

Table of Contents

1 Citrix Web Interface 5.1 Integration.....	1
2 Introduction.....	2
3 Prerequisites.....	3
4 Baseline.....	4
5 Architecture.....	5
6 Swivel Configuration.....	6
6.1 Configuring the RADIUS server.....	6
6.2 Enabling Session creation with username.....	6
6.3 Setting up PINsafe Dual Channel Transports.....	6
7 Citrix Web Interface Configuration.....	7
7.1 Copy across the Web Interface Files.....	7
7.2 Edit the Radius_secret.txt.....	7
7.3 Edit the Web.config file.....	7
7.4 Citrix Web Interface RADIUS Configuration.....	7
8 Additional Configuration Options.....	9
8.1 Self Reset.....	9
9 Testing.....	10
10 Uninstalling.....	11
11 Troubleshooting.....	12
11.1 Error Messages.....	12
12 Known Issues and Limitations.....	13
13 Additional Information.....	14
14 Citrix Web Interface 5.2 Integration.....	15
15 Introduction.....	16
16 Prerequisites.....	17
17 Baseline.....	18
18 Architecture.....	19
19 Swivel Configuration.....	20
19.1 Configuring the RADIUS server.....	20
19.2 Enabling Session creation with username.....	20
19.3 Setting up PINsafe Dual Channel Transports.....	20
20 Citrix Web Interface Configuration.....	21
20.1 Copy across the Web Interface Files.....	21
20.2 Edit the Radius_secret.txt.....	21
20.3 Edit the Web.config file.....	21
20.4 Citrix Web Interface RADIUS Configuration.....	22
21 Additional Configuration Options.....	23
22 Testing.....	24
23 Uninstalling.....	25
24 Troubleshooting.....	26
24.1 Error Messages.....	26
25 Known Issues and Limitations.....	27
26 Additional Information.....	28
27 Citrix Web Interface 5.3 Integration.....	29
28 Introduction.....	30
29 Prerequisites.....	31
30 Baseline.....	32
31 Architecture.....	33
32 Swivel Configuration.....	34
32.1 Configuring the RADIUS server.....	34
32.2 Enabling Session creation with username.....	34
32.3 Setting up PINsafe Dual Channel Transports.....	34

Table of Contents

33 Citrix Web Interface Configuration.....	35
33.1 Copy across the Web Interface Files.....	35
33.2 Edit the Radius_secret.txt.....	35
33.3 Edit the Web.config file.....	35
33.4 Citrix Web Interface RADIUS Configuration.....	36
34 Additional Configuration Options.....	37
35 Testing.....	38
36 Uninstalling.....	39
37 Troubleshooting.....	40
37.1 Error Messages.....	40
38 Known Issues and Limitations.....	41
39 Additional Information.....	42
40 Citrix Web Interface 5.4 Integration.....	43
41 Introduction.....	44
42 Prerequisites.....	45
43 Baseline.....	46
44 Architecture.....	47
45 Swivel Configuration.....	48
45.1 Configuring the RADIUS server.....	48
45.2 Enabling Session creation with username.....	48
46 Citrix Web Interface Configuration.....	49
46.1 Edit the radius_secret.txt.....	49
46.2 Edit the web.config file.....	49
46.3 Citrix Web Interface RADIUS Configuration.....	49
47 Additional Configuration Options.....	51
47.1 Changing the OTC label.....	51
47.2 Configuring Single Channel: Modifying the Web Interface Files.....	51
47.3 Configuring Single Channel: Edit the Web.config file.....	51
47.4 Challenge and Response Authentication with Count Down Timer.....	52
48 Testing.....	53
49 Uninstalling.....	54
50 Troubleshooting.....	55
50.1 Error Messages.....	55
51 Known Issues and Limitations.....	56
52 Additional Information.....	57

1 Citrix Web Interface 5.1 Integration

2 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.1 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.

3 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 5.1.1 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:

- PINsafeClient.dll ? PINsafe authentication client library.
- include.aspxf ? Customised include file.
- 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: [File:Citrix_WI_5.1_Integration.zip](#)

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

4 Baseline

PINsafe 3.5

Citrix Web Interface build 5.1.1

5 Architecture

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

6 Swivel Configuration

6.1 Configuring the RADIUS server

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

6.2 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.

6.3 Setting up PINsafe Dual Channel Transports

See [Transport Configuration](#)

7 Citrix Web Interface Configuration

7.1 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.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 copied files, Authenticated users need read permissions.

7.2 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.

7.3 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 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="" />

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

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="" />

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

7.4 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.

Properties - http://W15Delaware.longhorn.ctx/Citrix/XenApp

General

Domain Restriction

Explicit

Authentication Type

Two-Factor Authentication

Password Settings

Account Self-Service

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

Add...

Edit...

Remove

☒ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

8 Additional Configuration Options

see [Citrix Xen App 5.x additional login page options](#)

8.1 Self Reset

This outlines how to add the self reset option to the Citrix Web Interface.

The Citrix Web Interface 5.1 self reset files can be downloaded here: [File:Citrix_WI_5.1_SelfReset.zip](#)

Download PINsafeClient.dll and copy to the bin folder overwriting the existing file installed above. Copy reset.aspx and reset.aspx.cs into the auth folder.

Add reset.aspx to the list of unprotected pages in web.config. Locate key="AUTH:UNPROTECTED_PAGES", and at the end of the value field, insert ",./reset.aspx".

Insert a link on the Citrix login page to open the reset page.

Edit app_data\include\loginMainForm.inc, and insert the following line after the login button row, immediately before the </table> tag.

```
<tr><td><a href="./reset.aspx" target="_blank">Forgotten my PIN</a></td></tr>
```

9 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.

10 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 PINsafe RADIUS entries.

11 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 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 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

11.1 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.

12 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.

13 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

14 Citrix Web Interface 5.2 Integration

15 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.2 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.

16 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 5.2 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:

- include.aspxf ? Customised include file.
- 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: [File:Citrix_WI_5.2_Integration.zip](#)

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

17 Baseline

PINsafe 3.5

Citrix Web Interface build 5.2

18 Architecture

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

19 Swivel Configuration

19.1 Configuring the RADIUS server

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

19.2 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.

19.3 Setting up PINsafe Dual Channel Transports

See [Transport Configuration](#)

20 Citrix Web Interface Configuration

20.1 Copy across the Web Interface Files

The 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 copied files, Authenticated users need read permissions.

20.2 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.

20.3 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="" />

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

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

<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="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" />

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

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

20.4 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.

Properties - http://W15Delaware.longhorn.ctx/Citrix/XenApp

- General
 - Domain Restriction
- Explicit
 - Authentication Type
 - Two-Factor Authentication**
 - Password Settings
 - Account Self-Service

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

Add... Edit... Remove

☒ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

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.

21 Additional Configuration Options

see [Citrix Xen App 5.x additional login page options](#)

22 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.

23 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.

24 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 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 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

24.1 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.

25 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.

26 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

27 Citrix Web Interface 5.3 Integration

28 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.

29 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.

30 Baseline

PINsafe 3.5

Citrix Web Interface build 5.3

31 Architecture

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

32 Swivel Configuration

32.1 Configuring the RADIUS server

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

32.2 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.

32.3 Setting up PINsafe Dual Channel Transports

See [Transport Configuration](#)

33 Citrix Web Interface Configuration

33.1 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 copied files, Authenticated users need read permissions.

33.2 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.

33.3 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" />
```

33.4 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.

The screenshot shows the 'Properties - http://WISDelaware.longhorn.ctx/Citrix/XenApp' window. On the left, a tree view shows 'General' and 'Explicit' categories. Under 'Explicit', 'Two-Factor Authentication' is selected and highlighted with a red box. The main panel is titled 'Two-Factor Authentication'. It contains a 'Two-factor setting:' dropdown menu with 'RADIUS' selected, also highlighted with a red box. Below this, it states 'RADIUS authentication is enabled. Check the settings below:'. A section titled 'RADIUS server addresses (in order):' contains a table with two columns: 'Address' and 'Port'. The table lists two entries: '10.7.142.128' and '10.7.142.129' in the 'Address' column, and '1812' and '1812' in the 'Port' column. The first row of the table is highlighted with a red box. To the right of the table are 'Move Up' and 'Move Down' buttons. Below the table are 'Add...', 'Edit...', and 'Remove' buttons, with 'Add...' highlighted by a red box. At the bottom, there is a checkbox 'Use the server list for load balancing' which is checked. Below this are two rows of settings: 'Bypass any failed server for:' with a value of '1' and a unit of 'Hours', and 'Timeout period:' with a value of '30' and a unit of 'Seconds'.

Address	Port
10.7.142.128	1812
10.7.142.129	1812

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.

34 Additional Configuration Options

see [Citrix Xen App 5.x additional login page options](#)

35 Testing

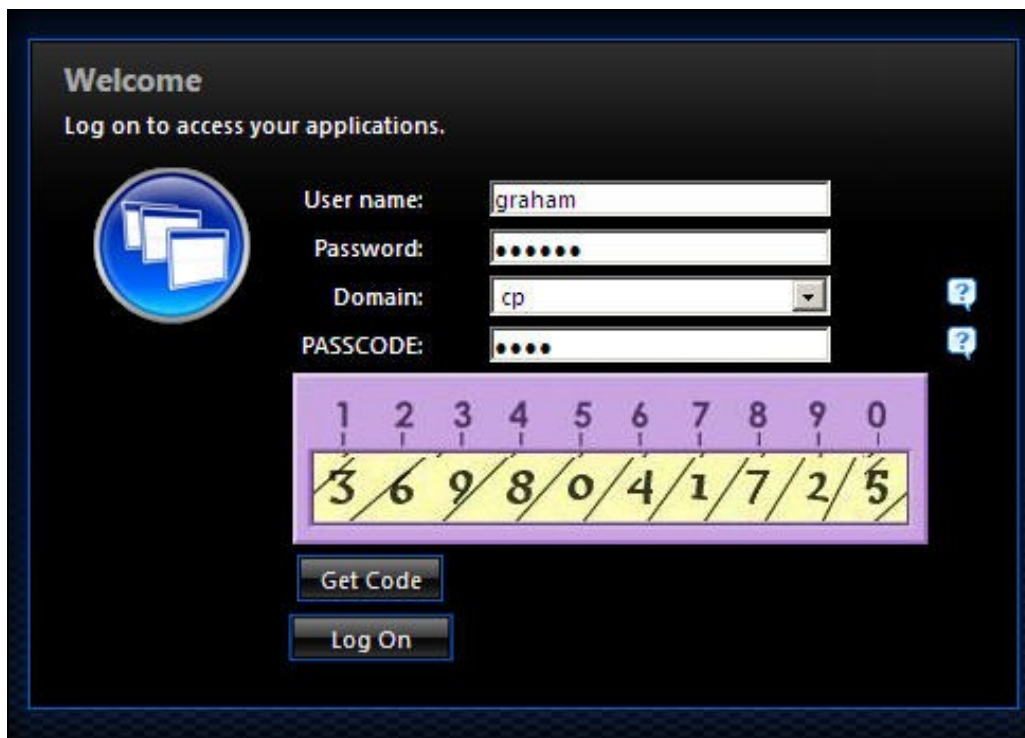
Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered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

Login using Dual channel authentication



The image shows a Citrix Web interface login page with a dark blue background. At the top left, there is a circular icon with three overlapping white squares. Below the icon, the text "Welcome" is displayed in a bold, white font, followed by "Log on to access your applications." in a smaller white font. The login form consists of four fields: "User name:" with the text "graham" entered, "Password:" with six dots, "Domain:" with a dropdown menu showing "cp", and "PASSCODE:" with four dots. To the right of the "Domain:" and "PASSCODE:" fields are small blue question mark icons. Below the fields are two buttons: "Get Code" and "Log On".

Login Using Single Channel Graphical Turing Image



The image shows the same Citrix Web interface login page as above, but with a graphical Turing image overlay. The Turing image is a rectangular box with a purple border and a yellow background. It contains a grid of numbers. The top row of the grid has numbers 1 through 9 and 0. The bottom row of the grid has numbers 3, 6, 9, 8, 0, 4, 1, 7, 2, 5. The numbers are arranged in a way that they are slightly offset from each other, creating a visual distortion. Below the Turing image are the "Get Code" and "Log On" buttons.

36 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.

37 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

37.1 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.

38 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.

39 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

40 Citrix Web Interface 5.4 Integration

41 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 5.4 web interface/Xen App. 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.

A statement from Citrix: All 7.x versions of XenApp and XenDesktop now support the use of Web Interface 5.4. Citrix has extended support of Web Interface for XenApp 7.5, XenDesktop 7.5, XenDesktop 7.1 and XenDesktop 7.0 to allow more time for planning and transition to StoreFront. Note, no new features will be added to Web Interface and its end-of-life remains August 2016.

42 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 5.4 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 and need to be edited as required (see below):

- pinsafe_image.aspx ? Serves single channel images from PINsafe to users.
- login.js.add ? Customised login page client script.
- loginStyle.inc.add ? Customised login form style.
- loginMainForm.inc.add ? Customised login form.
- web.config.add ? Additional configuration entries for PINsafe integration.
- Radius_secret.txt ? RADIUS server secret key.

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

An alternative solution, which includes buttons for TURING image and message request, can be found [here](#). This solution includes two additional files: pinsafe_message.aspx and pinsafe_ping.aspx.

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

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

NOTE: you cannot use a virtual IP as the RADIUS address, as this will not work.

NOTE: the files with the extension ".add" cannot simply be copied into the appropriate directories. They are text files containing notes as to how you should modify the corresponding files to implement PINsafe customisation. See the notes below for more details.

43 Baseline

PINsafe 3.7

Citrix Web Interface build 5.4

44 Architecture

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

45 Swivel Configuration

45.1 Configuring the RADIUS server

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

45.2 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.

45.2.1 Setting up PINsafe Dual Channel Transports

See [Transport Configuration](#)

46 Citrix Web Interface Configuration

46.1 Edit the radius_secret.txt

On the Citrix Web Interface server

Edit the conf/radius_secret.txt file so that it has the same shared secret as has been entered on the PINsafe server. A copy of this file is included in the zip archive.

46.2 Edit the web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

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

```
<add key="RADIUS_NAS_IDENTIFIER" value="citrix_wi" />
```

Note: It is recommended that you use the same value as the identifier in the NAS entry in the PINsafe admin console.

If the Web Interface server has multiple network interfaces, the value of RADIUS_NAS_IP_ADDRESS may need to be set to the IP address used by the NAS. This is the IP address of the Web Interface server, NOT the PINsafe server.

Make sure that the following entry is included, if it is not there already:

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

To allow access to the TURing image from the login page, locate the following line:

```
<add key="AUTH:UNPROTECTED_PAGES" ...
```

The value attribute on this entry is a list of URLs that can be accessed without authentication. Add the following to the end of this list (before the closing quote):

```
, /auth/pinsafe_image.aspx
```

If you are using the alternative integration, you will need to include the other files:

```
, /auth/pinsafe_image.aspx, /auth/pinsafe_message.aspx, /auth/pinsafe_ping.aspx
```

46.3 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.

Properties - http://W15Delaware.longhorn.cbx/Citrix/XenApp

- General
 - Domain Restriction
- Explicit
 - Authentication Type
 - Two-Factor Authentication**
 - Password Settings
 - Account Self-Service

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

Add... Edit... Remove

☒ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

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.

47 Additional Configuration Options

The above modifications will allow authentication to the Web Interface using some of the PINsafe authentication mechanisms such as SMS, mobile Phone applet, and [Taskbar](#). Additional configuration options including the single channel [TURING](#) image are listed below.

see also [Citrix Web Interface 5.X additional login page options](#)

47.1 Changing the OTC label

To change the label for the PINsafe one-time code field from the default of ?PASSCODE:?, locate the file C:\Program Files\Citrix\Web Interface\5.4.0\Languages\accessplatform_strings.properties. (If the language is not English, locate the appropriate file for the appropriate language, if it exists). Edit this file, and locate the line containing ?Passcode=PASSCODE:?. Replace the second word PASSCODE with OTC, or an appropriate text.

47.2 Configuring Single Channel: Modifying the Web Interface Files

The required files (see prerequisites) are of two types: those NOT ending in ".add" need to be copied to the following locations below the root of the Citrix web interface site. Those ending in ".add" contain instructions describing how to modify the corresponding file without the ".add" extension. Where an existing file is being replaced or modified, 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. The below files contained within the zip file should extract to the relevant locations.

The majority of the files included in the integration are modifications to existing files. These are stored with the same name as the file they are intended to modify, but with the additional extension of .add. Each file contains instructions as to how the original files should be added. More details are given below:

1. Copy pinsafe_image.aspx to /auth. This is a new file, not a modification to an existing one.
2. Edit login.js in /auth/clientscripts. Insert the contents of login.js.add at the start of this file, below the header, as indicated in the file itself.
3. Edit loginMainForm.inc in /app_data/include. Insert the contents of loginMainForm.inc.add as indicated in this file: locate a particular section of the file and insert a line.
4. Edit loginstyle.inc in /app_data/include. Insert the contents of loginstyle.inc.add at the bottom of this file, before the footer text, as indicated in the file.
5. Ensure file permissions are set correctly on the copied files, Authenticated users need read permissions.

47.3 Configuring Single Channel: Edit the Web.config file

On the Citrix Web Interface Server:

Edit the web.config file.

The web.config.add 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.

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.

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="" />

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

The settings for a software install of PINsafe 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="" />
```

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

47.4 Challenge and Response Authentication with Count Down Timer

Citrix Web Interface can be configured to use Challenge and Response whereby a user enters a username and password, and if that is correct the user is sent an SMS message and will be prompted to enter an OTC. By default the OTC sent is valid for two minutes only, so a count down timer is provided to show how long the user has left.

For information on configuring the PINsafe RADIUS Challenge and response see [Challenge and Response How to Guide](#).

The required files can be downloaded here: [Challenge and Response with count down files](#)

Extract the files ensuring their correct locations

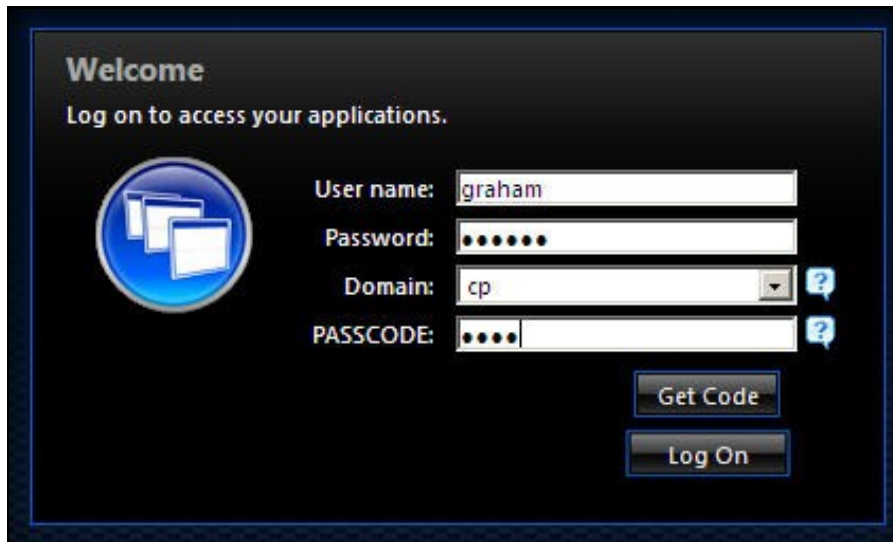
challenge.inc is copied to app_data/include

challenge.js to auth/clientscripts

48 Testing

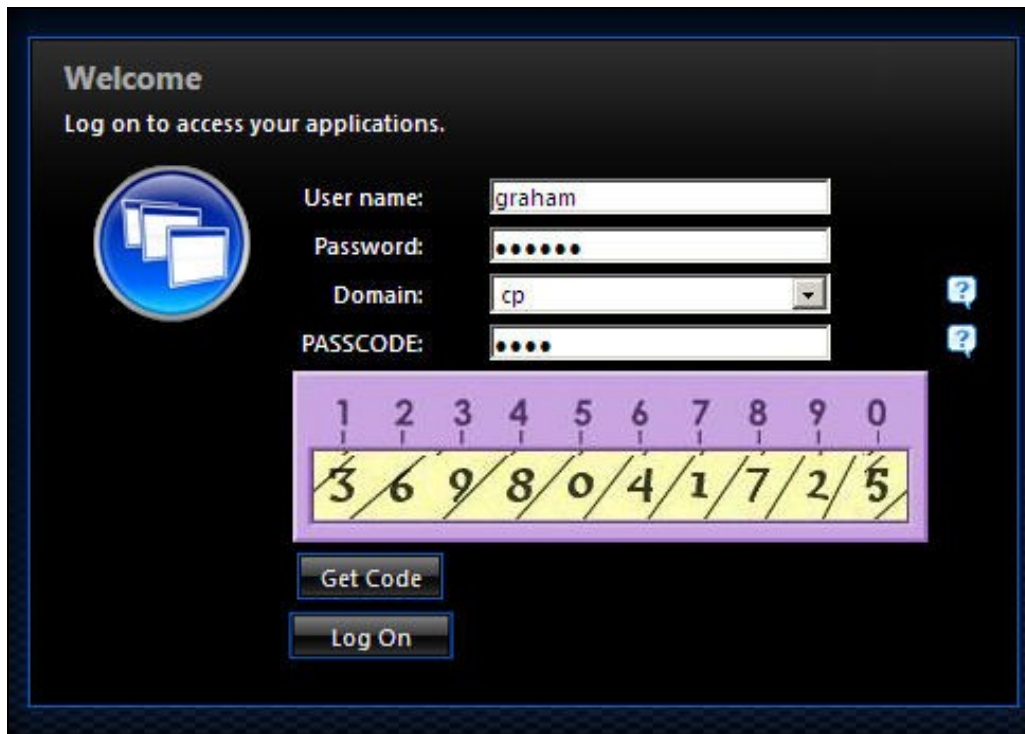
Navigate to the Citrix Web interface login page. The customisation is visible in the addition of a One Time Code field and a Get Code button. Attempting to login with a correct Citrix username and password but no one time code should result in failure. Only when a correct PINsafe one time code is entered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

Login using Dual channel authentication



The image shows a Citrix Web interface login page with a dark blue background. At the top left, there is a circular icon with three overlapping white squares. Below the icon, the text "Welcome" is displayed in a bold, white font, followed by "Log on to access your applications." in a smaller white font. The login fields are arranged vertically: "User name:" with a text box containing "graham", "Password:" with a masked text box (dots), "Domain:" with a dropdown menu showing "cp", and "PASSCODE:" with a masked text box (dots). To the right of the "Domain:" and "PASSCODE:" fields are small blue question mark icons. Below the fields are two buttons: "Get Code" and "Log On".

Login Using Single Channel Graphical Turing Image



The image shows the same Citrix Web interface login page as above, but with a graphical Turing image added. The Turing image is a rectangular box with a purple border and a yellow background. It contains a grid of numbers. The top row of the grid contains the numbers 1 through 9 and 0. The bottom row of the grid contains the numbers 3, 6, 9, 8, 0, 4, 1, 7, 2, 5. The numbers are arranged in a way that they are slightly tilted and have a shadow effect. Below the Turing image are the "Get Code" and "Log On" buttons.

49 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.

50 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 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, you need to add the following entry to web.config:

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

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

50.1 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.

51 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.

If you need to use userPrincipalName to authenticate to Swivel, you may find that the domain name is removed before sending the username to Swivel. To avoid this, make the following changes:

Locate and edit the file `app_code\PagesJava\com\citrix\wi\pageutils\TwoFactorAuth.java`

Find the following method:

```
public static String getUsername(UPNCCredentials token, boolean fullyQualified) {
    if (fullyQualified) {
        return token.getShortDomain() + "\\\" + token.getShortUserName();
    } else {
        return token.getShortUserName();
    }
}
```

Replace it with the following:

```
public static String getUsername(UPNCCredentials token, boolean fullyQualified) {
    return token.getUserIdentity();
}
```

52 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