ChangePIN How to Guide

Contents

- 1 Overview
- 2 ChangePIN software
- 3 Configure The PINsafe Server
- 4 Installing ChangePIN
- 5 Connecting to ChangePIN
- 6 Default Configuration files
    - 6.1 Default settings for a non-appliance PINsafe installation
    - 6.2 Default settings for a PINsafe virtual or hardware appliance installation
- 7 ChangePIN options explained
- 8 ChangePIN Custom Page Configuration
    - 8.1 ChangePIN version 4290 (appliance version 2.0.12 and later)
    - 8.2 ChangePIN version 3573 (appliance version 2.0.11 and earlier)
        - 8.2.1 ChangePIN Custom Text Formatting
        - 8.2.2 ChangePIN Changing the Text and Language
        - 8.2.3 ChangePIN Custom Background Colour Editing
    - 8.3 Modifying ChangePIN for SMS only
- 9 Multiple Instances of ChangePIN
- 10 ChangePIN Sample
- 11 Troubleshooting ChangePIN
    - 11.1 Incorrect Credentials Used
    - 11.2 Single Channel Image fails to display
        - 11.2.1 Private IP is being used
    - 11.3 Incorrect values for Swivel virtual or hardware appliance
    - 11.4 PIN not complex enough
    - 11.5 The user does not belong in the correct group
    - 11.6 You must supply a valid password
    - 11.7 Change PIN failed for user: username, error: CHANGE_PIN_PASSWORD_ERROR
    - 11.8 SSL certificate errors
    - 11.9 Changes to the ChangePIN settings.xml don't take effect
    - 11.10 ChangePIN related error messages

Overview

This document covers installation, configuration and administration of the the PINsafe XML ChangePIN application. See also the user guide at ChangePIN User Guide and for sample screen shots see ChangePIN Samples. PINsafe also supports RADIUS ChangePIN.

ChangePIN may be used by a user to change their PIN. A user must know the current PIN in order to change their PIN.

It can be used with:

- Dual channel (SMS), the user should not click start session.
- Single Channel (TURing, PINpad, Pattern, BUTton).

ChangePIN uses XML authentication, not RADIUS to authenticate to the PINsafe server. It uses a session ID rather than a username for authentication, so 'Allow session request by username' is not required.

- Changes to the ChangePIN application may be applied by restarting Tomcat.
- Additionally there is a IIS version of the ChangePIN application.
- PINsafe mobile phone apps allow the user to generate security strings to change their PIN.
- **The troubleshooting section describes a modified web page that avoids problems with SSL certificates.**

If a repository password is being used (i.e. on the PINsafe server Check Password with Repository is set to Yes), then the repository password should also be entered. The Password setting may need to be configured to display the password field.

ChangePIN software

The Swivel virtual or hardware appliance already has the changePIN software installed. The ChangePIN software can be downloaded from the PINsafe software page

A modified changepin web page is available that serves the image from the same host and port. It assumes that the host, that changepin is running on can also deliver TURing images. This can be downloaded here

Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

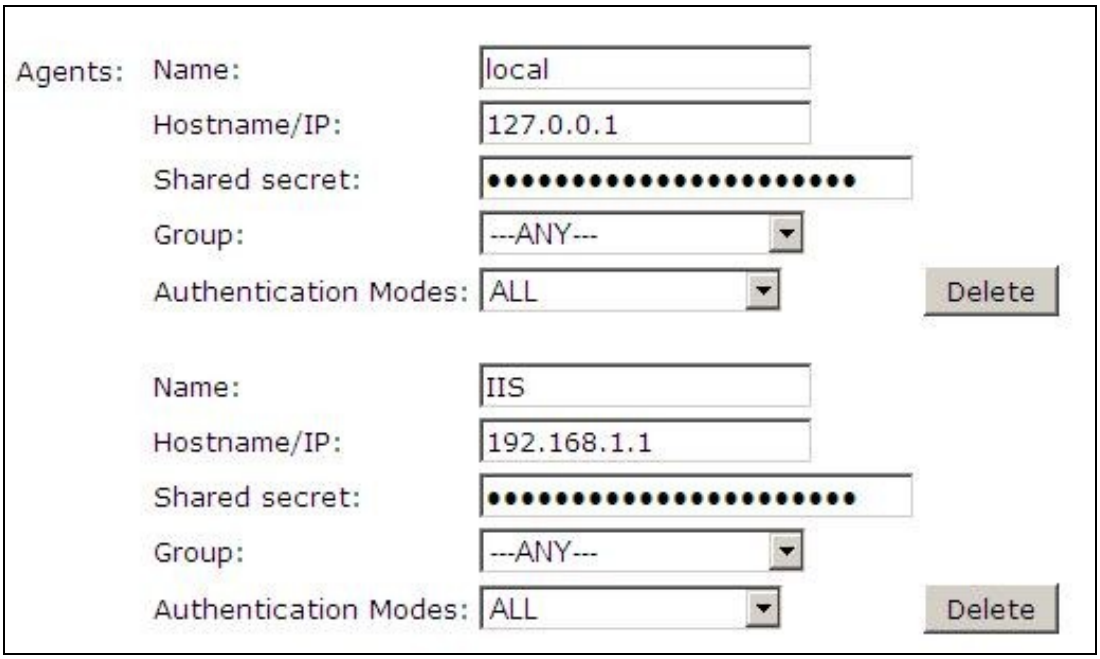
1. On the PINsafe Management Console select Server/Agent

2. Enter a name for the Agent

3. Enter the IP address or hostname of the Swivel server (see the local entry below which will already exist on a Swivel virtual or hardware appliance)

4. Enter the shared secret

5. Click on Apply to save changes



Installing ChangePIN

ChangePIN is already installed on the virtual or hardware appliances in the **webapps2** folder

To install extract from the zip file and copy the change.war file to the webapps folder. It will automatically deploy when Tomcat is running.

Connecting to ChangePIN

The URL's for connecting to the ChangePIN application are by default:

- virtual or hardware appliance: https://IP:8443/changepin
- Software installation: http://IP:8080/changepin

Default Configuration files

The **settings.xml** file contains the ChangePIN configurations and is usually found in the following locations:

- For a software only install:

<Path to Tomcat>/webapps/changepin/WEB-INF/**settings.xml**

- For a Swivel virtual or hardware appliance:

/usr/local/tomcat/**webapps2**/changepin/WEB-INF/**settings.xml**

(Note that the virtual or hardware appliance ChangePIN is hosted in webapps2 directory, not webapps. webapps2 hosts applications which are accessible on port 8443, such as ChangePIN, proxy and ResetPIN)

Default settings for a non-appliance PINsafe installation

Default settings for a software only install may be as follows (those that often need changing are in **red**):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
 <entry key="ssl">false</entry>
 <entry key="server">localhost</entry>
 <entry key="port">8080</entry>
 <entry key="context">pinsafe</entry>
 <entry key="secret">secret</entry>
 <entry key="redirect">http://www.swivelsecure.com</entry>
 <entry key="explicit">false</entry>
 <entry key="imagecontext">pinsafe</entry>
 <entry key="imageserver">localhost</entry>
 <entry key="imageport">8080</entry>
 <entry key="imagessl">false</entry>
 <entry key="password">false</entry>
 <entry key="changepassword">false</entry>
</properties>
```

Default settings for a PINsafe virtual or hardware appliance installation

The default settings for a virtual or hardware appliance may be the following (The entries that may need changing are in **red**):

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
 <entry key="ssl">false</entry>
 <entry key="server">localhost</entry>
 <entry key="port">8181</entry>
 <entry key="context">pinsafe</entry>
 <entry key="imagecontext">proxy</entry>
 <entry key="imageserver">localhost</entry>
 <entry key="imageport">8443</entry>
 <entry key="imagessl">true</entry>
 <entry key="secret">secret</entry>
 <entry key="explicit">false</entry>
 <entry key="redirect">http://www.google.com</entry>
</properties>
```

ChangePIN options explained

Each option below, corresponds to the entry keys defined in the configuration files above. Provided is a description for each option.

- **ssl**: true/false, for communication between ChangePIN and the PINsafe server. *On virtual or hardware appliances leave as false*;
- **server**: the PINsafe server hostname for IP address, for communication between ChangePIN and the PINsafe server. *On virtual or hardware appliances leave as localhost*;
- **port**: the port used to communicate with the PINsafe server for IP address, for communication between ChangePIN and the PINsafe server. *On virtual or hardware appliances leave as 8181*;
- **context**: the install name of the PINsafe application, usually pinsafe for IP address, for communication between ChangePIN and the PINsafe server; *On virtual or hardware appliances leave as pinsafe*;
- **secret**: the shared secret, must also be entered on the PINsafe Administration Console, under **Server** -> **Agent**; *On virtual or hardware appliances this is preconfigured*;
- **redirect**: redirects on completion of changePIN. Remove the line to disable a redirect, this must be an address users can get to publicly;
- **explicit**: true/false, if **false**, the user must extract their old PIN and new PIN from the Turing image to change their PIN and they do not enter PIN directly; If **true** then user enters PIN as it is to change their PIN, without extracting it from a Turing image. Note the use of explicit mode set to true requires SCText to be enabled, see SCText How To Guide.
- **imagecontext**: the publicly available install location where PINsafe obtains its single channel image from, e.g. **proxy** (if using port 8443) or **pinsafe** (if using port 8080);

> So if you had a Turing image URL of:
>
> https://turingimage.company.com:8443/**proxy**/SCImage?username=jsmith
>
> ...the imagecontext would be **proxy**.

- **imageserver**: the hostname or IP address where the user obtains a single Channel image, for communication between user and ChangePIN must be accessible by user (e.g. public address, proxy or NAT). Since the user requests the image it **must be changed from "localhost"**.

> So if you had a Turing image URL of:
>
> https://**turingimage.company.com**:8443/proxy/SCImage?username=jsmith
>
> ...the imageserver would be **turingimage.company.com**.

- **imageport**: the publicly available port where PINsafe obtains its single channel image from;

> So if you had a Turing image URL of:
>
> https://turingimage.company.com:**8443**/proxy/SCImage?username=jsmith
>
> ...the imageport would be **8443**

- **imagessl**: true/false, set to true if SSL communications are used for the ChangePIN image;

So if you had a Turing image URL of:

https://turingimage.company.com:8443/proxy/SCImage?username=jsmith

...the imagessl would be set to **true**

If you had a Turing image URL of:

http://turingimage.company.com:8443/proxy/SCImage?username=jsmith

...the imagessl would be set to **false**

- **password**: true/false set to true if a password is used for ChangePIN;
- **changepassword**: true/false to control if the password can be changed;

ChangePIN Custom Page Configuration

ChangePIN version 4290 (appliance version 2.0.12 and later)

The ChangePIN page can be modified to change the text, such as for differing languages. Backup the changepin folder to a safe location then edit the file changepin.jsp

On the PINsafe server the ChangePIN is located at:

/usr/local/*<apache-tomcat-version>*/webapps2/changepin/prompts.xml

Example:

/usr/local/apache-tomcat-5.5.20/webapps2/changepin/prompts.xml

The following text may be changed:

```
<entry key="introduction">ChangePIN Introduction"</entry>

<entry key="usernamePrompt">Step 1: To begin enter your username</entry>

<entry key="existingPasswordPrompt"> Step 1a: Enter any password associated with the account </entry>

<entry key="existingPrompt">Step 2:  Enter your OTC based on your current PIN</entry>

<entry key="newOTCPrompt">Step 3: Enter your OTC based on your new PIN</entry>

<entry key="confirmNewOTCPrompt">Step 4: Re-enter your OTC based on your new PIN</entry>
```

ChangePIN version 3573 (appliance version 2.0.11 and earlier)

The ChangePIN page can be modified to change the text, such as for differing languages. Backup the changepin folder to a safe location then edit the file changepin.jsp

On the PINsafe server the ChangePIN is located at:

/usr/local/*<apache-tomcat-version>*/webapps2/changepin/changepin.jsp

Example:

/usr/local/apache-tomcat-5.5.20/webapps2/changepin/changepin.jsp

ChangePIN Custom Text Formatting

The ChangePIN page accepts HTML code for various functions such as bold and colour.

Example:

final String NEW_OTC_PROMPT = "Step 3 : Enter the One-Time-Code using your
new PIN and the Security String shown below.";

Note: In this example we use a \ to allow the " to be used.

ChangePIN Changing the Text and Language

The text can be altered as required, perhaps into different languages.

To change the prompt edit the line

```
 <td class="label">Step 1: Enter your username and
press the Get Image button if you need a TURing image </td>
```

To change the name on the button

```
<input name="sessionstart" id="sessionstart" type="submit"
       onclick="return check_username()" value="Get Image">
```

The following attribute text may be changed

final String USERNAME_PROMPT = "Step 1: Enter your username and
press the Security String button if you need a TURing image";

final String CURRENT_OTC_PROMPT = "Step 2 : Enter the OTC (one-time-code) using the PIN
your current PIN and the Security String shown below.";

final String NEW_OTC_PROMPT = "Step 3 : Enter the OTC using your
new PIN and the Security String.";

final String CONFIRM_OTC_PROMPT = "Step 4 : Re-enter the OTC using your new PIN";

final String CLICK_BUTTON_PROMPT = "
then click on Change PIN button";

final String PASSWORD_PROMPT = "Step 2a: If your PINsafe has a password, enter it here:";

final String NEW_PASSWORD_PROMPT = "Step 5: If you are also changing your PINsafe password
 Enter New Password:";

final String CONFIRM_PASSWORD_PROMPT = "Step 6: Re-enter your new password";

final String PIN_CHANGE_SUCCESSFUL = "PIN change successful.
";

final String REDIRECTING_PROMPT = "Please wait while you are redirected. If your
browser doesn't automatically redirect
click";

final String REDIRECT_LINK_PROMPT = "here";

final String REDIRECTING_PROMPT2 = "to continue.";

final String CURRENT_PIN_PROMPT = "Enter your current PIN";

final String NEW_PIN_PROMPT = "Enter your new PIN";

final String CONFIRM_PIN_PROMPT = "Confirm your new PIN";

final String DEFAULT_ERROR = "An error occured, please check your
credentials. If the error persists
 contact your PINsafe Administrator.";

final String INVALID_PIN_ERROR = "Your chosen PIN was not valid.
Please try again with a different PIN.
For more details contact your PINsafe Administrator";

final String INVALID_PASSWORD_ERROR = "Your chosen Password was not valid.
Please try again with a different Password.
For more details contact your PINsafe Administrator";

final String SESSION_START_ERROR = "Cannot start PINsafe Session";

final String INVALID_USERNAME_ERROR = "Invalid Characters in username";

final String PASSWORD_REQUIRED_ERROR = "You must supply a valid password";

ChangePIN Custom Background Colour Editing

To modify the colours, you would also make a backup of changepin.css and modify the following 'background-color' attribute to manipulate the box:

```
######################

table#box {
  margin: 20px auto;
  border: 2px solid #909090;
  background-color: #d0d0d0;
}

######################
```

Modifying ChangePIN for SMS only

Security strings can be used from SMS text messages and Mobile Phone Clients to change the PIN. Where the single channel graphical image is not being used, it is possible to modify the ChangePIN to request a SMS message. To allow an SMS request the On Demand Delivery and /or if the standard present security string delivery is not being used the On Demand Authentication must be enabled. The user must be a Dual Channel User and a Single Channel user, and have Dual Channel allow session request by username allowed, although single channel session request by user name is not required.

Edit the file changepin.jsp located within the changepin folder, usually within <path to Tomcat>\webapps\changepin or <path to Tomcat>\webapps2\changepin

Replace both occurrences of SCImage? with DCMessage?

```
src="https://<%=clientProps.getProperty("imageserver", "localhost")%>:<%=clientProps.getProperty("imageport", "8080")%>/<%=clientProps.getPro

src="http://<%=clientProps.getProperty("imageserver", "localhost")%>:<%=clientProps.getProperty("imageport", "8080")%>/<%=clientProps.getProp
```

to

```
src="https://<%=clientProps.getProperty("imageserver", "localhost")%>:<%=clientProps.getProperty("imageport", "8080")%>/<%=clientProps.getPro

src="http://<%=clientProps.getProperty("imageserver", "localhost")%>:<%=clientProps.getProperty("imageport", "8080")%>/<%=clientProps.getProp
```

To change the button Get SMS

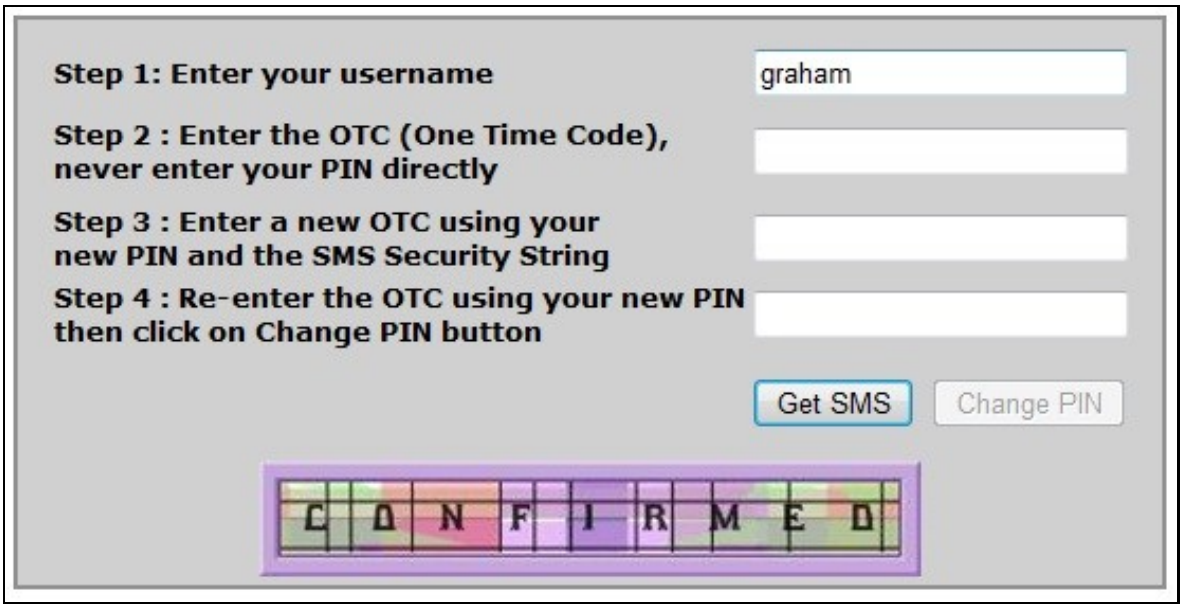
find the line containing *Get Image*

```
onclick="return check_username()" value="Get Image">
```

Replace the text with *Get SMS* or appropriate text

```
onclick="return check_username()" value="Get SMS">
```

The below picture shows a modified ChangePIN page with additional text modification.



Multiple Instances of ChangePIN

It is possible to install multiple instances of changepin. create a copy of the changepin.war and then copy webapps folder or for the virtual or hardware appliance, the webapps2 folder. This should create a folder with the new name, and should be accessible using the new name.

Example for a file called changepin2.war:

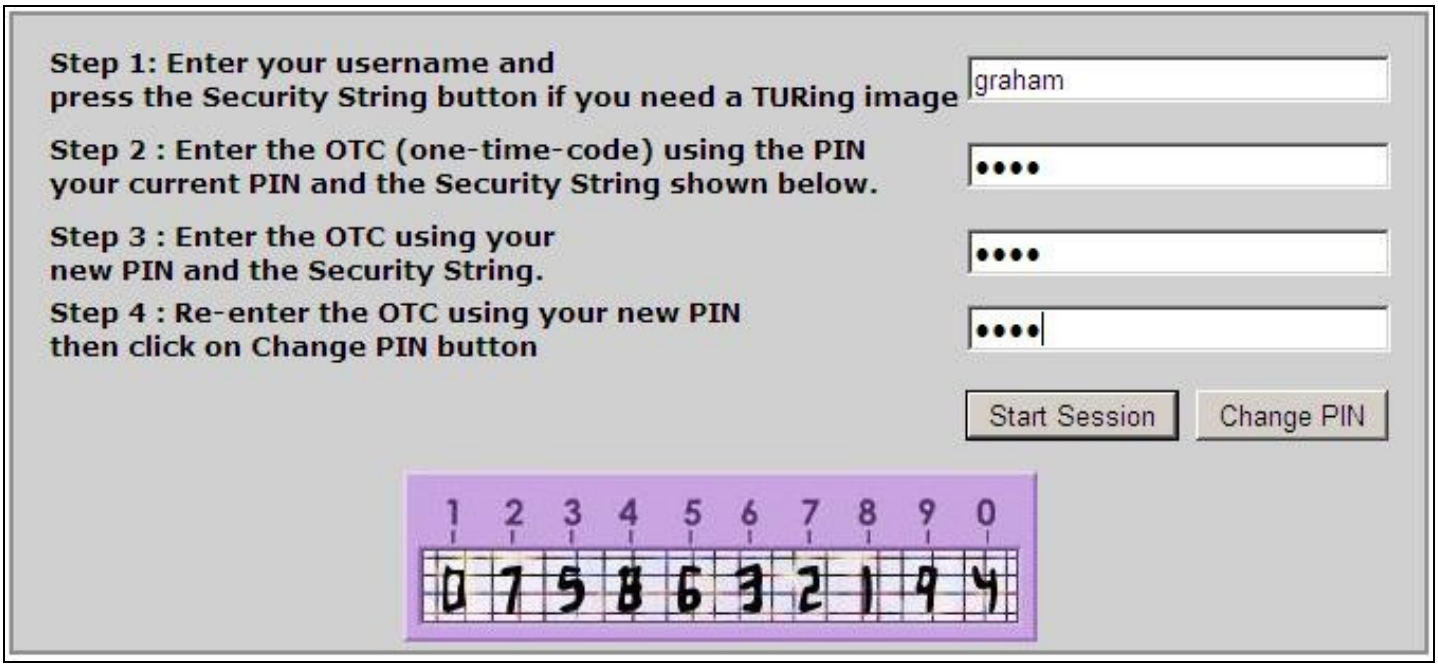
Virtual or hardware appliance: https://IP:8443/changepin2

software install: http://IP:8080/changepin2

ChangePIN Sample

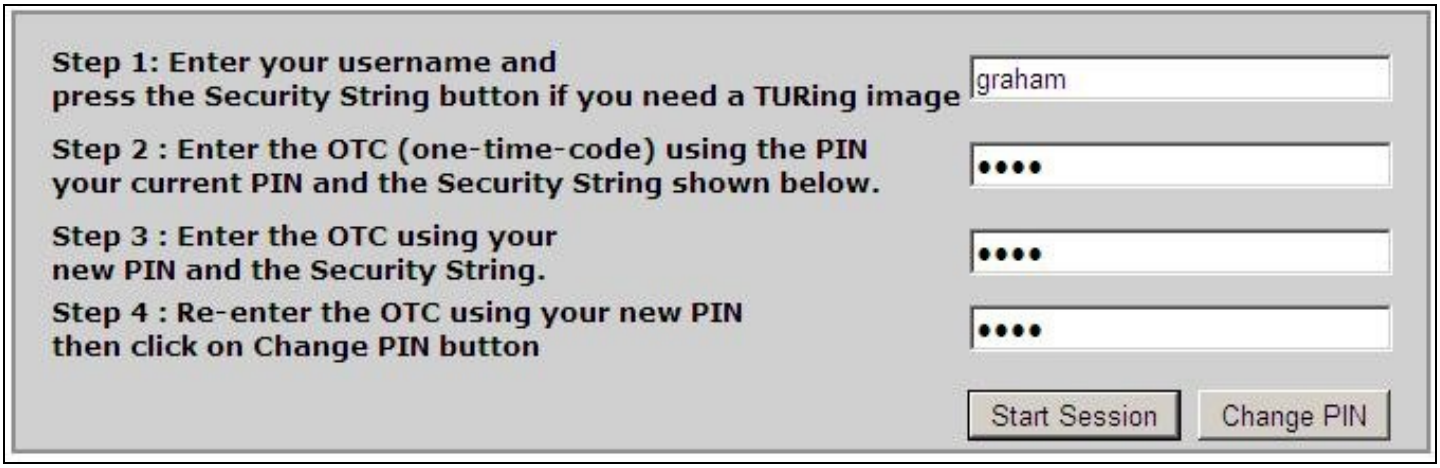
See also ChangePIN Samples

Turing ChangePIN



SMS ChangePIN

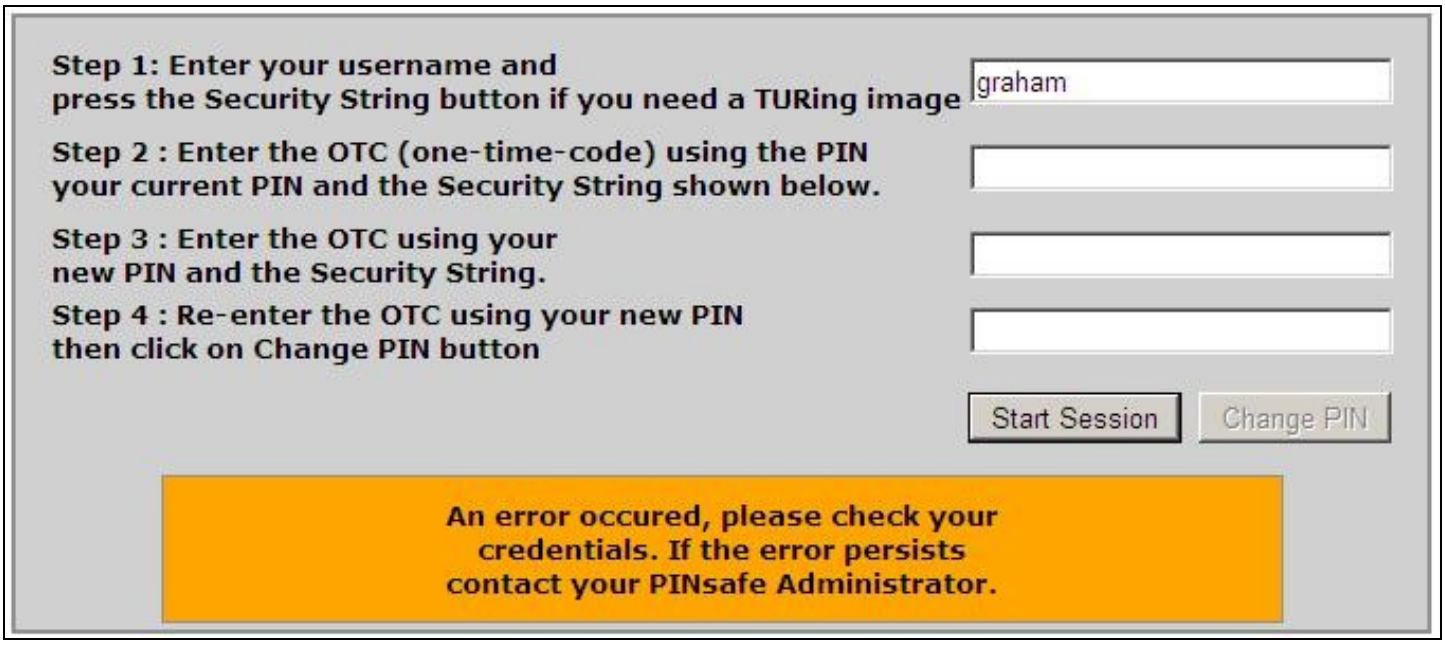
Note: When using SMS, the security string from the dual channel should be used (e.g. text on a mobile phone). **DO NOT** click start session.



Troubleshooting ChangePIN

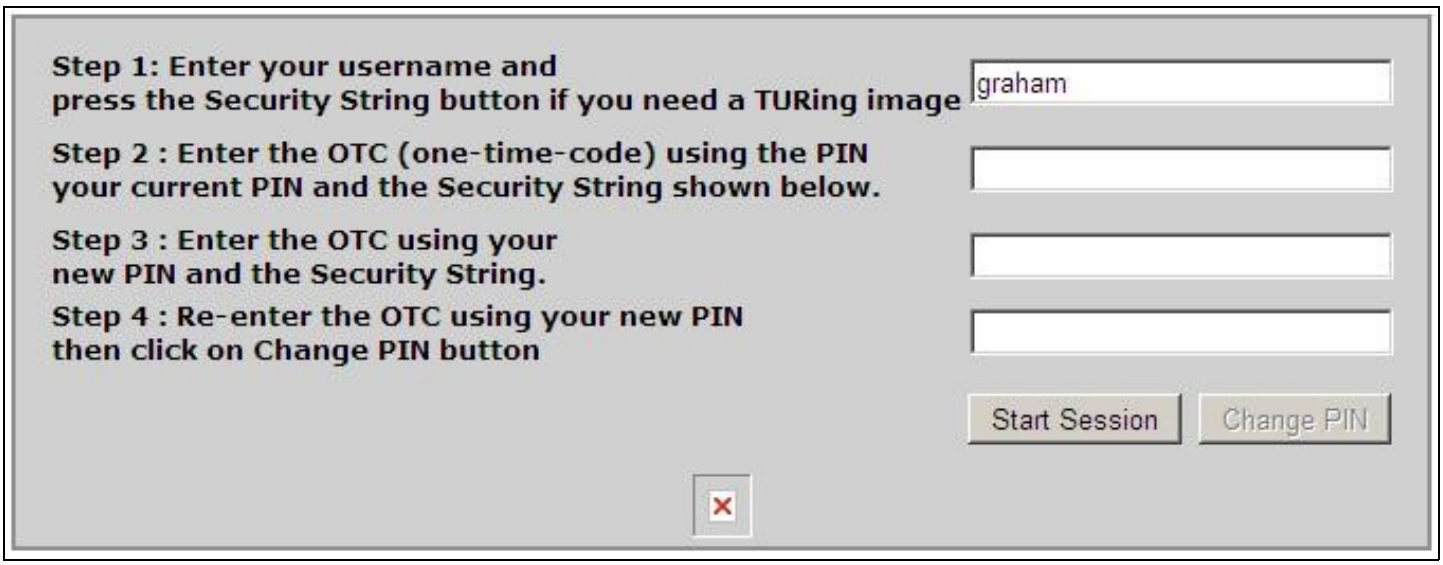
If using IE 9 test with compatibility mode enabled.

Incorrect Credentials Used



Single Channel Image fails to display

Single Channel Image fails to display due to incorrect image server setting. Verify the path by right clicking on the red cross and looking at the image properties.



If a self signed or invalid certificate is being used, or if the IP address instead of the hostname is used, then the image may not be displayed. Copy the URL from the properties of the red cross and paste into a browser and see if it is displayed with a certificate error.

Private IP is being used

If the url for change pin references the virtual or hardware appliance private IP not the public one then the image will not be displayed. Edit the entry for *imageserver* as detailed above.

Incorrect values for Swivel virtual or hardware appliance

Virtual or hardware appliance values incorrectly set. Ensure the following values are used for Swivel appliances:

```
<entry key="ssl">false</entry>
<entry key="server">localhost</entry>
<entry key="port">8181</entry>
```

PIN not complex enough

ChangePIN failed for user: xxxx, Error: The PIN is not complex enough.

The PIN entered is too simple and breaks the PINsafe rules defined in the Administration Console, The default for repeated digits is 0 and allows for no repeated digits.

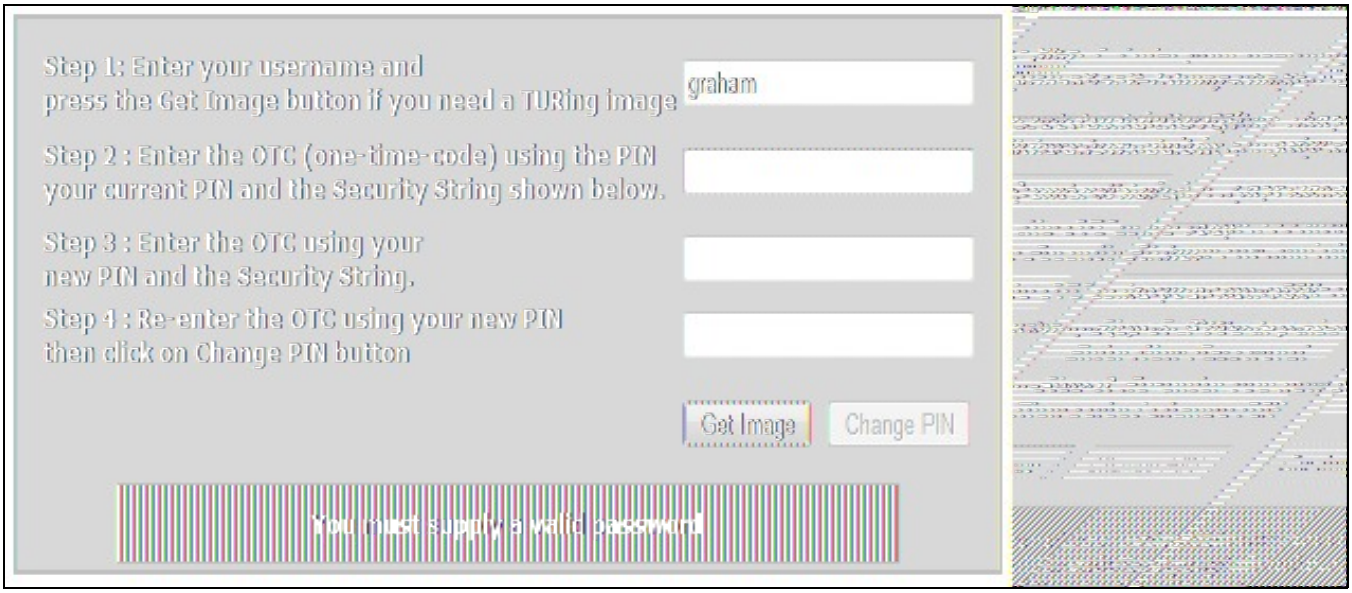
The user does not belong in the correct group

127.0.0.1 local:Session start failed for user: xxxxxx, error: The user does not belong in the correct group within the user repository to continue the authentication attempt.

The user may be attempting to start a single channel session when they are not part of the Single Channel group. This can occur when the user is permitted to use changePIN using SMS only. In this case do not click 'start session'.

You must supply a valid password

The option to Require Password is set to Yes under Policy > Password on the Swivel Admin Console, and the user has not entered a password. If this is not what is expected then verify on the Swivel server that the Policy > Password setting for require password is set to No.



Change PIN failed for user: username, error: CHANGE_PIN_PASSWORD_ERROR

On the Swivel administration console check to see if the setting under Policy/PIN and OTC that the *require password for PIN change* is set to Yes or No.

SSL certificate errors

One problem with the current changepin page is that the image is served by a different host from the main page. If that host uses HTTPS, and the certificate is not valid, then the image will not be displayed.

This is a modified changepin web page that gets around this problem by serving the image from the same host and port. It assumes that the host that changepin is running on can also deliver TURing images. This will be the case with all reasonably new Swivel virtual or hardware appliances, as the changepin and proxy applications run on the same host. The properties imagessl, imageserver and imageport are therefore ignored, and only imagecontext is relevant.

Another improvement in the attached file is that all text displayed on the page is listed at the top of the file. This makes it easy to customise the page to set your own text.

To deploy this file, download and extract the file changepin.jsp. Then use webmin, or a program such as WinSCP to upload the file to /usr/local/tomcat/webapps2/changepin, replacing the existing file. See also Copying appliance files How to Guide. **IMPORTANT: make sure you set the owner and group of this file to swivel.** Restart Tomcat to ensure the file is deployed.

You may find you need to clear the cached compiled version of the file before the new one will display. You can find this in /usr/local/tomcat/work/Catalina-proxy/localhost/changepin. Delete the contents of this **only when Tomcat is stopped**

Changes to the ChangePIN settings.xml don't take effect

If changes are made to the HTML and are not reflected in the ChangePIN page then they may be cached by the PINsafe server:

You may find you need to clear the cached compiled files for changepin before the new settings will take effect. You can find these in /usr/local/tomcat/work/Catalina-proxy/localhost/changepin. Delete the contents of this folder **only when Tomcat is stopped**.

This folder will be automatically re-created the next time it is required, so it is safe to delete.

Also consider completely closing down all of your web browser windows before accessing ChangePIN.

ChangePIN related error messages

User "graham" has been locked, reason: The user was required to change their PIN before this authentication.

The user account has been locked. This will occur if the user is required to change their PIN such as after an admin reset or after first login. When they try and login again, this error message will be displayed. Unlock the user account, ensure user knows they must change their PIN.

Access-Request by graham Failed: AccessRejectException: AGENT_ERROR_PIN_NOT_CHANGED

The users PIN was not changed. This could be caused by the account being locked, such as through a previous failed changePIN attempt.

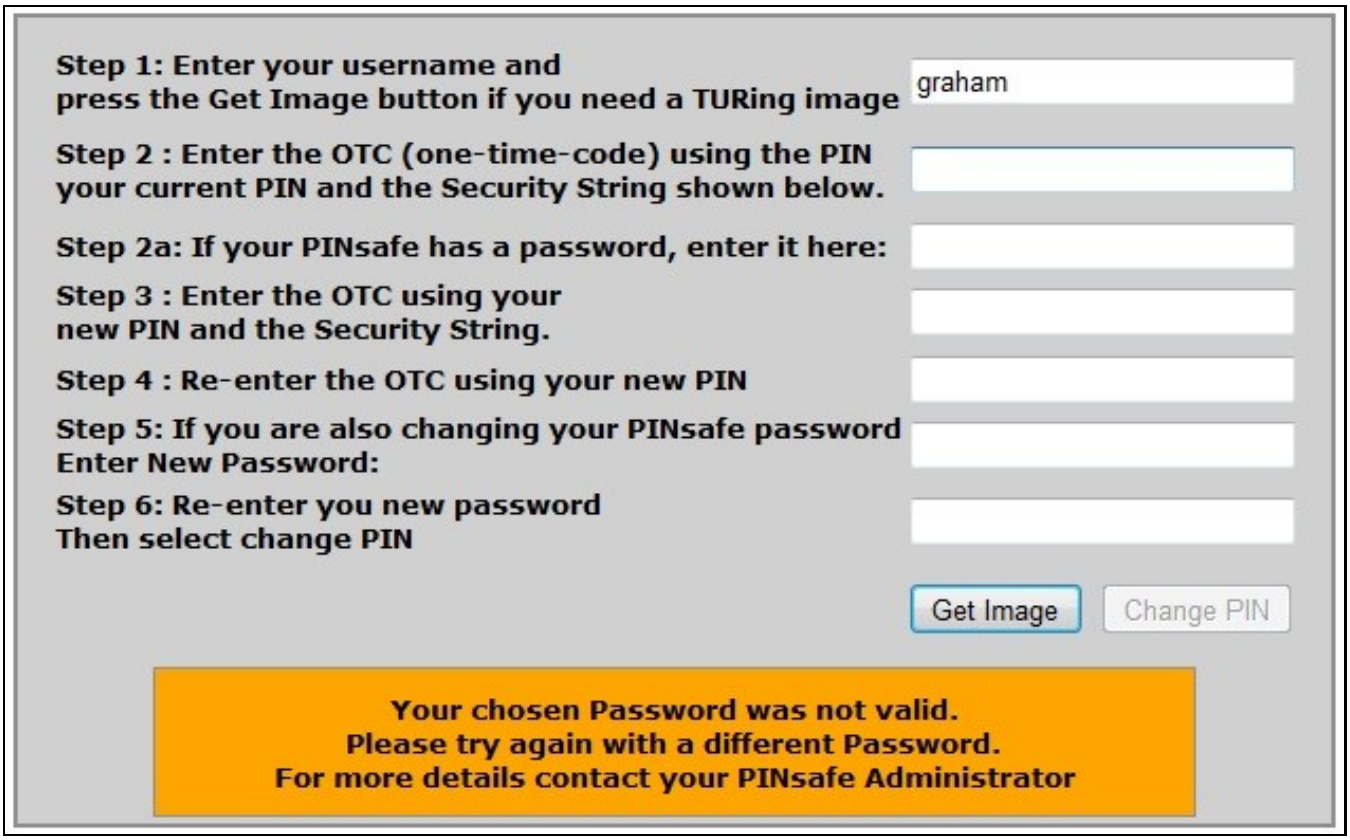
Change PIN failed for user: graham, error: The use of a static password is mandatory

The option to Require Password is set to yes under Policy Password, and the user has not entered a password.

Your chosen Password was not valid. Please try again with a different Password. For more details contact your PINsafe Administrator

Change PIN failed for user: graham, error: The password fails complexity policy.

A complex password was not entered. Retry with a more complex password. The password policy will determine if a password is valid for user. The password policy is set under Policy/password.



Cannot start PINsafe Session

The user does not exist in the Swivel database of users.

Cannot start PINsafe Session

Session start failed for user: graham, error: The user does not belong in the correct group within the user repository to continue the authentication attempt.

The user has started a Single Channel Image Request but is not a member of the correct group. Use SMS or Mobile Phone security strings to changePIN.



AgentXML request failed, error: The agent is not authorised to access the server.

The AgentXML may not be configured or have the wrong shared secret or IP address/Hostname. On the PINsafe Administration Console select the Server Agents and verify the values. On the ChangePIN settings, verify that the shared secret is correct, and that the IP Address or Hostname is correct. This may need to the a NAT address since it is usually the client that requests an Image.

CHANGE_PIN_PIN_ERROR:

The original OTC is incorrect. A correct OTC must be entered before a new OTC is entered. If using the single Channel TURing image, ensure session request by username is enabled under Server/Single Channel.