PINsafe®

SWIVEL®
AUTHENTICATION YOU CAN IDENTIFY WITH

Citrix Web Interface 5.3 Installation Notes

Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.3 web interface.

Acknowledgements

Swivel would like to thank Magnar Johnsen of Firstpoint AS
in their assistance in preparing this documentation.

Prerequisites

This installation guide assumes that a Presentation Server site has been configured with **Explicit** authentication enabled. The customised files provided are based on build **5.3** of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update. Your PINsafe server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Two-factor Authentication.

The following files are required to complete the installation:

1. **pinsafe_image.aspx** – Serves single channel images from PINsafe to users.
2. **login.js** – Customised login page client script.
3. **loginstyle.inc** – Customised login form style.
4. **loginMainForm.inc** – Customised login form.
5. **Constants.java** – Customised login logic constants.
6. **web.config.PINsafe** – Additional configuration entries for PINsafe integration.
7. **Radius_secret.txt** – RADIUS server secret key.

Note: The default Citrix Install path is C:\Inetpub\wwwroot\Citrix\XenApp

Installation

The included files need to be copied to the following locations below the root of the Citrix web interface site. Where an existing file is being replaced ensure you make a backup copy so that the integration can be removed at a later date. The zip file is structured to copy the relevant files to the correct locations. Files in the root of the zip file are not for direct deployment.

1. **pinsafe_image.aspx** to **/auth**.
2. **login.js** to **/auth/clientscripts**.
3. **loginstyle.inc** and **loginMainForm.inc** to **/app_data/include**.
4. **Constants.java** to **/app_code/PagesJava/com/citrix/wi/pageutils**
5. **Radius_secret.txt** to **/Conf**
6. **Ensure file permissions are set correctly on the coped files, Authenticated users need read permissions.**

Make the following adjustments to **/web.config**.

7. Add **/auth/pinsafe_image.aspx** to the comma separated list of URLs under the **<appSettings>** key **AUTH:UNPROTECTED_PAGES**.
8. Copy the additional keys from **web.config.PINsafe** into the **<appSettings>** section. Adjust the key values to reflect your PINsafe installation.
9. Check that the value RADIUS_SECRET_PATH is set to "/radius_secret.txt".
10. Enter a value for RADIUS_NAS_IDENTIFIER. The value can be anything, but it must be at least 3 characters long.

Edit the file \inetpub\wwwroot\sitepath\conf\radius_secret.txt, and enter a secret value of your own choice.

Adjust the PINsafe configuration to allow access from the Citrix server.

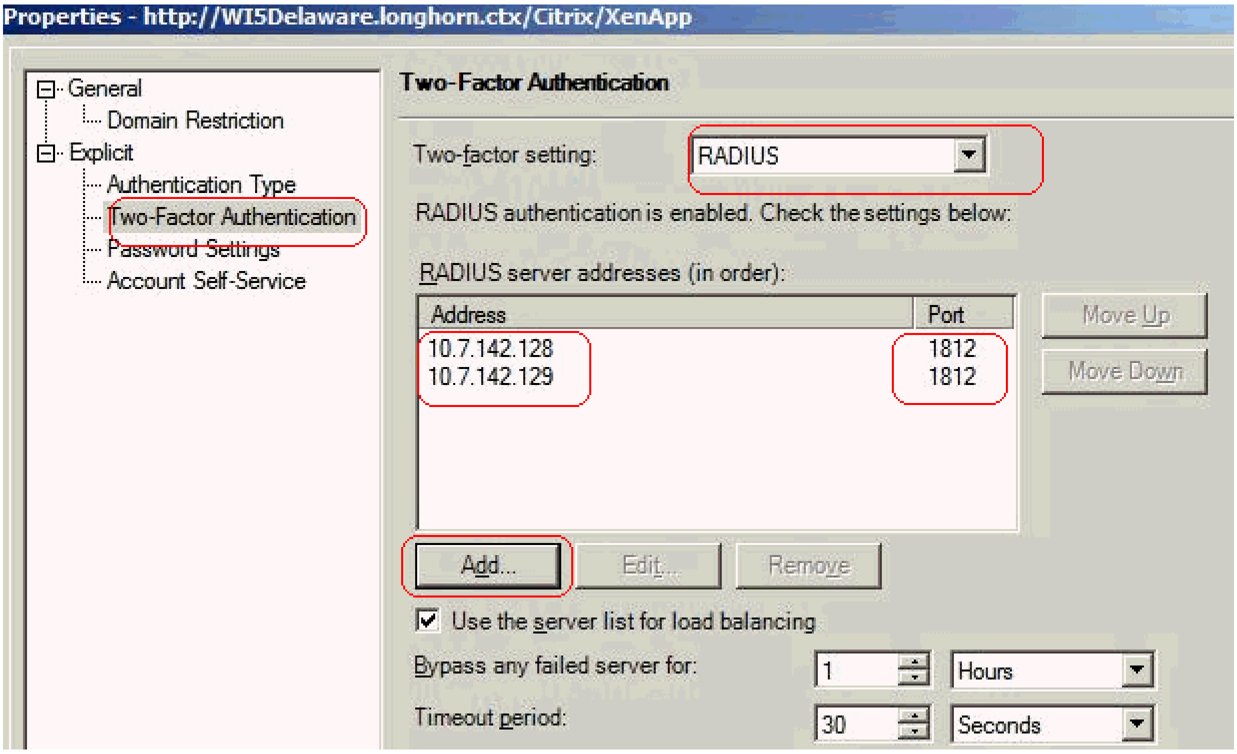
11. Ensure that the RADIUS server is started in PINsafe: under **RADIUS** > **Server**, set Server enabled to Yes.
12. Add an entry in the **RADIUS > NAS** section for the Citrix server. It is suggested, but not required, that you use the RADIUS NAS identifier entered on the web interface as the identifier. Hostname should be the name or IP address of the Citrix server. If you use the name, make sure it can be resolved by DNS. Ensure that the secret entered here is exactly the same as that entered in radius_secret.txt. All other values should be left as defaults, unless you have special requirements, for example, if you want to use two-stage authentication.
13. Enable **Allow session creation with username** in the **Server > Single Channel** section.

Radius Configuration

Web Interface 5.x Configuration

1. Launch the Access Management Console on the Web Interface 5.x server and select the appropriate site. Under Common Tasks, select **Configure Authentication methods > explicit.**

2. Click **Properties > Two-factor authentication**, the select **Radius** from the dropdown list.



Properties - http://WI5Delaware.longhorn.ctx/Citrix/XenApp

Two-Factor Authentication

Two-factor setting: RADIUS

RADIUS authentication is enabled. Check the settings below:

RADIUS server addresses (in order):

Address	Port
10.7.142.128	1812
10.7.142.129	1812

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

3. Configure the PINSAFE server as RADIUS server. If you have more than 1 PINsafe server, you may need to configure all of them in the preferred order. **NOTE:** you cannot use a virtual IP as the RADIUS address, as this will not work.

Verifying Installation

Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a **One Time Code** field and a **Get Code** button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Troubleshooting

If following the installation steps the Citrix web interface fails to display properly edit **web.config** and set the **customErrors mode** to **Off**. This will enable the display of detailed error messages which may assist in troubleshooting.

Check the PINsafe log and Windows application event log on the Citrix server for clues as to what the problem might be.

To verify the Turing image works from the Citrix server, enter the following into a web browser, preferably from the Citrix server, which should display a Turing image if the sever is functioning correctly:

http://<pinsafe_server_ip>:8080/pinsafe/SCImage?username=<username>

Try copying across again the install files checking to ensure that they are not read only. Also check the install files have not been overwritten by the Citrix software.

Additional Information

For assistance in the PINsafe installation and configuration please contact your reseller or email Swivel Secure support at support@swivelsecure.com