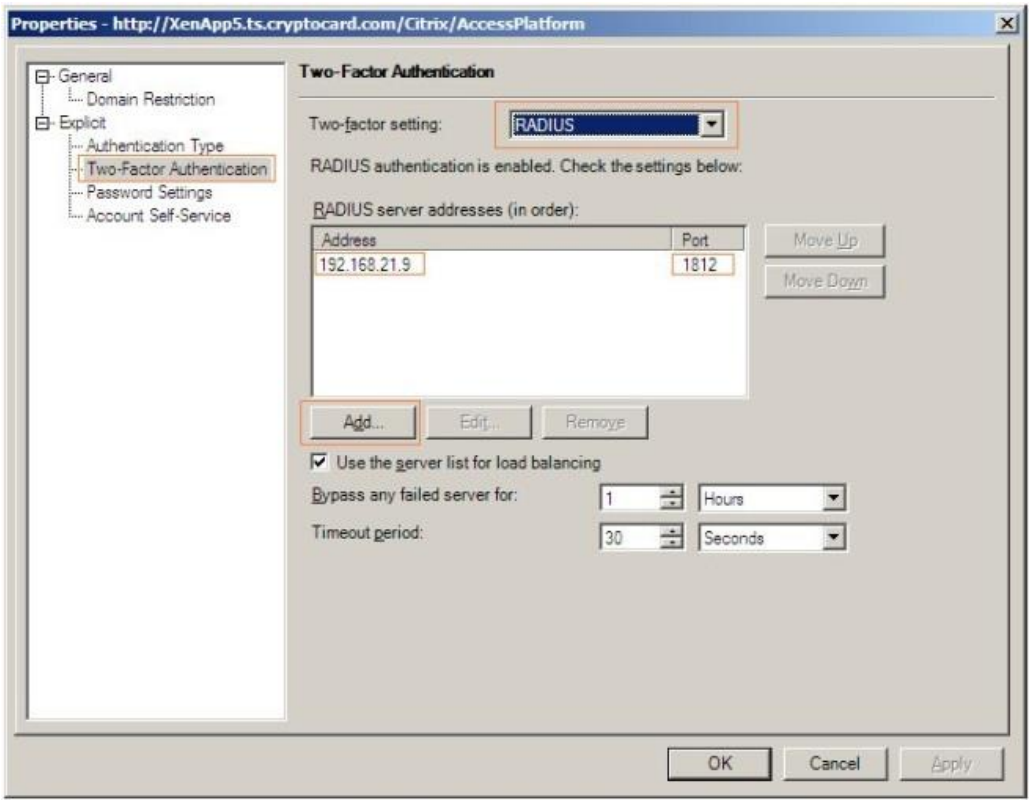
Citrix Web Interface 5.x now supports 2-factor authentication with SAS using its built-in RADIUS authentication support. Configuring SafeNet authentication consists of the following steps:

- **Step 1.** Enable RADIUS authentication and define a RADIUS server using the Citrix Access Management Console.
- **Step 2.** Create a RADIUS shared secret file.
- **Step 3.** Modify the **web.config** file (Citrix Web Interface 5.2/5.3 only)
- **Step 4.** Define Citrix Web Interface as a RADIUS client in Microsoft Internet Authentication Service (IAS) or Network Policy Server (NPS).

Enabling RADIUS Authentication

The SAS Agent for Internet Authentication Service (IAS), Network Policy Server (NPS) or Juniper Steel Belted RADIUS must be defined as a RADIUS server within the Citrix Access Management Console.

1. Launch the Citrix Access Management Console on the Web Interface 5.x server and select the appropriate site.
2. Under **Common Task**, select **Configure Authentication Methods > Explicit**.
3. Click **Properties**.
4. In the **Two-Factor Setting** field, select **RADIUS**.
5. Enter the RADIUS server information used by SAS.



Create a RADIUS Shared Secret File

A shared secret file must be manually created for the RADIUS server defined within the Two-Factor Authentication method.

1. On the Citrix Web Interface server, browse to the **\inetpub\wwwroot\Citrix\sitepath\conf** directory.
2. Create a file called **radius_secret.txt** and enter a shared secret (for example, **testing123**).

Modifying the web.config File(Citrix Web Interface 5.2/5.3 only)

If using Citrix Web Interface 5.2 or 5.3, the following additional steps must be performed:

1. On the Citrix Web Interface server, browse to the **\inetpub\wwwroot\Citrix\sitepath** directory.
2. Open the **web.config** file with a text editor.
3. Search for **RADIUS_NAS_IDENTIFIER** and, for the value, enter **citrixwi**.
4. Search for **RADIUS_NAS_IP_ADDRESS** and, for value, enter the IP address assigned to the Citrix Web Interface server.

Adding the Citrix Web Interface as a RADIUS Client

The following steps will permit RADIUS authentication traffic from the Citrix Web Interface server to the SAS Agent for Internet Authentication Service (IAS) or Network Policy Server (NPS):

1. On the Microsoft Internet Authentication Service (IAS) or Network Policy Server (NPS) server, select **Start > Control Panel > Administrative Tools**.
2. Select **Internet Authentication Service** or **Network Policy Server**.
3. If required, expand **RADIUS Clients and Servers**.
4. Right-click **RADIUS Clients** and select **New RADIUS Client**.
5. Enter the friendly name and IP address or DNS of the Citrix Web Interface server.
6. For **Vendor Name** or **Client-Vendor**, enter **RADIUS Standard**.
7. Enter the shared secret that was entered into the **radius_secret.txt** file.
8. Click **Apply**.
9. Restart the Network Policy Server or Internet Authentication Service for the setting to take effect.
10. Logon to Citrix Web Interface 5.x, entering the one-time password in the **PASSCODE** field.

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 phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 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 SafeNet Knowledge Base.	