Table of Contents

Table of Contents

Table of Contents

1 Citrix Web Interface 4 with Presentation Server 4

1.1 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.

1.2 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

1.3 Baseline

PINsafe 3.x

Citrix Web Interface build 3.x, 4.0, 4.2

1.4 Architecture

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

1.5 PINsafe Configuration

1.5.1 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.

1.5.2 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

1.6 Citrix Web Interface Configuration

1.6.1 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 coped files, Authenticated users need read permissions.

1.6.2 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.

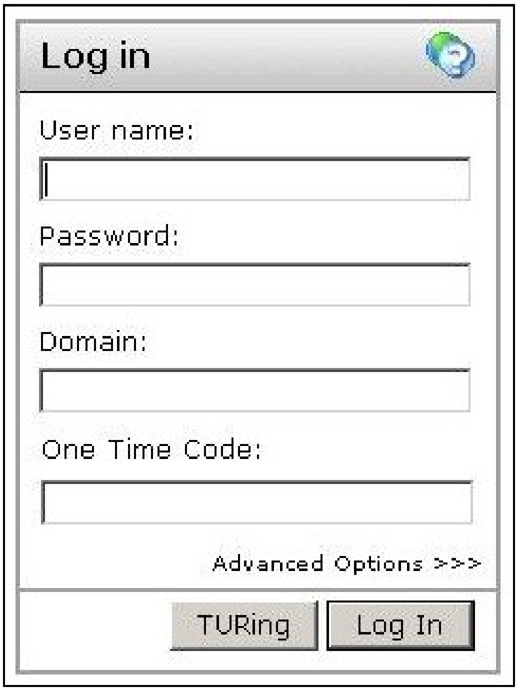
```
<add key="PINsafe_SSL" value="true" />

<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="" />
```

1.7 Additional Configuration Options

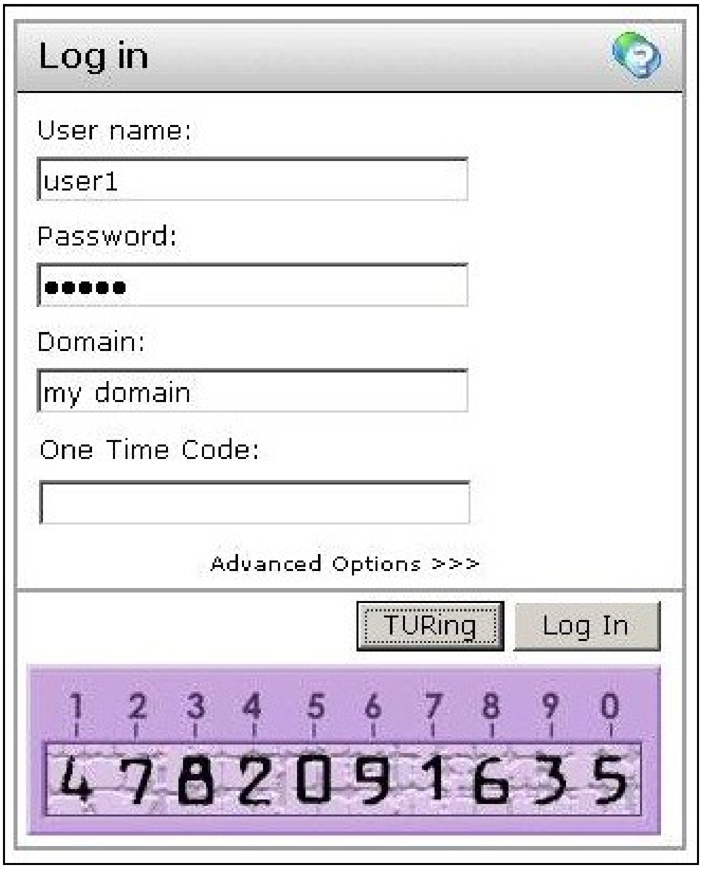
1.8 Testing

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)



Citrix Web Interface login with Turing



User name: user1

Password: ●●●●●

Domain: my domain

One Time Code:

1.9 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.

1.10 Uninstalling

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

1.11 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.

1.12 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

2 Citrix Web Interface 4.5 Integration

2.1 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.

2.2 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

2.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.5.1.8215

2.4 Architecture

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

2.5 PINsafe Configuration

2.5.1 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.

2.5.2 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

2.6 Citrix Web Interface Configuration

2.6.1 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 coped files, Authenticated users need read permissions.

2.6.2 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="" />
```

2.7 Additional Configuration Options

2.7.1 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, "", otc))

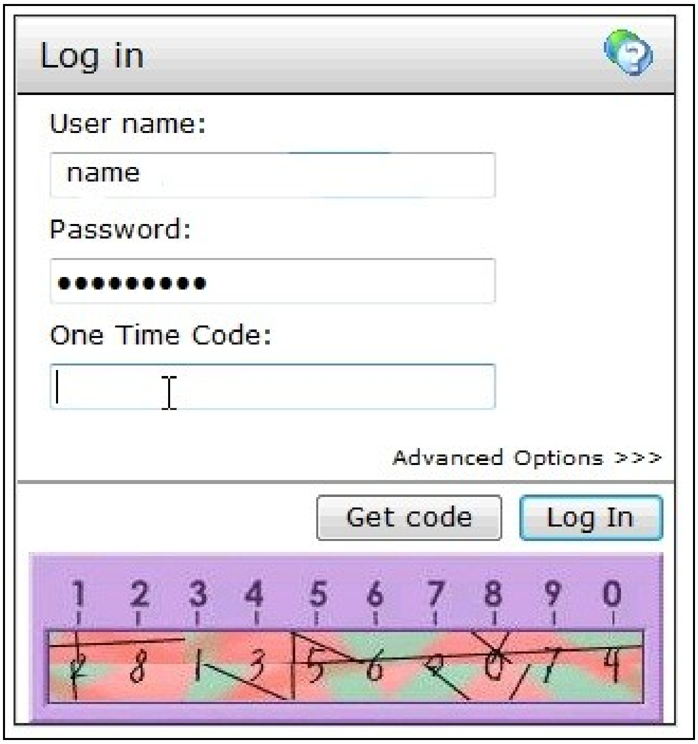
to

if (!pc.Login(user,password, otc))

2.8 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)



Log in

User name: name

Password: ●●●●●●●●●●

One Time Code:

2.9 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.

2.9.1 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>

2.10 Uninstalling

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

2.11 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.

2.12 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

3 Citrix Web Interface 4.6 Integration

3.1 Introduction

This document outlines the necessary steps to integrate PINsafe authentication into the Citrix 4.6 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.

3.2 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 4.6.0.18291 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\AccessPlatform

3.3 Baseline

PINsafe 3.5

Citrix Web Interface build 4.6.0.18291

3.4 Architecture

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

3.5 PINsafe Configuration

3.5.1 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.

3.5.2 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

3.6 Citrix Web Interface Configuration

3.6.1 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 coped files, Authenticated users need read permissions.

3.6.2 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="" />
```

3.7 Additional Configuration Options

3.7.1 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, "", otc))

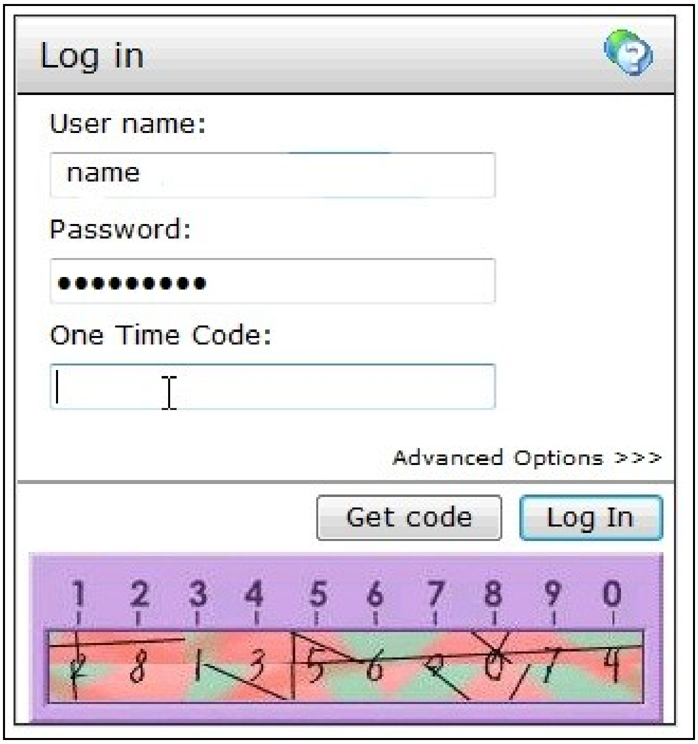
to

if (!pc.Login(user,password, otc))

3.8 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)



Log in

User name:

name

Password:

●●●●●●●●●

One Time Code:

3.9 Uninstalling

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

3.10 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.

3.10.1 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>

3.11 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.

3.12 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

4 Citrix Web Interface 5.0 Integration

4.1 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.

4.2 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

4.3 Baseline

Swivel 3.5

Citrix Web Interface build 5.0.1.29110

4.4 Architecture

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

5 Swivel Configuration

5.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

5.2 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.

5.2.1 Setting up Swivel Dual Channel Transports

See Transport Configuration

5.3 Citrix Web Interface Configuration

5.3.1 Copy accros 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 /

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

5.3.2 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 Swivel server.

5.3.3 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 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" />
```

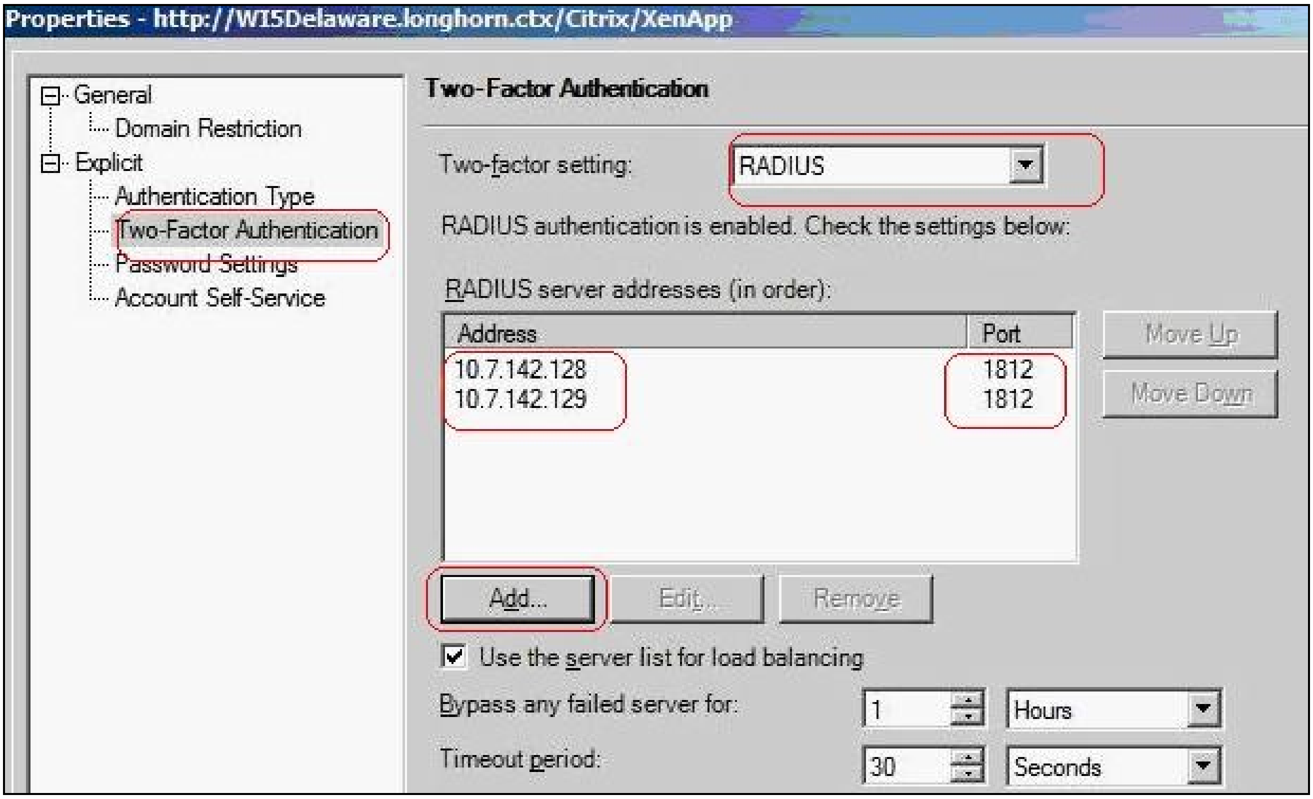
```
<add key="PINsafe_Port" value="8443" />

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

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

5.3.4 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, the select Radius from the dropdown list.



Properties - http://WI5Delaware.longhorn.ctx/Citrix/XenApp

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

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

5.4 Additional Configuration Options

see Citrix Web Interface 5.X additional login page options

5.5 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.

5.6 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.

5.7 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

5.7.1 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 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.

5.8 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.

5.9 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

6 Citrix Web Interface 5.1 Dual Channel button

6.1 Citrix Web Interface Dual Chanel Integration Notes

This outlines how to replace the Single Channel Image request button with a Dual Channel button. This is a supplement to the Citrix Web Interface 5.1 Integration guide.

6.2 Log-in page Customisation

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
<div class="otcButtonPane"><a
       href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
       onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
       onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
       tabIndex="<%=Constants.TAB_INDEX_FORM%>"
       id="dcmessage"
       name="dcmessage"
    ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

6.3 Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

7 Citrix Web Interface 5.1 Integration

8 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.

9 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

10 Baseline

PINsafe 3.5

Citrix Web Interface build 5.1.1

11 Architecture

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

12 Swivel Configuration

12.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

12.2 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.

12.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

13 Citrix Web Interface Configuration

13.1 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 coped files, Authenticated users need read permissions.

13.2 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.

13.3 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.

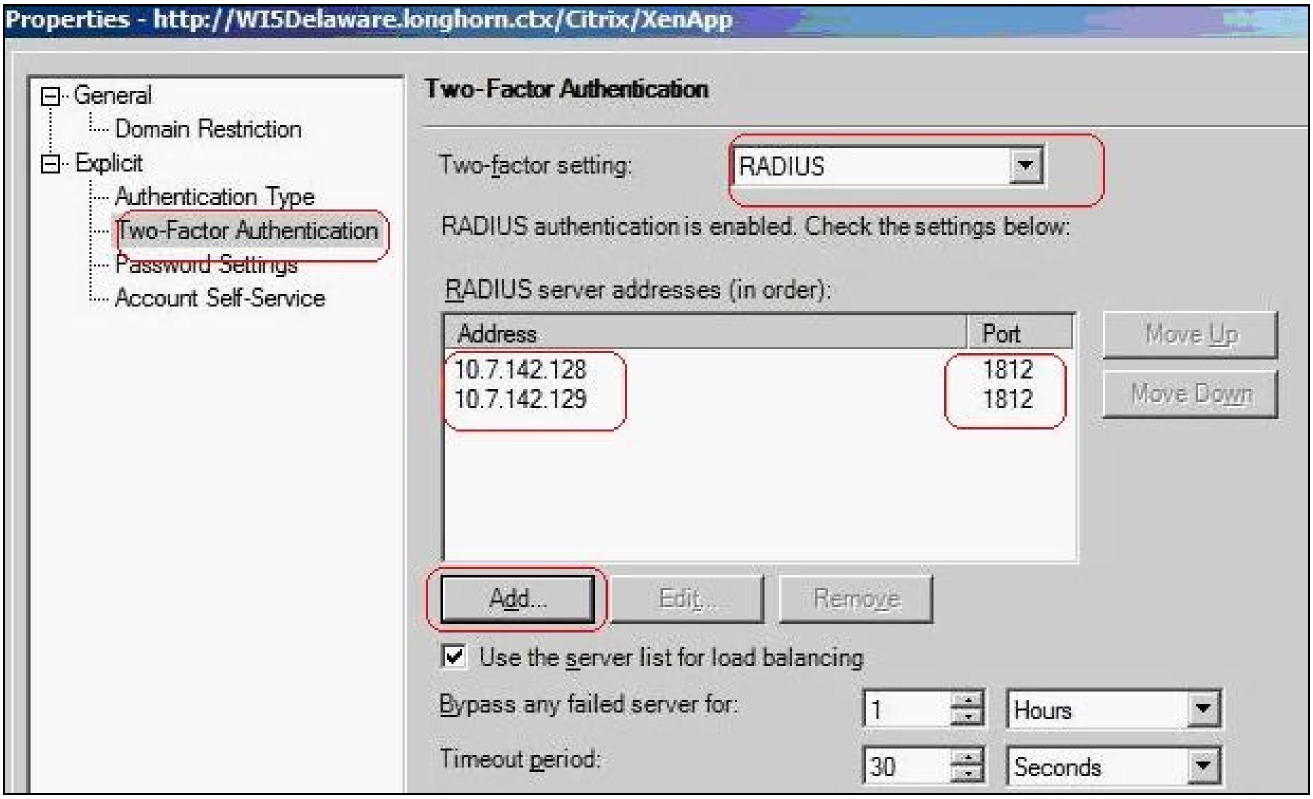
```
<add key="PINsafe_SSL" value="true" />

<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" />
```

13.4 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://WI5Delaware.longhorn.ctx/Citrix/XenApp

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

☑ Use the server list for load balancing

Bypass any failed server for: 1 Hours

Timeout period: 30 Seconds

14 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

14.1 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>
```

15 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.

16 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.

17 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

17.1 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.

18 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.

19 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

20 Citrix Web Interface 5.2 Integration

21 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.

22 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

23 Baseline

PINsafe 3.5

Citrix Web Interface build 5.2

24 Architecture

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

25 Swivel Configuration

25.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

25.2 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.

25.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

26 Citrix Web Interface Configuration

26.1 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 coped files, Authenticated users need read permissions.

26.2 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.

26.3 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" />
```

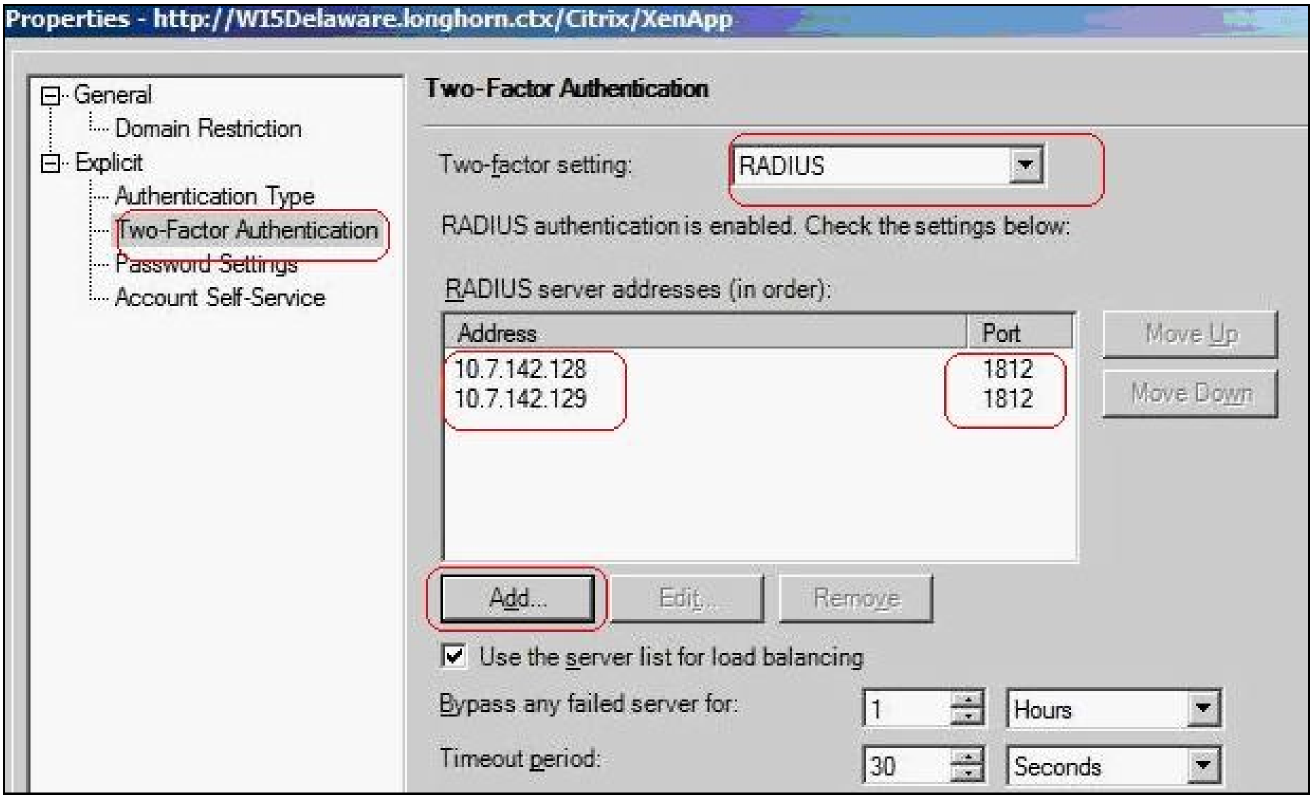
```
<add key="RADIUS_NAS_IDENTIFIER" value="pinsafe" />
```

26.4 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://WI5Delaware.longhorn.ctx/Citrix/XenApp

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

☑ 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.

27 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

28 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.

29 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.

30 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

30.1 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.

31 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.

32 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

33 Citrix Web Interface 5.3 Integration

34 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.

35 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.

36 Baseline

PINsafe 3.5

Citrix Web Interface build 5.3

37 Architecture

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

38 Swivel Configuration

38.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

38.2 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.

38.3 Setting up PINsafe Dual Channel Transports

See Transport Configuration

39 Citrix Web Interface Configuration

39.1 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 coped files, Authenticated users need read permissions.

39.2 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.

39.3 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" />
```

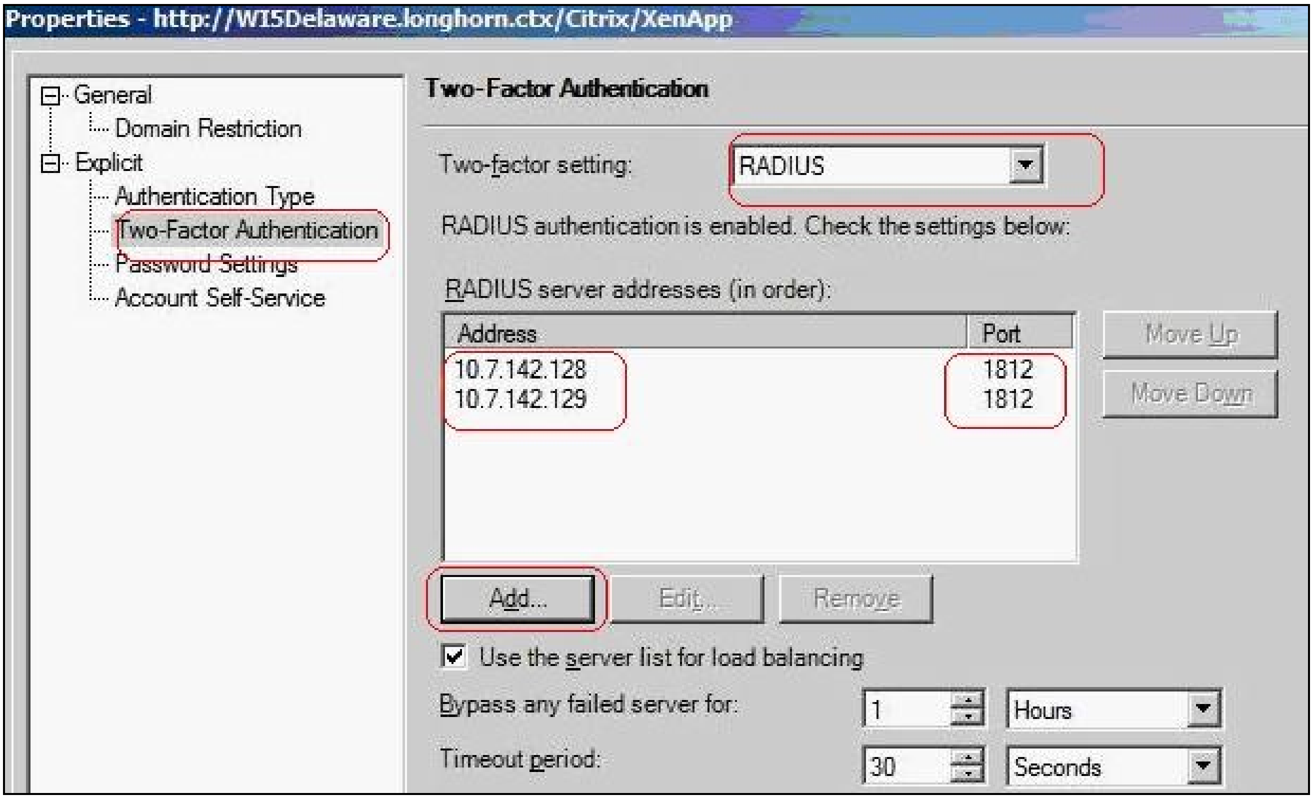
```
<add key="PINsafe_Secret" value="" />

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

39.4 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://WI5Delaware.longhorn.ctx/Citrix/XenApp

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

☑ 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.

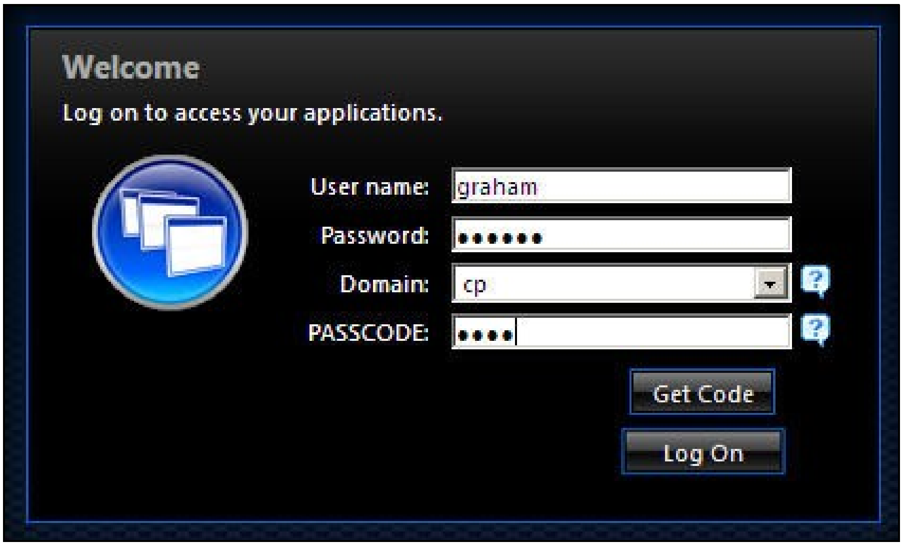
40 Additional Configuration Options

see Citrix Xen App 5.x additional login page options

41 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



Welcome

Log on to access your applications.

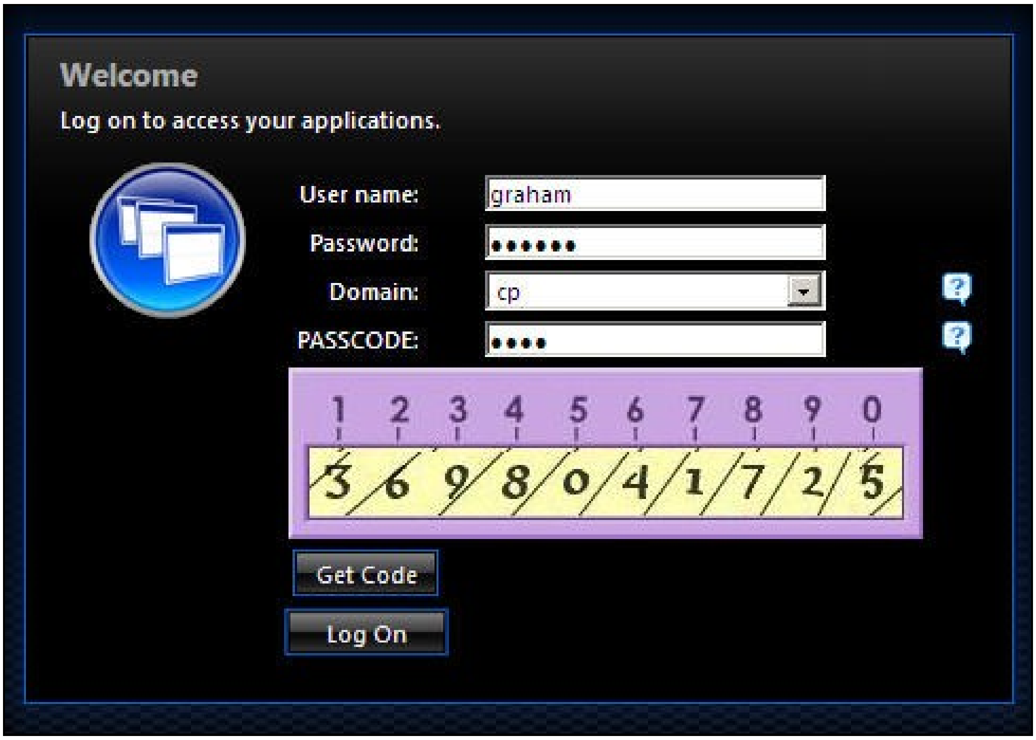
User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

Login Using Single Channel Graphical Turing Image



Welcome

Log on to access your applications.

User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

1	2	3	4	5	6	7	8	9	0
3	6	9	8	0	4	1	7	2	5

42 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.

43 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

43.1 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.

44 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.

45 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

46 Citrix Web Interface 5.4 Integration

47 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.*

48 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.

49 Baseline

PINsafe 3.7

Citrix Web Interface build 5.4

50 Architecture

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

51 Swivel Configuration

51.1 Configuring the RADIUS server

On the Swivel Administration console configure the RADIUS Server and NAS, see RADIUS Configuration

51.2 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.

51.2.1 Setting up PINsafe Dual Channel Transports

See Transport Configuration

52 Citrix Web Interface Configuration

52.1 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.

52.2 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:

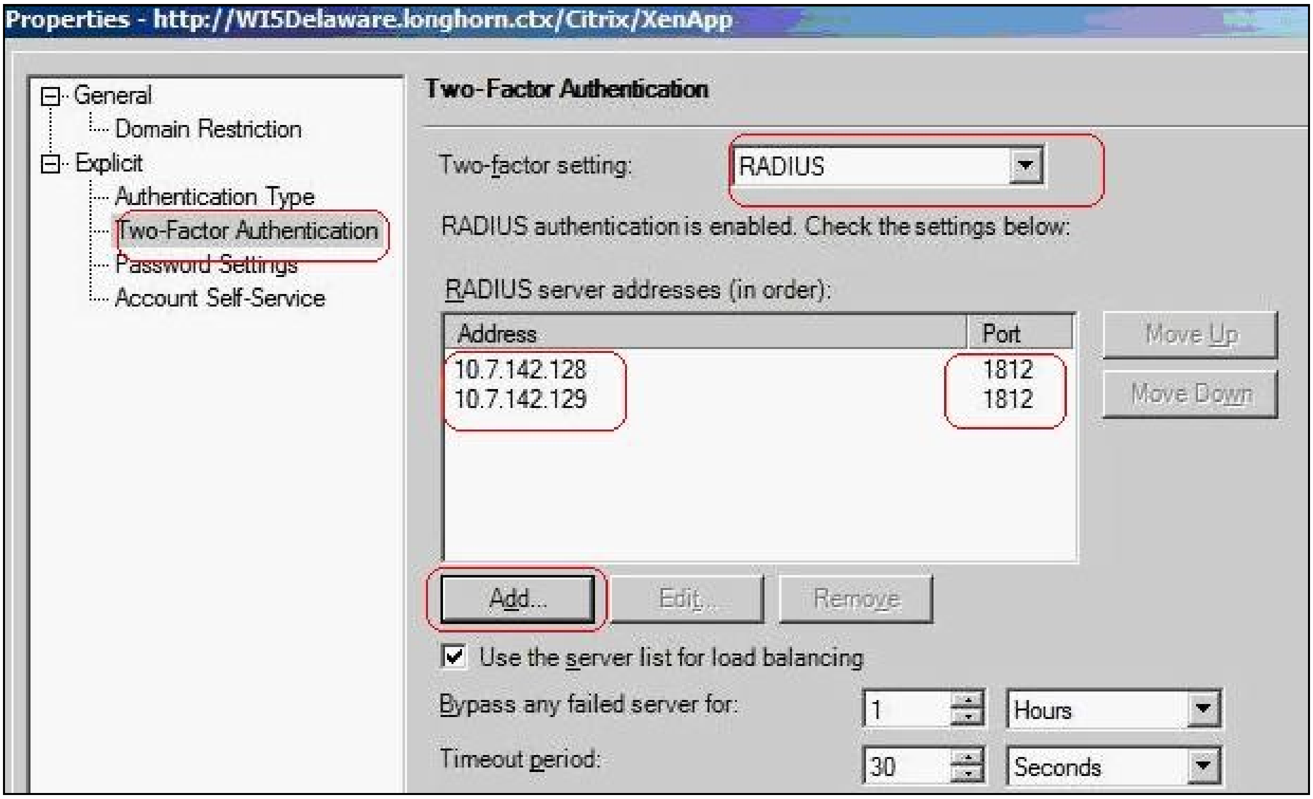
```
,/auth/pinsafe_image.aspx,/auth/pinsafe_message.aspx,/auth/pinsafe_ping.aspx
```

52.3 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://WI5Delaware.longhorn.ctx/Citrix/XenApp

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

☑ 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.

53 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

53.1 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.

53.2 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. This 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.

53.3 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" />
```

53.4 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

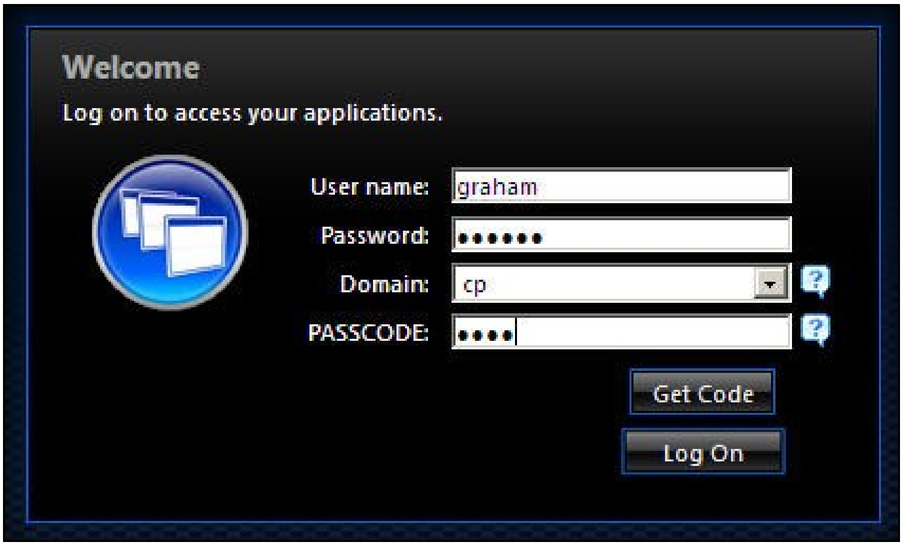
challenge.inc is copied to app_data/include

challenge.js to auth/clientscripts

54 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



Welcome

Log on to access your applications.

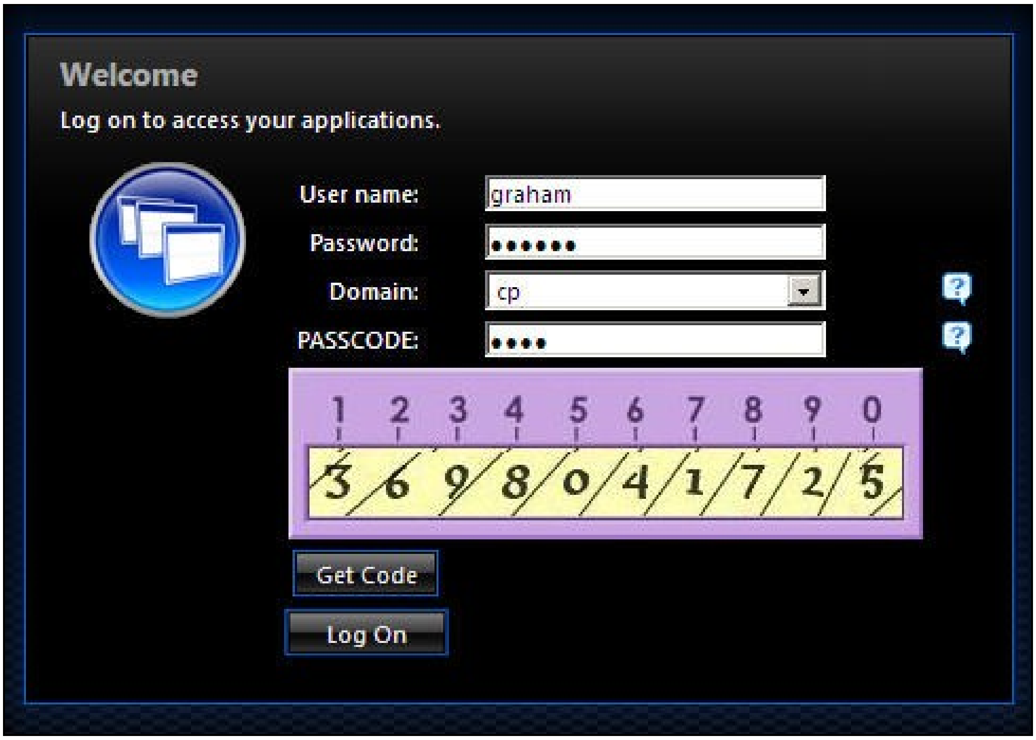
User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

Login Using Single Channel Graphical Turing Image



Welcome

Log on to access your applications.

User name: graham

Password: ••••••

Domain: cp

PASSCODE: ••••

55 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.

56 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

56.1 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.

57 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(UPNCredentials token, boolean fullyQualified) {
  if (fullyQualified) {
    return token.getShortDomain() + "\\" + token.getShortUserName();
  } else {
    return token.getShortUserName();
  }
}
```

Replace it with the following:

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

58 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

59 Citrix Web Interface 5.X additional login page options

59.1 Citrix Web Interface 5.x additional login page options

This outlines how to further customise the Citrix login page. This is a supplement to the Citrix Web Interface 5.x Integration guides.

59.2 Removing the Single Channel Button

To remove the *refresh image*, delete the following text:

```
 "<a class='leftDoor' href='javascript:onTuringButtonClick();'>" +
                                "Refresh Image" +
                                "</a>
```

59.3 Replacing the Single Channel Button with a Dual Channel Button

59.3.1 Replacing TURing image with a Dual Channel (SMS) request

Edit the file pinsafe_image.aspx

find the following line:

```
       url.AppendFormat("{0}:{1}/{2}/SCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

Replace with:

```
       url.AppendFormat("{0}:{1}/{2}/DCImage?username={3}", server, port, context, Request.QueryString["username"]);
```

59.3.2 Compatibility

This has been tested on Citrix Web Interface 5.1

59.3.3 Dual Channel Button modification

On the Swivel Administration console under Server/Dual Channel, ensure Allow message request by username: is set to Yes.

On the Citrix Web Interface Installation create a copy of auth/pinsafe_image.aspx, and call it pinsafe_message.aspx

You will also need to ensure that pinsafe_message.aspx is included in the list of unprotected pages.

In auth/clientscripts/login.js, make a copy of the function onTuringButtonClick(), calling it onMessageButtonClick (). Change image.src in this function to point to pinsafe_message.aspx.

Edit app_data/include/loginMainForm.inc. Locate the text '<div class="otcButtonPane"'. Copy from here up to the ending </div>, and paste it immediately after this div. Change "href=javascript:onTuringButtonClick" to "href=onMessageButtonClick".

Change the title and id of this div, as well as the id of the enclosed img and span elements. The new div element should be something like this:

```
     <div class="otcButtonPane"><a
            href="javascript:onMessageButtonClick()" title="Click this button to retrieve a PinSafe message."
            onmouseover="changeOtcBtnColor(true);" onmouseout="changeOtcBtnColor(false);"
            onfocus="changeOtcBtnColor(true);" onblur="changeOtcBtnColor(false);"
            tabIndex="<%=Constants.TAB_INDEX_FORM%>"
            id="dcmessage"
            name="dcmessage"
         ><img id="msgButtonBg" src="../media/LoginButtonGlow.gif" alt="" /><span id="msgButtonWrapper">Get Message</span></a></div>
```

To make sure the new button looks right, you will also need to edit app_data/include/loginStyle.inc. Look for occurrences of #otcButtonWrapper and add ", #msgButtonWrapper". Also, for the entry #<%=Constants.ID_OTC_BTN%>, add ", #dcmessage".

To change the Refresh Image button modify the file under auth\clientscripts\login.js.add and search for the line Refresh Image and change to the required text, such as Request Code or Request SMS.

```
           "<span class='rightDoor'>Refresh Image</span>" +"
```

59.3.4 Dual Channel Testing

Test the button from the login page. Check the Swivel logs for the dual channel requests.

59.4 Single Channel Button with an automated Single Channel Image

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to automatically show the Turing image without the need for pressing the button when the user enters into the required field.

59.4.1 Compatibility

This has been tested on Citrix Web Interface 5.1 using the Single Channel Turing Image

59.4.2 Single Channel Button to automated Single Channel Image modification

Edit the loginMainForm.inc file on the Citrix server. Locate the username field - look for the following:

```
<input type='text' name='<%=Constants.ID_USER%>' ...
```

insert the following line after that one:

```
onblur='onTuringButtonClick()'
```

This causes the turing image JavaScript function to be called when the user leaves the username field.

59.4.3 Automated Single Channel Image Testing

Test the image from the login page. Check the Swivel logs for the single channel image requests.

59.5 Turing, Dual channel and Display Index buttons

The Citrix Web Interface 5.x integration has a button to generate the Single Channel Image. This can be modified to add additional buttons of Show Turing Image, Send Dual Channel Security String and Display Index number. See also Multiple Security Strings How To Guide

59.5.1 Compatibility

This has been tested on Citrix Web Interface 5.3

59.5.2 Required Files

The following files are required and should be used for installation: [1]

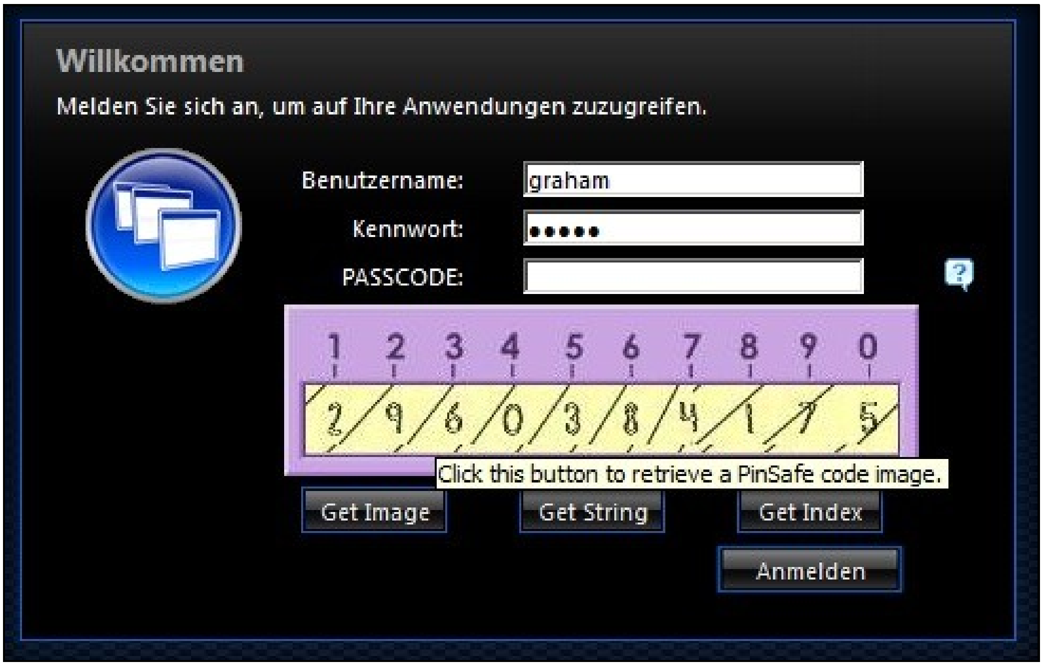
59.5.3 Installation Instructions

Follow the installation instructions for the relevant Citrix version.

59.5.4 Testing

Verify that three buttons are displayed and that they show the expected results when selected.

The following screen shots show the different buttons in use



Willkommen

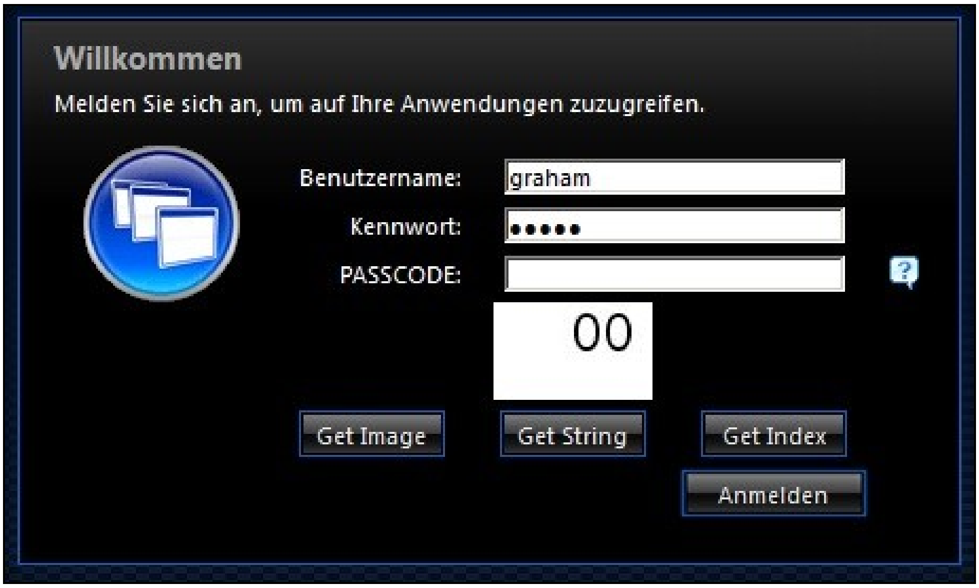
Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

Benutzername: graham

Kennwort: •••••

PASSCODE:

Single Channel TURing Image request



Willkommen

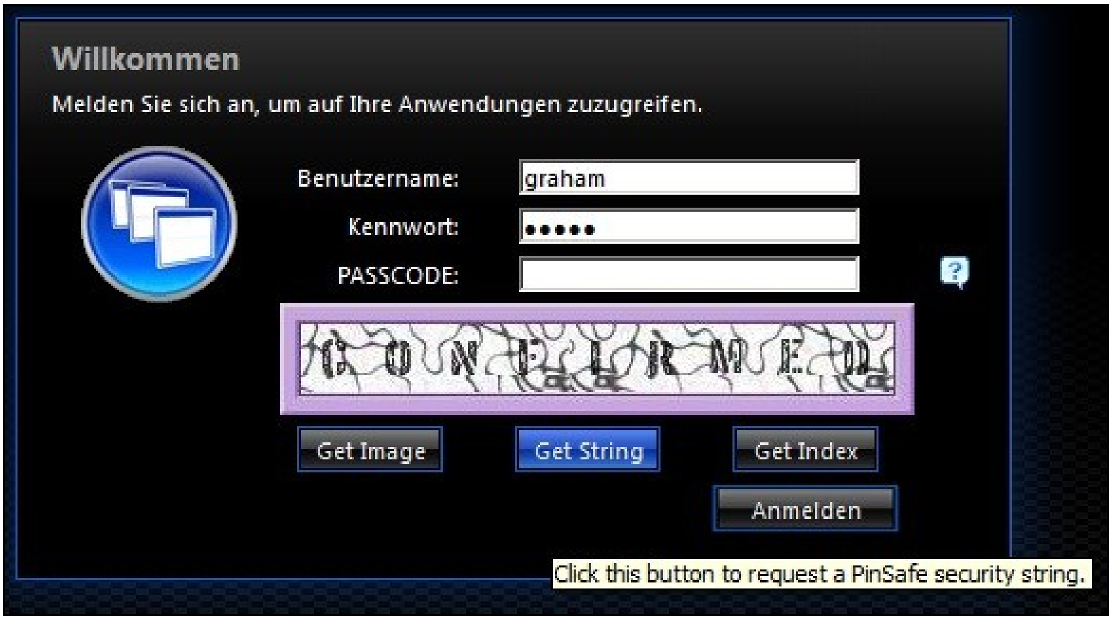
Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

Benutzername: graham

Kennwort: •••••

PASSCODE:

Multiple Security String Message index number telling user which security string to use for authentication



Willkommen

Melden Sie sich an, um auf Ihre Anwendungen zuzugreifen.

Benutzername: graham

Kennwort: ●●●●●

PASSCODE:

CONFIRMED

Click this button to request a PinSafe security string.

Securiy String On Demand Confirmation message of sending the user a Security String