

Citrix Web Interface 4 with Presentation Server 4

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
- 8 Testing
- 9 Troubleshooting
- 10 Uninstalling
- 11 Known Issues and Limitations
- 12 Additional Information

Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix Presentation Server 4 web interface. This also works with Citrix Secure Gateway v3.0. 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 45083 of the Citrix web interface and have been tested with versions 4.0 and 4.2, for later versions 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.cs ? Customised login logic constants.
- login.cs ? Customised login logic.
- web.config.PINsafe ? Additional configuration entries for PINsafe integration.

The files can be downloaded from here: [File:Citrix_PS_4.0_Integration.zip](#)

Note: The default Citrix Install path is C:\inetpub\wwwroot\Citrix\AccessPlatform

Baseline

PINsafe 3.x

Citrix Web Interface build 3.x, 4.0, 4.2

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.cs and login.cs 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 URL's 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" />

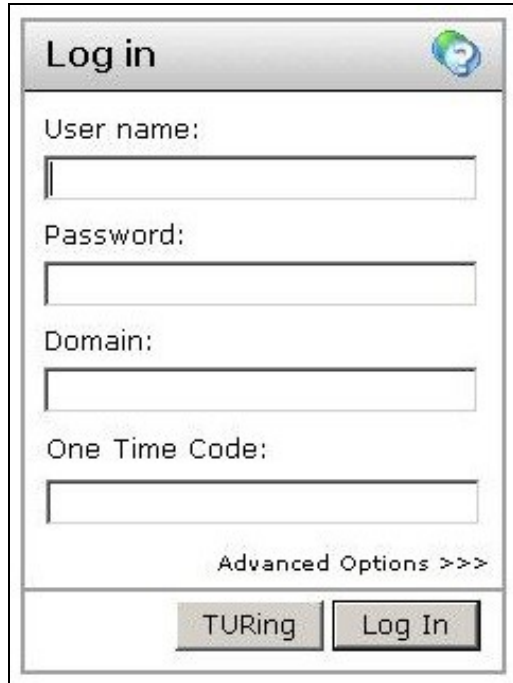
<add key="PINsafe_Secret" value="" />
```

Additional Configuration Options

Testing

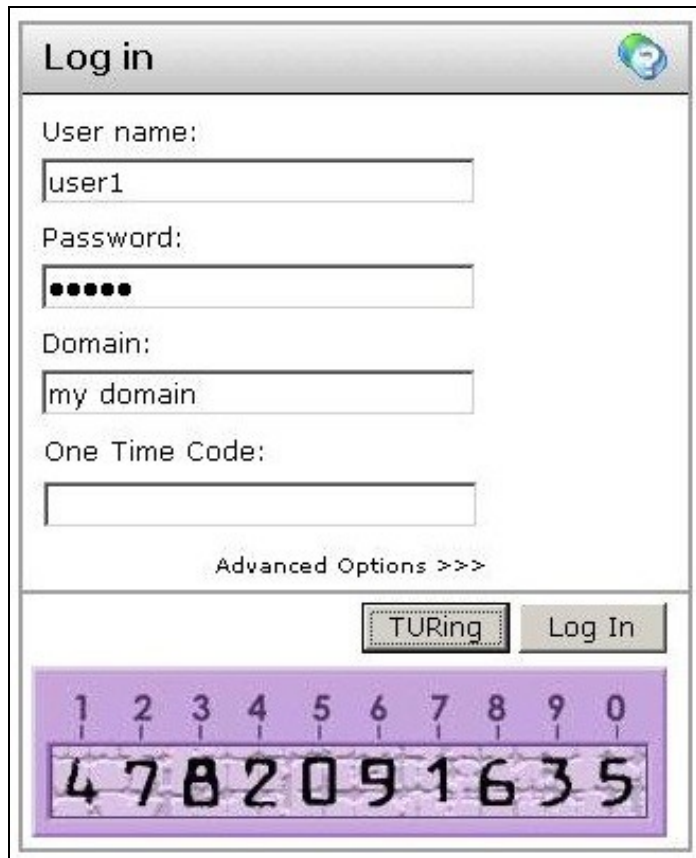
Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered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

Citrix Web Interface login with SMS (Do not click on the Turing Button)



The login form is titled "Log in" and features a Citrix logo in the top right corner. It contains four input fields: "User name:", "Password:", "Domain:", and "One Time Code:". Below the "One Time Code:" field is a link that says "Advanced Options >>>". At the bottom of the form are two buttons: "TURING" and "Log In".

Citrix Web Interface login with Turing



The login form is titled "Log in" and features a Citrix logo in the top right corner. It contains four input fields: "User name:" (with "user1" entered), "Password:" (with "*****" entered), "Domain:" (with "my domain" entered), and "One Time Code:". Below the "One Time Code:" field is a link that says "Advanced Options >>>". At the bottom of the form are two buttons: "TURING" and "Log In". Below the buttons is a purple rectangular area containing a numeric keypad with digits 1 through 0. Below the keypad, the numbers "4 7 8 2 0 9 1 6 3 5" are displayed in a large, bold font.

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.

Uninstalling

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

Known Issues and Limitations

Self signed certificates are not supported with this version of the integration, either use a valid certificate, or non SSL communications or upgrade the Web Interface version.

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