

# Citrix Web Interface 5.0 Integration

## Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Swivel Configuration
  - ◆ 5.1 Configuring the RADIUS server
  - ◆ 5.2 Enabling Session creation with username
    - ◇ 5.2.1 Setting up Swivel Dual Channel Transports
  - ◆ 5.3 Citrix Web Interface Configuration
    - ◇ 5.3.1 Copy accros the Web Interface Files
    - ◇ 5.3.2 Edit the Radius\_secret.txt
    - ◇ 5.3.3 Edit the Web.config file
    - ◇ 5.3.4 Citrix Web Interface RADIUS Configuration
  - ◆ 5.4 Additional Configuration Options
  - ◆ 5.5 Testing
  - ◆ 5.6 Uninstalling
  - ◆ 5.7 Troubleshooting
    - ◇ 5.7.1 Error Messages
  - ◆ 5.8 Known Issues and Limitations
  - ◆ 5.9 Additional Information

## Introduction

This document outlines the necessary steps to integrate Swivel authentication into the Citrix 5.0 web interface. If the Single Channel Image for authentication is to be used, a NAT is not required to the Swivel 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 5.0.1.29110 of the Citrix web interface, if you have a later version please contact your Swivel reseller for an update. Your Swivel server must be configured for radius authentication and your Citrix Web interface must be using RADIUS for Authentication.

The following files are required to complete the installation:

- PINsafeClient.dll ? Swivel authentication client library.
- include.aspxf ? Customised include file.
- pinsafe\_image.aspx ? Serves single channel images from Swivel to users.
- login.js ? Customised login page client script.
- loginstyle.inc ? Customised login form style.
- loginMainForm.inc ? Customised login form.
- Constants.java ? Customised login logic constants.
- web.config.PINsafe ? Additional configuration entries for Swivel integration.
- Radius\_secret.txt ? RADIUS server secret key.

The files can be downloaded from here: [File:Citrix\\_WI\\_5.0\\_Integration.zip](#)

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

## Baseline

Swivel 3.5

Citrix Web Interface build 5.0.1.29110

## Architecture

The Citrix Web Interface makes authentication requests against the Swivel server by RADIUS.

## Swivel Configuration

### Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see [RADIUS Configuration](#)

### Enabling Session creation with username

To allow the TURing image, PINpad and other single channel images, under Server/Single Channel set [Allow session request by username](#) to Yes.

## Setting up Swivel Dual Channel Transports

See [Transport Configuration](#)

## Citrix Web Interface Configuration

### Copy across the Web Interface Files

The required files (see prerequisites) need to be copied to the following 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. Move any backup copy files to a separate location. Do NOT rename the file and leave it in place within the same directory.

PINsafeClient.dll to /bin.

include.aspx to /app\_data/serverscripts

pinsafe\_image.aspx to /auth.

login.js to /auth/clientscripts.

loginstyle.inc and loginMainForm.inc to /app\_data/include.

Constants.java to /app\_code/PagesJava/com/citrix/wi/pageutils

Radius\_secret.txt to /

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

### Edit the Radius\_secret.txt

On the Citrix Web Interface server

Edit the radius\_secret.txt file so that it has the same shared secret as has been entered on the Swivel server.

### 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 coied into the <appSettings> section of the web.config file. Adjust the key values to reflect your Swivel 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 Swivel virtual or hardware appliance, then the following settings may need to be used.

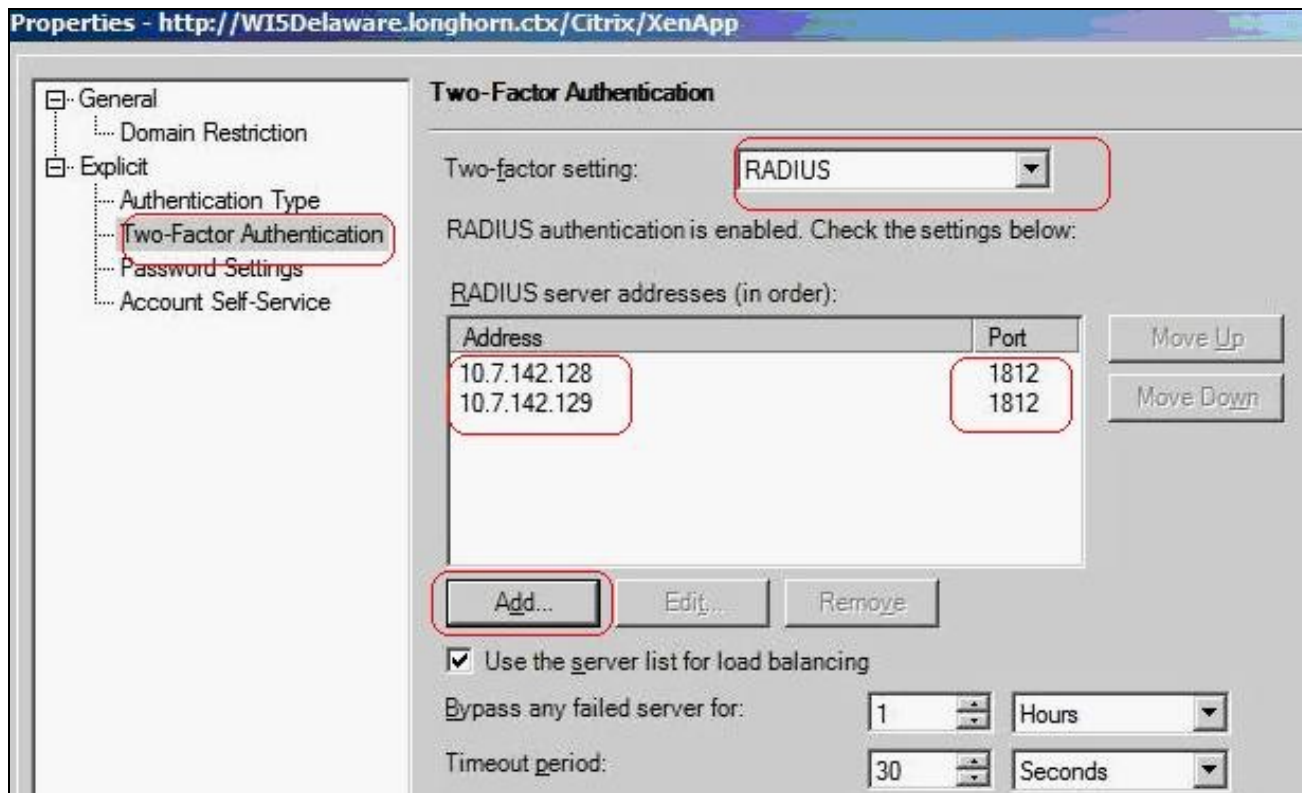
```
<add key="PINsafe_SSL" value="true" />
<add key="PINsafe_Server" value="192.168.2.254" />
<add key="PINsafe_Port" value="8443" />
<add key="PINsafe_Context" value="proxy" />
<add key="PINsafe_Secret" value="" />
```

## Citrix Web Interface RADIUS Configuration

On the Citrix Web Interface server:

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.

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



## Additional Configuration Options

see [Citrix Web Interface 5.X additional login page 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 Swivel one time code is entered in addition to the Citrix credentials should the user be logged in.

## Uninstalling

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

On the Citrix Web Interface server:

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.

Click Properties > Two-factor authentication, then select Radius from the dropdown list. Remove the Swivel RADIUS entries.

## Troubleshooting

Check the Swivel logs for any error messages, or absence of session starts and RADIUS requests.

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:

For a Swivel virtual or hardware appliance:

`https://<pinsafe_server_ip>:8443/proxy/SCImage?username=<username>`

For a software only install see [Software Only Installation](#)

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.

If the virtual or hardware appliance is using a self signed certificate it may be necessary turn off https connections between the virtual or hardware appliance and the Citrix server.

If a red cross appears, possible causes may be:

- Self Signed Certificate, either install a valid certificate on the Swivel server or for testing the client can accept the certificate (load Image URL into browser)
- Swivel server not accessible, check networking and firewalls. Check the Swivel server logs for a session started message.
- Incorrect Swivel URL, either http, IP/hostname or context (pinsafe or proxy). Right click on the red cross and view the properties

## **Error Messages**

**INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - MESSAGE AUTHENTICATOR IS INCORRECT**

This indicates that the shared secret on the access device and the Swivel NAS setting do not match.

**INFO RADIUS: <0> Access-Request(1) LEN=78 192.168.1.1:4175 PACKET DROPPED - Duplicate packet from NAS**

When an authentication fails the RADIUS client may retry sending additional authentication requests. Resolve the initial issue causing the failure.

## **Known Issues and Limitations**

Upgrading the Citrix Web Interface will overwrite the Swivel settings and files so the Swivel integration may need to be applied again.

## **Additional Information**

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at [support@swivelsecure.com](mailto:support@swivelsecure.com)