

SafeNet Authentication Service Integration Guide

Strong Authentication for Citrix Web Interface 5.x



THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012632-001, Rev A
Release Date	Sept 2010

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.

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

Contents

- Introduction 4
 - Third-Party Software Acknowledgement 4
 - Overview 4
 - Applicability 4
- Prerequisites..... 4
- Configuration 5
 - Enabling RADIUS Authentication 5
 - Create a RADIUS Shared Secret File..... 6
 - Modifying web.config (Citrix Web Interface 5.2/5.3 only) 6
 - Adding Citrix Web Interface as a RADIUS Client 6
- Support Contacts..... 7

Introduction

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Citrix Web Interface 5.x.

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.

Overview

By default, Citrix Web Interface logons 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 generated by a SafeNet token using the implementation instructions below.

Applicability

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

Authentication Service Delivery Platform Compatibility	
SafeNet Authentication Service	All versions

Prerequisites

- Ensure end users can authenticate through Citrix Web Interface with a static password before configuring RADIUS authentication.
- For SAS PCE/SPE:
 - SAS Agent for NPS IAS has been installed and configured on the NPS IAS server to accept RADIUS authentication from the Citrix Web Interface.
 - Ensure that Ports 1812 UDP and 1813 UDP are open to the NPS IAS server.
 - The NPS IAS Agent must be configured to use either port 80 or port 443 to send authentication requests to the SAS server.

- For SAS Cloud:
 - Add a RADIUS Auth Node configured to accept authentication requests from Citrix Web Interface.
- For SAS PCE/SPE or SAS Cloud:
 - Create or define a “Test” account that will be used to verify that Citrix Web Interface has been properly configured. Ensure that the user name for this account exists in SAS by locating it on the **Assignment** tab.
 - Verify that the “Test” user account can successfully authenticate with a static password to Citrix Web Interface before attempting to apply changes and test authentication using a token.
 - A “Test” user account has been created and assigned with a SafeNet token.

Configuration

Citrix Web Interface 5.x now supports two-factor authentication with SAS using its built-in RADIUS authentication support.

Configuring SAS 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

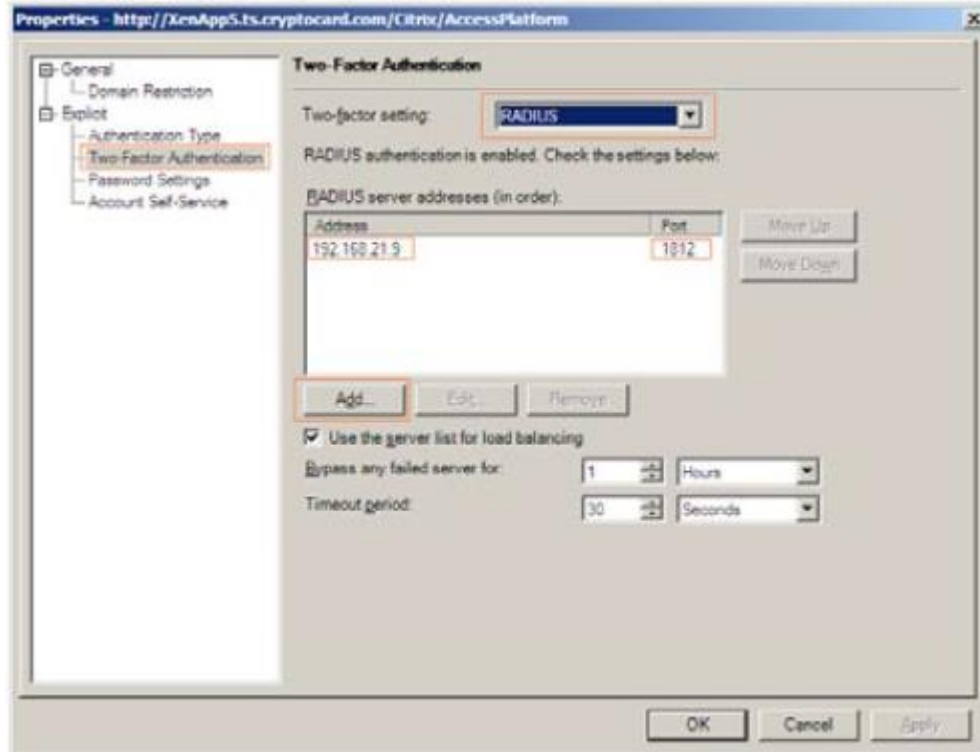
The SAS Agent for Internet Authentication Service (IAS), Network Policy Server (NPS), or Juniper Steel Belted RADIUS must be defined as a RADIUS server within the Citrix Access Management Console.

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 > Two-Factor Authentication** and then select **RADIUS**. Add 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 web.config (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 in the value, enter the IP Address assigned to the Citrix Web Interface server.

Adding 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**, and then launch Internet Authentication Service or Network Policy Server.
2. If required, expand **RADIUS Clients and Servers**. Right-click RADIUS Clients and select New RADIUS Client.

3. Enter the Friendly name and IP Address or DNS of the Citrix Web Interface server.
4. For **Vendor Name** or **Client-Vendor**, enter **RADIUS Standard**.
5. Enter the Shared Secret that was entered into the **radius_secret.txt** file and then apply the setting.
6. Restart the Network Policy Server or Internet Authentication Service for the setting to take effect.
7. Log on 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.

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.	