Citrix Web Interface 5.3 Integration

Contents

Introduction

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

The following files are required to complete the installation:

- pinsafe_image.aspx ? Serves single channel images from PINsafe 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 PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

The files can be downloaded from here

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

PINsafe uses .NET so is not dependant on the OS being 32 bit or 64 bit.

Baseline

PINsafe 3.5

Citrix Web Interface build 5.3

Architecture

The Citrix Web Interface makes authentication requests against the PINsafe 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 PINsafe 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.

include.aspxf 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 /Conf

Ensure file permissions are set correctly on the coped 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 PINsafe 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 copied into the <appSettings> section of the web.config file (not the <switches> section). Adjust the key values to reflect your PINsafe installation.

Note: The setting <add key="RADIUS_NAS_IDENTIFIER" value="" /> is present in the file and needs to be set to <add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

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

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<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="" />

<add key="PINsafe_AcceptSelfSigned" value="True" />
```

The settings for a software install of PINsafe are:

```
<add key="RADIUS_SECRET_PATH" value="/radius_secret.txt" />

<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />

<add key="PINsafe_SSL" value="false" />

<add key="PINsafe_Server" value="192.168.2.254" />
```

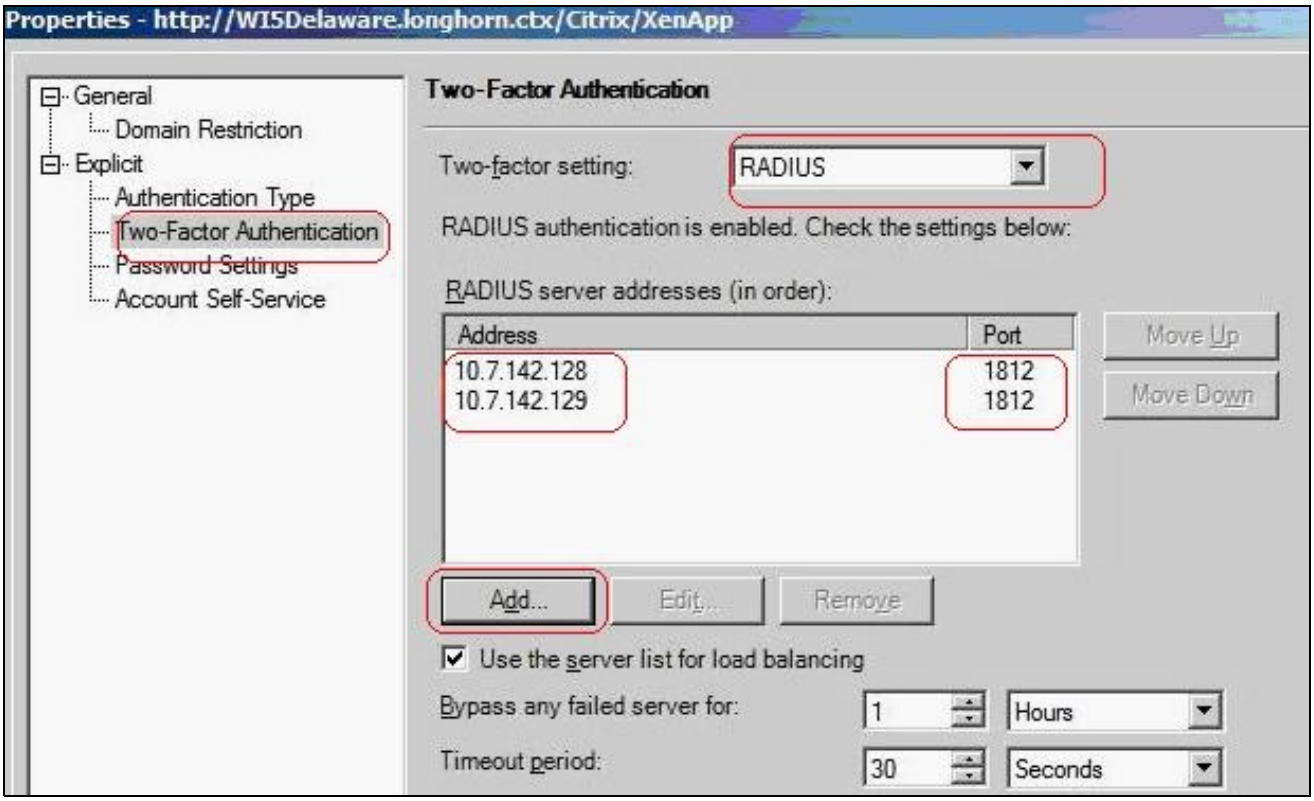
```
<add key="PINsafe_Port" value="8080" />

<add key="PINsafe_Context" value="pinsafe" />

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

<add key="PINsafe_AcceptSelfSigned" value="false" />
```

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 drop down list.



Configure the PINSAFE server as RADIUS server. If you have more than one 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.

Additional Configuration Options

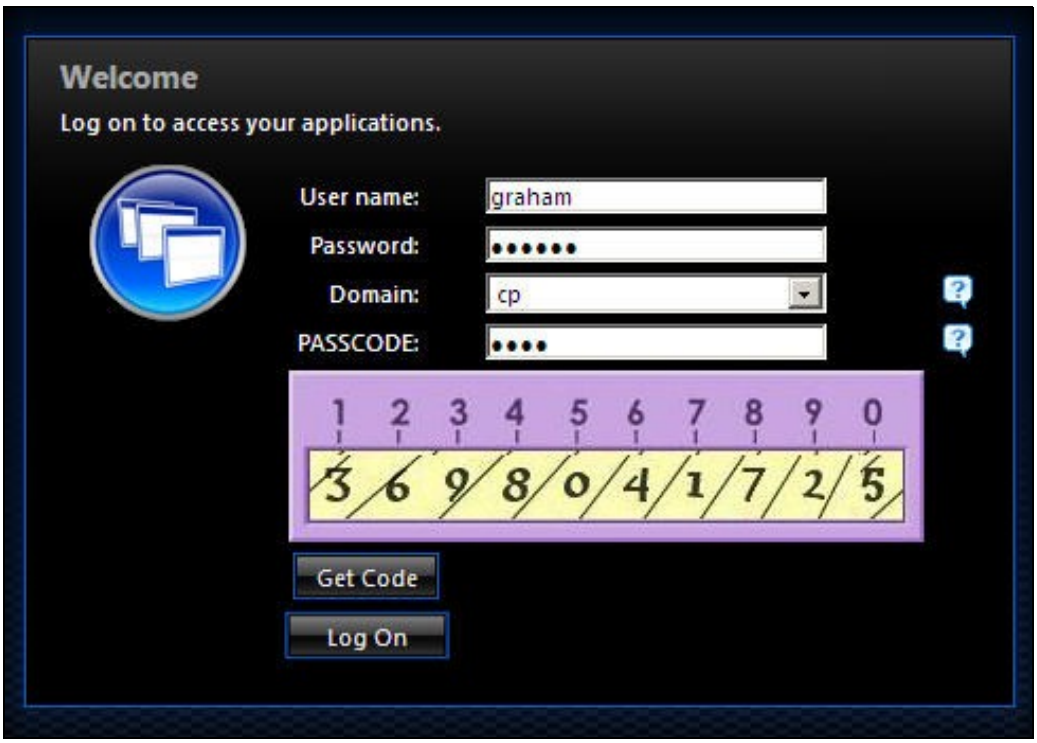
see Citrix Xen App 5.x additional login page options

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 PINsafe one time code is entered in addition to the Citrix credentials should the user be logged in.

Login using Dual channel authentication

Login Using Single Channel Graphical Turing Image



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 drop down list. Remove the PINsafe RADIUS entries.

Troubleshooting

Check the PINsafe 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 PINsafe 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 PINsafe server or for testing the client can accept the certificate (load Image URL into browser)
- PINsafe server not accessible, check networking and firewalls. Check the PINsafe server logs for a session started message.
- Incorrect PINsafe 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 PINsafe 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 PINsafe settings and files so the PINsafe integration may need to be applied again.

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