

Citrix Web Interface 4.5 Integration

Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 PINsafe Configuration
 - ◆ 5.1 Configuring the PINsafe Agent
 - ◆ 5.2 Enabling Session creation with username
- 6 Citrix Web Interface Configuration
 - ◆ 6.1 Copy across the Web Interface Files
 - ◆ 6.2 Edit the Web.config file
- 7 Additional Configuration Options
 - ◆ 7.1 Optional: Using Static Password
- 8 Testing
- 9 Troubleshooting
 - ◆ 9.1 Error Messages
- 10 Uninstalling
- 11 Known Issues and Limitations
- 12 Additional Information

Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.5 web interface. If the Single Channel Image for authentication is to be used a NAT is not required to the PINsafe server as the Image is proxied through the Web Interface server.

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 4.5.1.8215 of the Citrix web interface, if you have a later version please contact your PINsafe reseller for an update.

The following files are required to complete the installation:

- PINsafeClient.dll ? PINsafe authentication client library.
- login.aspx ? Customised login page.
- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js ? Customised login page client script.
- loginButtons.inc ? Customised login form buttons.
- loginMainForm.inc ? Customised login form.
- loginView.aspxf ? Customised login logic constants.
- login.aspxf ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from [here](#)

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

Baseline

PINsafe 3.5

Citrix Web Interface build 4.5.1.8215

Architecture

The Citrix Web Interface makes authentication requests against the PINsafe server by XML.

PINsafe Configuration

Configuring the PINsafe Agent

On the PINsafe server:

Select Server then Agents, and create an agent for the Web Interface server, required parameters are:

Name: a Descriptive name

Hostname/IP: Web Interface server details

Shared Secret: To be also used on the Web Interface server

Click Apply to save settings.

Enabling Session creation with username

The PINsafe server can be configured so that it returns a Single Channel image by presenting the username via the XML API or the SCIMage servlet.

On the PINsafe server:

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

Click Apply to save settings.

To test your configuration you can use the following URL using a valid PINsafe username:

Virtual or hardware appliance (use 8080/pinsafe and not the proxy port)

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Software install

https://PINsafe_server_IP:8080/pinsafe/SCImage?username=testuser

Citrix Web Interface Configuration

Copy across the Web Interface Files

On the Citrix Web Interface Server:

The following files need to be copied to the listed locations, below the root of the Citrix web interface site. Where an existing file is being replaced and for modified files, ensure you make a backup copy so that the integration can be removed at a later date.

PINsafeClient.dll to /bin.

login.aspx and pinsafe_image.aspx to /auth.

login.js to /auth/clientscripts.

loginButtons.inc and loginMainForm.inc to /app_data/auth/include.

loginView.aspxf and login.aspxf to /app_data/auth/serverscripts.

Ensure file permissions are set correctly on the copied files, Authenticated users need read permissions.

Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

Find the the comma separated list of URLs under the <appSettings> key AUTH:UNPROTECTED_PAGES and add Add /auth/pinsafe_image.aspx to the list.

The web.config.PINsafe file contains additional keys that need to be copied into the <appSettings> section of the web.config file. Adjust the key values to reflect your PINsafe installation.

The default settings are:

```
<add key="PINsafe_SSL" value="false" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

If using a PINsafe virtual or hardware appliance, then the following settings may need to be used.

```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8080" />
<add key="PINsafe_Context" value="pinsafe" />
<add key="PINsafe_Secret" value="" />
```

Additional Configuration Options

Optional: Using Static Password

On the Citrix Web Interface Server:

When using a static PINsafe password with the OTC, edit the login.aspxf file as follows:

change the following line from

```
if (!pc.Login(user, "", etc))
```

to

```
if (!pc.Login(user,password, etc))
```

Testing

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.

Citrix Web Interface with **TURing** image (For SMS do not click on Get Code button)

The screenshot shows a web browser window with the title "Log in". The page contains the following elements:

- User name:** A text input field containing the text "name".
- Password:** A password input field with masked characters (dots).
- One Time Code:** A text input field with a cursor.
- Advanced Options >>>** A link below the input fields.
- Get code** and **Log In** buttons.
- Numeric keypad:** A keypad at the bottom with numbers 1-0. The input fields for the keypad contain handwritten numbers: 2, 8, 1, 3, 5, 6, 2, 0, 7, 4.

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.

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.

Error Messages

Server Error in ~/Citrix/AccessPlatformSwivel? Application

Parser Error Message: An error occurred while parsing EntityName. Line 86, position 63.

Source Error gives line with <add key=?PINsafe_Secret? value=?&&&&&&? />

Source File: c:\inetpub\wwwroot\Citrix\AccessPlatformSwivel\web.config

You cannot use some special characters in the secret key file, such as &</nowiki>

Uninstalling

Copy the backup files made at the start of installation back to their original locations.

Known Issues and Limitations

The integration does not support the use of the virtual or hardware appliance proxy port for Agent-XML authentication, use port 8080 and the context pinsafe.

Additional Information

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