Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

1 8443 To 443 Port Address Translation

See 8443 to 443 Port Address Translation

2 AD Credential Change How to Guide

2.1 Overview

PINsafe uses an Active Directory Username and Password to read AD groups using LDAP. This document outlines how and where to change the Active Directory Username and Password Credentials on the PINsafe Administration Console.

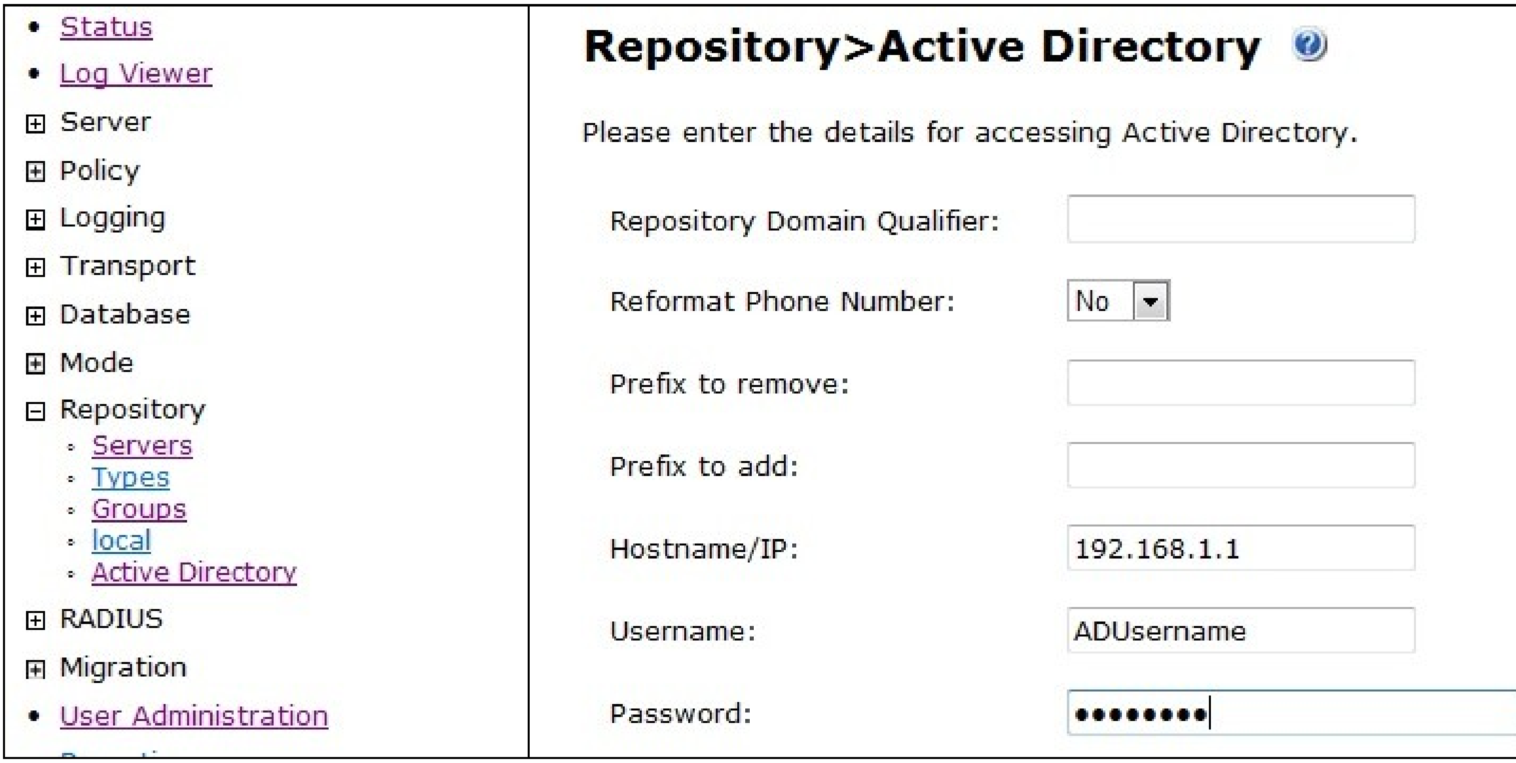
2.2 Prerequisites

PINsafe 3.x

2.3 Changing Active Directory Credentials

2.3.1 Active Directory Repository

On the PINsafe Administration Console select Repository, then the name of the required Active Directory Domain. The IP/Hostname, Username and Password can be changed as desired.



Repository>Active Directory

Please enter the details for accessing Active Directory.

Repository Domain Qualifier:

Reformat Phone Number: No

Prefix to remove:

Prefix to add:

Hostname/IP: 192.168.1.1

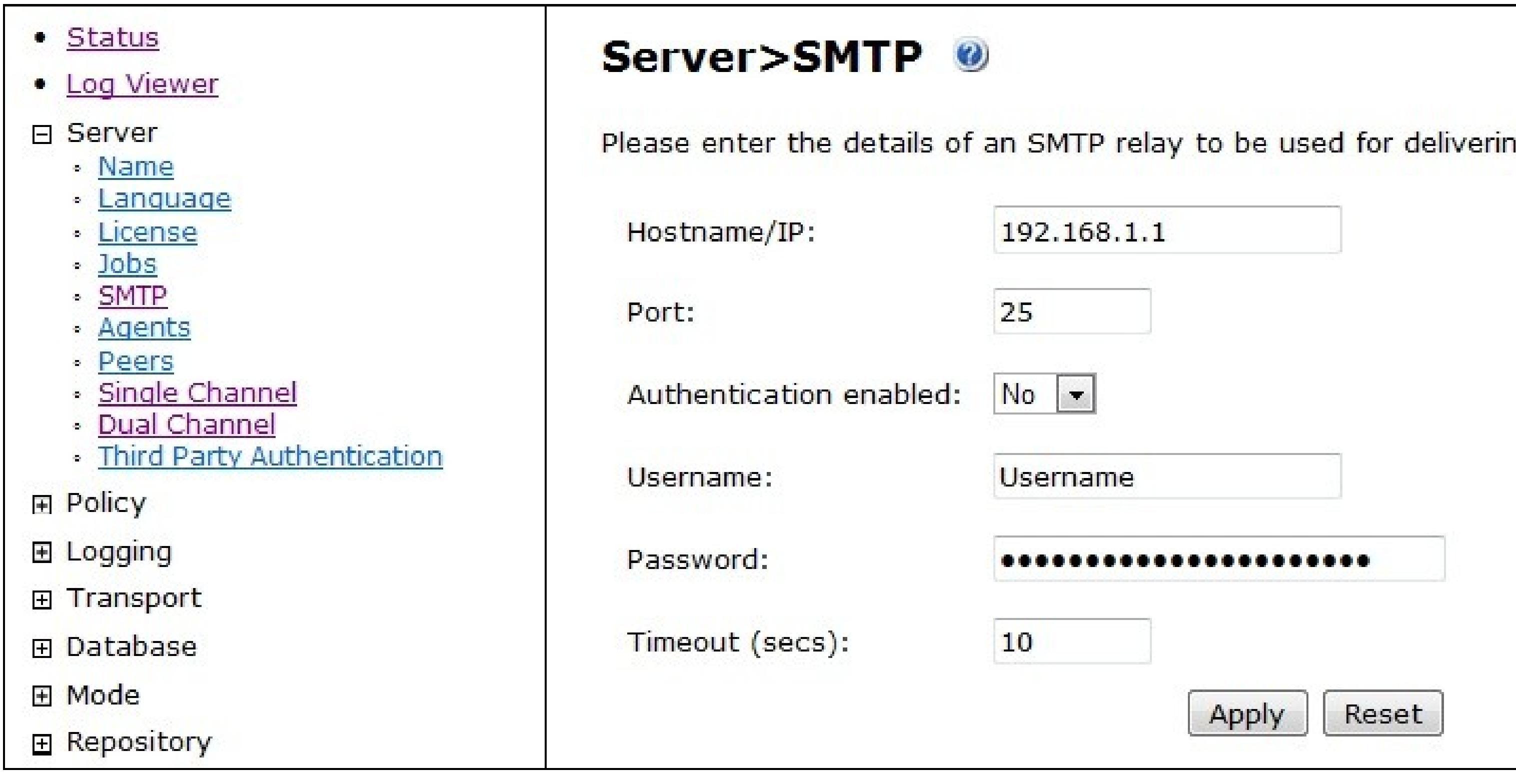
Username: ADUsername

Password: ••••••••

Repeat the AD credentials change on each PINsafe instance that has an entry for the AD server that requires the change.

2.3.2 Mail Server

Where the Active Directory Credentials are also used for Email authentication they will also need to be changed. On the PINsafe Administration Console select Server/SMTP, then change the credentials as required.



Server>SMTP

Please enter the details of an SMTP relay to be used for deliverin

Hostname/IP: 192.168.1.1

Port: 25

Authentication enabled: No

Username: Username

Password: ••••••••••••••••••••••

Timeout (secs): 10

The credentials must be changed on all PINsafe instances with an SMTP configuration.

2.4 Testing

To test the AD credentials are correct for AD authentication, try to browse the AD server, on the PINsafe Administration Console select Repository then the AD server name, and click on browse in Window. Correct credentials will allow browsing of the AD.

To test the SMTP credentials, force the system to send an email, such as resending a PIN on a test account that uses SMTP as its transport class. Observe the PINsafe logs for any errors.

2.5 Known Issues

2.6 Troubleshooting

3 AD data source configuration

4 Overview

Swivel carries out a **Read Only** lookup of the AD server using LDAP so no information is written to the AD server and there is no software to install on the AD server. Each Swivel instance must be configured separately.

Also see the Active Directory FAQ

The following steps are required for AD Configuration:

- On the AD server create distribution or security groups and populate with users
- On the AD server create a service account for Swivel to use
- On the Swivel server create an AD Repository
- On the Swivel server configure the Repository Groups
- On the Swivel server configure Transport Attributes
- On the Swivel server configure Transport Groups
- On the Swivel server Synchronise the AD Users

Swivel reads users from Containers (CN), groups in AD, and nested groups, but not directly from containers (OU). It is not possible to traverse domains unless Global Catalog is used, or Swivel reads that domain.

For further information on LDAP data sources see the LDAP How to Guide

5 Prerequisites

Swivel 3.x system

Repository Configuration Importing users from External Sources

6 AD configuration checks

Ensure network connectivity from the Swivel server to the AD server for LDAP

Check AD Groups exist

Check Swivel error logs for messages

Check Service account username and password

Use and LDAP browser to confirm the LDAP path (Swivel 3.6 has a built in LDAP browser)

Ensure Transport Attribute is correct in Transport\Attributes, this is usually mail for SMTP and mobile for SMS by Cell Phone.

If SMTP is to be used, ensure SMTP gateway has been configured under Servers/SMTP

Swivel can read the Global Catalog if this is configured on the AD server, this saves each appliance having to be connected to individually. The Global Catalog port must be configured and the Swivel server must connect to the Global Catalog server.

6.1 Configuring A/A instances of Swivel

Each instance of Swivel should be configured separately. The following should be noted:

- Ensure Synchronisation with AD occurs at different times on each Swivel instance with a suitable gap between synchronisations.
- Ensure that the configuration of each virtual or hardware appliance is the same as incorrect configuration can lead to users being removed/added and PIN numbers resent. Specifically check Repository Groups and Transports are the same on the Primary and Standby.
- Under Transport General it is recommended to disable **Resend credentials if destination changes:** by setting it to No. (This option removed in Swivel 3.9.6).

6.2 Configuring multiple AD repositories

- Where multiple AD sources are used, ensure that the SAM account name (**sAMAccountName**) is different for the sources. It may be useful to use the User Principal name (**userPrincipalName**) instead.

7 Active Directory Server Configuration Steps

There is no software to install on the AD server, and Swivel reads AD groups. For multiple AD Domains create the required groups on each domain, or use a global catalog server.

7.1 Create the Active Directory Groups

Users are added to Active Directory (AD) groups to allow them access to differing authentication resources. By creating additional AD groups different configurations can be made to suit the required environment. Existing groups can be used. The following documentation assumes the following configuration:

Swivel Users - who have access to all authentication methods

Swivel Administrators ? who have access to all authentication methods and admin rights

On the AD server:

Create a Swivel Organizational Unit (OU) Right Click on the domain then select New and then OU, enter the name Swivel

Within the Swivel OU create a Swivel Admin Group (CN) Right click on the Swivel OU then select New Group, enter the name Swivel Admin

Within the Swivel OU create a Swivel Users Group (CN) Right click on the Swivel OU then select New Group, enter the name Swivel Users

Note: Ensure that Distribution or Security Groups are used and not an OU, as Swivel cannot directly read an OU. Swivel will not read users in CN=Users,DC=domain,DC=com

7.2 Add users to the Active Directory Groups

On the AD server:

Add users to the Swivel Users and Swivel Admin group as appropriate. Ensure users have the correct information for transport, i.e. an email address and mobile phone number. It is recommended to test with a small number of users first to ensure all settings such as transports etc are correct.

NOTE: Swivel cannot handle primary groups or group membership that refers to trusted domains. These relationships are handled by Active Directory in a non-standard way that standard LDAP queries cannot discover. Do not use groups that are configured as primary groups for any user within Swivel , and do not use groups that contain users from trusted domains. If you need to include user from other domains, use Global Catalog as described above.

8 Swivel Server Configuration Steps

8.1 Configure SMTP Server Settings

On the Swivel server:

Select Server then SMTP, enter the IP address/Hostname of the SMTP gateway

click Apply to save the settings

8.2 Add the AD Repository Servers

On the Swivel Server:

Select Repository/General and create an Active Directory Repository, the name is descriptive and must be unique and up to 32 characters in length, and when created it should appear on the left hand side below Repository. Create additional Swivel servers for each AD Domain, or use a global catalog server.

Click Apply to save settings

8.3 Configure the AD Repository Server Settings

On the Swivel Server Administration Console:

Select Repository then the required AD server, its name will be that defined in the step above for adding the AD repository.

The following information needs to be entered on each AD Repository Configuration

- Hostname/IP address of AD Server
- Service Account User Name
- Service Account Password

Do not configure Synchronization schedule at this stage.

For further details see AD Repository Configuration Settings below.

Click Apply to save settings.

For information on changing AD Credentials see AD Credential Change How to Guide

8.4 Create Swivel Groups

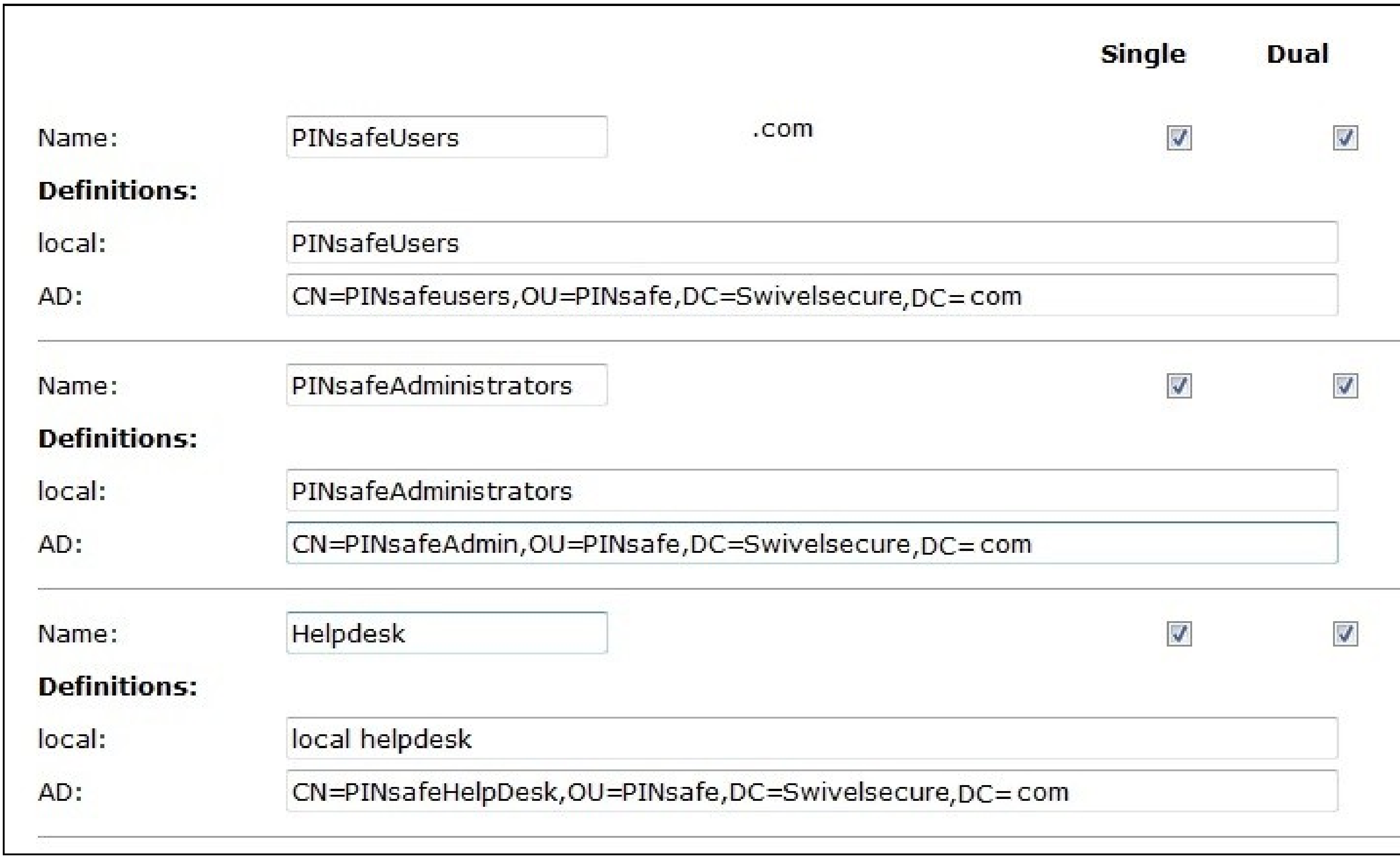
On the Swivel Server:

Select Repository/Groups and enter the Repository Group names corresponding to those created in Active Directory. Leave the fields blank that are not required. The input fields are case sensitive. Use an LDAP browser if unsure of the path, or if using Swivel 3.6 or higher use the inbuilt LDAP browser.

The format must be:

CN=<AD Container>,OU=<Organizational Unit>,DC=<mydomain>,DC=<com>

Example: CN=Swivel Admin,OU=Swivel,DC=swivelsecure,DC=com



Single Dual

Name: PINsafeUsers .com ☑ ☑

Definitions:

local: PINsafeUsers

AD: CN=PINsafeusers,OU=PINsafe,DC=Swivelsecure,DC= com

Name: PINsafeAdministrators ☑ ☑

Definitions:

local: PINsafeAdministrators

AD: CN=PINsafeAdmin,OU=PINsafe,DC=Swivelsecure,DC= com

Name: Helpdesk ☑ ☑

Definitions:

local: local helpdesk

AD: CN=PINsafeHelpDesk,OU=PINsafe,DC=Swivelsecure,DC= com

8.5 Configure Transport Attributes

On the Swivel Server:

Select Transport then Attributes. Ensure the settings are correct for each AD repository, usually:

- mobile for mobile phone
- mail for email

Other fields that are used may be telephoneNumber

For further information see Transport_Attribute

8.6 Configuring Transport Groups

Assign the AD groups to the required Transport class, the following Transport attributes are used for assigning groups:

- Group: Where security strings are sent to
- Alert Repository Group: Where information is sent regarding the user such as PIN numbers

For further information see Transport_Configuration

8.7 Sync the AD Database

On the Swivel Administration console, select User Admin and from the Repository drop down menu select the required AD server name then click on "User Sync". Users from the AD repository should appear. See also User Synchronisation.

8.8 Enable Automatic AD Synchronisation

If all the synchronisation is working as fully expected, the Swivel server can now be configured to automatically read the AD server at regular intervals. It is recommended that synchronisation should be configured once per hour. If an A/A pair is configured to synchronise then each Swivel instance must synchronise at differing times. See also User Synchronisation.

On the Swivel Server:

Select Repository then the required AD server. Set the required Synchronisation Schedule. For custom schedules see Schedule.

Click Apply to save the settings

8.9 AD Repository Configuration Settings

AD Import Information on the Swivel server is required as follows:

Repository Domain Qualifier: AD Domain name, this is used with the **Add domain qualifier:**

Reformat Phone Number: Yes No When the phone number is imported then Swivel will carry out some basic formatting as determined by the prefix to remove and add. Swivel will also remove extraneous characters and white spaces.

Prefix to remove: Swivel will remove a prefix from the phone number

Prefix to add: Swivel will add a prefix to the phone number, this could be for instance a country code.

Hostname/IP: AD server name, or entering an AD domain will pick up available AD server. If an AD replica is used, be aware that it may take some time for user information to be pushed out to replica AD servers. For redundancy an active directory with a Virtual IP or DNS can be used. Additionally two Swivel servers could be used, but ensure that they synchronise at differing times.

Username: AD service account, usually it is best to use a fully qualified domain name e.g. swivel@swivelsecure.com. The user needs to have permission to connect and bind using LDAP to the AD server.

Password: AD service account password, ensure that password ageing is not set or it is changed regularly

Allow self-signed certificates: Yes No Are certificates used on the AD server?

Username attribute: The username that the AD account reads. By default this is the SAM Account name, **sAMAccountName** for example; bob. It is possible to use the User Principle Name **userPrincipalName** so that the user has to enter their full username, for example bob@swivelsecure.com, users would need to enter this full address to authenticate. It is also possible to use the email address of a user by setting the Username attribute to **mail**. Note that this should be set during initial configuration, if the attribute is changed, then new users will be created with this different username and the old users deleted.

PIN attribute: Swivel can read an AD LDAP attribute that contains the users first PIN number, this AD LDAP attribute can be added here. It is not recommended to have a default PIN, but instead to use a randomly generated PIN that is sent to the user.

Password attribute: Swivel can read an AD LDAP attribute that contains the users first password, this AD LDAP attribute can be added here. It is not recommended to have a default password, but instead to use a randomly generated Password that is sent to the user. Note this is not the AD password but a Swivel password.

Import disabled state: Yes No Default: No. If the account is disabled in AD, should it be disabled or enabled when imported into Swivel. Contractors and 3rd parties can be configured as disabled so they cannot login to AD, but may still authenticate using Swivel.

Import disabled users: Yes No Default: No. If the account is disabled in AD, should it be imported into Swivel.

Ignore FQ name changes: Yes No Default: Yes. Changes to the AD infrastructure can lead to users account being deleted and re-created, users see this as new PIN numbers being generated. To stop this occurring Swivel can be set to ignore these changes.

Reformat Phone Number: Yes No Default: No. Reformat the mobile phone number using the fields **Prefix to remove:** or **Prefix to add:**

Mark missing users as deleted: Yes No If a user is deleted from the AD group that Swivel references, Swivel can mark it as deleted without actually deleting the account. If it is reinstated, then the user can be undeleted/restored in Swivel, and the user will retain their current PIN and security strings.

Port: 389 (Domain LDAP) 636 (Domain LDAP SSL) 3268 (Global Catalog LDAP) 3269 (Global Catalog LDAP SSL) Select the required port for communication.

Add domain qualifier: None Prefix Suffix When the user is imported from Active Directory into Swivel , the AD domain qualifier can be added either as a prefix or suffix to the username, or not used. For example a user imported from ad as *bob* may have the suffix @swivelsecure.com added and stored in Swivel as bob@swivelsecure.com.

Synchronization schedule: Choose how often Swivel will synchronise with the AD server. Note: an immediate synchronisation can be performed from the User Admin Screen

8.10 Check Password With Repository

It is possible for Swivel to check the AD password with some access devices. For Active Directory The username must be passed to AD as username@domain in order to authenticate via LDAP. This can be specified by using the the administrator or service account username for the repository configuration as administrator@domain.name, rather than just administrator or service account username, Swivel will automatically append the domain to the username when authenticating to AD, if one is not specified.

The AD domain used for Check Password with Repository is taken from the AD configuration. If it is authenticating with a different domain or sub domain the Check password with Repository may fail. Verify using the debug log. Also see Password How to Guide

8.11 Upgrading from Active Directory on a 2003 server to a 2008 server

Swivel supports Active Directory on 2008 Server

When upgrading from a 2003 to a 2008 server, ensure that the BaseDN remains the same. or you will encounter issues when attempting to sync. Specifically, it would be trying to look for the old FQDN and then abort. If you intend to change the BaseDN then you can avoid this issue by upgrading to the latest version of Swivel before migrating to AD 2008. The latest version would attempt to find the user elsewhere in the directory when performing a user sync if the BaseDN had changed, thus avoiding the abort issue.

8.12 Limiting users in a Repository

Swivel does not limit the number of users in a repository, but it may be possible to limit the number of users in the source group, see Active Directory Quotas

9 Additional Tools

9.1 Powershell commands

Powershell supports the use of commands to view AD details and may be of use in configuring Swivel, and are provided here for reference.

```
Import-Module activedirectory
```

```
get-aduser -Identity theadusername
```

```
get-aduser -Identity theadusername -properties *
```

10 Swivel log AD Error Messages

Repository "Active Directory", cannot be added to the database: possibly already exists.

This error can occur if the repository name already exists or the Database is still set to shipping mode. The repository "local" can be used but will also generate this error but can be ignored.

Exception occured during repository group member query, group: CN=SwivelUsers,OU=Groups,DC=swivelsecure,DC=com, exception 192.168.0.1:389; socket closed

A connection is being made but the socket is closed. This could be caused if the AD/LDAP server is restarted or if there is another AD/LDAP query in place. Check that the AD/LDAP synchronisations are set to occur at differing times and that they are not run too often. Typically synchronisation is set to occur every 60 or 120 minutes.

AcceptSecurityContext error, data 525, vece]

This is usually caused by when incorrect authentication is made against an AD domain. Check the username and password being used for the LDAP synchronisation, check the password has not been changed and the account is still active.

Test the user account with an LDAP browser.

Other possible errors for AcceptSecurityContext: *AcceptSecurityContect error, data xxx, vece* are as follows:

- 525 user not found
- 52e invalid credentials
- 530 not permitted to logon at this time
- 531 not permitted to logon at this workstation
- 532 password expired
- 533 account disabled
- 701 account expired
- 773 user must reset password
- 775 user account locked

Exception occurred: during repository attribute query, object: ERROR Exception occurred: during repository attribute query, object:<name>, attribute: sAMAccountName, exception:java.naming.InvalidNameException:<name>: [LDAP: error code 34 ? 000208F: NameErr: DSID-031001B3, problem 2006 (BAD_NAME), data 8350, best match of:?<name>?]; remaining name <name>

Names have failed to be found and existing names are not found. Check the AD paths and names.

No value for username attribute ?sAMAccountName?. The user "CN=x-x-x-x,CN=y,DC=z,DC=company,DC=com" has no value for username attribute "sAMAccountName". User not added.

A user has been added to a trusted domain where Swivel is looking for users within that group.

Java.net.NoRouteToHostException: No route to host? Exception occurred: during repository group member query, group: javax.naming.CommunicationException: xxx.xxx.xxx.xxx:389 [Root exception is java.net.NoRouteToHostException: No route to host],exception %2

or

Exception occured during repository group member query, group: CN=Swivel Users,OU=Groups,DC=swivelsecure,DC=com, exception javax.naming.CommunicationException: ad.swivelsecure.com:389 [Root exception is java.net.UnknownHostException: ad.swivelsecure.com]

Check the network connectivity to the AD server, ports, firewalls, routing, DNS, IP, etc.

ERROR 192.168.1.1 admin:Exception occurred during repository group member query, group: CN=Swivel users,OU=Swivel,DC=xxx,DC=swivelsecure,DC=com, exception ADserver1.xxx.swivelsecure.com:389

This can be caused by a user who is a member of the group Swivel users but is part of another domian. Swivel will not be able to read the attributes for that user. Swivel would need to connect to that AD domain or read a Global Catalogue Server.

No value for username attribute <attributeName> The user CN=x-x-x-x,CN=y,DC=z,DC=company,DC=com has no value for username attribute <AttributeName>. User not added
ERROR - Exception occured during repository attribute query, object: CN=something,OU=oux,offices,OU=Com,DC=bob,DC=corp, attribute: sAMAccountName, exception:javax.naming.NameNotFoundException: [LDAP: error code 32 -0000208D: NameErr: DSID-031001CD, problem 2001 (NO_OBJECT)

The user within the repository has no value set for the attribute that is configured to be used as the Swivel username; therefore an account cannot be created for that user. For example if Swivel was configured to use the Active Directory attribute for email address for the Swivel account name and this value was not set in AD for a given user.

This may happen when a user has been added to a trusted domain where Swivel is looking for users within that group, only the fact that the user is a member of the group is available, and not the attributes of that user.

admin:Sending alert to user "username" failed, error: The user does not have an associated alert transport.

A transport has not been defined for the user

Exception occured during repository group member query, group: CN=Swivel 2factor,CN=Users,DC=Swivel,DC=swivel,DC=secure, exception javax.naming.CommunicationException: 192.168.0.1:389 [Root exception is java.net.NoRouteToHostException: No route to host]

The error No Route to Host indicates a networking issue. Check to see if the Swivel server can Ping or Telnet on port 389 (or required port) to the AD or LDAP server.

11 Known Issues

Swivel cannot use the Active Primary Group as a Data Source of users, the effects of this are:

- A Swivel user must have a Primary Group (usually the Domain Users group), and a member of the group for which Swivel users are being read from.
- The Domain User group cannot be used as a group of Swivel users (unless another Primary Group is defined for the users)

Where AD groups are synced from Novell, combining multiple groups may create issues, remove the interlinking and retest.

User Sync Issues

Swivel 3.8 release 2 onwards, any error retrieving user details will skip over that user, but mark it as deleted (or actually delete the user, if mark as deleted is disabled).

Swivel 3.5 to 3.8 first release, if an error occurs trying to read a specific user?s details, it will only skip that particular user if the error is ?Not found?. Any other LDAP error will cause it to abort.

Group Sync Issues

Swivel 3.5 and later, Errors attempting to access LDAP or to read the group details will cause the user sync to abort. In earlier versions of Swivel, such errors could cause all users to be deleted.

<username> Failed to login. RADIUS: <86> Access-Request(1) LEN=57 <IP address>:12004 Access-Request by <username> Failed: AccessRejectException:

Swivel 3.8 userPrincipleName (UPN) fails, but using the sAMAccountName (SAM) account name authentication succeeds. This is caused by a bug and is resolved in Swivel 3.9

Note, this error can also be caused by other issues:

If RADIUS based auth attempt and RADIUS logging enabled. Possible options are: This indicates the user has failed to authenticate successfully. If no other errors are logged in relation to the authentication attempt then the cause is that the user entered the wrong credentials.

This can be caused when an SMS message is to be entered but a Single Channel Image is started, if so then it is expecting a single channel OTC login, until the image times out (default 120 seconds).

The wrong security string index was used (use OTC-String Index, Example 9381-01).

A previously used OTC was attempted to be used again.

12 Troubleshooting

Enable debugging in the Swivel Administration console under logging/XML and check for errors.

Cannot Sync with Active Directory

Use the LDAP browser under Repository/Groups or under the Repository/<AD repository>/Browse in window, and check for any errors.

If it is an existing system where synchronisation has been previously working, the sync may have stopped. Restart Tomcat and see if synchronisation works, if this is Swivel 3.7 or earlier, consider upgrading.

Cannot import users into AD

Is the AD Server accessible? Check by making a telnet connection from the Swivel server on port 389 or required port. Possible causes are firewalls, routing and network issues, SSL communications only to the AD server. AD server is down. Swivel Log will report an error.

Is DNS functioning? Check with a NSlookup. Swivel Log will report an error.

Does the AD group have any users in it?

License exceeded. Swivel Log will report an error.

Can the AD group be browsed through AD and does it show any users?

Are some users imported and not others?

Cannot import some users

Are users across multiple domains? Swivel can only read domains for AD domains that it is configured to read. Either create another AD domain or use Global Catalog.

If using the Global Catalog, is Swivel reading from the Global Catalog AD server? Is the Global Catalog port selected?

The same username exists on multiple AD servers? Use userPrincipalName

userPrincipalName is used but the user does not have a userPrincipalName set, this can occur with Administrator users where by default this is not set.

User Sync takes a long time

Swivel version 3.9.6 includes some enhancements to close LDAP connections and may improve performance for synchronizations.

If SSL is being used, try without SSL and see if User Sync time improves.

If domain name is beiing used, try sepcifying a specific hostname and see if User Sync time increases.

Network Troubleshooting

Can you ping the AD server?

Can you Telnet to the AD server?

Telnet using diagnostics or the command line of the virtual or hardware appliance to see if you can initiate a connection to port 389 (or port being used) of the ip address of the AD server?

Try the following:

```
[admin@primary ~]# telnet AD_Server_IP 389
```

If the connection succeeds you will get:

```
Trying 192.168.0.1...

Connected to 192.168.0.1(192.168.0.1).

Escape character is '^]'.

(You can press Ctrl-C to exit at this point) Connection closed by foreign host.
```

If the connection fails you will get:

```
Trying 192.168.0.1...

telnet: connect to address 192.168.0.1: Connection refused

telnet: Unable to connect to remote host: Connection refused
```

Null Values

If you try and read a user from an Active Directory but get a Null Value error message, it may be that there is no referential integrity. This means that a user can be deleted from AD but when you perform a get Members on the group that user will still be returned.

Prefix is not added to Telephone Number

See Phone Number Format incorrect

12.1 Error Messages

Abandoned User Sync for repository <repository name>

If a synchronisation encounters an error then the sync job will stop. Check the settings are correct, particularly LDAP group names, and check the logs for further associated errors. Has the AD infrastructure had any changes such as the renaming or move of an OU or CN?

LDAP: error code 49 and **AcceptSecurityContext error**

Swivel cannot authenticate to the AD server. Has the AD service account password Expired? Is the username/password correct? Try using different account details such as:

- userPrincipalName (username@domain) for the service account to login to AD
- domain\username
- CN=user,DC=domain,DC=local

Test the user account with an LDAP browser, and see if the LDAP can be browsed. We recommend the use of third-party software from Softerra called LDAP Browser. This is available as freeware and as a commercial paid-for product. Available here: http://www.ldapbrowser.com/

Membership of multiple alert transport group is not permitted for user

This occurs when users are member of more than one group that is assigned to a string transport entry or alert transport entry. The cause for this can be when users are added either purposely or accidentally to additional groups on the Active Directory or whichever repository type you are syncing with and a subsequent User Sync takes place in Swivel.

To resolve this issue, on the Swivel administration console select the User Administration screen. Find a user that is suffering from this problem. Change the View drop down on the User Administration screen to be 'Groups'. Make a note of the groups that the user is assigned to (represented by a tick/check mark). Then visit the Transport -> General screen. You now need to look for Transports you have defined, where these groups have a 'Alert repository group' drop down containing either of the groups you noted in the previous step. It is not possible to have a user assigned to more than one transport sting or transport alert. So you will need to remove the users from the offending group which has led to this situation.

No Transport Attribute found for User or **No Alert Transport Attribute found for User** Possible causes are:

Email Address (optional), if no value exists in AD a no transport attribute error message is logged

Phone Number (optional), if no value exists in AD a no transport attribute error message is logged

Transport has not been defined for user, see Transport_Configuration

Transport Attribute has bot been defined, see Transport_Attribute

Modifications have not been made but Swivel has not been Synchronised with Active Directory

The object "CN=swivel-users,OU=Groups,OU=Swivel,DC=swivel,DC=local" on repository "AD" is not a valid group.

This could be caused by:

- The swivel-users is actually a Container, rather than a group.
- swivel-users is not defined as a group, according to the LDAP standard. Swivel only looks for objects with objectClass=group.
- If it is a global group, it is possible that the account used to connect to AD does not have permission to read the group properties.
- Swivel cannot read primary groups.

13 AD LDS How to guide

Please see: ADAM How to guide

14 ADAM How to guide

14.1 Overview

PINsafe can use ADAM as a data source, this document covers the integration with ADAM.

This document is in the process of being written

14.2 Prerequisites

PINsafe 3.8 ADAM release

14.3 CSV Import to ADAM

PINsafe will only import those attributes that it requires to ADAM: those attributes are:

- username
- given name
- surname
- disabled flag
- transport attributes (e.g. mail)

Any other attributes given in the imported file will be ignored.

Therefore, if you need to import userPrincipalName, you will need to set that as the username attribute before importing. This will mean that uid will not be populated, but uid is not a required attribute, so that is not a problem. If both uid and userPrincipalName exist, PINsafe will ignore any value set for uid if the username attribute is set to be userPrincipalName.

In short, it doesn't matter whether you use uid or userPrincipalName as far as PINsafe is concerned, but it will only take notice of the one you have set as username attribute.

14.4 Testing

14.5 Known Issues

14.6 Troubleshooting

14.6.1 Error Messages

Error creating LDAP user "Username": [LDAP: error code 20 - 0000217B: AtrErr: DSID-03050758, #1: 0: 0000217B: DSID-03050758, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 90290 (userPrincipalName)]

User already exists

"Error creating LDAP user "Username": [LDAP: error code 19 - 0000052D: AtrErr: DSID-033807A4, #1: 0: 0000052D: DSID-033807A4, problem 1005 (CONSTRAINT_ATT_TYPE), data 2245, Att 9005a (unicodePwd)]"

When a user is created in ADAM it gets created and is reflected in PINsafe Console. If the user is created in PINsafe it is not reflected in ADAM.

This is due to policy settings in ADAM. When you create a user directly in ADAM without a password, it is created but marked as disabled.

When you create a user through the PINsafe console, you have to choose the repository option either to generate a random password or to enter one manually. If you choose not to enter a password, you need to change the policy settings in ADAM to allow empty passwords. If they are entering a manual password, it might not meet the requirements.

admin:Exception occurred during repository attribute query, object: , attribute: rootDomainNamingContext, exception: [LDAP: error code 49 - 8009030C: LdapErr: DSID-0C0903CF, comment: AcceptSecurityContext error, data 533, v2580]

First of all, ensure that the password has been set and is correct for your bind user.

If you find that you are unable to use the Distinguished Name and password of the bind user you have created, it could be one of two problems:

- The ADAM or AD LDS instance (service) you created may not be running as a Domain user. This can be the cause if you are attempting to bind with a domain user from an existing Windows Domain.
- The ADAM or AD LDS user you created within the directory is disabled by default. Try changing the msDS-UserAccountDisabled attribute from TRUE to FALSE. Also note that if a password is not set then this can cause this attribute to be set to TRUE. If the user account is disabled by this attribute then you will not be able to bind with it.

15 Administration console customization

16 Overview

This page outlines customizations that can be made to the Swivel Administration console. Such customizations should only be carried out with agreement with Swivel support. Customizations will be overwritten on upgrade so will need to be backed up and reapplied to each Swivel instance after upgrade.

17 Prerequisites

Swivel 3.x

18 Custom modifications

18.1 Background Colours

The background colours are set by a style sheet called interface.css under pinsafe/interface

Appliance: /usr/local/tomcat/webapps/pinsafe/interface/interface.css

The key entry to change black to white on the background colour as shown below

```
 td#banner-left, td#banner-center, td#banner-bottomright {
 border-bottom: 1px solid black;
 background-color: white;
 color: white;
}
```

18.2 Background Logo

The background colours are set by a style sheet called logo.gif under pinsafe/interface

Appliance: /usr/local/tomcat/webapps/pinsafe/interface/logo.gif

19 Testing

20 Known Issues

21 Troubleshooting

22 Administration Console Login Guide

22.1 Overview

This document outlines how to login to the Swivel Administration Console.

22.2 Prerequisites

Swivel 3.x

22.3 Swivel Administration Console Login Guide

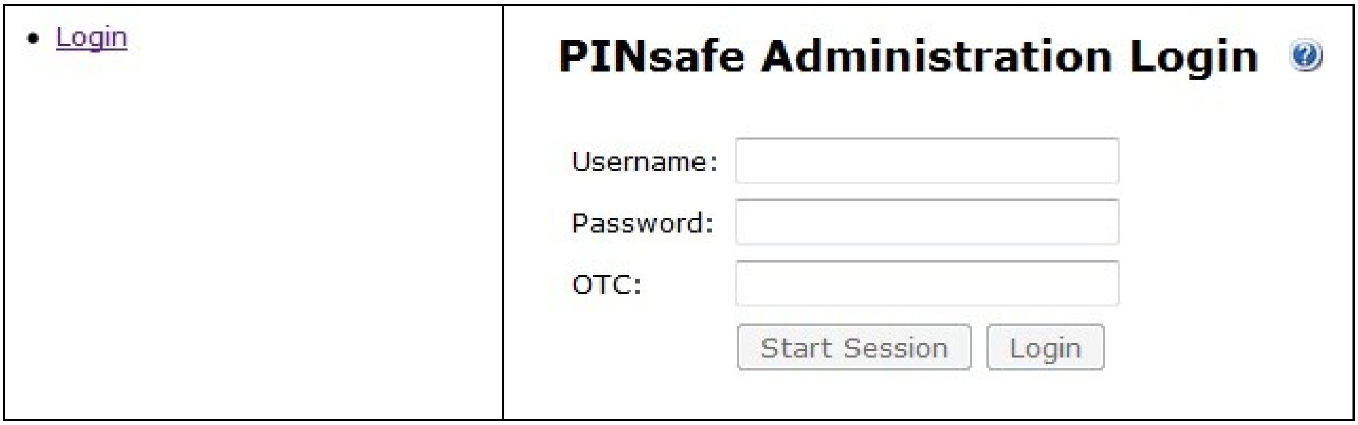
22.3.1 Connect to the Swivel Administration Console

In a web browser open a connection to the Swivel instance, this may vary depending upon the installation, the typical Swivel configurations are given below:

- Swivel Appliance: https://<IP>:8080/pinsafe
- Swivel software install: http://<IP>:8080/pinsafe

For issues with Administration Console Login see Cannot login to PINsafe admin console

A login screen should appear with fields to enter Username, Password and OTC



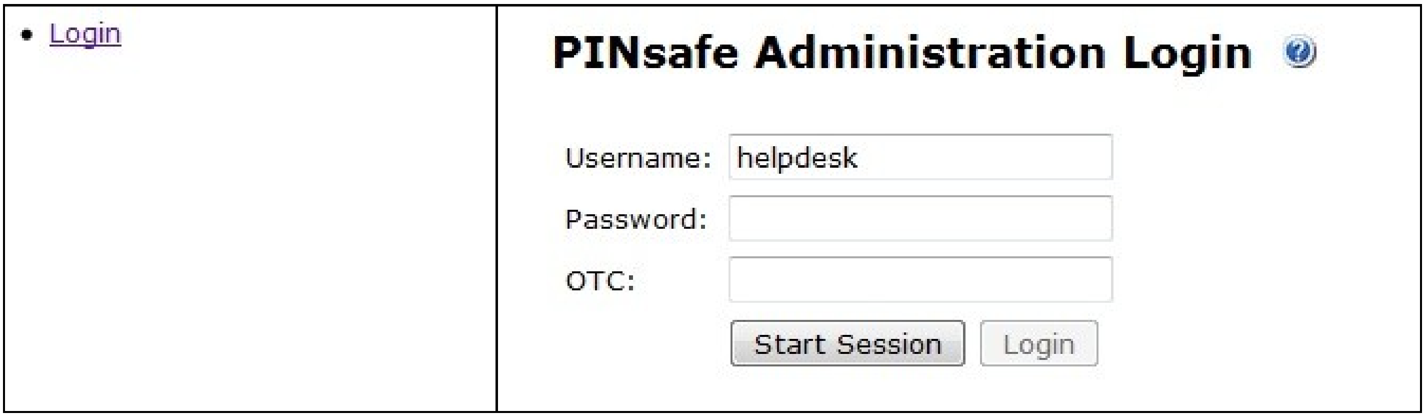
22.3.2 Login to the Administration Console

The Swivel Administrator should have configured access to the Swivel Administration console, which may have been delivered automatically in an email or by SMS, with the following information:

- Username
- Password (optional)
- PIN number
- Security String for login (optional), by SMS, email, mobile phone client

For information on how to extract the One Time Code from the Security String, using the PIN number see PINsafe User Guide

Enter the Username



PINsafe Administration Login

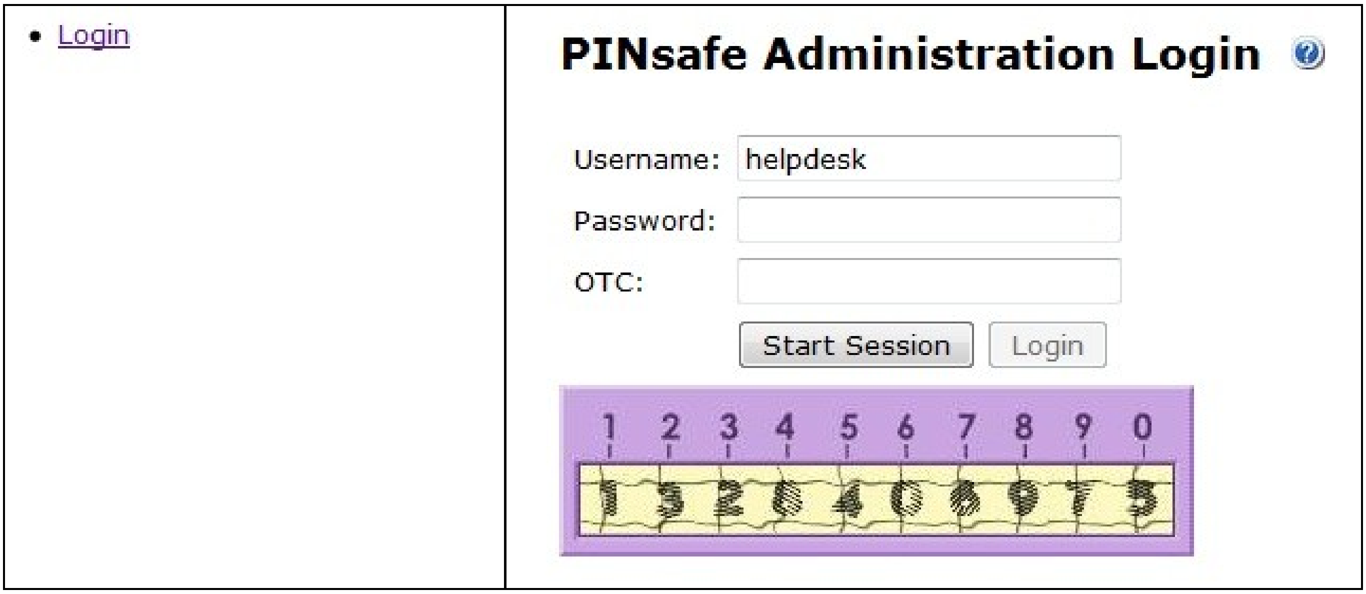
Username: helpdesk

Password:

OTC:

If you have been assigned a Swivel password enter it, otherwise leave the password field empty.

If you have a security string already, then using the PIN enter the OTC, (never enter the PIN number), otherwise click start session to generate a security string, as below.



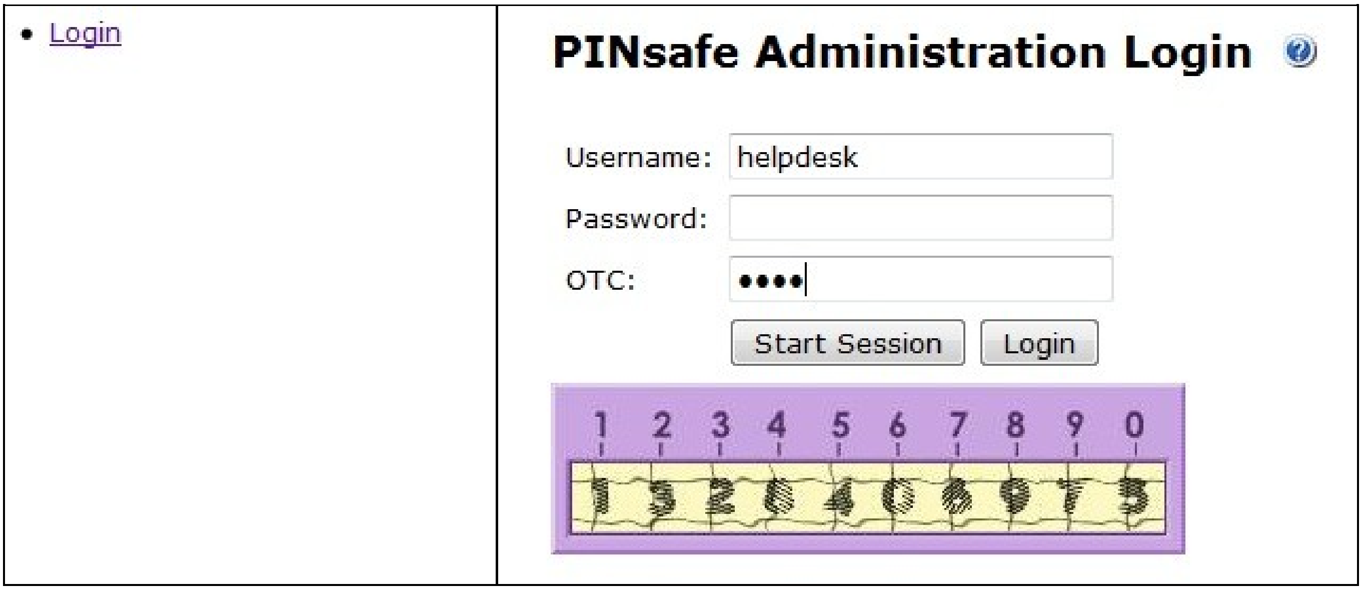
PINsafe Administration Login

Username: helpdesk

Password:

OTC:

Enter the One Time Code in the OTC field as below, then click login.



PINsafe Administration Login

Username: helpdesk

Password:

OTC: ●●●●

A successful login should either display the Status Page for Administrators, or the User Administration for Helpdesk users.

22.4 Known Issues

The cursor will automatically revert back to the password field rather than the OTC field.

22.5 Troubleshooting

Check the Swivel logs, see Troubleshooting Files FAQ

You cannot login to the Administration console unless you have either Admin or Helpdesk level access rights.

see Cannot login to PINsafe admin console

23 Administration Synchronisation

24 Overview

Administration Synchronisation allows the Swivel configuration allows changes on one Swivel instance to be pushed out to other Swivel instances. Changes on any Swivel instance can be configured to be sent to other Swivel instances.

One Swivel instance is configured as a Broker to show which which settings are synchronised.

Allowing the **Synchronise configuration** adds a **Config sync type** drop down menu and a **Sync now** button to pages that allow synchronisation.

There are 3 synchronisation settings:

- Automatic - push out changes to other Swivel instances (configured as Automatic or Manual)
- Manual - do not push out changes, but receive changes from other Swivel instances
- Disable Sync - do not push out or receive changes

24.1 What can be Synchronised

The following may be synchronised

- Swivel Administration console Policy>General settings
- Swivel Administration console Policy>PIN and OTC settings
- Swivel Administration console Policy>Password settings
- Swivel Administration console Policy>Self-Reset settings
- Swivel Administration console Policy>Helpdesk settings
- Swivel Administration console Policy>Console Login settings
- Swivel Administration console Policy>Mobile Client settings
- Swivel Administration console Policy>Banned Credentials settings
- Swivel Administration console Policy>Reporting settings
- Swivel Administration console Repository>Groups settings (new Groups requires a Sync)
- Swivel Administration console Repository>Attributes settings

24.2 What cannot be Synchronised

The following settings (among others) are not synchronised

- CMI configuration (Networking, backup, etc)
- Webmin configuration
- Swivel Administration console Transport>General
- Swivel Administration console Transport>Transport_Name
- Swivel Administration console Repository>Repository_Name
- Swivel Administration console RADIUS>Server
- Swivel Administration console RADIUS>NAS

25 Prerequisites

Swivel 3.9.7 onwards

Firewall rule to allow synchronisation, see Firewall Appliance Configuration The Swivel appliance firewall is automatically updated as part of the Swivel core patch release version patch.3.10.2.1950.swivel onwards to allow access on port 61616.

26 Configuration

26.1 Synchronisation Administration Settings

Synchronise configuration: default No, Options Yes/No

Broker IP: IP address of the Broker. You need to designate one Swivel appliance as the broker, and use the IP of that for all appliances.

Broker port: default 61616, the port to be used for sharing configuration information

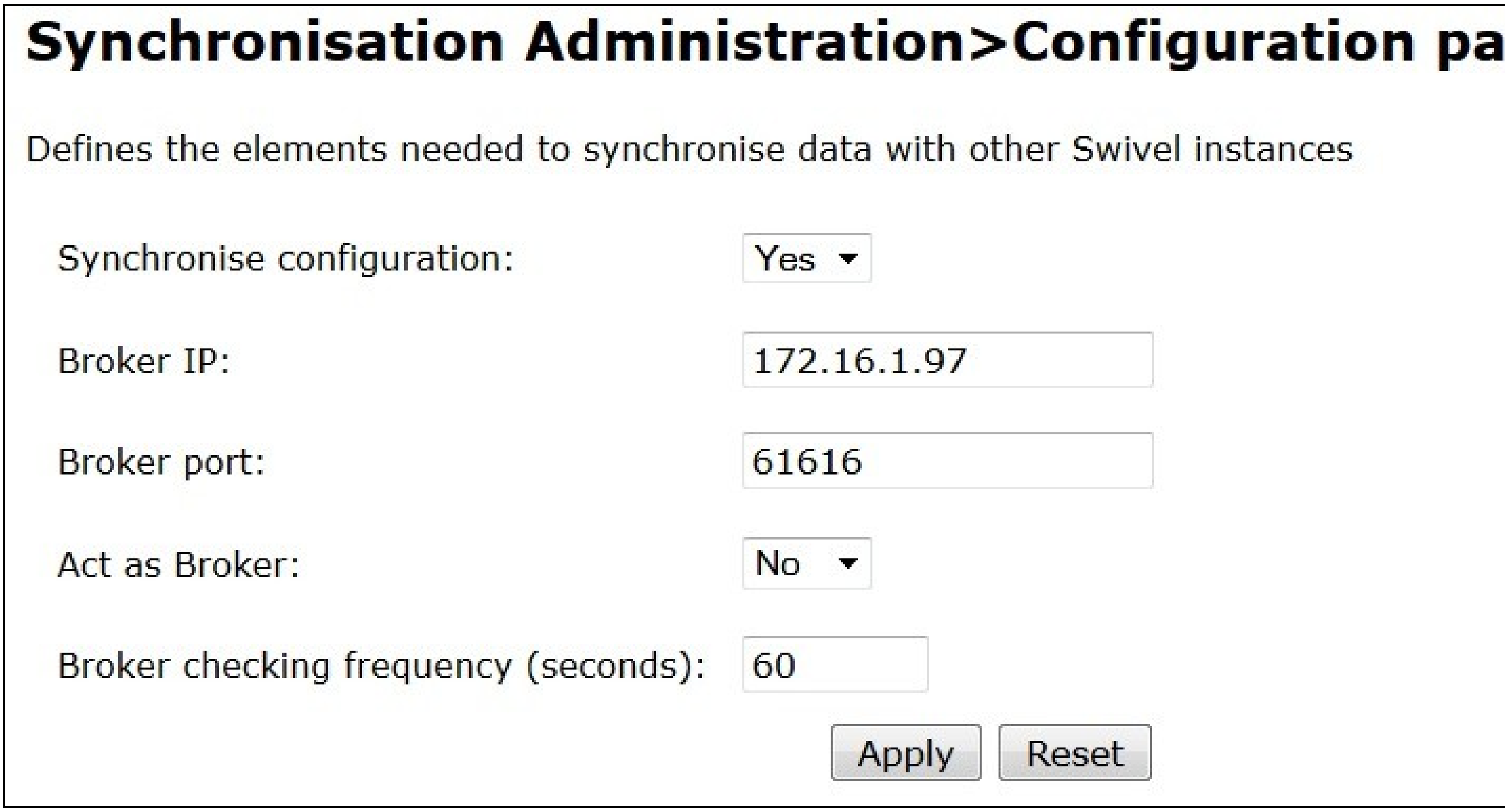
Act as Broker: default No, Options Yes/No, define a Swivel instance as the broker from which configuration information can be read

Broker checking frequency (seconds): default 60, time interval to reconnect if connection is lost from the broker

Synchronisation settings

Swivel Synchronisation setting	Action on Apply	Action on Sync Now ?	Apply from other Swivel server	Sync now from other Swivel server ?
Manual	no settings pushed out	push all settings in page	receive changes	receive all settings in page
Automatic	push all changes	push all settings in page	receive changes	receive all settings in page
Disable Sync	No Synchronisation	Disabled	No change	No change

? Note where groups are synchronised with Sync now, the settings are synchronised, but groups not on the target will not be created.



Synchronisation Administration>Configuration pa

Defines the elements needed to synchronise data with other Swivel instances

Synchronise configuration: Yes

Broker IP: 172.16.1.97

Broker port: 61616

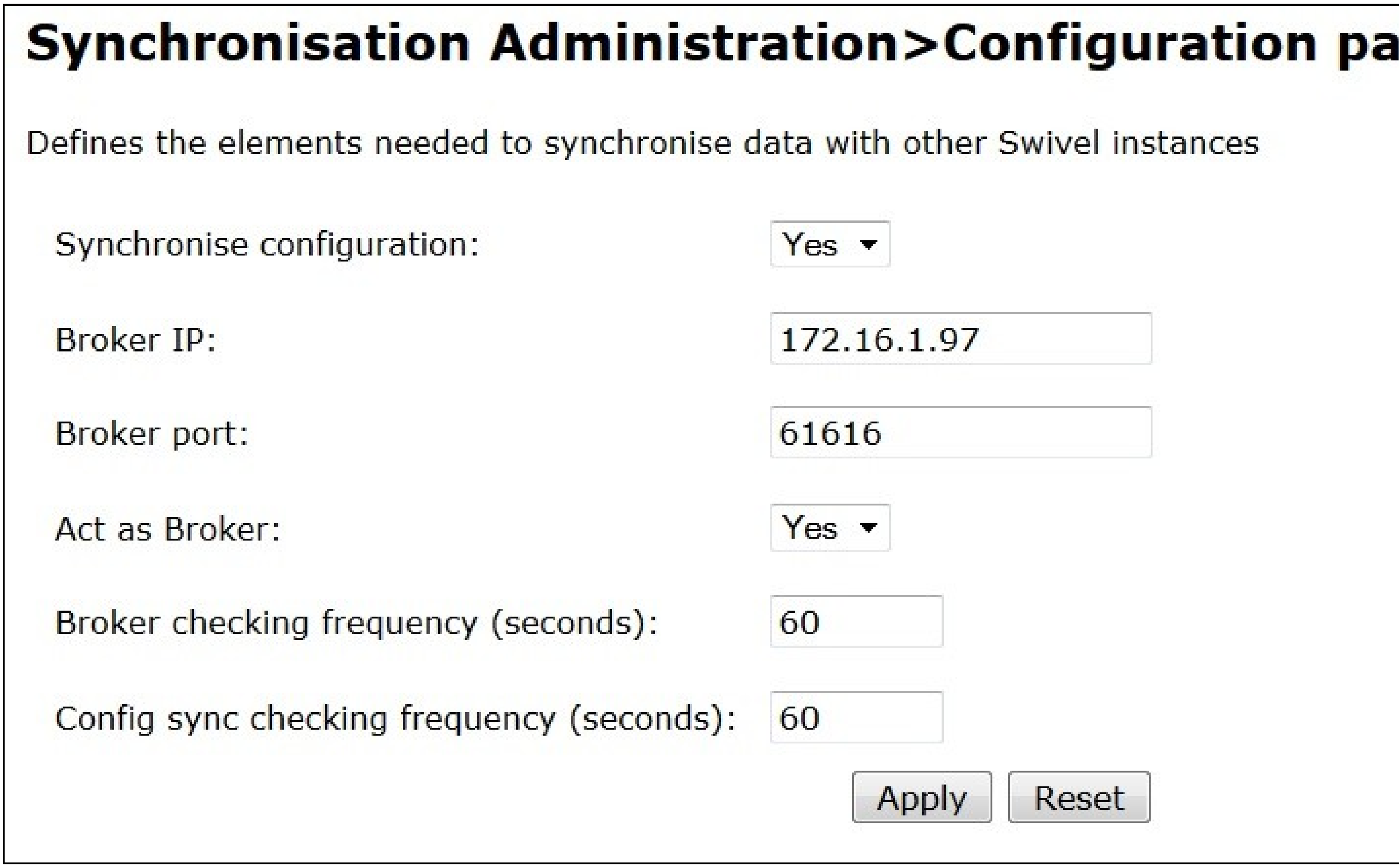
Act as Broker: No

Broker checking frequency (seconds): 60

26.2 Synchronisation Administration additional Broker Setting

The broker additionally has the following setting:

Config sync checking frequency (seconds): default 60 seconds, this how often the synchronisation state is checked. The broker will send information about configurations with a sync type **Manual** or **Automatic** and show the sync status compared to the broker in the status screen.



Synchronisation Administration>Configuration pa

Defines the elements needed to synchronise data with other Swivel instances

Synchronise configuration: Yes

Broker IP: 172.16.1.97

Broker port: 61616

Act as Broker: Yes

Broker checking frequency (seconds): 60

Config sync checking frequency (seconds): 60

26.3 Synchronisation settings

The settings that can be synchronised have an option for;

Config sync type', Default Disable sync, options: Disable sync, Manual, Automatic

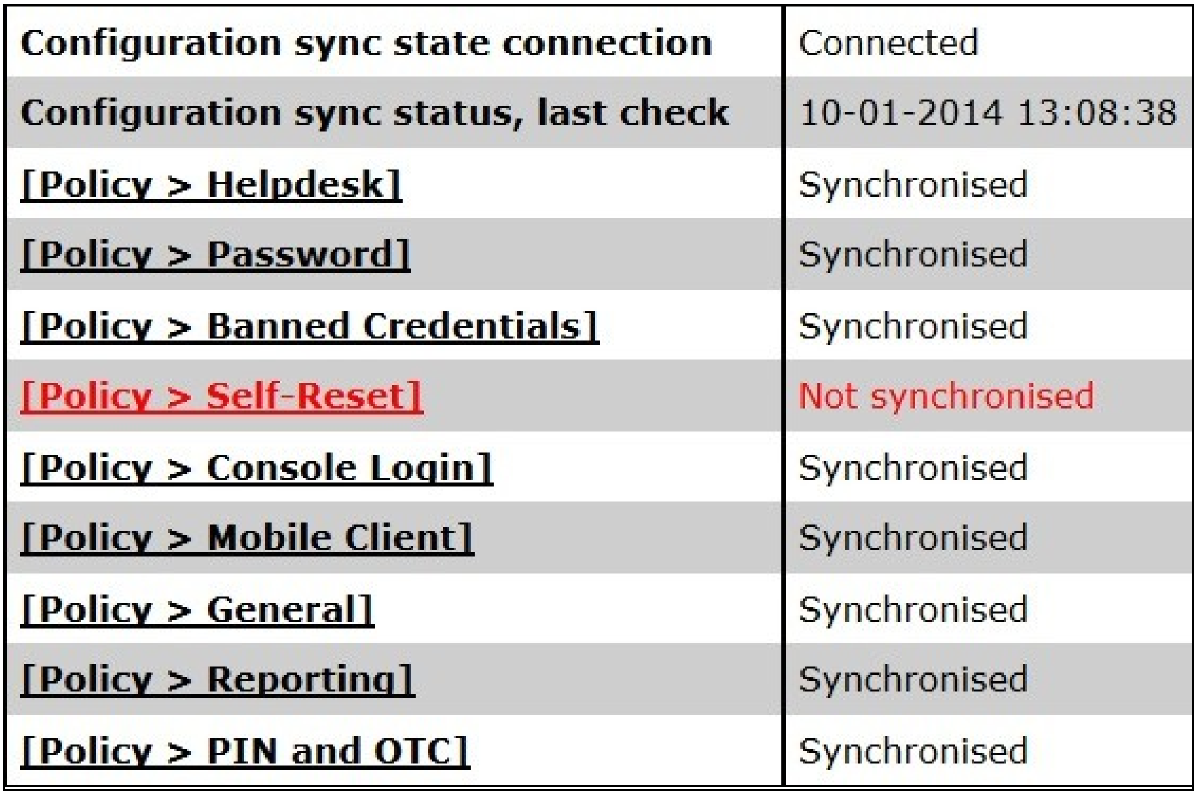
Disable sync - There is no synchronisation

Manual - Changes applied will not be synchronised, but the appliance will be able to receive synchronisation messages and they will be applied when the **Sync now** button is used.

Automatic - the changes applied on that Swivel instance will be applied to other Swivel instances who are configured as Manual or Automatic. A *Synchronisation data have been sent* will be displayed.

26.4 Synchronisation Status

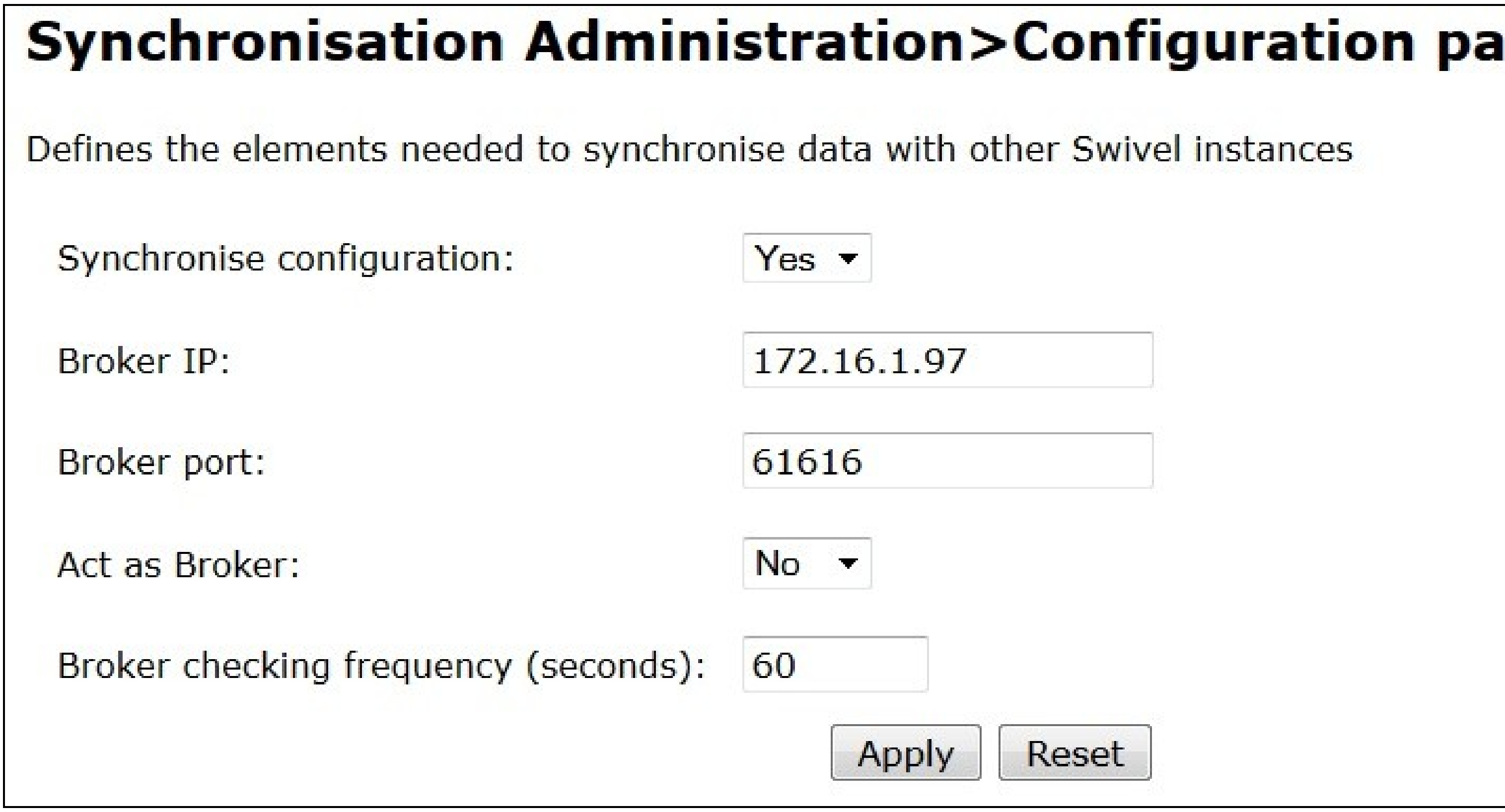
The status page shows the synchronisation status of the Swivel instance. Entries are listed as either Synchronised or Not Synchronised for that Swivel instance.



Configuration sync state connection	Connected
Configuration sync status, last check	10-01-2014 13:08:38
[Policy > Helpdesk]	Synchronised
[Policy > Password]	Synchronised
[Policy > Banned Credentials]	Synchronised
[Policy > Self-Reset]	Not synchronised
[Policy > Console Login]	Synchronised
[Policy > Mobile Client]	Synchronised
[Policy > General]	Synchronised
[Policy > Reporting]	Synchronised
[Policy > PIN and OTC]	Synchronised

27 Testing

On configuration a successful synchronisation will display a Connected message.



Synchronisation Administration>Configuration pa

Defines the elements needed to synchronise data with other Swivel instances

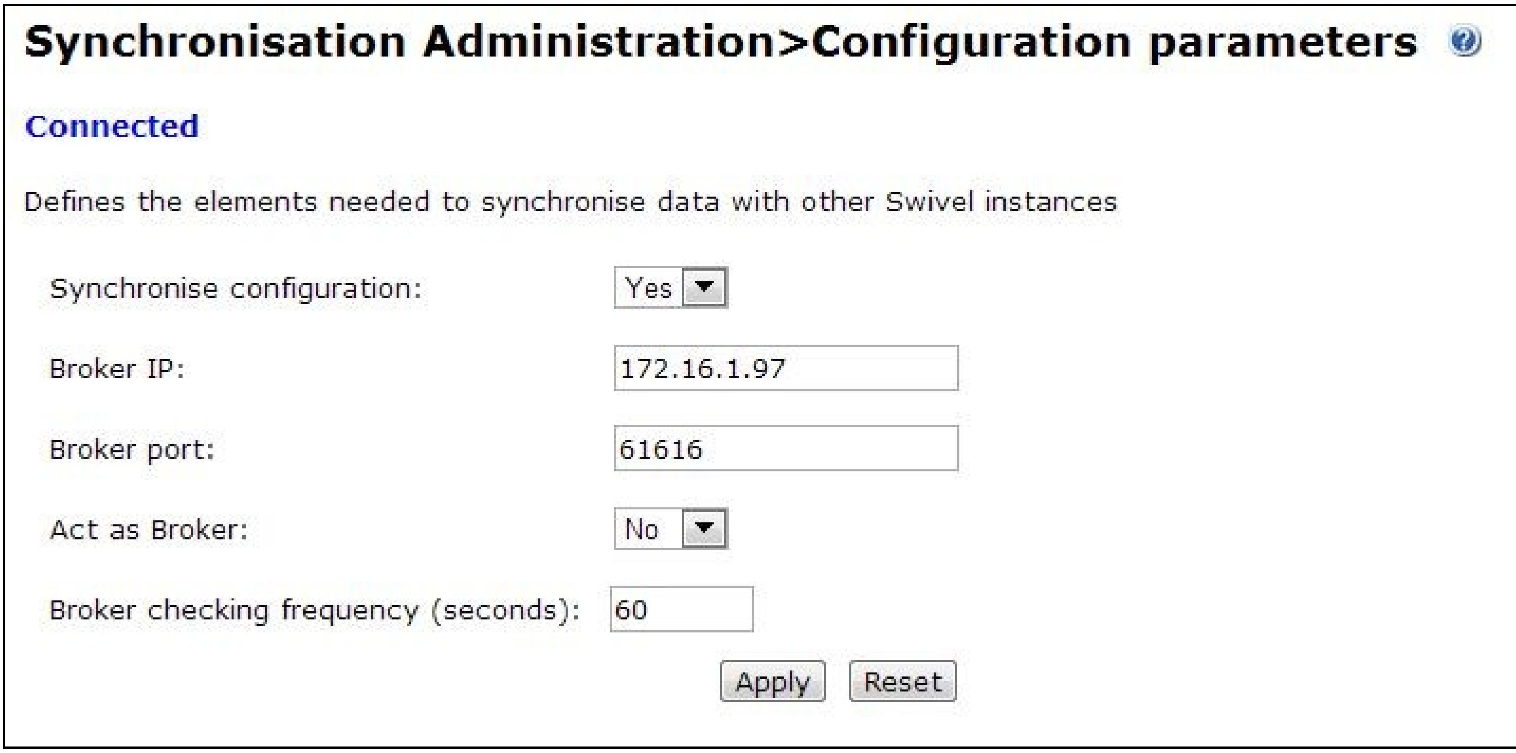
Synchronise configuration: Yes

Broker IP: 172.16.1.97

Broker port: 61616

Act as Broker: No

Broker checking frequency (seconds): 60



Synchronisation Administration>Configuration parameters

Connected

Defines the elements needed to synchronise data with other Swivel instances

Synchronise configuration: Yes

Broker IP: 172.16.1.97

Broker port: 61616

Act as Broker: No

Broker checking frequency (seconds): 60

The Status page will show the status for Broker or or connected to the broker:

State local sync broker Active

Configuration sync state connection Connected

Check connectivity with telnet to the broker

```
telnet 172.16.1.97 61616
```

```
CacheEnabledSizePrefixDisabled MaxInactivityDurationInitalDelay'TcpNoDelayEnabledMaxInactivityDurationu0TightEncodingEnabledStackTraceEnable
```

27.1 Standard Startup Messages

From Swivel version 3.10.3

27.1.1 Standard Non Broker Startup

Sync connection broker established, topic: PINsafe.Sync.Config.State

Subscriber created on topic: PINsafe.Sync.Config.State

Sync connection broker established, topic: PINsafe.Sync.Config

Subscriber created on topic: PINsafe.Sync.Config

Publisher created, topic: PINsafe.Sync.Config

27.1.2 Standard Broker Startup

Sync connection broker established, topic: PINsafe.Sync.Config.State

Publisher created, topic: PINsafe.Sync.Config.State

Sync connection broker established, topic: PINsafe.Sync.Config

Subscriber created on topic: PINsafe.Sync.Config

Publisher created, topic: PINsafe.Sync.Config

Sync broker has been started

28 Known Issues

29 Troubleshooting

Configuration fails to synchronise

Ensure that the Broker is running and can be contacted

Ensure Port and IP address details are correct

Under Synchronisation Administration>Configuration, set Synchronise configuration to No, Apply, set to Yes and Apply, then test

Config sync type' drop down menu and **Sync now** are missing. These are only enabled when the Synchronisation Administration>Configuration Parameters is set to Yes

29.1 Error Messages

Error establishing connection:

A connection cannot be made to the Administration Broker. Has a firewall rule to allow synchronisation been configured, see Firewall Appliance Configuration, are there any network devices blocking configuration? The Swivel appliance firewall is automatically updated as part of the Swivel core patch release version patch.3.10.2.1950.swivel onwards to allow access on port 61616.

Error starting sync broker

If a Swivel instance is connected to another broker, it is not possible to start the broker.

Error establishing connection 192.168.1.10: 61616

The Broker may be starting up, restarting or not running

30 Agents How to Guide

30.1 Overview

Agents are required to allow Agent-XML authentications to be made against the Swivel server. This document outlines how to use, configure and add agents.

30.2 Prerequisites

Swivel 3.x

30.3 How to add an Agent

The Agents allows devices to communicate with the Swivel core for authentication information. Only devices specified by IP address and shared secret are permited to authenticate. Multiple Agent entries can be created, even from the same IP address provided the shared secrets are different for each device.

On the Swivel administration console select Server/Agents. Enter the details for the agent and click on apply, the agent will then be saved. The following attributes are available:

Name: A descriptive name that is used in the Swivel logs

Hostname/IP: The Hostname or IP address of the device that will be making the agent requests. Ranges can be specified using CIDR (Classless Inter-Domain Routing) notation, for example if you put an IP address of 192.168.1.0/24, this will cover all IP addresses starting with 192.168.1.x.

Shared secret: A password that must be entered on the Swivel server agent and the device that will be making agent requests.

Group: Default: ANY, Options: ANY, Swivel group names. Here a specific access device can be configured to only allow certain groups of users to authenticate to that device.

Authentication Modes: Default: ANY, Options: ANY, Dual Channel Only, Single Channel Only. The access device can be configured to allow any type of authentication or to only allow only dual channel or allow only single channel authentication.

Check Password with repository: Yes/No, default No, This allows the repository password to be checked against the repository, by Swivel for the specified Agent. This option was moved from a global setting to an Agent and also to RADIUS NAS setting in Swivel 3.8. See Password How to Guide and LDAP How to Guide.

Username attribute for repository: Default: blank, the attribute to be used for this Agent. See also User Attributes How To.

Allow alternative usernames: Yes/No, default No. See also User Attributes How To.

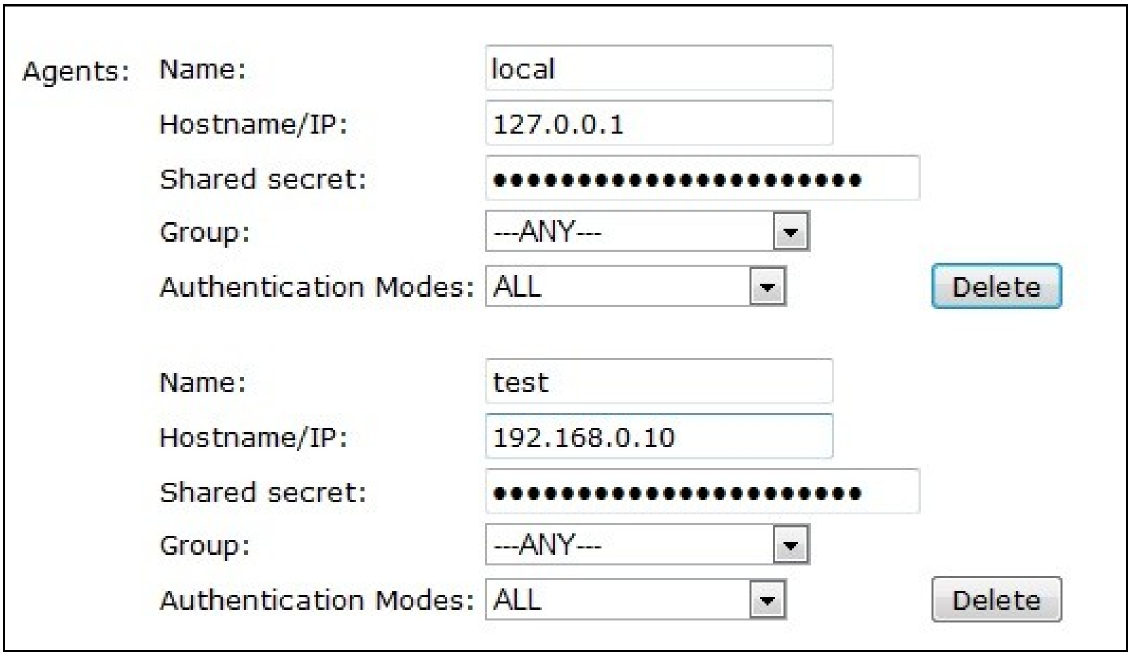
Alternative username attributes: Default: blank, the additional attributes to be used for this Agent, each attribute should be seperated by a comma, ','. See also User Attributes How To.

Can act as Repository: Yes/No, default No, the Agent can act as a repository

URL Check Password: Default: blank, used by the Remote Sync Agent to check a password against a repository

Encryption/Decryption key: Default: blank, used by the Remote Sync Agent for secure communications

Example configuration



Agents:

Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: test
Hostname/IP: 192.168.0.10
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

30.4 Using additional attributes for authentication

When using additional attributes for authentication see User Attributes How To

30.5 Testing

Configure the agents, make agent requests and check the logs.

30.6 Known Issues

30.7 Troubleshooting

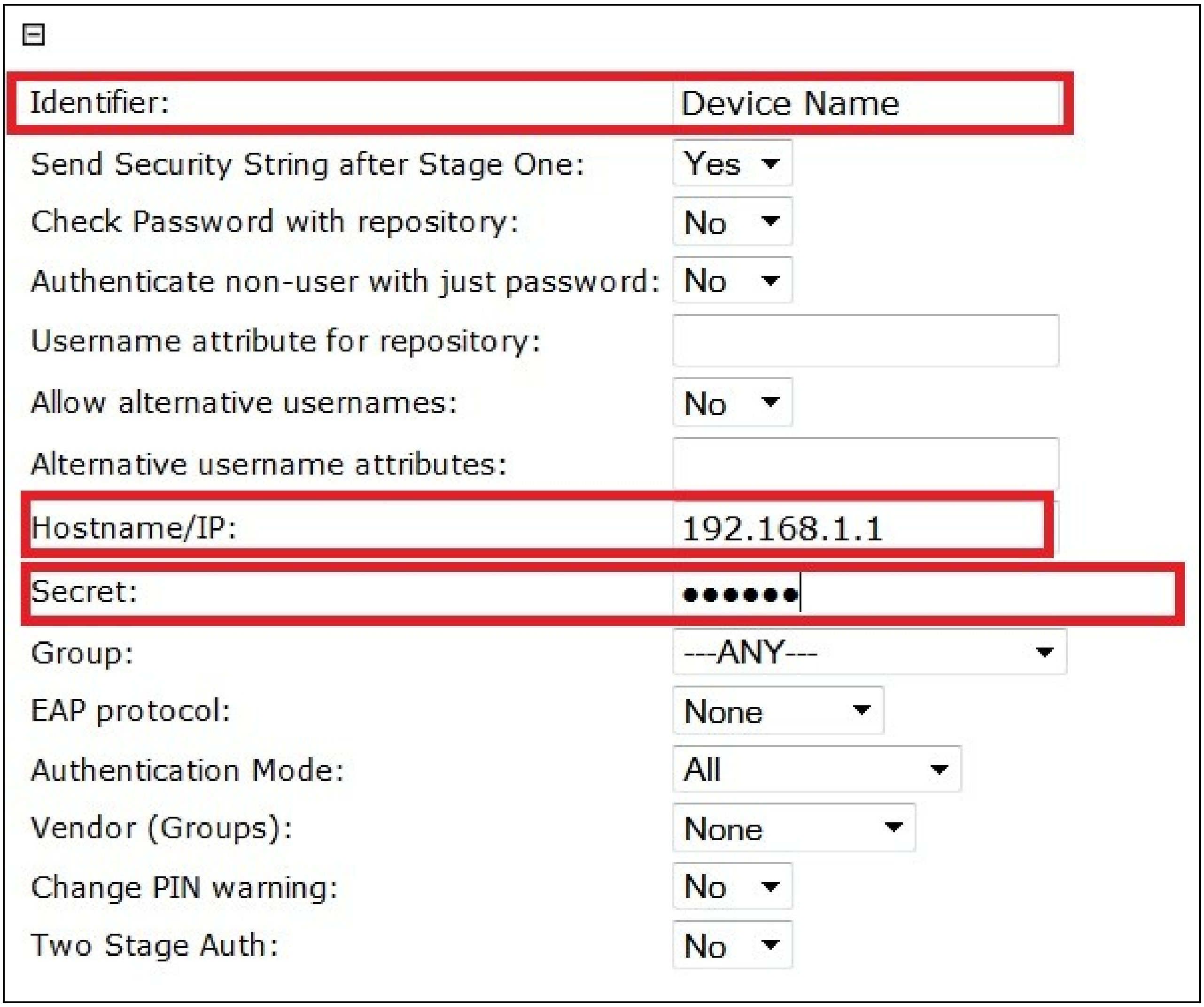
AgentXML request failed, error: The agent is not authorised to access the server.

An Agent-XML request is being made against the Swivel server but is not permitted to do so. If access should be allowed create an entry on the Swivel Administration Console under Server/Agents. If an entry exists verified the shared secret is the same on Swivel and the access device.

31 Allow session request by username

The Swivel server can be configured to return an image stream containing a TURing image by presenting the username via the XML API or the SCImage servlet.

On the Swivel Administration console under Server/Single Channel, set ?Allow Session creation with Username:? to YES.



Identifier:	Device Name
Send Security String after Stage One:	Yes
Check Password with repository:	No
Authenticate non-user with just password:	No
Username attribute for repository:	
Allow alternative usernames:	No
Alternative username attributes:	
Hostname/IP:	192.168.1.1
Secret:	••••••
Group:	---ANY---
EAP protocol:	None
Authentication Mode:	All
Vendor (Groups):	None
Change PIN warning:	No
Two Stage Auth:	No

To test your configuration you can use the following URL using a valid Swivel username:

Appliance

https://Swivel_server_IP:8443/proxy/SCImage?username=testuser

Software install

http://Swivel_server_IP:8080/pinsafe/SCImage?username=testuser

32 Appliance Disk full

33 Symptoms

Log files fill the disk space as they are not correctly being purged.

33.1 Checking Disk Space

The following command from the command line may show the disk space usage as 100%

df ?k

```
/dev/sda3      Use 100% Mounted on /backups
```

The disk space on a healthy system will look similar to the below sample output

```
[admin@standby ~]# df -k
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/sda2             20641788   2196276  17396872  12% /
/dev/sda3             10317860   1940240   7853500  20% /backups
/dev/sda1               124427     13761    104242  12% /boot
none                    517268         0    517268   0% /dev/shm
/dev/sda7              7091968     48636   6683076   1% /support
/dev/sda5              2063504     35952   1922732   2% /tmp
```

or df -m to see usuage in Mb

The following command may be of use in viewing where the disk usage is:

du -h --max-depth=1

Where depth is the number of folders to look within

33.2 Common file locations to check

As well as disk space, it is also important to check the number of files, as a large number of small or even 0 byte files can cause issues.

33.2.1 Disk space in /backups

View the backups using ls -la

Each backup is stored in the format as ddmmyy.number.tar.gz

The file size can be seen, large backups (200 Mb+) can cause the disk space to fill up, the backups contain some logging data as described below.

33.2.2 Disk space in /var/log/messages

Log files may build up in /var/log/messages

33.2.3 Disk space in /var/log/swivel

This folder contains Swivel log messages for differing error levels such as : Warning, Error, Fatal

33.2.4 Disk space in /var/lib/mysql

Transaction logs may build up in /var/lib/mysql, this is caused by A/A appliances being out of synchronisation. The transaction logs consist of binaries that contain data edits and/or relays that is information sent to a MySQL slave.

33.2.5 Disk space in /var/spool/clientmqueue

Mail logs for events are stored here

33.2.6 Disk space in /var/spool/mail

Mail logs for users are stored here

33.2.7 Swivel 3.7.3727

Swivel 3.7.3727 contains debugging information for Repository syncs that may produce a large number of files and the files may need to be purged. To prevent the files being generated upgrade to a more recent version of Swivel. As a temporary measure they can be deleted and a low frequency of repository sync can be set. The files are named:

profile.<date>.data

and reside in:

<path to Tomcat>/webapps/pinsafe/WEB-INF/logs

34 Prerequisites

The error has been seen on the following systems:

Appliance build 2.0.10, to 2.0.14

34.1 Error Messages

ERROR - Saving the XML config file "/usr/local/tomcat/webapps/pinsafe/WEB-INF/conf/config.xml" failed, error: java.io.IOException: No space left on device.

java.io.IOException: No space left on device at java.io.FileOutputStream.writeBytes(Native Method)

The above message can be seen when there are Tomcat errors related to no disk space.

cp: cannot create regular file ?/backups/.default/tomcat/logs???. No space left on device

The above error message can be seen when performing a backup.

35 Solutions

35.1 Purge script fix

Edit the following script /etc/cron.daily/PINsafe_backup_purge.sh

There are two lines in that script that should read

```
p_arch=`grep "archives" /etc/pinsafe.conf|cut -d\= -f2`
p_logs=`grep "logs" /etc/pinsafe.conf|cut -d\= -f2`
```

35.2 Logrotate

In the file /etc/logrotate.d/tomcat add notifempty as below

```
/var/log/tomcat/*.log {
       daily
       missingok
       copytruncate
       rotate 30
       missingok
       compress
}
```

To

```
/var/log/tomcat/*.log {
       daily
       missingok
       copytruncate
       rotate 30
       missingok
       compress
       notifempty
}
```

35.3 Reducing the MySQL transaction logs

35.3.1 Removing Transaction logs Using MySQL Commands

From the MySQL command line run

STOP SLAVE;

RESET SLAVE;

RESET MASTER;

35.3.2 Setting Transaction Log Size

When the appliance is back in synchronisatuon, then the transaction logs should sync, by default these are stored for 7 days. It is possible to change these in /etc/my.cnf, look fior the following line:

1. Delete BIN LOG Files After 7 Days.

expire_logs_days=7 max_binlog_size=256000000

Change expire_logs_days=7 to the required value

35.4 Manually deleting files

Note: Take care when using the rm command so that only the correct files are deleted. Deleted files can only be recovered from valid backups.

The following commands are run from the command line, see Command Line Access How to guide

- Ensure that you are in the correct directory
- Using ./filename or ./folder ensures that only the file or folder with the directory is removed.

If there are too many files to list then the following command can be used to remove the files. This example is for files within the Tomcat logs folder which will delete all instances of localhost.

find . -iname 'localhost.*' | xargs rm

35.4.1 Deleting log files

To delete log files older than 5 days the following commands can be used.

cd /var/log/tomcat

```
find /var/log/tomcat/ -iname 'localhost.*' -mtime +5 | xargs rm
```

```
find /var/log/tomcat/ -iname 'manager.*' -mtime +5 | xargs rm
```

```
find /var/log/tomcat/ -iname 'catalina.*' -mtime +5 | xargs rm
```

```
find /var/log/tomcat/ -iname 'admin.*' -mtime +5 | xargs rm
```

```
find /var/log/tomcat/ -iname 'host-manager.*' -mtime +5 | xargs rm
```

If the following error message is shown, and providing the commands have been correctly typed, then there are no files older than 5 days.

```
"rm: too few arguments
Try `rm --help' for more information."
```

35.4.2 Deleting Mail queue files

The following command will remove all files in the clientmqueue folder

```
ls /var/spool/clientmqueue/ xargs rm
```

and mail for the root user can be removed with the following command

```
echo > /var/spool/mail/root
```

35.5 Known Issues

Please be aware: As a side effect of a Full Disk, is that the config.xml file can become corrupt. After the disk space has been freed, please ensure that the config.xml is not showing as 0 bytes. This is located under:

v3.9.1 or newer - /home/swivel/.swivel/conf

v3.9 or older - /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf

You must restore a config.xml from a valid and most recent backup.

35.6 Troubleshooting

/bin/rm: Argument list too long

This can occur where there are too many files to delete using the rm command. Either specify a specific file e.g. catalina.* or use the commands given above.

36 Appliance Hardware

37 Swivel Appliance Hardware

This document covers aspects of the Swivel Appliance Hardware.

For installation see Hardware Appliance Installation and the Getting Started Hardware Appliance

For the Hardware Specification see Hardware Appliance Specification

For general questions see the Appliance General FAQ

For Hardware Troubleshooting see Appliance Hardware Troubleshooting

38 Appliance support logs

39 Overview

When reporting an error on either an appliance or with Swivel it is advisable to generate a support file. The support file contains versioning information and log files.

The instructions contained in this document have been tested on a **V2.x appliance**: (Appliance General FAQ)

Check also: (Troubleshooting Files FAQ)

If you find that they are not applicable to your appliance, please contact Swivel Secure support (support@swivelsecure.com) for assistance.

It is assumed that the appliance is already configured, and has a valid IP address on your network.

39.1 Sending Support file by email

1. Login to the appliance CMI using the console or an SSH client (Using SSH and SFTP)
2. Select "Advanced Options" from the Main Menu.
3. Select "Admin menu" from the Advanced Menu.
4. Select "Diagnostics" from the Admin Menu.
5. Select "Support logs and information".
6. Enter an email address. the email will be sent from the appliance, so using an internal server is recommended to avoid email relay issues.
7. Enter an IP address or DNS name for an SMTP server. Note that the hostname or IP address needs to be specifically entered and just pressing return will not enter any listed SMTP server.

39.2 Sending Support file manually using external method

1. Follow all of the previous steps, using a non-existent SMTP server.
2. Use SFTP to connect to the appliance (Using SSH and SFTP)
3. Navigate to the "/backups/upload" directory.
4. Download the "support_info.tar.gz" file.
5. Manually email the support file.

39.3 Troubleshooting

Check that the IP address is the correct IP for the appliance.

Ensure the appliance can connect to a mail server using port 25.

Unless an SMTP server is configured to allow un-authenticated relaying, which they never are, the SMTP server must be on the same network as the PINsafe appliance.

Type in the SMTP server address explicitly, do nt just press enter.

If any error messages are reported after the rpm command please contact Swivel Secure support (support@swivelsecure.com) for assistance.

The Diagnostics uses its own Mail server and not Sendmail, so the logs will not appear in /var/log/maillog.

39.4 Sample Support logs

```
Support Information

Gathering support files, and creating a zip archive.

1. Send zip archive to local mail server
2. Create zip archive in /backups/upload and collect with SFTP
0. Diagnostics

Select: 1

Please enter an email address to send the support archive to.

Email: support@swivelsecure.com
```

```
Support Information

Gathering support files, and creating a zip archive.

1. Send zip archive to local mail server
2. Create zip archive in /backups/upload and collect with SFTP
0. Diagnostics

Select: 1

Please enter an email address to send the support archive to.

Email: support@swivelsecure.com
SMTP server (smtptest.swivelsecure.com): smtptest.swivelsecure.com
```

```
Support Information
```

```
Gathering support files, and creating a zip archive.

1. Send zip archive to local mail server
2. Create zip archive in /backups/upload and collect with SFTP
0. Diagnostics

Select: 1

Please enter an email address to send the support archive to.

Email: support@swivelsecure.com
SMTP server (smtptest.swivelsecure.com): smtptest.swivelsecure.com

The support log file may be download using SFTP from /backups/upload

Press Return to Continue
```

40 Appliance Synchronisation

41 Overview

Appliance synchronisation allows certain elements to be synchronised across appliances or another Swivel instance that is using a shared database. This method of sharing session information supersedes Single Channel Session Cache and Session Sharing and it is recommended to disable these if they have been enabled. By default session sharing and Appliance Synchronisation are not enabled.

Sessions that can be synchronised across appliances include:

- Single Channel Sessions (TURing, Pinpad)
- SMS by On Demand Authentication authentication
- Mobile Provision Codes

42 Prerequisites

Swivel 3.9.5 or later

Swivel Appliance 2.0.14 or later

Shared database between Swivel instances.

Where the older session sharing is used it is recommended to disable it before enabling the Appliance Synchronisation.

43 Appliance Synchronisation

From the Swivel Administration console select **Appliance Synchronisation**. Options available are:

Partner Appliance IP: The IP address or hostname of the partner appliance.

Context: The name of the Swivel installation, usually pinsafe.

Port: The port used for communication between appliances, usually 8080.

Ignore SSL Cert Errors: Options Yes/No. Ignore invalid certificates such as self-signed or expired.

Connection Timeout (ms): Default 3000. How long the server attempts to connect to the partner before stopping.

Use SSL: Options Yes/No. Select this if SSL is used on the appliances for the selected ports.

Shared Secret: Shared secret, also required on the other partner. For versions 3.9.6 and 3.9.7 the only shared secret that can be used is *secret*

Synchronise Sessions: Options: Yes/No. When enabled this will synchronise sessions between Swivel appliances. Sessions are used for Single Channel authentication images such as TURing and SMS on demand.

44 Testing

Enable the Appliance synchronisation. A single channel image generated for an admin user on one appliance should allow a login on the partner appliance (must allow a admin console login).

For each session sharing the follwing log message will be generated:

```
SESSION_UPDATE, <SyncResponse><Session><Data Username="admin"/></Session></SyncResponse>
```

45 Known Issues

45.1 Session sharing and Appliance Synchronisation

Disable Session Sharing where Appliance Synchronisation is used, as this may cause incompatibilities.

45.2 SSL vulnerability updates stop Appliance Synchronisation working

The following error may be displayed

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

This can be resolved by editing the file /usr/local/tomcat/conf/server.xml and changing both instances of 'sslProtocols=' or 'sslProtocol=' to be 'sslEnabledProtocols=', i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

45.3 3.9.6 and 3.9.7 appliance session sync issue

Swivel versions 3.9.6 and 3.9.7 contain a bug that allows session sharing to a second Swivel instance but breaks it when a session is started on that second instance, to resolve this download the Session Sync patch file and copy the contents to the following locations:

LocalSessionManager.class to: /usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/session

SyncXML.class to: /usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/sync

For a software only install substitute /usr/local/tomcat with the Tomcat install path

This issue is fixed in Swivel 3.10 Resolution, use shared secret of secret or to upgrade to 3.10

46 Troubleshooting

Check the Swivel log.

Check connectivity by a Telnet from each Swivel server to the other:

```
Telnet 192.168.1.100

Trying 192.168.1.100

connected to standby@swivel.local (192.168.1.100).

Escape character is '^]'.

Connection closed by foreign host.
```

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

1. This can be resolved by editing the file /usr/local/tomcat/conf/server.xml and changing both instances of 'sslProtocols=' or 'sslProtocol=' to be 'sslEnabledProtocols=', i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

2. The error is also seen on **Version 3 Appliances**, there you will need to enable TLSv1 either via the CMI menu (if available) or editing the server.xml from sslEnabledProtocols="TLSv1.1,TLSv1.2" To sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" for both connector ports and restart Tomcat.

Appliance Synchronisation unavailable

If the appliance synchronisation is not available in the Administration console, it may be due to Session Sharing. Disabling this will allow the appliance synchronisation to be selectable. Edit the /home/swivel/.swivel/conf/config.properies (path will be different for a non appliance) and change the following:

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.DistributedCacheSessionManager

to

SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.LocalSessionManager

Then restart Tomcat

SYNC_ERROR, 404: Not Found, Time out now 10

Synchronisation has failed between appliances. Check the IP/Hostname, port, context, network connectivity, SSL, SSL errors permitted, on each partner.

SYNC_ERROR_UNAUTHORIZED

The shared secrets do not match, re-enter them on both instances. for 3.9.6 and 3.9.7 the only available option for the shared secrets is *secret*

SYNC_ERROR Unknown Time out now 10

Swivel instance has failed to send the synchronisation data to the partner. Check all settings and network connectivity on each partner. If the appliances have http/https enabled then the settings need to be used for no SSL or SSL respectively.

SYNC_ERROR, java.net.UnknownHostException: standby-swivel-local-pinsafe, Time out now 30

The hostname is not known to the Swivel instance, check the hostname and DNS servers are correct, or try with the IP address.

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target, Time out now 20

Certificate error in communication, used a valid certificate or use option to **Ignore SSL Cert Errors:**

SYNC_ERROR, Unexpected end of file from server, Time out now 60

Check to see if SSL or non SSL communications are used. On the Admin Console, navigate to Appliance > Appliance Synchronisation and check the setting Use SSL.

SYNC_ERROR, java.net.SocketTimeoutException: Read timed out, Time out now 20

Check Network connectivity between the Swivel instances.

47 Audit scripts

48 Overview

The audit scripts can be run on Swivel appliances and allow information to be emailed to one or more addresses.

The same scripts can be installed on a Windows Swivel installation.

49 Prerequisites

AuditScripts.zip

Swivel Appliances: If you use localhost on an appliance, Sendmail must be configured and running

50 Audit Script Swivel Appliance Installation

The Audit scripts can be run on Swivel Hardware and Virtual Appliances. Installing the scripts requires the use of a SFTP program such as WinSCP and may require Command Line access through the CMI, as well as access to the Swivel Administration Console.

50.1 Configuring the Swivel Appliance for Agent XML Authentication

To allow communication from the Audit scripts to the Swivel core, configure an agent on the Swivel Administration console, see Agents How to Guide . If running 3.9 or later, you must indicate that the agent can acts as a repository

50.2 Download the Audit Script

Download AuditScripts.zip then Copy zip file to /usr/local/bin

Unzip files so that

/usr/local/bin/com/swiveltechnologies/pinsafe/client/admin

contains

AdminAPI.class, BaseAdminXmlRequest.class, UserAudit.properties etc etc

permissions need to be -rwxr-x--x

50.3 Configure the Audit Script for Swivel Appliances

Edit UserAudit.properties (/usr/local/bin/com/swiveltechnologies/pinsafe/client/admin/UserAudit.properties)

customer=customerName The name of the end-customer

swivelurl=http://localhost:8181/pinsafe The url of the Swivel server, default will work for appliance install

swivelsecret = secret Shared secret, needs to match that as set on the Swivel Server for the local agent

mailhost = localhost Host that will forward the email

mailfrom = admin@localhost The sender email address

mailto = billing@swivelsecure.com To where the email will be sent, mulitple addresses separated by a semi-colon

mailsubject= Customer User Count The subject of the email

billday = 25 The day of the month that the report will be sent out. It will only email reports out on this date. If the date is not current then no email will be sent.

50.4 Running the Audit Script on Swivel Appliances

To run the script within the /usr/local/bin/ folder type:

```
./audit.sh
```

The script interrogates the Swivel Server and appends to a csv file the result, in the folder /usr/local/bin with the date and number of users in the database.

The filename is in the format /usr/local/bin/<customername><repositoryname><month>.<year>.csv

On the billing day of each month the script emails a summary of the results to the specified email address. No email is sent if it is not a billing day.

You can specify a specific reposistory for the report, so it only counts users in that repository eg:

```
./audit.sh XML
```

For testing you can set the billing date to today's date

```
./audit.sh XML
```

If you want the count to include all users, use ALL as the repository name

```
./audit.sh ALL
```

50.5 Configure the Audit script to run automatically on Swivel Appliances

Edit the audit.sh file itself to select the repository you want the script to run against:

java -cp mail.jar:. com.swiveltechnologies.pinsafe.client.admin.UserAudit $1 $2

Replace $1 and $2 with the repository name(s).

E.g. java -cp mail.jar:. com.swiveltechnologies.pinsafe.client.admin.UserAudit localxml

Note - If the repository name is two words (or more) then you must put the repository name in speechmarks. I.e "local xml".

Once the script works you can copy to /etc/cron.daily and the script should run everyday.

You can edit the audit scipt to change what users are counted. eg

```
java -cp mail.jar:. com.swiveltechnologies.pinsafe.client.admin.UserAudit rep1
```

java -cp mail.jar:. com.swiveltechnologies.pinsafe.client.admin.UserAudit rep2

would create two separate reports to be generated and sent.

If you need to install the script elsewhere, you need to edit the AUDIT_HOME variable in the script.

51 Audit Script Windows Installation

Unlike Swivel Appliances, Swivel Windows installations are not standardised.

The general principles of how to deploy and use the scripts is described here.

1) Download File:AuditScripts.zip then Copy zip file to a suitable location eg c:\Users\user

2) unzip files so that

c:\Users\user\AuditScripts\com\swiveltechnologies\pinsafe\client\admin contains

AdminAPI.class, BaseAdminXmlRequest.class, UserAudit.properties etc etc

3) Edit UserAudit.properties

customer=customerName *The name of the end-customer*

swivelurl=http://localhost:8080/pinsafe *The url of the Swivel server*

swivelsecret = secret *Shared secret, needs to match that as set on the Swivel Server for the local agent*

mailhost = localhost *Host that will forward the email*

mailfrom = admin@localhost *The sender email address*

mailto = billing@swivelsecure.com *To where the email will be sent, mulitple addresses separated by a semi-colon*

mailsubject= Customer User Count *The subject of the email*

billday = 25 *The day of the month that the report will be sent out*

You need to configure local as an agent on the server/appliance.

If running 3.9 or later, you must indicate that the agent can acts as a repository

4) To run the script type you need to create a batch file, audit.bat

```
cd c:\Users\crussell\AuditScripts
```

set CLASSPATH=.;.\mail.jar

java com.swiveltechnologies.pinsafe.client.admin.UserAudit %1 %2

The filename is in the format <customername><repositoryname><month>.<year>.csv

On the billing day of each month the script emails a summary of the results to the specified email address.

You can specify a specific repository for the report, so it only counts users in that repository eg: `audit.bat XML`

For testing you can set the billing date to today's date

If you want the count to include all users, use ALL as the repository name

```
audit.bat ALL
```

5) Once the batch file is working it can be run automatically by creating a scheduled task to call the batch file

Refer to http://www.hosting.com/support/windows-server-2008/create-a-scheduled-task-in-windows-server-2008

52 Testing

Once you are happy with changes you have made within UserAudit.properties, you can send a test e-mail to the e-mail address configured in this file. In order to do this, you must change the 'billingday' to the day you are testing on. For example, if you are testing on the 12th May, then billingday = 12.

53 Troubleshooting

On Swivel hardware and Virtual appliances the emails are logged under /var/log/maillog, to view the logs use;

```
tail /var/log/maillog
```

No email is sent if it is not a billing day.

If mails are not being sent check the 'mailhost' in UserAudit.properties

try to telnet to it on port 25

Example: your mailhost is 'mail.yourcompany.net' then try:

```
telnet mail.yourcompany.net 25
```

Wait a few moments, do you get a connection or any feedback from the server e.g.

```
[admin@primary bin]# telnet mail.yourcompany.net 25 Trying 1.2.3.4...

Connected to mail.yourcompany.net (1.2.3.4).

Escape character is '^]'.

220 mail.yourcompany.net Microsoft ESMTP MAIL Service ready at Thu, 27 Nov 2014 11:38:32 +0000
```

53.1 Error Messages

Error Occurred - Check PINsafe logs: This error may arise for a number of reasons but make sure that UserAudit.properties contains the correct information. Also, if you are running the command ./audit.sh ALL, this may throw up the error so try running ./audit.sh.

./audit.sh: Permission denied Check the file permissions on the audit.sh and other files.

54 Authentication Methods

55 Overview

Swivel provides a variety of Authentication methods and Authentication Protocols to verify a users identity.

56 One Time Code passwords and Passcodes

Swivel can provide a One time Code for user authentication in the following ways;

56.1 Two Factor Authentication One Time Code Solutions

SMS

Mobile Phone Client

hardware Token

56.2 Single Factor One Time Code solutions

Stronger than a username and password, sometimes termed 1.5 factor, this ads a One Time Code to the authentication.

TURing

Pinpad

57 PIN protection

As well as One Time Codes, Swivel can protect the delivery of a One Time Code using PIN protection, see PINsafe User Guide.

58 Authentication Protocols

Swivel supports the following Authentication protocols

RADIUS

SAML

Agent-XML an API for authentication

59 Azure AD as a Data Source

60 Overview

This document describes how to use Azure AD as a Data Source.

61 Prerequisites

- Enable Azure AD Domain Services.
- Enable Secure LDAP.
- It is also necessary a connection between Swivel and Azure AD SLDAP

61.1 Implementation

You can follow the instructions on this article here.

Please have a read in this instructions on this article [1] and also [2]

62 Backup PINsafe How to Guide

62.1 Overview

PINsafe should be regularly backed up to ensure that configuration information and user data are secure, the following areas of information need to be backed up:

- User Data
- PINsafe Configuration
- Custom modifications including, transports, IP filters, Single Channel Images

Additionally Swivel virtual or hardware appliances include OS information.

Also see the Appliance Backup FAQ.

62.2 Prerequisites

PINsafe 3.x

62.3 Backup Guides

The following guides are available for backing up PINsafe

Backup Appliance using CMI

Backup PINsafe on a Active/Active appliance using CMI

Backup PINsafe on a Software Only Install

Backup PINsafe on a Active/Passive appliance using command line

62.4 Testing

62.5 Known Issues

62.6 Troubleshooting

63 Change Configuration Location

64 Overview

This document describes how to change the location of Swivel configuration files.

65 Prerequisites

- Software-only installation - it is not recommended that you change the location of the configuration files on an appliance.
- Swivel software version 3.9.1 or later

66 How to Guide

66.1 Check the Current Location

Before you start moving the configuration, you need to check where Swivel has deployed the configuration initially. We are assuming here that Swivel has been initially deployed using default settings.

Log into the Administration console and go to the status page (you will probably be shown this initially anyway).

Look for the entry "Data Storage Root" and make a note of the location shown.

66.2 Move the Current Configuration

Stop Tomcat.

Go to the Data Storage Root location you noted earlier. Copy all folders and files from this location to the desired location.

66.3 Change the Setting for Swivel Home

Go to the Tomcat home folder, then into webapps\pinsafe\WEB-INF

Edit the file web.xml that you should find there.

Search for "env-entry". You should find the following:

```
        <env-entry>
                <description>If non empty value, will be the root for all the data - takes precedence over default and environment variable</
                <env-entry-name>swivelHome</env-entry-name>
                <env-entry-type>java.lang.String</env-entry-type>
                <env-entry-value></env-entry-value>
        </env-entry>
```

Insert the new folder containing the configuration files within <env-entry-value>, for example:

```
<env-entry-value>E:\Swivel</env-entry-value>
```

You can now restart Tomcat

67 Testing

To demonstrate that this works, simply log into the administration console and check that Data Storage Root is showing your new location.

68 Known Issues

We have occasionally seen Swivel fail to start, showing a stack trace which includes a reference to MissingResourceException for "config". This is due to a configuration file not having been copied over correctly - the exact cause for this is not known. However, there is a simple workaround:

Go to the Data Storage Root folder, and to the conf sub-folder within that. Look for a file called config.properties. It is likely that this file does not exist. In this case, simply create a new, empty text file called "config.properties", then restart Tomcat.

69 Troubleshooting

70 ChangePIN How to Guide

71 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.

72 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

73 Configure The PINsafe Server

Configure a PINsafe Agent (For standard XML Authentication)

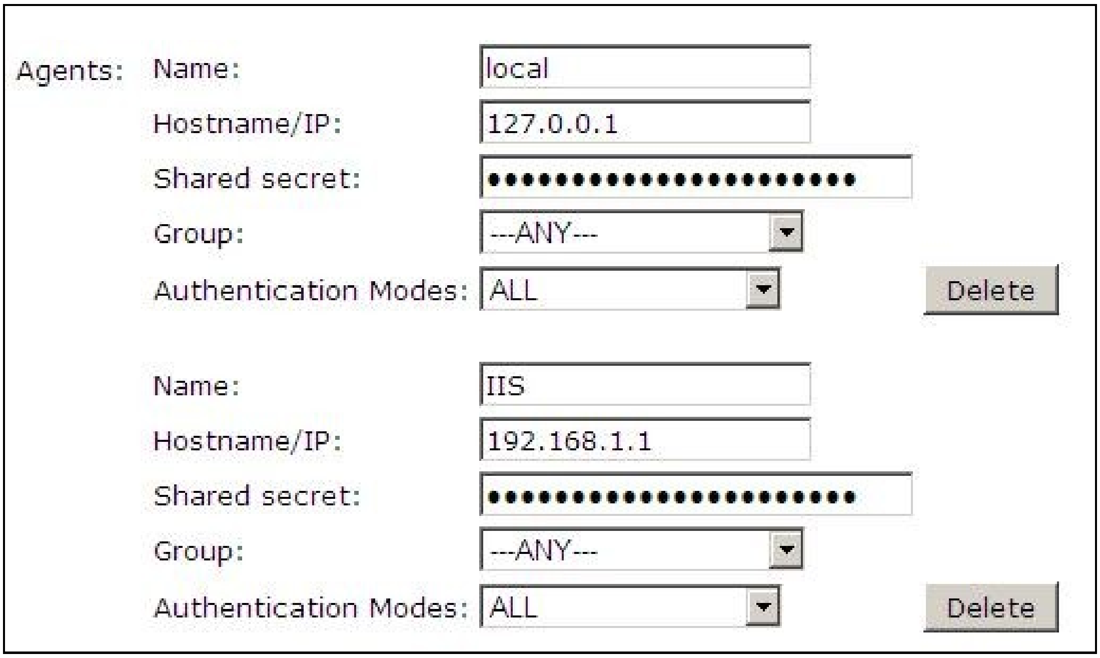
1. On the PINsafe Management Console select Server/Agent

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



Agents: Name: local
Hostname/IP: 127.0.0.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

Name: IIS
Hostname/IP: 192.168.1.1
Shared secret: ●●●●●●●●●●●●●●●●●●●●●●
Group: ---ANY---
Authentication Modes: ALL

74 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.

75 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

76 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)

76.1 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>
```

76.2 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>
```

77 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;

78 ChangePIN Custom Page Configuration

78.1 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>
```

78.2 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

78.2.1 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<br><font color=\"#FF0000\">new PIN</font> and the Security String shown below.";

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

78.2.2 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<br>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<br>your current PIN and the Security String shown below.";

final String NEW_OTC_PROMPT = "Step 3 : Enter the OTC using your<br>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 = "<br/>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<br /> Enter New Password:";

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

final String PIN_CHANGE_SUCCESSFUL = "PIN change successful.<br>";

final String REDIRECTING_PROMPT = "Please wait while you are redirected. If your<br>browser doesn't automatically redirect <br/>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<br />credentials. If the error persists<br /> contact your PINsafe Administrator.";

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

final String INVALID_PASSWORD_ERROR = "Your chosen Password was not valid.<br />Please try again with a different Password.<br />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";

78.2.3 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;
}

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

78.3 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

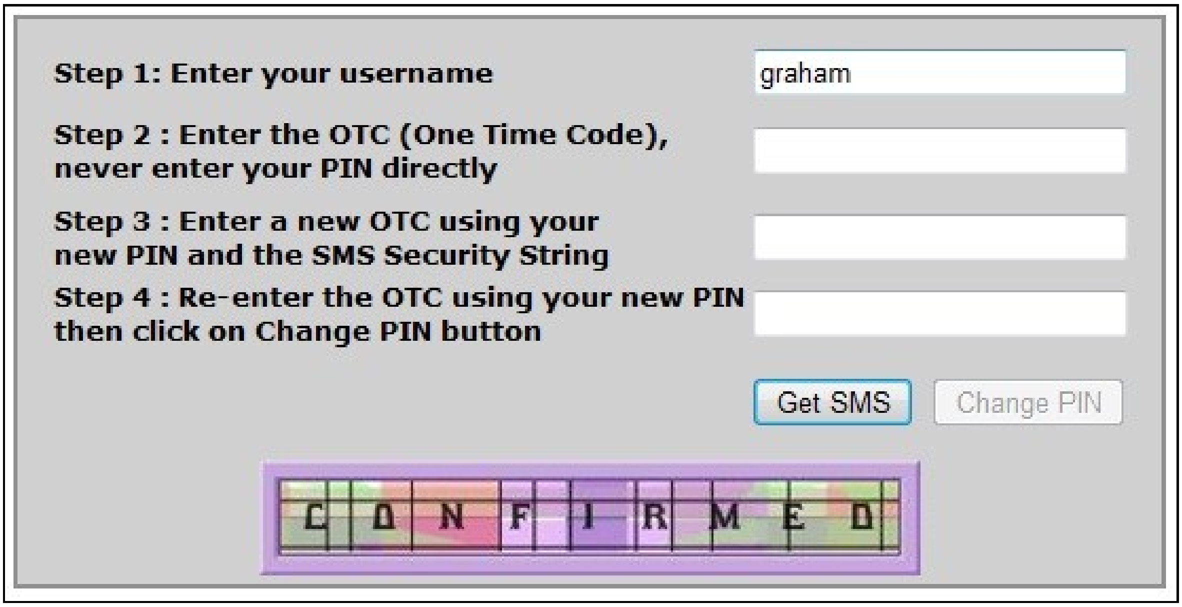
find the line containing *Get Image*

```
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.



Step 1: Enter your username graham

Step 2 : Enter the OTC (One Time Code), never enter your PIN directly

Step 3 : Enter a new OTC using your new PIN and the SMS Security String

Step 4 : Re-enter the OTC using your new PIN then click on Change PIN button

79 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:

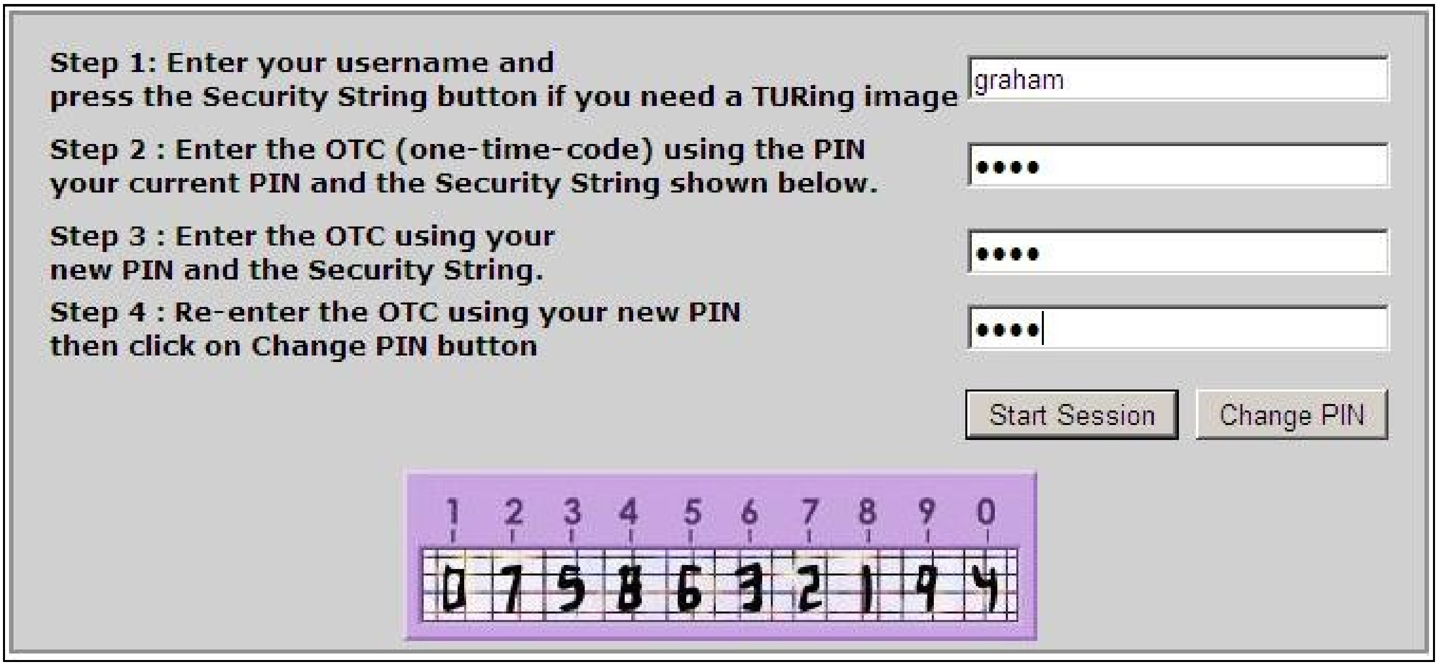
Virtual or hardware appliance: https://IP:8443/changepin2

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

80 ChangePIN Sample

See also ChangePIN Samples

Turing ChangePIN



Step 1: Enter your username and
press the Security String button if you need a TURing image

graham

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

••••

Step 3 : Enter the OTC using your
new PIN and the Security String.

••••

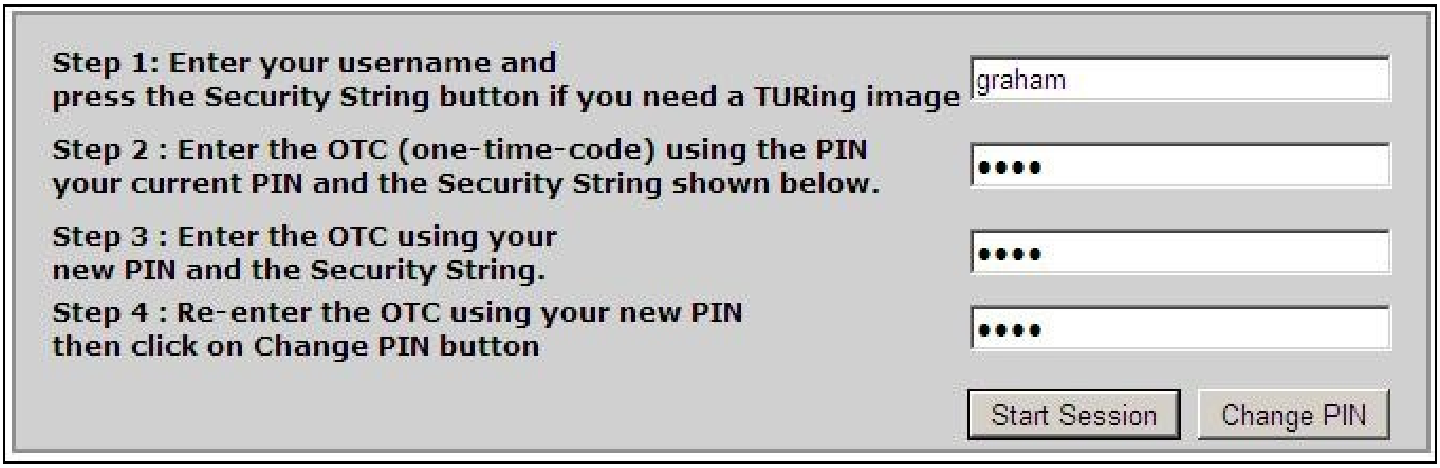
Step 4 : Re-enter the OTC using your new PIN
then click on Change PIN button

••••

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

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.



Step 1: Enter your username and
press the Security String button if you need a TURing image

graham

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

••••

Step 3 : Enter the OTC using your
new PIN and the Security String.

••••

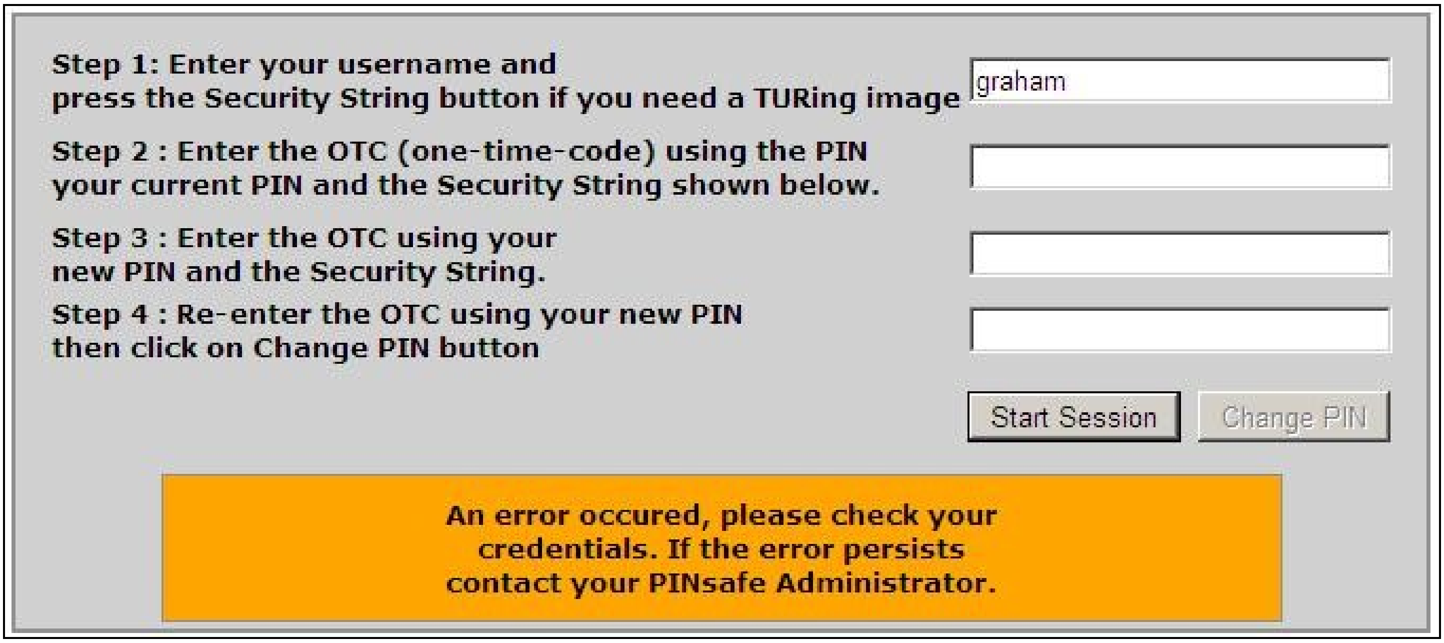
Step 4 : Re-enter the OTC using your new PIN
then click on Change PIN button

••••

81 Troubleshooting ChangePIN

If using IE 9 test with compatibility mode enabled.

81.1 Incorrect Credentials Used



Step 1: Enter your username and press the Security String button if you need a TURing image: graham

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

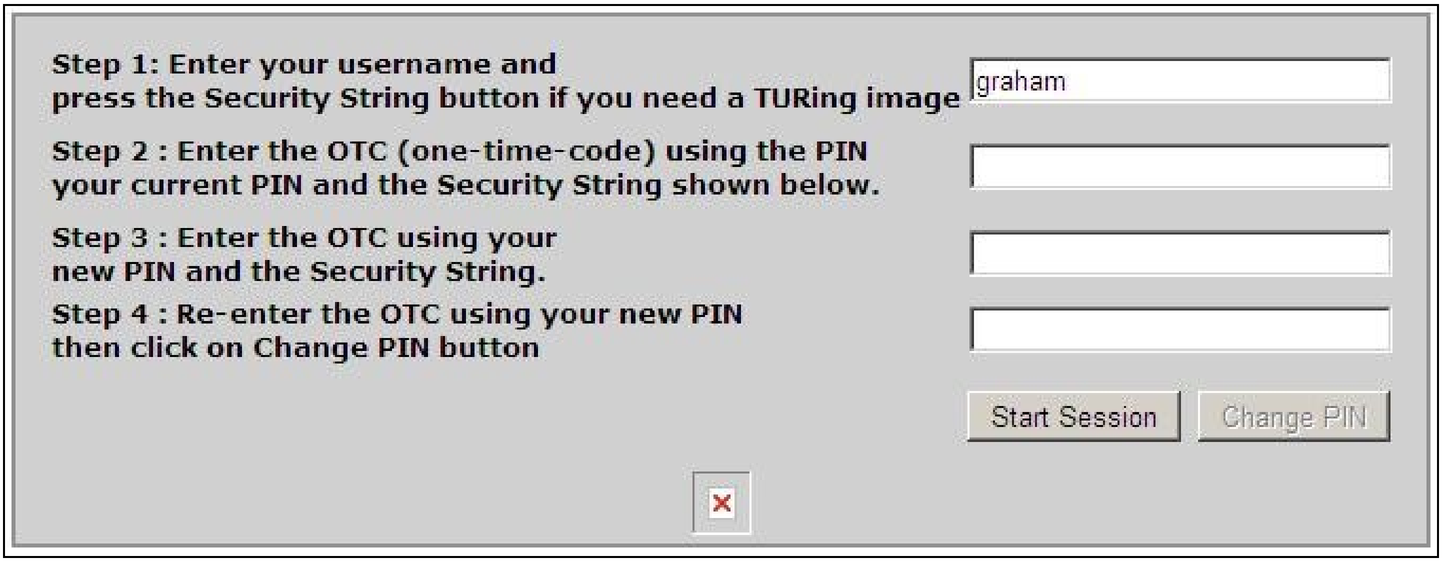
Step 3 : Enter the OTC using your new PIN and the Security String.

Step 4 : Re-enter the OTC using your new PIN then click on Change PIN button

An error occured, please check your credentials. If the error persists contact your PINsafe Administrator.

81.2 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.



Step 1: Enter your username and press the Security String button if you need a TURing image: graham

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

Step 3 : Enter the OTC using your new PIN and the Security String.

Step 4 : Re-enter the OTC using your new PIN then click on Change PIN button

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.

81.2.1 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.

81.3 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>
```

81.4 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.

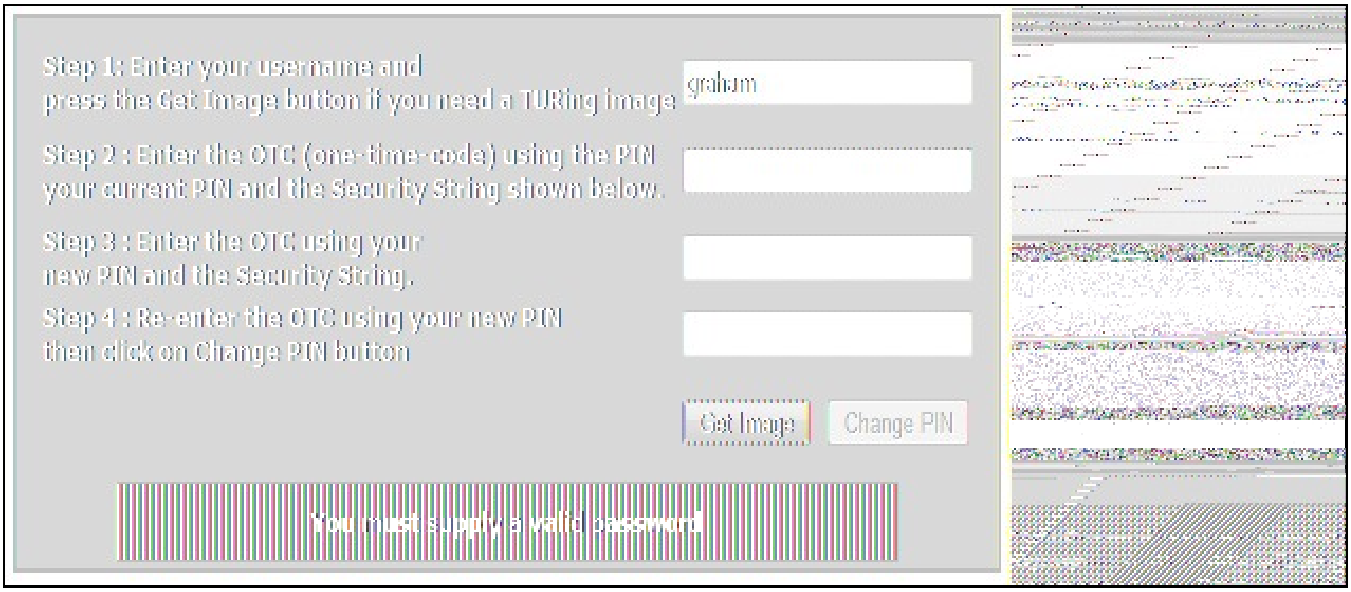
81.5 The user does not belong in the correct group

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'.

81.6 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.



Step 1: Enter your username and press the Get Image button if you need a TURing image: graham

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

Step 3 : Enter the OTC using your new PIN and the Security String.

Step 4 : Re-enter the OTC using your new PIN then click on Change PIN button

You must supply a valid password

81.7 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.

81.8 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**

81.9 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.

81.10 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.

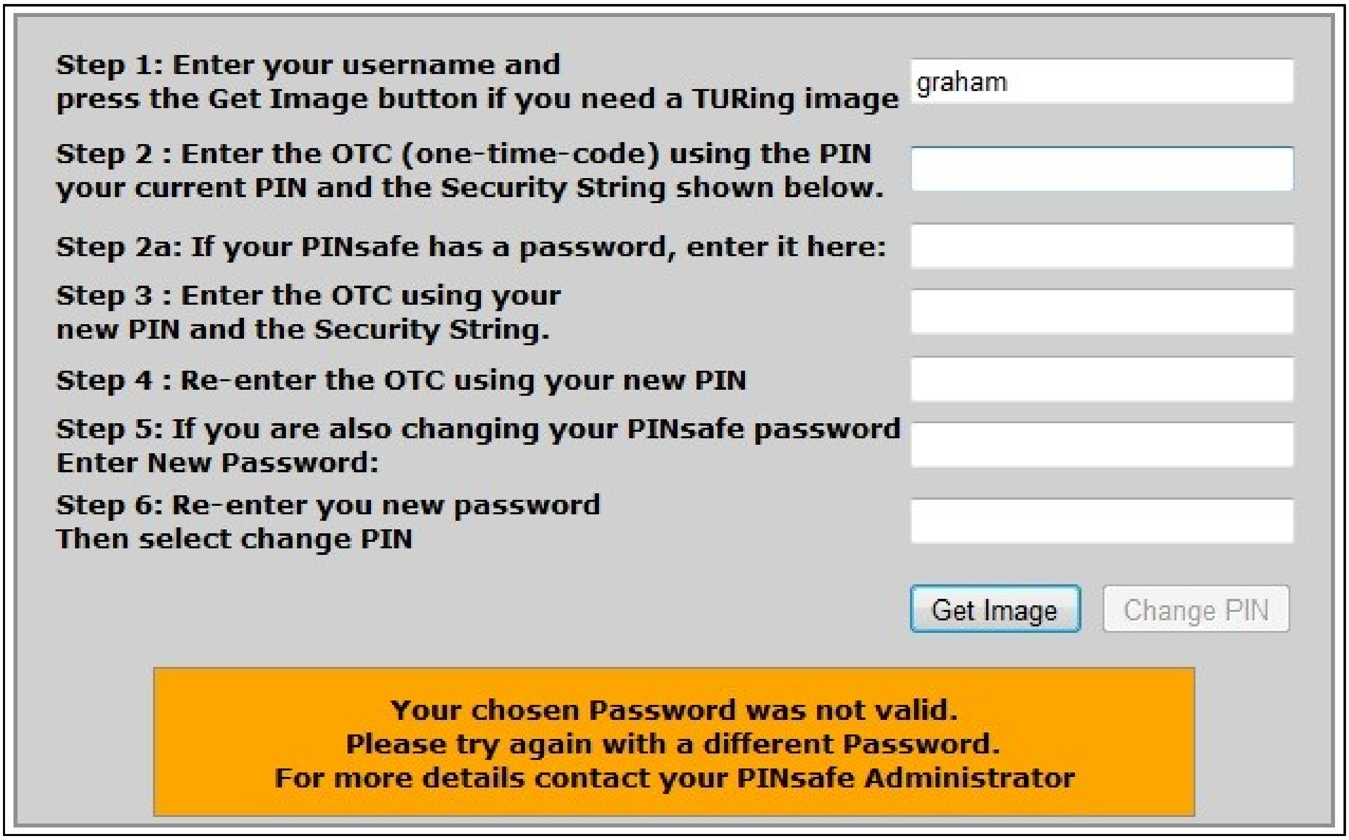
Change PIN failed for user: graham, error: The use of a static password is mandatory

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.



Step 1: Enter your username and press the Get Image button if you need a TURing image: graham

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

Step 2a: If your PINsafe has a password, enter it here:

Step 3 : Enter the OTC using your new PIN and the Security String.

Step 4 : Re-enter the OTC using your new PIN

Step 5: If you are also changing your PINsafe password Enter New Password:

Step 6: Re-enter you new password Then select change PIN

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

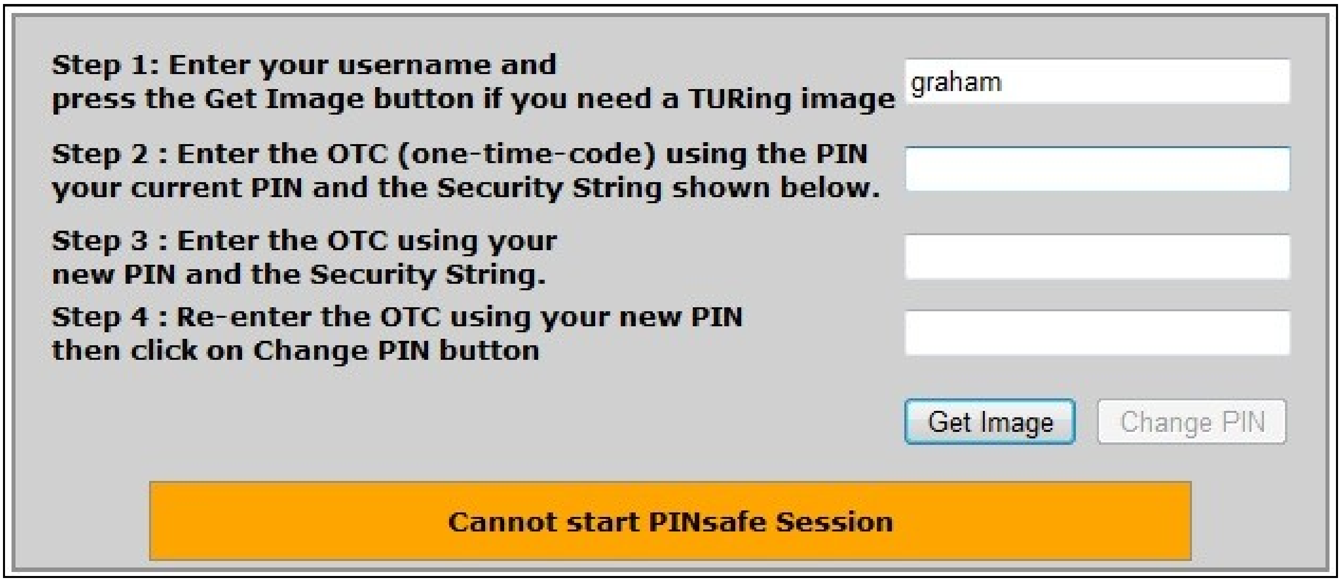
Cannot start PINsafe Session

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.



Step 1: Enter your username and press the Get Image button if you need a TURing image: graham

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

Step 3 : Enter the OTC using your new PIN and the Security String.

Step 4 : Re-enter the OTC using your new PIN then click on Change PIN button

Cannot start PINsafe Session

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.

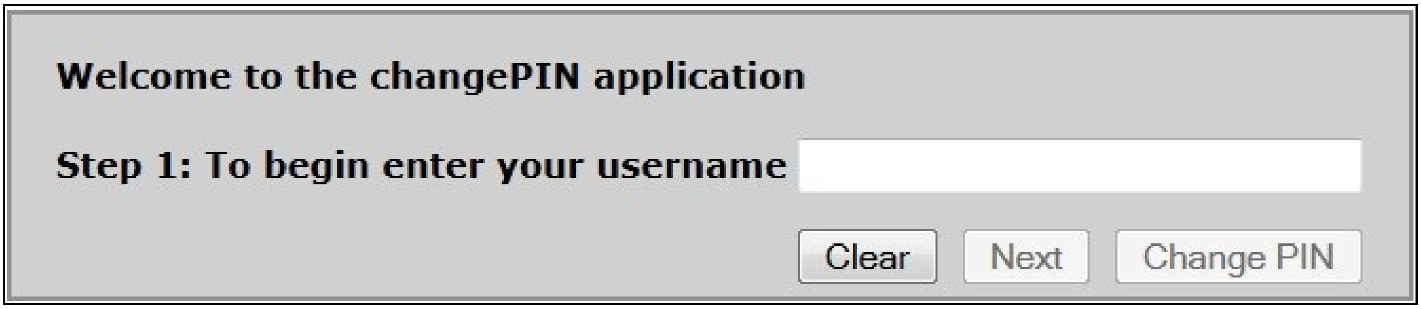
82 ChangePIN Samples

83 Overview

This page shows sample configurations for ChangePIN

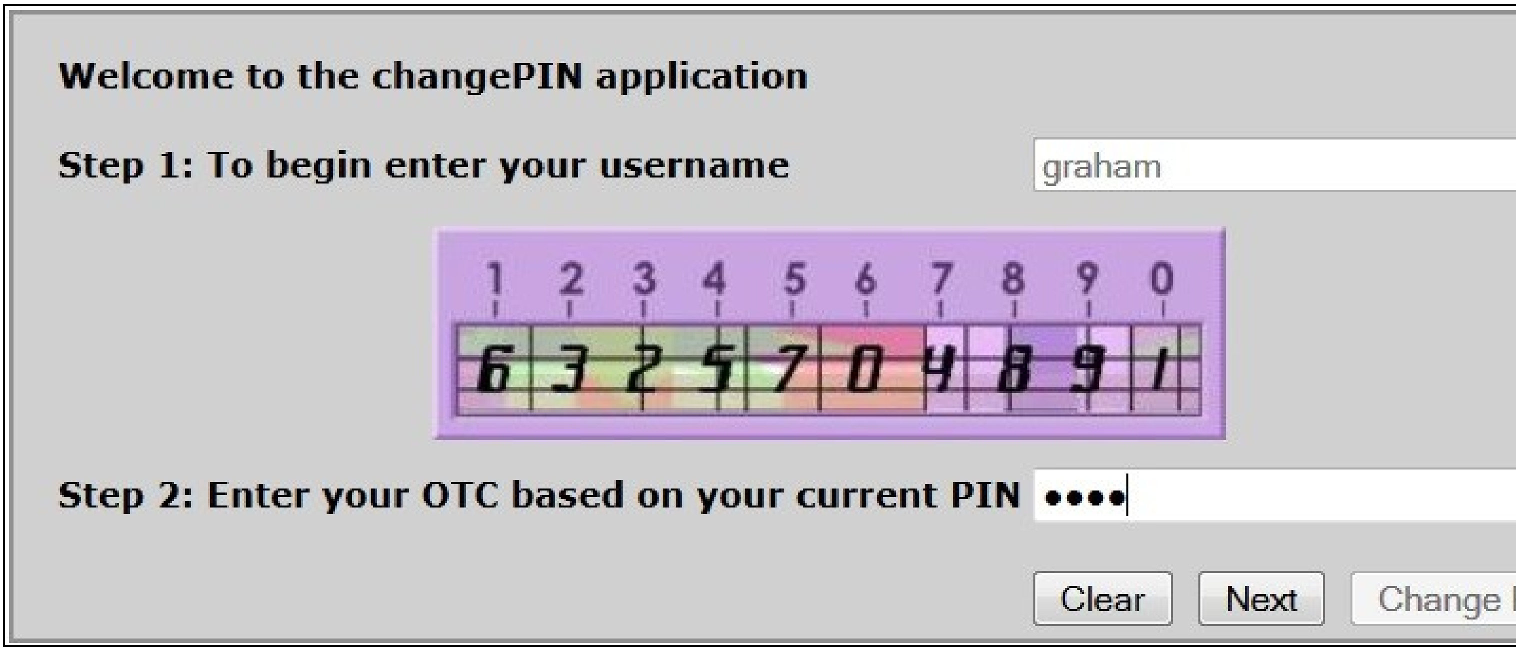
84 Version 3573

84.1 ChangePIN version 3573



Welcome to the changePIN application

Step 1: To begin enter your username

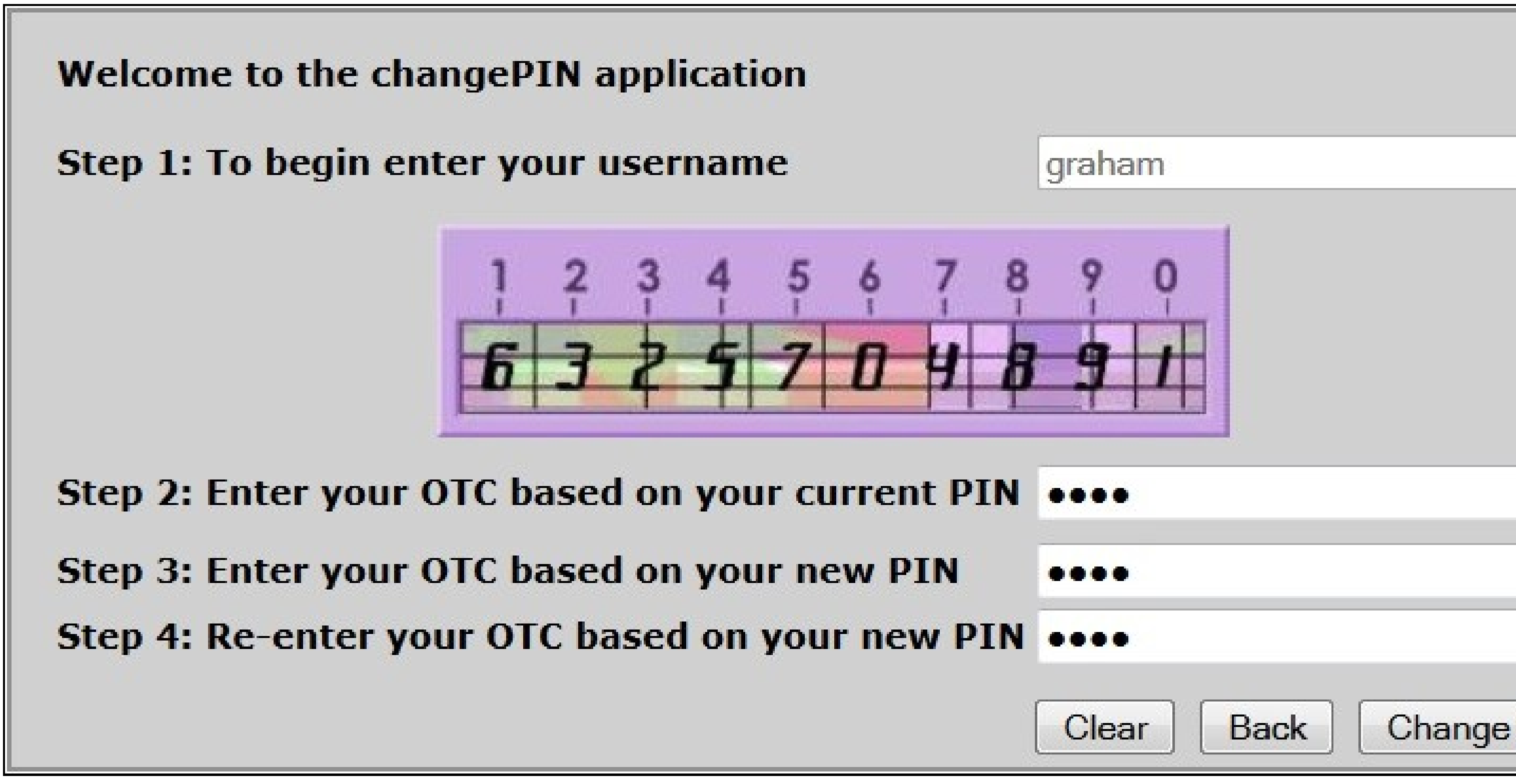


Welcome to the changePIN application

Step 1: To begin enter your username graham

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

Step 2: Enter your OTC based on your current PIN ••••



Welcome to the changePIN application

Step 1: To begin enter your username graham

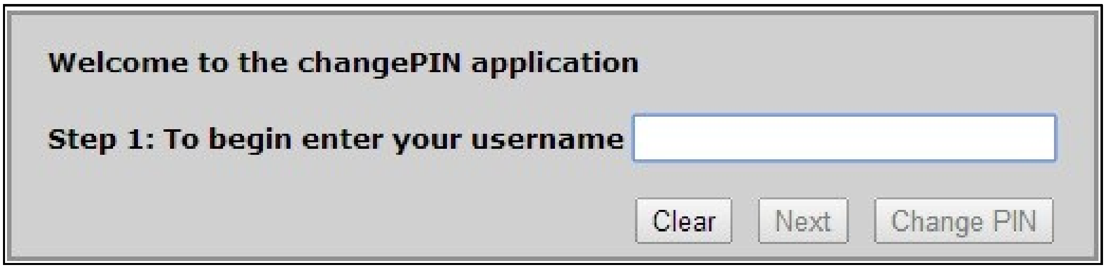
1	2	3	4	5	6	7	8	9	0
6	3	2	5	7	0	4	8	9	1

Step 2: Enter your OTC based on your current PIN ••••

Step 3: Enter your OTC based on your new PIN ••••

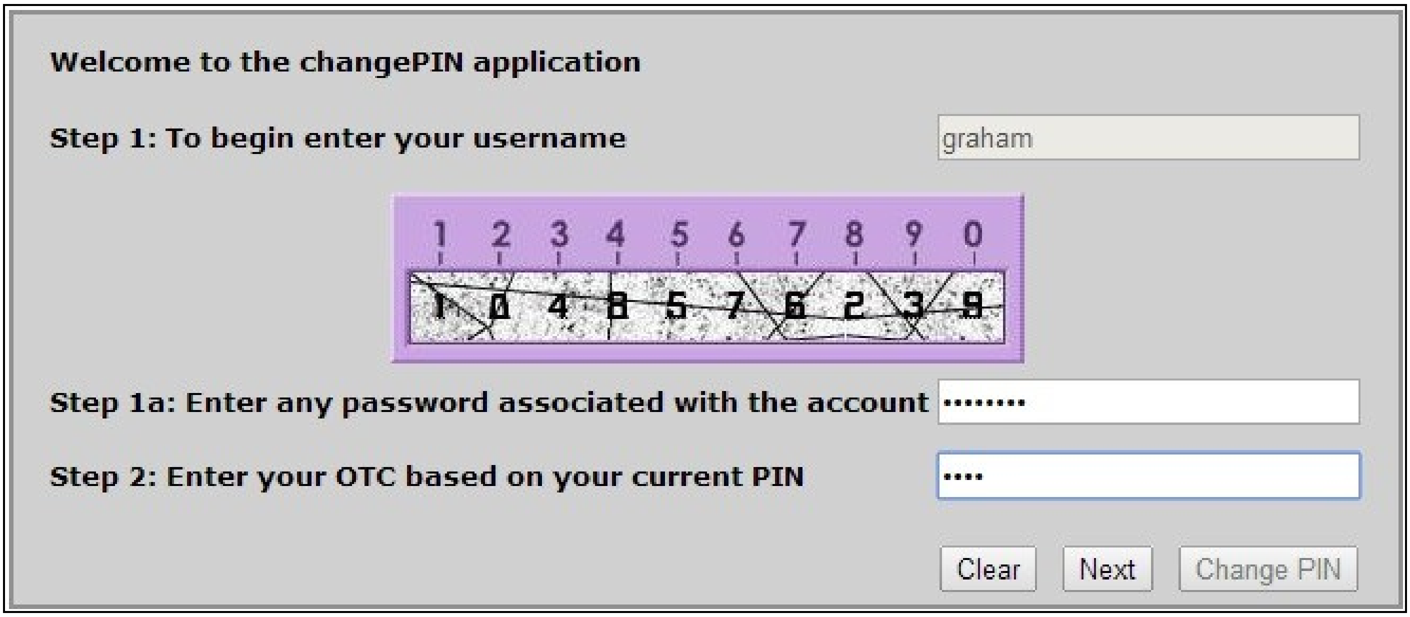
Step 4: Re-enter your OTC based on your new PIN ••••

84.2 ChangePIN with Password version 3572



Welcome to the changePIN application

Step 1: To begin enter your username

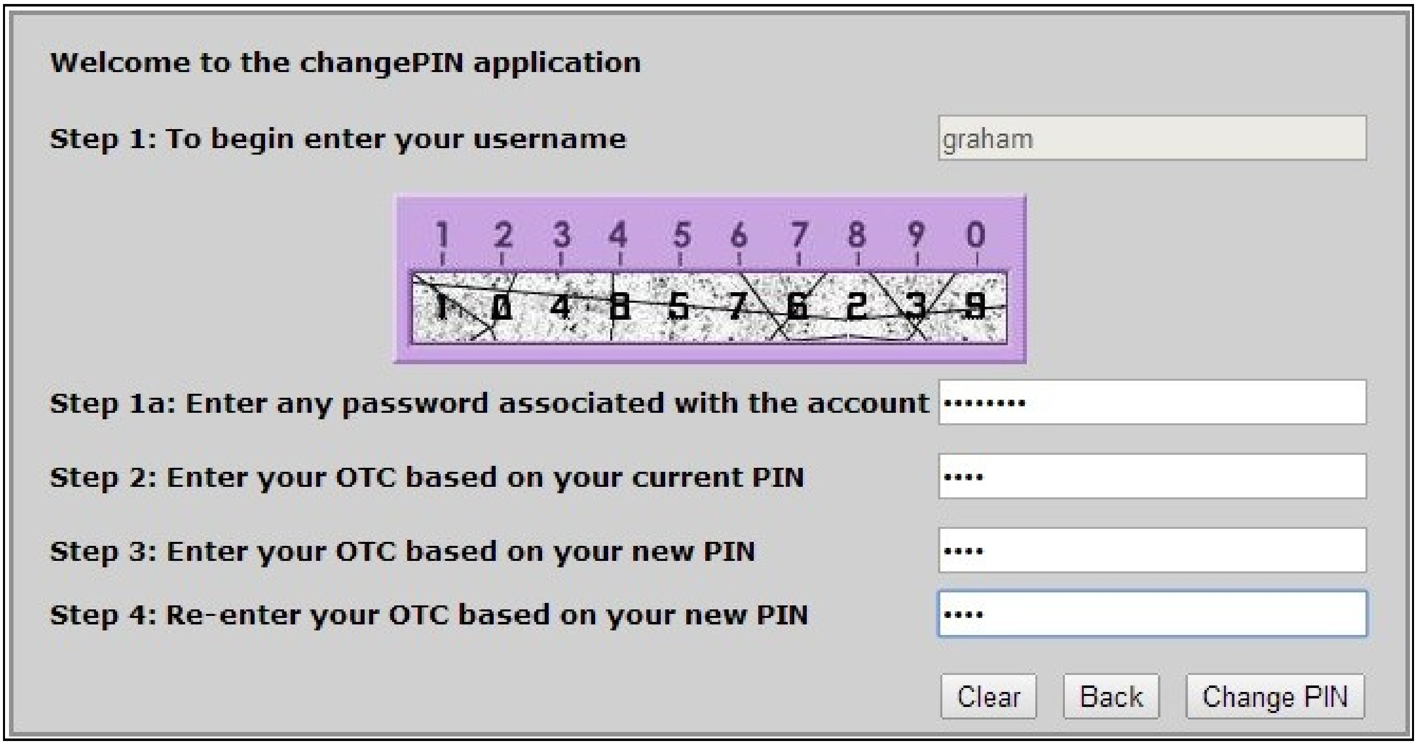


Welcome to the changePIN application

Step 1: To begin enter your username graham

Step 1a: Enter any password associated with the account ••••••••

Step 2: Enter your OTC based on your current PIN ••••



Welcome to the changePIN application

Step 1: To begin enter your username graham

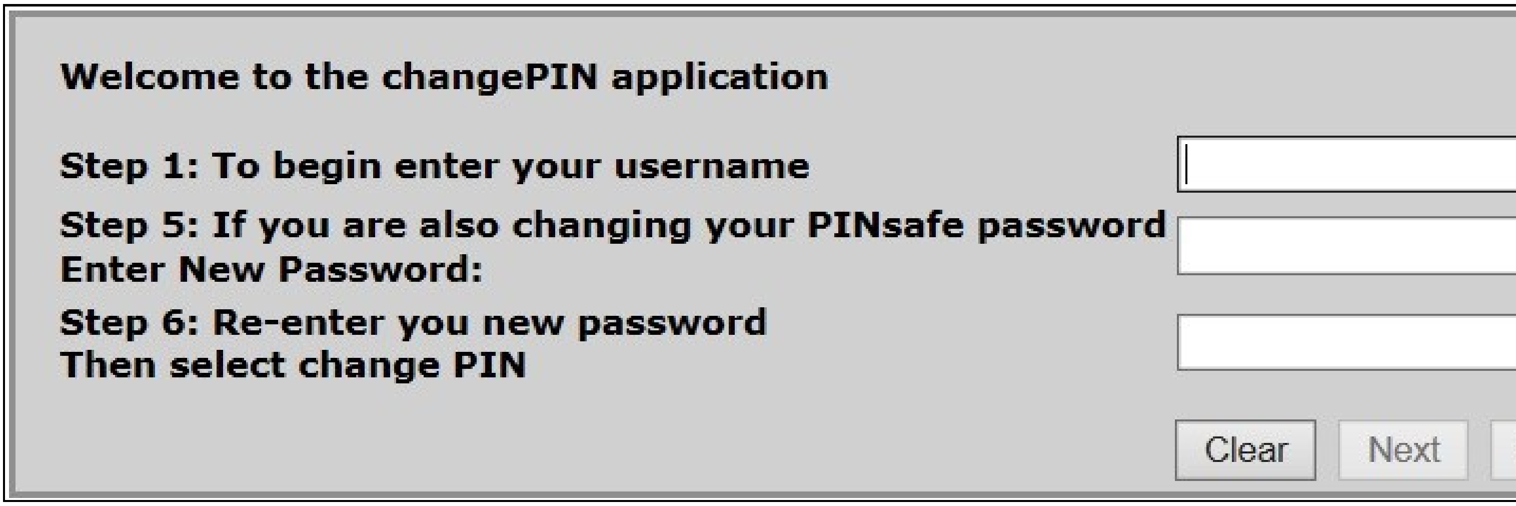
Step 1a: Enter any password associated with the account ••••••••

Step 2: Enter your OTC based on your current PIN ••••

Step 3: Enter your OTC based on your new PIN ••••

Step 4: Re-enter your OTC based on your new PIN ••••

84.3 ChangePIN with Password and Change Password version 3572

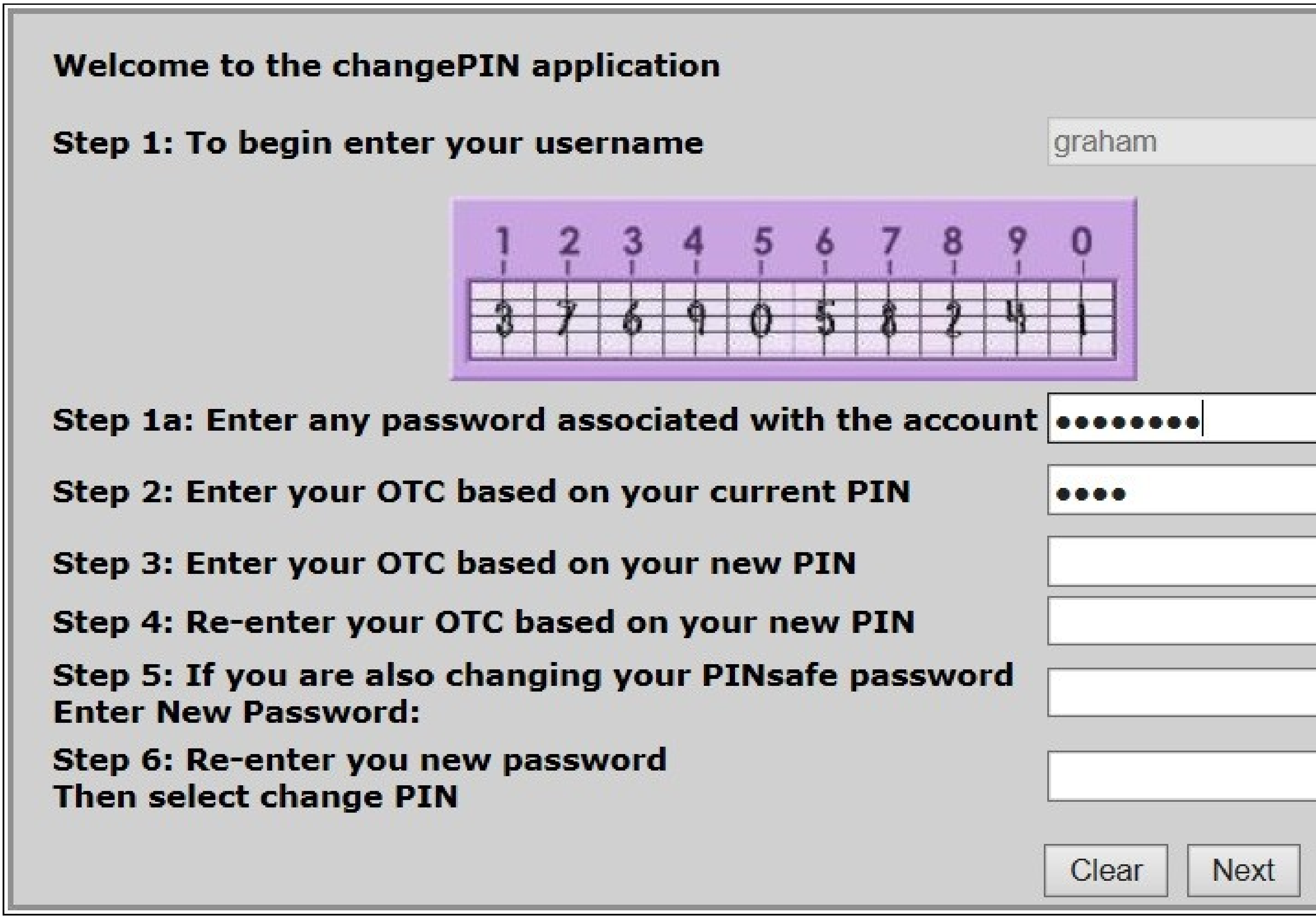


Welcome to the changePIN application

Step 1: To begin enter your username

Step 5: If you are also changing your PINsafe password
Enter New Password:

Step 6: Re-enter you new password
Then select change PIN



Welcome to the changePIN application

Step 1: To begin enter your username graham

Step 1a: Enter any password associated with the account ●●●●●●●●●

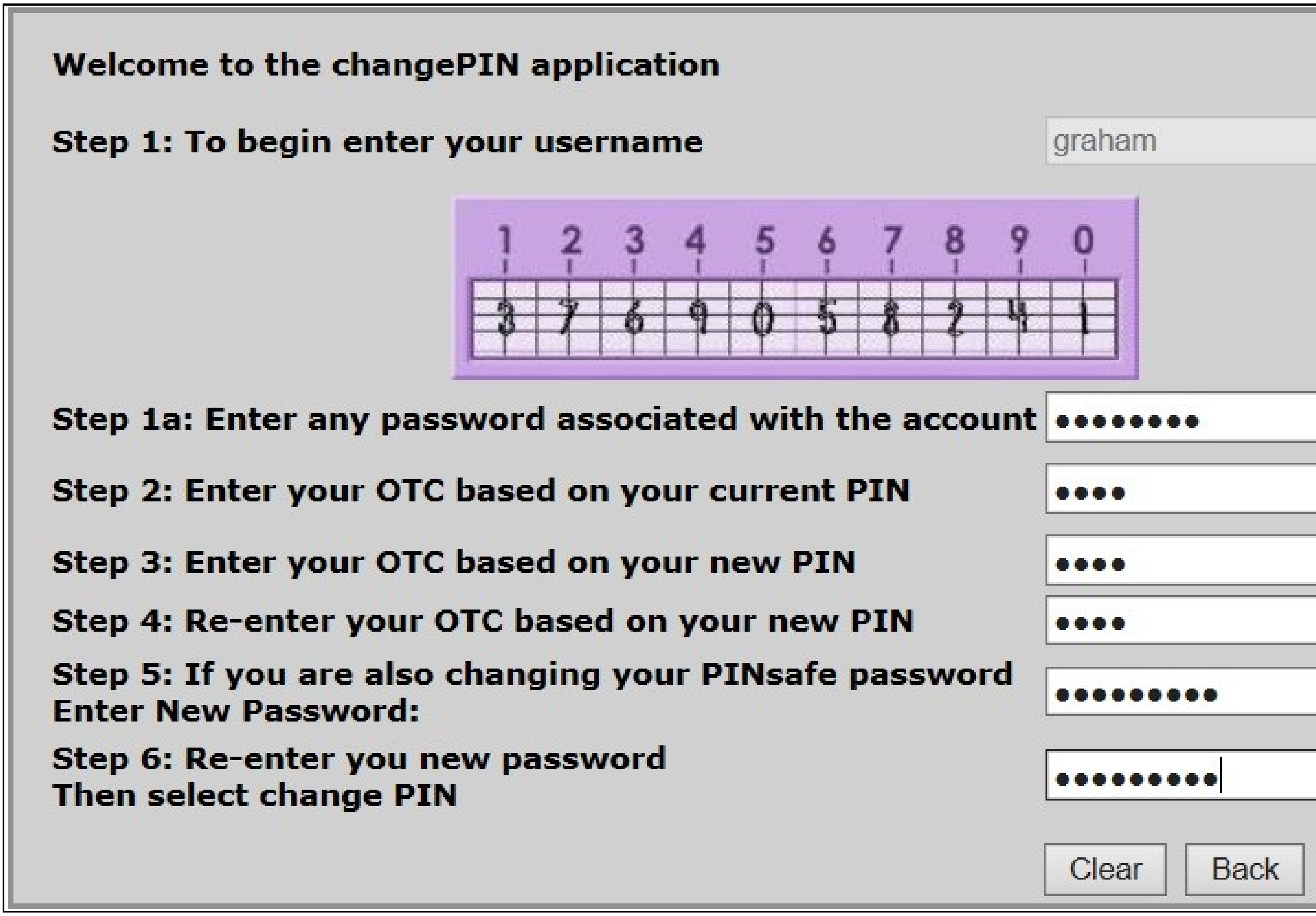
Step 2: Enter your OTC based on your current PIN ●●●●

Step 3: Enter your OTC based on your new PIN

Step 4: Re-enter your OTC based on your new PIN

Step 5: If you are also changing your PINsafe password
Enter New Password:

Step 6: Re-enter you new password
Then select change PIN



Welcome to the changePIN application

Step 1: To begin enter your username graham

1 2 3 4 5 6 7 8 9 0

3 7 6 9 0 5 8 2 4 1

Step 1a: Enter any password associated with the account ●●●●●●●●●

Step 2: Enter your OTC based on your current PIN ●●●●

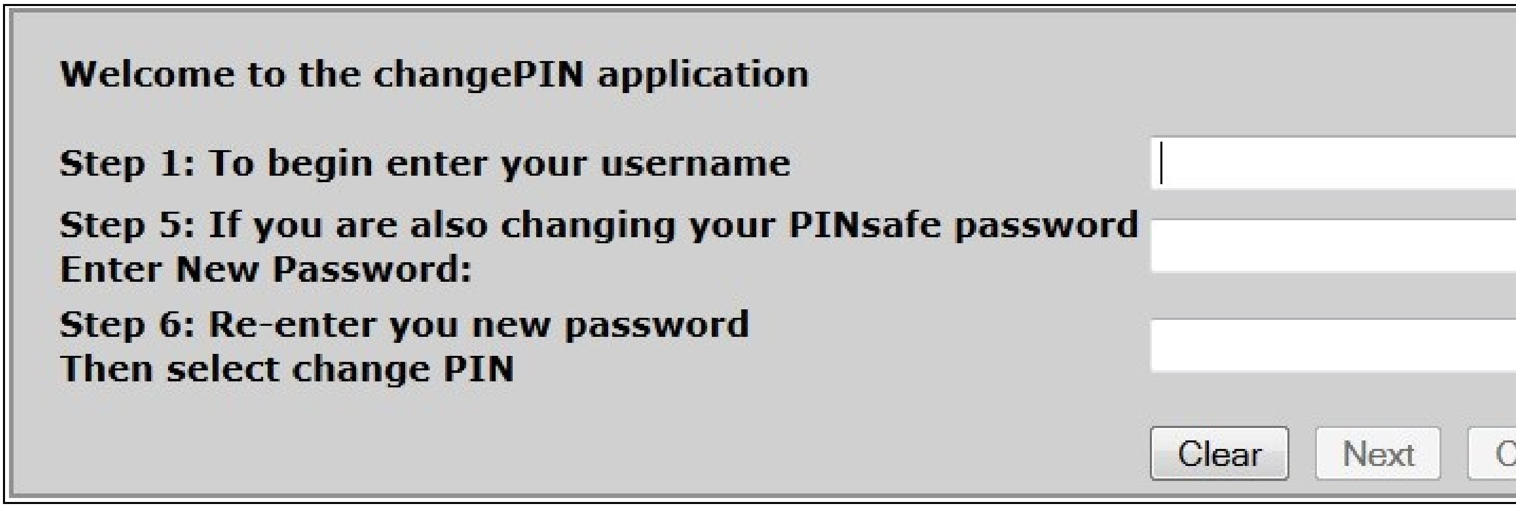
Step 3: Enter your OTC based on your new PIN ●●●●

Step 4: Re-enter your OTC based on your new PIN ●●●●

Step 5: If you are also changing your PINsafe password
Enter New Password: ●●●●●●●●●●

Step 6: Re-enter you new password
Then select change PIN ●●●●●●●●●●

84.4 ChangePIN with Change Password version 3572

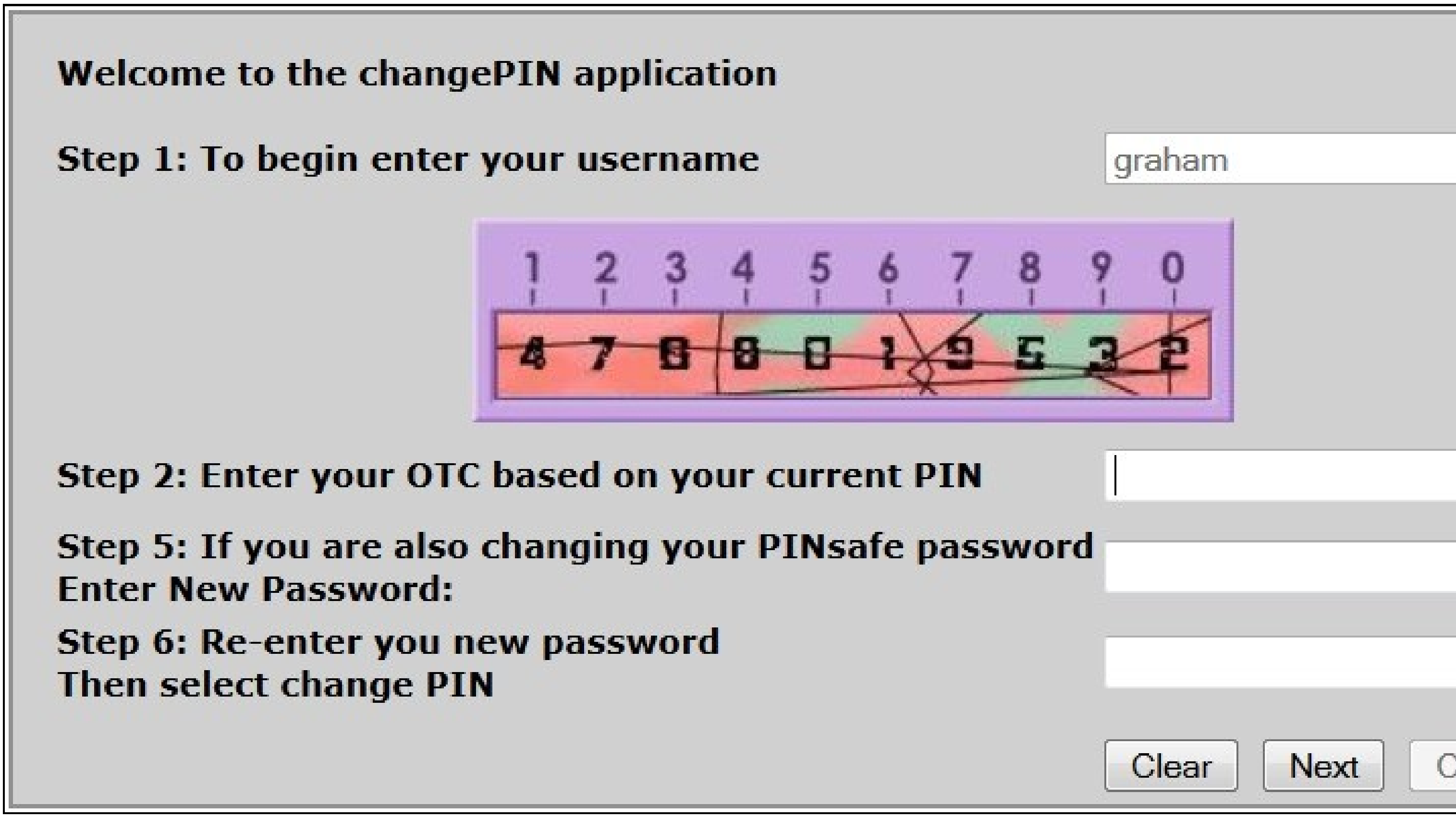


Welcome to the changePIN application

Step 1: To begin enter your username

Step 5: If you are also changing your PINsafe password
Enter New Password:

Step 6: Re-enter you new password
Then select change PIN



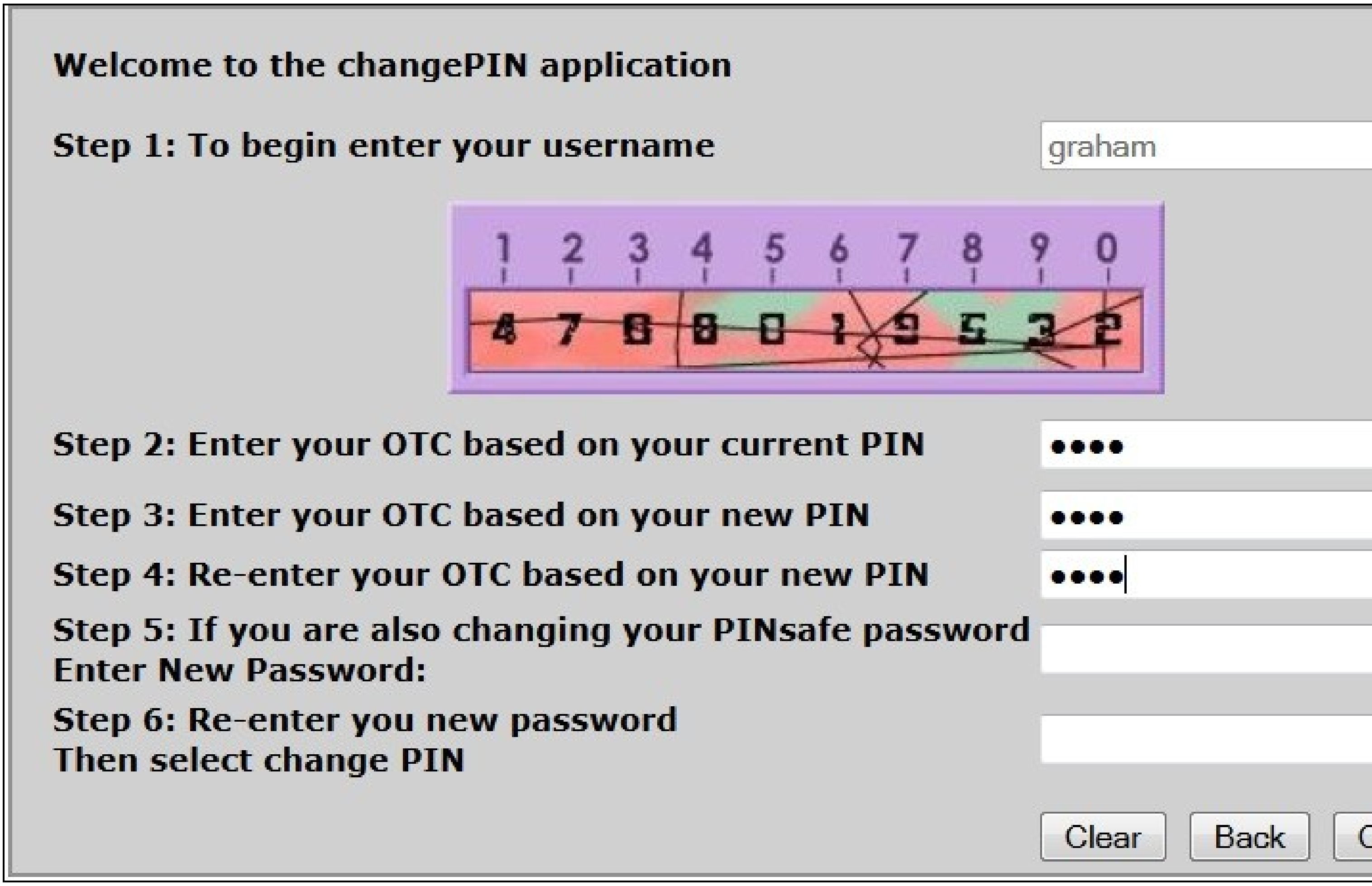
Welcome to the changePIN application

Step 1: To begin enter your username graham

Step 2: Enter your OTC based on your current PIN

Step 5: If you are also changing your PINsafe password
Enter New Password:

Step 6: Re-enter you new password
Then select change PIN



Welcome to the changePIN application

Step 1: To begin enter your username graham

Step 2: Enter your OTC based on your current PIN ●●●●

Step 3: Enter your OTC based on your new PIN ●●●●

Step 4: Re-enter your OTC based on your new PIN ●●●●

Step 5: If you are also changing your PINsafe password
Enter New Password:

Step 6: Re-enter you new password
Then select change PIN

85 ChangePINpad How to Guide

86 CMI

87 Overview

The Command Management Interface (CMI) is a menu interface to configure the Swivel appliances.

88 Prerequisites

Swivel appliance 2.x

89 Accessing the CMI

The CMI can be accessed in a number of different ways, see Console Access How to guide

90 Basic Configuration of the Appliance through the CMI

For the initial configuration steps see Getting Started Basic CMI configuration

91 Basic Appliance Administration

92 Advanced CMI utilities

Password change for CMI How to Guide

Recovering admin console access for the Swivel Administration

Backup Appliance

Restore Appliance

Automated FTP Backups

Patch Swivel Install

Patch Appliance Install

SNMP PINsafe How to Guide

SSL Solutions

MySQL Appliance Database Synchronisation

Static Routes How to Guide

92.1 Hardware Appliances

Recovery Disk for Appliances How to Guide

93 Testing

94 Known Issues

95 Troubleshooting

Tomcat stops after logout out of CMI

NTP Settings are not saved

Hostname change fails on appliance

Password recovery for appliance How to guide

VIP problem

96 Command Line Access How to guide

97 Overview

Swivel appliances are configured using the Command Management Interface (CMI) through which access to the Command Line can be obtained. document details how to access the Command Line. For information on how to access the appliance console see Console Access How to guide

98 Prerequisites

Swivel appliance 2.x

Swivel Appliance Command Line password. This is not normally given out unless directed by Swivel Secure support, and is only obtainable from Swivel Secure support.

99 Command Line Access

On the Swivel Administration console, select the Advanced Option then Command Line. Enter the Command Line Access password.

100 Returning to the CMI

To leave the Command line and return to the CMI type exit

100.1 Known Issues

100.2 Troubleshooting

Root password does not work

Root access is not allowable directly, the user needs to login through admin and then access through the CMI to the Commmand Line Access.

Older appliances may have no CMI and differing root passwords.

101 Console Access How to guide

102 Overview

Swivel appliances are configured using the Command Management Interface (CMI) through the console, this document outlines how to access the console. For access to the Command Line see Command Line Access How to guide.

103 Prerequisites

Swivel appliance 2.x

104 Console Access Methods

Console access to Swivel appliances is available in the following ways:

104.1 Virtual Machine (VM) Console

Virtual machines provide console access using the **admin** user through the Virtual Machine management tools.

104.2 Secure Shell (SSH)

SSH access can be made using the **admin** user to the appliance IP address on port 22. See PuTTY How To Guide for more information.

104.3 WinSCP

For uploading and Downloading files using the **admin** user , see WinSCP How To Guide.

104.4 Hardware Appliance Console (KVM)

Hardware appliances support the use of a Keyboard, Video and Mouse for console access using the **admin** user .

104.5 Hardware Appliance Dell Remote Access Card (DRAC)

Hardware appliances support where present the out of band Dell Remote Access Cards, see DRAC Card How To Guide

105 Issuing Commands through the command line

Different keyboard mappings may make it difficult to enter some commands, this can commonly occur when a VPN or remote desktop sharing is used to further access the command line through the console. The following describes the use of Ascii codes to obtain the correct character.

105.1 Using Ascii codes at the command line

When using Ascii codes press the Alt key together with the number keys of the Ascii code. This is done using the numeric keypad (laptops may require the Fn key and the Alt key to be used).

e.g. FnALT124

105.2 Commonly used Ascii codes

! 33

' 39

- 45

/ 47

\ 92

| 124

106 Known Issues

107 Troubleshooting

108 Contact Details

109 Overview

Details on contacting Swivel

110 Product updates and news

Technical bulletins are sent to partners and end-users, to subscribe send an email to hq@swivelsecure.com

111 Technical Support

Customers should contact their reseller for initial support. If the knowledgebase does not resolve your query, resellers are encouraged to submit a support Ticket. You should receive a trouble ticket reference number, if you do not receive one within an hour please check your spam filter then do try again.

112 Sales

To contact a sales representative please email info@swivelsecure.com

113 Product Enhancement and Product development

To submit a request for a product enhancement please email support@swivelsecure.com

114 Wiki Submission

To submit a wiki article please email support@swivelsecure.com

115 Anything Else

Further contact details are available here

116 Date How to guide

117 Overview

It is important that each Swivel instance has the correct date set, and it is recommended to use NTP to automatically set this. This document covers viewing and changing dates on Swivel appliances.

Note: Do not change the Timezone on a Swivel appliance except during the initial installation. Remember to restart the database i.e. for internal restart Swivel or MySQL for appliances when the timezone is set.

The default timezone for a Swivel hardware or virtual Appliance is GMT.

The default timezone for a Software installation is dependent on the default timezone of the OS.

118 Prerequisites

Swivel 3.x

Swivel appliance 2.x

119 Date and Time functions

119.1 Viewing the appliance date

The date and time can be viewed using the Webmin utility, see Webmin How To Guide

The date can also be viewed through the command line using the *date command*

See Console Access How to guide

119.2 Appliance Network Time Protocol to automatically set the system time and date

See NTP servers

119.3 Changing Appliance time and date

If NTP is not used, then the date can be set through the webmin, see Webmin How To Guide under Hardware\System Time, or the command line using the **date** command.

119.4 Appliance Log Files

Date and time is taken from the local system time

119.5 Swivel Log files

The timestamp in the log file is converted to a date and time using a JavaScript function on the client. This means that it always refers to local time for the client machine, not on the appliance itself. Swivel log files use the Swivel Date Format.

119.6 Date Format

The Swivel logging and reporting date format is set on the Swivel Administration console under Server/Language.

120 Known Issues

Do not change the Timezone on a Swivel appliance except during the initial installation. Restart the database i.e. for internal restart Swivel or MySQL for appliances.

121 Troubleshooting

122 Debug how to guide

123 Overview

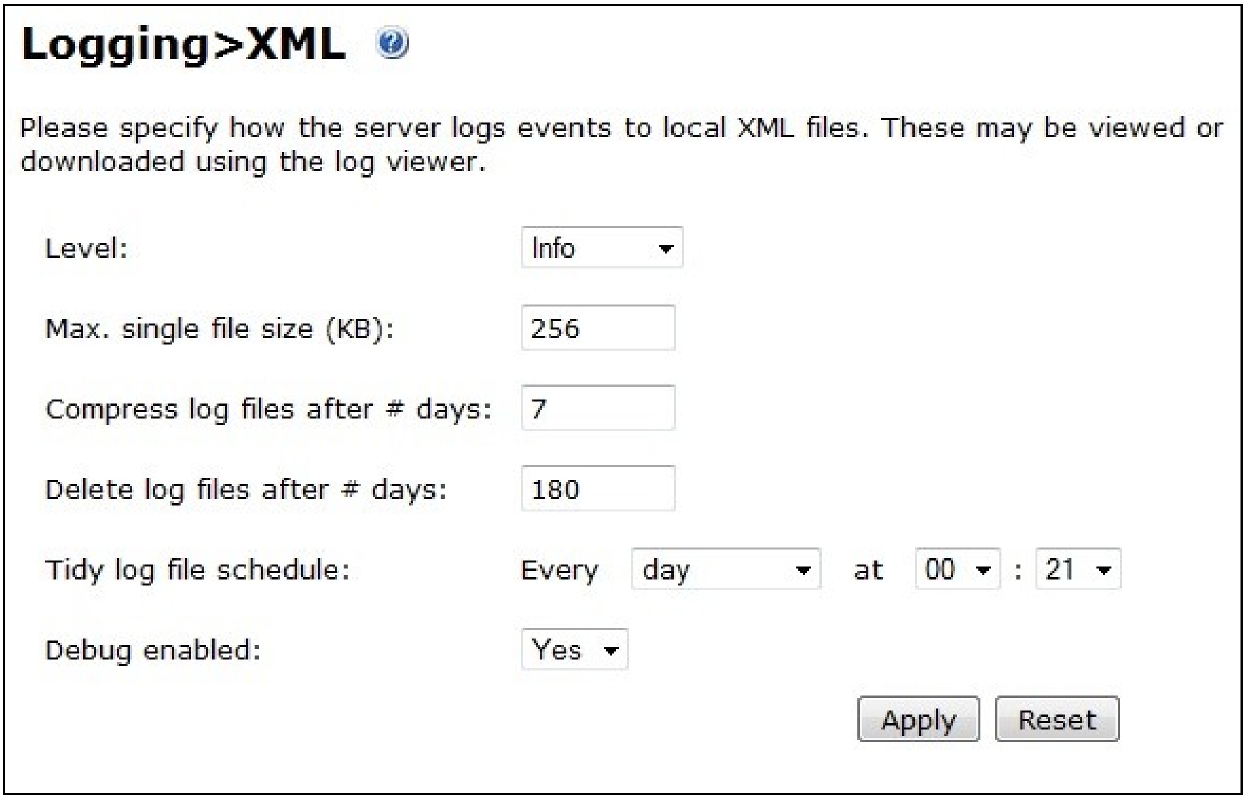
Swivel can log events in detail to resolve issues, this document outlines how to enable debug logging.

124 Prerequisites

Swivel 3.x

125 How to enable debug logging

On the Swivel Administration console select Logging, then XML, from version 3.9 set **Debug enabled:** to Yes. Earlier versions have debug under level.



Logging>XML

Please specify how the server logs events to local XML files. These may be viewed or downloaded using the log viewer.

Level:	Info
Max. single file size (KB):	256
Compress log files after # days:	7
Delete log files after # days:	180
Tidy log file schedule:	Every day at 00 : 21
Debug enabled:	Yes

125.1 RADIUS Debug

RADIUS debugging has an additional option under RADIUS Server, Ensure **Enable debug:** is set to Yes. However, you also need to enable debug logging as above in order for it to take effect.

126 Debug Files

The Debug files are stored in the same folder as the log files see Troubleshooting Files FAQ, and may be imported into the Log Viewer Application

127 Testing

Check the logs for the required level of logging

128 Known Issues

129 Troubleshooting

130 Download repository creation

130.1 Overview

It is possible to create a repository on the PINsafe server where users can download client software from.

130.2 Prerequisites

PINsafe appliance or software install

130.2.1 Creating the repository

Upload the required software to the pinsafe folder. Note: ensure that executable scripts are not uploaded to the PINsafe server:

130.2.1.1 For an PINsafe appliance

For information on uploading files to a PINsafe appliance see: WinSCP How To Guide

/usr/local/tomcat/webapps/pinsafe

or for the proxy port

/usr/local/tomcat/webapps2/proxy

130.2.1.2 For a Windows Server:

/Program Files/ Apache Software Foundation/Tomcat 6.0/webapps/pinsafe

or

/Program Files/ Apache Software Foundation/Tomcat 5.0/webapps/pinsafe

130.3 Testing

Browse to the file location which should give the opportunity to download the software:

PINsafe Appliance

https://<IP>:8080/pinsafe/<filename>

or

https://<IP>:8443/proxy/<filename>

Software Install

http://<IP>:8080/pinsafe/<filename>

130.4 Known Issues

130.5 Troubleshooting

131 DR Appliance

131.1 Overview

This document outlines the use and options of the PINsafe appliance. The PINsafe DR appliance acts as a MySQL slave against which authentications may be made. It is designed for use in Disaster Recovery sites where in standard operations there are no authentications, and when the DR site is invoked, will handle authentications.

Note: When an account is locked on the DR server, the account lock is not replicated back to the PINsafe Master appliances.

131.2 Prerequisites

PINsafe DR appliance version 2

131.3 Restoring Data from a DR server

Note: Ensure backups are taken before following these steps.

DR servers can act as a source of data if the PINsafe Master servers cannot be read. A MySQL dump can be made from the DR appliance and copied to the PINsafe Primary Master.

```
mysql
stop slave;
exit;
mysqldump --single-transaction --flush-logs pinsafe_rep > /tmp/master_dump.sql
```

The data can then be copied to the remaining PINsafe appliances, see MySQL Appliance Database Synchronisation

131.4 How to promote a DR to Synchronise with data sources in the event of a disaster

DR servers will authenticate users in the event of a disaster. If the disaster is prolonged perhaps with the permanent loss of the PINsafe Master servers, new users may be required to be added to the DR appliance. PINsafe DR servers in the event of a Disaster Recovery Scenario can be configured to read data sources to add users for authentication.

Note: This assumes that the PINsafe Master servers are no longer accessible and should only be carried out in a Disaster Recovery scenario. Ensure that a backup has been made of the DR appliance.

131.4.1 DR Preparation

Configuring the DR server with the required settings in advance will save time in a disaster scenario and ensure the data is known. The steps below for Data Repositories, Add Groups, Configure transports can be pre-configured and should match those of the Master appliances, incorrect data may result in PIN numbers being resent or users being deleted/added.

131.4.2 Set Mode to Synchronised

On the PINsafe DR appliance Administration Console select Mode/General then set the Mode to Synchronised then Apply. This should only be done when the DR is to be used to write data to the MySQL database. In standard DR operation it should be left in Slave Mode.

131.4.3 Add Data Repositories

On the PINsafe Administration console select Repository Server, then add the required repository. Synchronisation schedule should not be set unless data is to be imported as in a disaster scenario. A DR data source should be specified as the repository.

131.4.4 Add Groups

PINsafe groups can be created and should match those on the PINsafe Master servers.

131.4.5 Configure Transports

PINsafe Transports can be created and should match those on the PINsafe Master servers.

131.5 Post Disaster (Returning back to standard DR)

When the main site is back in operation, the MySQL database replication would need to be established again, with the Master PINsafe servers. If the data on the DR site is to be used, it would need to be copied to the PINsafe Primary Master server. The changes to make a DR would need to be reversed so that it once again runs in slave mode.

If the DR site is to become the main site, then Primary/Standby Masters servers should be deployed.

131.6 Testing

131.7 Known Issues

131.8 Troubleshooting

132 Filter IP How to Guide

133 Overview

The Swivel Administration Console can be protected by allowing access to a defined IP or range of IP addresses. The administrative filter is included as part of the Swivel 3.2 software and all subsequent releases.

134 Prerequisites

Swivel 3.2 onwards

Swivel 3.1.x filter can be added

135 How to use the IP Filter

135.1 Configuration

135.1.1 Swivel Core File location

The filter configuration is controlled by two files found in the conf folder

filter.properties, Determines the way the filter behaves when access is denied or granted.

ranges.xml, is a list of IP ranges that can access the Admin Console.

These files are located in:

Swivel version 3.9.1 onwards, see Transient Data Storage, <path to .swivel>/conf

Earlier versions of Swivel <path to Tomcat>/webapps/pinsafe/WEB-INF/conf:

135.1.2 Swivel Applications File Location

Applications such as the Sivel Authentication manager will have their filter located under home/swivel/<application_name>/security.properies and is similar to the ranges.xml file.

135.2 Editing filter.properties

The default filter.properties file is shown below.

```
#
# Admin Console Filter Localization
#
# Commented lines will result in no message being logged
#
# ALLOWED = Access Allowed
DENIED = Access Denied
ERROR = Page Not Found
# FILTERING = Filtering
STATUS = 404
```

The entries are as follows:

ALLOWED Message written to TOMCAT console with request IP address when the filter allows access. When Commented out; filter is silent. Default: Commented out

DENIED Message written to TOMCAT console with request IP address when the filter denies access. Default: Access Denied

ERROR Message reported back to browser when access is denied. If not set, no response is sent and the browser will eventually time out. Default: Page Not Found

FILTERING Message written to TOMCAT console followed by address ranges as TOMCAT initializes the filter. When Commented out; filter is silent. Default: Commented out

STATUS The http status code reported back when access is denied. This should match the error message. Default: 404

135.3 Editing ranges.xml

The ranges.xml file holds the list of IP addresses that are allowed to access the admin console

The default ranges.xml file is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
        <entry key="anyone">0/0</entry>
        <entry key="anyone6">::0/0</entry>
        <entry key="localhost">127.0.0.1/255.255.255.255</entry>
        <entry key="localhost6">::1/128</entry>
</properties>
```

The default configured ranges.are named ?anyone? and ?localhost? and represent access from any IP address and localhost only respectively.

An address range is specified as an IP address followed (optionally) by a mask. The mask can be a single integer representing the number of significant address bits that must match for access to be allowed or it can be an IP-style dotted decimal. Both styles are present in the default file, but further examples are shown below.

The default entries allow access from all IP addresses. Removing the entry for ?anyone? will restrict access to localhost. Further ranges can be added to ease administration. All ranges should have a unique name.

IP Range Meaning

A /0 mask means that no bits need to match in the address. This allows access from all IP addresses.

Example 1:

0/0

123.123.123.123/0

A /32 mask means all 32 bits must match. The equivalent dotted-decimal is 255.255.255.255. Specifying no mask is the same as specifying a /32 mask.

Example 2:

127.0.0.1/32

127.0.0.1/255.255.255.255

127.0.0.1

To allow access from any address on the 192.168.0 subnet.

Example 3:

192.168.0.0/24

192.168.0.0/255.255.255.0

The values for <entry key="anyone6">::0/0</entry> and <entry key="localhost6">::1/128</entry> are for IPv6

135.4 Editing what is filtered

By default all access to the admin port is filtered. It is possible to define specific access using the filter. What is filtered is controlled by the web.xml file, this file is usually located as follows:

Appliance: /usr/local/tomcat/webapps/pinsafe/WEB-INF/web.xml

Software only: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\pinsafe\WEB-INF\web.xml

Look for the following entry:

```
<filter-mapping>
               <filter-name>adminConsoleFilter</filter-name>
               <url-pattern>/*</url-pattern>
       </filter-mapping>
```

To filter just the TURing image request, change this to:

```
<filter-mapping>
               <filter-name>adminConsoleFilter</filter-name>
               <url-pattern>/SCImage</url-pattern>
       </filter-mapping>
```

135.5 Activating the filter

Restart Tomcat

136 Testing

When someone attempts to access any part of the admin console they are redirected to the admin log-in page. At this point the filter intercepts the request and checks to see if the IP address is on the allowed list. If it is not allowed then a message will display **Swivel is running. Click here to open Swivel admin console.** but clicking on the link has no effect. Older versions return the error code and message defined in the filter.properties file.

137 Known Issues

Swivel version 3.10.4 increases the filtering and additional access may need to be added for Agents and other resources accessing Swivel.

More recent versions display **Swivel is running. Click here to open Swivel admin console.** instead of the messages in the filter.properties file.

Windows Server 2008 by default treats "localhost" as an IPv6 address (::1), rather than IPv4 (127.0.0.1), so if the ranges file doesn't include the IPv6 address, it will fail. The one that comes with Swivel 3.8 includes additional entries to cover IPv6 addresses.

If you have customised your ranges.xml, then you can try the following:

Connect to Swivel using 127.0.0.1 rather than localhost

Disable IPv6 on the server

Add the following entries to ranges.xml:

```
::1/128 (to allow localhost on IPv6)

::0/0 (to allow any address on IPv6)
```

138 Troubleshooting

Check the Tomcat logs, these are located under <path to Tomcat>/logs. The localhost.<date> log will contain failed connection attempts

INFO: Access Denied x.x.x.x

139 Firewall Appliance Configuration

140 Overview

Each Swivel appliance has a firewall protecting access to that sever. This document details how to add and change the Firewall configurations on Swivel appliances. For information on configuring Port Address Translation, see How to run PINsafe on non-default ports, this allows ports such as 443 or 80 to be used. Forinformation on ports used by Swivel appliances see Ports.

The Swivel Administration console access can also have IP access control, see Filter IP How to Guide

141 Prerequisites

Swivel Appliance 2.x

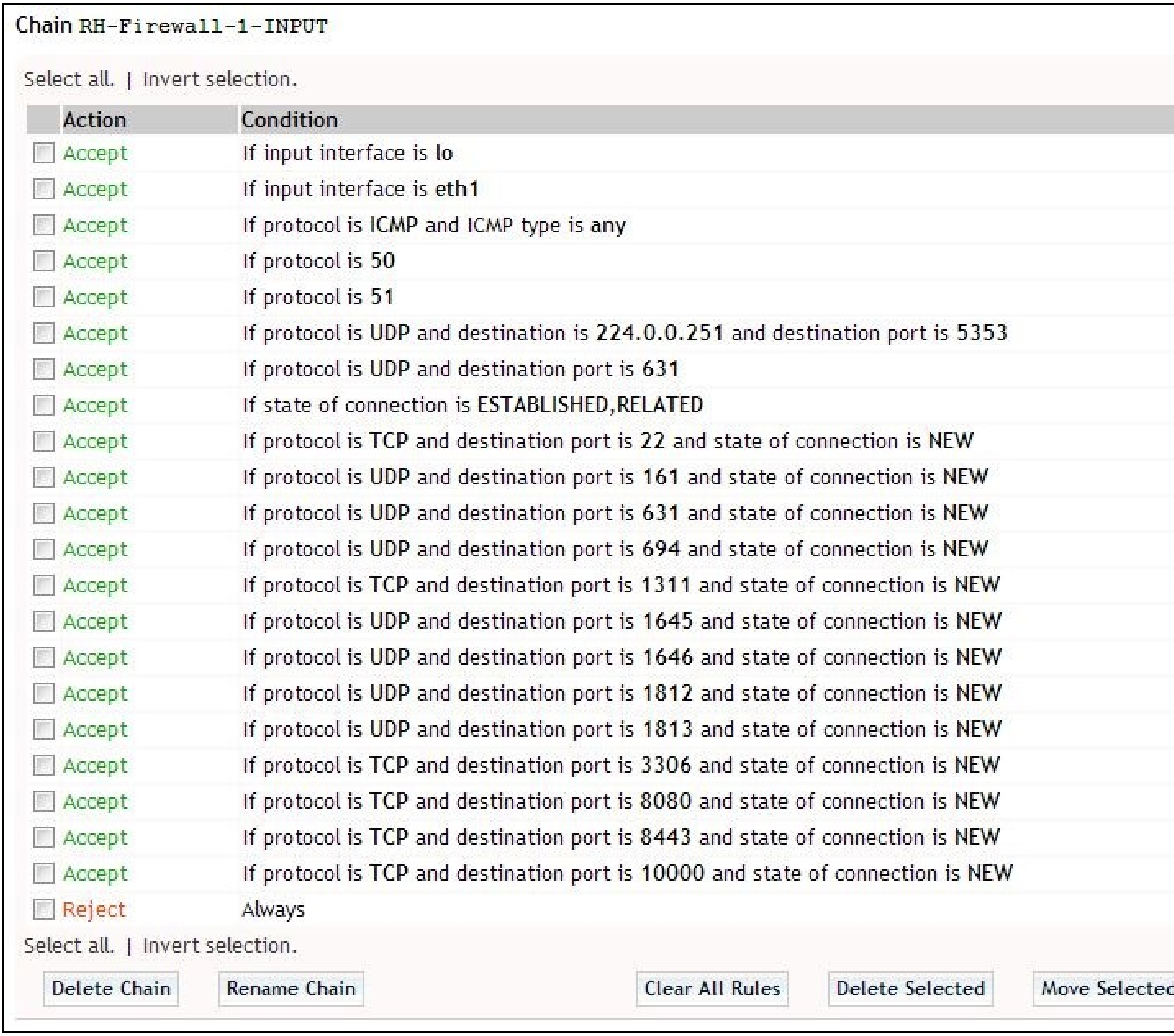
142 Configuring the Firewall

142.1 Webmin

Configuration of the firewall is usually carried out using Webmin

142.2 Firewall Add Rule

Once logged in select Networking then Firewall. Locate the Chain RH-Firewall-1-INPUT then below this click on **Add Rule**.



Chain RH-Firewall-1-INPUT

	Action	Condition
□	Accept	If input interface is lo
□	Accept	If input interface is eth1
□	Accept	If protocol is ICMP and ICMP type is any
□	Accept	If protocol is 50
□	Accept	If protocol is 51
□	Accept	If protocol is UDP and destination is 224.0.0.251 and destination port is 5353
□	Accept	If protocol is UDP and destination port is 631
□	Accept	If state of connection is ESTABLISHED,RELATED
□	Accept	If protocol is TCP and destination port is 22 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 161 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 631 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 694 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 1311 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1645 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1646 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1812 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1813 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 3306 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8080 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8443 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 10000 and state of connection is NEW
□	Reject	Always

Enter the following parameters:

Rule Comment description of the rule

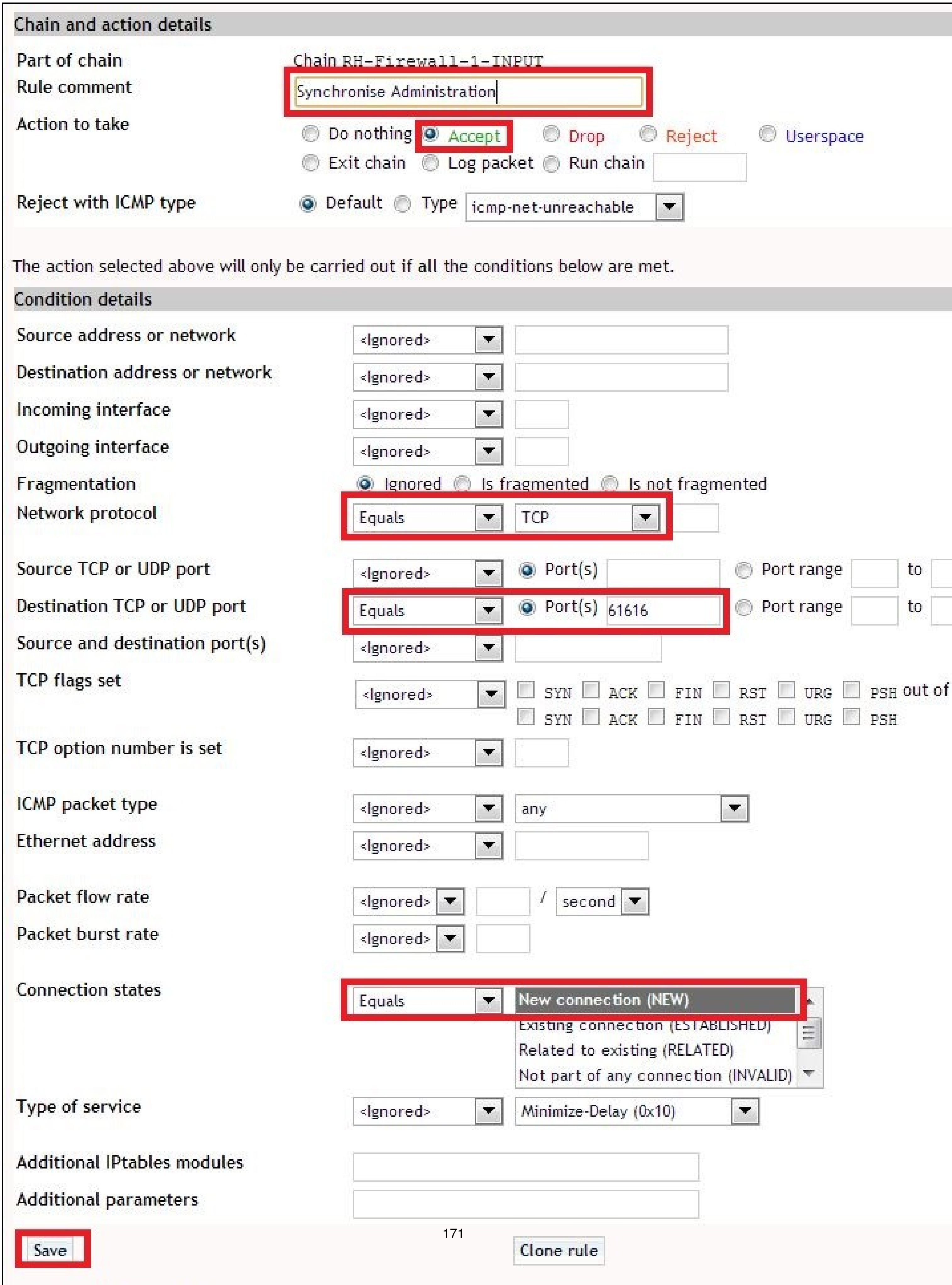
Action to take select **Accept** to allow the rule

'*Network Protocol **select** Equals* and TCP or UDP as appropriate

'*Destination TCP or UDP port **select** Equals* and set the port required

Connection states select **Equals** and **New connection (NEW)**

When complete click on Save.



Chain and action details

Part of chain: Chain RH-Firewall-1-INPUT

Rule comment: Synchronise Administration

Action to take: ○ Do nothing ● Accept ○ Drop ○ Reject ○ Userspace ○ Exit chain ○ Log packet ○ Run chain

Reject with ICMP type: ● Default ○ Type icmp-net-unreachable

The action selected above will only be carried out if **all** the conditions below are met.

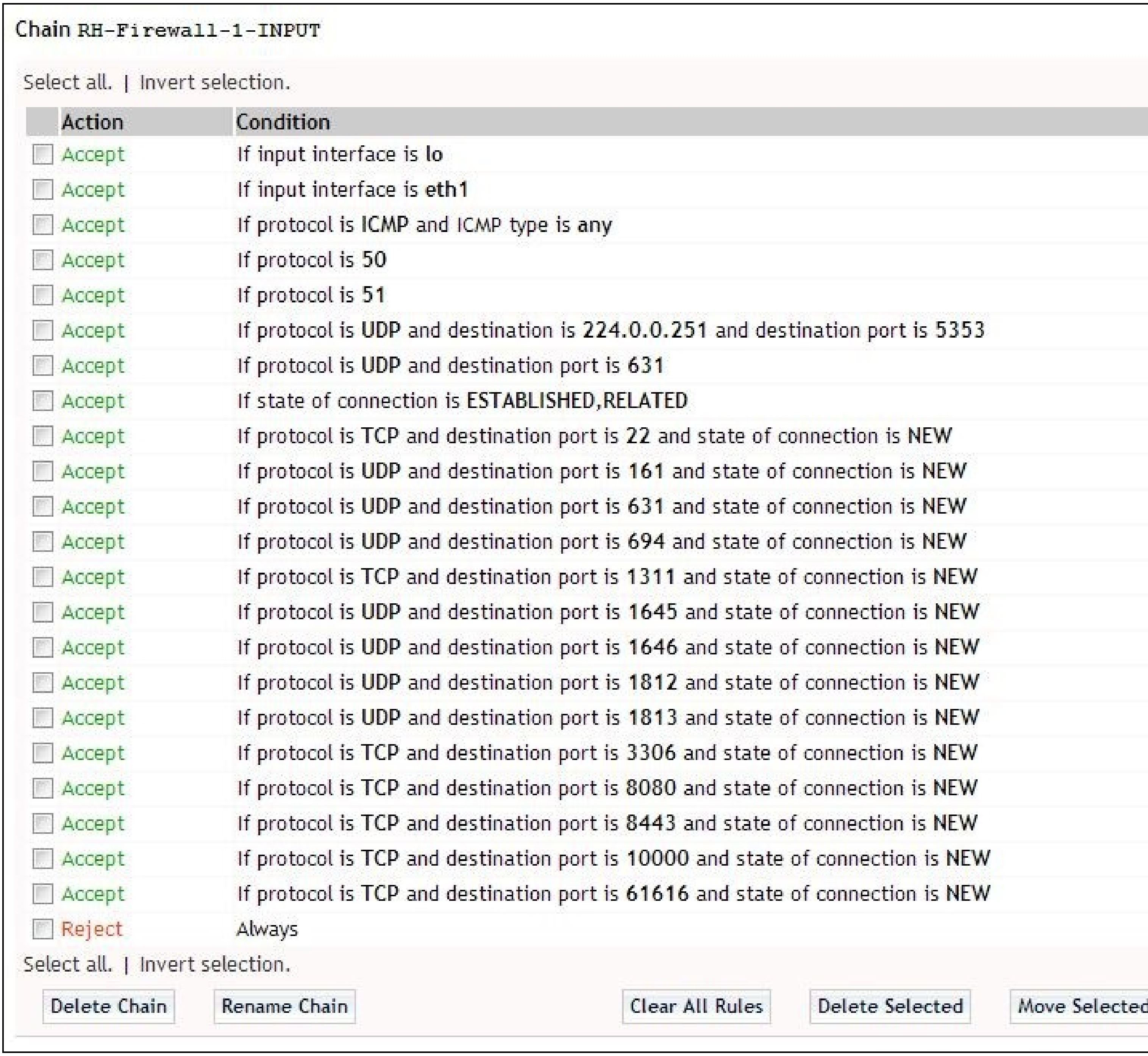
Condition details

Source address or network	<Ignored>	
Destination address or network	<Ignored>	
Incoming interface	<Ignored>	
Outgoing interface	<Ignored>	
Fragmentation	● Ignored ○ Is fragmented ○ Is not fragmented	
Network protocol	Equals	TCP
Source TCP or UDP port	<Ignored>	● Port(s) ○ Port range to
Destination TCP or UDP port	Equals	● Port(s) 61616 ○ Port range to
Source and destination port(s)	<Ignored>	
TCP flags set	<Ignored>	□ SYN □ ACK □ FIN □ RST □ URG □ PSH out of □ SYN □ ACK □ FIN □ RST □ URG □ PSH
TCP option number is set	<Ignored>	
ICMP packet type	<Ignored>	any
Ethernet address	<Ignored>	
Packet flow rate	<Ignored>	/ second
Packet burst rate	<Ignored>	
Connection states	Equals	New connection (NEW) Existing connection (ESTABLISHED) Related to existing (RELATED) Not part of any connection (INVALID)
Type of service	<Ignored>	Minimize-Delay (0x10)
Additional IPtables modules		
Additional parameters		

Save | Clone rule

142.3 Change the rule priority

Increase the rule priority so that it is above the Reject rule by clicking on the green up arrow.



Chain RH-Firewall-1-INPUT

Select all. | Invert selection.

	Action	Condition
□	Accept	If input interface is lo
□	Accept	If input interface is eth1
□	Accept	If protocol is ICMP and ICMP type is any
□	Accept	If protocol is 50
□	Accept	If protocol is 51
□	Accept	If protocol is UDP and destination is 224.0.0.251 and destination port is 5353
□	Accept	If protocol is UDP and destination port is 631
□	Accept	If state of connection is ESTABLISHED,RELATED
□	Accept	If protocol is TCP and destination port is 22 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 161 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 631 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 694 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 1311 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1645 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1646 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1812 and state of connection is NEW
□	Accept	If protocol is UDP and destination port is 1813 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 3306 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8080 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 8443 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 10000 and state of connection is NEW
□	Accept	If protocol is TCP and destination port is 61616 and state of connection is NEW
□	Reject	Always

Select all. | Invert selection.

142.4 Apply Configuration

Click on Apply Configuration to make the firewall rules active.

[Image:Swivel Appliance Webmin Firewall apply configuration.JPG]]

143 Testing

144 Known Issues

145 Troubleshooting

146 Google Authenticator

147 Overview

Google Authenticator supports the use of OATH HOTP such as used with the Swivel Token, and software tokens with a valid Seed can be used to authenticate Swivel users. Google Authenticator uses HMAC-SHA1 seeds.

Currently Swivel is not compatible with the Authenticator Time Based OATH TOTP token as Swivel tokens use a 30 second refresh, and Google Authenticator uses a 60 second refresh.

148 Prerequisites

Swivel 3.9.6

Google Authenticator

149 Configure the Swivel User

For configuring the seeds on the Swivel server see Token. Configuring a software token is similar to configuring a hardware token.

Swivel uses a Hexadecimal seed, to generate a valid seed see seed.

150 Configure the Google Authenticator App

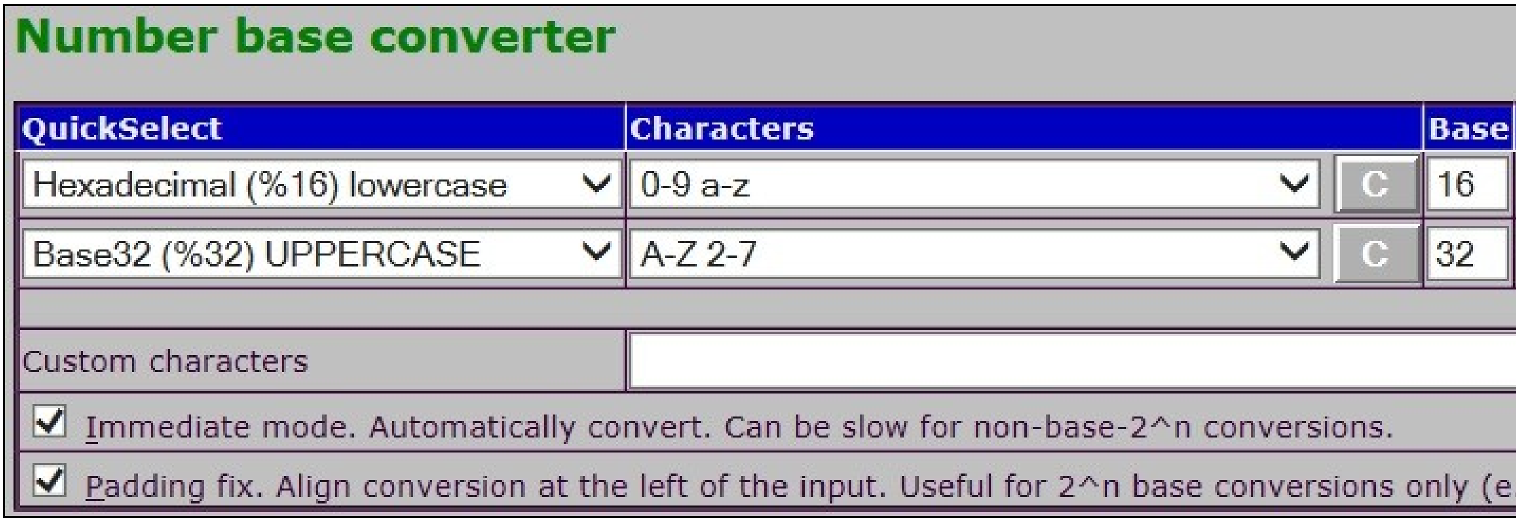
Convert the Hexadecimal seed ((A-Z, 0-9) into Base32 (A-Z, 2-7 and = for padding), for Google. Google enforces a minimum seed length of 16 characters or 80-bits. The following online tool can be used for converting the seed:

http://www.darkfader.net/toolbox/convert/

Example:

Base16 seed: e0b10ee3a4bb2598c0575539529f33 (used by Swivel)

Base 32 seed: 4CYQ5Y5EXMSZRQCXKU4VFHZT (used by Google Authenticator)



Number base converter

QuickSelect	Characters		Base
Hexadecimal (%16) lowercase	0-9 a-z	C	16
Base32 (%32) UPPERCASE	A-Z 2-7	C	32
Custom characters			

☑ Immediate mode. Automatically convert. Can be slow for non-base-2^n conversions.

☑ Padding fix. Align conversion at the left of the input. Useful for 2^n base conversions only (e

Download the Google Authenticator from the appropriate app store.

On the Google Authenticator App select Set up account, then Enter key provided

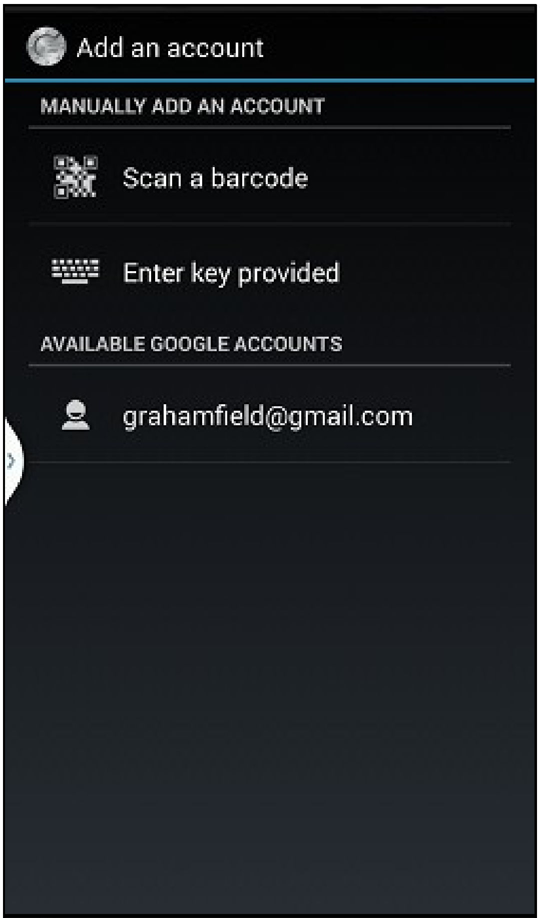
Enter account name The Swivel user name

Enter your key The seed

Time-based change to **Counter-based**

Select Add

Then synchronise the token (see Token)



Add an an account

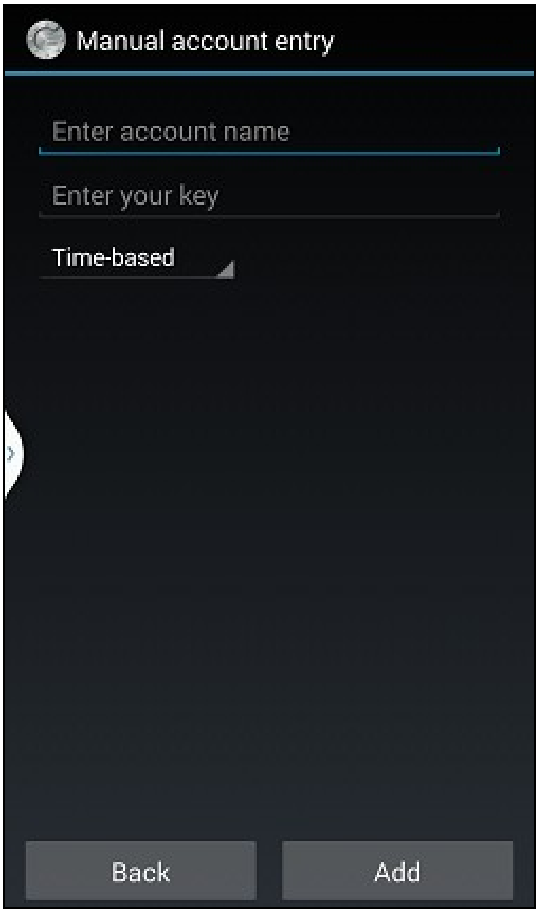
MANUALLY ADD AN ACCOUNT

Scan a barcode

Enter key provided

AVAILABLE GOOGLE ACCOUNTS

grahamfield@gmail.com

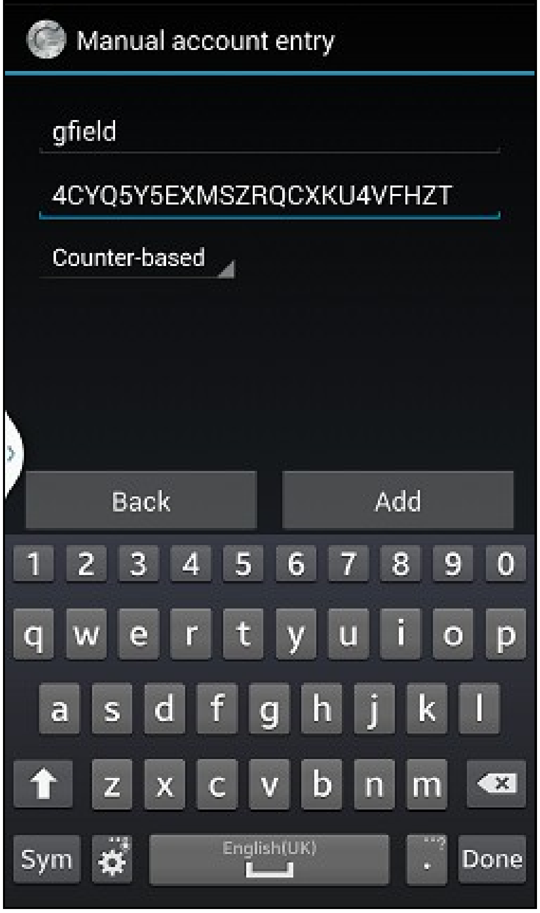


Manual account entry

Enter account name

Enter your key

Time-based

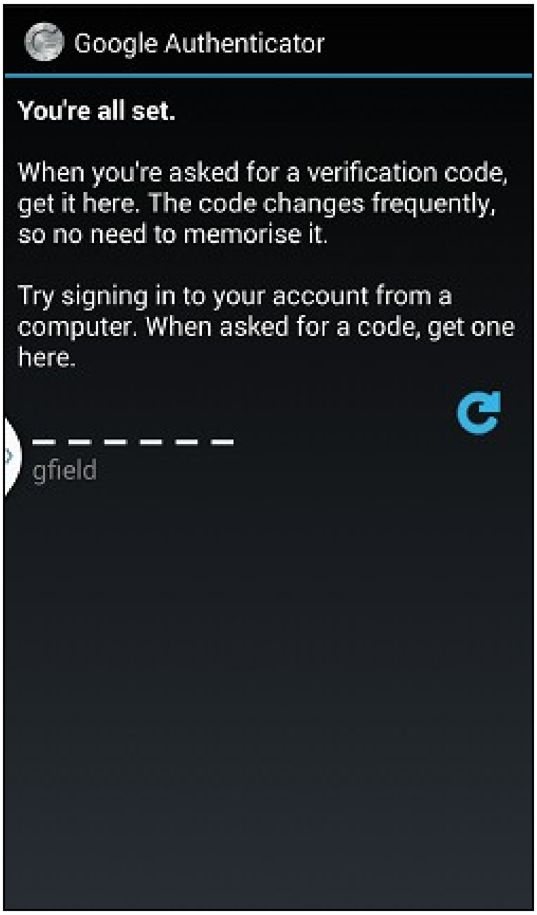


Manual account entry

gfield

4CYQ5Y5EXMSZRQCXKU4VFHZT

Counter-based



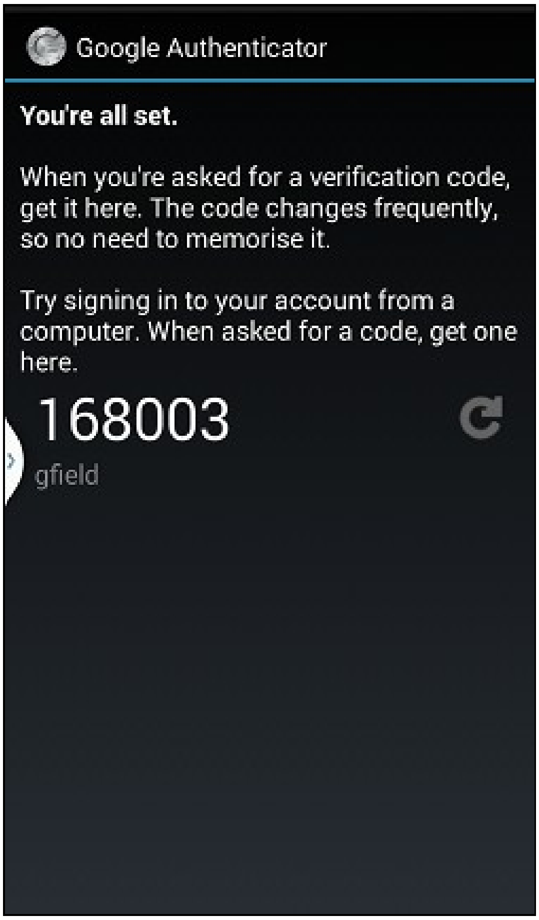
You're all set.

When you're asked for a verification code, get it here. The code changes frequently, so no need to memorise it.

Try signing in to your account from a computer. When asked for a code, get one here.

– – – – – –

gfield



You're all set.

When you're asked for a verification code, get it here. The code changes frequently, so no need to memorise it.

Try signing in to your account from a computer. When asked for a code, get one here.

168003

gfield

151 Testing

152 Known Issues

153 Troubleshooting

154 Health Check Swivel

155 Overview

This document outlines health checks that can be made on Swivel installs.

156 Prerequisites

Swivel 3.x

157 Client reported issues

Have any issues been reported by users

158 Swivel application checks

158.1 Swivel Version

On the Swivel Administration Console check the Swivel version given in the top right corner. Check to see if an upgrade is required. See Versions FAQ

158.2 Status

Check the Status page for:

- Excessive number of locked, deleted, disabled, inactive accounts
- Server is running in synchronised mode
- License has not or will soon expire or has been exceeded by the number of users.

158.3 Logs

On the Swivel Administration Console check the Swivel logs on each Swivel instance, see Log how to guide and Troubleshooting Files FAQ. Look for;

- NAS/AGENT requests not recognised by Swivel
- Repository Sync errors
- Syncs run at different times on servers
- Reasonable space between syncs
- RADIUS errors
- Large numbers of account creations/deletions

159 Tomcat checks

159.1 Tomcat logs

For a Swivel Virtual or hardware appliance check /var/log/tomcat, particularly the catalina.out, see also Troubleshooting Files FAQ.

Check that there are not an excessive number of logs

Are the logs recording the required amount of logging data

160 Operating system checks

160.1 Disk space

On each Swivel virtual or hardware appliance see Appliance Disk full

160.2 System logs

On each Swivel virtual or hardware appliance check the /var/log/messages, see also Troubleshooting Files FAQ.

Also dmesg using the dmesg command

```
dmesg
```

160.3 Date, time and timezone

On each Swivel virtual or hardware appliance check the date, time and timezone using the date command or Webmin.

```
date
```

160.4 Proccesses

```
ps -aux
```

160.5 socket information

The following commands are useful

```
ss -s
```

```
ss -t
```

```
ss -l
```

160.6 Networking

```
netstat -lanp
```

160.7 Backups

On each Swivel virtual or hardware appliance ensure there is sufficient disk space

Are the backups in /backups and expected size

If FTP backups or scp backups are made ensure that they exist, see Backup Appliance

161 Swivel virtual or hardware CMI checks

161.1 Versions

On each Swivel virtual or hardware appliance check in the CMI under Advanced/version for the versions running to see if an upgrade is required, see Appliance Versions FAQ

161.2 Appliance Heartbeat

On each Swivel virtual or hardware appliance check in the CMI under heartbeat status that the VIP is running on the primary. If required test the fail over to the standby by stopping heartbeat on the primary. Check Heartbeat and Mon are set to start at boot. See VIP Status.

161.3 Appliance Database Synchronization

On each Swivel virtual or hardware appliance check the MySQL status to ensure that they are in synchronization, see also MySQL Appliance Database Synchronisation.

162 Swivel hardware appliance Checks

Verify the DRAC card is accessible and working, see DRAC Card How To Guide

Is the an ISO image for bare metal recovery, see Recovery Disk for Appliances How to Guide

Are the Hardware appliances still under maintenance

163 Escalating issues found on the health check

Issues found on a health check should be checked against the Knowledgebase and if required escalated through the reseller and raised as a support ticket, see Support Ticket How To Guide.

164 Known Issues

165 Troubleshooting

166 Heap Space Memory Management How to guide

167 Overview

NOTE: This article is only relevant to version 2 appliances. Please do not refer to it when trying to manage memory in later appliances. Please contact supportdesk@swivelsecure.com for further information

This document outlines how to configure how much memory is used within Apache Tomcat. It may be useful when running multiple instances of Swivel.

168 Prerequisites

Swivel 3.x

Apache Tomcat

169 PINsafe Appliance

Login to the Command line through the CMI and verify the memory being used with the command *top*

The heap space value should be set already, but you can verify and if necessary set the values, see WinSCP How To Guide.

To increase the Heap Space of a Swivel appliance you need to edit catalina.sh in the /usr/local/apache-tomcat-5.5.20/bin folder Add the line at the start of the file after the comments

JAVA_OPTS="$JAVA_OPTS "-Xmx192m

You should be able to keep adding heap. We have tested over half a Gb of heap (-Xmx512m)

170 Additional Commands

170.1 Memory Usuage

```
cat /proc/meminfo
```

170.2 Freeing up Memory Cache

frees up page cache, dentries and inodes:

```
sh -c "sync; echo 3 > /proc/sys/vm/drop_caches"
```

171 Testing

172 Known Issues

173 Troubleshooting

174 Helpdesk Configuration Guide

175 Overview

This document outlines how to setup and configure Swivel Helpdesk Users. Helpdesk users can be setup to manage users in a number of ways, such as to manage all users or will only be able to view the users that are in the same repository or the repository they can manage. Additional restrictions may also be in place such as resetting PIN numbers, administering local repositories and Admin user accounts. Accounts with administrator rights can manage all user accounts. Helpdesk accounts cannot manage or create administrator or other helpdesk accounts.

The Helpdesk Operations User Guide provides information for Helpdesk users to manage users within the Swivel Administration console.

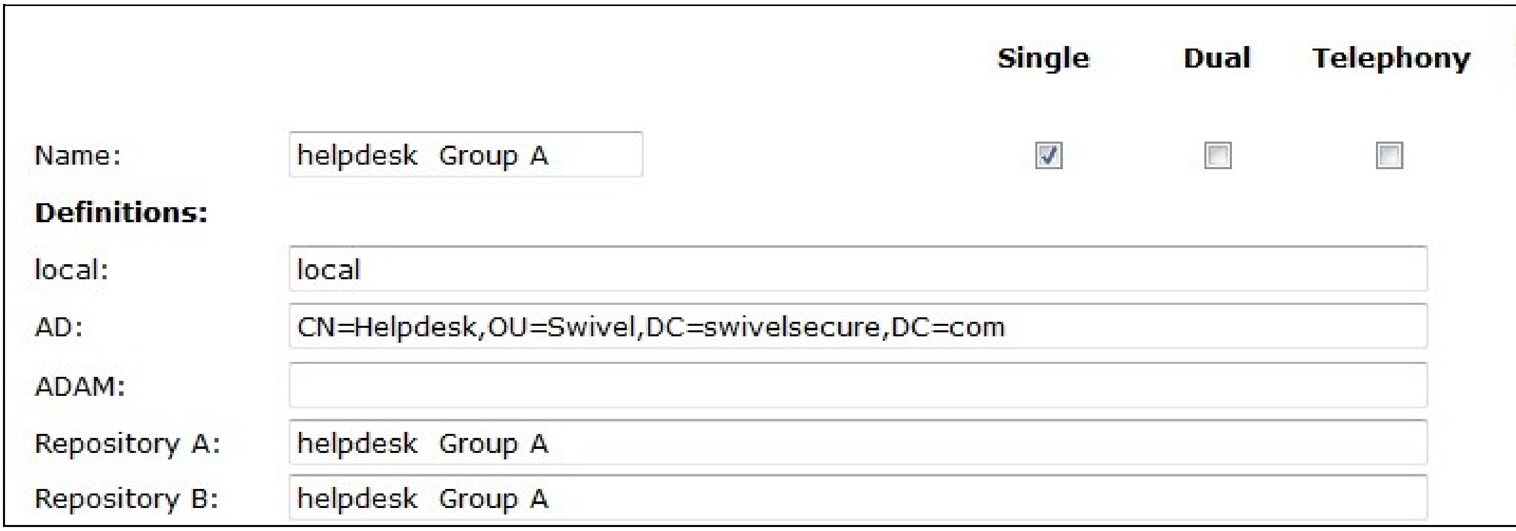
176 Prerequisites

Swivel 3.x

177 Creation of Helpdesk Users and Groups

177.1 Creating Helpdesk Groups

On the Swivel Administration Console select Repository/Groups, then enter a name for the Group and enter under the Definitions, then the repository for the users to be assigned these permissions, and tick the method to login to the Swivel Administration console, together with the Helpdesk check box . Click Apply to save the settings. Create multiple helpdesk groups as required.



		Single	Dual	Telephony
Name:	helpdesk Group A	☑	□	□
Definitions:				
local:	local			
AD:	CN=Helpdesk,OU=Swivel,DC=swivelsecure,DC=com			
ADAM:				
Repository A:	helpdesk Group A			
Repository B:	helpdesk Group A			

177.2 Assigning Helpdesk groups management

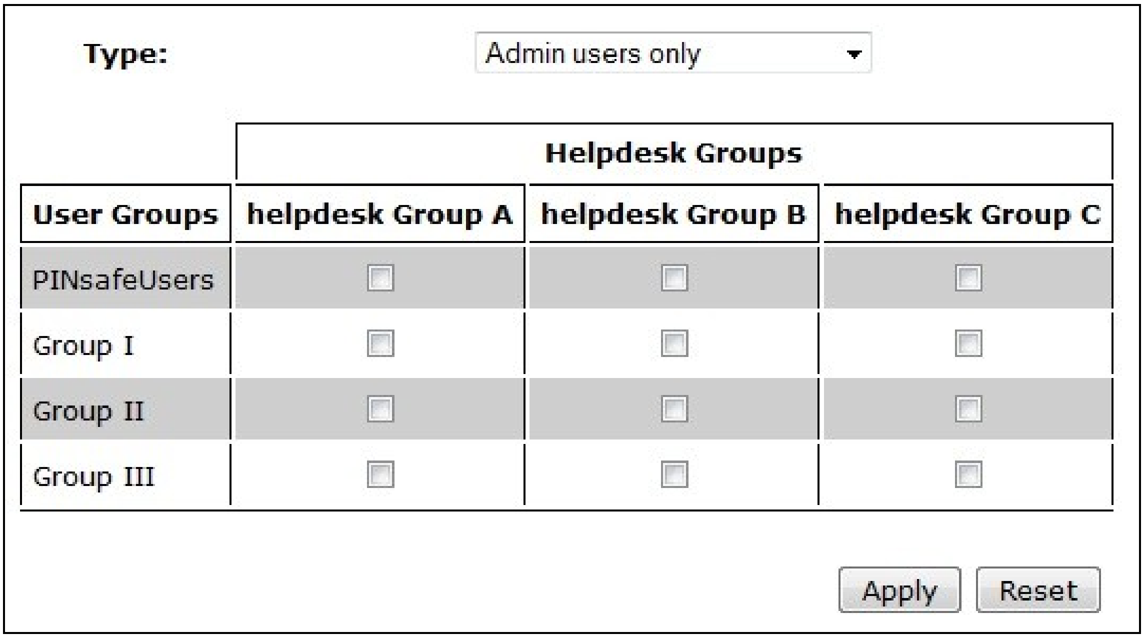
Granular Helpdesk management is available from Swivel 3.9 onwards. On the Swivel Administration Console select Policy/Helpdesk, and set allow **Helpdesk Users can manage other repositories:** to Yes, then select Repository/Groups, scroll down and click on Group Rights. On the Helpdesk Group Management page select Type:

Admin users only - only administrators can manage editable repositories. Helpdesk users have no rights.

Helpdesk users all groups - all helpdesk users (and admin users) can manage all non- admin accounts.

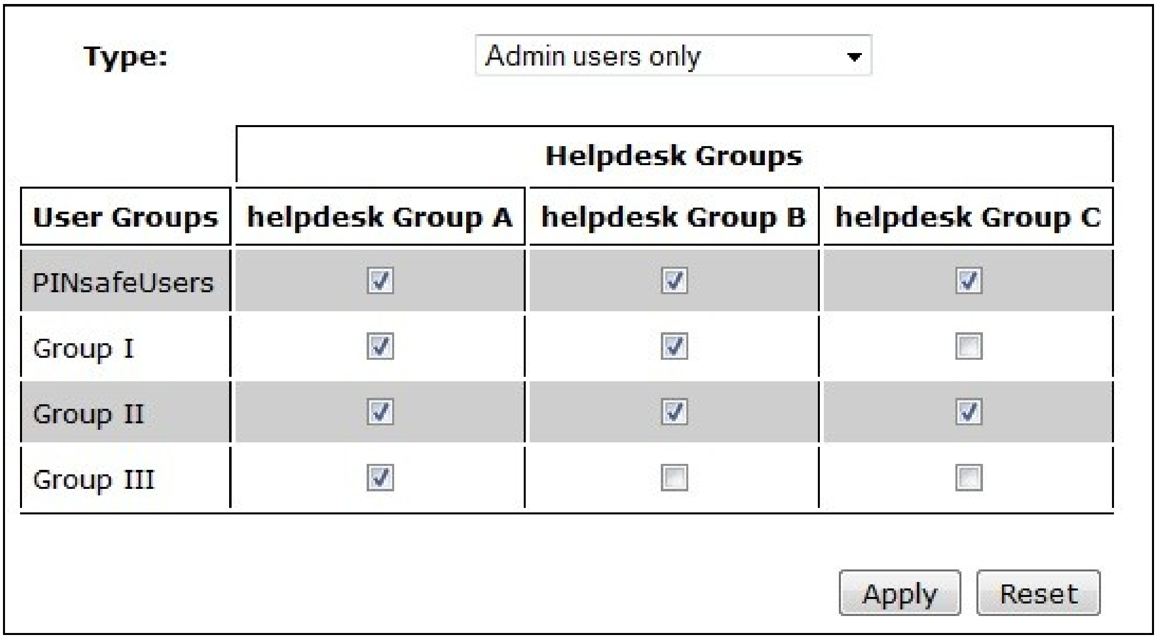
Helpdesk groups - helpdesk users have restricted rights as indicated below. If this option above is selected, then the group rights matrix comes into effect. Across the top of the matrix is a list of repository groups with helpdesk rights. Down the left of the matrix is a list of repository groups without helpdesk or admin rights. Tick checkboxes to indicate which helpdesk groups can manage which user groups." The Swivel groups that can be managed by the Helpdesk groups can be selected. Click on Apply to save the settings. Users will be assigned helpdesk rights when their repository synchronisation occurs.

In the below example, all the helpdesk users can manage the PINsafeUsers, but Group I can only be managed by members of *helpdesk Group A* and *helpdesk Group B*



Type: Admin users only ▾

	Helpdesk Groups		
User Groups	**helpdesk Group A**	**helpdesk Group B**	**helpdesk Group C**
PINsafeUsers	□	□	□
Group I	□	□	□
Group II	□	□	□
Group III	□	□	□



Type: Admin users only

	Helpdesk Groups		
User Groups	helpdesk Group A	helpdesk Group B	helpdesk Group C
PINsafeUsers	☑	☑	☑
Group I	☑	☑	□
Group II	☑	☑	☑
Group III	☑	□	□

177.3 Helpdesk user configuration

Swivel version 3.9.3 onwards contains all the configuration options within one menu. On the Swivel Administration Console select Policy\Helpdesk. Options available are listed below.

Helpdesk Users can manage other repositories: Options: Yes/No, Default: No, This determines if Helpdesk users can manage other repositories.

Helpdesk can reset PINs: Options: Yes/No, Default: Yes, this option can be used to prevent the helpdesk user to setting a PIN number to a known value and they can only use the resend PIN to send the user a new PIN.

Helpdesk Users can administer editable repositories: Options: Yes/No, Default: No, this option can allow or deny the helpdesk user to manage users in a repository which Swivel can write data to.

Helpdesk can view Status page: Options: Yes/No, Default: Yes, this option can allow or deny access to the status page.

Helpdesk can view Log Viewer page: Options: Yes/No, Default: Yes, this option allows or denies access to the log viewer. The log viewer may contain troubleshooting information, but may also provide information on users in differing repositories.

Helpdesk can view reports: Options: Yes/No, Default: No, this option specifies whether or not helpdesk users are allowed to run and view reports.

Helpdesk can manage OATH tokens: Options: Yes/No, Default: Yes, this option specifies whether or not helpdesk users are allowed to allocate OATH tokens to users.

Helpdesk can edit user policy: Options: Yes/No, Default: Yes, this option specifies whether or not helpdesk users can view and alter the Policy settings for individual users in User Administration.

178 Testing

179 Known Issues

After an upgrade of Swivel from an older version the Helpdesk user may not be able to see any users until the correct permissions are set.

Swivel versions 3.9 and 3.10 had the ability to manage other Helpdesk users removed, but after popular demand, this feature was added back again in Swivel version 3.10.1. A Patch exists to add the Helpdesk rights for 3.9.6 and 3.10, see Versions FAQ.

Swivel version 3.9.7 When searching for username and logged in as a Helpdesk user, then the search may crash. May affect other versions. Upgrade to resolve.

180 Troubleshooting

Helpdesk role only allows only sees accounts that have been directly created on Swivel.

Either create helpdesk accounts in the same data source as the users (e.g. AD) or enable the Global helpdesk option, on the Swivel Administration console under Policy > Helpdesk (or Policy > General on older versions).

181 Helpdesk Operations User Guide

182 Overview

This document details the common helpdesk operations tasks related to user administration. The Helpdesk Configuration Guide contains information on setting up and configuring Helpdesk users and groups.

183 Prerequisites

Swivel 3.x

184 Helpdesk login Guide

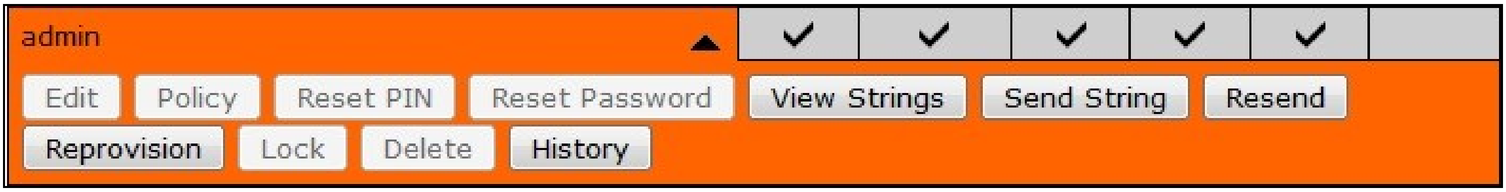
The Administration Console Login Guide details how to login to the Swivel Administration Console. Upon a successful login, the User Administration Console should be viewable, for further information see the User Administration How to guide

185 User Administration

185.1 Help Desk Users

Help Desk users have a limited access to the Swivel Administration Console. They may also have further restricted access on the User Administration Console. This restriction can be:

- Only Manage users in their own repositories or All users
- Reset PIN number to a known value not allowed
- Create local XML users not allowed
- Restrictions on Admin and other helpdesk accounts where they cannot Edit the rights of local users, reset PIN, change Password, edit the Policy, Lock account, Delete user



186 Helpdesk Operations Tasks

The following tasks are commonly carried out by helpdesk users

186.1 Check user Status

On the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), verify the user status, see User Status. If the user is not present verify that the correct repository or All Repositories has been selected and none of the filters are excluding them.

186.2 Check the Swivel log

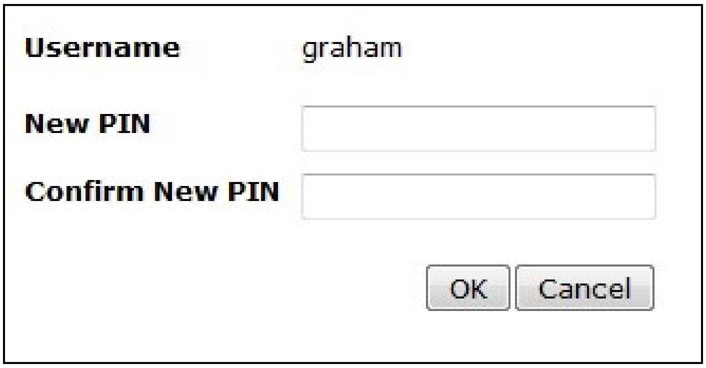
On the Swivel Administration Console, select Log Viewer, then either look for an authentication at the time the user attempted login or search on their username. Searching using time will allow detection of incorrect username.

186.3 Send User a new PIN

Resend which will send the user a new PIN by their predefined transport. To resend a new PIN, on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on Resend, verify in the Swivel log that the PIN has been sent. There is no limit to the number of times a PIN may be resent.

186.4 Reset a Users PIN

Note ResetPIN may not be available to all helpdesk users. Consider also using **Resend** which will send the user a new PIN by their predefined transport. To reset a users PIN on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on Reset PIN, enter the new PIN and again to verify it is correct. ResetPIN is not available to PINless users as they have no PIN. There is no limit to the number of times a PIN may be reset.



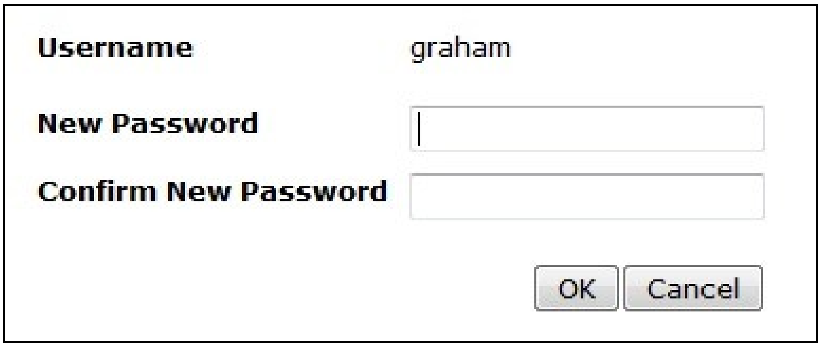
Username graham

New PIN

Confirm New PIN

186.5 Reset a Users Password

Note Reset Password may not be available to all helpdesk users. This is for setting a Swivel password for a user, it is not for changing AD passwords. To reset a users Password on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on Reset Password, enter the new Password and again to verify it is correct. If a Password has been accidentally set, then leave the password fields blank and Apply password.



Username graham

New Password

Confirm New Password

186.6 Unlock an Account

To Unlock a users account, on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on Unlock. If the account is not locked then another issue may be preventing login. An account is usually locked through failed login attempts, ensure that the user knows correctly how to login. See Also How to Unlock, and Lockout Account How to guide

186.7 Disable or Enable an Account

If the option to import disabled state is being used then it is not possible to manually set the disabled status and the Disabled entry will be greyed out. If disabled status is not being imported from the data source, it can be set from the Administration Console by selecting the user under User Administration then Policy, and entering or removing the tick next to Disabled.

186.8 Send a security String

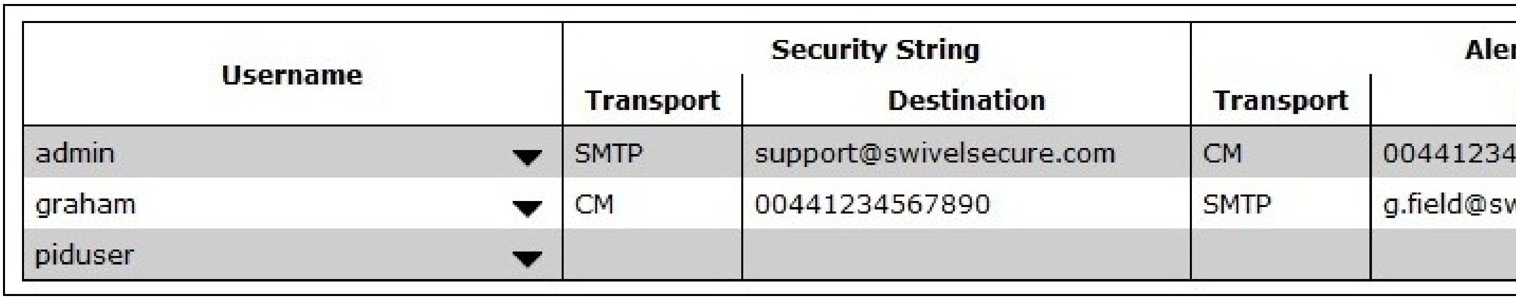
To send the user a new security string by email or SMS, on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on Resend. Check the Swivel log to ensure that the message has been sent. PINless users will not be sent security strings. There is no limit to the number of times a security string may be resent.

186.9 View a users security String

To view a users security string that they have been sent by email or SMS, on the Swivel Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on View Strings. See also View Security Strings How To Guide

186.10 View a users transport

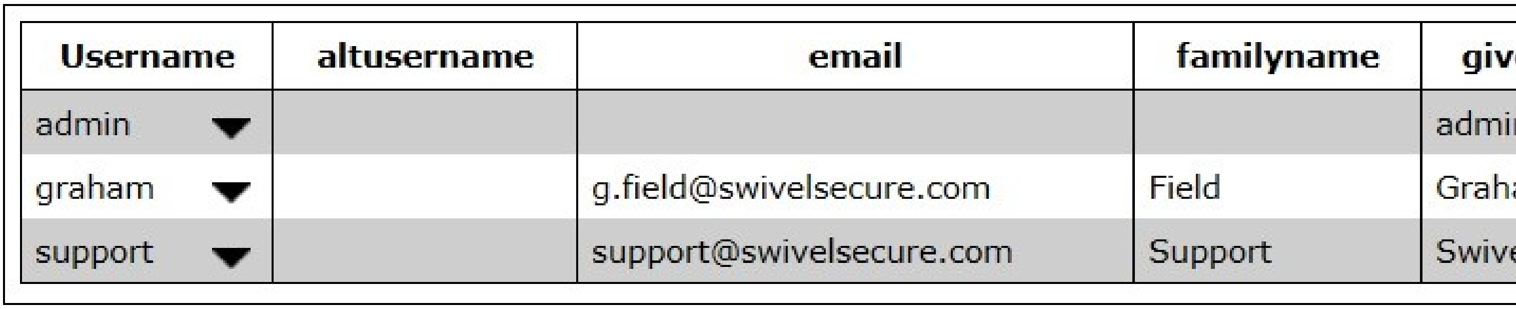
To view a user has correct transport details, on the Swivel Administration Console, select User Administration, then select View Transport. Apply any appropriate filters to see the required user. The Transports for Security Strings and Alerts should be listed. If the user is not a dual channel user, then there will be no entry under security strings.



Username	Security String		Aler	
	Transport	Destination	Transport	
admin ▼	SMTP	support@swivelsecure.com	CM	00441234
graham ▼	CM	00441234567890	SMTP	g.field@sw
piduser ▼				

186.11 Viewing User Attributes

To view a users Attributes from the User Administration page select View then Attributes.



Username	altusername	email	familyname	giv
admin ▼				admi
graham ▼		g.field@swivelsecure.com	Field	Graha
support ▼		support@swivelsecure.com	Support	Swive

186.12 Purge Deleted Users

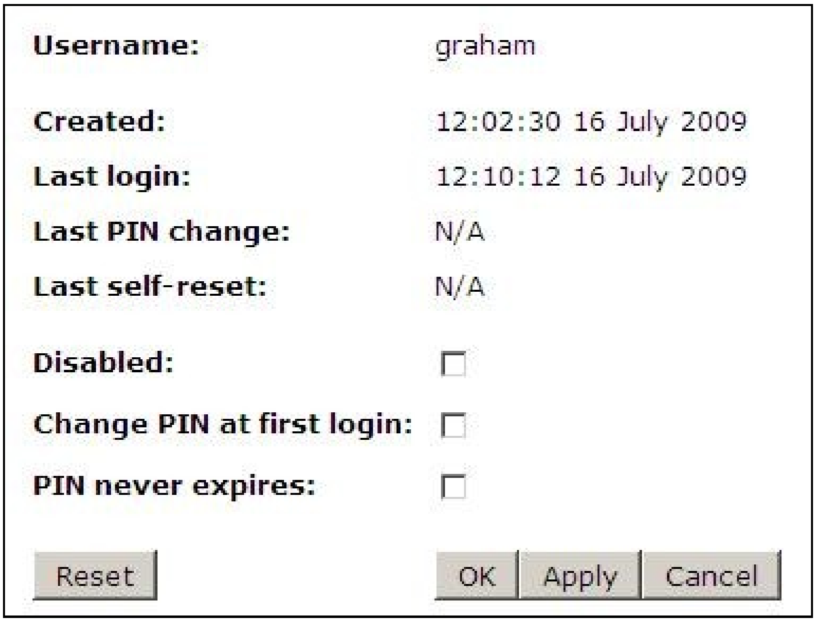
Helpdesk users may have rights to Purge users marked as deleted by clicking on the user and clicking on Purge. Bulk purge for many users can be carried out by an Admin account. See also Delete a Swivel user.

186.13 Provision a mobile Phone Client

To provision or reprovision a mobile phone client user, select the user and click on Quick Reprovision. This will send to the user an email or SMS with a Mobile Provision Code. Manual Provision will send the settings for a user if permitted to manually enter their details.

186.14 View a users last login details

You can view a users login details by selecting on the Swivel Administration console the User Administration, then the required user, click on the user, then policy.



Username: graham

Created: 12:02:30 16 July 2009

Last login: 12:10:12 16 July 2009

Last PIN change: N/A

Last self-reset: N/A

Disabled: □

Change PIN at first login: □

PIN never expires: □

187 Known Issues

In an Active/Active-DR installation, an account locked on a DR Swivel appliance will not be replicated to the Active/Active instances and must be unlocked directly on that appliance.

188 Troubleshooting User Issues

188.1 User cannot login

Has the user previously logged in successfully? Verify that the user knows how to login correctly, see PINsafe User Guide

Check status of the user. If the account is locked, try to verify why the account has been locked such as checking the logs.

Check Logs to if there are any error messages.

Was the user required to change their PIN at first login?

Reset the Password (even to a blank value if passwords are not used)

Is the login failing another authentication method on the login e.g. AD password?

If they are using SMS, Email, Mobile Phone Client, ensure that they are not generating a TURing image (Swivel will expect a TURing login in the following 2 minutes (by default))

Has the users PIN changed recently Check Logs

Can the user login with one attribute such as email but fails on another such as their SAM Account Name? verify the user attributes are correct

See also User login fails

188.2 User is not receiving their security string

Verify if the user is using single channel TURing, SMS, Email, or mobile client.

If using the Single Channel TURing image or PINpad is the image shown correctly if not see Single Channel troubleshooting.

Check Swivel Logs for the user

Verify that they have a transport configured, see View a users transport

Try to send a new security string using Send String

see also Security Strings are not being sent

If they are SMS or SMTP users ensure that they are Dual Channel users and have a tick for dual channel listed under the User Administration page for View by rights.

Has the user been added to Swivel Check user Status if not then see User is not added to Swivel

188.3 User is not added to Swivel

A Check user Status may indicate that the user has not been added to Swivel, check the following:

Is the user a member of the correct source repository, such as the correct AD group?

Has a User Synchronisation occurred? See User Synchronisation

Check Swivel Logs and look for syncronisation messages or messages that the license has been exceeded, see Installing a license key.

See also User Missing

188.4 User forgets their PIN

It may be appropriate to encourage the user to use the ResetPIN utility see ResetPIN User Guide

see Resend new PIN

188.5 User must Change their PIN

It may be appropriate to encourage the user to use the ChangePIN utility see ChangePIN User Guide, this can also be changed using the Windows GINA and Credential Provider.

188.6 Loss/Replacement of Mobile Device

The user will have to download the Swivel app to their phone, and be sent a new provision code, see Provision a mobile Phone Client To send a user a new provision code See Mobile Provision Code, it may be appropriate to encourage the user to reprovision their own mobile device, see Mobile Provision User Guide. If sending an SMS text message it may be necessary to change the mobile number if this has changed, and is usually done in the data source such as Active Directory.

see View Security Strings How To Guide

188.7 User cannot provision a Mobile Device

See Mobile Phone Client

188.8 User deletes/loses their SMS security string

If a request SMS button is present on the login page it may be appropriate to ask the user to use this.

The user may be able to fail a login (without generating a singe channel TURing image) and a new SMS should be sent if standard SMS delivery is being used

Try to send new Security String using Resend

188.9 User differences between Swivel instances

Differences between Swivel appliances can indicate that they have become out of synchronisation. This requires the assistance of an Swivel Admin to resolve in order to bring the appliances back into synchronisation, see MySQL Appliance Database Synchronisation, symptoms of this are:

- Status page shows differences in number of users and status (locked, deleted, disabled and inactive accounts).
- PIN numbers may work on one server and not another (updated on one and not another).
- User status changes are applied on other appliances (locked, deleted, disabled and inactive accounts).

188.10 Additional Symptoms

The following additional Symptoms may occur

189 High Availability on MySQL service faillure

189.1 Overview

This document outlines the steps required to configure Swivel clusters to trigger fail-over on MySQL failure.

Originally any Swivel HA cluster is configured to fail-over on Tomcat service failure; this will add MySQL service motorization to trigger fail over.

189.2 Configuration Considerations

MySQL is extremly robust. If MySQL fails, the probability of having an underlying bigger problem (that could lead to database corruption) is high.

For this reason, the configuration doesn't perfectly mimmic the Tomcat Failure setting. In truth, the Tomcat setting is set not only to fail-over to a different node when one fails, but also to look for the primary node to come up, and then shift load to it.

Due to the causes of a MySQL service faillure, this "shift back to primary node" behaviour is not set.

189.3 Swivel configuration for both nodes

1- Enter the Swivel console, and then follow to command line, using Advanced menu (option 8), and then Command line (option 6).

2- To install the correct software packages that will support the monitoring functions, run command:

rpm -ivh http://vault.centos.org/4.9/centosplus/i386/RPMS/mysqlclient14-4.1.22-1.el4s1.1.i386.rpm

3- We need to update the mysql.monitor file by running the command:

wget ?qN http://yum.swivelsecure.net/upgrades/mysql.monitor -O /usr/lib/mon/mon.d/mysql.monitor

4- Add executable permitions to the newlly updated file, by running command:

chmod +x /usr/lib/mon/mon.d/mysql.monitor

This next step can be performed directly by editing the files, or using webmin to do that form you.

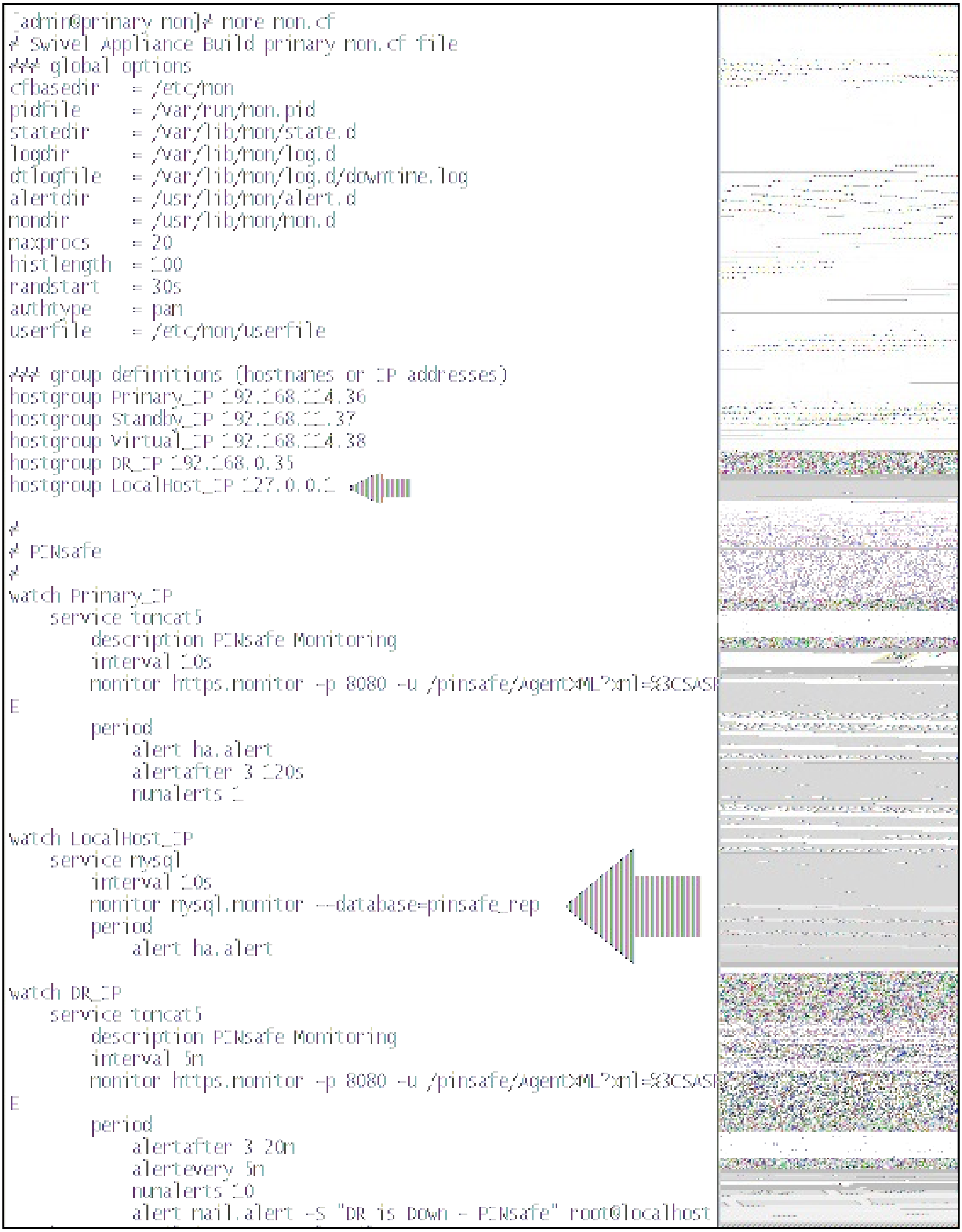
189.3.1 Option A - Command line

1- Enter the Swivel console, and then follow to command line, using Advanced menu (option 8), and then Command line (option 6).

2- Run command:

nano /etc/mon.cf

3- Add the LocalHost hostgroup, and then add the LocalHost_IP watch section exemplified bellow.



```
[admin@primary mon]# more mon.cf
# Swivel Appliance Build primary mon.cf file
### global options
cfbasedir   = /etc/mon
pidfile     = /var/run/mon.pid
statedir    = /var/lib/mon/state.d
logdir      = /var/lib/mon/log.d
dtlogfile   = /var/lib/mon/log.d/downtime.log
alertdir    = /usr/lib/mon/alert.d
mondir      = /usr/lib/mon/mon.d
maxprocs    = 20
histlength  = 100
randstart   = 30s
authtype    = pam
userfile    = /etc/mon/userfile

### group definitions (hostnames or IP addresses)
hostgroup Primary_IP 192.168.114.36
hostgroup Standby_IP 192.168.11.37
hostgroup Virtual_IP 192.168.114.38
hostgroup DR_IP 192.168.0.35
hostgroup LocalHost_IP 127.0.0.1

#
# PINsafe
#
watch Primary_IP
    service tomcat5
        description PINsafe Monitoring
        interval 10s
        monitor https.monitor -p 8080 -u /pinsafe/AgentXML?xml=%3CSASR
E
        period
            alert ha.alert
            alertafter 3 120s
            numalerts 1

watch LocalHost_IP
    service mysql
        interval 10s
        monitor mysql.monitor --database=pinsafe_rep
        period
            alert ha.alert

watch DR_IP
    service tomcat5
        description PINsafe Monitoring
        interval 5m
        monitor https.monitor -p 8080 -u /pinsafe/AgentXML?xml=%3CSASR
E
        period
            alertafter 3 20m
            alertevery 5m
            numalerts 10
            alert mail.alert -S "DR is Down - PINsafe" root@localhost
```

4- Use ctrl+o to write the changes to the file, and ctrl-x to quit nano.

5- Use the 'exit' command to quit the command line and return to the appliance menu.

6- use 0 to return to the main menu and then use command 3 to enter Monitor service control

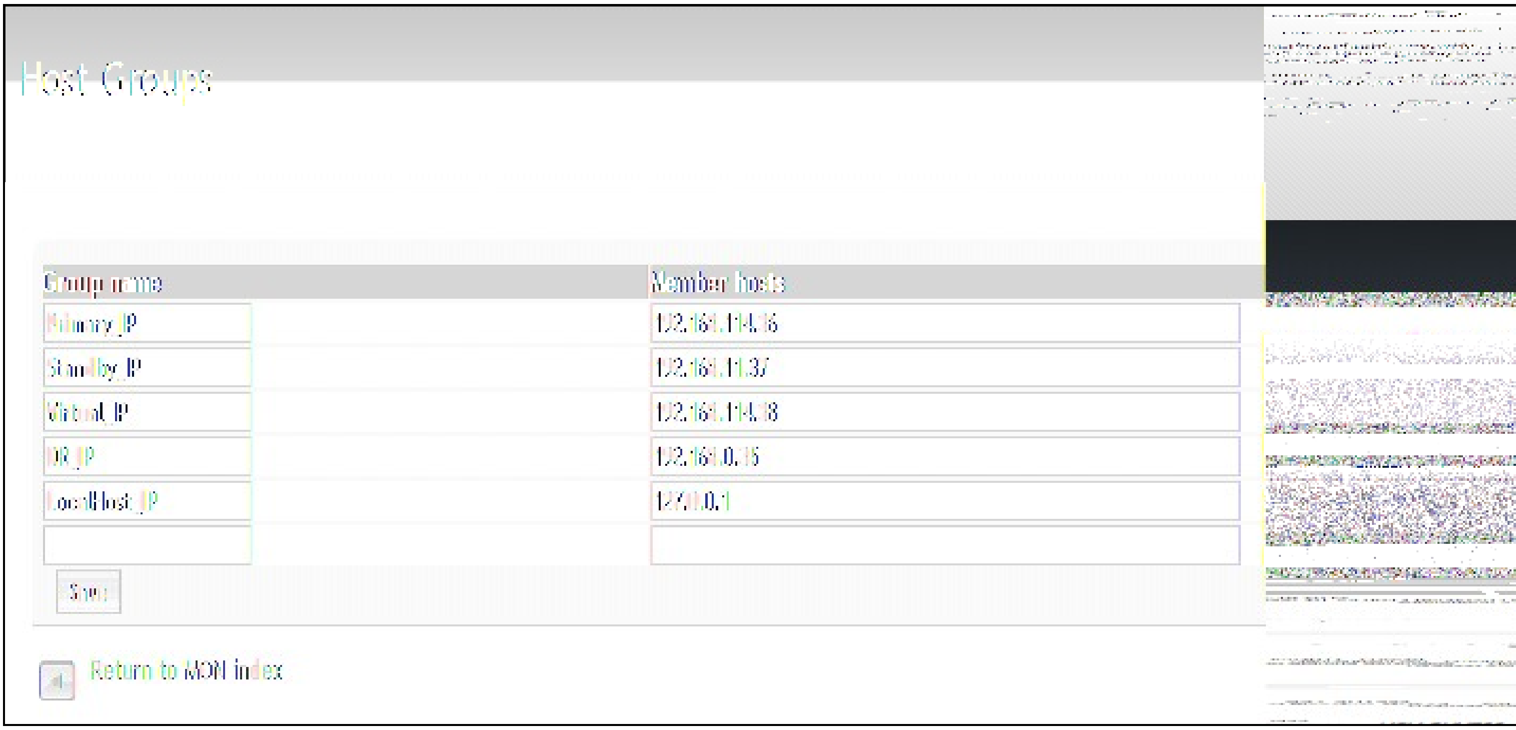
7- use 1 to stop monitor and then 1 to start it back on.

189.3.2 Option B - Webmin

1- Login to Webmin on https://serverIP:10000

2- Goto SYSTEM menu, then MON menu

3- Select Host groups icon, and then add the LocalHost_IP group to the last line, just as shown in the picture



Host Groups

Group name	Member hosts
Primary_IP	192.168.114.16
Standby_IP	192.168.11.37
Virtual_IP	192.168.114.18
DR_IP	192.168.0.15
LocalHost_IP	127.0.0.1

4- On the watchlists menu, add a new watch list for Localhost, then add a service watch and configure it to:

- Name of service: musql

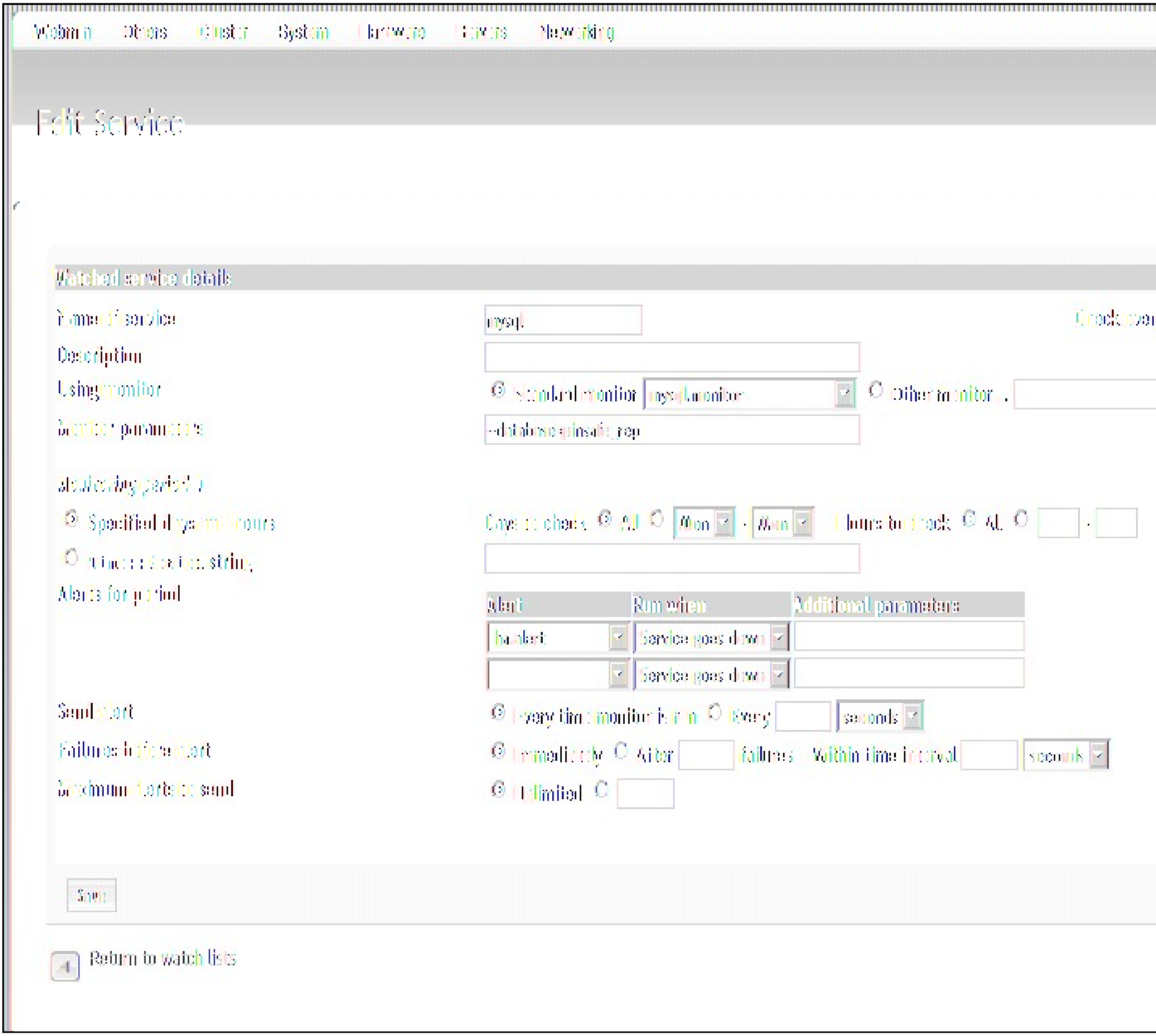
- Check every: 10 seconds

- Standard Monitor: mysql.monitor

- Monitor parameters: --database=pinsafe_rep

- Alerts for period: ha.alert on Service goes down

...according to the following image.



Edit Service

Watched service details

Name of service: mysql

Description:

Using monitor: ● Standard monitor mysql.monitor ○ Other monitor ..

Monitor parameters: -database=insafe_rep

Monitoring period

● Specified days and hours — Days to check ● All ○ Mon - Mon — Hours to check ● All ○ -

○ Time specification string

Alerts for period

Alert	Run when	Additional parameters
hpalert	Service goes down	
	Service goes down	

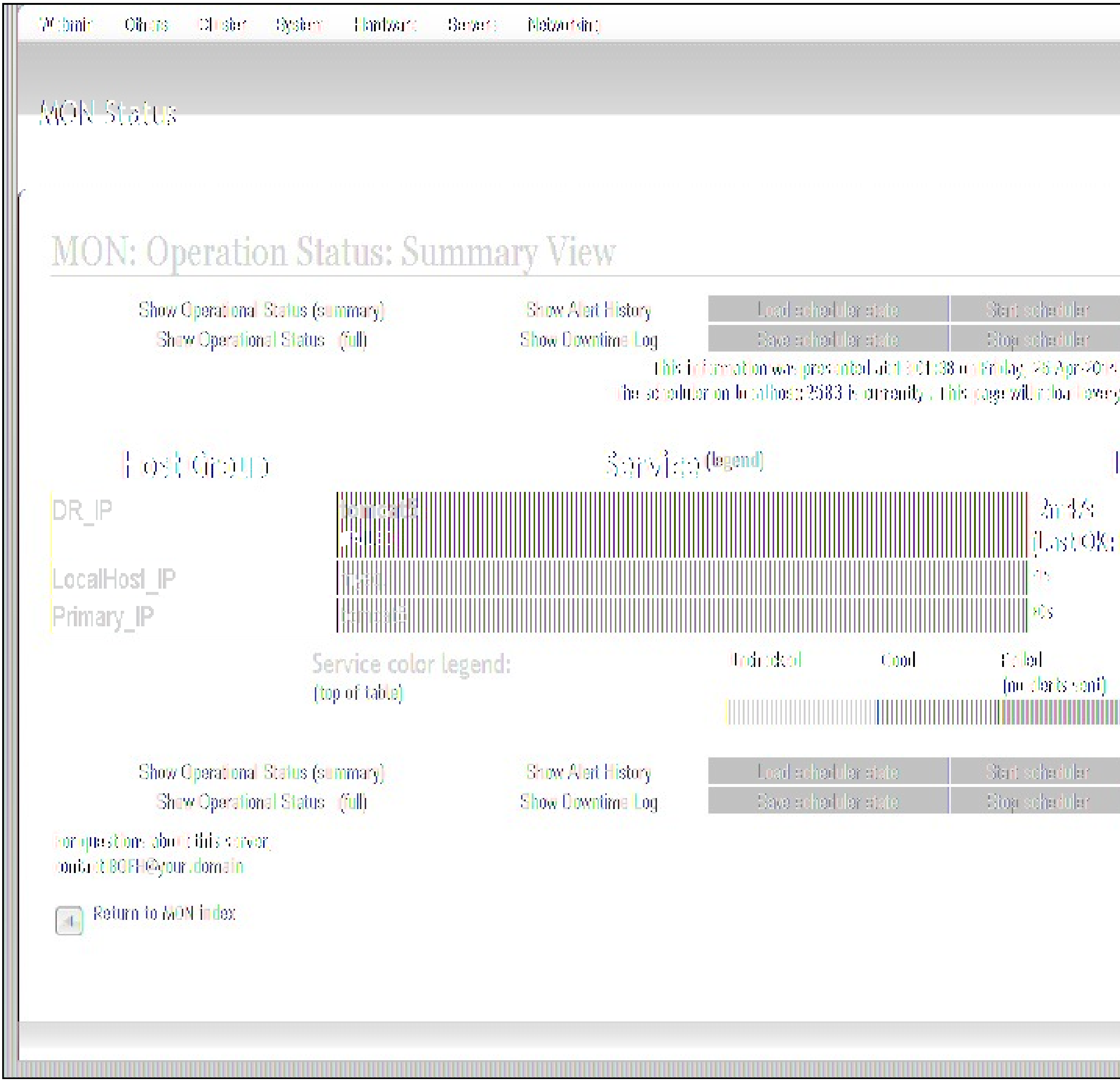
Send alert: ● Every time monitor is run ○ Every seconds

Failures before alert: ● Immediately ○ After failures Within time interval seconds

Maximum alerts to send: ● Unlimited ○

5- return to MON services and choose MON service restart

6- The final result on MON Status, should be something like this:



MON Status

MON: Operation Status: Summary View

This information was presented at 13:01:38 on Friday, 26 Apr 201

The scheduler on localhost:2583 is currently . This page will reload every

Host Group	Service (legend)	
DR_IP	tomcat6 [illegible]	2m 4s (Last OK:
LocalHost_IP	mysql	1s
Primary_IP	tomcat6	0s

Service color legend:
(top of table)

For questions about this server,
contact BOFH@your.domain

189.4 Swivel configuration to support the new HA settings

So far, we managed to setup the HA routines on Swivel secure appliance cluster to faill-over when the MySQL service stops responding.

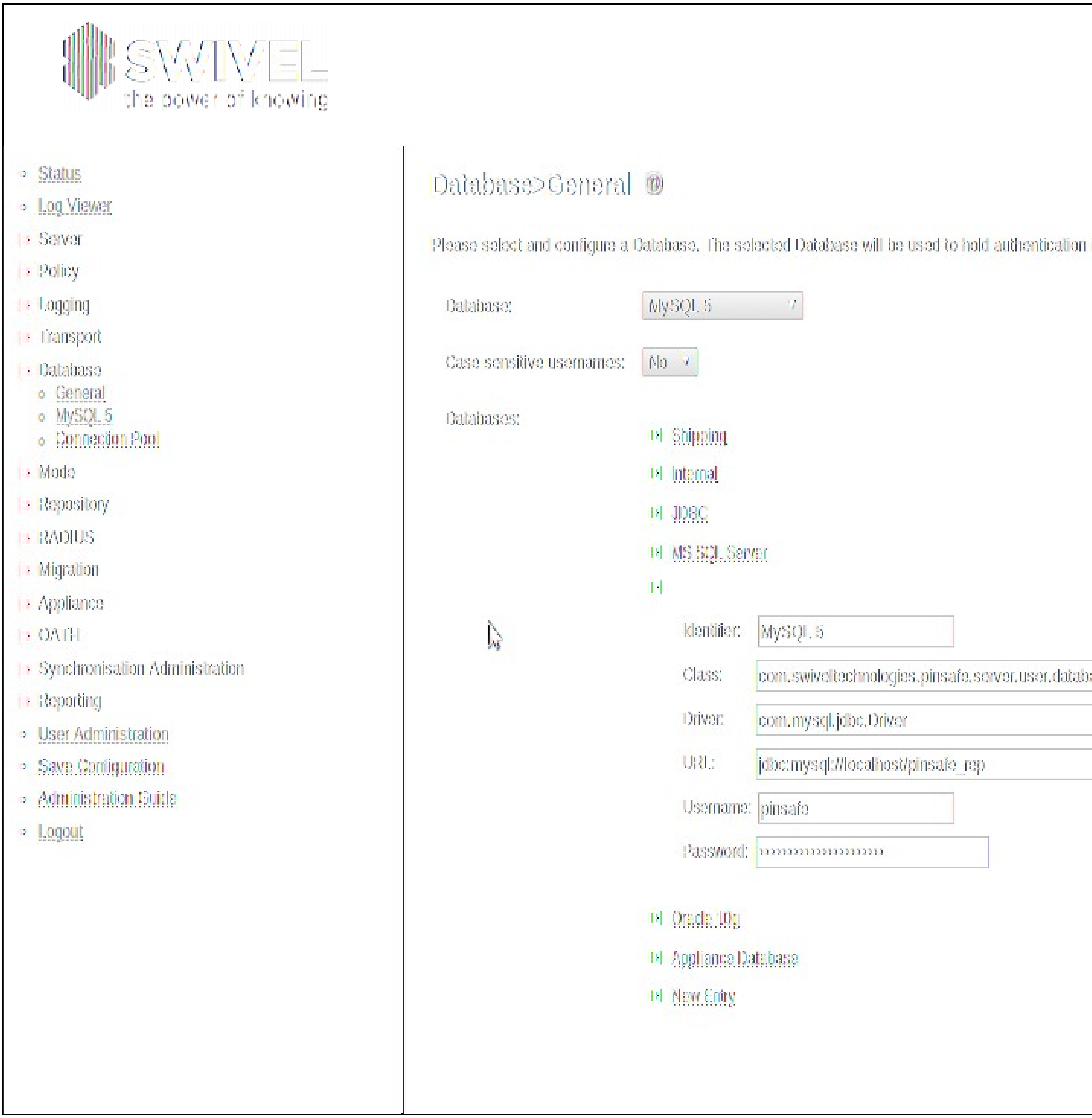
By default it is setup to do so when the Tomcat service fails, bringing the RADIUS server down with it. However, in the event of a MySQL service failure without Tomcat failure, Radius will still be functional and responding to requests. This will generate an error, because most swivel integrations support radius servers as primary and secondary RADIUS. If the RADIUS service on the down machine accepts the RADIUS request, the integrated client hardware or software will not try the secondary RADIUS. The primary RADIUS however will fire an database connectivity error due to fact that the local host mysql service is down.

To avoid that, we need to assure that both appliance nodes connect to running MySQL service, and that is the on indicated by the appliance Virtual IP.

On both nodes:

1- Enter the Swivel web console, and then navigate to Database.

2- Choose General from the menu, and then edt the MySQL5 connection, replacing Localhost by the VIP assigned to the cluster, on the MYSQL5 connector URL setting



Database>General

Please select and configure a Database. The selected Database will be used to hold authentication i

Database: MySQL 5

Case sensitive usernames: No

Databases:

Identifier: MySQL 5

Class: com.swiveltechnologies.pinsafe.server.user.databa

Driver: com.mysql.jdbc.Driver

URL: jdbc:mysql://localhost/pinsafe_rep

Username: pinsafe

Password: ••••••••••••••••••••

190 High Availability with PINsafe

191 Overview

Swivel can be made to be resilient in a number of ways. Specific appliances are used for each setup and need to be specified at time of purchase. This document looks at the differing approaches. Configuration is carried out during the Networking setup of the appliances through the CMI. See also Swivel Deployment.

192 Prerequisites

Swivel 3.x

193 Types of Swivel Appliance resilience

193.1 Standalone

This is where there is no resilience and there is a single instance of Swivel.

193.2 Active/Active

This is a pair of Swivel appliances named **Primary Master** and **Standby Master** that are able to provide authentication. They are usually deployed at a single site. Resilience is provided by MySQL clustering using database replication. Note user data is replicated, not the Swivel configuration. Additional features include:

- A Virtual IP Address to allow a floating IP address to be attached to a Swivel appliance, which in the event of failure, can move to a second Swivel appliance on the same subnet. The VIP is bound to ETH0.
- Appliance Synchronisation and formerly Session Sharing allows a Single Channel TURing image request to be made from one Swivel server and an authentication request such as using RADIUS from another Swivel server.
- RADIUS Proxy from a Swivel server by RADIUS, this can be configured to make a request when a single channel authentication is made but no image has been requested, see PINsafe RADIUS Proxy
- Replication interface: Information is usually transferred across a dedicated network interface, on hardware appliances, a cross over cable is used on ETH1, and this provides the maximum resilience since there are no network devices between the appliances that can fail. Replication traffic may also be directed to run of ETH0 instead, with the loss of some resilience capability.

193.3 DR

The DR appliances are deployed at Disaster Recovery sites. They are not intended for use as day to day authentication. Resilience is provided by MySQL, the DR acting as a MySQL slave.

193.4 Active/Passive

This refers to one of two solutions:

- An older version of the Swivel HA solution using disk replication, where only one instance of a Swivel pair is active. It is limited to two Swivel servers at one site only. This solution is being phased out by the Active/Active solution and is no longer offered for sale. To verify which appliance version you have see Appliance_General_FAQ
- Enterprise HA, where by an appliance pair is Active/Passive and a second appliance pair is Active/Passive and uses MySQL across sites.

194 Types of Third Party resilience

194.1 External Database

An external database can be used with multiple Swivel servers connecting to the Database. This database should be clustered to provide resilience in itself.

194.2 Load Balancers

Load balancers may be deployed to provide resilience.

194.3 VM resilience

Additional tools may be deployed such as VMware VMotion to bring up another Swivel instance in the event of a failure

195 Testing

196 Known Issues

197 Troubleshooting

To check the HA VIP status see VIP Status

Heartbeat will not start see Heartbeat issues

198 How to run PINsafe on non-default ports

199 Overview

Some networks allow only traffic on certain ports, and therefore it may be necessary to make requests to Swivel over ports that are accessible, such as 80 or 443. This can be done by the following methods:

- Using Port Address Translation (PAT) on the organisations firewall.
- Using Port Address Translation (PAT) on the Swivel hardware or virtual appliance.
- Changing the port on which Swivel runs (not recommended on Swivel virtual or hardware appliances).

For software installations and ports above 1024 then the port which Tomcat runs can be changed. If it is a Swivel virtual or hardware appliance or Linux install where the required port is less than 1024 then for security reasons, the section on Port Address Translation should be followed.

Where the port is changed then references to that port would need to be changed in the integrations, such as login pages.

200 Port Address Translation: Running Swivel on port 443

There may be times when it is required for Swivel to respond on port 443, the default port for https. It is not recommended to do this by editing the server.xml file as this has other implications. An alternative approach is to use the Appliance firewall to re-route inbound traffic on port 8443 to port 443. Once the port is changed all Swivel references using 8443 must be updated.

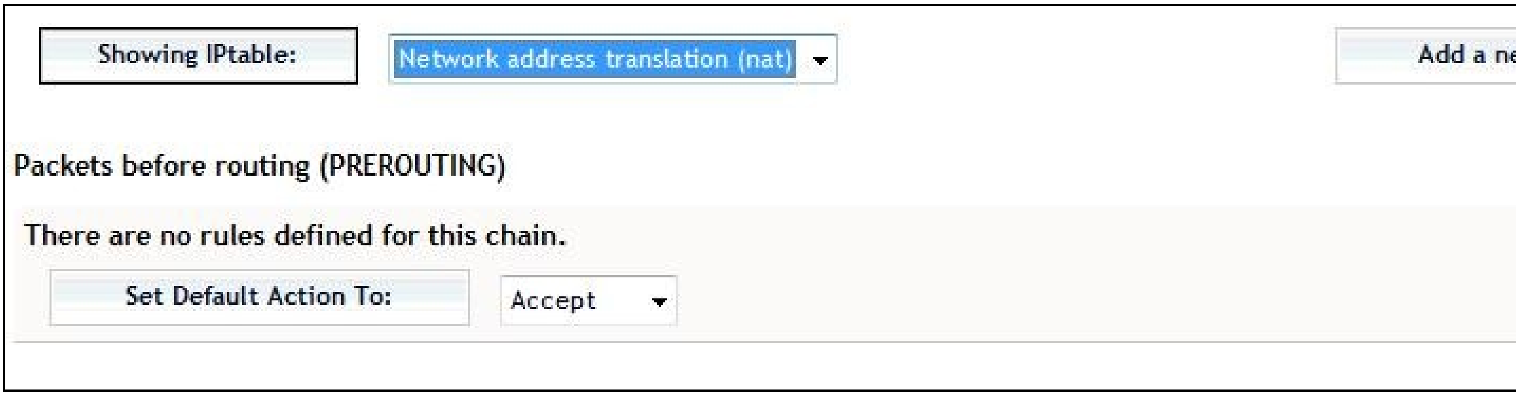
The options for this are:

- Use Port Address Translation (PAT) on the firewall device
- Use Port Address Translation (PAT) on the Swivel Appliance, as detailed below for access to the webmin see Webmin How To Guide

These are the steps required to achieve this.

Log onto the Swivel WEBMIN interface on https://<IPADDRESS>:10000

Select the Networking->Firewall option



Showing IPtable: Network address translation (nat)

Packets before routing (PREROUTING)

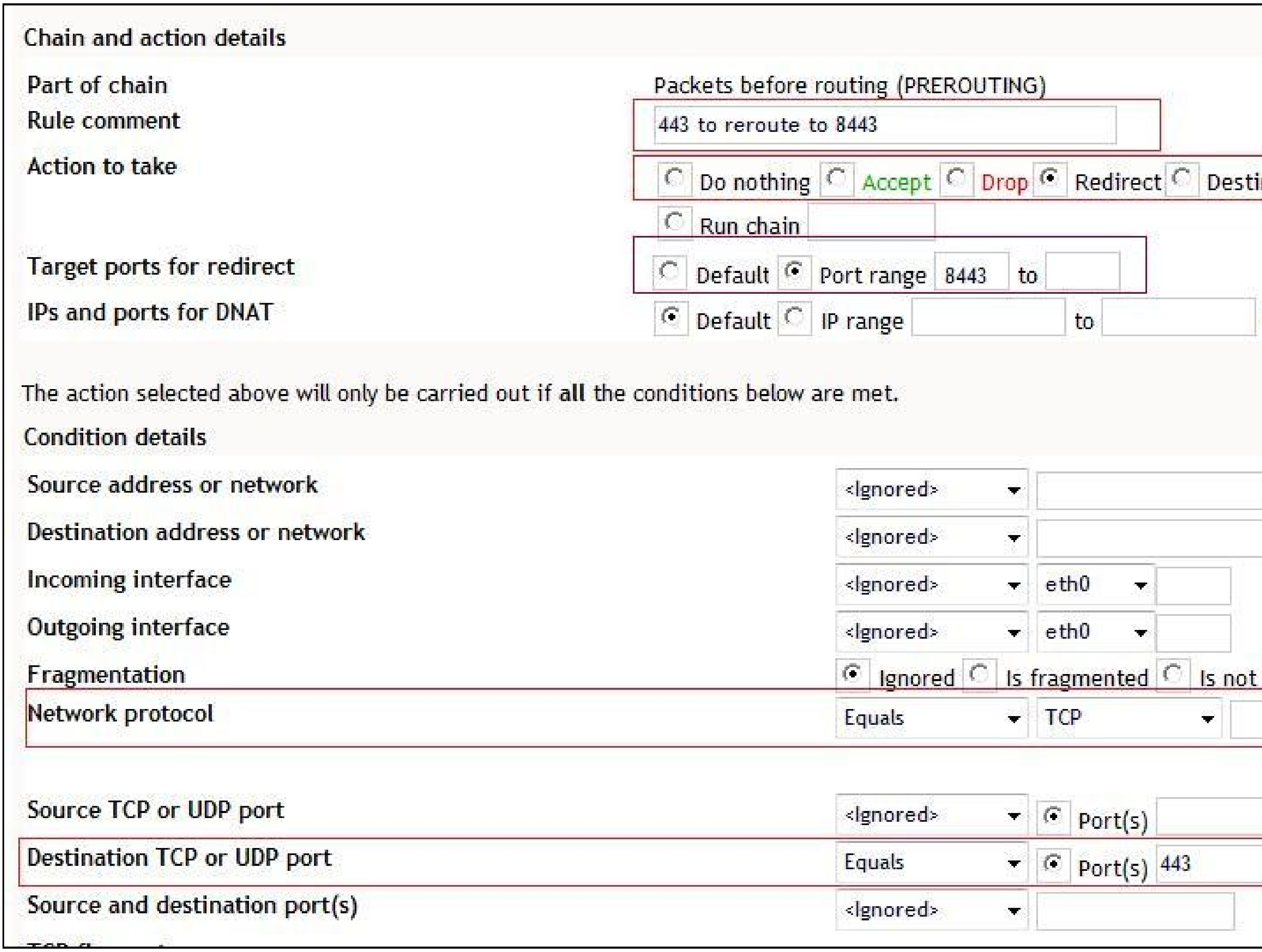
There are no rules defined for this chain.

Set Default Action To: Accept

Selecting NAT option

Then select the NAT option (as shown) and click Showing IPTable

Under the PREROUTING (top) section select **Add Rule**



Chain and action details

Part of chain	Packets before routing (PREROUTING)
Rule comment	443 to reroute to 8443
Action to take	○ Do nothing ○ Accept ○ Drop ● Redirect ○ Desti ○ Run chain
Target ports for redirect	○ Default ● Port range 8443 to
IPs and ports for DNAT	● Default ○ IP range to

The action selected above will only be carried out if **all** the conditions below are met.

Condition details

Source address or network	<Ignored>	
Destination address or network	<Ignored>	
Incoming interface	<Ignored>	eth0
Outgoing interface	<Ignored>	eth0
Fragmentation	● Ignored	○ Is fragmented ○ Is not
Network protocol	Equals	TCP
Source TCP or UDP port	<Ignored>	● Port(s)
Destination TCP or UDP port	Equals	● Port(s) 443
Source and destination port(s)	<Ignored>	

Firewall Rule required to reroute from 443 to 8443
The rule has the following elements:

A comment or name, eg 443 to reroute to 8443

Specify that it is a re-direct action required.

Target port, the port TO which traffic is to be directed, in this case 8443.

Network protocol for which the rule applies, in this case TCP

Destination port equals 443 in this case.

Once this is in place select **Create Rule**, then **Apply Configuration**

This rule means that any traffic inbound on port 443 will be redirected to port 8443 before being forwarded to Swivel.

You can test this by first retrieving a TURing image from https://<ip address>:8443/proxy/SCImage?username=test and then trying https://<ip address>:8443/proxy/SCImage?username=test, without the 8443. Both urls should produce the same result.

Remember to update authentication devices that reference the image port.

Restart networking or the firewall with

```
service iptables restart
```

The above steps create a firewall rule in the file /etc/sysconfig/iptables with the following entry:

```
 # 443 to 8443
 -A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
 COMMIT
 # Completed
```

If this is not present, ensure that the Apply Configuration button was pushed.

200.1 Swivel Firewall rules with PAT

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1311 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 61616 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
# Generated by webmin
*nat
:PREROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# Port Address Translation 443 to 8443
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
COMMIT
# Completed
```

200.2 Swivel Firewall rules with 443 and 80 PAT

```
# Firewall configuration written by system-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -i eth1 -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp --dport 5353 -d 224.0.0.251 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 631 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 694 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 1311 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1645 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1646 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1812 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m udp -p udp --dport 1813 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 3306 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8080 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 8443 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 10000 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 61616 -j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Generated by webmin
*mangle
:FORWARD ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
COMMIT
# Completed
# Generated by webmin
*nat
:PREROUTING ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
# Port Address Translation 443 to 8443
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
#80 to 8080
-A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
COMMIT
# Completed
```

201 Troubleshooting

PAT not started at boot time

Ensure that the **Apply Configuration** button has been pressed.

201.1 Known Issues

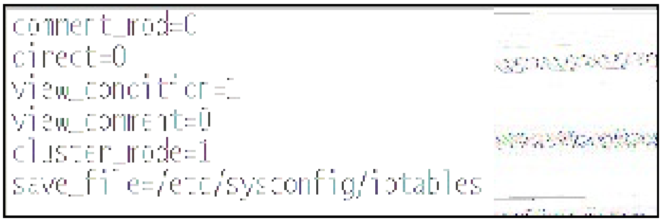
Some versions of the appliance up to 2.0.13 failed to save the firewall changes, so changes would disappear after the firewall was rebooted. To see if an appliance is affected, reboot the appliance after making configuration changes.

To overcome this issue, Ensure this fix is added then make changes to the firewall:

Edit the file /etc/webmin/firewall/config

Add the following line as in the image below. For information on how to edit files use WinSCP How To Guide or the PuTTY How To Guide

save_file=/etc/sysconfig/iptables



```
comment_mod=0
direct=0
view_condition=1
view_comment=0
cluster_mode=1
save_file=/etc/sysconfig/iptables
```

When changes are made to the webmin and applied they will be written to the file /etc/sysconfig/iptables. Once the changes are made, Webmin will recognise the new path and so no services require a restart.

202 Changing the Port on which Swivel Runs

There may be times where you wish to change the ports on which Swivel listens, for example if this clashes with another application or if particular ports are blocked by firewall policies.

Note This approach should not be used to run Swivel on Ports lower than 1024. eg port 443, as this has security implications, for example this would mean that Tomcat would have to be run as root on a linux system. The next section detailing Port Address Translation and firewall rewriting, provides a way of achieving the same result in a different way. For ports above 1024 the below method can be used.

To change the ports used by Swivel you need to edit the apache-tomcat/conf/server.xml file

In this file there will be definitions of connectors which specify the port to be used

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />
```

Therefore to change Swivel to run on port 8181, this would be changed to

```
<Connector port="8181" protocol="HTTP/1.1" connectionTimeout="20000" redirectPort="8443" />
```

Tomcat would then need to be restarted.

A Swivel appliance will have three connectors defined.

```
   <Connector address="localhost" port="8181" />
   <Connector address="0.0.0.0" port="8080" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.key
   <Engine name="Catalina" defaultHost="localhost">
     <Host name="localhost" appBase="webapps" />
   </Engine>
 </Service>

 <Service name="Catalina-proxy">
   <Connector address="0.0.0.0" port="8443" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="/home/swivel/.key
```

There is no need to change port 8181 as this is only used internally Port 8080 serves the admin console and port 8443 is used to the external interface, eg to supply the TURing image.

203 How to Template

204 Overview

205 Prerequisites

206 How to Guide

207 Testing

208 Known Issues

209 Troubleshooting

210 Import

211 Overview

This document described the User Administration function to import users from a CSV file into Swivel.

212 Prerequisites

Swivel 3.9 onwards

CSV file

213 Import users

213.1 Import Process

Check the file contents

Zip the file if necessary

On the Swivel Administration console select User Administration

Select the Repository that the users should be imported into, this will be an XML repository, LDAP Writeable or ADAM

An Import button should be available, then click Import.

Select the required import options, with the required file location then click Import

Click on User Sync to import the users from the repository

213.2 Import options

Groups: default None, a list of Swivel groups into which the users will be imported, or import groups from file.

File Type: default None, options: CSV XML

File to Import: Browse to import file

File is zipped Tick if the file is zipped. For users greater than 100, a zip file should be used to import the users.

Delete imported users Tick to select, this will delete the users from the source.

213.3 Importing a PIN number

It is recommended that Swivel generate a random PIN number that is sent to the user on account creation. However it is possible to import a PIN number for a user as detailed below:

Under Repository -> Attributes, create a new attribute in the empty space at the bottom, called "pin". You need only enter a name for this attribute for the repository you are trying to import into. If this is an XML repository, the attribute name should be "pin". If it is an ADAM or LDAP repository, use the attribute name set as initial PIN attribute.

Next, you need to add "pin" (or the appropriate attribute name) as the header field for the appropriate CSV column, and enter the initial PINs for the imported users.

Import the users from CSV. Note that this only imports the users into the repository. You need to run User Sync in order to import the users into the database. The PINs should be imported as well.

213.4 CSV File format

The CSV file should have as its first line the field names to be imported, then the data, with one line per entry, fields separated by a comma.

Examples:

```
Username,username,first-name,last-name,email,disabled,phone
psampr,psampr,Pete,Sampras,user1@email.com,FALSE,12345678
aagass,aagass,Andre,Agassi,user2@email.com,FALSE,12345678
rnadal,rnadal,Rafael,Nadal,user3@email.com,FALSE,12345678
```

```
Username,username,first-name,last-name,email,disabled,phone,group_1,group_2
user1,user1,Pete,Sampras,user1@email.com,FALSE,12345678,group-1,group-2
user2,user2,Andre,Agassi,user2@email.com,FALSE,12345678,group-1,group-2
user3,user3,Rafael,Nadal,user3@email.com,FALSE,12345678,group-1,group-2
```

The attributes in the header should be named as in the target repository, rather than the Sentry attribute names. For XML repositories, these are as follows:

- username
- first-name
- last-name
- email
- phone
- password
- pin
- custom
- custom2
- custom3
- custom4
- custom5

If groups are imported, rather than specified as fixed, use the convention shown in the second example of listing "group_" followed by an index in the header.

Note that username is shown twice in these examples: once as "Username" and once as "username". This is a workaround for an issue recently discovered, which is caused by having a custom attribute named "username". This hides the real Username field from the import, so you get the error "Username not given in header". Once this issue has been resolved, this article will be updated to reflect the resolution.

214 Testing

215 Known Issues

215.1 Importing existing users

If you try to import users with the same name as existing users, you get an error and the import fails. So to carry out the import again, you will need to delete all the users that you imported previously first.

215.2 Importing PIN as an attribute

If PIN has been added as a user attribute, it is displayed in the user administration page, if you view attributes. In the case of XML only, if you carry out a second user sync, the PIN attribute appears empty. However, the user's PIN is not removed.

216 Troubleshooting

217 Importing users from External Sources

217.1 Overview

How to Import users From an external data source into Swivel.

217.2 Prerequisites

Swivel 3.x initially configured with an internal data source and store see How to initially configure PINsafe

External Data source (AD, ADAM, LDAP, SQL)

217.3 Configuration

Create an external data source repository by selecting in the Swivel Administration Console Repository, then Servers. Enter a unique name for the repository Name, and then select Repository Type from the drop down menu, selecting Active or Simple LDAP. Click Apply, and a new data source will appear with the unique name given to it. One XML data source may be created, but multiple AD, LDAP or other data sources may be created.

Select the new data source from under Repository and configure the required parameters.

For more information on configuring the Data Sources see the following sections:

AD data source configuration

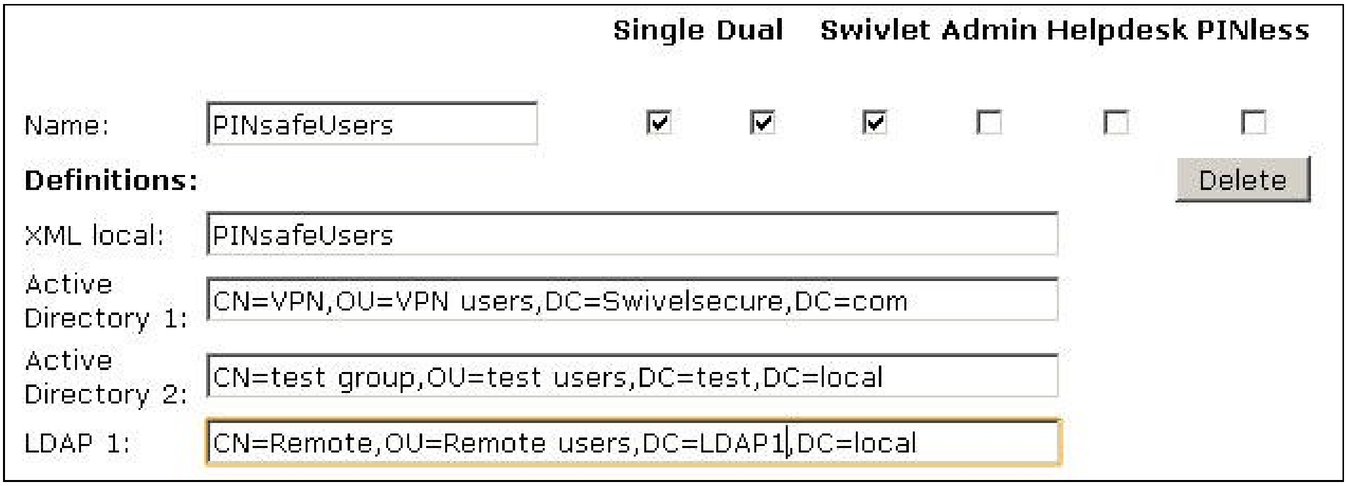
LDAP How to Guide

SQL as a data source How To Guide

The next step is to ensure that the transport groups have been set up so that users recive security strings and other information such as PIN numbers.

Configure the Transport Attribute and the settings in Transport Configuration

The next step is to tell Swivel what permissions which groups of users on the Data Source have. On the Swivel administration console select Repository/Groups. The group name is listed at the top, and below this are listed the data sources, defined by their unique names given above. Enter the LDAP path name to a group of users, this needs to be a group/Container and cannot directly be an OU.



		Single	Dual	Swivlet	Admin	Helpdesk	PINless
Name:	PINsafeUsers	☑	☑	☑	□	□	□

Definitions: Delete

XML local: PINsafeUsers

Active Directory 1: CN=VPN,OU=VPN users,DC=Swivelsecure,DC=com

Active Directory 2: CN=test group,OU=test users,DC=test,DC=local

LDAP 1: CN=Remote,OU=Remote users,DC=LDAP1,DC=local

Hint: for Swivel 3.6 or later, use the built in LDAP browser, for earler versions, use a LDAP browser.

The next step is to import users into the Swivel store. From the Swivel Administration console select the User Administration and then the required data source, and click on User Sync. This will occur automatic if a periodic synchronisation has been configured for that data source (recommended). Users will appear in the Swivel User Administration page. If no users appear, then check the system logs.

Typical issues with user import include:

Incorrect LDAP pathname

Incorrect username

Network connectivity (firewalls, IP configuration)

AD User has not replicated

218 Inactive Account Expiry

See Swivel Account Inactive

219 Initial Password How to Guide

219.1 Overview

This document outlines how to configure an Initial Password from a data source for a new user in PINsafe

Note: Configuring a default value for a Password may be a security risk and is **NOT RECOMMENDED** unless each default Password is unique and cannot be read by other users. It is recommended to use the randomly generated Password.

For further information on using Passwords with PINsafe see: Password How to Guide

219.2 Prerequisites

PINsafe

Password number in Data Source repository

219.3 Creating an Initial Password

219.3.1 Configure the Default Password Attribute on the data Source

1. On the Data Source locate a suitable attribute for the initial Password. For Active Directory this can be a new or existing LDAP attribute.

2. Populate the attribute for each user with the default Password value.

219.3.2 Configure the default Password attribute on PINsafe

1. On the PINsafe Administration console select Repository then the repository name.

2. Enter the Repository Data Source **Password attribute:**, this is an LDAP attribute for that user configured above.

3. Wait for an automatic synchronisation of the data source or select under User Administration the repository and click on Sync Now.

219.4 Testing

Test authentication using the Password.

219.5 Known Issues

219.6 Troubleshooting

220 Initial PIN How to Guide

220.1 Overview

This document outlines how to configure an Initial PIN for a new user in Swivel. Existing users are not affected if an Initial PIN is set.

Note: Configuring a default value for a PIN may be a security risk and is **NOT RECOMMENDED** unless each default PIN is unique and cannot be read by other users. It is recommended to use the randomly generated PIN.

220.2 Prerequisites

Swivel

PIN number in Data Source repository

220.3 Creating an Initial PIN

220.3.1 Configure the Default PIN Attribute on the data Source

1. On the Data Source locate a suitable attribute for the initial PIN number. For Active Directory this can be a new or existing LDAP attribute.

2. Populate the attribute for each user with the default PIN value.

220.3.2 Configure the default PIN attribute on PINsafe

1. On the Swivel Administration console select Repository then the repository name.

2. Enter the Repository Data Source **PIN attribute:**, this is the name of an LDAP attribute for that user configured above.

3. Wait for an automatic synchronisation of the data source or select under User Administration the repository and click on Sync Now.

220.3.2.1 Setting a Default PIN Directly

It is possible to set the same initial PIN for all users. This is not recommended for security reasons, but if you want to do this, rather than entering the name of an attribute, enter a "#" followed by the actual PIN you want to use for all new users.

Note that this does not affect existing users, only users created after this value is set.

220.4 Testing

Test authentication using the PIN.

220.5 Known Issues

220.6 Troubleshooting

221 Key and Certificate Generation

222 Overview

Communication between the Application and the IDP is encrypted using a certificate, this document outlines how to create keys and a certificate on a Swivel hardware or Virtual Appliance.

223 Prerequisites

Swivel IDP

Swivel hardware or Virtual appliance 2.x

224 Create private keys and certificates

Communication between the SAML application and the Swivel instance is secure through the use of certificates.

224.1 Creating DSA Private Key

DSA key generation involves two steps, and can be done through the command line on a Swivel virtual or hardware appliance, usually accessed through the CMI. Change directory to the key location, this can usually be found from the settings file.

Swivel Authentication Manager: keys/pinsafe/ssl

Backp the existing keys and certificates to a new location, then run the following commands:

1.

```
openssl dsaparam -out dsaparam.pem 2048
```

2.

```
openssl gendsa -out dsaprivkey.pem dsaparam.pem
```

The first step creates a DSA parameter file, dsaparam.pem, which in this case instructs OpenSSL to create a 2048-bit key in Step 2. The dsaparam.pem file is not itself a key, and can be discarded after the public and private keys are created. The second step actually creates the private key in the file dsaprivkey.pem which should be kept secret.

Export the key into a DER (binary) format. You can do so with the following steps:

1.

```
openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
```

2.

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
```

Step 1 extracts the public key into a DER format. Step 2 converts the private key into the pkcs8 and DER format. Once you've done this, you can use this public (dsapubkey.der) and private (dsaprivkey.der) key pair.

224.2 Creating a Certificate

Once you have your key pair, it's easy to create an X.509 certificate. The certificate holds the corresponding public key, along with some metadata relating to the organization that created the certificate. Follow this step to create a self-signed certificate from either an RSA or DSA private key:

```
openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
```

After you answer a number of questions, the certificate will be created and saved as dsacert.pem.

The created keys, dsapubkey.der and dsapubkey.der need to be copied to the keys folder or wherever specified within settings.xml

The **dsacert.pem** certificate needs to be uploaded to the Application server, using a program such as WinSCP, see the WinSCP How To Guide.

225 Example output

```
[admin@pinsafe-wby-01 ssl]# openssl dsaparam -out dsaparam.pem 2048
Generating DSA parameters, 2048 bit long prime
This could take some time
..............+.......+...................+...+..+++++++++++++++++++++++++++++++++++++++++++++++++++*.................+.+.+........+.+......
[admin@pinsafe-wby-01 ssl]# openssl gendsa -out dsaprivkey.pem dsaparam.pem
Generating DSA key, 2048 bits
[admin@pinsafe-wby-01 ssl]# openssl dsa -in dsaprivkey.pem -outform DER -pubout -out dsapubkey.der
read DSA key
writing DSA key
[admin@pinsafe-wby-01 ssl]# openssl pkcs8 -topk8 -inform PEM -outform DER -in dsaprivkey.pem -out dsaprivkey.der -nocrypt
[admin@pinsafe-wby-01 ssl]# openssl req -new -x509 -key dsaprivkey.pem -out dsacert.pem
You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:GB
State or Province Name (full name) [Berkshire]:West Yorkshire
Locality Name (eg, city) [Newbury]:Wetherby
Organization Name (eg, company) [My Company Ltd]:Swivel Secure Ltd
Organizational Unit Name (eg, section) []:Dev
Common Name (eg, your name or your server's hostname) []:pinsafe-wby-01
Email Address []:
[admin@pinsafe-wby-01 ssl]# ls -la
total 32
drwxrwxr-x  3 swivel swivel 4096 Aug 28 14:52 .
drwxrwxr-x  3 swivel swivel 4096 Aug 28 14:35 ..
-rw-r--r--  1 root   root   1980 Aug 28 14:52 dsacert.pem
-rw-r--r--  1 root   root    804 Aug 28 14:50 dsaparam.pem
-rw-r--r--  1 root   root    592 Aug 28 14:50 dsaprivkey.der
-rw-r--r--  1 root   root   1192 Aug 28 14:50 dsaprivkey.pem
-rw-r--r--  1 root   root    830 Aug 28 14:50 dsapubkey.der
drwxr-xr-x  2 root   root   4096 Aug 28 14:49 orig
```

226 Testing

227 Known Issues

228 Troubleshooting

229 Language customization

230 Overview

The Swivel Administration console can be configured to different languages and text. However the language files will need to be backed up and reapplied after an upgrade on each Swivel instance, although new features and changes may be displayed in English.. If the language files are supplied to Swivel, it may be possible to incorporate them within the Swivel build although new features and changes may be displayed in English.

See also Administration console customization.

231 Prerequisites

Swivel 3.x

232 How to create new language files

The language files are stored in <path to Tomcat>/pinsafe/WEB-INF/languages

Appliance: /usr/local/tomcat/pinsafe/WEB-INF/languages

Create copies of console.en.xml and errors.en.xml changing en for the required language abbreviation.

Example: console.jp.xml and errors.jp.xml.

233 Edit the language files

Edit these two files and replace the appropriate text in <PhraseContent>TEXT</PhraseContent>

However, it will probably be necessary to convert characters to UTF-8 encoding.

234 Setting the language file

On the Swivel Administration console change the language under Server/Language to the required language abbreviation used above. Click Apply and the language file should be applied immediately.

Example: jp

235 Testing

View the Swivel Administration console for new changes.

236 Known Issues

237 Troubleshooting

238 LDAP How to Guide

239 Overview

This document covers the use of LDAP with Swivel to read information from Active Directory and LDAP servers.

Swivel has a specific class for Active Directory imports, for further information see AD data source configuration

240 Prerequisites

Swivel 3.x

LDAP 3 compatible server

241 Creating the LDAP Repository

241.1 Add the LDAP Repository Servers

On the Swivel Server:

Select Repository/General and create an LDAP Repository, the name is descriptive and must be unique and up to 32 characters in length, and when created it should appear on the left hand side below Repository. Create additional Swivel servers for each LDAP server.

Click Apply to save settings

For information on creating custom synchronisation schedules see Schedule.

242 LDAP Repository Configuration

The following LDAP options can be configured.

Administrator: Administrative account username

Password: Administrative account password

Server: LDAP server Hostname/IP

Port: 389 LDAP, 636 LDAP SSL, 3268 Global Catalog, 3269 Global Catalog SSL

Base DN: If you set a base DN, user DNs will be relative to that. (specifying the base DN as part of the admin user name will result in the base DN being used twice). Whether Base DN needs to be specified varies on the implementation. Typically, you don't need to specify a base DN at all - Swivel will work it out for itself, sometimes the base DN needs to be specified.

Use SSL: The Swivel server or appliance can be configured to accept self signed certs by selecting the Accept self-signed certificates, located under the Repository/Name of LDAP server entry

Synchronization schedule: How often to synchronise with the LDAP server. A typical value is once per hour

Username attribute: The LDAP attribute to use as the primary key for user

Mark missing users as deleted: If set to Yes, when a user is removed from the LDAP group, then mark the user for deletion requiring a Purge. If set to No then the user will be deleted from Swivel.

Initial PIN attribute: An LDAP attribute that can containa PIN value to be read from the LDAP source.

Initial password attribute: An LDAP attribute that can containa password value to be read from the LDAP source. Be aware that this is a Swivel password, not a repository password. Setting a Swivel password is an additional security feature, but not all of our integrations support it: many assume the Swivel password is empty, and rely on the target system having its own password.

Import disabled users: If set to Yes then the disabled users will be imported. If set to No then disabled users will not be imported. It will not affect existing users but only applies to initial user import.

Import disabled state: Enable/disable the importing of users' disabled state from the user repository. When enabled the user repository will be consulted as to whether or not an account is disabled. Currently, Active Directory supports this functionality. Simple LDAP will support it if the name of the disabled attribute is entered in the appropriate settings. When enabled, it will no longer be possible to manually set the disabled state of the user within the Swivel administration interface. If Import disabled users is set to No, then this option has no effect, as disabled users will not be imported at all.

Base Search Context: The base DN used when searching the repository. This can normally be left blank unless you have difficulty synchronizing the repository.

Group ObjectClass Name: The objectClass attribute value to be used for groups. Only groups with this object class will be searched when synchronizing. For writeable LDAP repository, this is the objectClass that will be used when creating new groups. It must therefore be a valid LDAP objectClass. Required parent classes will automatically be added.

User ObjectClass Name: The objectClass attribute value to be used for users. The same comments apply as for Group ObjectClass

Member attribute name: The attribute used when locating or setting group membership for a user.

Member group attribute name: The attribute used when locating group membership for a sub-group. Typically, this need not be set, as it is the same as for users, but some LDAP implementations use a different attribute.

Ignore FQ name changes: Ignore changes in the FQ name for the users

User disabled flag name: The attribute used to indicate that a user account is disabled. This is an optional attribute: if empty, all users are treated as enabled. Values must be of boolean type.

User enabled flag name: The attribute used to indicate that a user account is enabled. This has the same use as the User disabled flag name, but with opposite logic: true indicates that the account is enabled, rather than disabled.

Reformat Phone Number: If this option is set to Yes, then any phone number imported from the repository is reformatted by removing all non-digits (including spaces), and removing or adding a prefix, according to the following two options.

Prefix to remove: If Reformat Phone Number is enabled and this option is not empty, then the first occurrence of the specified prefix is removed.

Prefix to add: If Reformat Phone Number is enabled and this option is not empty, then the value of this option is added to the beginning of the number. A typical example of usage for phone number reformatting, in the UK, would be to set Prefix to remove to "0" and Prefix to add to "+44". This will ensure that phone numbers imported as, for example, "01937 582 020" will be stored in Swivel as "+441937582020"

Add domain qualifier: This option and the next allow you to add a fixed prefix or suffix to all usernames in this repository. This option specifies whether it should be a prefix, a suffix or neither. The prefix or suffix can be used to ensure uniqueness where there is a danger of having the same username in multiple repositories. It can also be used to ensure that the format of the username is correct for the target authentication platform. Be aware that if a prefix or suffix is used, users must always use them when authenticating to Swivel.

Repository Domain Qualifier: This option allows you to specify what prefix or suffix should be added to users in this repository, as described in the previous option. If you use this option, make sure that any separator characters are included. For example, if usernames should be in the form domain\username, the prefix should be domain\.

242.1 Installing trusted CA certificates for LDAPS

Certificates for LDAPS can be added to the Swivel appliance or server using the keytool command to import the cert as a trusted CA cert. The location of the trusted certificates can be found under:

/usr/java/<java_version>/lib/security/cacerts

<java_version> depends on the version of Java you are using. To find this out, look under Version Information from the CMI. Locate JVM Version, but ignore anything following the last "-", so for example, if JVM version is 1.8.0_372-b07, replace <java_version> with 1.8.0_372.

242.2 Check Password With Repository

Agents and RADIUS NAS entries have the options to Check password with Repository. This requires that the LDAP servers supports an LDAP **simple bind authentication**.

243 Testing

244 Known Issues

User Sync Issues

Swivel 3.8 release 2 onwards, any error retrieving user details will skip over that user, but mark it as deleted (or actually delete the user, if mark as deleted is disabled).

Swivel 3.5 to 3.8 first release, if an error occurs trying to read a specific user?s details, it will only skip that particular user if the error is ?Not found?. Any other LDAP error will cause it to abort.

Group Sync Issues

Swivel 3.5 and later, Errors attempting to access LDAP or to read the group details will cause the user sync to abort. In earlier versions of PINsafe, such errors could cause all users to be deleted.

User Import Issues

Swivel version 3.8 (release 1) and earlier, usernames must be EXACTLY the same on both servers, including case. If the username is changed on the source, it may invalidate user credentials. Do not change the username case on the LDAP server (such as changing the uid attribute to or from upper case and lower case, as it will try to import the user as a new user, but fails as the user already exists.

There are two ways to fix this: either change the LDAP repository to have upper case (or lower case) usernames, or modify the PINsafe database to change usernames to lower case. The SQL statement to do this is as follows: UPDATE PINSAFEJ SET H = LOWER(H);

Moving LDAP servers Issues

The usernames must be exactly the same on each server. With PINsafe 3.8 release 1 and earlier the base DN on the two servers must be the same. The PINsafe user sync can handle situations where a user has been moved within the same LDAP directory (basically, the repository returns a "not found" error). However, if the base DN is different, an "authentication failed" error is produced which causes PINsafe to abort the user sync.

If the base DN is the same and usernames are the same, moving to a different repository with the same users is possible. Delete the current data source repository definition, making sure that "Delete users with repository" is set to "No", and then create a new repository with EXACTLY the same name (including case and spacing).

Base DN cannot be deleted

If the Base DN cannot be deleted it may be necessary to delete the LDAP repository and recreate it. This is resolved in Swivel 3.9.4.

245 Troubleshooting

Try with the base DN blank and try that first.

Usually you will require the username attribute, member attribute, user objectclass and group objectclass.

246 Licence key

246.1 Swivel Licence Keys

Since Version 3.11 the Swivel Licence keys work in a difference way. They differ from previous licence keys in the following ways.

- The licence is issued to a specfic installation and therefore cannot be transferred from one server/installation to another
- The licence key is used to contact the Swivel Licence Key server to download details of the entitlements the customer has purcahsed. This means when a customer wants to upgrade or renew their licence, they do not need to enter a new licence key, merely refresh the licence key they are given. See License Key Update.

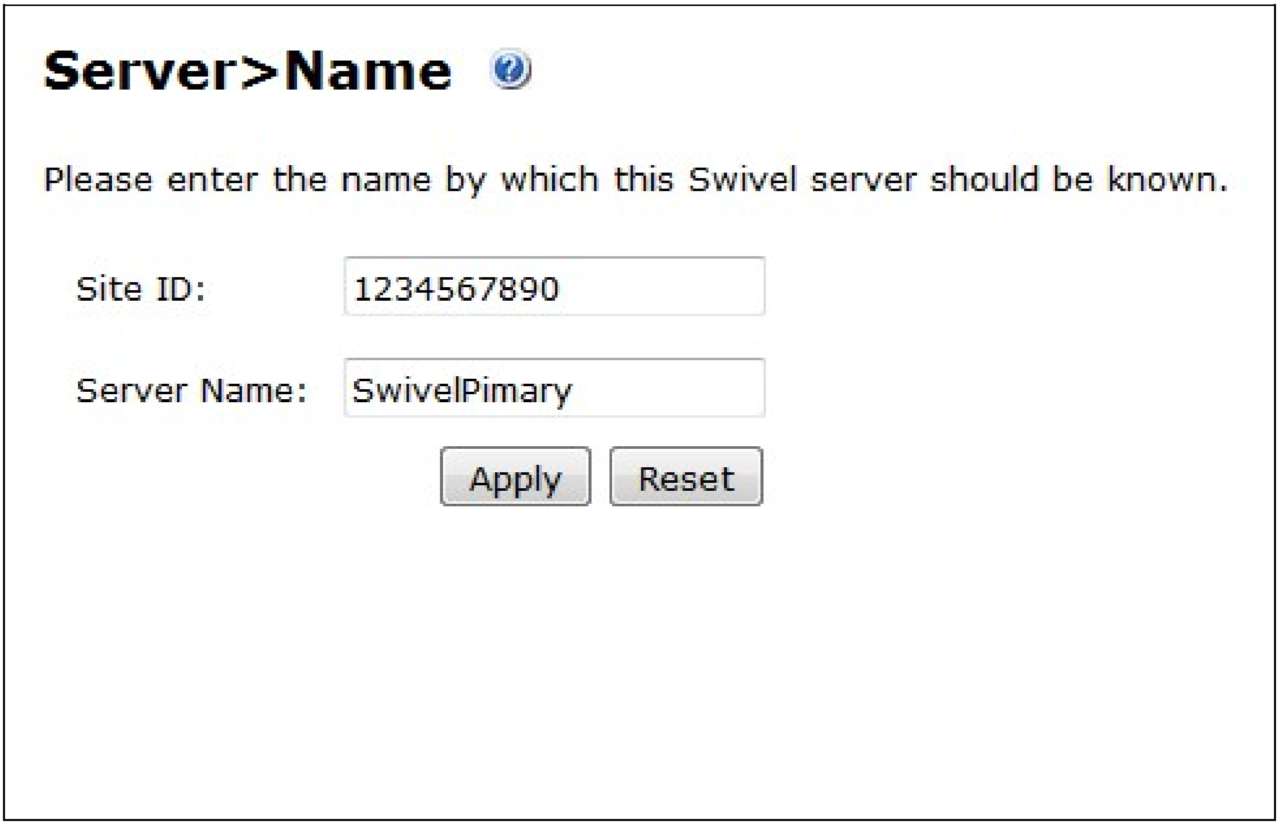
When an organisation become a Swivel customer they are allocated a Site ID. This uniquely identifies their installations and is used as part of the mobile device provisioning process and can also be quoted on support tickets etc.

It is also used as part of the key for encrypting licence keys, therefore licences will be issued for specific Site IDs. If, at the time of purchase, an organisation does not have a licence key, one will be allocated to them.

246.2 Entering Licence Keys

The licence information is sent in a document that contains both the **Site ID** and the **Licence Key**.

First you need to ensure that the Site ID has been set correctly. To do this go to the the Server->Name section and check that the site-id matches that on the licence document. If not then enter the Site-id procived and click apply.



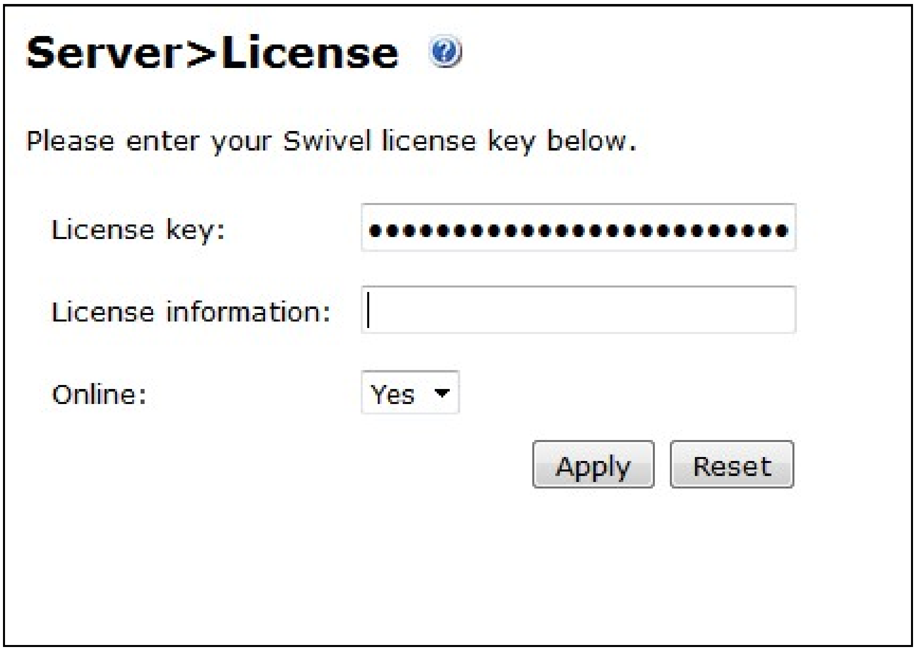
Server>Name

Please enter the name by which this Swivel server should be known.

Site ID: 1234567890

Server Name: SwivelPimary

Then go to the Server -> Licence screen and ensure that on-line is set to yes and then enter the Licence Key into the Licence Key field.



Server>License

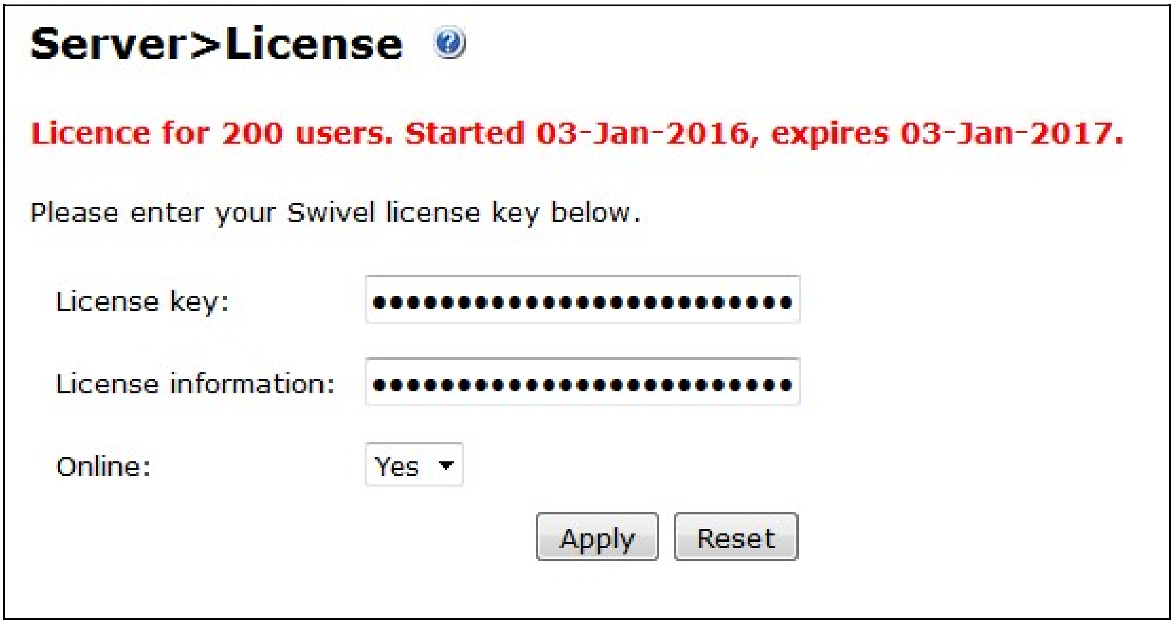
Please enter your Swivel license key below.

License key: ••••••••••••••••••••••••••

License information:

Online: Yes

Then click apply



Server>License

Licence for 200 users. Started 03-Jan-2016, expires 03-Jan-2017.

Please enter your Swivel license key below.

License key: ••••••••••••••••••••••••••

License information: ••••••••••••••••••••••••••

Online: Yes

The appliance will need access to the internet and to DNS to download the licence key information

You will see a message listing the licences associated with the licence key and the Licence Details will be populated.

246.2.1 Off Line Licence Key Entry

If, for any reason, it is not possible to allow the Appliance to contact the Swivel Licence Server then it is possible to set the On-Line mode to Off. In this case, the licence information needs to be entered manually. You can retrieve your current licence information from a browser, using the following URL:

https://ssd.swivelsecure.net/slksext/licence/my-licence-key

Replacing "my-licence-key" with your actual license key.

246.3 Updating Licence Information

With older versions of the software (prior to 3.11), requesting more users required a new licence key. With the new system, the licence key remains the same, but the license information changes.

246.3.1 Updating Licence Information Online

When you update your licence, it is not automatically updated in the appliance. However, if the appliance is online, all you need to do is to go back to the Server -> Licence page and click Apply for the latest licence information to be downloaded.

246.3.2 Updating Licence Information Offline

If your appliance is not able to connect to the internet, then you must retrieve your new licence information and replace it in the Server -> Licence page. Use the same URL as above:

https://ssd.swivelsecure.net/slksext/licence/my-licence-key

Replacing "my-licence-key" with your actual license key.

247 Lockout Account How to guide

248 Overview

Accounts may become locked for a variety of reasons. This document deals with issues, settings and options related to Account Lockout

249 Prerequisites

PINsafe 3.x

250 Account Lockout

Causes of Account lockout: User-account is locked

How to Unlock an Account: How to Unlock

250.1 Maximum Login Tries

This value gives the number of logins that may be attempted until the account is locked. This option is located on the Swivel Administration Console under Policy/General

Maximum login tries:

250.2 Automated Account Unlock

Swivel version 3.8 onwards has the option to automatically unlock accounts after a set duration. The length of time that the account is locked for is given in minutes. This option is located on the Swivel Administration Console under Policy/General. Note that in the administration console after the Auto Unlock period has been exceeded the account remains locked, and when an authentication attempt is made, the account lockout status is checked and the account is marked as unlocked.

Account lockout time (minutes):

A value of 0 means the account will remain locked.

Note: When the Account lockout time is used, an account will remain locked in the Swivel Administration console, until an attempt is made to login to the account, even if the account lockout time has been exceeded. The Account lockout time only applies to users who have been locked out because of too many incorrect login attempts, not to users that have been locked due to inactivity or PIN expiry. If it is set to 0 (the default), then such users are locked indefinitely (until an administrator unlocks them).

Note for SMS users, after a timed lockout a new SMS is not sent. If an authentication failure is made to attempt to get a new SMS, then the account will lock again. Use a Get SMS button to request a new SMS.

251 Testing

252 Known Issues

When the Account lockout time is used, an account will remain locked in the Swivel Administration console, until an attempt is made to login to the account, even if the account lockout time has been exceeded.

Login failures for SMS users will result in a time unlocked account to be locked again.

253 Troubleshooting

254 Log how to guide

255 Overview

By default Swivel logs all activity, with additional logging on Swivel appliances. This article covers Swivel logging and the options available.

256 Prerequisites

Swivel 3.x

257 Swivel XML Logs

Swivel logs data within each individual instance of Swivel. To consolidate logs from several instances of Swivel then Syslog or other log tool such as Splunk or Sawmill should be used.

257.1 Swivel Log Locations

The following article covers the log file locations and how to access the logs: Support logs

257.2 Swivel Log Settings version 3.9 and later

Level: Default: Info, options Off, Info, Warning, Error, Fatal. The lowest level of logging is Off and the highest level is Info, with decreasing log level from Warning to Error to Fatal. Each level of logging includes the level of logging above it, with the exception of OFF.

Max. single file size (KB): Default: 256. The size in KB of each log file. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On Swivel appliances the log data is backed up daily, and may result in large amounts of log data being backed up.

Compress log files after # days: Default: 7, compress the log files after the given number of days. If set to 0 the log files sill never be compressed.

Delete log files after # days: Default: 180, automatically delete the log files after the given number of days. If set to 0 the logs will never be deleted, possibly filling the disk space.

Tidy log file schedule: Every at : Default: daily at 00:21, Specifies when the service that tidies up log files will be run. Files are tidied according to the settings above. Files older than the specified times will be compressed or deleted. Turning this option off (by setting the schedule to Never), log files will never be deleted.

Debug enabled: If enabled this logs data to the debug.log file.

257.3 Swivel Log Settings version 3.8 and earlier

The log settings are configured from the Swivel administration console under Logging/XML. The following options are available:

Level: Default: Info, options Off, Info, Warning, Error, Fatal. The lowest level of logging is Off and the highest level is Info, with decreasing log level from Warning to Error to Fatal. Each level of logging includes the level of logging above it, with the exception of OFF.

Filesize (KB): Default: 256. The size in KB of each log file. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On Swivel appliances the log data is backed up daily, and may result in large amounts of log data being backed up.

File count: The number of log files to be kept. Older logs are rotated out and deleted. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On PINsafe appliances the log data is backed up daily, and may result in large amounts of log data being backed up. Also the files are renamed each time a new log file is created the older log files are renamed. PINsafe 3.9 uses a date stamp for the file name and files do not need to be renamed.

Debug enabled: If enabled this logs data to the debug.log file.

257.4 RADIUS Debug Log Settings

These are enabled under from the Swivel administration console under RADIUS/Server. However you also need to enable debugging under Logging/XML as described above.

The location of the RADIUS debug log is:

/usr/local/tomcat/webapps/pinsafe/WEB-INF/logs/debug.log

257.5 Viewing PINsafe log Files

Log files may be viewed in the Swivel Administration Console.

A Windows utility to view Swivel log files is also available, see the Log Viewer Application

258 Swivel Syslog

Syslog allows consolidation of several logs into one place and with additional tools can be used for security to provide a tamper proof record.

258.1 Syslog Settings

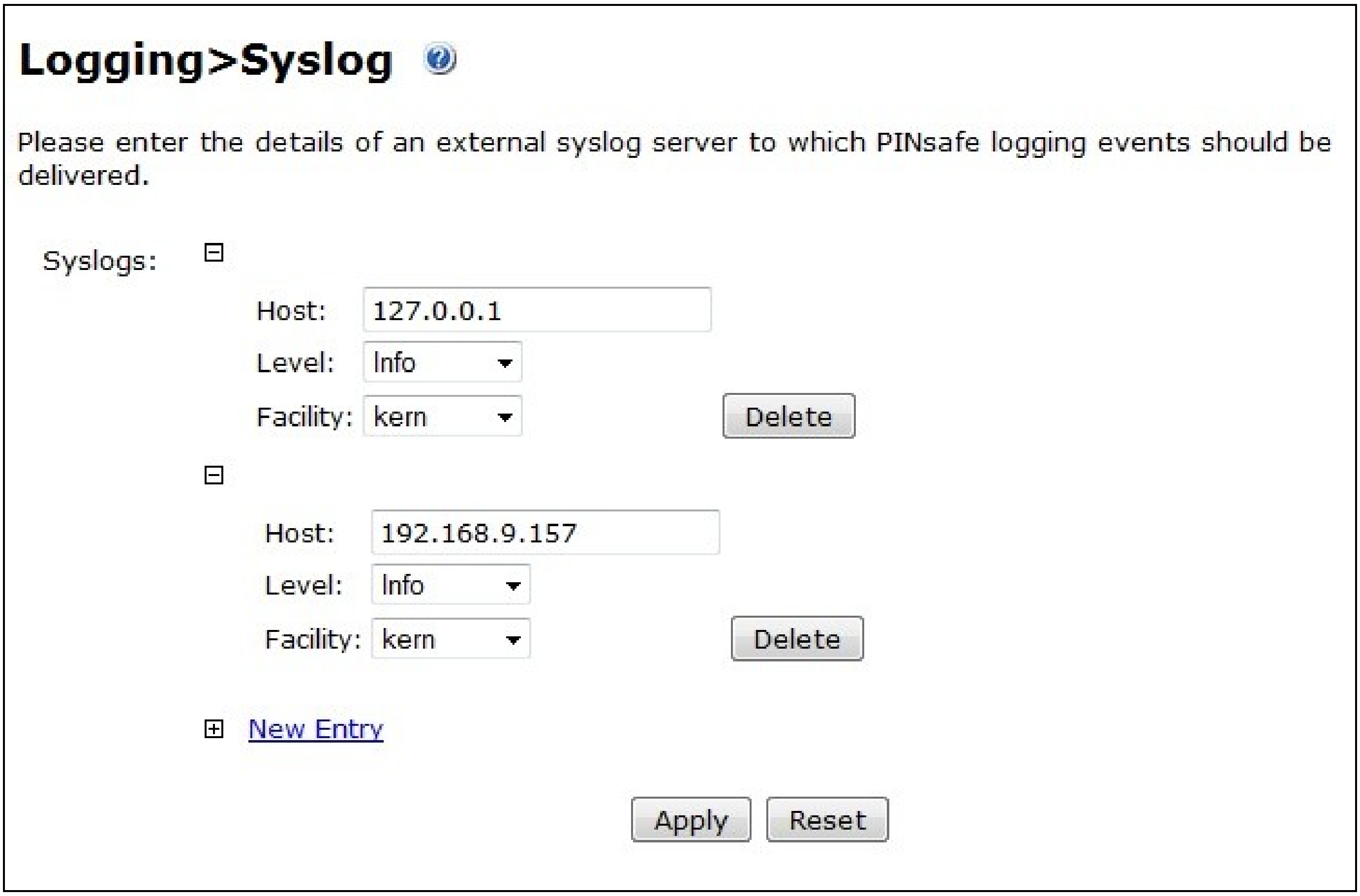
Syslog settings

Host: Default: blank. The IP address/hostname of the syslog server.

Level: Default: Off. The level of PINsafe logging see description above for details.

Facility: Default local0. The log type to use. Leave as the default for PINsafe logs.

Syslog Example



Logging>Syslog

Please enter the details of an external syslog server to which PINsafe logging events should be delivered.

Syslogs: ⊟

Host: 127.0.0.1

Level: Info

Facility: kern

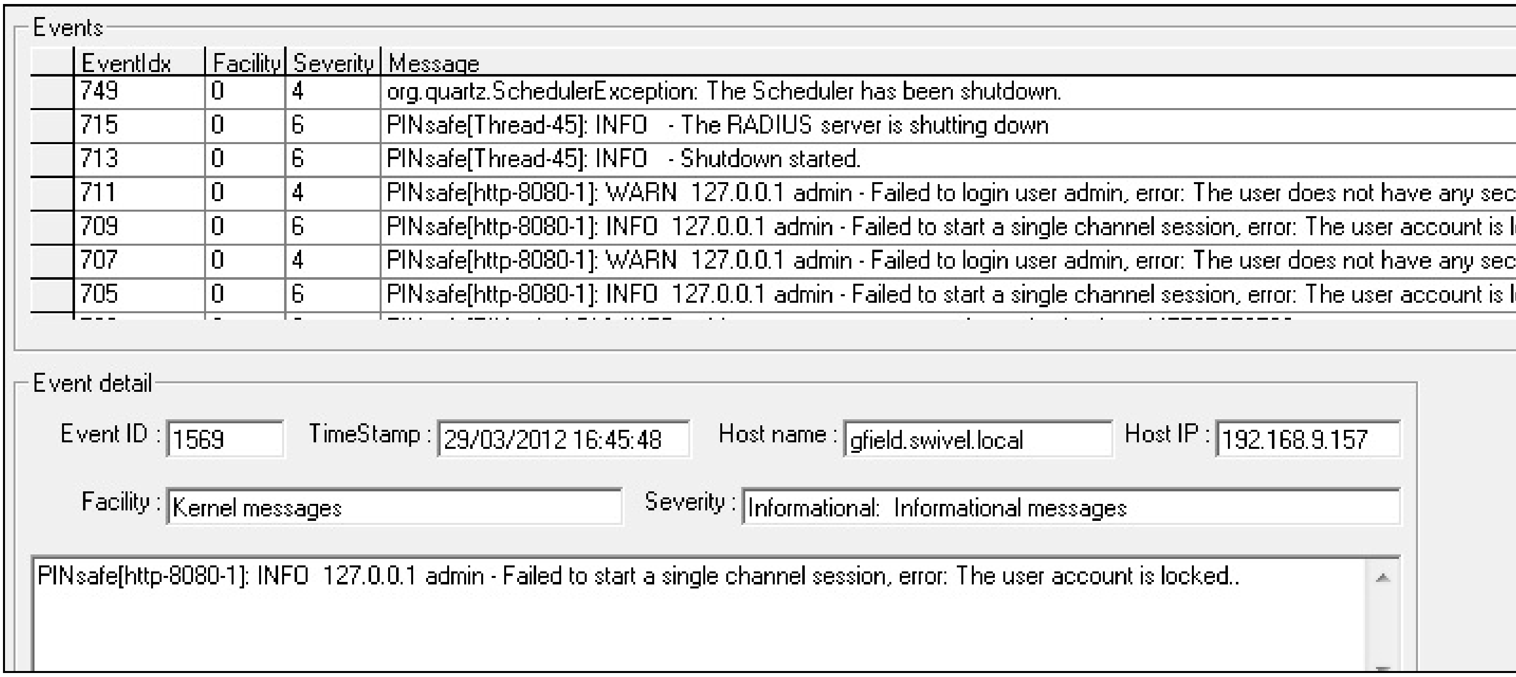
⊟

Host: 192.168.9.157

Level: Info

Facility: kern

Syslog Example output



Events

EventIdx	Facility	Severity	Message
749	0	4	org.quartz.SchedulerException: The Scheduler has been shutdown.
715	0	6	PINsafe[Thread-45]: INFO - The RADIUS server is shutting down
713	0	6	PINsafe[Thread-45]: INFO - Shutdown started.
711	0	4	PINsafe[http-8080-1]: WARN 127.0.0.1 admin - Failed to login user admin, error: The user does not have any sec
709	0	6	PINsafe[http-8080-1]: INFO 127.0.0.1 admin - Failed to start a single channel session, error: The user account is l
707	0	4	PINsafe[http-8080-1]: WARN 127.0.0.1 admin - Failed to login user admin, error: The user does not have any sec
705	0	6	PINsafe[http-8080-1]: INFO 127.0.0.1 admin - Failed to start a single channel session, error: The user account is l

Event detail

Event ID : 1569
TimeStamp : 29/03/2012 16:45:48
Host name : gfield.swivel.local
Host IP : 192.168.9.157

Facility : Kernel messages
Severity : Informational: Informational messages

PINsafe[http-8080-1]: INFO 127.0.0.1 admin - Failed to start a single channel session, error: The user account is locked..

259 Swivel email alerting

Swivel can send an email on triggering certain events. In addition the fail over of the VIP can be configured to send email alerts, see VIP on PINsafe Appliances.

The Swivel application supports the following email alerting:

- Account is locked
- Swivel email trigger for the following levels: Fatal, Error, Warning, Info
- Account creation audit
- User authenticated

260 Testing

261 Known Issues

Swivel 3.10.4 contains some fixes for previous versions where gaps may appear in the logs.

Increasing log files size may fill disk partitions and should be checked.

Increasing log file count fill disk partitions and versions prior to Swivel 3.9 may impact performance when they are renamed during file rotation.

Version 3.9 to 3.9.7, the compressed log files are deleted the day after they are compressed. To avoid this, set the log file compression to 0 so that they are never compressed.

262 Troubleshooting

The index file (.idx) controls the log entries. If any data is missing from the log file it may be possible to recreate the log index. Backup any of the files ending in .idx and then remove them from the log folder. This will cause a new index to be recreated. If the log files are often having to be reindexed, try setting a larger log size as this may mean that new log files are created less often.

Appliances, Swivel 3.9 onwards: /home/swivel/.swivel/log

If there are issues with the Swivel logs dissapearing, try changing the log size from 256 to 257 Kb.

263 Logger Transport

264 Overview

The logger transport allows user alert information and security strings to be sent to the Swivel log using an email transport, and is useful for testing and troubleshooting. See also Transport Configuration.

265 Prerequisites

Swivel 3.9 onwards.

Swivel group to use the logger transport (test users etc) that are not part of another transport group.

Email address entered for test users.

266 Configuring the Swivel logger transport

On the Swivel Administration console select Transport/General and then click on New Entry and enter the following information

Identifier: **logger**

Class: **com.swiveltechnologies.pinsafe.server.transport.LoggerTransport**

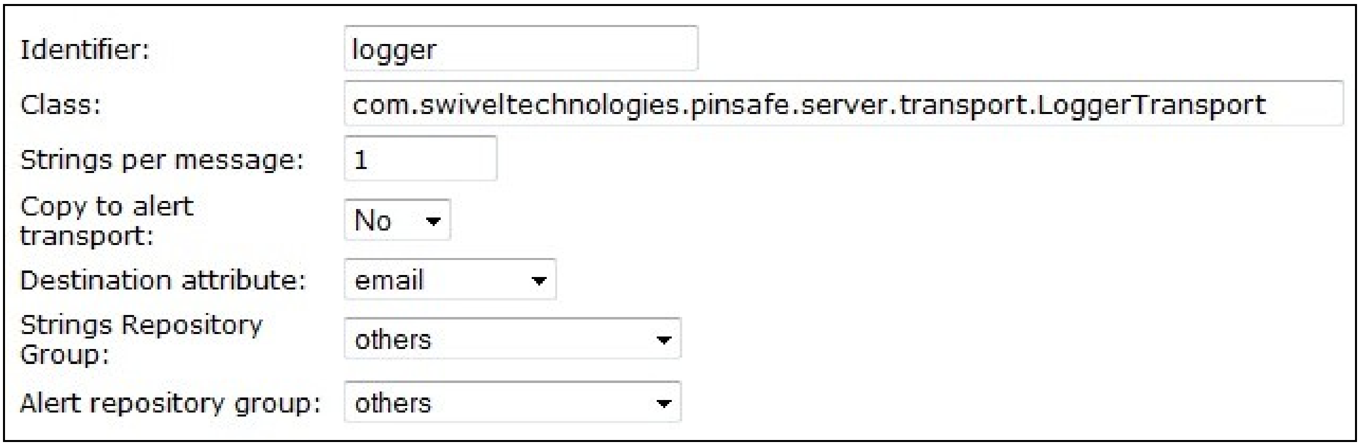
Strings per message: **1**

Copy to alert transport: **No**

Destination attribute: **email**

Strings Repository Group: <group>, example **test**

Alert repository group: <group>, example **test**



Identifier:	logger
Class:	com.swiveltechnologies.pinsafe.server.transport.LoggerTransport
Strings per message:	1
Copy to alert transport:	No
Destination attribute:	email
Strings Repository Group:	others
Alert repository group:	others

Click Apply to save the settings, then under User Administration, select the repository that the users are a member of and click on User Sync.

267 Testing

Check the swivel log to ensure that information is recorded in the log viewer on actions such as with a PIN reset.

Example output:

```
Security strings received for testuser@swivelsecure.com: PINsafe Security String Message 1 1234567890 4691087235

Alert message received for testuser@swivelsecure.com: Your new PINsafe credentials are: Username: testuser Password: PIN: 9430"
```

268 Known Issues

269 Troubleshooting

270 Md5

270.1 Overview

Md5 is a method of computing a unique digital fingerprint of a file. If that file is altered or incomplete then it will have a different digital fingerprint, this digital fingerprint is called a md5 hash. It is used to verify that files have:

- Been downloaded completely;
- Have not been tampered with.

When a file is downloaded, an additional file with the extension **.md5** may be supplied.

RADIUS authentication may also use the md5 hash for CHAP authentication

270.2 Prerequisites

- Downloaded file
- File with extension **.md5**, which contains the md5 sum of the downloaded file
- md5 tool such as *md5sum*. For various types of OS see [1]

270.3 Md5 Guide

270.3.1 Check the md5

For Example using the Unix command *md5sum*

md5sum filename

If the md5 hash and the value in the supplied .md5 file do not match then the file should be discarded.

270.4 Testing

270.5 Known Issues

270.6 Troubleshooting

271 Microsoft ADFS 2 Integration

272 Overview

This document describes how PINsafe authentication can be integrated with web-forms-based login for Active Directory Federation Services (ADFS). It works with ADFS web and ADFS proxy version 2. For ADFS version 3 see Microsoft ADFS 3 Authentication.

273 Updates

NOTE: updated to version 1.2.1.15 to fix error in JavaScript when allowing unknown users.

The version linked to below is version 1.2.1 The following changes have been made from 1.1.5:

- Client DLL and web pages for Swivel image proxy etc. have been incorporated into the filter DLL
- More granular logging available

There were several minor updates between version 1.1 and 1.1.5: mainly bug fixes.

The following changes were made between versions 1.0 and 1.1:

- Fixed some bugs in the login page customisation
- More control over which features are available in the login page
- Ability to share configuration with other ADFS servers
- Ability to control logging of authentication attempts

274 Prerequisites

- ADFS version 2.0 or later, or ADFS 2.0 proxy.
- Swivel ADFS filter, downloadable from here.

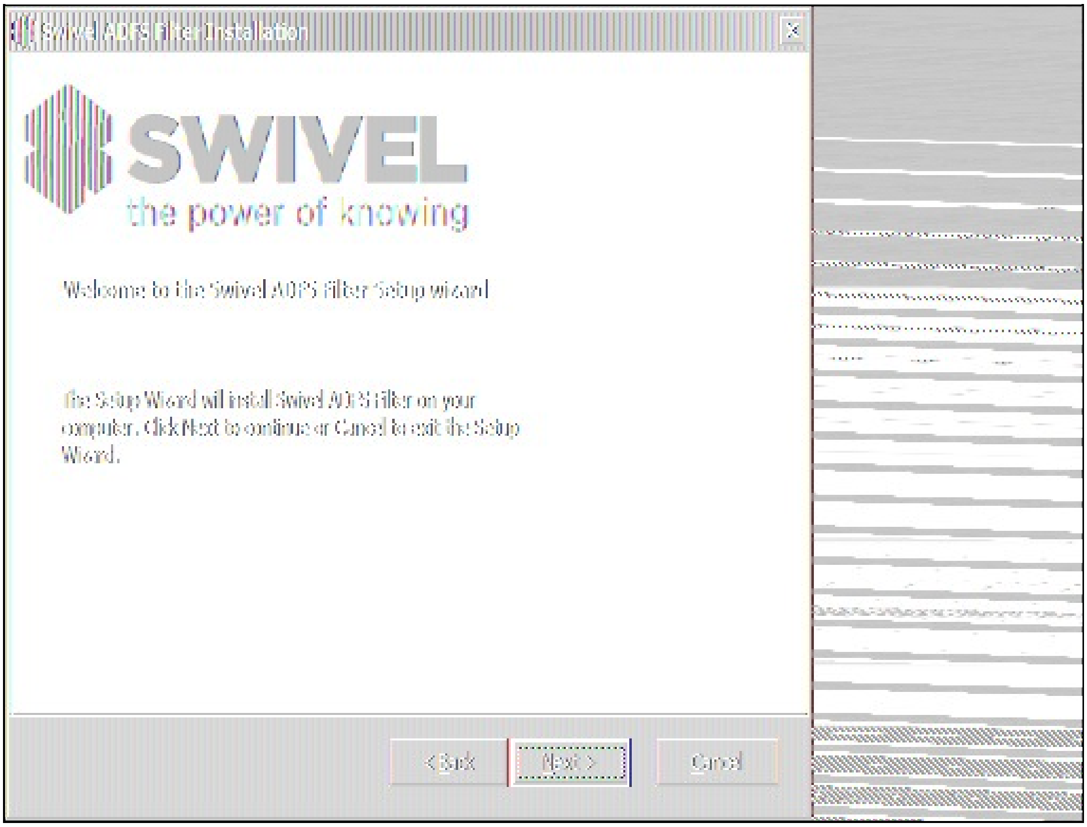
275 How to Guide

275.1 Swivel Configuration Changes

- Under Server -> Single Channel, ensure that ?Allow session start by username? is set to Yes.
- Under Server -> Agents, add the ADFS server as an Agent, and make a note of the secret you enter here.

275.2 Installing the Swivel ADFS Filter

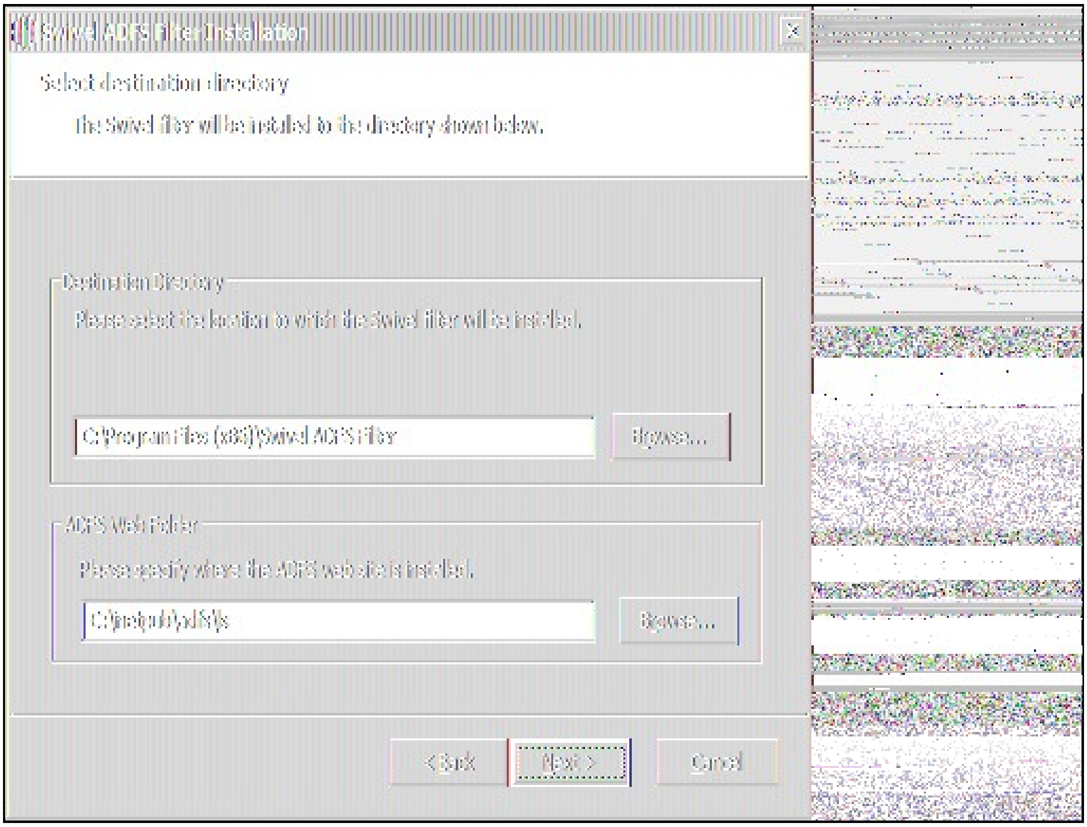
Copy ADFSFilterInstaller.exe to the ADFS server and run it. Note that the program must be run as an administrator. You will see the following display:



Welcome to the Swivel ADFS Filter Setup wizard

The Setup Wizard will install Swivel ADFS Filter on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Click Next to select the installation location:



Select destination directory

The Swivel filter will be installed to the directory shown below.

Destination Directory

Please select the location to which the Swivel filter will be installed.

C:\Program Files (x86)\Swivel ADFS Filter

ADFS Web Folder

Please specify where the ADFS web site is installed.

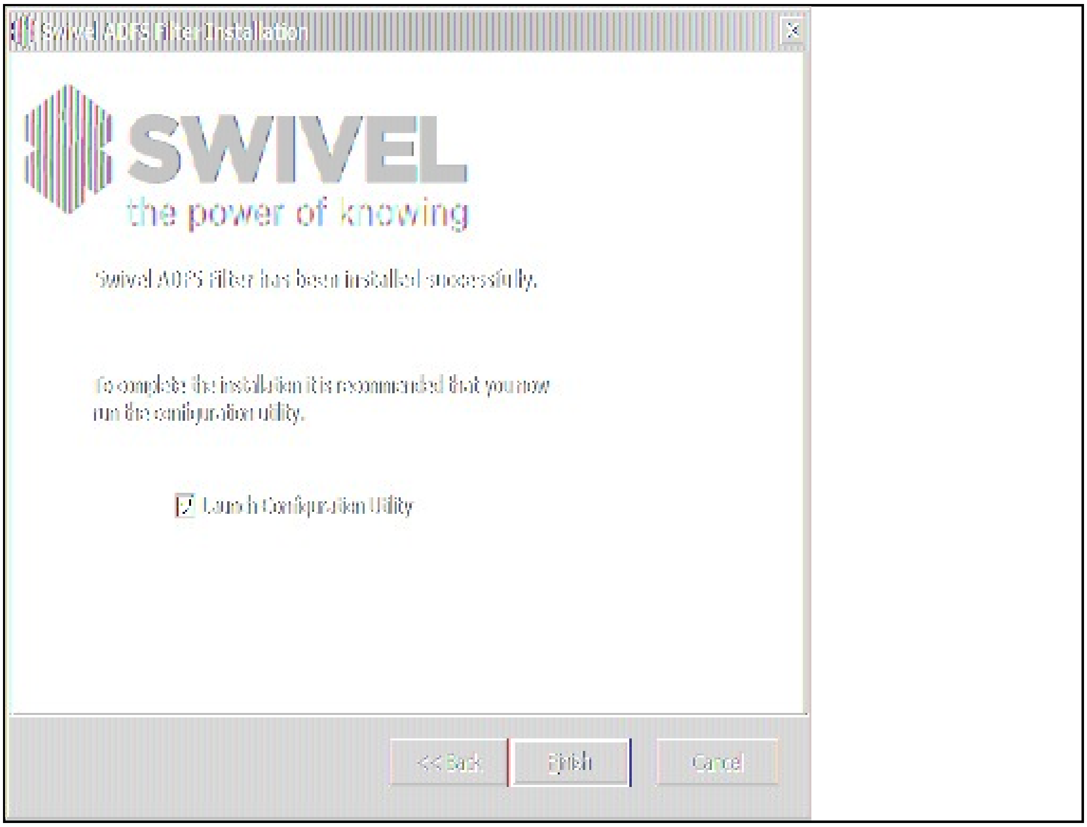
C:\inetpub\adfs\ls

You would normally accept the destination directory as default. Note, however, that if the ADFS Web folder is not in the default location, C:\inetpub\adfs\ls, then you should change the second location to match the correct location. Click Next when these values are correct.

The next screen allows you to specify the name for the Start Menu folder. You can also choose to install the menu for all users, rather than just the installer.

The next screen is a summary screen. Click Next to install the filter.

When installation is complete, you will see the following screen:



Swivel ADFS Filter has been installed successfully.

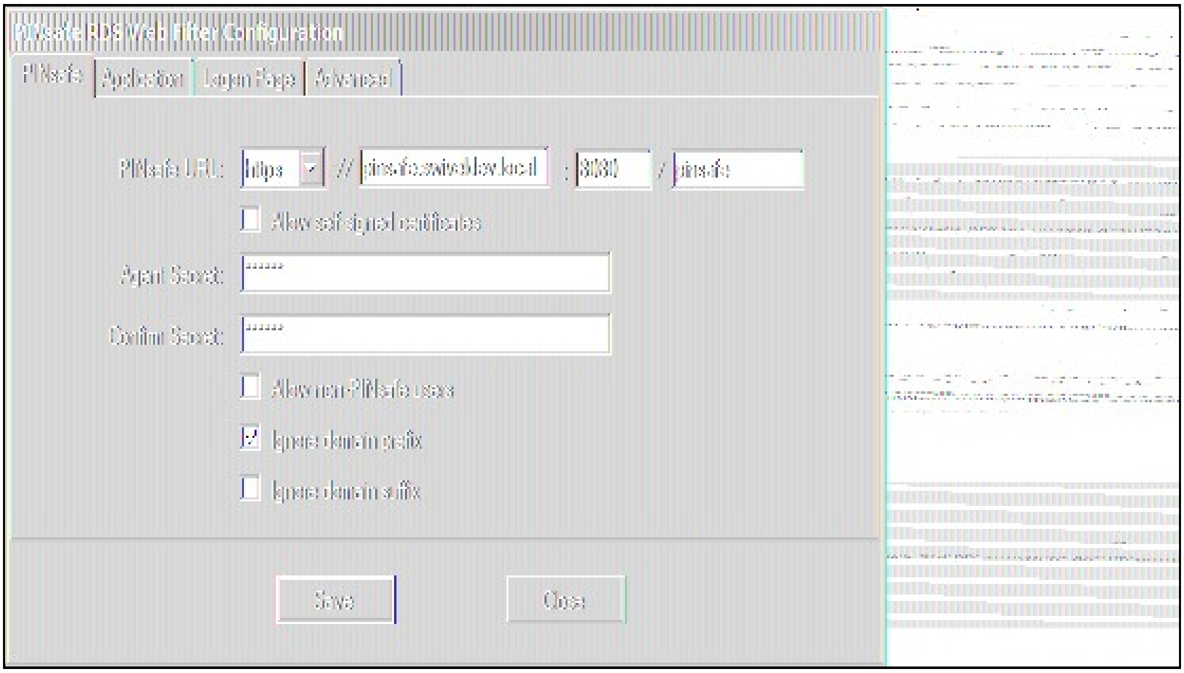
To complete the installation it is recommended that you now run the configuration utility.

☑ Launch Configuration Utility

You will need to run the configuration utility program in order to complete the installation and configuration, so it is recommended that you leave the option to Launch Configuration Utility checked. Click Finish to complete the installation and optionally run the configuration program.

275.3 Configuring the Swivel ADFS Filter

The configuration program consists of four tabs:



PINsafe URL: https :// pinsafe.swiveldev.local : 8080 / pinsafe

□ Allow self-signed certificates

Agent Secret: ******

Confirm Secret: ******

□ Allow non-PINsafe users

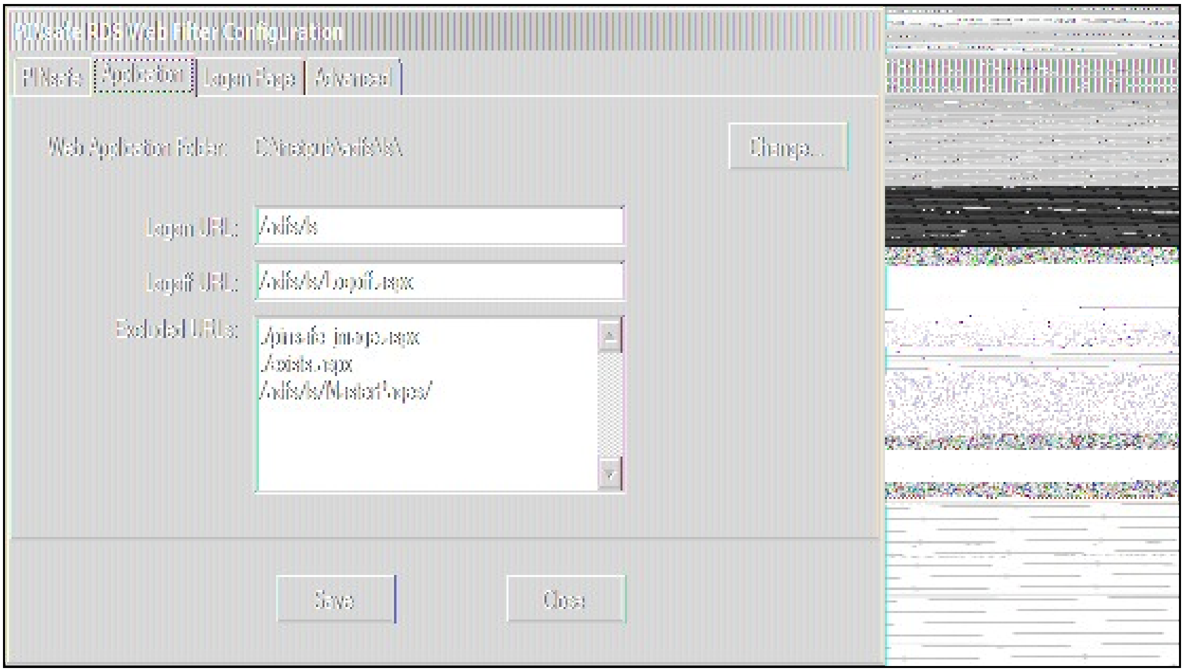
☑ Ignore domain prefix

□ Ignore domain suffix

The PINsafe tab allows you to specify the details for the Swivel server. Most of these settings should be obvious. You should check the option **Allow self-signed certificates** if you are using https and your SSL certificate is not either a commercial certificate or one generated by an internal certificate authority which is Trusted by the ADFS server.

Note: For a Swivel appliance port 8080 is required to be used, rather than the 8443 proxy port.

The option to allow unknown users to authenticate without Swivel authentication only applies to users not known to Swivel at all. You cannot specify that it only applies to a group of users, and not to other users who are known to Swivel, but not in a particular group.



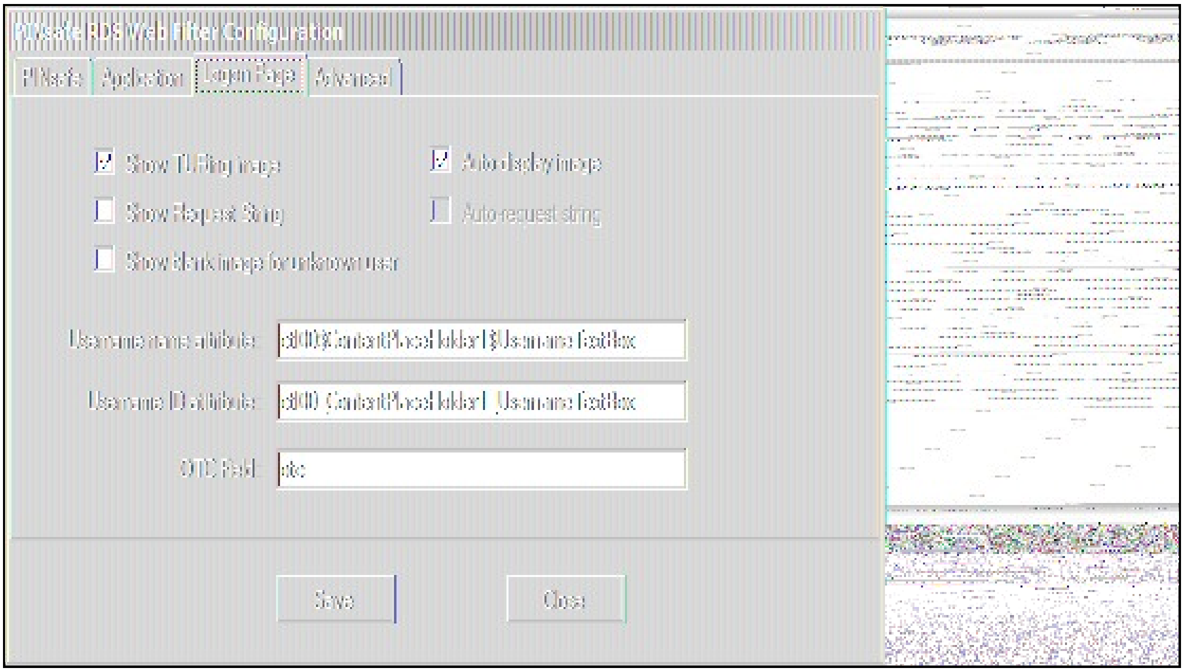
Web Application Folder: C:\inetpub\adfs\ls\

Logon URL: /adfs/ls

Logoff URL: /adfs/ls/Logoff.aspx

Excluded URLs:
/pinsafe_image.aspx
/exists.aspx
/adfs/ls/MasterPages/

The second page shows details of the ADFS web application. You should not normally need to change any of these settings. Ensure that the Excluded URLs section includes all the names listed above.



PINsafe RDS Web Filter Configuration

PINsafe | Application | Logon Page | Advanced

☑ Show TURing image ☑ Auto-display image

□ Show Request String □ Auto-request string

□ Show blank image for unknown user

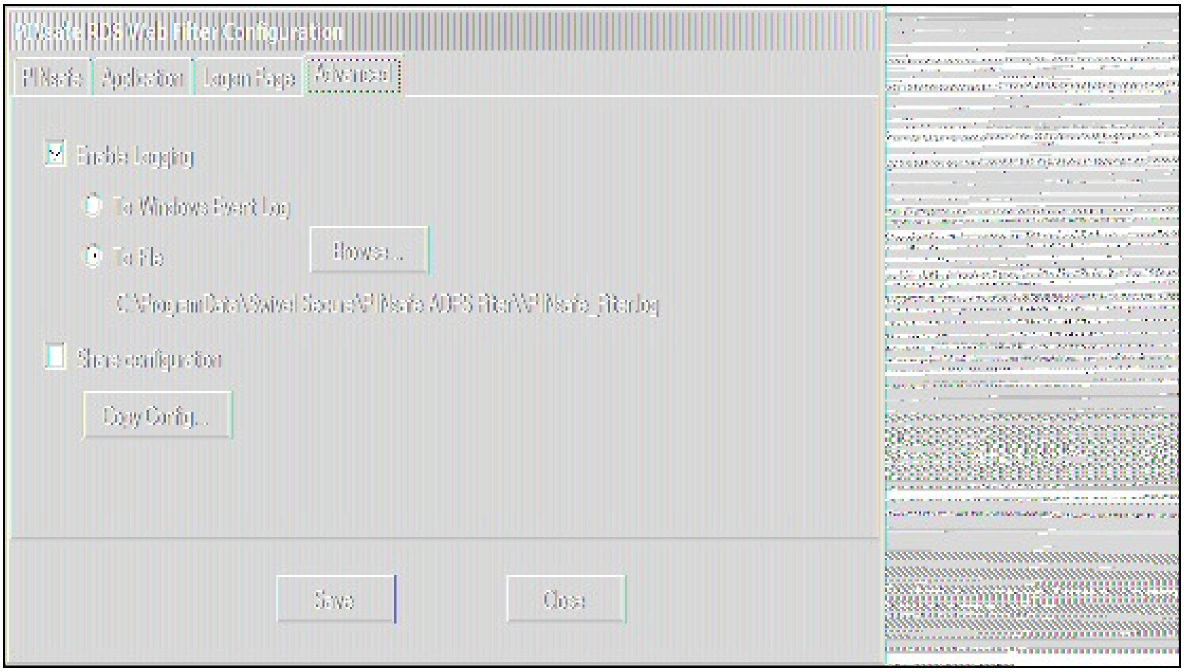
Username name attribute: ctl00$ContentPlaceHolder1$UsernameTextBox

Username ID attribute: ctl00_ContentPlaceHolder1_UsernameTextBox

OTC Field: otc

The Logon Page tab shows details relating to the Swivel filter's integration with the ADFS logon page. The Username name and ID attributes should reflect the values of the name and id attributes of the username text input field as displayed to the web client. The default values are correct as of latest available information.

NOTE: the "Auto-display image" and "Auto-request string" options will perform the relevant action as soon as you enter the username, without having to click on a button. Only one of these options can be active.



PINsafe RDS Web Filter Configuration

PINsafe | Application | Logon Page | Advanced

☑ Enable Logging

○ To Windows Event Log

● To File

C:\ProgramData\Swivel Secure\PINsafe ADFS Filter\PINsafe_Filter.log

□ Share configuration

The Advanced tab shows the logging and sharing options.

Logging enables you to record all attempts to authenticate via the PINsafe ADFS filter. By default, nothing is logged. You can choose to log to the Windows Event log, or to a file. Please note, however, that logging to the event log may fail, if the account running the ADFS web application does not have the right permissions. In this case, the log will be written to the default file location instead: C:\ProgramData\Swivel Secure\PINsafe ADFS Filter\PINsafe_Filter.log.

NOTE: this tab has changed slightly in version 1.2 Instead of a simple Yes/No, logging can be set to "None", "Error", "Info" and "Debug". The last option is only recommended for troubleshooting. Also, the default log method is to file: in order to log to the Windows Event log, you need to ensure that the account under which the ADFS web application is running has the relevant permissions.

If you have more than one ADFS server or proxy, you can save having to enter the settings twice. On the first installation (**Master**), configure the filter as required, and then check the "Share Configuration" checkbox. This will create a share on this server, containing the filter settings. On subsequent installations, click the "Copy Config" button and enter the name or IP address of the Master. The settings will be automatically copied from the Master server. Note that if you change any settings on the master, you will have to copy the configuration again on each slave server.

You are strongly advised to use this option if you have multiple servers, as the configuration includes a random value used to encrypt the authentication cookie. If you configure each server manually, this encryption value will be different, so if you authenticate to one server, and subsequently access another, the PINsafe authentication cookie will not be valid.

275.3.1 A Note on Versions

The first two versions of this application had no means of explicitly identifying the program version, other than right-clicking on the .exe or .dll and selecting Properties. However, you can identify version 1.0 of the program from the fact that it had only 3 tabs in the configuration application, whereas version 1.1 had 4.

From version 1.1.1 onwards, there is an "About..." button on the Advanced tab, which shows a pop-up dialog with version information. This, and the fact that the configuration program is forced to run as Administrator, is the only difference between 1.1 and 1.1.1.

276 Additional Configuration Options

276.1 PINpad

The single channel challenge "PINpad" is available for use. After the standard filter is installed replace the login page with the PINpad specific version, available here.

Note that you need Swivel core version 3.9.2 or later to use this integration.

The zip file linked above also includes the necessary code to display individual Pinpad digits, and static images for the additional buttons required. All these buttons must be added to the list of files excluded from authentication.

Please note that some login page customisations are not available in the PINpad version. It is possible to implement them, but they must be made manually, and any changes to the configuration may result in the non-PINpad login page being restored. The next version of the filter will have the PINpad option integrated.

276.2 Changing the Show TURing Button

After applying the Swivel customisation, go to C:\inetpub\adfs\ls and edit as an Administrator the FormsSignIn.aspx. Look for "Show TURing" and alter it as appropriate.

277 Testing

278 Known Issues

It has been observed that some browsers, noteably Chrome, will cause authentication to fail if the browser default language is not available in the filter. The filter is only provided with English. However, it is possible to add new languages in the configuration page, so please make sure you add any languages your users are likely to require.

279 Troubleshooting

280 Migrate How to guide

281 Overview

Migrate allows user data to be copied from one Swivel Data Store (database) to another, including to and from the Swivel internal data store, it is useful for copying data between different database types or even diferent versions.

CAUTION: The data in target database will be overwritten. Ensure that the data is backed up.

282 Prerequisites

Swivel 3.2 onwards.

Backup data and ensure a valid data backup set is available.

Source and Target serevrs should be set to use the same Timezone.

283 How to Migrate

The following options are available on the Swivel Administration console under Migration/Data

Target database: default: Appliance Database, options (version 3.9.4): Appliance database, JDBC, MS SQL Server, MySQL 5, Oracle 10g, PostgreSQL 8.2. This is where the data will be copied to.

Append to existing data: default: No, Options: Yes/No, allow the data to append to the target database or to overwrite it.

Enter 'MIGRATE': Enter the word *MIGRATE* to confirm that the data will be migrated. The target database will be overwritten, unless the Append option is used, where the data will be added to the target database.

283.1 Data Source

Ensure that the Swivel system is working and there are no errors in the logs.

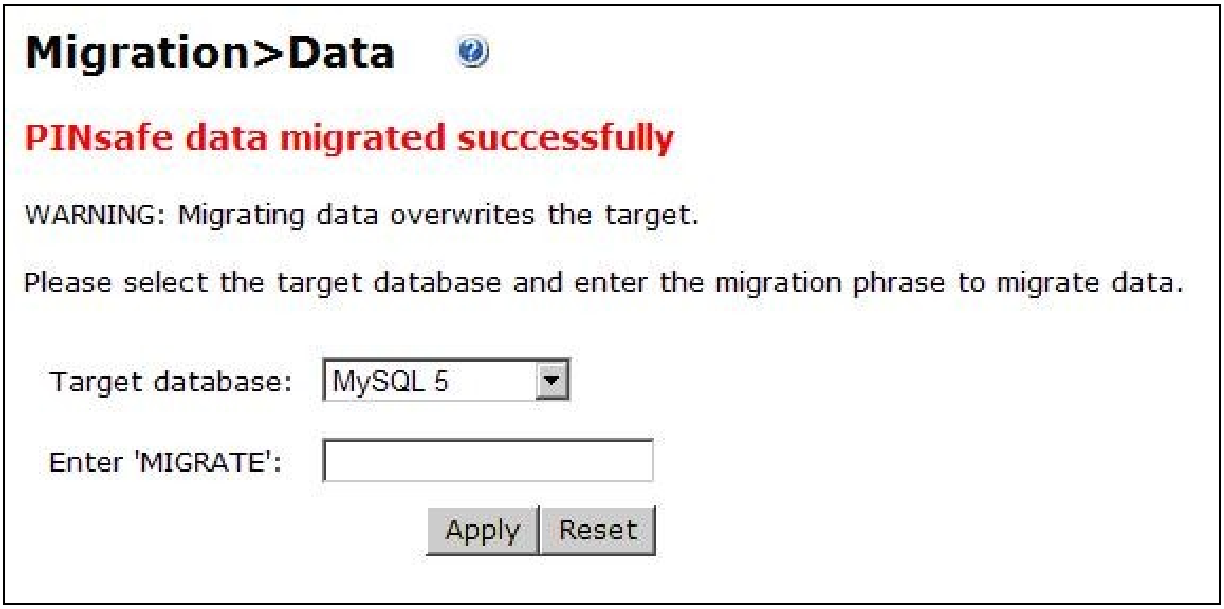
283.2 Data Destination

Tables are created on the target database as part of the Migration process. The target Swivel database configuration needs to be set up on each swivel instance but the Migration is only required on one Swivel instance and in a replicated environment such as the Swivel MySQL appliances the data is replicated to the other instances. Follow the database guides for setting up the databases, the PINsafe configuration and upload any required drivers, see MySQL Database How To Guide, see MS SQL Database How To Guide, see Oracle Database How To Guide. The database should not be selected on the PINsafe Administration console/Database/General until after the Migration.

Once the database has been configured, to migrate the data follow the below steps. **CAUTION: The data in target database will be overwritten** unless the option to Append data is used from Swivel version 3.9.2 onwards.

From the Swivel Administration console select Migration/Data then select the database type and enter MIGRATE, click on apply. A message indicates the data has been successfully migrated.

Example: MySQL database Migration.



Migration>Data

PINsafe data migrated successfully

WARNING: Migrating data overwrites the target.

Please select the target database and enter the migration phrase to migrate data.

Target database: MySQL 5

Enter 'MIGRATE':

The logs will indicate the following messages, the below show the logs for a MySQL example:

Database at jdbc:mysql://localhost/pinsafe_rep

Database com.mysql.jdbc.Driver loaded successfully.

The length of time for Migration will vary between install sites, but 500 users will approximately take 2 minutes.

283.3 Length of Time for Migration

This will vary with the amount of data and number of attributes that each user has, but for a internal Swivel database to a MySQL Swivel appliance database, it will take roughly 2-3 minutes per thousand users. Allow the Sync to complete fully.

284 Testing

Migrate the data and check the logs.

From the Swivel Administration console select Database/General select the target database type then click apply. View user data and status page to ensure correct users and numbers of users have been migrated.

285 Known Issues

IMPORTANT: you MUST use the migrate option when changing between databases of different types. Trying to use SQL export scripts from one database type in a different type will almost certainly cause user credentials to become invalid. This is because Swivel uses the user creation time (among other things) to encrypt the credentials, and different databases store timestamps in different formats, to different accuracies. The migrate function recalculates the credential encryption for the target database. You can use export scripts (such as mysqldump) when moving a database to another server of the SAME type (except internal), although using Migrate is still the preferred option.

286 Troubleshooting

Check the PINsafe logs

For database issues, refer to the relevant database guides.

286.1 Duplicate Entries

PINsafe data migration failed! com.swiveltechnologies.pinsafe.server.user.database.DatabaseException: SQL Exception: The statement was aborted because it would have caused a duplicate key value in a unique or primary key constraint or unique index identified by 'PINSAFENB' defined on 'PINSAFEN'.

Duplicate entries in the MySQL database may cause migration to a swivel internal database to fail with the above error message:

Ensure that the Swivel data is backed up.

To view the duplicate entries, the following command can be run from within the mysql command line:

SELECT A, C, COUNT(D) AS N FROM PINSAFEN GROUP BY A, C HAVING N > 1;

Example:

```
mysql> SELECT A, C, COUNT( D ) AS N FROM PINSAFEN GROUP BY A, C HAVING N > 1;
+------+----+---+
| A    | C  | N |
+------+----+---+
|  151 | 14 | 2 |
|  181 | 14 | 2 |
| 3781 | 14 | 2 |
| 4171 | 14 | 2 |
| 4191 |  0 | 2 |
| 4191 | 14 | 2 |
| 4571 | 14 | 2 |
| 5121 |  0 | 2 |
| 5121 | 14 | 2 |
| 5301 |  0 | 2 |
| 5301 | 14 | 2 |
| 5501 | 14 | 2 |
| 5811 | 14 | 2 |
| 5941 |  0 | 2 |
+------+----+---+
14 rows in set (0.01 sec)
```

The N column shows all the duplicate entries, A and N are values used elsewhere.

The duplicate entries must be removed. The simplest way to do this, is to delete the entries hen re-enter one entry

run the following command to find the existing date entry:

*SELECT * FROM PINSAFEN WHERE A=<value A from table> AND C=<value C from table>*

Example:

```
SELECT * FROM PINSAFEN WHERE A=151 AND C=14;
```

Then delete the entry

DELETE FROM PINSAFEN WHERE A=<value A from table> AND C=<value C from table>;

Example:

```
DELETE FROM PINSAFEN WHERE A=151 AND C=14;
```

Then insert the value using the date given above from the Select command

INSERT INTO PINSAFEN (A, C, D) VALUES (<value A from table>, <value C from table>, '<yyyy-mm hh:mm:ss>');

Example:

```
INSERT INTO PINSAFEN (A, C, D) VALUES (151, 14, '2012-01 12:00:00');
```

If the date field is empty then use:

INSERT INTO PINSAFEN (A, C) VALUES (<value A from table>, <value C from table>);

Example:

```
INSERT INTO PINSAFEN (A, C, D) VALUES (151, 14, '2012-01 12:00:00');
```

Run the count command again to see additional duplicates.

SELECT A, C, COUNT(D) AS N FROM PINSAFEN GROUP BY A, C HAVING N > 1;

When all have been removed then try the MIGRATE command again.

287 Mobile Re-Provision How to Guide

288 Overview

For the Mobile Provision user guide see Mobile Provision User Guide

A Mobile Phone user may request a Mobile Provision Code to allow their Mobile Phone Client to download security strings. The Swivel Helpdesk or Administrator can send the user a Site ID email or SMS message from Swivel version 3.9.7.

The User Portal and Reset Utility provide additional functionality of a self provision and re-provision of mobile clients. This document outlines how to configure the reset.war utility that provides Mobile Phone Provision and Re-Provision. Use of the User Portal should be considered over the ResetPIN and Re-Provision utility.

Also see Mobile Provision Code

289 Mobile Provision, Re-Provision and ResetPIN software

The ResetPIN software can be downloaded from here

290 Installing ResetPIN

ResetPIN is already installed on the virtual or hardware Appliances in the webapps2 folder. If it is virtual or hardware appliance version 2.0.12 or earlier then the ResetPIN software will need to be upgraded, see ResetPIN upgrade for PINsafe 3.8 How To Guide.

To install extract from the zip file and copy the resetpin.war file to the webapps or for virtual or hardware appliances the webapps2 folder. It will automatically deploy when Tomcat is running.

291 Connecting to Provision

Virtual or hardware appliance: https://IP:8443/resetpin/provision.jsp

software install: http://IP:8080/resetpin/provision.jsp

292 Configuring PINsafe to allow Mobile Re-Provision

Swivel must be configured to allow the Mobile Re-Provision utility. On the Swivel Administration console select Policy/Self-Reset then Allow User self-provision of mobile client: to Yes

Send provision code as security string: Yes/No. If set to Yes, then the users provision code will be sent by their security string transport instead of their Alert transport.

293 Default Configuration files

On a virtual or hardware appliance the file is located at:

/usr/local/apache-tomcat-5.5.20/webapps2/resetpin/WEB-INF/settings.xml

The configuration of ResetPIN is in the file settings.xml with the following default values

```
<?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="secret">secret</entry>
<entry key="redirect">http://www.swivelsecure.com</entry>
</properties>
```

294 ResetPIN options explained

The options configure both ResetPIN and the Re-Provision.

ssl: true/false, for communication between ResetPIN and the Swivel server

server: the Swivel server hostname for IP address, for communication between ResetPIN and the Swivelserver

port: the port used to communicate with the PINsafe server for IP address, for communication between ResetPIN and the Swivel server. For software installations use 8080, for virtual or hardware appliances where webapps2 is used, the port 8181 should be used.

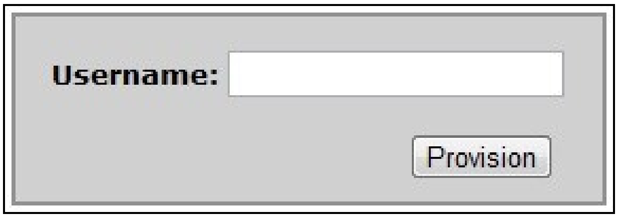
context: the install name of the Swivel application, usually pinsafe for IP address, for communication between ResetPIN and the Swivel server

secret: the shared secret, must also be entered under Server/Agent on the Swivel console for IP address, for communication between ResetPIN and the Swivel server

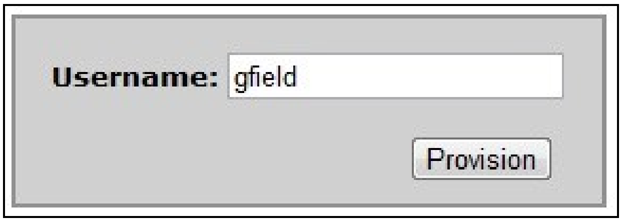
redirect: redirects on completion of ResetPIN, remove the line for no redirect, this must be an address uses can get to

295 Mobile Re-Provision Sample

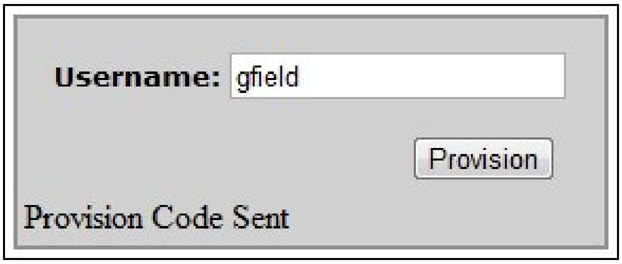
Browse to the Provision link



Enter username


Username: gfield

Click on Provision


Username: gfield

Provision Code Sent

User should receive by their pre-defined transport method a Mobile Provision Code to be entered on the Mobile Phone Applet

Example: Mobile provision code: 4835607192

296 Known Issues

297 Troubleshooting Mobile Re-provision

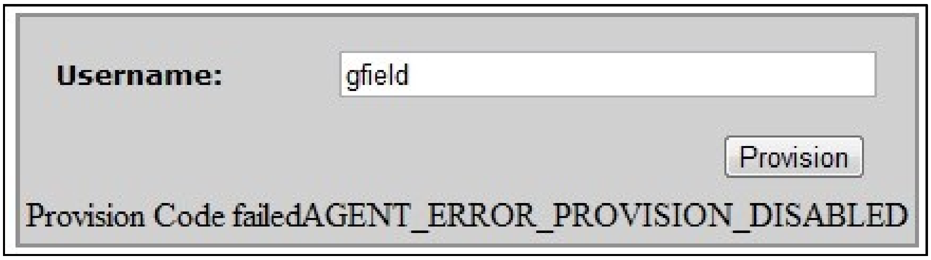
User not set

No username has been entered under options. Enter the username and retry.

Check the Swivel logs

Agent Error Message: **Provision Code failedAGENT_ERROR_PROVISION_DISABLED**

Swivel log message: **Provision code failed for user "username", AGENT_ERROR_PROVISION_DISABLED**



gfield

Provision Code failedAGENT_ERROR_PROVISION_DISABLED

The self Provision is not enabled. On the Swivel Administration Console select Policy/Self-Reset then Allow User self-provision of mobile client: to Yes

298 Mobile Security String Index

299 Overview

The Swivel mobile phone apps allow security strings and One Time Codes on the phone to be used for authentication. More recent versions of the apps, using **Allow String Browsing** allows the user to browse and select a security string or One Time Code for authentication, so it is possible to tell the user which security string to use for authentication.

For multiple security strings in transports such as SMS or email, see Multiple Security Strings How To Guide

300 Prerequisites

Swivel 3.8 or later

Mobile Phone App enabled user

The Swivel server needs to be able to accept the request for the String Index, either through a Proxy or a NAT connection.

301 Requesting the Security String Index

The security string Index is requested from the Swivel server using the following:

http://IP_Address:8080/pinsafe/TokenIndexImage?username=<username>

where username is the username for authentication

302 Testing

In a web browser make a request against the Swivel server with:

http://IP_Address:8080/pinsafe/TokenIndexImage?username=test

This should generate a log in the Swivel server as follows:

Token index image request for user test

303 Known Issues

Currently this command is not supported in the Swivel appliance proxy

Due to limitations within the RADIUS protocol, the Mobile Security String Index only works with PAP authentication and not CHAP or MSCHAP.

304 Troubleshooting

Check the Swivel logs for requests.

305 MobileIron Integration

AuthControl Sentry/Cloud to MobileIron

Integration Notes

306 Overview

Swivel Secure can provide strong and two factor authentication to the Mobile Iron. AuthControl Sentry is a linux based IdP for SAML federations. It is provided as on-prem or Cloud SaaS flavours, providing an adaptative authentication multifactor, managed by a system of points, depending on the factor used and the target app to access. This document outlines the details required to carry this out.

307 Prerequisites

Working MobileIron (MobileIron Sentry appliance) MobileIron Core 9.X and Connector 9.X AuthControl Sentry 4.x

308 How does it work

At App level we use conditional access to Cloud SaaS federated with SAMLv2. The Federated Identity works in 3-way trust with Access between Identity Provider (IDP), Service Provider (SP) and the Access provided by MobileIron AdminPortal/Access Gateway.

309 SwivelSecure Configuration

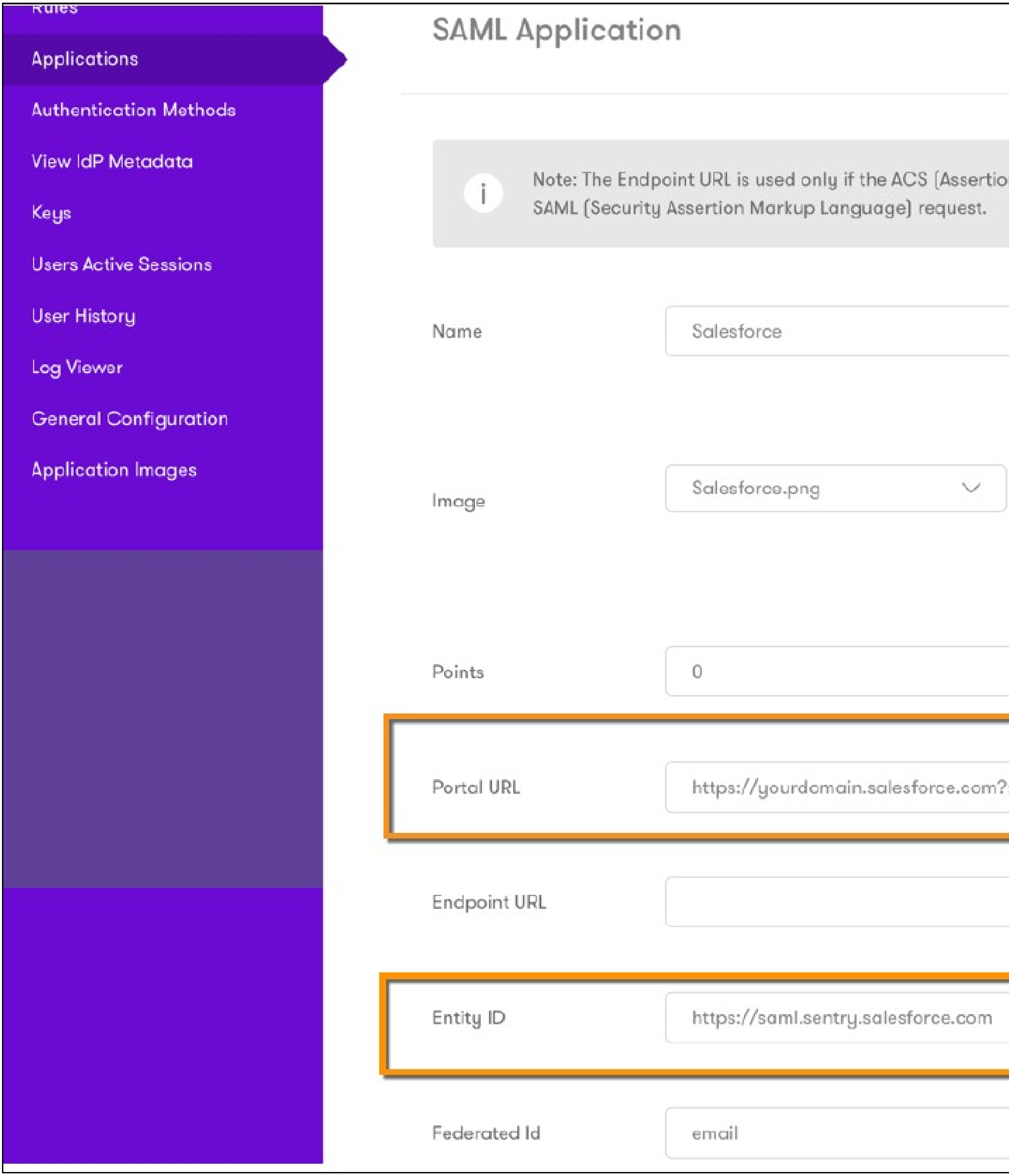
309.1 Enabling Standard Federation - Sales Force

The standard federation involves just this 3 fields:

- Portal URL: (this Endpoint URL can be found on the Setup -> Security Controls -> Single Sign-On

Settings page in Salesforce.com, listed as ?Salesforce Login URL? under the Endpoints section. It is unique to your Salesforce.com instance and domain.

- Entity ID:, Reflected on SalesForce SSO configuration for My Domain
- Federeated id: That needs to match with the attributed defined on Salesforce.com and Swivel



SAML Application

Note: The Endpoint URL is used only if the ACS (Assertio
SAML (Security Assertion Markup Language) request.

Name: Salesforce

Image: Salesforce.png

Points: 0

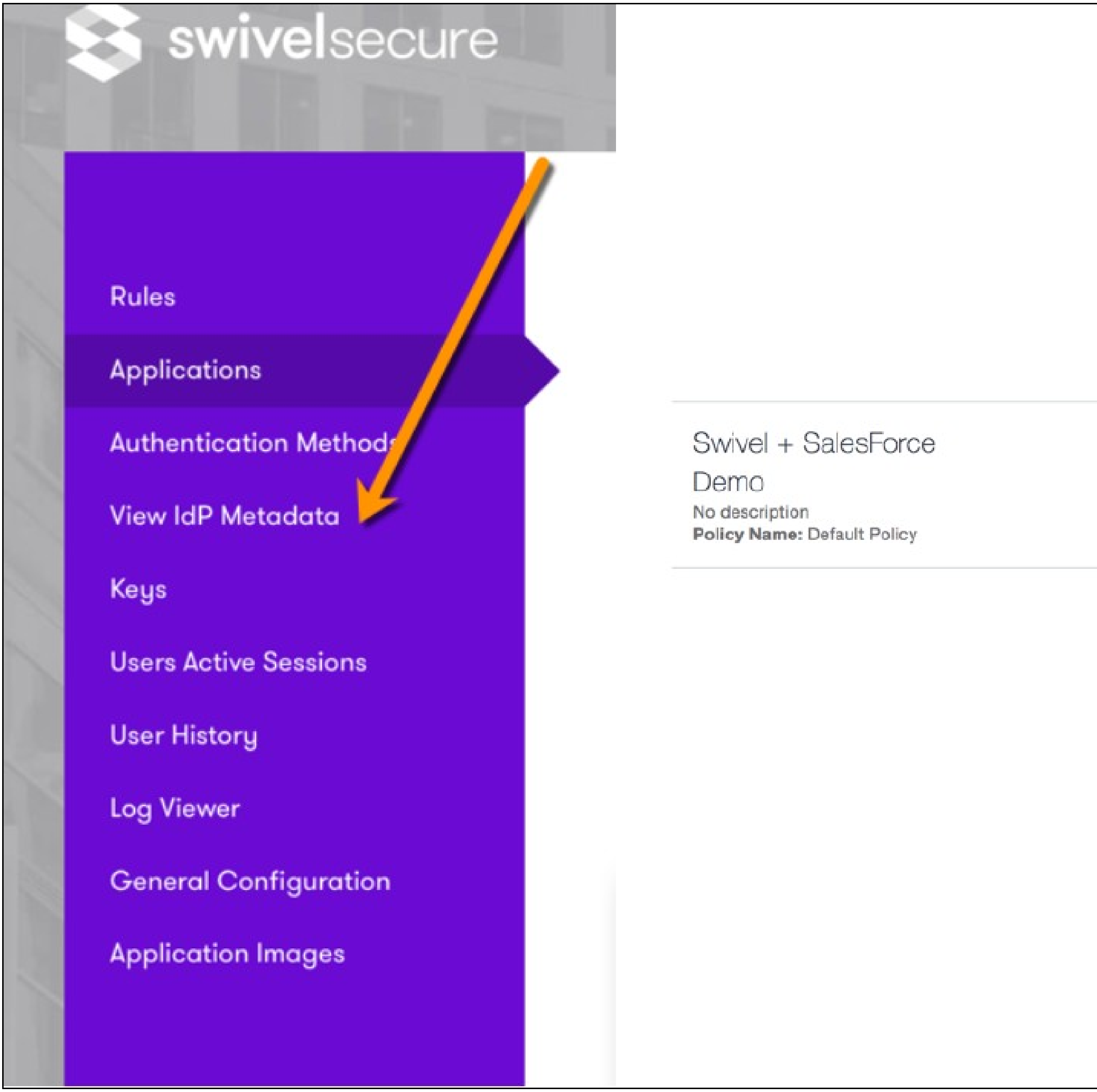
Portal URL: https://yourdomain.salesforce.com?

Endpoint URL:

Entity ID: https://saml.sentry.salesforce.com

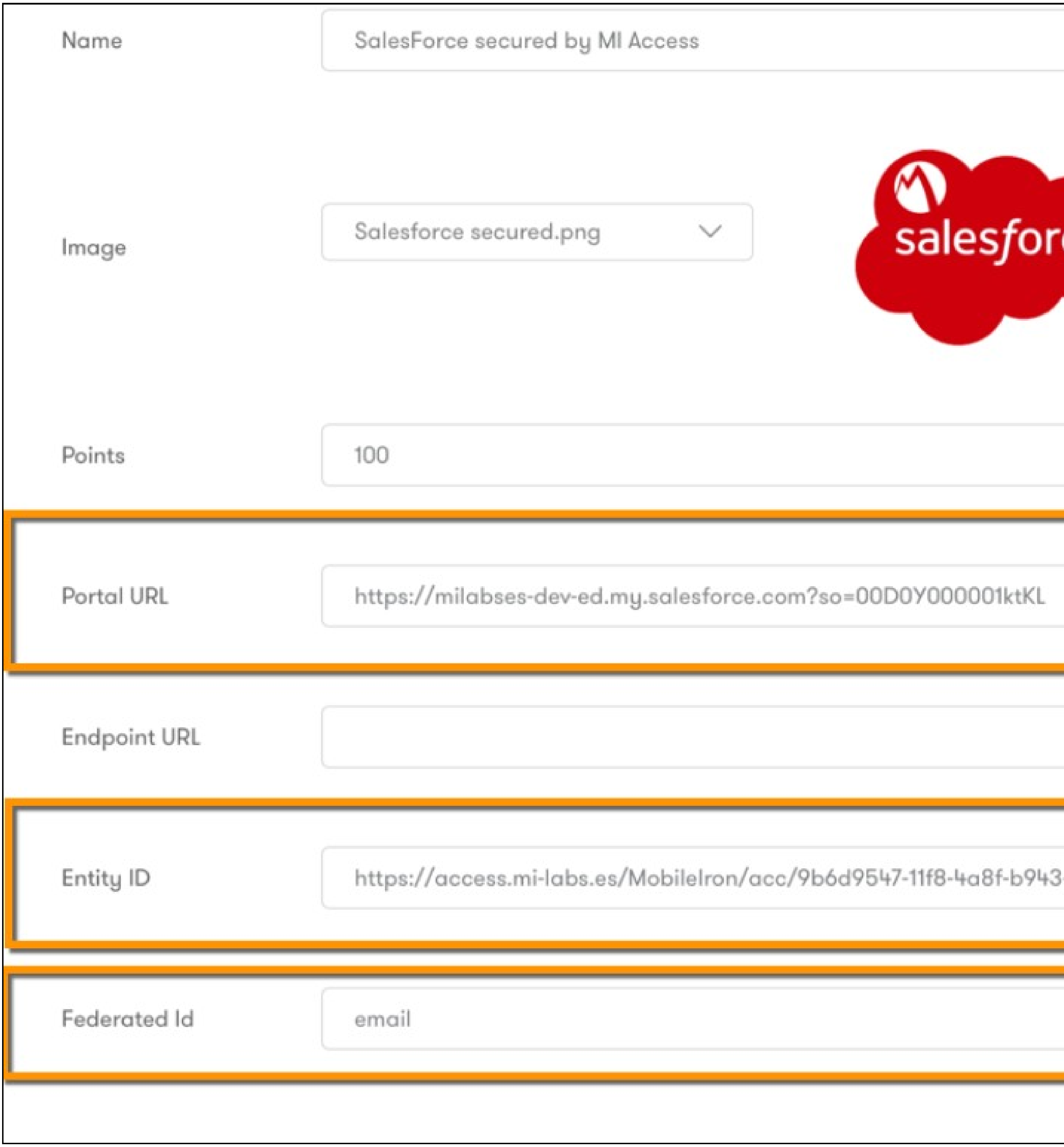
Federated Id: email

Once that we have a working federation from AuthControl Sentry and the SP, (in the example we will use SalesForce), this is just a standard SalesForce and Custom IdP federation on MI Access console, as the MFA part from Swivel will be triggered once the MI Access has approved the connection. AuthControl Sentry provides a metadata url to quickly get the XML from IdP. It uses POST method for federation.



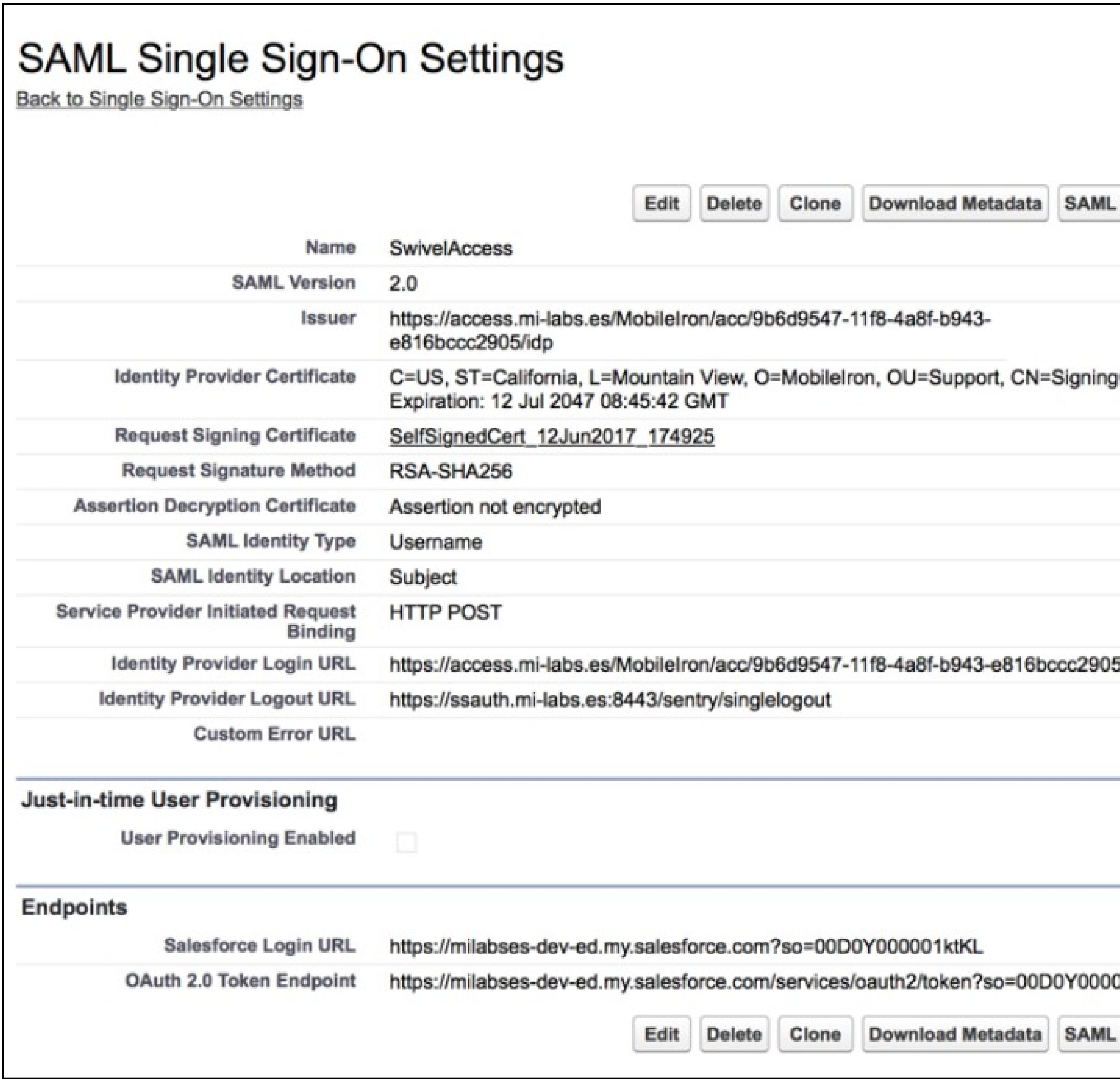
Swivel + SalesForce Demo
No description
Policy Name: Default Policy

SAML Customization of Mobile Iron settings, Portal URL, Entity ID and Federated ID:



Name	SalesForce secured by MI Access
Image	Salesforce secured.png
Points	100
Portal URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
Endpoint URL	
Entity ID	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943
Federated Id	email

SAML Customization in the Sales Force Side. Settings for Mobile Iron.



SAML Single Sign-On Settings

Name	SwivelAccess
SAML Version	2.0
Issuer	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905/idp
Identity Provider Certificate	C=US, ST=California, L=Mountain View, O=MobileIron, OU=Support, CN=Signing Expiration: 12 Jul 2047 08:45:42 GMT
Request Signing Certificate	SelfSignedCert_12Jun2017_174925
Request Signature Method	RSA-SHA256
Assertion Decryption Certificate	Assertion not encrypted
SAML Identity Type	Username
SAML Identity Location	Subject
Service Provider Initiated Request Binding	HTTP POST
Identity Provider Login URL	https://access.mi-labs.es/MobileIron/acc/9b6d9547-11f8-4a8f-b943-e816bccc2905
Identity Provider Logout URL	https://ssauth.mi-labs.es:8443/sentry/singlelogout
Custom Error URL	

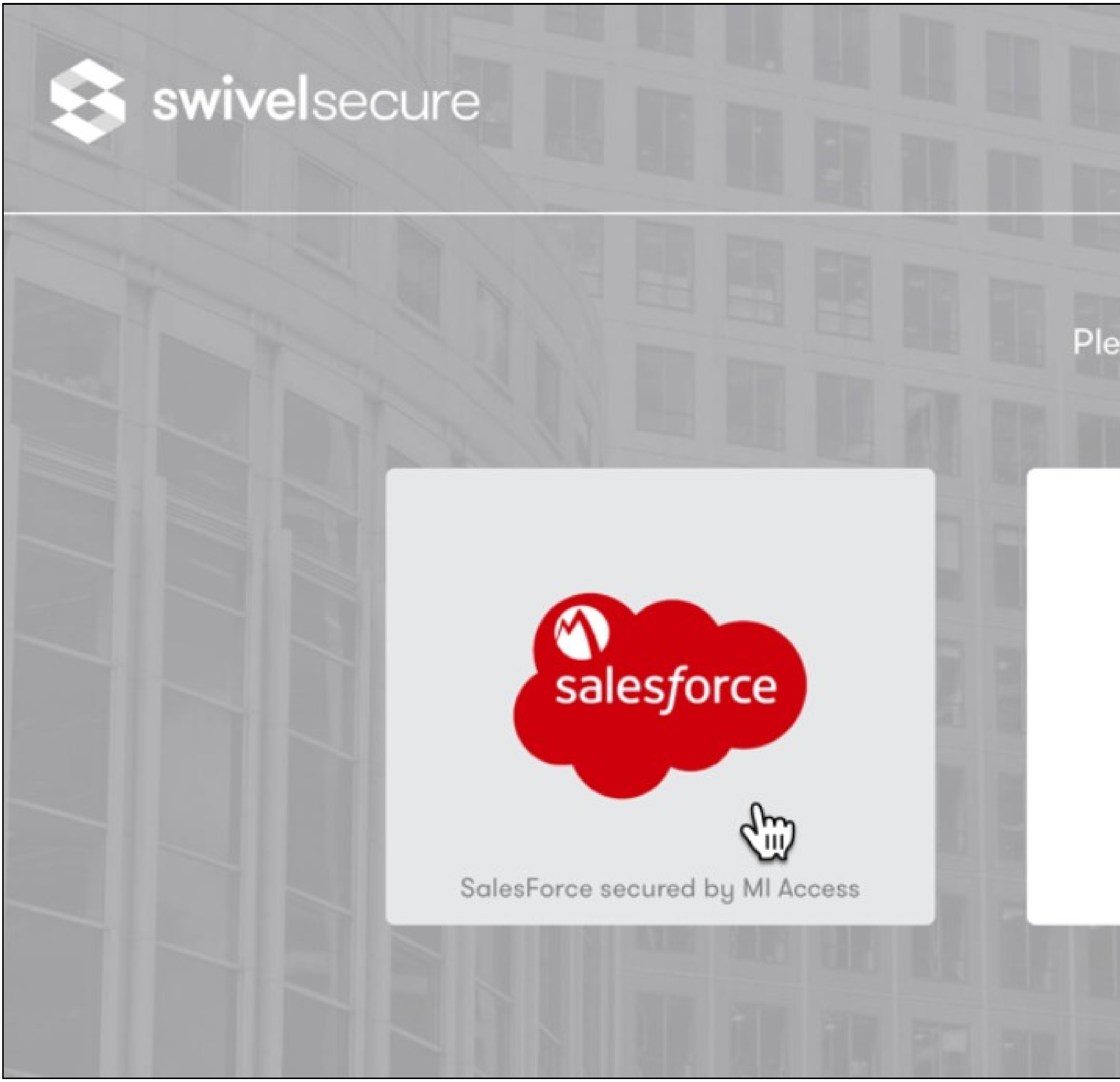
Just-in-time User Provisioning

User Provisioning Enabled	□

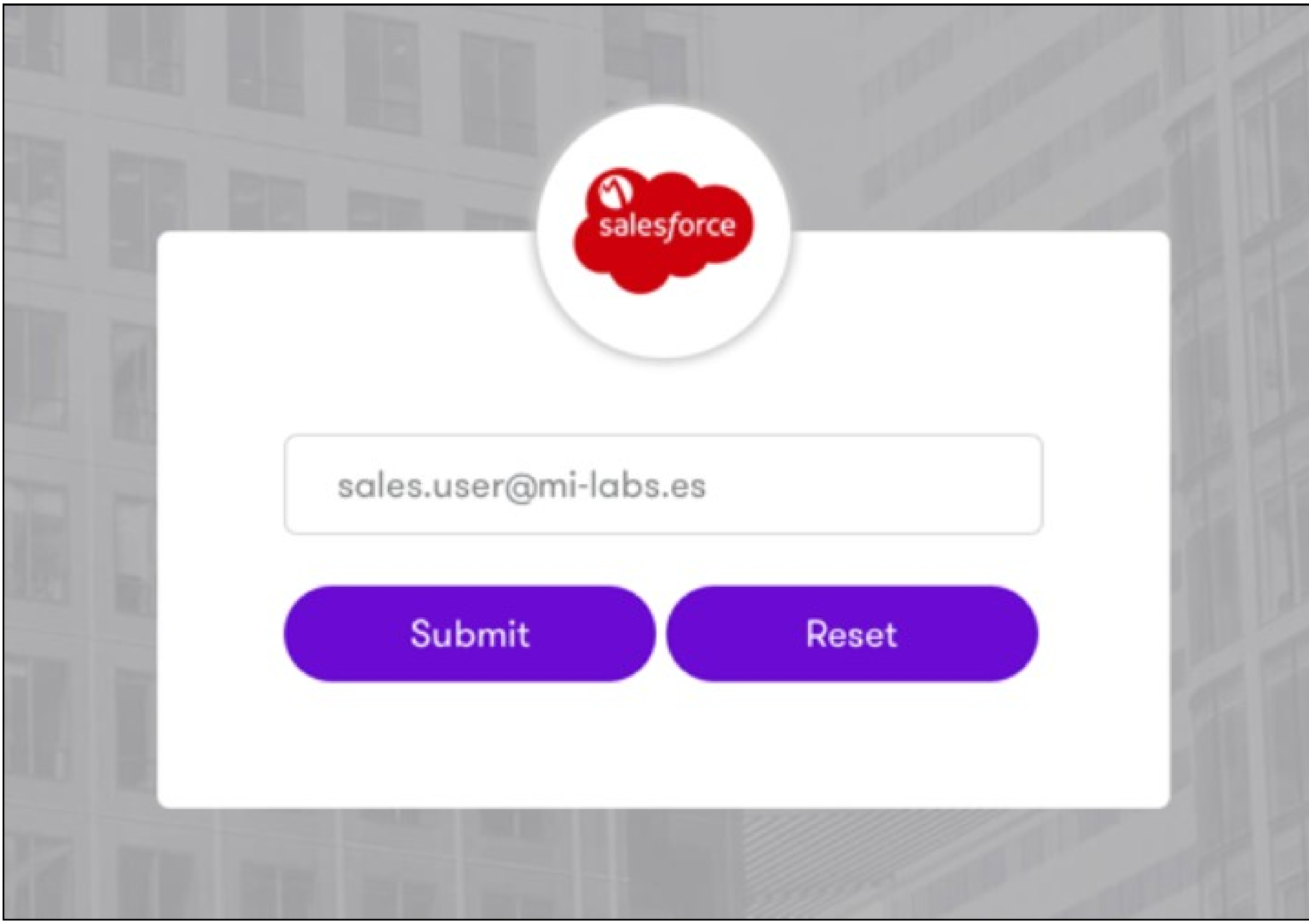
Endpoints

Salesforce Login URL	https://milabses-dev-ed.my.salesforce.com?so=00D0Y000001ktKL
OAuth 2.0 Token Endpoint	https://milabses-dev-ed.my.salesforce.com/services/oauth2/token?so=00D0Y0000

After the application settings definitions have been applied the aplications are available in AuthControl Sentry's web portal.

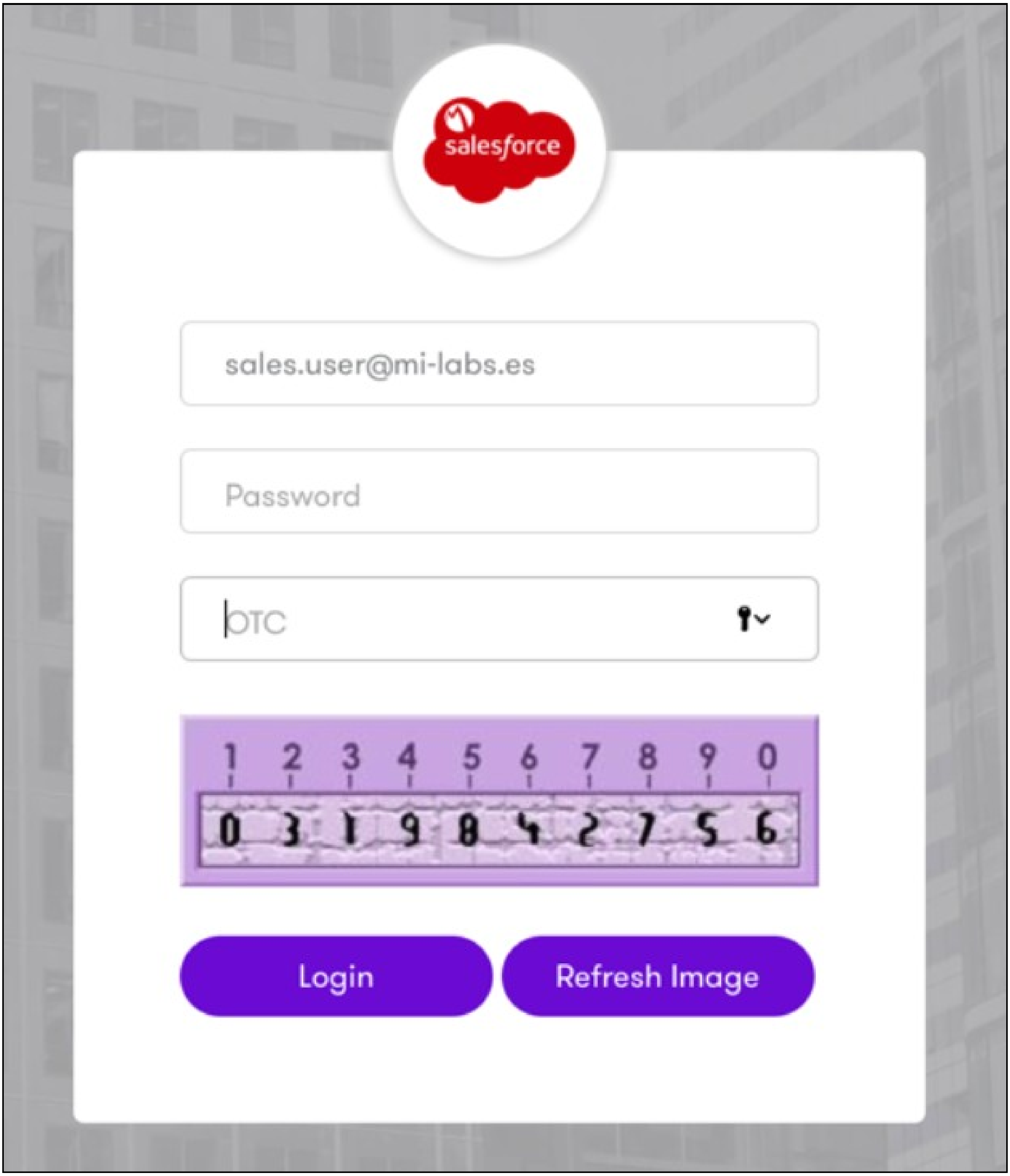


User Login in Authcontrol Sentry with SalesForce using the MI Account



sales.user@mi-labs.es

SSO for SalesForce using Mobile Iron and Turing image from SwivelSecure. This means that the user logs in using the Swivel Secure credentials, by the selected method (in this case Turing image) into the Sales Force (without the need of using Sales Force Credentials).



sales.user@mi-labs.es

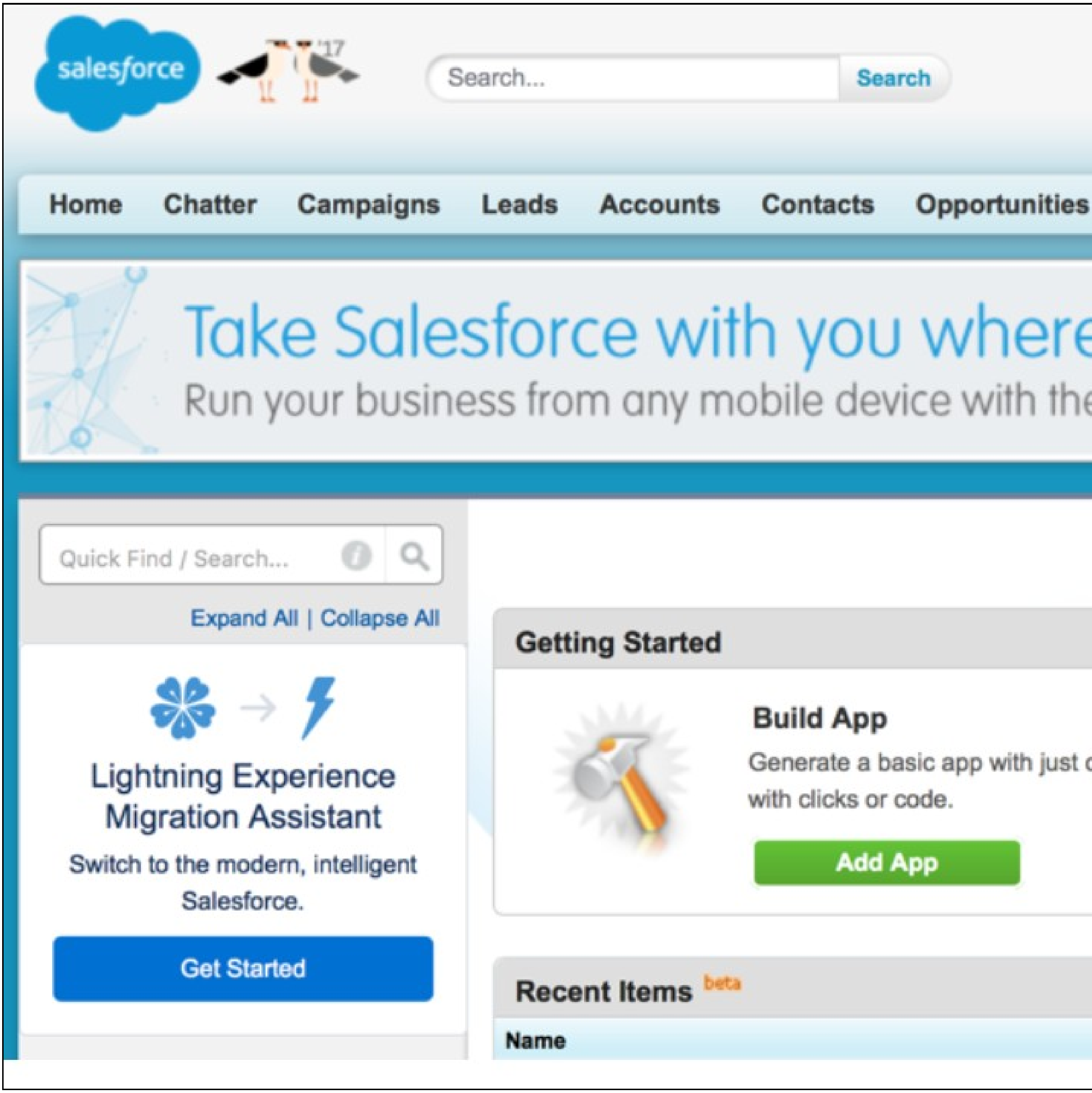
Password

OTC

1 2 3 4 5 6 7 8 9 0

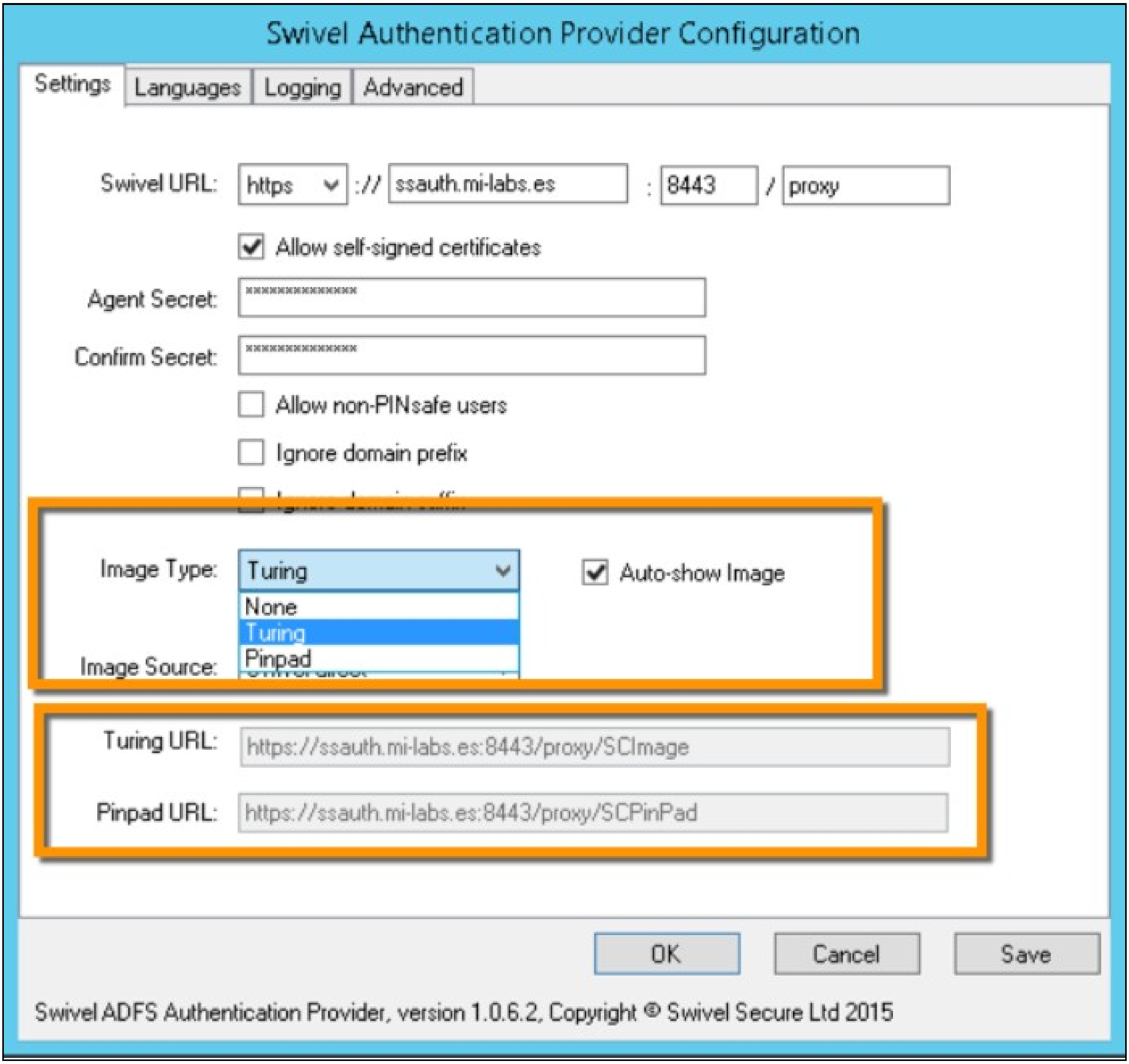
0 3 1 9 8 4 2 7 5 6

Successfull login in Sales Force.


salesforce
'17
Search...
Search
Home
Chatter
Campaigns
Leads
Accounts
Contacts
Opportunities
Take Salesforce with you where
Run your business from any mobile device with the
Quick Find / Search...
Expand All | Collapse All
Lightning Experience Migration Assistant
Switch to the modern, intelligent Salesforce.
Get Started
Getting Started
Build App
Generate a basic app with just o
with clicks or code.
Add App
Recent Items beta
Name

309.2 Enabling Standard Federation - Office 365

In the case of Office365, AuthControl requires that the main federation must be performed with ADFS. On a working federation, a complement has to be installed on ADFS 3.0 server.



Swivel URL: https ://ssauth.mi-labs.es : 8443 / proxy

☑ Allow self-signed certificates

Agent Secret: ***************

Confirm Secret: ***************

□ Allow non-PINsafe users

□ Ignore domain prefix

Image Type: Turing

None

Turing

Pinpad

☑ Auto-show Image

Image Source:

Turing URL: https://ssauth.mi-labs.es:8443/proxy/SCImage

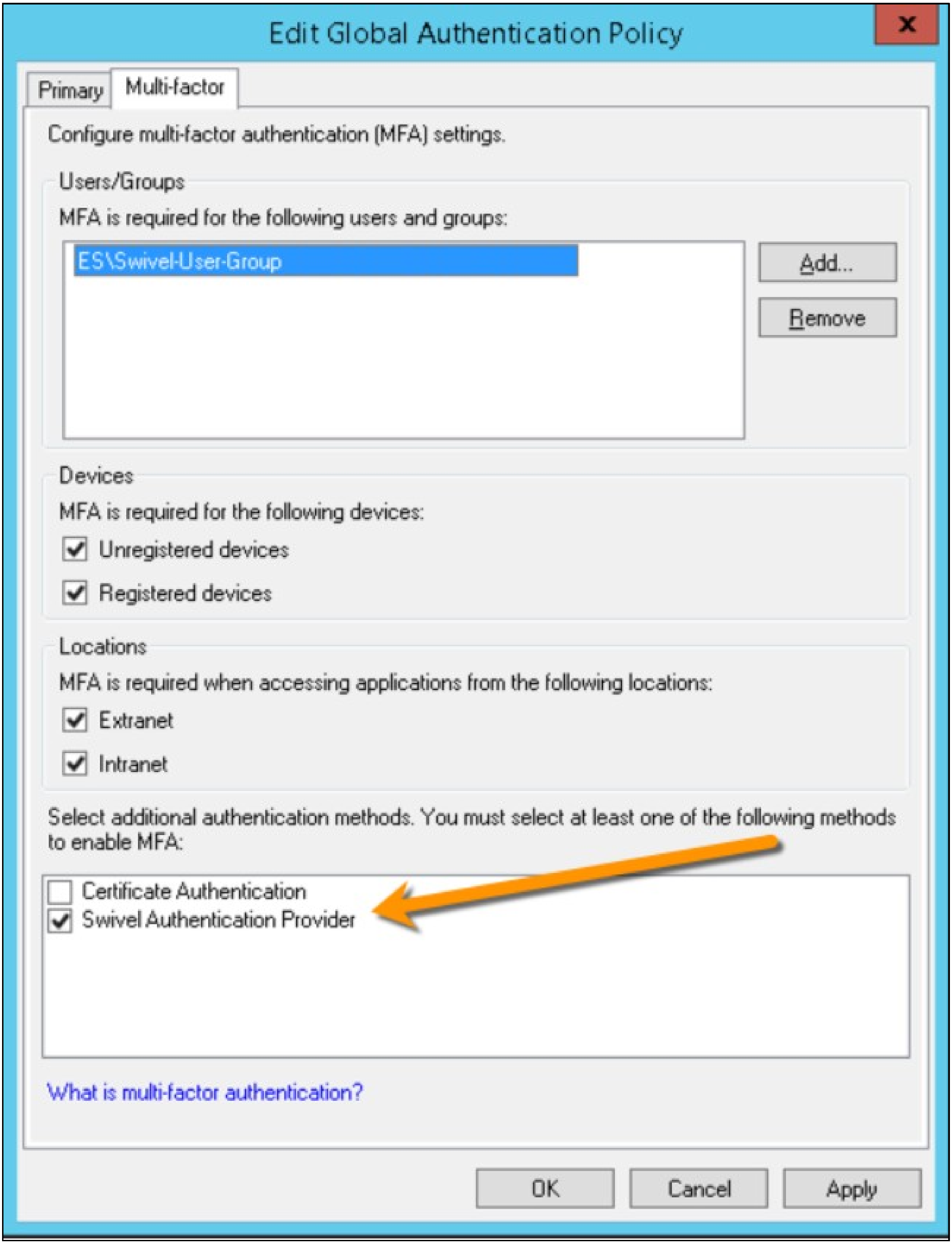
Pinpad URL: https://ssauth.mi-labs.es:8443/proxy/SCPinPad

Swivel ADFS Authentication Provider, version 1.0.6.2, Copyright © Swivel Secure Ltd 2015

There?s a couple of choices depending if the customer is using ADFS Proxy servers or not.

This plugin installs Swivel Secure product as an MFA to be applied via ADFS Authentication Policy Settings.

Set AuthControl Sentry / Swivel Secure as Authentication Provider



Edit Global Authentication Policy

Configure multi-factor authentication (MFA) settings.

Users/Groups

MFA is required for the following users and groups:

ES\Swivel-User-Group

Devices

MFA is required for the following devices:

☑ Unregistered devices

☑ Registered devices

Locations

MFA is required when accessing applications from the following locations:

☑ Extranet

☑ Intranet

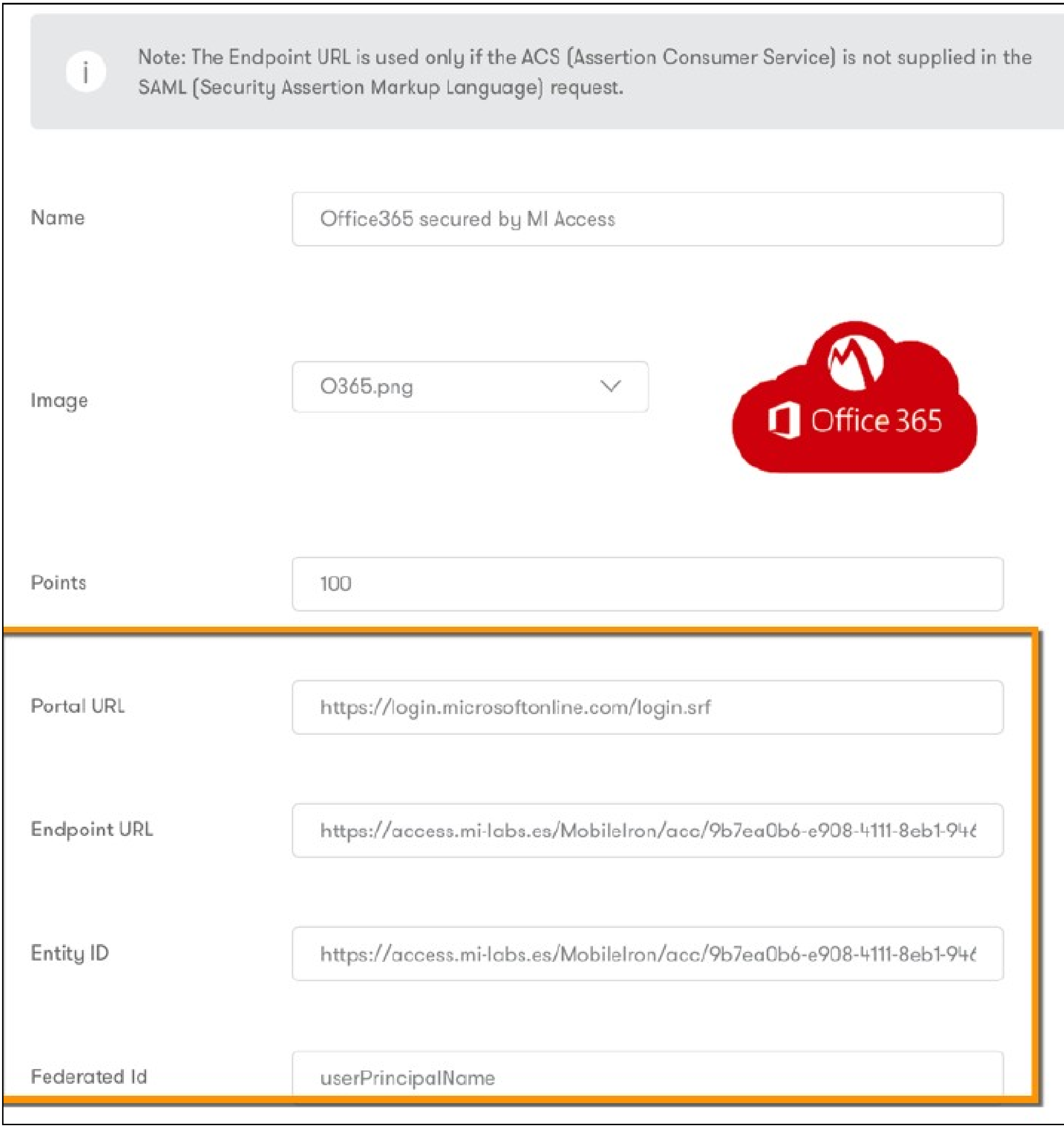
Select additional authentication methods. You must select at least one of the following methods to enable MFA:

☐ Certificate Authentication

☑ Swivel Authentication Provider

What is multi-factor authentication?

On AuthControl Sentry side, we will create an Application configuration with MI Access, IdP and Office365 endpoints:



Note: The Endpoint URL is used only if the ACS (Assertion Consumer Service) is not supplied in the SAML (Security Assertion Markup Language) request.

Name: Office365 secured by MI Access

Image: O365.png

Points: 100

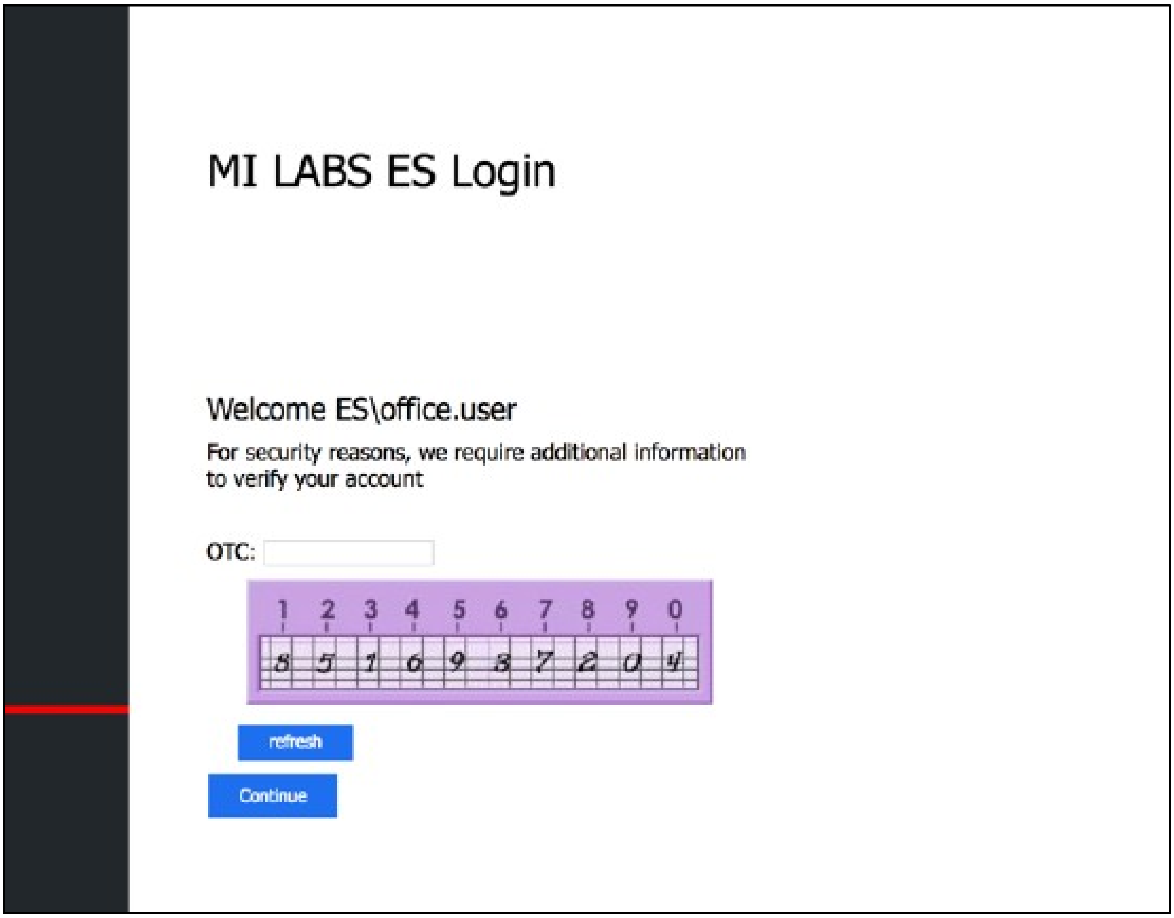
Portal URL: https://login.microsoftonline.com/login.srf

Endpoint URL: https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94

Entity ID: https://access.mi-labs.es/MobileIron/acc/9b7ea0b6-e908-4111-8eb1-94

Federated Id: userPrincipalName

This way, ADFS will require PINPAD or Turing image in order to validate and access Office365, in addition to ADFS primary authentication policy.



MI LABS ES Login

Welcome ES\office.user

For security reasons, we require additional information
to verify your account

OTC:

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

310 Related Articles

- ADFS configuration

https://kb.swivelsecure.com/w/index.php/Microsoft_ADFS_3_Authentication

311 Additional Information

For assistance in the Swivel Secure installation and configuration please firstly contact your reseller and then email Swivel Secure support at supportdesk@swivelsecure.com

312 MON Service Monitor How to guide

313 Overview

Mon can be used to monitor system processes and alert when they fail. The Swivel appliance can use MON to watch the Tomcat process, and even extended to other processes.

314 Prerequisites

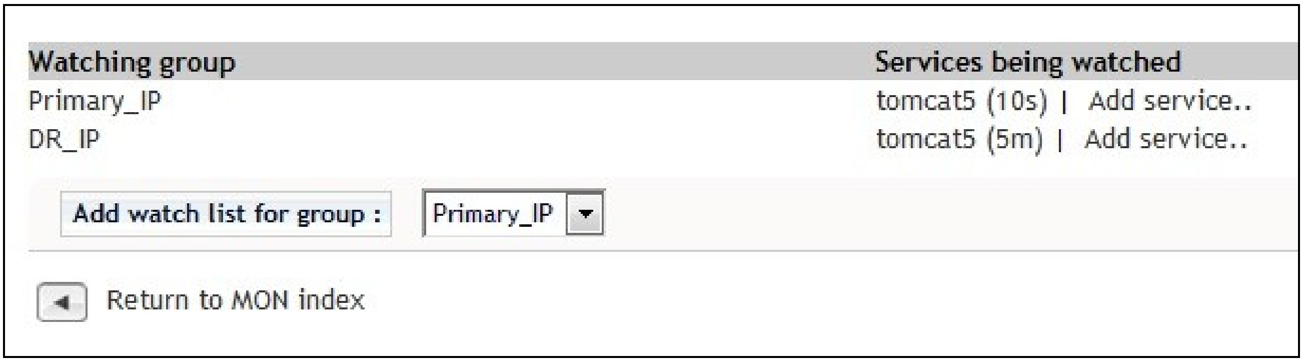
Swivel Appliance 2.x with Webmin

315 Backup the existing Mon Configuration

Before you make any changes, manually backup /etc/mon/mon.cf using WinSCP, see WinSCP How To Guide.

316 Configuring Mon

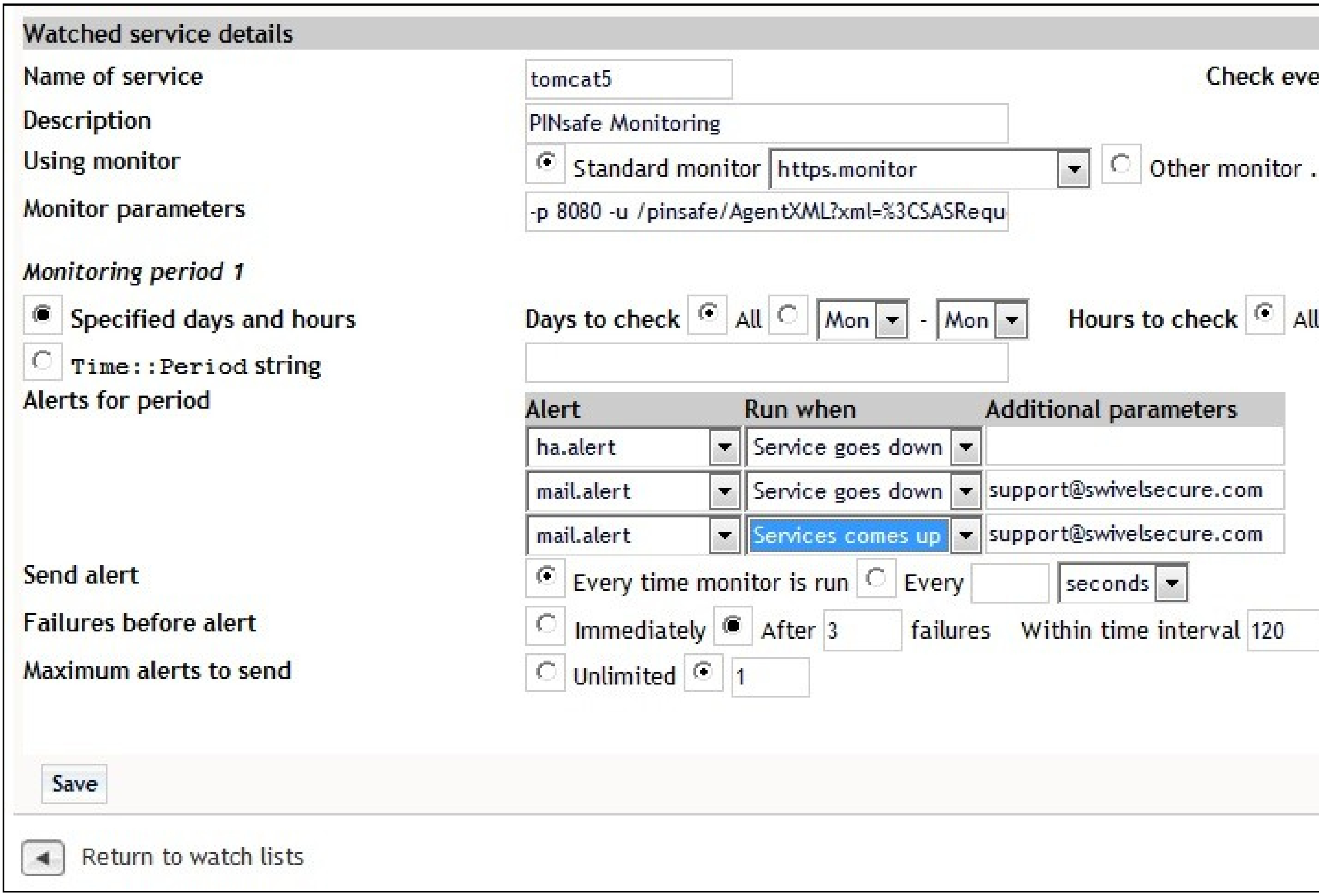
Login to Webmin (for more information see Webmin How To Guide, then select System -> MON Service Monitor/Watch Lists and against the required appliance select *tomcat5 (10s)*



Watching group	Services being watched
Primary_IP	tomcat5 (10s) | Add service..
DR_IP	tomcat5 (5m) | Add service..

Add watch list for group : Primary_IP

Under Alert, add a new alert named mail.alert from the drop down with the parameter being the email address you want to send to. Alerts can be defined on different events such as when the service stops or starts. Save the setting when complete.



Watched service details

Name of service: tomcat5

Check eve

Description: PINsafe Monitoring

Using monitor: ● Standard monitor https.monitor ○ Other monitor .

Monitor parameters: -p 8080 -u /pinsafe/AgentXML?xml=%3CSASRequ

Monitoring period 1

● Specified days and hours — Days to check ● All ○ Mon - Mon — Hours to check ● All

○ `Time::Period` string

Alerts for period

Alert	Run when	Additional parameters
ha.alert	Service goes down	
mail.alert	Service goes down	support@swivelsecure.com
mail.alert	Services comes up	support@swivelsecure.com

Send alert: ● Every time monitor is run ○ Every seconds

Failures before alert: ○ Immediately ● After 3 failures Within time interval 120

Maximum alerts to send: ○ Unlimited ● 1

317 Testing

- Stop the monitored service and verify email messages are sent.

318 Troubleshooting

At the command line enter monshow --full

Primary Example, mon working with

```
monshow --full

     server: localhost
       time: Fri Dec 19 12:48:52 2014
      state: scheduler running

  GROUP           SERVICE      STATUS      LAST       NEXT       ALERTS SUMMARY
R DR_IP           tomcat5      -           68s        00:03:51   none
R Primary_IP      tomcat5      -           6s         3s         none
```

Standby Example, mon working Primary and Standby

```
monshow --full

     server: localhost
       time: Fri Dec 19 12:51:38 2014
      state: scheduler running

  GROUP           SERVICE      STATUS      LAST       NEXT       ALERTS SUMMARY
R Standby_IP      tomcat5      -           7s         2s         none
R Primary_IP      tomcat5      -           12s        17s        none
```

Primary Example, mon in failed state:

```
Primary monshow --full

server: localhost
time Fri Dec 5 15:55:57 2014
state: scheduler running

  GROUP      SERVICE      STATUS      LAST      NEXT      ALERTS      SUMMARY
R Primary_IP tomcat5      FAIL        0s        0s        1
R DR_IP      tomcat5      FAIL        00:03:10  00:001:49 10
```

Standby Example, mon in failed state:

```
Primary monshow --full

server: localhost
time Fri Dec 5 15:55:47 2014
state: scheduler running

  GROUP      SERVICE      STATUS      LAST      NEXT      ALERTS      SUMMARY
R Standby_IP tomcat5      FAIL        5s        4s        1
R Primary_IP tomcat5      FAIL        2s        27s       1
```

318.1 SSL vulnerability updates stop Mon working

This can be resolved by editing the file /usr/local/tomcat/conf/server.xml and changing both instances of 'sslProtocols=' or 'sslProtocol=' to be 'sslEnabledProtocols=', i.e. adding Enabled. Restart Tomcat, check Tomcat is running then use monshow --full as above.

319 Move PINsafe How to Guide

320 Overview

This document outlines some of the best practices when moving a Swivel install or configuration and data from one instance, the source, to another, the destination.

321 Prerequisites

Swivel server or virtual or hardware appliance

Backup Swivel before any work is carried out

Ensure Swivel versions are the same between installations. If Swivel is to be upgraded as part of the process, verify the upgrade during testing.

Ensure that the Time zones are the same for all Swivel installations.

It may be necessary to schedule some downtime

322 Moving Swivel configuration and data from one install to another

Stop Tomcat on both old and new instances, copy the following files from the original installation to the new installation, then start Tomcat. For information on copying Swivel files on virtual or hardware appliances see Copying appliance files How to Guide.

323 Swivel File locations

323.1 Swivel 3.9.1 onwards

The Configuration and local data (Known as the Transient Data Storage), is stored in the .swivel folder, on virtual or hardware appliances this is:

/home/swivel/.swivel

On software installs this is dependant upon the installation such as c:\users\<username>\.swivel or c:\.swivel

Note this does not include java class files, such as those for transport classes or database drivers, these may need to be copied manually.

323.2 Swivel 3.9 earlier

<path to Tomcat>/webapps/pinsafe/WEB-INF/conf/config.xml

<path to Tomcat>/webapps/pinsafe/WEB-INF/conf/ranges.xml

Ensure any customisations are also copied, see Transport Configuration.

<path to Tomcat> for virtual or hardware appliances is /usr/local/tomcat.

324 Moving Swivel user data from one Swivel install to another similar install

324.1 Timezone

Determine Timezone of original Swivel installation. The new Swivel installation must be the same timezone. If you cannot login and receive errors regarding no PIN or invalid PIN, it is likely that the timezone is not that of the source.

324.2 Certificates and Keystore

A new SSL certificate can be requested for the new Swivel instance.

Another method if the hostnames are the same from the old Swivel instance and the new Swivel instance, may be to copy across the keystore. See also Moving Swivel Keystore

The keystore file location on a virtual or hardware appliance should be listed within your /usr/local/tomcat/conf/server.xml file, but the default keystore file location is:

/home/swivel/.keystore

(it's a hidden file with the '.' prefix)

The method would involve:

- Take a backup of the existing /home/swivel/.keystore file on the source and destination

- Make a note of the permissions assigned to the file, by default they are swivel:swivel 600

- Copy in the source .keystore file to the same location on the destination. See Copying appliance files How to Guide

- Run the following commands to ensure the permissions are set to their defaults:

chmod 600 /home/swivel/.keystore

chown swivel:swivel /home/swivel/.keystore

Where the source and/or destination is not a Swivel virtual or hardware appliance then the keystore password may be different and need to be set in the Tomcat server.xml file located under <path to Apache Tomcat>\conf

- Restart Tomcat

324.3 Moving from a standalone install to an Active/Active install

Swivel configuration and data can be manually setup through the administration console of the new instances or can be copied from a standalone installation to a Active/Active installation, however there are some additional considerations and settings that differ between each Active Active instance and will need to be configured separately, these include:

- Local XML repository names need to be different and contain unique usernames
- Server Name
- RADIUS Server IP where configured (usually left blank)
- Repository Sync times need to be different on the Primary Master and Standby Master
- Filter, if a filter is defined then this may need to be changed, see Filter IP How to Guide

An alternative is to copy the data and configuration to the primary and configure the standby manually.

Swivel configuration data is contained is contained within the file config.xml (see Swivel File locations above).

324.4 Exporting Databases to the Internal Swivel Database

- If the Swivel database is external and is not not being moved then the data does not need to be exported, the Swivel instance can point to the database after being moved.
- If a database external to the Swivel application is being used then the data can be copied to the internal Swivel database. As an internal Swivel database, the data can then be moved and exported to a new database or left using the internal database.
- If the database is the same type, and can be ported such as through a MySQL dump, see MySQL Database Export and Import
- For internal databases the data can be copied across to the new instance. If the destination is to be another database type then it can be Migrated at the destination (this will only need to be done once).

On the original Swivel installation, Migrate Data to internal Db. In the Swivel Administration console select Migration, and then select Internal as the target destination and enter the word "MIGRATE" to confirm migration. Note that this doesn't actually move the active database to Internal, it just makes a copy of the MySQL database in the Internal database. See also Migrate How to guide.

324.5 Moving the Internal Swivel Database

If the entire conf folder is moved then local repositories are copied across. To carry this out as a separate move then copy Swivel data in the db folder (see Swivel File locations above), to new Swivel Primary server. to do this stop Tomcat on the Swivel instance, when using the virtual or hardware appliance use the CMI to select Tomcat, then Stop. You now need to copy the database and configuration from the virtual or hardware appliance. We recommend using a tool such as WinSCP, see WinSCP How To Guide. Remember to check file and ownership permissions.

324.6 Moving the Swivel local XML Repository

If the entire conf folder is moved then local repositories are copied across. To carry this out as a separate move then stop Tomcat on source and destination then copy the repository data/repository.xml (see Swivel File locations above), from the source to the destination, then start Tomcat. Remember to check file and ownership permissions.

324.7 Importing Data on the new Swivel installation

If the data has been imported directly into a database external to the Swivel application, such as through a MySQL dump, then configure Swivel to use that database and do not Migrate the data, see MySQL Database Export and Import

Where data is to be imported from the Swivel internal database to another database, the import should only be carried out on one server, for the Swivel virtual or hardware appliance, this will be the Primary Master. Ensure that the Swivel instance is working correctly. Stop Tomcat then copy internal database the db folder (see Swivel File locations above). The Swivel instance should be configured with the database should be set to Internal, and the Mode set to Synchronised. Once the database is copied and the permissions and ownerships are verified as being correct, start Tomcat.

1. On the Swivel Administration console, under Database/General, ensure that the database configuration is set to internal and the new database configuration is correct, but keep the database as internal. For further information see MySQL Database How To Guide. Do not select an external database type such as MySQL until after Migration.

2. Migrate the data on the on destination Swivel installation to the required database. The migration should be carried out on one Swivel server only. On the Swivel virtual or hardware appliance, this should be the primary Master. On the Swivel Administration console select Migration, selecting the configured database as the target destination. Check the logs for any error messages. see also Migrate How to guide.

3. Then select the database. On the Swivel Administration console select Database/General, set the database then apply. Check logs for any error messages.

4. For Swivel virtual or hardware appliances check synchronisation is working. see MySQL Appliance Database Synchronisation

325 Testing

326 Known Issues

326.1 Troubleshooting

Exception occurred during database access, exception: com.swiveltechnologies.pinsafe.server.user.database.DatabaseException: Error opening the internal database

The permissions and/or ownership are not correctly set on the repository, see Permissions and Ownership

admin:The user "xxxxx" cannot be created as an existing user with the same name already exists.

admin:Exception occurred checking agent: com.mysql.jdbc.exceptions.MySQLIntegrityConstraintViolationException: Cannot add or update a child row: a foreign key constraint fails (`pinsafe_rep/PINSAFEJ`, CONSTRAINT `PINSAFEJ_ibfk_1` FOREIGN KEY (`I`) REFERENCES `PINSAFEL` (`A`) ON DELETE CASCADE).

This has been seen on importing internal data from the db folder from version 3.6 to 3.9.5, and them migrating to a MySQL database, and is followed by a user sync. Setting the option under Repository, to allow the user to change repository and then restarting Tomcat resolved the issue, although the logs indicated that the users had been deleted, this was not the case.

Is the timezone on the source, the same as the destination?

327 Moving Repository How to guide

328 Overview

Users may be required to move repository, such as from one AD domain to another, this details the process to handle this within Swivel.

329 Prerequisites

Swivel 3.3 or higher

330 How to Guide

330.1 Swivel 3.9

Swivel version 3.9 allows users to optionally move repository, so they will not need a new PIN number to be sent out (Swivel 3.8 and earlier deletes and creates the user)

330.2 Swivel 3.3 to 3.8

Moving repository requires the account to be moved to the new repository and Swivel will delete the user from the existing repository and create the user in the new repository. This will result in a new PIN number being generated for the user.

Create the new repository on the Swivel Server see AD Repository Server Settings, and assign the path for the groups see AD Groups. If new groups are to be created, then new transports will need to be configured.

- Move the user in AD to the new domain, removing them from the old AD group and adding them to the new AD group.
- On the Swivel primary Synchronise the old AD by selecting User Administration, and the Old AD repository
- On the Swivel primary select User Administration, and the Old AD repository then click on purge
- Under User Administration select the new AD domain then click on user Sync and the user should appear. They should be sent a new PIN number. If the user does not appear, check the logs. If there is a duplicate user entry, then the user will still be in the old Ad and will need to be purged, see above

331 Testing

Ensure users are moved to the new repository

332 Known Issues

333 Troubleshooting

334 MOXA NPort Ethernet to Serial

335 Overview

The MOXA NPort 5000 and 6000 Series device allows a Serial GSM modem to be connected to a Swivel appliance through a ethernet network connection. See also the NowSMS How to guide.

336 Prerequisites

- MOXA NPort 5000 or 6000 series device

tested with

-
    - NP5110
    - NP6150

- Serial GSM modem

- Swivel appliance v2.x
- Swivel appliance v3.x

- New version of the GSM Modem Transport class - **ModemTransport.class**. Please contact Swivel support for this, if it does not exist under /webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/transport. Since it is still under development at the time of writing this article (this is required in order to detect the new Serial Port ttyS99 from within the Swivel Core).

337 Configuring the Swivel appliance

Versions 2.0.15 appliances (not 2.0.16) have the NPort software pre-installed. Earlier versions of the appliance will need to install and then configure the appliance.

337.1 Swivel 2.0.15

These appliances have the Nport software installed, continue with configuration.

337.2 Swivel 2.0.16 appliances and Swivel 2.0.14 and earlier appliances - Nport Software Installation

This is for appliances 2.0.14 or older where the NPort software is not installed.

From the command line install the software using the following command (requires internet connectivity from the appliance.

rpm ?ivh http://yum.swivelsecure.net/files/drivers/npreal-2.1.18.1-5.i386.rpm

or locally using

rpm -ivh npreal-2.1.18-1-5.i686.rpm

Example:

```
[admin@single swivel]# rpm -ivh ./npreal-2.1.18-1.i686.rpm

Preparing...                ########################################### [100%]
   1:npreal                 ########################################### [100%]

Loading TTY Driver...
Complete.
```

338 Configure the MOXA NPort Adapter

The Official MOXA NPort User Guide - http://www.moxa.com/doc/manual/nport/5110/NPort_5110_Users_Manual_v2.pdf

338.1 Connecting the MOXA to the Network

Connect one end of the Ethernet cable to NPort's 10/100M Ethernet port and the other end of the cable to the Ethernet network. The MOXA NPort will indicate a valid connection to the Ethernet in the following ways:

- The Ethernet LED maintains a solid green colour when connected to a 100 Mbps Ethernet network.
- The Ethernet LED maintains a solid orange colour when connected to a 10 Mbps Ethernet

network.

- The Ethernet LED will flash when Ethernet packets are being transmitted or received.

The MOXA adapter are configured with the following default private IP address:

192.168.127.254

Once the adapter is connected to the network, you MUST assign it a static IP address which should be accessible by the GSM and pingable by the Swivel Appliance.

338.2 Edit the NPreal2 File

To change the remote modem IP address edit the file /etc/init.d/npreal2

The default IP used is 192.168.127.254

Edit the below line to the new Static IP

DEVICE_IP=192.168.127.254

338.3 Setting up a Virtual Serial Port in VMware

Note - You will need to power down the VM before adding a new serial port.

1. Select a virtual machine.

2. In the VM Hardware panel, click Edit Settings.

3. Click "Add..." and then Serial Port.

4. Click Next and select "Connect via Network".

5. Under Network Backing, select Client (VM initiates connection).

6. The Port URI must be the static IP address set for the MOXA adapter, with a telnet prefix and port number of 4001.

Example: telnet://192.168.0.1:4001

7. Click Finish.

338.4 Connecting to the MOXA Adapter

Plug the MOXA NPort Adpater into the GSM Modem and ensure that you can see the serial port ttyS99 from the Swivel Appliance. To confirm, please run the following commands:

```
 dmesg | grep tty
```

E.g Output ttyS99 at 0x03f8 (irq = 4) is a 16550A

OR

```
 setserial ?g /dev/ttyS99
```

338.5 Start and Stop the MOXA NPort service

The MOXA NPort service has the following commands:

To start the service

service npreal2 start

To stop the service

service npreal2 stop

Please Note: The NPreal (MOXA) service does not start automatically on boot up and has be started manually (if the Appliance has been rebooted).

Example:

```
  [admin@single ~]# service npreal2 start

  Adding Server...

  ttyr00, cur00
```

```
Added RealCom server: ip : 192.168.0.100
mknod -m 666 ttyr00 c 33 0
mknod -m 666 cur00 c 38 0
Complete.
```

Example:

```
service npreal2 stop
Delete Server ...
rm -f /dev/ttyr00
rm -f /dev/cur00
Deleted server: 192.168.0.100
Complete.
```

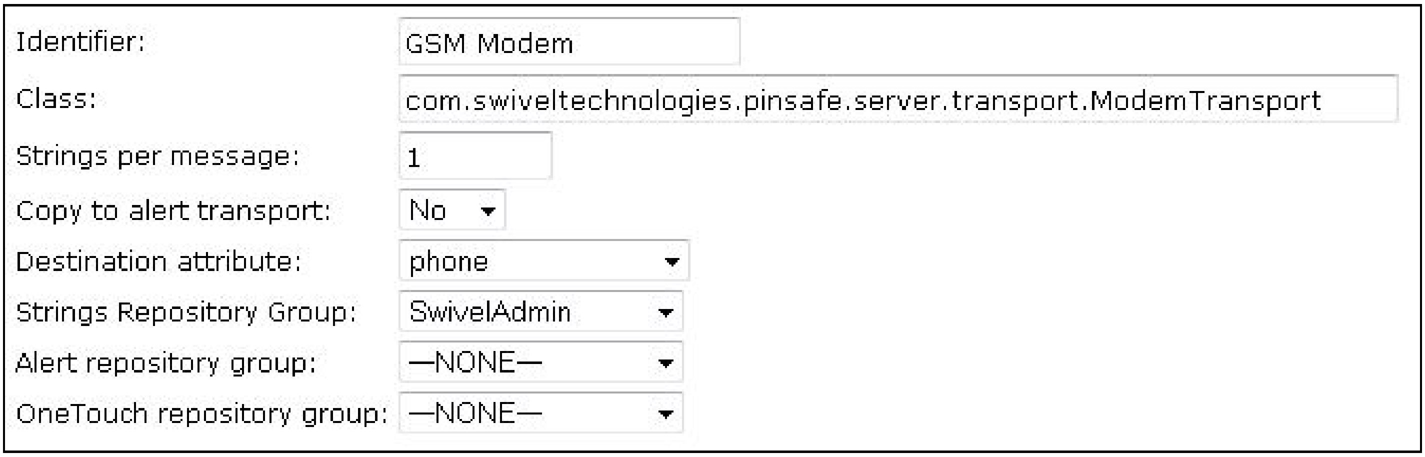
339 Configure a GSM Modem

On the Swivel Administration console configure a Swivel group to use a GSM modem. For further information on configuring transports see Transport Configuration

Destination Attribute: Ensure this is set to phone

Strings Repository group: To send security strings by SMS ensure that this is set to a group

Alert Repository Group: To send alerts by SMS ensure that this is set to a group



Identifier:	GSM Modem
Class:	com.swiveltechnologies.pinsafe.server.transport.ModemTransport
Strings per message:	1
Copy to alert transport:	No
Destination attribute:	phone
Strings Repository Group:	SwivelAdmin
Alert repository group:	—NONE—
OneTouch repository group:	—NONE—

339.1 Configure the GSM Modem Settings

On the Swivel Administration console configure the GSM modem created above

Serial Port: The serial port /dev/ttyS99 should be selectable

Bit Rate: 115200 - The Baud Rate MUST be set to 115200 and not 9600.

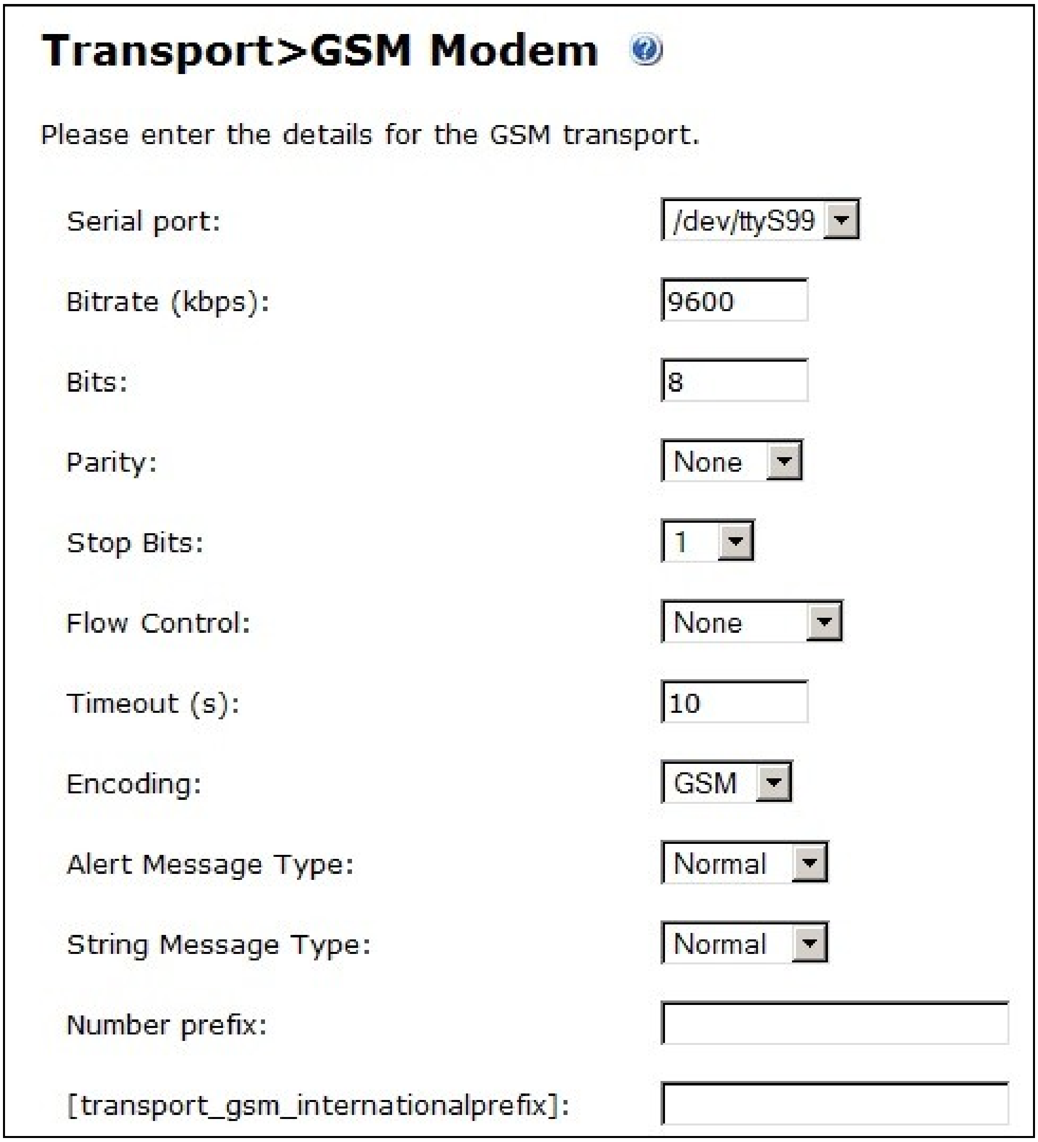
Bits: 8

Parity: None

Stop Bits: 1

Flow Control: None

These settings may need to be varied for some installation.



Transport>GSM Modem

Please enter the details for the GSM transport.

Serial port:	/dev/ttyS99 ▾
Bitrate (kbps):	9600
Bits:	8
Parity:	None ▾
Stop Bits:	1 ▾
Flow Control:	None ▾
Timeout (s):	10
Encoding:	GSM ▾
Alert Message Type:	Normal ▾
String Message Type:	Normal ▾
Number prefix:	
[transport_gsm_internationalprefix]:	

340 Testing

Send a SMS from the Swivel Appliance using minicom - please see Send a Test Message.

Also, from the User Administration screen, navigate to a User and Send String. Check in the Swivel logs and check that a SMS message has been added to the message queue and then message sent can be seen in the log.

To check if the module (driver) is loaded From the command line run the following command

lsmod | grep -i npreal2

Example:

```
lsmod | grep -i npreal2

npreal2               223556  1
```

If there is a 1, that means it's loaded.

341 Known Issues

If the GSM Modem is timing out or a Message is Added to Queue, please ensure that the Baud Rate is set to 115200 within the minicom setup and Swivel.

Please see: Minicom Setup.

The Moxa driver service must be started before Tomcat. If you have difficulty getting it working, try restarting Tomcat.

342 Troubleshooting

Can the MOXA NPort device be pinged from the Swivel appliance?

Is port 80 or 443 open to the MOXA NPort, are any ports being blocked.

Check the Swivel logs.

MODEM_EXCEPTION Port name - NONE; Method name - openPort(); Exception type - Port not found.

This is seen when a Serial Port is set to NONE under the GSM Modem Transport. It is known, if the ModemTransport.class is being used, then you may need to restart Tomcat after changing the Serial Port from NONE. Or the serial port is not set to ttyS99 within minicom.

343 Network Interface

344 Overview

This document outlines Network Interface issues and tasks.

345 Prerequisites

Swivel appliance 2.x

CMI

346 Add a third Network Interface ETH2

VM systems allow the creation of additional interfaces. Make a note of teh VM assigned MAC address to enter in the below file.

From the CMI select the Command line and change directory to /etc/sysconfig/network-scripts

```
cd /etc/sysconfig/network-scripts
```

Ensure ifcfg-eth2 does not exist

```
ls -la ifcfg-eth2
```

Create a ifcfg-eth2 by copying ifcfg-eth1

```
cp -pr ifcfg-cfg1 ifcfg-cfg2
```

Edit the file ifcfg-cfg using vi or WinSCP, see WinSCP How To Guide

Example

```
DEVICE=eth2
BOOTPROTO=static
# HWADDR=00:00:00:AA:AA:AA
IPADDR=10.0.1.27
NETMASK=255.255.255.0
ONBOOT=yes
NETWORK=10.0.1.0
TYPE=Ethernet
NOZEROCONF=YES
BROADCAST=255.255.255.255
ETHTOOL_OPTS="autoneg on"
```

Save the file and restart networking through the command line or CMI

```
service network restart
```

On Swivel appliance builds 2.0.14, the ETH2 interface should be visible and configurable in the CMI networking

347 Testing

348 Known Issues

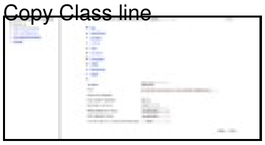
349 Troubleshooting

350 New SMTP Transport

351 Overview

Create a new SMTP Transport and use it to send security strings via email, using PINless method.

352 Images

-
  Create New Group
-
  Copy Class line
- 
  Create New SMTP entry
-
  Modify SMTP messages

353 Process

1. Create a group (SwivelEmailOTC) under Repository->Groups and link it to an AD group
2. Under Transport-General, expand the SMTP box, and copy the Class line
3. Scroll to the bottom of the page, and click New Entry
4. Give the Entry a name (OTCbySMTP)
5. Paste the class entry into the class line
6. Set Destination attribute to email
7. Set Strings Repository Group to your group name (i.e. SwivelEmailOTC)
8. Set Alert Repository Group to your group name (i.e. SwivelEmailOTC)
9. Apply
10. On right hand side menu select the name of the Entry you just made (OTCbySTMP)
11. Change any messages to meet your needs

354 Adding users, and sending email messages

Go to user admin, and select the correct repository and then user sync.

All new users in the linked AD group will receive both a welcome email, and a OTC via email. The OTC delivered will be a 6 digit code, as opposed to protected by PINsafe protocol.

355 Precautions

Before the first user sync, only have a single user in the AD group to test the process and the emails sent.

356 On Demand Authentication

356.1 Overview

On-demand authentication

This is configured under Server > Dual Channel.

Options Yes/No, Default No

Normally a dual channel message is delivered to the user following an authentication, so that they will always have a security string available to them to login. Enabling on-demand authentication disables this behaviour, requiring an explicit request for a message to be sent. The message sent this mode must be used within the session timeout (default 120 seconds see Session Cleanup) to authenticate. On demand authentication will only send one security string at a time.

Methods of making an On Demand Security String request are:

Button in a login page (see below)

As a Taskbar, see Taskbar How to Guide

RADIUS Challenge and Response, see Challenge and Response How to Guide

See Also On Demand Delivery

356.2 On Demand Authentication Dual Channel Message Request

Virtual or hardware appliance

https://pinsafe_server_ip:8443/proxy/DCMessage?username=username

Software Only Install

http://pinsafe_server_ip:8080/pinsafe/DCMessage?username=username

Where username is the name of the user to whom the dual channel message should be sent

356.3 Troubleshooting

SMS Timeout

Resolving Security String Issues

Only one security string is sent. On demand authentication will only send one security string.

357 On Demand Delivery

358 Overview

On-demand delivery

Options Yes/No, Default No

This allows a user to explicitly request a new message, for example in the event that they have lost the security string sent to them.

See Also On Demand Authentication

359 On Demand Delivery Request

Virtual or hardware appliance

https://pinsafe_server_ip:8443/proxy/DCMessage?username=username

Software Only Install

http://pinsafe_server_ip:8080/pinsafe/DCMessage?username=username

Where username is the name of the user to whom the dual channel message should be sent

359.1 Only one security string or OTC is sent

On Demand Delivery will only send one security strong or One Time Code.

360 OneTouch

361 Overview

OneTouch authentication allows a mobile device to be prompted by the Swivel server to let the user authenticate by:

- Pressing a confirm button on the mobile device screen, via a Swivel mobile application.
- Pressing # or other defined characters on phone keypad

There are two methods of authentication with OneTouch, a user can be configured to authenticate by Mobile Client or Voice but not both.

OneTouch Mobile using the Swivel Mobile Phone Client

OneTouch Voice

For other forms of authentication see: Transports How To Guide

361.1 OneTouch Videos

Swivel OneTouch Voice & Juniper

Swivel OneTouch Mobile & Juniper

361.2 Integrations

Juniper_OneTouch

VPN_OneTouch_Integration

361.3 Technical explanation

1) User goes to authenticate, enters their username and password.

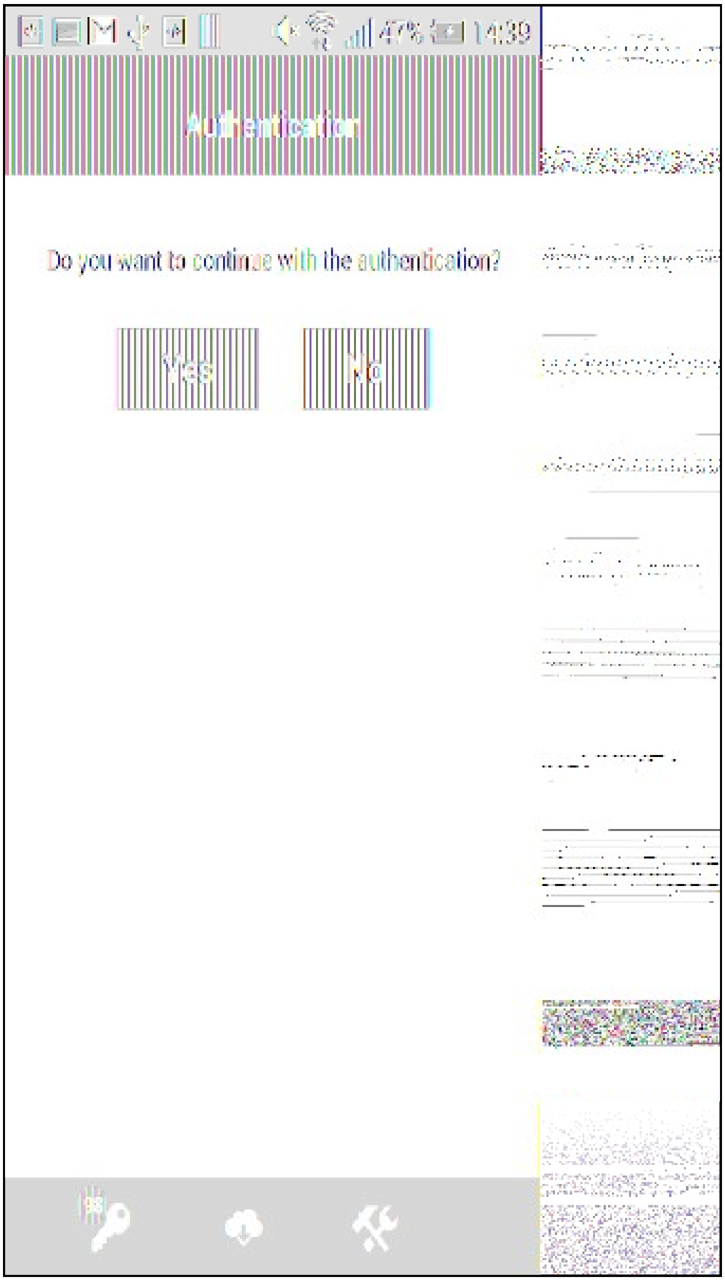
2) The login page requests a push message (or telephone call) to be sent to the user, the login page receives a unique session id as the response.

3) The user receives the message/call and responds via a single keypress on the mobile phone client or via the telephone keypad to validate the authentication

4) The login page detects that the user has responded and the login form is submitted with the session ID

5) The core platform cross references the session id with the user?s response to allow the authentication

OneTouch login screen



For configuration of the OneTouch please see the relevant links above.

361.3.1 VPN explanation

The VPN mode works slightly differently

1) The user goes to the VPN Login page

2) The modified VPN page detects that the user has not instigated a push message or call and redirects the user to a OneTouch Login Page

3) The user supplies and requests a push message, the login form stores the SessionID in the password field

4) When the OneTouch form detects that the user has responded to the push, it redirects the user back to the VPN login page passing the username and sesionid as parameters

5) The login page populates the login page form with the username and session id and submits the form

6) The VPN submits the username and session id via RADIUS to the Swivel Core for verification.

7) User gains access

Refer to VPN_OneTouch_Integrationfor sample implementation

362 OneTouch Demo Application

363 Overview

This document outlines the installation and configuration of the Swivel OneTouch Demo application. The application is designed to be installed withing a Tomcat Webappss folder such as the webapps2 on a Swivel appliance.

364 Prerequisites

Download the software from Downloads

Ensure the Latest version of the Swivel Appliance Proxy is installed from Downloads

365 Swivel OneTouch Demo Application Installation

Copy the war file to the /webapps2 folder on a Swivel appliance. It should automatically deploy and create a folder.

365.1 Swivel OneTouch Demo Application Installation

To configure the parameters to point to the Core and/or Proxy it?s necessary to modify the file usr/local/tomcat/webapps2/onetouch/WEB-INF/classes/settings.properties

The following configuration will allow access to a local Swivel instance.

```
pinsafessl=false

pinsafeserver=127.0.0.1

pinsafecontext=pinsafe

pinsafesecret=secret

pinsafeport=8181

imagessl=true

imageserver=your.swivel.public.DNS

imagecontext=proxy

imageport=8443

selfsigned=true

vpnHomeURLFor2Stages=https://your.vpn.public.DNS/onetouch2stages

timeoutPolling=60000
```

vpnHomeURLFor2Stages is used on the authentication with 2 stages.

timeoutPolling indicates the maximum time that the One Touch login page will wait for OTC Core response. This time is in milliseconds.

365.2 Swivel Core Configuration

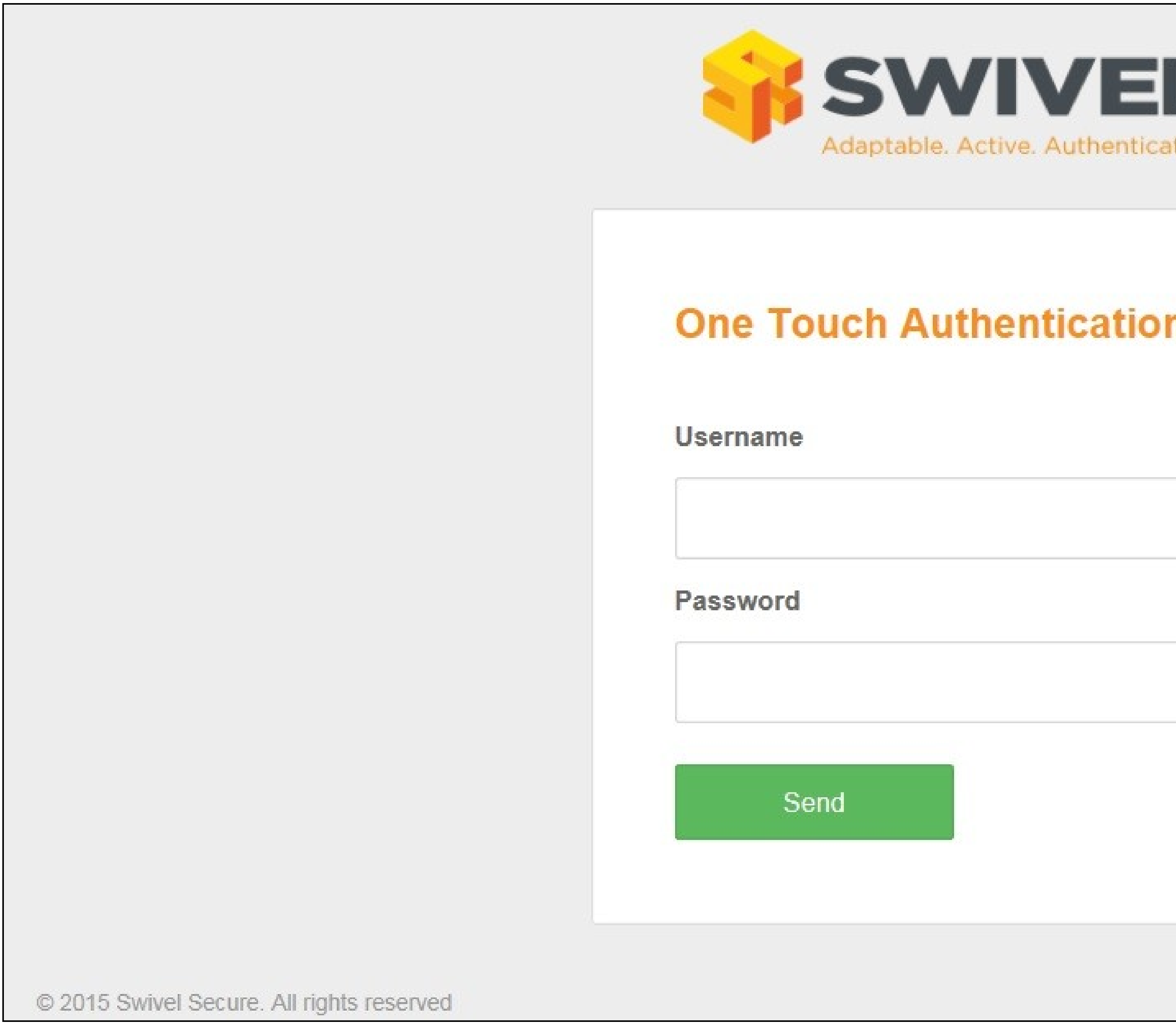
For the 2 stage authentication with RADIUS one needs to define a new challenge. Create the file and add the following in the file /home/swivel/.swivel/conf/radius-challenges.txt

With the contents:

```
Name-One touch-group, identifier of the challenge on Juniper, 0
```

366 Testing

Browsing to the One Touch application https://OneTouch_URL:8443/onetouch should present a login page as below.



SWIVEL
Adaptable. Active. Authenticat
One Touch Authenticatio
Username
Password
Send
© 2015 Swivel Secure. All rights reserved

367 Known Issues

368 Troubleshooting

369 OneTouch Mobile

370 Overview

OneTouch authentication allows a mobile device to be prompted by the Swivel server to let the user authenticate by pressing a confirm button on the mobile device screen, via a Swivel mobile application.

For other forms of authentication see: Transports How To Guide and OneTouch Voice

371 Prerequisites

Swivel 3.10.4 onwards

Swivel Mobile Phone Client Version 2.1.2 for One Touch Mobile client based solution.

Latest version of the Swivel Appliance Proxy available from Downloads

Swivel Server Details SSD for mobile client with OneTouch Push enabled

372 Swivel SSD Configuration

Swivel Mobile Phone Client must be configured to obtain its details from the Swivel SSD. For the configuration options see SSD.

373 Swivel core configuration

In order for a user to receive the OneTouch Mobile push message they must be allocated the right to use the OneTouch mode of operation. This is done by ensuring that they are a member of a group that has this right.

In addition they must be in a group associated with an OneTouch transport. The transport must be the PNA (push notification authentication) Transport for OneTouch Mobile client users.

OneTouch Mobile client users must install the Swivel Mobile Phone Client from the app store.

373.1 Configuring Dual Channel settings

On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set **On-Demand Delivery:** to Yes

Set **Allow message request by Username:** to Yes

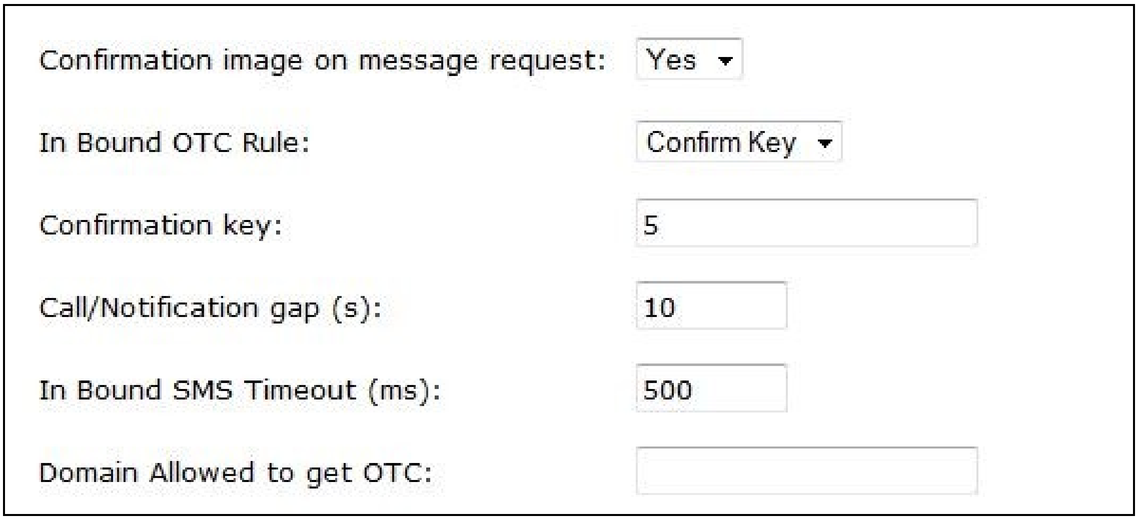
In Bound OTC Rule:

- Confirm key - enter the digits defined under Confirm Key to authenticate, example: if 1234 is entered then confirm by entering 1234 on the telephone keypad. OneTouch Mobile client solution currently only supports the confirm key mode of operation

Confirmation key: (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication

Call/Notification gap(s) (may be shown as [server_dualchannel_inboundcallgap]):

Domain Allowed to get OTC: Indicates the domain (e.g. http://localhost:8080, http://domain) authorized to get OTC. That is used by 2 way transport like OneTouch Voice telephone or OneTouch Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. Userportal, Juniper, ...). If the value is * it will allow all the domains.

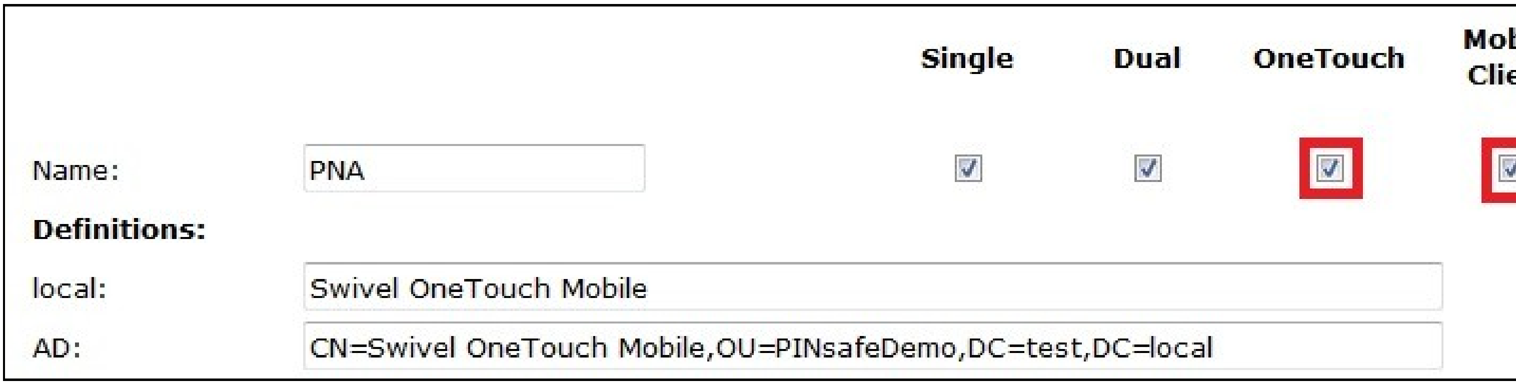


Confirmation image on message request:	Yes
In Bound OTC Rule:	Confirm Key
Confirmation key:	5
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500
Domain Allowed to get OTC:	

373.2 Define a group of OneTouch Users

On the Swivel Administration console, select a group of users that will be using OneTouch authentication and ensure that the OneTouch box is ticked then click Apply.

373.2.1 OneTouch Mobile Users



		Single	Dual	OneTouch	Mob Clie
Name:	PNA	☑	☑	☑	☑

Definitions:

local: Swivel OneTouch Mobile

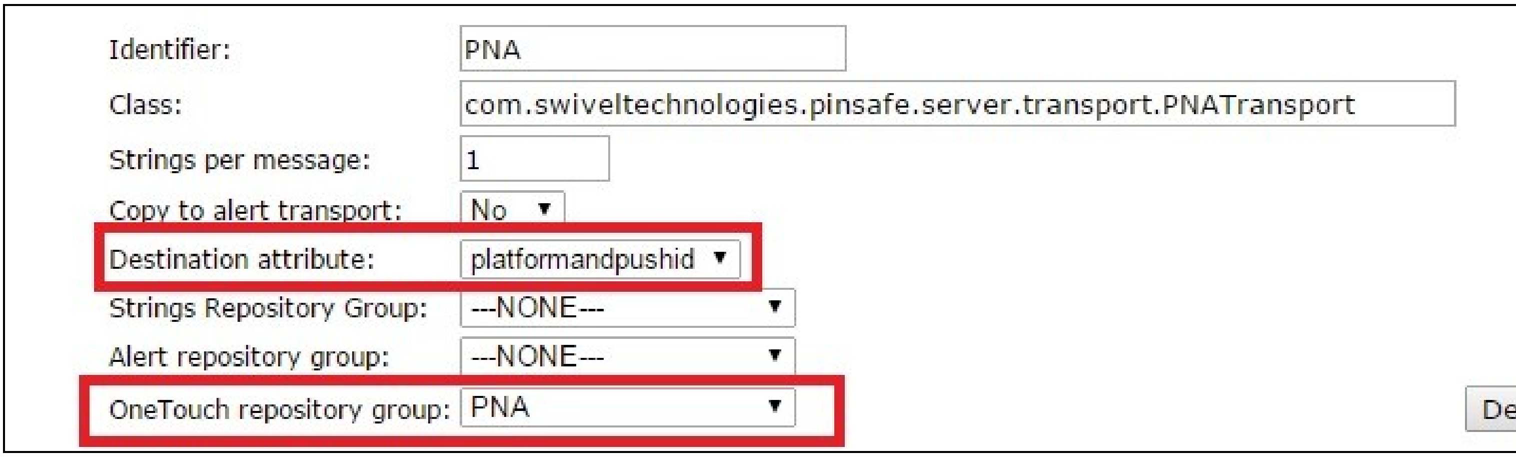
AD: CN=Swivel OneTouch Mobile,OU=PINsafeDemo,DC=test,DC=local

373.3 Define a OneTouch Transport

On the Swivel Administration console, select or create a OneTouch Transport

For OneTouch Mobile Client this will be the PNA (push notification authentication) Transport

373.3.1 One Touch Mobile Client Transport



Identifier:	PNA
Class:	com.swiveltechnologies.pinsafe.server.transport.PNATransport
Strings per message:	1
Copy to alert transport:	No ▼
Destination attribute:	platformandpushid ▼
Strings Repository Group:	---NONE--- ▼
Alert repository group:	---NONE--- ▼
OneTouch repository group:	PNA ▼

373.4 Configure OneTouch Transports

373.4.1 Configure a One Touch Mobile Client (PNA) Transport

The PNA (push notification authentication) Transport is preconfigured, no configuration changes are required unless requested by Swivel support

Timeout (ms): default 30000. Notification timeout. If the notification is pressed or arrives after the specified time, a message will be shown to the user to indicate that the Authentication Request has expired. 0 is no Timeout.

Notification title: Text displayed on the device notification.

Notification body: Text displayed on the authentication screen of the Swivel Mobile App.

iOS cert password: iOS certificate password which should correspond with the kind of certificate that is being used: production or development. The certificate used will depend of the attribute 'Production environment'.

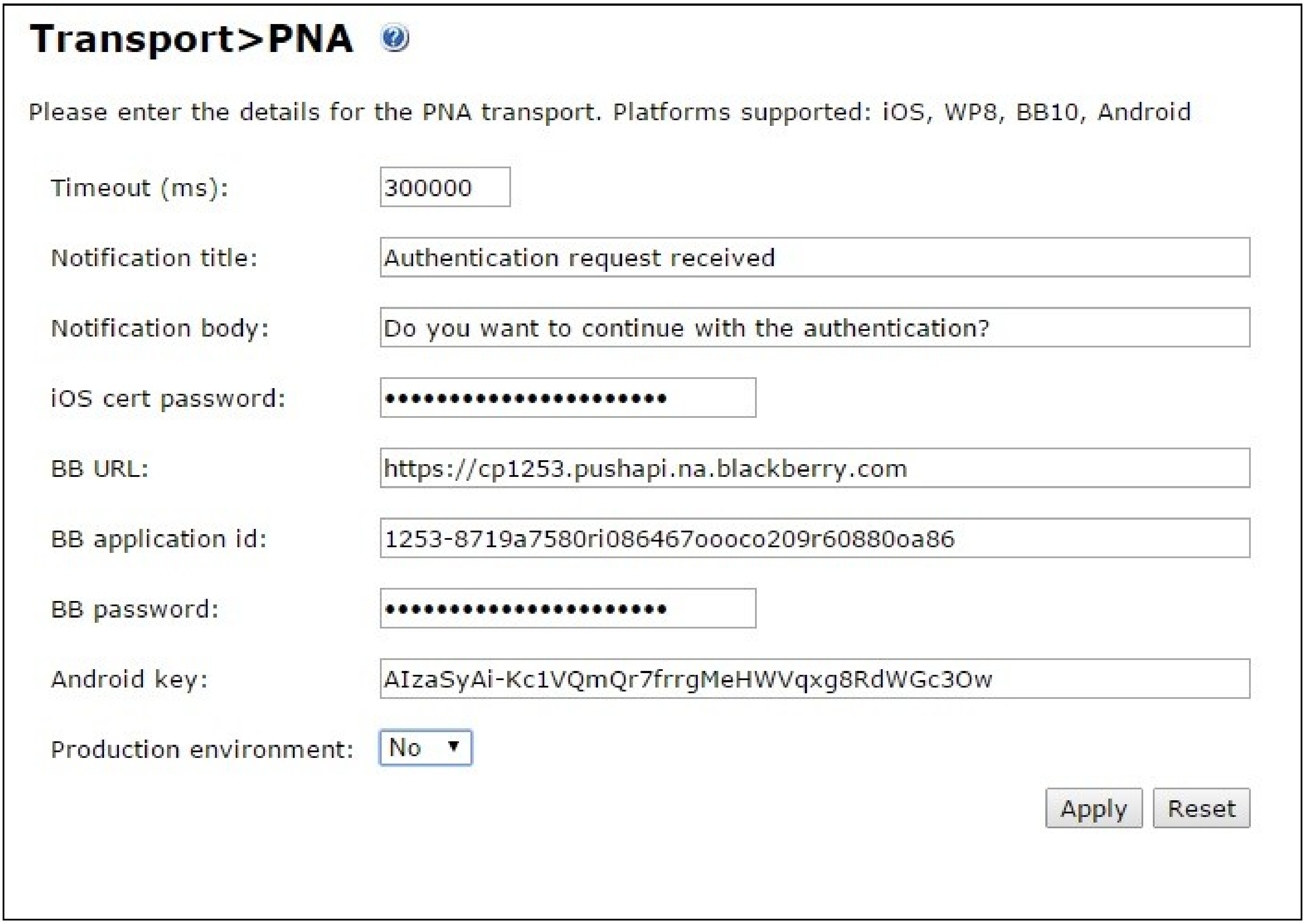
BB URL: Push URL for BB10 Swivel Mobile App.

BB application id: BB10 Swivel Mobile App's identifier.

BB password: Push password for BB.

Android key: Key related with the Swivel Mobile app used.

Production environment: Indicates if the current environment is development or production. Depending of this value the certificate used to send the notification to the device will be the production one or the development one.



Transport>PNA

Please enter the details for the PNA transport. Platforms supported: iOS, WP8, BB10, Android

Timeout (ms):	300000
Notification title:	Authentication request received
Notification body:	Do you want to continue with the authentication?
iOS cert password:	••••••••••••••••••••••
BB URL:	https://cp1253.pushapi.na.blackberry.com
BB application id:	1253-8719a7580ri086467oooco209r60880oa86
BB password:	••••••••••••••••••••••
Android key:	AIzaSyAi-Kc1VQmQr7frrgMeHWVqxg8RdWGc3Ow
Production environment:	No ▾

374 Testing

The Swivel OneTouch can be configured to work with a test authentication page available for download.

374.1 Configuring the Test Page

Edit the userportal/js/ajax.js file and make sure the top line has the serverContext variable set

var serverContext = https://localhost:8080/pinsafe

If it is installed on a different server then a Hostname or IP address will need to be specified. If HTTP is used instead of HTTPS then this may need to be changed.

374.2 Integrating OneTouch

The OneTouch Mobile can be initiated in much the same way as the sending of an SMS message.

The login page needs to start an authentication session then include a GET request to TCImageCall servlet passing in the session ID. This generates the call.

The login page can also include logic to detect when the core platform has received the user?s response.

Once the user response has been received the form can be submitted, using the sessionID as the users? one-time code.

An example OneTouch login page is available for Juniper.

374.2.1 VPN Integration

As it may not be possible to perform some of the stages of the integration within the constraints of a VPN login page, we have developed a different approach for OneTouch integration with VPNs.

Rather than creating a login page that handles the authentication we have created a custom VPN login page that redirects the user to a different server that hosts the OneTouch login page.

The user enters their username and password on this page and this page requests the push-message/call. When this page detects that the user has responded it redirects the user back to the VPN login page, complete with username, password and session ID. The modified login page automatically submits the form and the authentication then proceeds.

375 Known Issues

376 Troubleshooting

Check the Swivel logs for error messages

376.1 Error Messages

Calling or sending notification to user "onetouch" failed, error: The transport destination is empty.

This error can be seen where the user is authenticationg with the PNA and if the Mobile device has not been provisioned.

Authentication failure. Please Reprovision the device

The mobile device needs to be provisioned.

The authentication request expired

The authentication request took too long to reach the Mobile Client and is no longer valid. A large time difference between the mobile client and the Swivel server can cause this error. To increase the value, change the PNA Transport *Timeout (ms):* to a larger value or to 0 to prevent timeout.

PNA user id error

The wrong User is associated with the Provisioned mobile device. Provision with the correct user.

Calling or sending notification to user "gfield" failed, error: The transport destination is empty.

This can be caused wherethe SSD has a value of false for **Push**. To allow OneTouch Mobile this value needs to be true. To check this, verify on the Swivel Administration Console User Administration, View by Attributes to see **platformandpushid**.

377 OneTouch Voice

378 Overview

OneTouch Voice authentication allows a mobile device to be called by the Swivel server to let the user authenticate by:

- Entering the OTC on the same on the telephone keypad and in the login
- Entering the OTC comes only on the phone
- Pressing the Confirm key(s) example: if # is entered then confirm by entering # on the telephone keypad.

For other forms of authentication see: Transports How To Guide and OneTouch Mobile uing the Swivel Mobile Phone Client

379 Prerequisites

Swivel 3.10.4 onwards

Nexmo Account (or other Telephony provider) for OneTouch Voice telephone-based solution.

380 Swivel configuration

In order for a user to receive the OneTouch Voice telephone call they must be allocated the right to use the OneTouch mode of operation. This is done by ensuring that they are a member of a group that has this right. In addition they must be in a group associated with an OneTouch transport.

The transport must be a suitable telephony based transport (eg Nexmo) for the the telephone call based approach.

380.1 Configuring Dual Channel settings

On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set **On-Demand Delivery:** to Yes

Set **Allow message request by Username:** to Yes

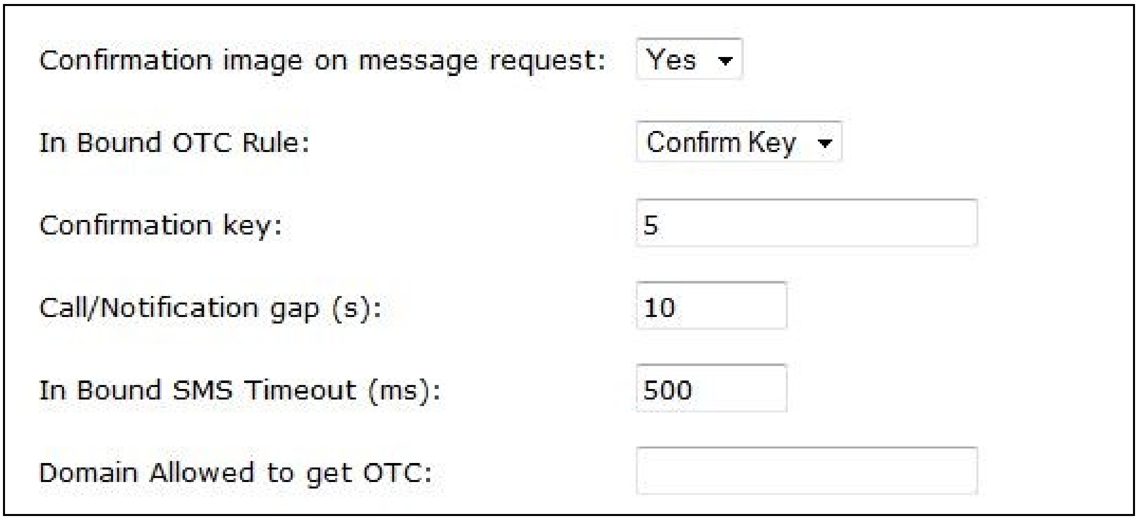
In Bound OTC Rule:

- None - No inbound
- Match - Must be the same on the telephone keypad as in the login
- Message - OTC comes from phone only
- Confirm key - enter the digits defined under Confirm Key to authenticate, example: if 1234 is entered then confirm by entering 1234 on the telephone keypad.

Confirmation key: (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication

Call/Notification gap(s) (may be shown as [server_dualchannel_inboundcallgap]):

Domain Allowed to get OTC: Indicates the domain (e.g. http://localhost:8080, http://domain) authorized to get OTC. That is used by 2 way transport like OneTouch Voice telephone or OneTouch Mobile PNA (push notification authentication). The domain will correspond with the domain client (e.g. Userportal, Juniper, ...). If the value is * it will allow all the domains.



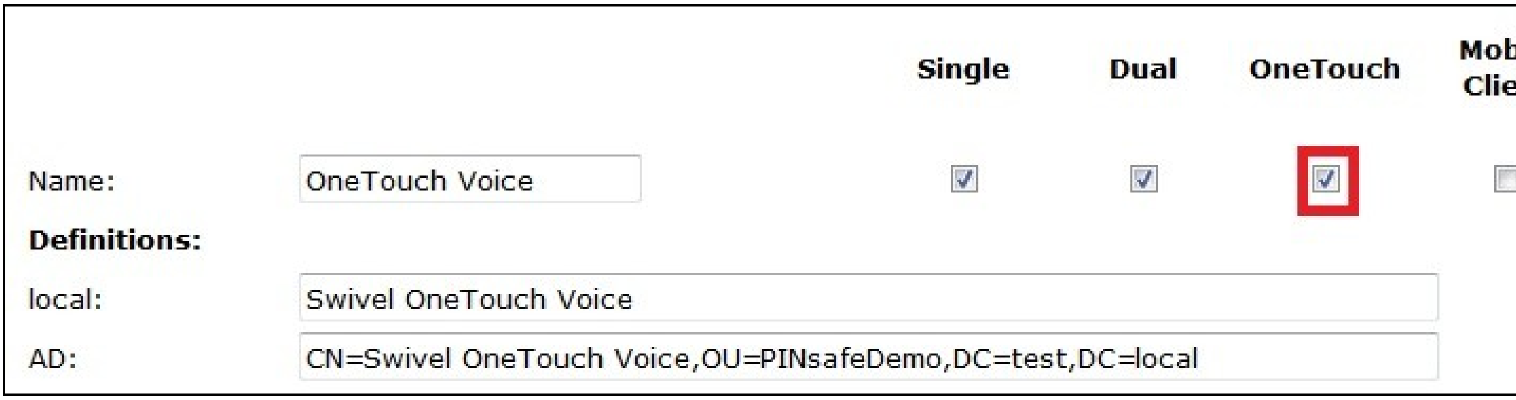
Confirmation image on message request:	Yes
In Bound OTC Rule:	Confirm Key
Confirmation key:	5
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500
Domain Allowed to get OTC:	

NOTE: The Server -> Voice Channel page is not required any more. The options on this page are replaced by the Dual Channel and NexmoVoice options.

380.2 Define a group of OneTouch Users

On the Swivel Administration console, select a group of users that will be using OneTouch authentication and ensure that the OneTouch box is ticked then click Apply.

380.2.1 OneTouch Voice Users



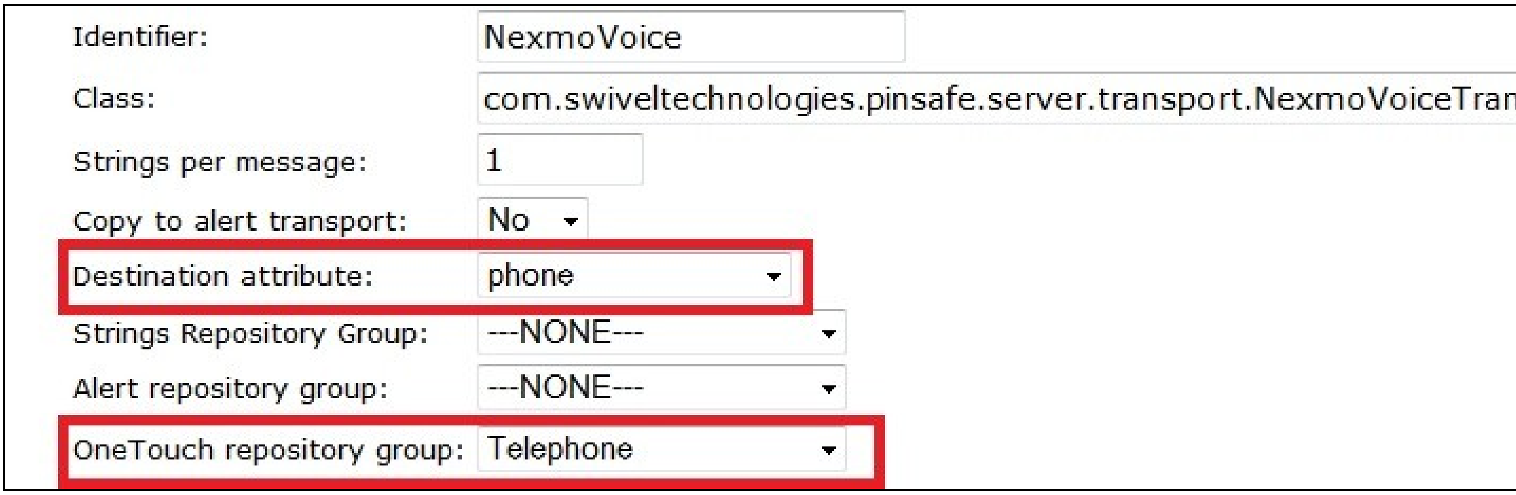
		Single	Dual	OneTouch	Mob Clie
Name:	OneTouch Voice	☑	☑	☑	□
Definitions:					
local:	Swivel OneTouch Voice				
AD:	CN=Swivel OneTouch Voice,OU=PINsafeDemo,DC=test,DC=local				

380.3 Define a OneTouch Transport

On the Swivel Administration console, select or create a OneTouch Transport

For OneTouch Voice this will be a telephopny proivder such as NexmoVoice

380.3.1 One Touch Voice Transport



Identifier:	NexmoVoice
Class:	com.swiveltechnologies.pinsafe.server.transport.NexmoVoiceTran
Strings per message:	1
Copy to alert transport:	No
Destination attribute:	phone
Strings Repository Group:	---NONE---
Alert repository group:	---NONE---
OneTouch repository group:	Telephone

380.4 Configure OneTouch Transports

380.4.1 Configure a One Touch Voice Transport

HTTP Timeout (ms): default: 180000

Enter a prompt: default: Enter your one-time code:bye

Message URL: set to: https://api.nexmo.com/tts/xml

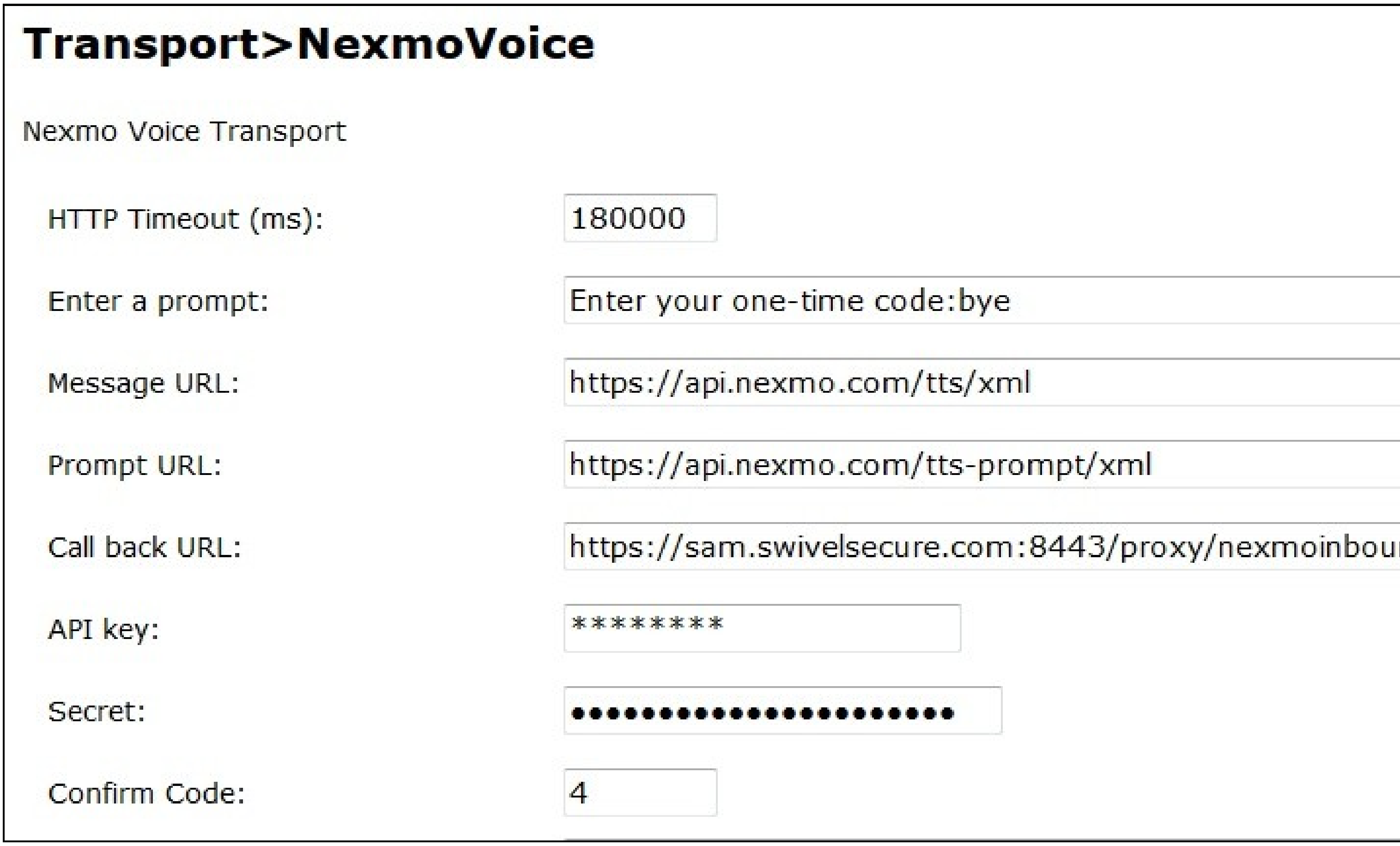
Prompt URL: set to: https://api.nexmo.com/tts-prompt/xml

Call back URL: set to: https://your_url:8443/proxy/nexmoinbound

API key: Your Nexmo account API key

Secret: Your Nexmo account secret

Confirm Code: default: 4



Transport>NexmoVoice

Nexmo Voice Transport

HTTP Timeout (ms):	180000
Enter a prompt:	Enter your one-time code:bye
Message URL:	https://api.nexmo.com/tts/xml
Prompt URL:	https://api.nexmo.com/tts-prompt/xml
Call back URL:	https://sam.swivelsecure.com:8443/proxy/nexmoinbou
API key:	*********
Secret:	●●●●●●●●●●●●●●●●●●●●●●●
Confirm Code:	4

381 Testing

The Swivel OneTouch can be configured to work with a test authentication page available for download.

381.1 Configuring the Test Page

Edit the userportal/js/ajax.js file and make sure the top line has the serverContext variable set

var serverContext = https://localhost:8080/pinsafe

If it is installed on a different server then a Hostname or IP address will need to be specified. If HTTP is used instead of HTTPS then this may need to be changed.

381.2 Integrating OneTouch

The OneTouch Voice telephone call can be initiated in much the same way as the sending of an SMS message.

The login page needs to start an authentication session then include a GET request to TCImageCall servlet passing in the session ID. This generates the call.

The login page can also include logic to detect when the core platform has received the user?s response.

Once the user response has been received the form can be submitted, using the sessionID as the users? one-time code.

An example OneTouch login page is available for Juniper.

381.2.1 VPN Integration

As it may not be possible to perform some of the stages of the integration within the constraints of a VPN login page, we have developed a different approach for OneTouch integration with VPNs.

Rather than creating a login page that handles the authentication we have created a custom VPN login page that redirects the user to a different server that hosts the OneTouch login page.

The user enters their username and password on this page and this page requests the push-message/call. When this page detects that the user has responded it redirects the user back to the VPN login page, complete with username, password and session ID. The modified login page automatically submits the form and the authentication then proceeds.

382 Known Issues

383 Troubleshooting

Check the Swivel logs for error messages

Try with the country code

If a phone number is not receving calls, check the Swivel logs

Nexmo have a number of error Codes on their website which may be returned: What are Nexmo delivery error codes?

383.1 Error Messages

Calling or sending notification to user "onetouch" failed, error: The transport destination is empty.

This error can be seen where the user is authenticationg with the PNA and if the Mobile device has not been provisioned.

NEXMO_ERROR <?xml version="1.0" encoding="UTF-8"?> <response> <call_id /> <to /> <status>17</status> <error_text>Cannot route the call</error_text> </response>

The telephone number may be in the wrong format such as no country code etc.

More than one user was found with the attribute "phone" = "1234567890123"

Ensure that the telephone number is unique.

384 OpenManage

385 Overview

OpenManage is a set of tools on the Swivel Dell Hardware Appliances from appliance version 2.0.10 onwards. OpenManage uses port 1311.

386 Prerequisites

Swivel Hardware appliance 2.0.10 onwards.

387 How to Disable OpenManage

from the command line run;

```
/opt/dell/srvadmin/sbin/srvadmin-services.sh disable
```

388 Testing

389 Known Issues

390 Troubleshooting

391 OTC

392 Overview

A One Time Code (OTC) is a password or passcode that can be used once for authentication. After it is used it cannot be used a second time for authentication, and a new One Time Code must be supplied.

393 Prerequisites

Swivel Authentication server

394 Testing

Enter the OTC and verify that an incorrect OTC fails an authentication.

395 Known Issues

396 Troubleshooting

397 Password change for CMI How to Guide

397.1 Overview

PINsafe uses a default username and password for the Command Management Interface (CMI) and it is recommended to change this password. This document outlines how and where to change the Password Credentials on the CMI. See Also Password change for Webmin How to Guide

397.2 Prerequisites

PINsafe 3.x

PINsafe appliance with CMI

Ensure a copy of the password is held in a secure location.

397.3 Changing CMI Password

397.3.1 Password Change for User

On the PINsafe CMI select the Advanced Options, then Admin Menu, then change admin password. Enter the new password and then again to confirm it is correct.

397.4 Testing

Login as user admin with the new password.

397.5 Known Issues

397.6 Troubleshooting

Try entering the password as the username so that the entered characters can be viewed, this will reveal if the keyboard mapping is not as expected.

Try a login through the hardware monitor console or VM console, as well as through an SSH session.

It is possible to reset the admin back to its default by the following precedure Password recovery for appliance How to guide

398 Password change for Webmin How to Guide

398.1 Overview

PINsafe uses a default username and password for the Webmin Interface and it is recommended to change this password. This document outlines how and where to change the Password Credentials on the Webmin. See Also Password change for CMI How to Guide

398.2 Prerequisites

PINsafe 3.x

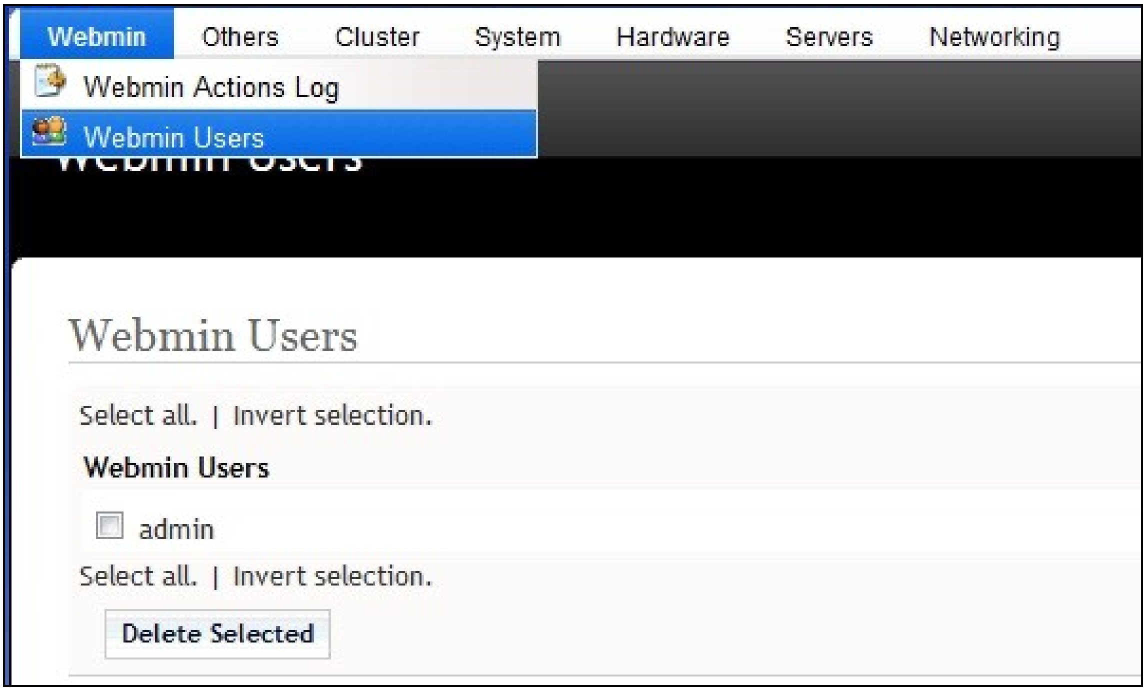
PINsafe appliance with webmin

Ensure a copy of the password is held in a secure location.

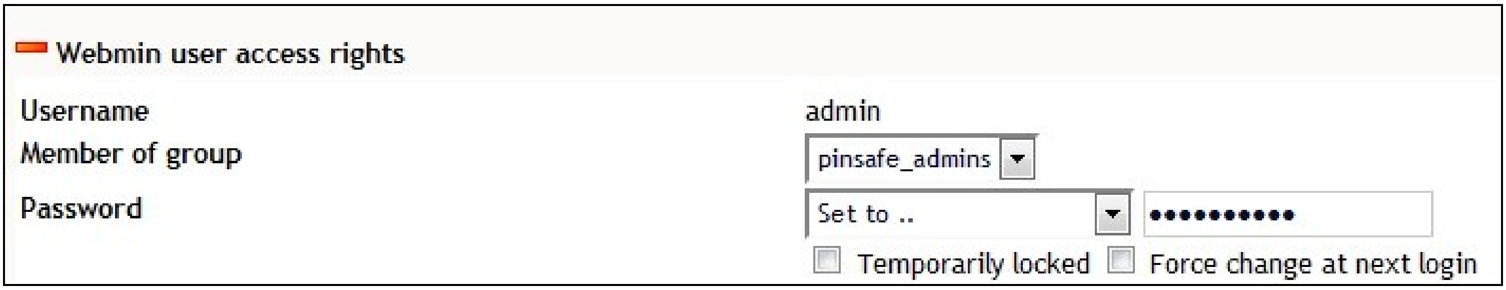
398.3 Changing Webmin Password

398.3.1 Password Change for User

On the PINsafe Webmin/Webmin Users, click on the required user i.e. admin.



On the Password menu change the value from *Don't Change* to *Set to* and enter a new password. Click on Save to make the password change.



Webmin user access rights

Username	admin
Member of group	pinsafe_admins
Password	Set to .. ●●●●●●●●●●●
	□ Temporarily locked □ Force change at next login

398.4 Testing

Login as user webmin with the new password.

398.5 Known Issues

398.6 Troubleshooting

399 Password How to Guide

400 Overview

Swivel can use a static password in addition to a One Time Code. The static password may be used to make shoulder surfing techniques less effective, since it will be difficult to discern password from OTC, as well as its length. When a Swivel password is set for a user, it must be used.

401 Passwords

There are two types of password that Swivel can use in addition to the One Time Code:

1. A Swivel password, set on the Swivel server. If a Swivel password is set, then it must be used for all Swivel authentications.

2. A Repository password, defined on the repository such as AD or LDAP. This is used with the 'Check password with repository' option on the Swivel server under Policy/Password or Authenticate non-user with just password under RADIUS NAS.

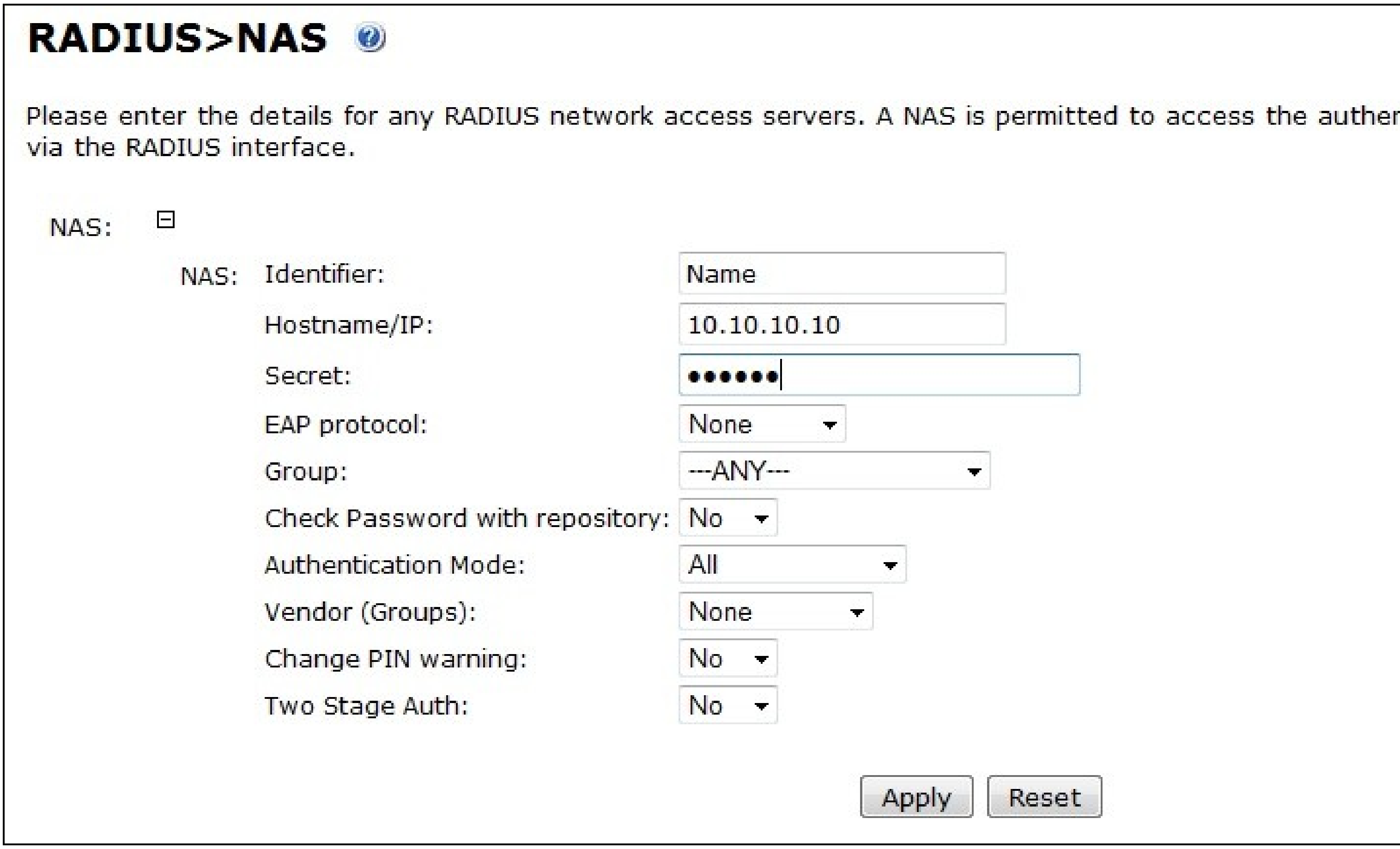
401.1 Check password with repository

From Swivel 3.8 onwards the option for Check Password with Repository is applied for an agent or RADIUS NAS entry, see RADIUS How To Guide and Agents How to Guide.

For Swivel versions prior to Swivel 3.8, the Check Password with Repository is a global option located under Policy then Password.

When this option is selected the user must enter their password with their OTC. If the password is an external repository such as AD, then they must enter their AD password. If there is a Swivel password then this must be entered. If the Swivel password is not set, then the field should be left empty, see below.

Note: For Active Directory (see AD data source configuration) and LDAP (see LDAP How to Guide) the username must be passed as username@domain in order to authenticate via LDAP. This can be specified by using the the administrator or service account username for the repository configuration as administrator@domain.name, rather than just administrator or service account username, Swivel will automatically append the domain to the username when authenticating, if one is not specified.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: ⊟

NAS:	Identifier:	Name
	Hostname/IP:	10.10.10.10
	Secret:	••••••
	EAP protocol:	None
	Group:	---ANY---
	Check Password with repository:	No
	Authentication Mode:	All
	Vendor (Groups):	None
	Change PIN warning:	No
	Two Stage Auth:	No

401.1.1 Check Password with Repository with local users

The local XML repository uses the repository.xml file as a repository, so a password cannot be set for the XML repository data source unless manually edited.

It is possible to set a password for the user in the data store and if the *Check password with repository* is set to No, it will check the password for that user.

When Check password with repository is used the Reset Password option is greyed out in some versions and not selectable, since there is no XML repository data source password.

401.2 Authenticate non-user with just password

This setting under RADIUS NAS allows a external Repository to be checked for a password when the user is not a Swivel user, See RADIUS How To Guide. The server to be used is configured under Repository/Servers with the setting **Server to use to attempt to authenticate non-users:**. See also RADIUS Static Password.

402 Swivel Password

The Swivel password can be set in a number of ways:

- On the Swivel administration console. See Reset Password
- Automatically generated at account creation time
- Set using Change PIN, see ChangePIN How to Guide
- Imported from the data repository source as a password attribute

402.1 Swivel Password settings

The Swivel password is configured on the Swivel Administration console under Policy/Pasword, the available settings are:

Require password: , default No, Options Yes/No. If set to Yes then the user is required to have a Swivel password, a password is created for the user if credentials are automatically created for the user.

Password mask: , default adsxxx. This is the password requirements for creation and automatic generation of a password. The following parameters are used for the creation or as a password requirement:

a alpha character a-Z,

d decimal 0-9,

s special character such as !"£$%^&*()-_=+,

x a random character also defining password length.

403 External Repository Password

Swivel does not know what this password is and cannot change it. However Swivel can check if a password entered by the user is correct by making an LDAP bind against the AD or LDAP server. This is used with the 'Check password with repository' option on the Swivel server under Policy/Password.

Note: When using Check Password with Repository and RADIUS is being used, then the RADIUS authentication method must be set to PAP. CHAP, MSCHAP and MSCHAP v2 will not work. See RADIUS How To Guide

Note: the local XML Repository does not have a password, passwords that are set, are entered into the Swivel Data Store.

404 Where do I use the Passwords

There is a large degree of flexibility in the configuration of how a password can be used, and can be adapted to suit certain environments thus the password to be used varies with each deployment. Below are the common use cases.

1. An Access device may have a single RADIUS field defined for authentication, in which case the password, is configured with the One Time Code in the format:

```
Password Field:  passwordOTC
```

2. Where Swivel is defined as a secondary authentication server, it is usual to have the LDAP or AD server defined as the Primary password field, usually to enable sign on to AD/LDAP resources, and the Swivel field used just for a One Time Code.

```
Primary Password Field 1:  AD or LDAP Password
Secondary Password Field 2:  OTC
```

3. Where the 'Check password with repository' option is used then the password is entered with the One Time Code in the format:

```
Password Field: passwordOTC
```

404.1 Swivel Administration Console Passwords

Check password with repository option is not available for the Administration console login. The Swivel Administration console uses only Swivel Passwords and not data source passwords such as that from Active Directory or LDAP.

405 Known Issues

406 Troubleshooting

406.1 Error Messages

x.x.x.x Identifier:Failed to get LDAP context for username@domain

Password has failed to be matched from a LDAP data source when using Check Password with repository. This could be due to an incorrect password being entered or not recognised. On the Swivel Administration console when using AD try setting the AD server settings username to the UPN name. Below version 3.9.1 the domain is taken from the AD configuration, if a different domain is required, use a service account with the same domain.

RADIUS: <0> Access-Request(1) LEN=64 x.x.x.x:1265 Access-Request by username Failed: AccessRejectException: Two Stage Password Fail

x.x.x.x Identifier:Failed to get LDAP context for username@domain

The check password with repository is failing for the first stage of two stage authentication. This could be due to an incorrect password being entered or not recognised. On the Swivel Administration console when using AD try setting the AD server settings username to the UPN name. If the AD domain is incorrect then authentication will fail. Below version 3.9.1 the domain is taken from the AD configuration, if a different domain is required, use a service account with the same domain.

RADIUS: Exception in thread: DATAGRAM LEN = 155 FROM 192.168.1.2:53987 java.lang.NumberFormatException: For input string: "D5368" at java.lang.NumberFormatException.forInputString(Unknown Source) at java.lang.Integer.parseInt(Unknown Source) at java.lang.Integer.parseInt(Unknown Source) at com.swiveltechnologies.pinsafe.server.utility.Utility.extractIndex(Utility.java:265) at com.swiveltechnologies.pinsafe.server.user.LocalAuth.getChannelAndSecurityString(LocalAuth.java:527) at com.swiveltechnologies.pinsafe.server.user.LocalAuth.login(LocalAuth.java:729) at com.swiveltechnologies.pinsafe.server.radius.RadiusAccess.authenticatePAP(RadiusAccess.java:1107) at com.swiveltechnologies.pinsafe.server.radius.RadiusAccess.authenticate(RadiusAccess.java:499) at com.theorem.radserver3.RADIUSSession.o(Unknown Source) at com.theorem.radserver3.RADIUSSession.e(Unknown Source) at com.theorem.radserver3.RADIUSSession.run(Unknown Source) at java.lang.Thread.run(Unknown Source)

This is caused by a - or ' in a Check Password with repository for a RADIUS authentication and Swivel interpreting the String Index. Seen in version 3.9.6. Workaround 1. Do not use ' or - in the password. Workaround 2. If the access device supports checking AD password then configure it so that Swivel is only checking the Swivel OTC.

407 Password recovery for appliance How to guide

408 Overview

This document outlines how to reset the admin password back to factory defaults for a Swivel hardware or VM appliance.

409 Prerequisites

Swivel Appliance 2.x, 3.x, 4.x

409.1 Admin Console Password Reset Procedure using Sysresccd

This procedure can be used when the Webmin cannot be logged into.

409.1.1 Boot from sysrescue CD

See System Rescue CD

409.1.2 Mount file system

Mount the root partition. Note: If sda2 is not found then try sdb2 instead.

```
mkdir /root/temp
```

```
mount /dev/sda2 /root/temp
```

```
export SHELL=/bin/bash
```

```
chroot /root/temp
```

This will take you to a different prompt. Then run the following command:

```
passwd admin
```

Type in the default password. You will be asked to confirm it.

409.1.3 Known Issues

When trying to the above step of "passwd admin" and you are present with the error "Unknown user 'admin'" then vi /etc/passwd and add the following line to the list:

admin:x:0:0::/home/admin:/bin/bash

410 Testing

Login with the default username and password.

411 PIN

412 Overview

Swivel can use a One Time Code OTC or protect the delivery using a PIN number so the OTC is instead delivered as a Security string. The PIN number is a neric value 4-10 digits in length.

413 Prerequisites

Swivel 3.x

414 How to Guide

For information on PIN security see PIN Security How To Guide

For information on using only a One Time Code see PINless How To Guide

415 Testing

416 Known Issues

417 Troubleshooting

418 PIN Expiry How to Guide

419 Overview

Swivel has a PIN expiry feature which allows PIN numbers to expire and not be usable after a certain length of time or to resend a new PIN. This document explains how the PIN Expiry feature works

420 PIN Expiry Setting

PIN Expiry is a global setting affecting all users on the Swivel instance and is located under Policy\PIN and OTC. To change the PIN Expiry setting, on the Swivel Administration Console select Policy then PIN and OTC.

PIN expiry (days): Default 0. A value in days that the PIN will expire if the PIN is not changed. A value of 0 disables PIN expiry.

The PIN expiry time is reset after the following:

- ChangePIN
- Reset PIN from the Admin/helpdesk
- Resend PIN from the Admin/helpdesk
- ResetPIN from the ResetPIN utility

421 PIN expiry after auto/admin reset (days):

PIN expiry after auto/admin reset (days): default 0 (Disabled). The requirement for a user to change their PIN following its automatic setting by the server. A user's PIN may be set automatically in two situations: during their initial import into the user population and during a self-reset. Enabling this option requires the user to change their PIN following either of these events. The user may be informed of this requirement via an alert or by an agent that supports the display of warnings to the user.

422 PIN Expiry related settings

422.1 PIN expiry warning (days)

This option is located under Policy\PIN and OTC and allows the user to be notified in advance that their PIN number should changed.

PIN expiry warning (days): Default 7

How often the PIN expiry reminder is sent to the user is determined by the **PIN expiry check** located under Server then Jobs. Also when *Auto-reset PIN on expiry* is used, this is how far in advance that the new PIN is sent out, if it is set 0 then no new PIN will be sent.

422.2 PIN Expiry Check

This is located under Server\Jobs and is how often users are checked for expired PIN numbers. Each time it is run it will check for expired PIN numbers, and if it is within the PIN expiry warning period, the user is notified it must be changed. To change how often PIN expiry messages are sent change this value. For information on creating custom schedules see Schedule.

Note: If this value is set to 0 days, users will not be given any notice of PIN expiry.

Note: A users PIN may expire at a time before the PIN expiry check becoming locked but not being marked as locked, the account may only become marked as locked when the PIN expiry check is run.

422.3 Auto-reset PIN on expiry

The user can be automatically sent a new PIN number when the PIN expires. This option is located under Policy\PIN and OTC. A transport will need to be setup to send the user a PIN number, see Transport Configuration. The *PIN Expiry Warning* will determine how far in advance the new PIN is sent out before expiry, and if this is set to 0 then no new PIN is sent out.

To change the PIN Expiry setting, on the Swivel Administration Console select Policy then PIN and OTC.

Auto-reset PIN on expiry: Default: No, Options Yes/No

422.4 PIN change grace period (days):

The grace period only applies to users that have become locked because their PIN has expired and then the user account is unlocked. This option is located under Policy\PIN and OTC and gives users an additional period to change their PIN before the account becomes locked again. Users whose account has become locked because of too many wrong login attempts are not affected by this.

PIN change grace period (days): Default 0

422.5 Only warn user, do not lock account

This option is located under Policy\PIN and OTC and allows the user to be told that they should change their PIN. but does not lock the users account.

Only warn user, do not lock account:, Default: No, Options Yes/No

422.6 PIN Expiry exemption

Certain users can be exempted from PIN expiry by selecting **PIN never expires:** option located under User Administration, select the required user, then click on policy.

423 PIN Expiry Implementation

If PIN Expiry is to be applied to an existing Swivel instance, all users that have not had their PIN changed within the PIN expiry value will have their accounts locked. Therefore a process of warning users and not enforcing the PIN change for a certain period or using Auto-reset PIN on expiry may be suitable.

Users who are required to Change their PIN should have available a method of changing their PIN, for more information see the **ChangePIN How to Guide**

424 PIN Expiry Troubleshooting

424.1 Known Issues

Swivel 3.10 to 3.10.4 - A user is sent a new PIN instead of a warning that their PIN is about to expire. To overcome this, update to a more recent version or increase the PIN expiry by the PIN expiry warning period, although the user will not receive a warning message.

Swivel 3.9.1 to 3.9.5 the PIN expiry may fail if the user has never reset their PIN. Upgrade to a version later than 3.9.5.

PIN expiry messages are not sent to users in some versions of 3.5 to 3.8. This is fixed in Swivel version 3.9.

424.2 Error Messages

Access-Request(1) LEN=192.168.1.1.:12685: Access-Request by username Failed: AccessRejectException: AGENT_ERROR_PIN_EXPIRED

Login failed for user; username, error The user's PIN has expired

User "username" has been locked, reason: The users's PIN has expired.

This is the sequence of messages for an expired PIN

ERROR - Job (DEFAULT.PIN_EXPIRY threw an exception

```
ERROR - Job (DEFAULT.PIN_EXPIRY threw an exception.
org.quartz.SchedulerException: Job threw an unhandled exception. [See nested exception: java.lang.NullPointerException]
at org.quartz.core.JobRunShell.run(JobRunShell.java:206)
at org.quartz.simpl.SimpleThreadPool$WorkerThread.run(SimpleThreadPool.java:520)
* Nested Exception (Underlying Cause) ---------------
java.lang.NullPointerException
at java.util.Calendar.setTime(Unknown Source)
at com.swiveltechnologies.pinsafe.server.policy.PinExpiry.doCheckExpiry(PinExpiry.java:159)
at com.swiveltechnologies.pinsafe.server.policy.PinExpiry.execute(PinExpiry.java:225)
at org.quartz.core.JobRunShell.run(JobRunShell.java:195)
at org.quartz.simpl.SimpleThreadPool$WorkerThread.run(SimpleThreadPool.java:520)
```

This error has been seen in Swivel versions 3.93, and is resolved in 3.9.4. It only affects systems where the grace period has been set to a value other than 0. Setting the grace period to 0 prevents this issue from occurring.

425 PIN Security How To Guide

425.1 Overview

PINsafe provides a number of ways to ensure that PIN numbers are effectively and securely used.

- PIN is never typed directly into the keyboard
- PIN extraction to generate a One Time Code
- PIN policy prevents repeated PIN digits
- PIN policy prevents sequences of numbers being used
- Minimum PIN length of 4 numbers
- Randomly generated PIN number
- ChangePIN utility to securely allow a user to change a PIN number
- ResetPIN utility for lost and forgotten PIN numbers to perform a PIN reset
- Use of one channel for security string and another channel or method for the PIN number

For information on using an OTC without PIN protection see PINless How To Guide

425.2 PIN Policy

The following security policies may be used to enhance PIN security.

425.3 Account Lockout

Where an attempt has been made to log into an account several times, the account may be locked after a set number of attempts.

425.3.1 Maximum Repeated Digits

Used with ChangePIN

This is the permitted sum of all repeated digits.

0 = No repeated digits, Example: 7204 is permitted 6260 is not permitted.

1 = One Digit may be repeated once, Example 7202 is permitted 3833 is not permitted, and 1122 is not permitted as 1 is repeated once and 2 repeated once giving a total of two repeated digits.

425.3.2 Do Not Allow Number Sequences

Used with ChangePIN

This option prevents users from having numeric sequences in their PIN number, such as 1234, 2468, 7654, 1357.

The following are not treated as sequences: 1123, 8901.

425.3.3 Banned Credentials

Used with ChangePIN

PINsafe 3.8 introduces banning of custom PIN numbers.

For example 19?? stops the creation of PIN numbers beginning with 19

425.3.4 PIN Expiry

The PIN number can be optionally set to expire after a certain length of time, see also PIN Expiry How to Guide. The following actions may be taken depending on the configuration used:

425.3.4.1 Account Lockout

Account becomes locked preventing its use.

425.3.4.2 Automatically Resend New PIN

This option allows a new random PIN number is sent to the user when the current PIN number has expired.

425.3.4.3 ChangePIN on login or ChangePIN after Admin Reset or on First Login

When this is set the user receives a notification that their PIN must be changed. If they do not change their PIN, the the account will become locked and not allow the next attempted login. Using RADIUS or Agent-XML the user can be redirected to a ChangePIN page when required to Change their PIN, see also ChangePIN How to Guide.

425.3.5 PIN Change Grace Period

The grace period only applies to users that have become locked because their PIN has expired and then the user account is unlocked. This option gives users an additional period to change their PIN before the account becomes locked again. Users whose account has become locked because of too many wrong login attempts are not affected by this.

425.3.6 PIN Notifications

- User must Change their PIN
- A PIN number has changed

425.3.7 Helpdesk User cannot Reset PIN

This option prevents the helpdesk user from setting a PIN number to a known value for an account, see also Helpdesk Configuration Guide.

425.3.8 Static Passwords

PINsafe can use a static passwod in addition to a One Time Code. The static password may be used to make shoulder surfing technques less effective due to the length of the OTC and Password. When a PINsafe password is set for a user, it must be used, see Password How to Guide.

425.4 PIN delivery Security

425.4.1 PIN Transport

The PIN number can be configured to be delivered in a different method to the security string.

425.4.2 Require Change of PIN

The user may be required to change their PIN on their first login.

425.5 Initial/Default PIN numbers

Although possible, setting initial default PIN numbers is not recommended, but a randomly generated PIN is more secure.

425.6 Minimum PIN Size

The default PIN size is 4 digits. Increasing this may make it more difficult for users to remember. For security reasons the PIN can be used with a static password.

425.6.1 Changing Minimum PIN Size

Changing the minimum PIN size will not affect existing PIN users unless a new PIN is sent to them or they perform a change PIN.

426 Pinsafe

426.1 PINsafe

PINsafe is the former name of the Swivel Secure core authentication platform. As from version 4, it is known as **Sentry**. Specifically, we refer to **Sentry Core** where we need to distinguish the core authentication engine from the adaptive authentication and single-sign-on engine, **Sentry SSO**.

You can find a reference guide to the Sentry Core Administration Console here.

427 PINsafe config.xml Guide

427.1 Overview

The config.xml file controls the settings for PINsafe, this document outlines the use of the config.xml file.

427.2 Prerequisites

PINsafe 3.x

427.3 Saving the config.xml

On the PINsafe Administration console select **Save Config**, and choose a download location. Note the PINsafe appliance automatically makes a backup of the config.xml, see also Backup PINsafe How to Guide.

427.4 Restoring the config.xml

Note the following:

- Ensure that the current config.xml is backed up if required
- Avoid copying the config.xml to an older version of PINsafe
- Having a browser open on the Administration console may keep the Administration session open
- Some settings such as PINsafe server name, and RADIUS server IP address will be carried across, and may need to be changed manually where required

To restore the config.xml file the following steps are required:

Stop Tomcat

copy the config.xml file to <path to Tomcat>/webapps/pinsafe/WEB-INF/conf overwriting the current config.xml file.

start Tomcat

428 PINsafe Configuration Best Practices

429 Overview

Each Swivel installation will have its own requirements that will require changes to standard configurations. However below are some best practices for configuring Swivel policies and settings.

429.1 Policy>General

- Security String Type: Numbers, Upper Case Letters, Lower Case Letters, Mixed numbers and letters

Default: Numbers

Best Practice: Numbers or Upper Case Letters

- Account lockout time (minutes):

Default: 0

Best Practice: 30 minutes

- Maximum login tries: 0-99

Default: 5

Best Practice: Testing 0 (no lockout), Initial provisioning: 5, Long Term production: 3

- Increment Login failure count if user has no security strings: Yes/No

Default: Yes

Best Practice: Yes

- Inactive account expiry (days):

Default 0 (no expiry)

Best Practice: 90

- Auto. set credentials on user creation: Yes/No

Default: Yes

Best Practice: Yes

429.2 Policy>PIN and OTC

- PIN expiry (days): 0-99

Default: 0 (no expiry)

Best Practice: as PIN expiry (where change PIN is available)

- PIN expiry after auto/admin reset (days): 0-99

Default: 0

Best Practice: Yes (where change PIN is available)

- PIN expiry warning (days): 0-99

Default: 0 (no expiry)

Best Practice: 14

- Auto-reset PIN on expiry: Yes/No

Default: No

Best Practice: Yes

- PIN change grace period (days): 0-99

Default: 0

Best Practice: 7

- Require PIN change after auto. setting:

Default: No

Best Practice: Yes (where change PIN is available)

- Require PIN change after admin. reset:

Default: No

Best Practice: Yes (where change PIN is available)

- Require password for PIN change: Yes/No

Default: Yes

Best Practice: Yes (where change PIN is available)

- Only warn user, do not lock account: Yes/No

Default: No

Best Practice: No, (Yes if Auto-reset PIN on expiry is used)

- Minimum PIN size: 4-10

Default: 4

Best Practice: 4

- PINless OTC length: 4-10

Default: 6

Best Practice: 6

- Maximum repeated PIN digits:

Default: 0 (digits may not be repeated)

Best Practice: 0

- Allow numerical sequences for PIN:

Default: Yes

Best Practice: No

429.3 Policy>Password

- Require password:

Default: No

Best Practice: No (Where another primary/secondary authentication server is used in access device)

429.4 Policy>Self-Reset

- Allow user self-reset: Yes/No

Default: No

Best Practice: Yes

- Send reset code as security string: Yes/No

Default: No

Best Practice: No

- Maximum self-reset tries: 0-99

Default: 3

Best Practice: 3

- Allow user self-provision of mobile client: Yes/No

Default: No

Best Practice: Yes

- Send provision code as security string: Yes/No

Default: No

Best Practice: No

- Log device information when provisioning: Yes/No

Default: No

Best Practice: Yes

- Provision Code Validity period (seconds): 10-1000000

Default: 600

Best Practice: 86400

429.5 Policy>Helpdesk

- Helpdesk Users can manage other repositories: Yes/No

Default: No

Best Practice: No

- Helpdesk can reset PINs: Yes/No

Default: Yes

Best Practice: No

- Helpdesk Users can administer editable repositories: Yes/No

Default: No

Best Practice: No

- Helpdesk can view Status page: Yes/No

Default: Yes

Best Practice: Yes

- Helpdesk can view Log Viewer page: Yes/No

Default: Yes

Best Practice: No

- Helpdesk can view reports:

Default: No

Best Practice: No

429.6 Policy>Console Login

- Show the password field: Yes/No

Default: Yes

Best Practice: No

- Use single channel login: Yes/No

Default: Yes

Best Practice: Yes

- Update TURing immediately after entering username: Yes/No

Default: No

Best Practice: Yes

429.7 Policy>Banned Credentials

Default: None

Best Practice: 19??, 200?, 201?

429.8 Policy>Mobile Client

- Allow user to enter PIN: Yes/No

Default: No

Best Practice: No

- Allow user to choose how to extract OTC: Yes/No

Default: No

Best Practice: No

- Allow user to browse strings: Yes/No

Default: No

Best Practice: No

429.9 Logging>SMTP

- Send errors:

Default: No

Best Practice: No (where Syslog is used)

- Send account locks:

Default: No

Best Practice: Yes

- Send User Account Create/Delete:

Default: No

Best Practice: No

429.10 Transport>User Alerts

- PIN changed: Yes/No

Default: Yes

Best Practice: Yes

- PIN change required: Yes/No

Default: Yes

Best Practice: Yes

- PIN expiry warning: Yes/No

Default: Yes

Best Practice: Yes

- Account locked: Yes/No

Default: Yes

Best Practice: Yes

- Account unlocked: Yes/No

Default: Yes

Best Practice: Yes

- Account inactive: Yes/No

Default: Yes

Best Practice: Yes

- Device key allocated: Yes/No

Default: Yes

Best Practice: Yes

- No transport is error: Yes/No

Default: No

Best Practice: No

429.11 Database>General

- Case sensitive usernames: Yes/No

Default: No

Best Practice: No

429.12 Server Agents and RADIUS NAS

- Check password with Repository:

Default: No

Best Practice: No (Where another primary/secondary authentication server is used in access device)

430 Ports

431 Overview

This document outlines the ports used by Swivel appliances for communication.

432 Prerequisites

Swivel Appliance 2.x

432.1 Port Configuration

Swivel Appliance Communication Ports

Service	Direction	Port Number	TCP/UDP/ICMP	Source	Destination
Swivel Administration	Inbound	8080	TCP	Management Console	Swivel Appliance (SSL by default)
Swivel Proxy	Inbound	8443	TCP	External connections	Swivel Appliance (SSL by default)
SSH	Inbound	22	TCP	Management Console	Swivel Appliance
Webmin	Inbound	10000	TCP	Management Console	Swivel Appliance
RADIUS Authentication	Inbound	1812	UDP	Access device	Swivel Appliance
RADIUS Accounting	Inbound	1813	UDP	Access device	Swivel Appliance
Agent-XML	Inbound	8080	TCP	Access device using Agent-XML	Swivel Appliance (SSL by default)
DNS	Outbound	53	TCP/UDP	Swivel Appliance	DNS Server
NTP	Outbound	123	UDP	Swivel Appliance	Time Server
SMTP	Outbound	25	TCP	Swivel Appliance	Email Server
Syslog	Outbound	514	UDP	Swivel Appliance	Syslog Server
FTP	Outbound	20	TCP	Swivel Appliance	FTP Backup Server
Web	Outbound	443	TCP	Swivel Appliance	SMS Server (SSL by default)
SMPP	Outbound	2775	TCP	Swivel Appliance	SMPP SMS Server
LDAP	Outbound	389	TCP	Swivel Appliance	AD, ADAM or LDAP Server
LDAPS	Outbound	636	TCP	Swivel Appliance	AD, ADAM or LDAP Server over SSL
Global Catalog	Outbound	3268	TCP	Swivel Appliance	AD, ADAM or LDAP Server
Global Catalog Secure	Outbound	3269	TCP	Swivel Appliance	AD, ADAM or LDAP Server
SNMP	Inbound	161	UDP	SNMP server	Swivel Appliance
Dell OpenManage	Inbound	1311	UDP	Dell OpenManage server	Swivel Appliance

Swivel Additional A/A Appliance Communication Ports

Service	Direction	Port Number	TCP/UDP/ICMP	Source	Destination
Ping	Bi-directional	-	ICMP	Swivel Appliance	Gateway
SSH	Bi-directional	22	TCP	Swivel Appliance	Swivel Appliance
MySQL	Bi-directional	3306	TCP	Swivel Appliance	Swivel Appliance
Heartbeat	Bi-directional	631	UDP	Swivel Appliance	Swivel Appliance
Heartbeat	Bi-directional	694	UDP	Swivel Appliance	Swivel Appliance
Administration Synchronisation	Bi-directional	61616	TCP	Swivel Appliance	Swivel Appliance
Appliance Synchronisation	Bi-directional	8080	TCP	Swivel Appliance	Swivel Appliance (SSL by default)

Older A/A Appliance Communication Ports

Service	Direction	Port Number	TCP/UDP/ICMP	Source	Destination
Session Sharing	Bi-directional	4446	UDP	Swivel Appliance	Swivel Appliance

433 PositiveID How to Guide

434 PositiveID

Positive ID is no longer developed and is no longer available for purchase.

434.1 Overview

Positive ID fingerprints a desktop, laptop or server to uniquely identify the device. A PositiveID user is required to authenticate using one of their devices. A PositiveID user who is not registered to a device will not be able to authenticate using that device using Single or dual channel. A user who is not a PositiveID user will be able to authenticate using a device that is registered to PositiveID user. A PC may be registered for access by several PositiveID users.

434.2 Prerequisites

PINsafe 3.x

PINsafe 3.7 requires a patch available here PINsafe PositiveID Server Patch

PINsafe Taskbar see Taskbar How to Guide

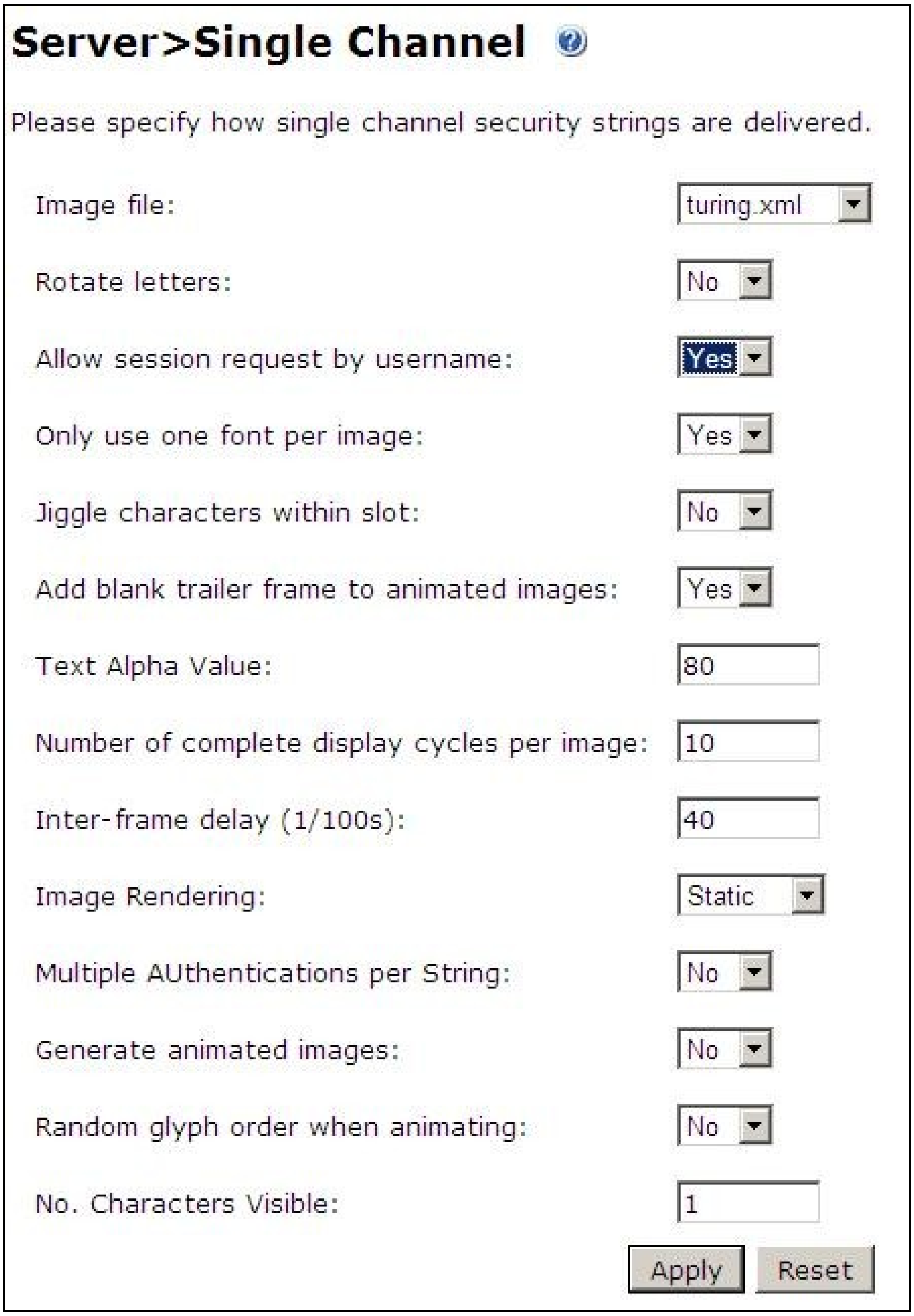
434.3 PositiveID Configuration

434.3.1 Allow session request by username

If the Single Channel Image request is to be used allow username to be used for authentication requests.

1. On the PINsafe Management Console select Server/Single Channel

2. Ensure ?Allow session request by username? is set to YES



Server>Single Channel

Please specify how single channel security strings are delivered.

Image file:	turing.xml
Rotate letters:	No
Allow session request by username:	Yes
Only use one font per image:	Yes
Jiggle characters within slot:	No
Add blank trailer frame to animated images:	Yes
Text Alpha Value:	80
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	40
Image Rendering:	Static
Multiple AUthentications per String:	No
Generate animated images:	No
Random glyph order when animating:	No
No. Characters Visible:	1

434.3.2 Create a Positive ID Group

Create a group of users for which PositiveID authentication will be required. If a group of users already exists for which PositiveID is required, then skip to the next step.

Note on a Active Active setup the user data is transferred in the database, but in order to see the groups, the Positive ID group needs to be created on all PINsafe instances.

1. On the PINsafe Administration Console select Repository/Groups

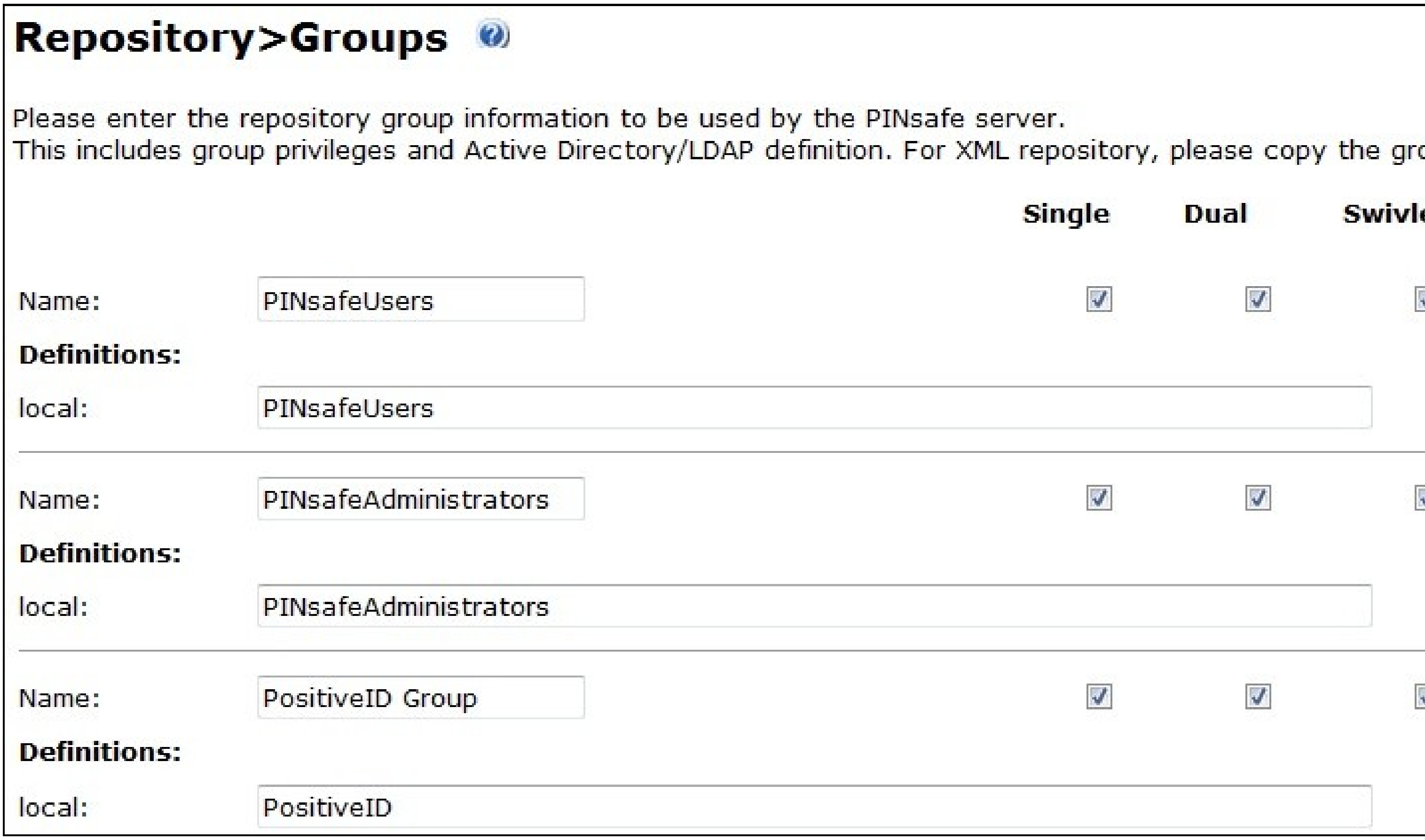
2. Create a PositiveID Group

3. Assign Single, Dual, Swivlet (PINless?) permissions as appropriate

4. Add additional data sources for users as required

5. When complete click Apply to save the settings

Note: Do not synchronise the users at this stage from the data source.



Repository>Groups

Please enter the repository group information to be used by the PINsafe server.
This includes group privileges and Active Directory/LDAP definition. For XML repository, please copy the gro

		Single	Dual	Swivl
Name:	PINsafeUsers	☑	☑	☑
Definitions:				
local:	PINsafeUsers			
Name:	PINsafeAdministrators	☑	☑	☑
Definitions:				
local:	PINsafeAdministrators			
Name:	PositiveID Group	☑	☑	☑
Definitions:				
local:	PositiveID			

434.3.3 Create transports for PositiveID group

Create the transports for the users, If the transports are already configured for the groups which PositiveID is required, then skip to the next step.

1. On the PINsafe Administration Console select Transport/General

2. Assign select the transport for the PositiveID Group of users by using the drop down menu to select the PositiveID group for the transport required. For further information on transports see Transport Configuration

3. When complete click Apply to save the settings

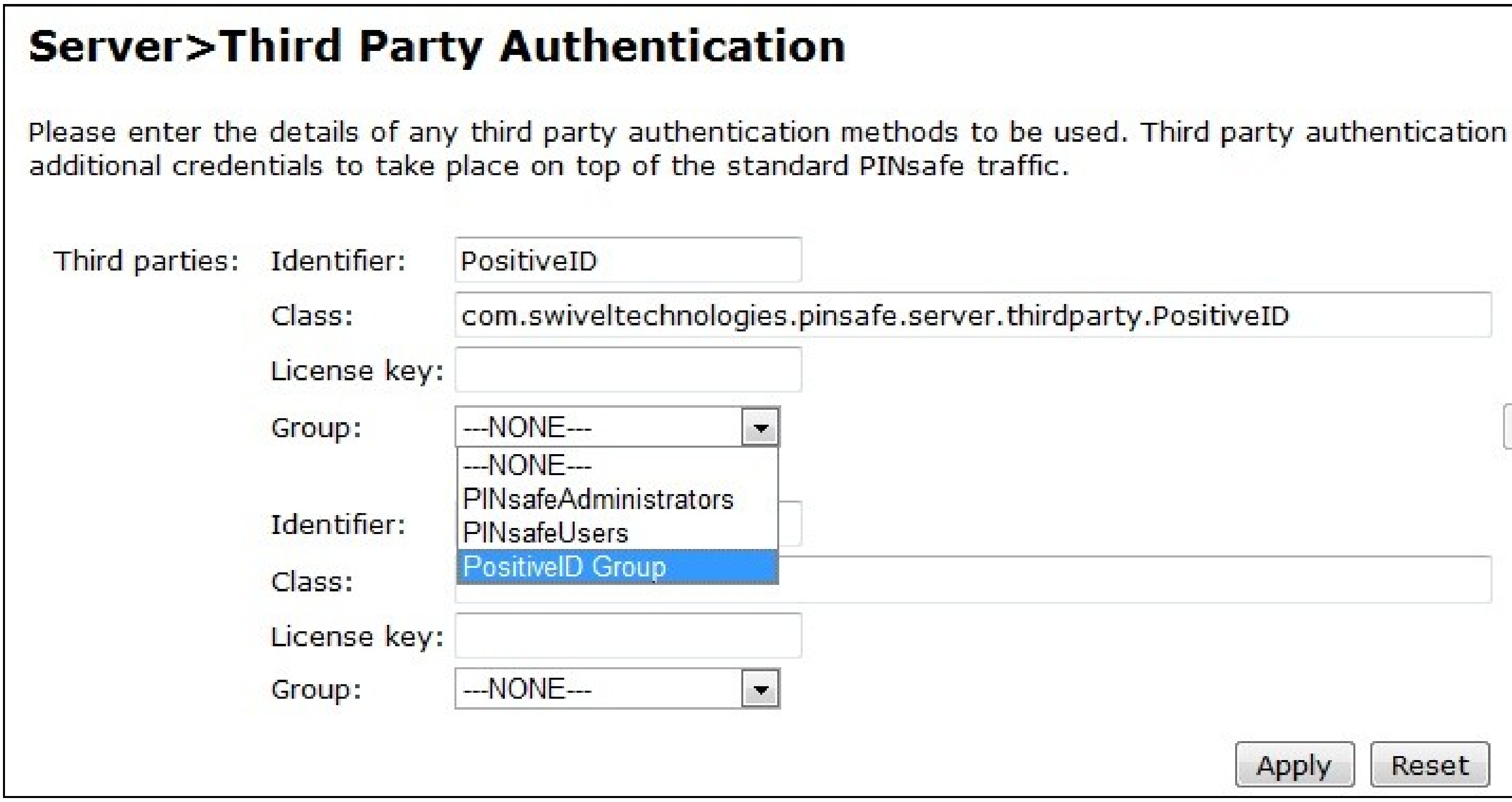
4. Select the new transport created under Transport and enter required configuration information.

434.3.4 Assign PositiveID Authentication to User Group

1. On the PINsafe Administration Console select Server/Third Party Integration

2. Assign the Group of users who will use Positive ID (A 5 user evaluation license is automatically used)

3. When complete click Apply to save the settings. A PositiveID menu item should now appear



Server>Third Party Authentication

Please enter the details of any third party authentication methods to be used. Third party authentication
additional credentials to take place on top of the standard PINsafe traffic.

Third parties: Identifier: PositiveID

Class: com.swiveltechnologies.pinsafe.server.thirdparty.PositiveID

License key:

Group: ---NONE---

Identifier:

Class:

License key:

Group: ---NONE---

434.3.5 Configure PositiveID Session Management

The Session management details when a Positive ID authentication should occur.

1. On the PINsafe Administration Console select PositiveID/Session Management

2. Select the appropriate settings

3. When complete click Apply to save the settings

The possible options for the settings are listed below:

Number of auto-allocated devices: Default: 0, Options 1,2,3..., This allows a user to be automatically sent one or more Registration Keys when the account is created. A value of 0 means that no Registration Keys are sent. This is particularly useful when provisioning large numbers of users.

Session timeout: (seconds) Default: 120, The maximum time that PositiveID authentication can occur before PINsafe considers it to be invalid.

PositiveID auth. required before PIN change: Default: Yes, Options Yes/No, When enabled requires a successful PositiveID authentication before a ChangePIN change is permitted.

PositiveID auth. required before login: Default: Yes, Options Yes/No, When enabled requires a successful PositiveID authentication before the PositiveID user can login

PositiveID auth. required before self-reset: Default: No, Options Yes/No, When enabled requires a successful PositiveID authentication before a Self Reset is permitted.

PositiveID auth. required before self-reset code request: Default: No, Options Yes/No, When enabled requires a successful PositiveID authentication before a Self Reset code is sent to the user.

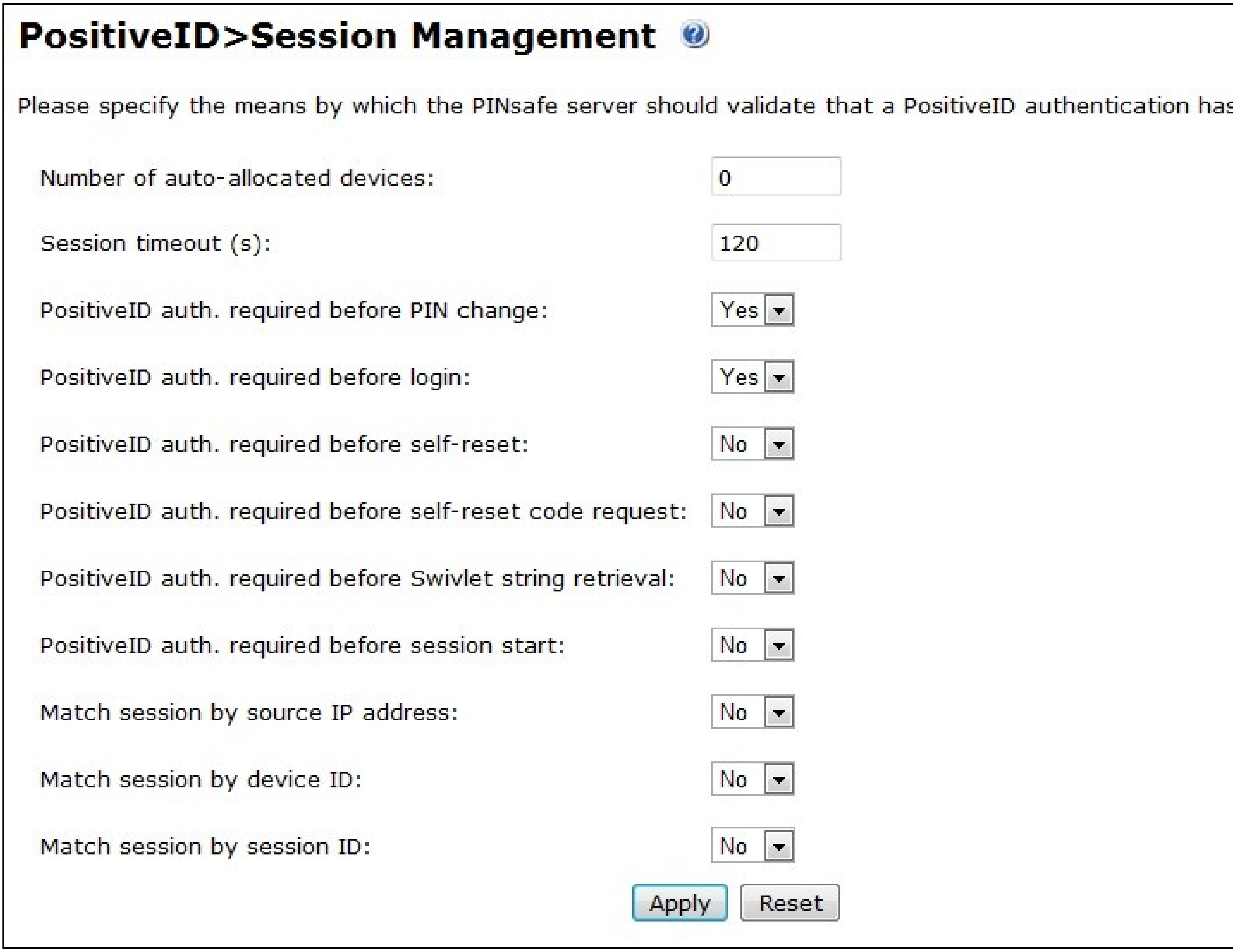
PositiveID auth. required before Swivlet string retrieval: Default: No, Options Yes/No, When enabled requires a successful PositiveID authentication before security strings can be downloaded by the mobile phone application see IPhone, Swivlet Java Applet, Windows Mobile.

PositiveID auth. required before session start: Default: No, Options Yes/No, Requires a successful PositiveID authentication before a single channel session can be started.

Match session by source IP address: Default: No, Options Yes/No, When enabled the server checks that the request for PINsafe authentication is coming from the same IP address as PositiveID authentication. If the IP addresses don't match, or can't be determined, the authentication will fail.

Match session by device ID: Default: No, Options Yes/No, When enabled the PINsafe agent must pass, as part of the AgentXML traffic, the identifier of the PositiveID device that has been previously authenticated.

Match session by session ID: Default: No, Options Yes/No, When enabled the PINsafe agent must pass, as part of the AgentXML traffic, the session identifier returned by the PositiveID client after authentication.



PositiveID>Session Management

Please specify the means by which the PINsafe server should validate that a PositiveID authentication has

Number of auto-allocated devices: 0

Session timeout (s): 120

PositiveID auth. required before PIN change: Yes

PositiveID auth. required before login: Yes

PositiveID auth. required before self-reset: No

PositiveID auth. required before self-reset code request: No

PositiveID auth. required before Swivlet string retrieval: No

PositiveID auth. required before session start: No

Match session by source IP address: No

Match session by device ID: No

Match session by session ID: No

434.3.6 Configure PositiveID Device Policy

The settings in this group determine which devices are checked for equality when PositiveID authentication takes place. If any device is disabled, changes of that device on the client will not cause PositiveID authentication to fail.

1. On the PINsafe Administration Console select PositiveID/Device Policy

2. Select the appropriate settings

3. When complete click Apply to save the settings

The possible group options are:

BIOS: Default: Yes, Options Yes/No

On board device: Default: Yes, Options Yes/No

Processor: Default: Yes, Options Yes/No

System enclosure: Default: Yes, Options Yes/No

Network adapter: Default: Yes, Options Yes/No

Network adapter configuration: Default: Yes, Options Yes/No

Desktop monitor: Default: Yes, Options Yes/No

Computer system: Default: Yes, Options Yes/No

Base board: Default: Yes, Options Yes/No

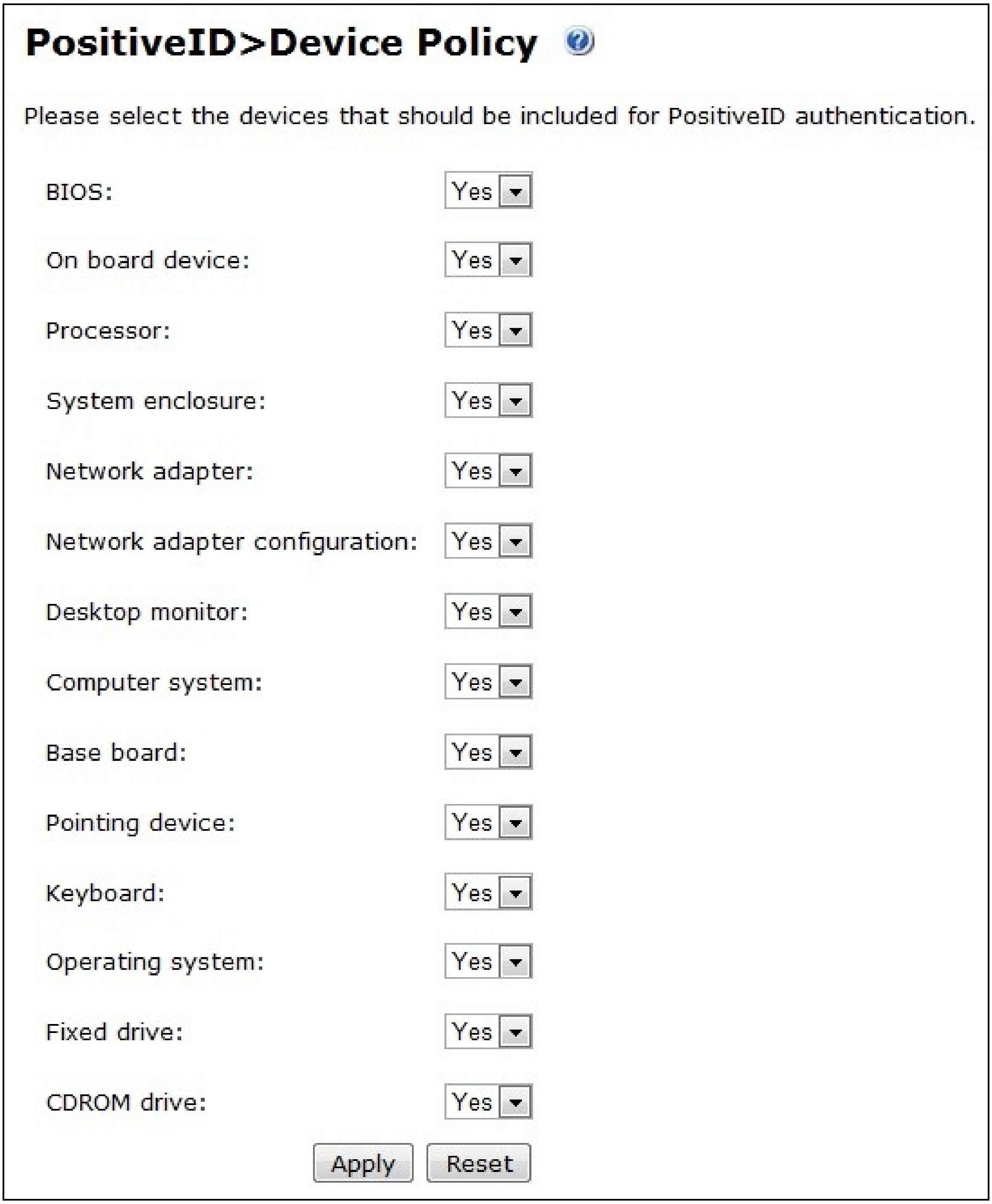
Pointing device: Default: Yes, Options Yes/No

Keyboard: Default: Yes, Options Yes/No

Operating system: Default: Yes, Options Yes/No

Fixed drive: Default: Yes, Options Yes/No

CDROM drive: Default: Yes, Options Yes/No



PositiveID>Device Policy

Please select the devices that should be included for PositiveID authentication.

BIOS: Yes

On board device: Yes

Processor: Yes

System enclosure: Yes

Network adapter: Yes

Network adapter configuration: Yes

Desktop monitor: Yes

Computer system: Yes

Base board: Yes

Pointing device: Yes

Keyboard: Yes

Operating system: Yes

Fixed drive: Yes

CDROM drive: Yes

FAQ: Q). Does PINsafe read a machines certificate to uniquely verify the device?

A). No PositiveID does not use certificates for identification.

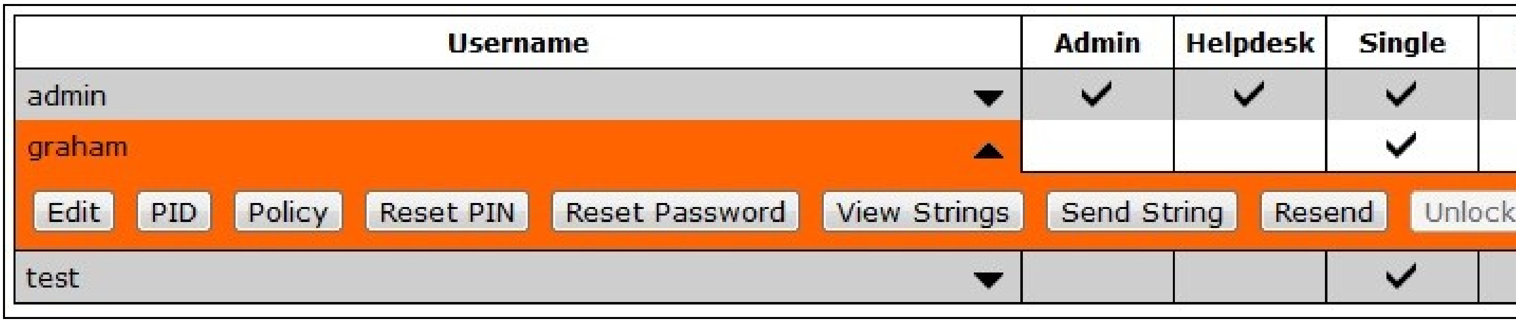
434.3.7 Provision PositiveID Registration Keys

If the auto provision **Number of auto-allocated devices:** is set to a value greater than 0 then the user will automatically receive a Registration Key. They can also be manually provisioned a Registration Key.

1. On the PINsafe Administration Console select User Administration

2. Synchronise users from the required Positive ID group by clicking on User Sync for that group. Check the logs to see if any automated Registration Keys are sent out, the following message can be seen: **New PositiveID device automatically allocated, username: Graham, id: 9**

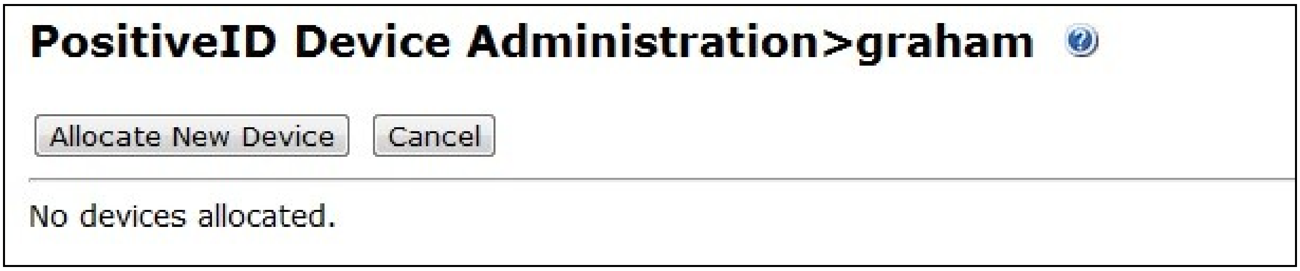
3. left click on user name then PID. If it is greyed out then they are not part of a PositiveID group



Username	Admin	Helpdesk	Single
admin	✓	✓	✓
graham			✓
test			✓

4. If a Registration Key has been automatically allocated it will appear here for the user. To manually create a Registration Keys click on Allocate New Device, a new Registration Key then should appear below. Check logs to ensure Registration Key has been sent to user by their transport.

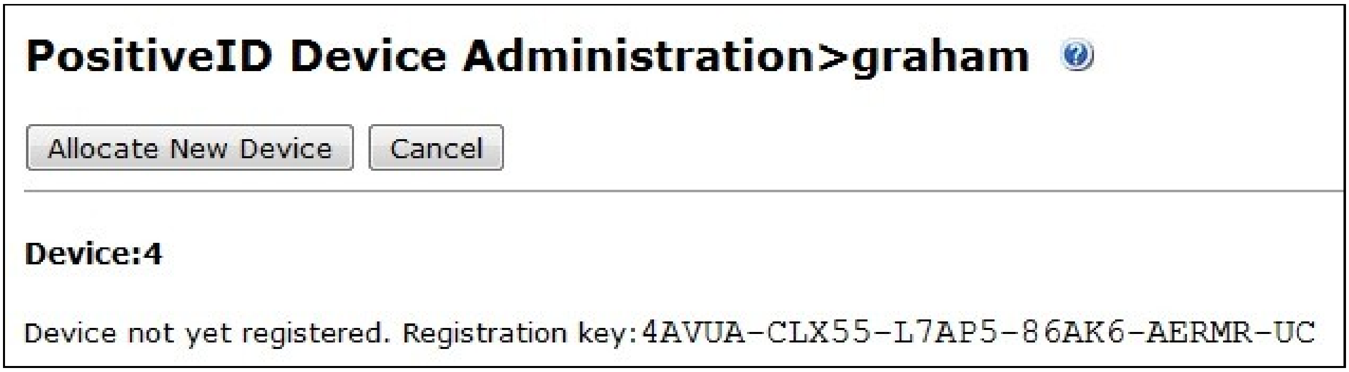
No Registration Keys



PositiveID Device Administration>graham

No devices allocated.

Unregistered Registration Key

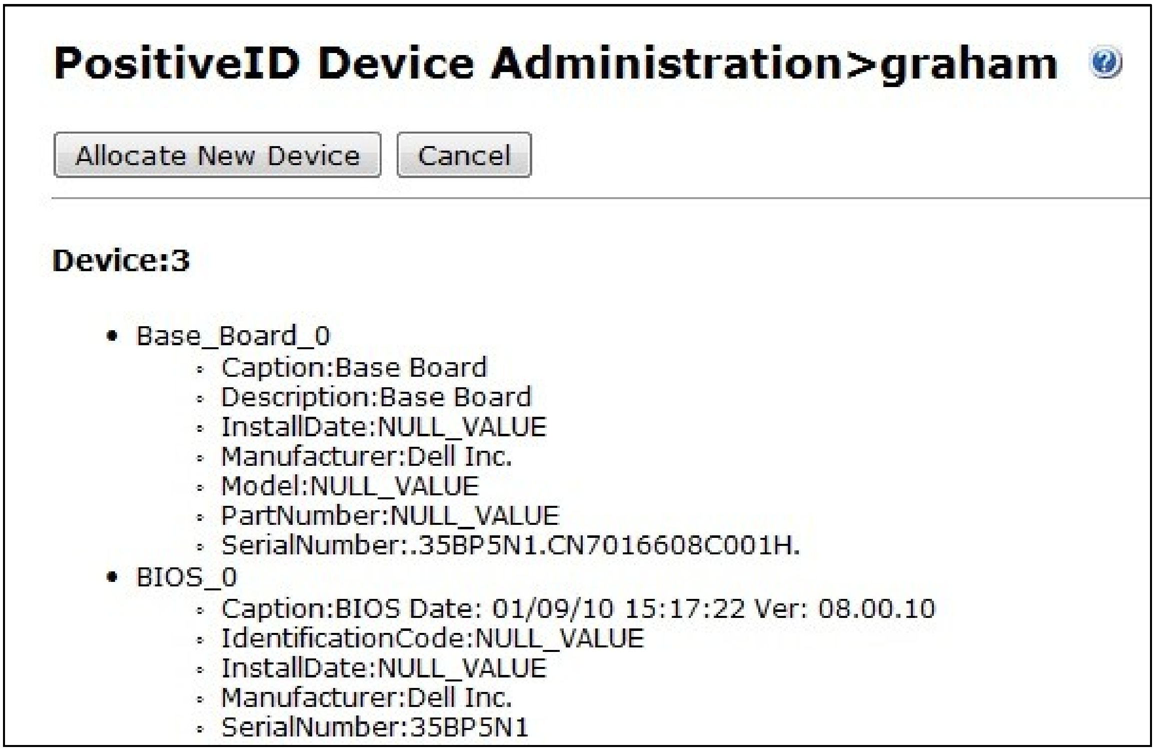


PositiveID Device Administration>graham

Device:4

Device not yet registered. Registration key:4AVUA-CLX55-L7AP5-86AK6-AERMR-UC

Registered Device



PositiveID Device Administration>graham

Device:3

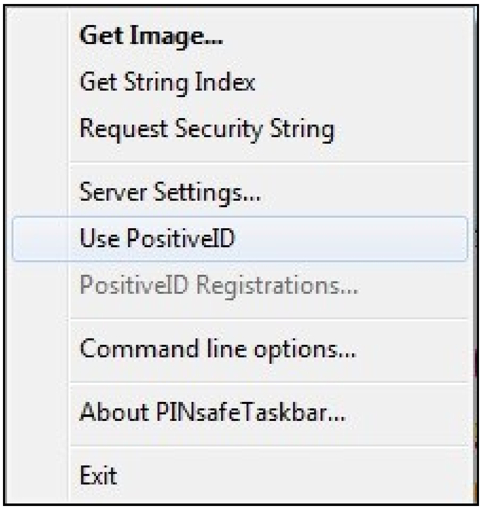
- Base_Board_0
  - Caption:Base Board
  - Description:Base Board
  - InstallDate:NULL_VALUE
  - Manufacturer:Dell Inc.
  - Model:NULL_VALUE
  - PartNumber:NULL_VALUE
  - SerialNumber:.35BP5N1.CN7016608C001H.
- BIOS_0
  - Caption:BIOS Date: 01/09/10 15:17:22 Ver: 08.00.10
  - IdentificationCode:NULL_VALUE
  - InstallDate:NULL_VALUE
  - Manufacturer:Dell Inc.
  - SerialNumber:35BP5N1

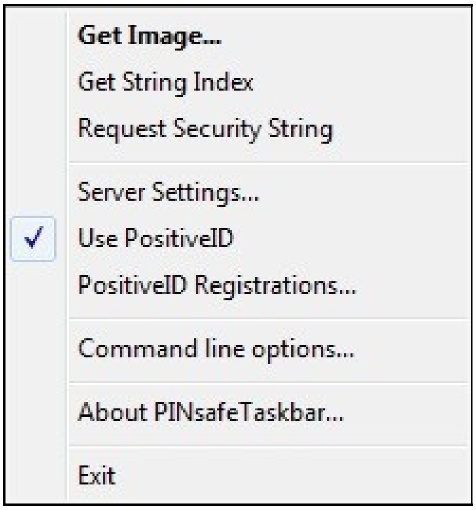
434.4 Provision a Device

On the device which is to be provisioned follow the instructions for installing and using the PINsafe Taskbar, see Taskbar How to Guide Ensure that the required authentication method is tested and available, for example the Turing image. Additional steps for Positive ID authentication are listed below.

434.4.1 Enable PositiveID Authentication on the Taskbar

Right click on the PINsafe Taskbar and click on the line Use PositiveID, ensure a tick appears next to the menu item.

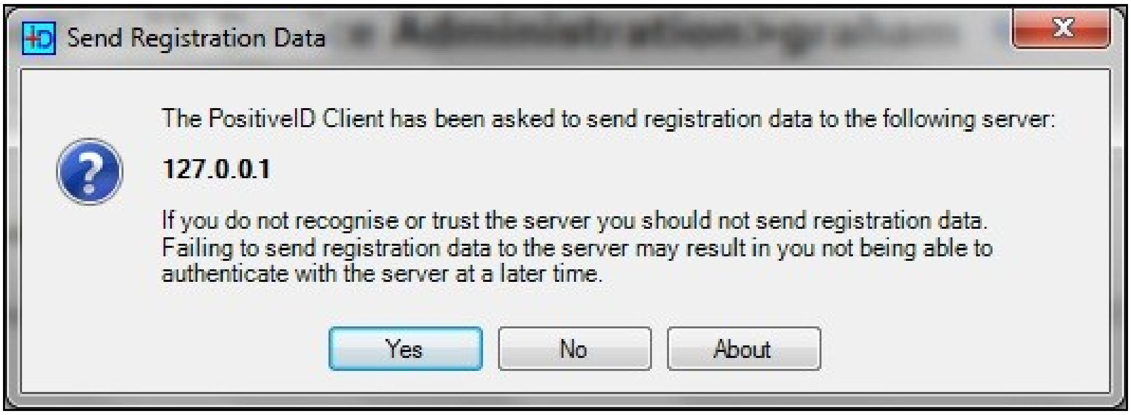




434.4.2 Enter Registration Key

From the PINsafe Taskbar click on Get Image, a box will appear confirming the IP or hostname of the PINsafe server, if correct click Yes and when prompted enter the Registration Key sent. If the registration completes then a Turing Image should appear. The PINsafe log should say: **PositiveID: Registration successful for device n.** where n is the device number registered. If it fails check the error message.

PINsafe Positive ID send Registration information confirmation



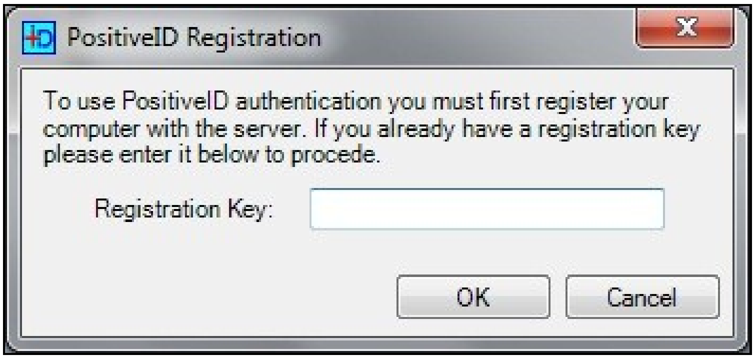
Send Registration Data

The PositiveID Client has been asked to send registration data to the following server:

127.0.0.1

If you do not recognise or trust the server you should not send registration data. Failing to send registration data to the server may result in you not being able to authenticate with the server at a later time.

PositiveID Registration Key

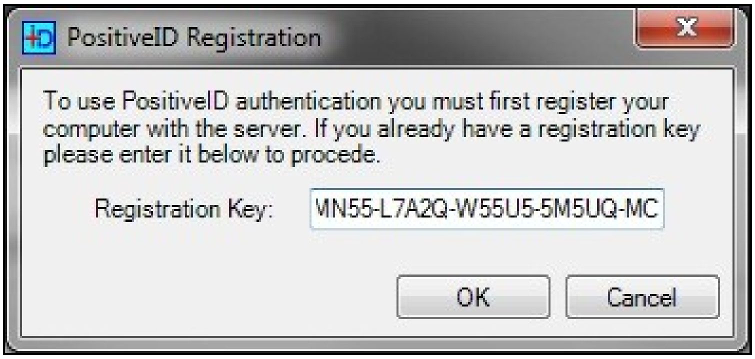


PositiveID Registration

To use PositiveID authentication you must first register your computer with the server. If you already have a registration key please enter it below to procede.

Registration Key:

PositiveID Registration Key entered



PositiveID Registration

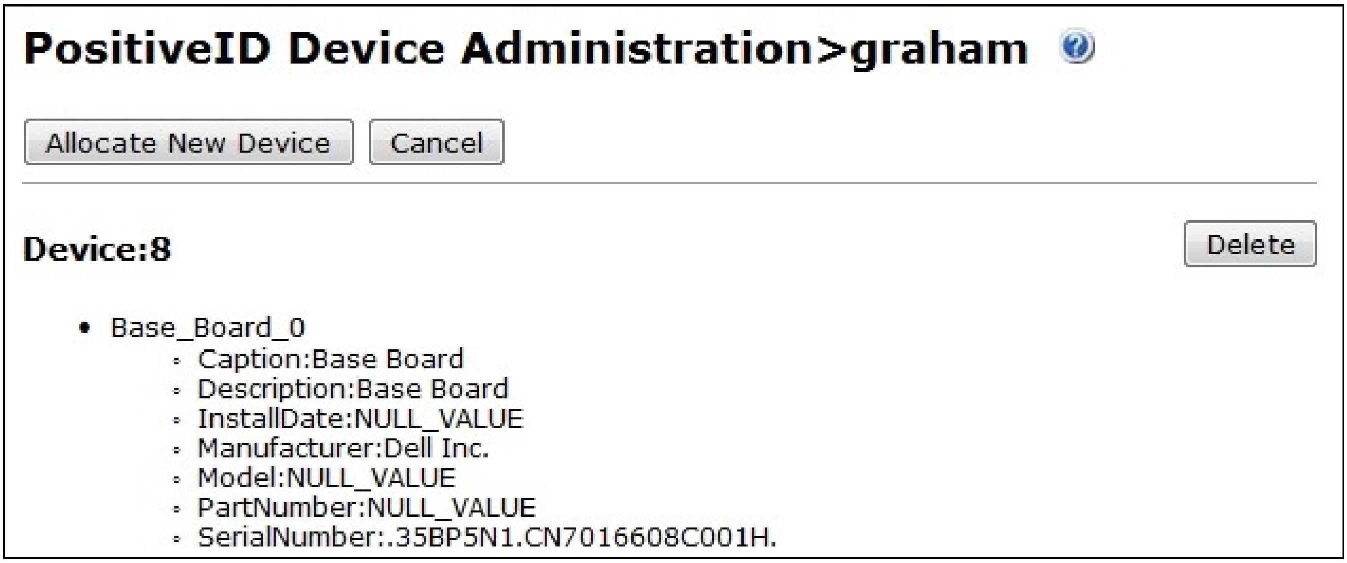
To use PositiveID authentication you must first register your computer with the server. If you already have a registration key please enter it below to procede.

Registration Key: MN55-L7A2Q-W55U5-5M5UQ-MC

434.4.3 Deleting a Registered Device on the PINsafe Administration Console

1. On the PINsafe Administration Console select User Administration then left click the required username, click on PID for that user.

2. Locate the Registered device to be removed then click on Delete. The device should be removed and the PINsafe log will record the following message: **PositiveID device deleted, username: username, id: n**



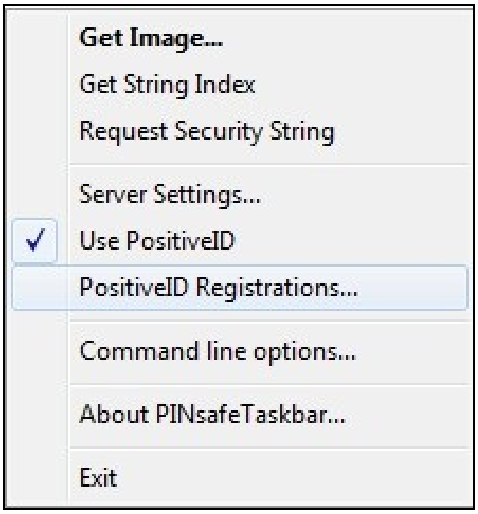
PositiveID Device Administration>graham

Device:8

- Base_Board_0
  - Caption:Base Board
  - Description:Base Board
  - InstallDate:NULL_VALUE
  - Manufacturer:Dell Inc.
  - Model:NULL_VALUE
  - PartNumber:NULL_VALUE
  - SerialNumber:.35BP5N1.CN7016608C001H.

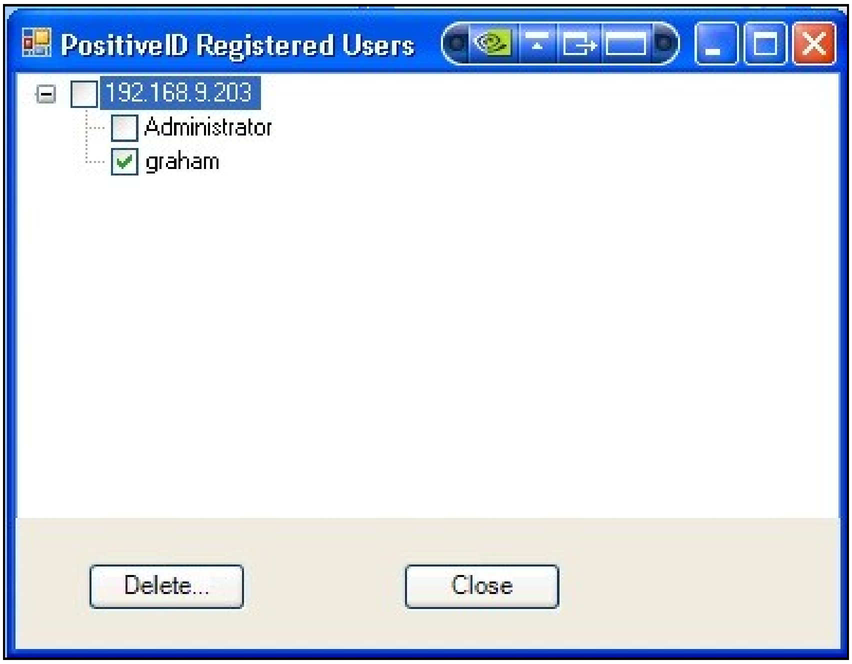
434.4.4 Deleting a Registered Device local PC

1. Right click on the Taskbar and select PositiveID Registrations.



2. Select or expand the PINsafe server with which the device is registered and then select the users from which PositiveID registered devices are to be removed.

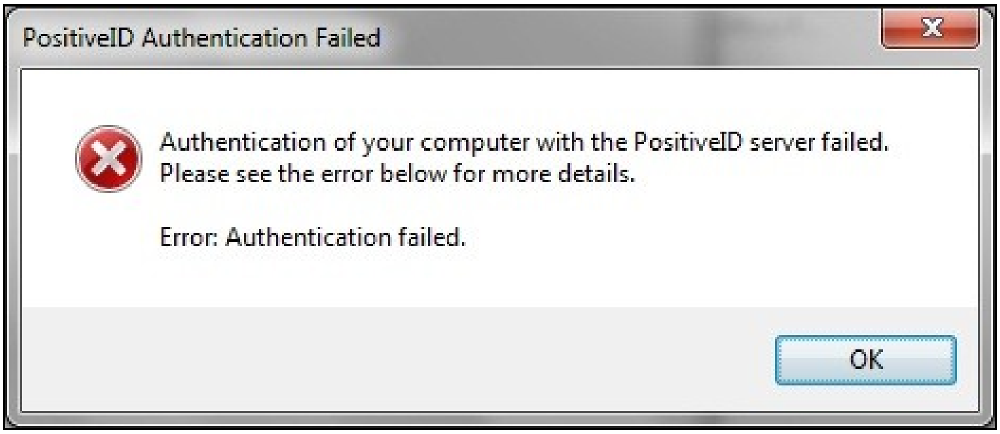
3. Click on Delete to complete the removal.



434.5 Testing

Try to authenticate the user with PositiveID authentication enabled. The user should be able to authenticate. The PINsafe log should have the following:
PositiveID: Authentication successful for device n

Try to authenticate the user with PositiveID authentication disabled in the Taskbar, the authentication should fail.



PositiveID Authentication Failed

Authentication of your computer with the PositiveID server failed.
Please see the error below for more details.

Error: Authentication failed.

434.6 Known Issues and Limitations

The current PINsafe PositiveID does not function with the Windows GINA or Windows Credential provider at login time, but may provide authentication after login to Windows. If this feature is required please contact support.

The current PINsafe PositiveID will not function with the Swivlet/Mobile Phone Client.

434.7 Troubleshooting

PID button is not present

PINsafe patch may not have been applied.

PID button is greyed out and not selectable

PositiveID may not be enabled for that user.

Admin user is a PositiveID User and cannot login

If admins users are created as PositiveID users and cannot login to the Administration console, it is possible to disable the PositiveID authentication.

1). Stop Tomcat

2). Edit the file <path to PINsafe>/webapps/pinsafe/WEB-INF/conf/config.xml and locate the following section.

```
 <string name="class" readonly="true">
           <value>com.swiveltechnologies.pinsafe.server.thirdparty.PositiveID</value>
         </string>
         <choice name="group">
           <option displayValue="repository_groups_no_group">-</option>
           <option generated="true">PINsafeAdministrators</option>
           <option generated="true">PINsafeUsers</option>
           <option generated="true" selected="true">PositiveID</option>
         </choice>
```

3). Remove the line (Where PositiveID is the name of the group of PositiveID users).

```
          <option generated="true" selected="true">PositiveID</option>
```

4). Save the file

5). Start Tomcat

6). Login

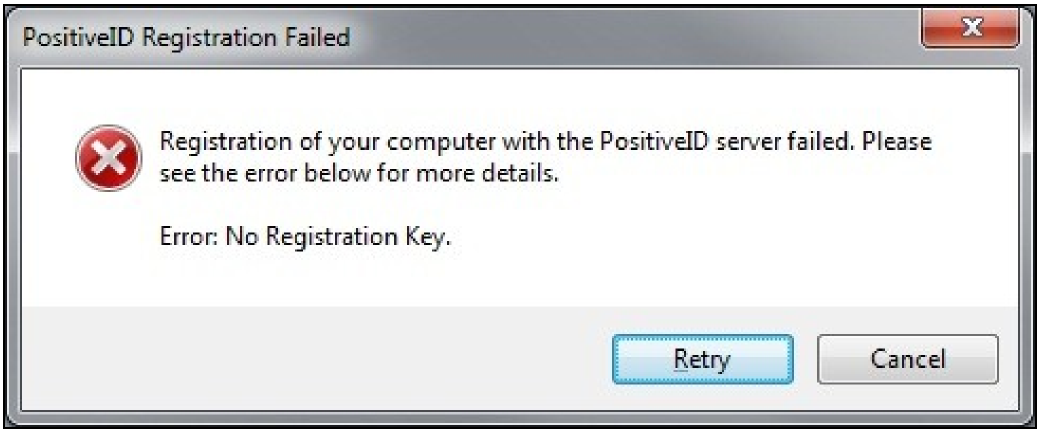
If you still cannot login then see: Administration login

434.7.1 Error Messages

Authentication failed, error: PID_ERROR_DEVICE_NOT_REGISTERED.

An attempt was made by a PositiveID user to authenticate from a device that they were not permitted to authenticate from. If the user should be authenticating correctly, ensure that the device is registered. This error message can also occur if the registered device is removed and the user is trying to register the device again with a new registration key, but the device is already registered to them. See PositiveID How to Guide#Deleting a Registered Device local PC

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: No Registration Key.



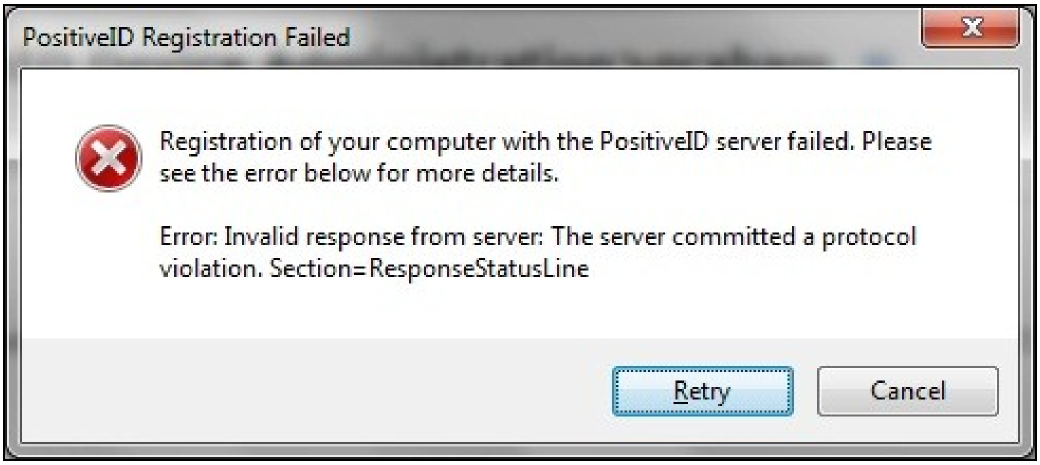
PositiveID Registration Failed

Registration of your computer with the PositiveID server failed. Please see the error below for more details.

Error: No Registration Key.

No registration key was entered during registration of the device

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: Invalid response from the server. The server committed a protocol violation. Scetion=ResponseStatusLine



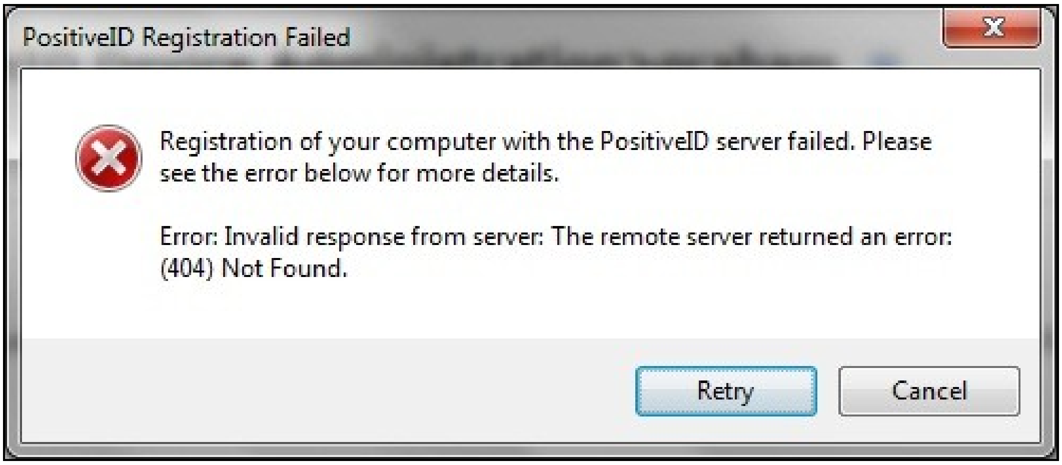
PositiveID Registration Failed

Registration of your computer with the PositiveID server failed. Please see the error below for more details.

Error: Invalid response from server: The server committed a protocol violation. Section=ResponseStatusLine

Check the protocol being used is correct in the Taskbar, and if using https, if a self signed certificate s being used.

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: Invalid response from the server. The remote server returned an error:(404) Not Found



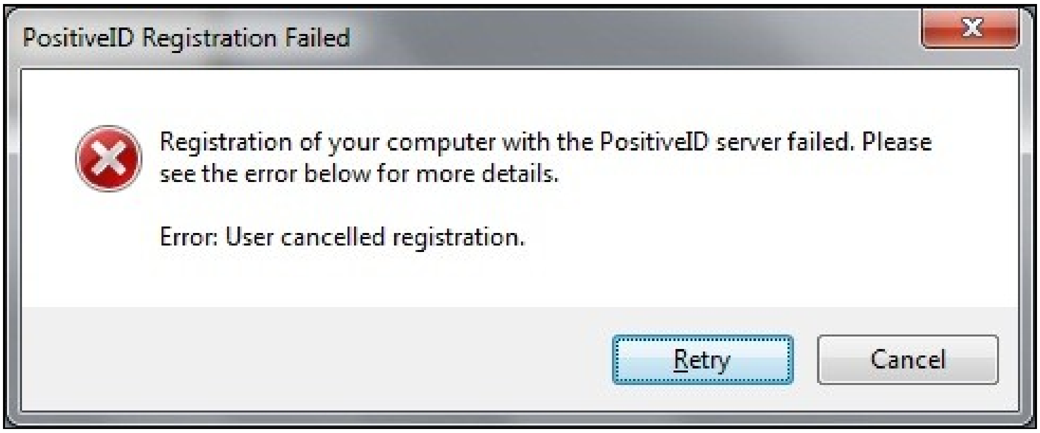
PositiveID Registration Failed

Registration of your computer with the PositiveID server failed. Please see the error below for more details.

Error: Invalid response from server: The remote server returned an error: (404) Not Found.

The PINsafe server has reached a web page that has returned a 404 error, Ensure PINsafe server is available, and that the hostname or IP address and port is correct, or if it is using SSL.

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: User Cancelled registration



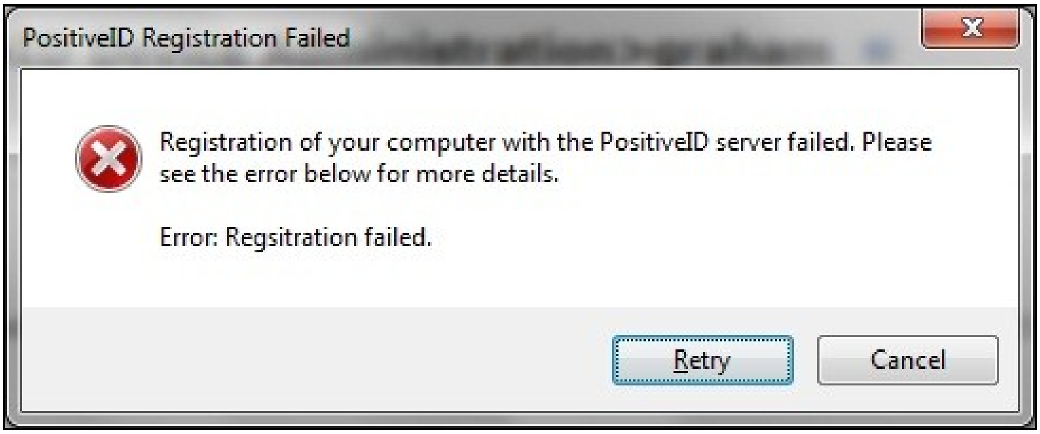
PositiveID Registration Failed

Registration of your computer with the PositiveID server failed. Please see the error below for more details.

Error: User cancelled registration.

The user registering the device cancelled the PositiveID registration process.

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: Registration failed.



PositiveID Registration Failed

Registration of your computer with the PositiveID server failed. Please see the error below for more details.

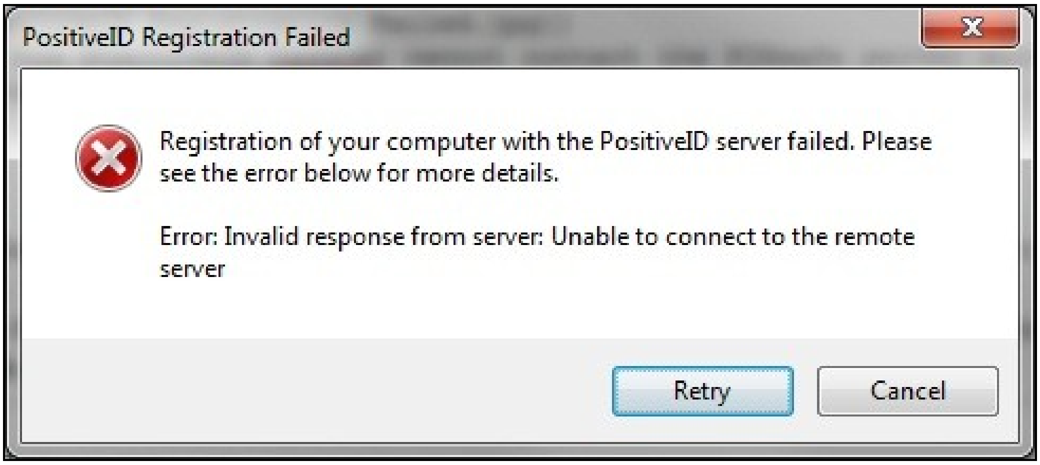
Error: Regsitration failed.

This can occur if the PositiveID Taskbar cannot contact the PINsafe server such as if the PINsafe server is not available or the IP address is incorrect. This can also occur if the Registration key is incorrect and will give the following message in the PINsafe log: **PositiveID: Registration failed for device, error: No such device.** Also if a user has previously registered on that PC they may need to clear out their previous registration, see PositiveID_How_to_Guide#Deleting_a_Registered_Device_local_PC

PositiveID: Registration failed for device, error: No such device.

The PositiveID Registration key was not valid or has been deleted on the PINsafe server before the device could be registered.

Registration of your computer with the PositiveID Server failed. Please see the error below for more details. Error: Invalid response from the server: Unable to connect to the remote server



Registration of your computer with the PositiveID server failed. Please see the error below for more details.

Error: Invalid response from server: Unable to connect to the remote server

The PositiveID registration has received an invalid response, check the IP, Hostname, Port, SSL communications are correct

```
INFO RADIUS: <5> Access-Request(1) LEN=65 192.168.1.1:25292 Access-Request by graham Failed: AccessRejectException:
AGENT_ERROR_THIRDPARTY
```

```
INFO 192.168.1.1 VPN:Login failed for user: graham, error: Third party authentication failed.
```

A Third party authentication such as PositiveID, has failed for the PINsafe user.

435 RADIUS ChangePIN

435.1 Overview

This document covers the RADIUS ChangePIN whereby a user makes an authentication attempt using RADIUS authentication and if they are required to change their PIN Swivel responds with a changepin challenge. The access device can then redirect the user to a ChangePIN page.

435.2 Prerequisites

Swivel 3.x

Access device which supports ChangePIN

RADIUS ChangePIN requires the use of PAP authentication and will not work with CHAP or MSCHAP as these require the OTC to be sent from the Swivel server to the Access device to verify if it is correct.

435.3 Enabling RADIUS ChangePIN

On the Swivel Administration console select RADIUS/NAS, then select the RADIUS NAS entry for which ChangePIN is required. Set the Change PIN warning: to Yes.

435.4 ChangePIN on the Access device

The access device must support RADIUS ChangePIN, and it may be required to modify the request that is sent to the Swivel server.

The Swivel server is expecting a RADIUS response from the Access device in the following format:

cp1=<oldotc>cp2=<newotc>

where <oldotc> is a One Time Code from the security string (Single Channel, SMS, SMTP, Mobile Phone applet)

and <newotc> is the One Time Code from the security string based on what the new PIN is meant to be.

Note: Remember the PIN is never entered, only One Time Codes.

Example: cp1=8593cp2=8791

435.4.1 Example: Juniper

See Juniper ChangePIN

To configure the Juniper to use change pin via RADIUS you need to

- Set a new RADIUS rule on the Authentication server being used, If received packet is Radius-Challenge, action is Show New PIN page.
- Create a customer new New Pin page (NewPin.thtml) that includes the Swivel functionality. Like this Example

435.5 Testing

Test an authentication with a user for which a ChangePIN is required, such as ChangePIN on first login or ChangePIN after an admin reset.

435.6 Known Issues

435.7 Troubleshooting

RADIUS: <0> Access-Request(1) LEN=73 192.168.0.1:52392 Access-Request by null Failed: AccessRejectException: AGENT_ERROR_NO_USER_DATA

INFO Netscaler:Login failed for user: null, error: No data for the user was found.

Check to see if the user exists and the username is correct, if so, on the Swivel Administration console select RADIUS server and set Allow Empty Attributes to Yes.

RADIUS: <15> Access-Challenge(11) LEN=65 192.168.1.100:25292 Access-Request by graham resulted in Access-Challenge.

The Swivel server has returned an Access Challenge response to the Access device. This is expected for ChangePIN.

INFO 192.168.1.100 VPN:User must change their PIN before they can authenticate via Radius: graham.

The user must change their PIN before being allowed to login, this is expected for ChangePIN.

RADIUS: <16> Access-Request(1) LEN=65 192.168.1.100:25292 Access-Request by graham Failed: AccessRejectException: AGENT_ERROR_PIN_NOT_CHANGED

and

INFO 192.168.1.100 VPN:Login failed for user: graham, error: The user was required to change their PIN before this authentication.

User was required to change their PIN but did not, so the next login attempt fails and locks the user account.

WARN 192.168.1.100 VPN:User "graham" has been locked, reason: The user was required to change their PIN before this authentication.

User was required to change their PIN but did not, so the next login attempt has failed and locked the user account.

Users not able to change their PIN

On the Swivel server under RADIUS/Server Try increasing the Session TTL to a higher value and verify that a ChangePIN can be carried out.

436 RADIUS Proxy How to guide

437 Overview

This document outlines how to configure the RADIUS Proxy functionality of PINsafe. For information relating to RADIUS configuration see RADIUS How To Guide. The PINsafe RADIUS proxy has cyclical loop prevention to prevent RADIUS requests being continuually bounced between two RADIUS servers.

438 Prerequisites

PINsafe 3.7 onwards

PINsafe 3.8 onwards for Single Channel Session Proxy

439 Architecture

A PINsafe server can be a RADIUS Client to another RADIUS server, this may be a PINsafe server, requesting authentication information from that server.

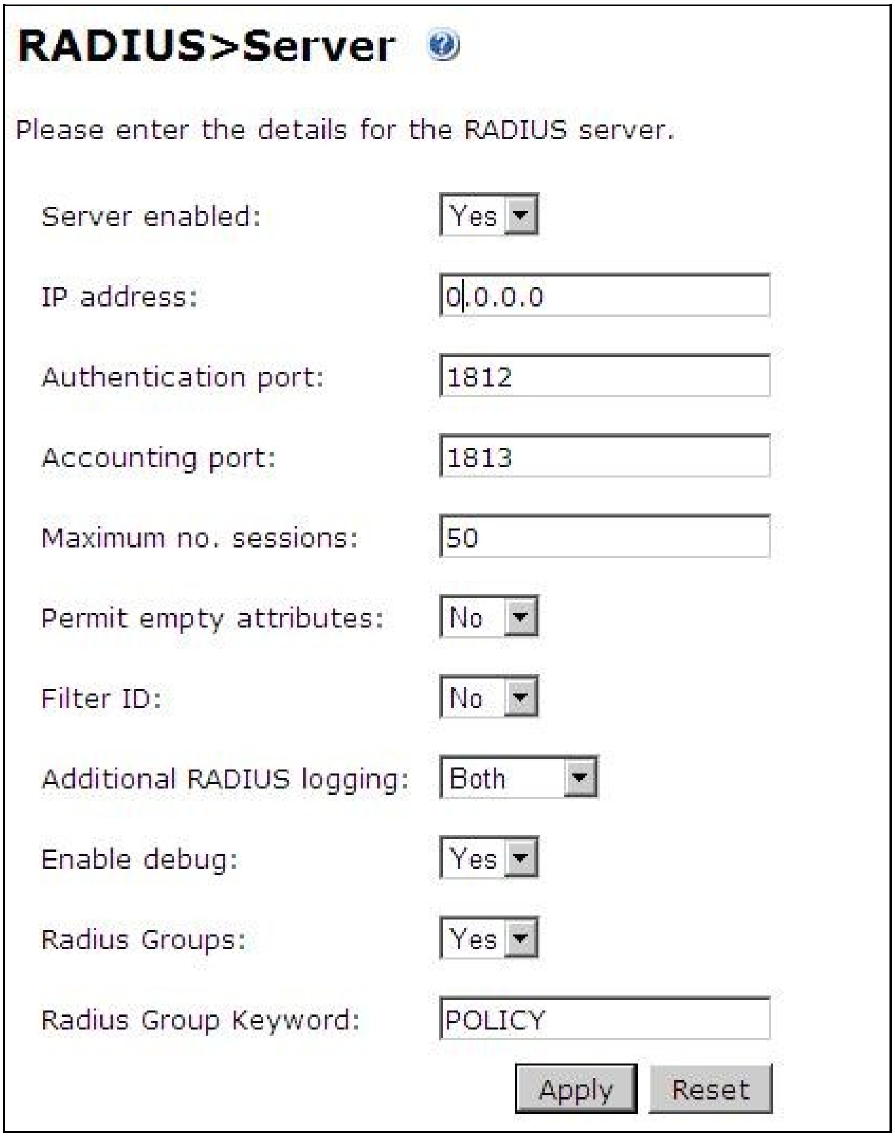
440 RADIUS Proxy Setup

440.1 RADIUS Server Configuration

If the remote RADIUS server is not a PINsafe RADIUS server, follow the vendor documentation for setting up and configuring the RADIUS server.

If the remote RADIUS server is a PINsafe server, configure that PINsafe server with the following. On each instance of PINsafe to be used as a RADIUS server, on the PINsafe Administration console select RADIUS/Server. Ensure Server enabled is set to yes. Leave the IP address field blank unless you wish to explicitly enter the IP address to be used for RADIUS requests (the physical IP address, but not the virtual IP if using a PINsafe HA Pair). Using a blank value or 0.0.0.0 means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for appliances, the PINsafe VIP should not be used as the server IP address, see VIP on PINsafe Appliances



RADIUS>Server

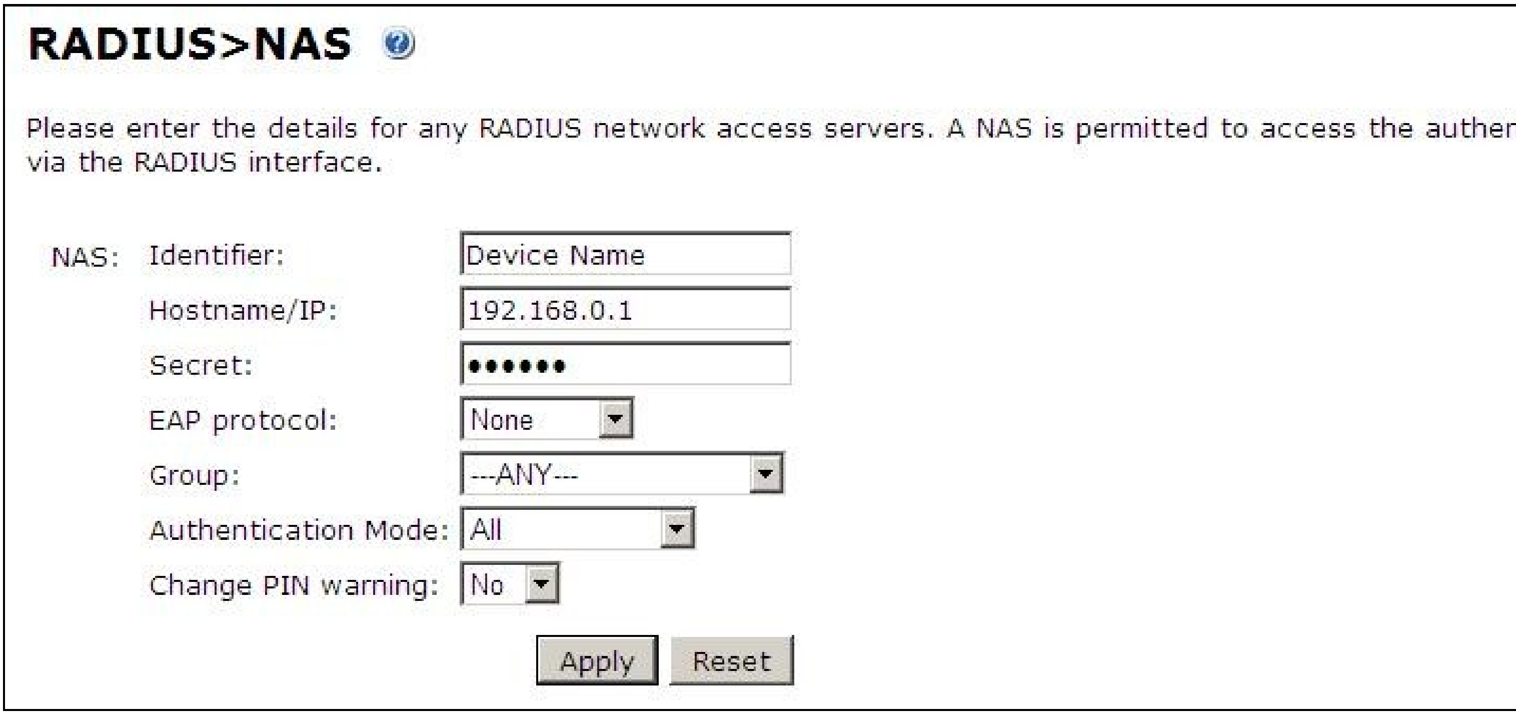
Please enter the details for the RADIUS server.

Server enabled:	Yes
IP address:	0.0.0.0
Authentication port:	1812
Accounting port:	1813
Maximum no. sessions:	50
Permit empty attributes:	No
Filter ID:	No
Additional RADIUS logging:	Both
Enable debug:	Yes
Radius Groups:	Yes
Radius Group Keyword:	POLICY

440.2 RADIUS NAS Configuration

Set up the NAS using the Network Access Servers page in the PINsafe Administration console under RADIUS/NAS. In this case the remote PINsafe server will be the client to the PINsafe server being configured. Create a New Entry and enter a descriptive name and IP address for the other instances of PINsafe that will connect for RADIUS information. The secret assigned will be used on both the PINsafe RADIUS server, and the PINsafe RADIUS Proxy.

Note: If Check Password with repository is configured on the PINsafe appliance making the RADIUS request, then the PINsafe Proxy receiving the request needs to have Check Password with repository enabled, from PINsafe 3.7 onwards this is on the NAS entry.



RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the auther
via the RADIUS interface.

NAS: Identifier: Device Name

Hostname/IP: 192.168.0.1

Secret: ••••••

EAP protocol: None

Group: ---ANY---

Authentication Mode: All

Change PIN warning: No

440.3 Configure the RADIUS Proxy

On the PINsafe instance that will be the RADIUS client, configure it to talk to the remote RADIUS server. On the PINsafe Administration console select Servers/Proxy. Enter a name for the RADIUS server, IP address or hostname, RADIUS authentication port, shared secret that is entered under the RADIUS NAS, and for RADIUS Proxy the conditions that should be met to proxy the request. See the RADIUS Proxy options below.

440.3.1 PINsafe RADIUS Proxy Options

PINsafe 3.7 onwards can proxy RADIUS requests against other RADIUS servers. This allows PINsafe to be inserted into an existing RADIUS infrastructure such as where tokens are being used, so such solutions can be used in parallel.

The RADIUS proxy is set on the PINsafe Administration Console under Server/Peers

The RADIUS proxy functions in the following manner.

Peers: Name: Descriptive Name used for logging information

Hostname/IP: Hostname/IP address of RADIUS server to be proxied against

HTTP port: Default: 8080. Not used in RADIUS Proxy

SSL: Options: Yes/No, Default: No. Not used in RADIUS Proxy

Context: Default: pinsafe. Not used in RADIUS Proxy

RADIUS authentication port: Authentication port to be used for RADIUS server to be proxied against. Usually 1812 or 1645

RADIUS accounting port: Accounting port to be used for RADIUS server to be proxied against. Usually 1813 or 1646

Shared secret: A shared secret which must be the same as that entered on the RADIUS server to be proxied against.

RADIUS Proxy: Options Never/On Passcode/Unknown User. Default: Never. How to handle the RADIUS password that the PINsafe server receives and if it should be proxied, the options for this are:

- Never: No Proxy request is made.
- Unknown User: If the user is not in the PINsafe Database then a proxy request is made.
- On Passcode: If it sees that the user has submitted a one-time code that is at least 6 characters long and that the user: Either (a) does not have an account: Or (b) has an account but has not started a session (eg requested a TURing image or on-demand SMS) then it is treated as a third party code and passed to another RADIUS server.
- No User Session: Available in PINsafe 3.8 onwards. PINsafe can proxy RADIUS requests purely in the absence of a local session for the user making the RADIUS request. Both single channel image requests and dual channel on demand session requests can be used for this entry.

440.4 Testing

RADIUS messages should be seen in the Swivel logs

Access Request(1) LEN=192.168.1.1:1025 PROXY REQUEST to Swivel-Primary (/192.168.1.1)

440.5 Known Issues

440.6 Troubleshooting

Check the Swivel logs.

Some access devices such as the Cisco ASA have a RADIUS test tool

It may be useful to use tcpdump for troubleshooting from the command line

tcpdump -i eth0 port 1812

Check that RADIUS is listening using *netstat -a*

440.6.1 Error Messages

Access Request(1) LEN=192.168.1.2:1025 PACKET DROPPED - Access-Request by username REQUEST PACKET FAILED PROXY VALIDATION AccessDropException: PROXYING to Swivel-Standby FAILED - No such proxy target.

There is a problem connecting to the proxy server. On the Swivel Administration console under RADIUS/Server Stop RADIUS, then Start RADIUS. Check the logs for any error messages, such as RADIUS port cannot be bound or is already in use, if so restart Tomcat and check again.

Access Request(1) LEN=192.168.1.2:1025 PACKET DROPPED - Access-Request by username REQUEST PACKET FAILED PROXY VALIDATION AccessDropException: Packet DROPPED - Proxy target is in a Proxy Loop (Configuration error).

There is a loop whereby each RADIUS server requests RADIUS information from the other. This error usually can be ignored.

441 RADIUS Static Password

442 Overview

Swivel version 3.9.6 onards allows non Swivel users to authenticate with a password set in their repository instead of a Swivel OTC.

This allows a non Swivel user to be authenticated with just their repository password, and can be used for RADIUS testing and health checks.

443 Prerequisites

Swivel 3.9.6 onwards.

Repository with password for user

444 swivel RADIUS setup

The Swivel RADIUS server must be configured, see RADIUS How To Guide.

On the RADIUS NAS set authenticate non-user with just password: to Yes

445 Swivel Repository Configuration

Configure a Repository for user authentication, such as Active Directory, see AD data source configuration. Set the option **Server to use to attempt to authenticate non-users:** to the repository that non Swivel users will have their password checked against.

446 Testing

Attempt a login with the non Swivel user, see RADIUS Testing.

447 Known Issues

448 Troubleshooting

See RADIUS How To Guide.

LOG_LOGIN_NON_USER_PASS, non-swivel-username

This is displayed for a succesful user authentication against a remote repository

Failed to get LDAP context for user CN=non-swivel,CN=Users,DC=swiveldemo,DC=swivelsecure,DC=net

This error can be displayed if the username is correct but the password is incorrect

RADIUS: <18> Access-Request(1) LEN=50 192.168.1.10:49317 Access-Request by non-swivel Failed: AccessRejectException: NON_USER_PASSWORD_FAIL

This error is dispalyed if the password is incorrect

RADIUS DEBUG: Exception in thread: DATAGRAM LEN = 56 FROM 192.168.1.10:57788 java.lang.NullPointerException at com.swiveltechnologies.pinsafe.server.user.repository.AbstractRepositoryBase.getAttribute(AbstractRepositoryBase.java:149) at com.swiveltechnologies.pinsafe.server.radius.RadiusAccess.authenticate(RadiusAccess.java:480) at com.theorem.radserver3.RADIUSSession.o(Unknown Source) at com.theorem.radserver3.RADIUSSession.e(Unknown Source) at com.theorem.radserver3.RADIUSSession.run(Unknown Source) at java.lang.Thread.run(Unknown Source)

This error may be displayed if the username is incorrect

449 Recovery Disk for Appliances How to Guide

449.1 Overview

PINsafe Hardware appliances allow an ISO image to be generated to build a new hardware appliance from new hardware, also known as a 'bare metal recovery'. The created ISO image creates a system backup at the moment of its creation. This can then be brought up to date using regular backups, see Automated FTP Backups. The CMI is not available during ISO creation.

It is recommended to create ISO images before and after any major system changes.

449.2 Prerequisites

449.2.1 Recovery CD Creation Prerequisites

PINsafe hardware appliance

CDROM

Writeable CD's

449.2.2 Recovery CD Usage Prerequisites

PINsafe Hardware appliance to be installed. **Note: This must be of the same hardware type**

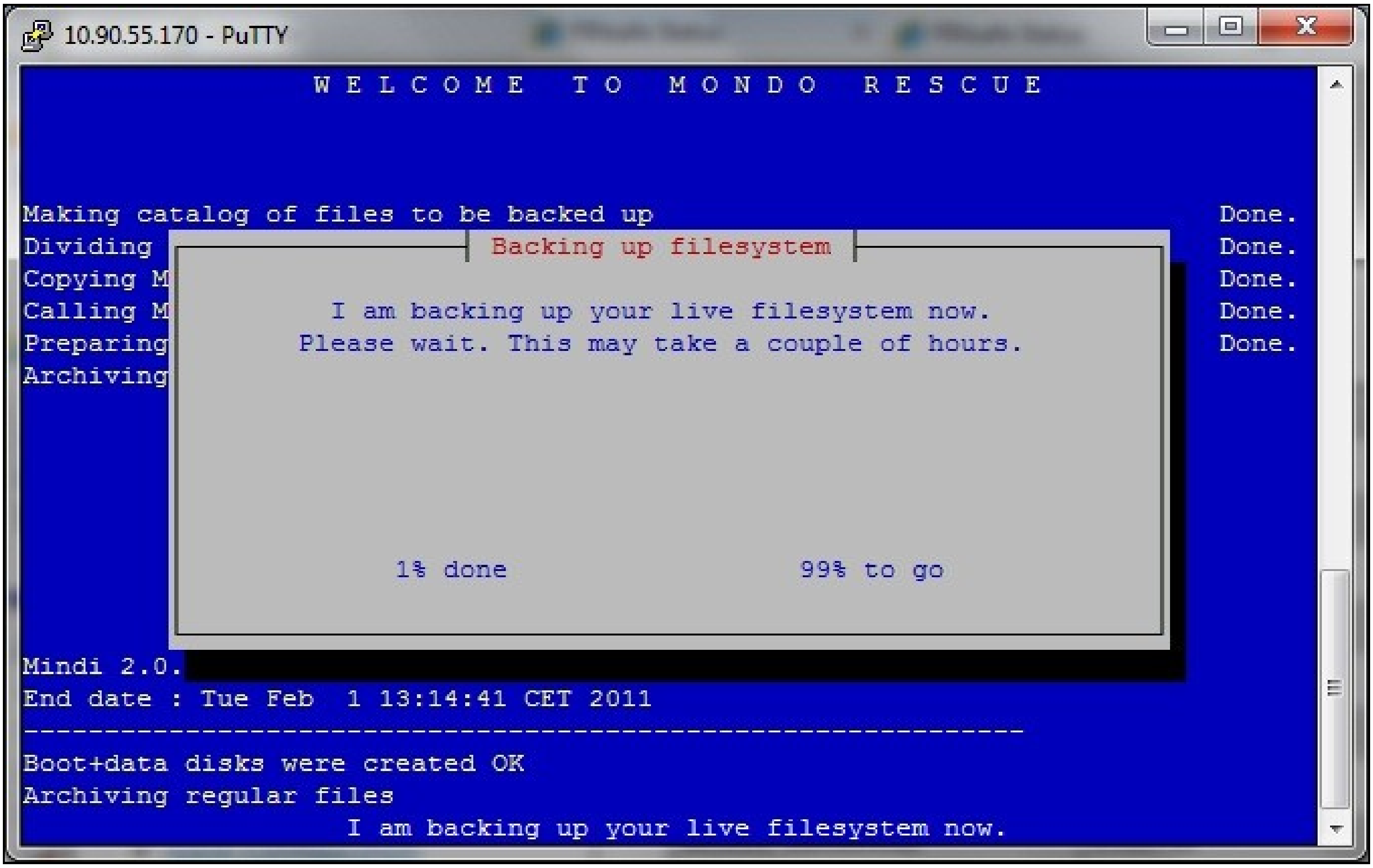
Recovery CD's created earlier

Keyboard, Monitor attached to PINsafe Hardware appliance

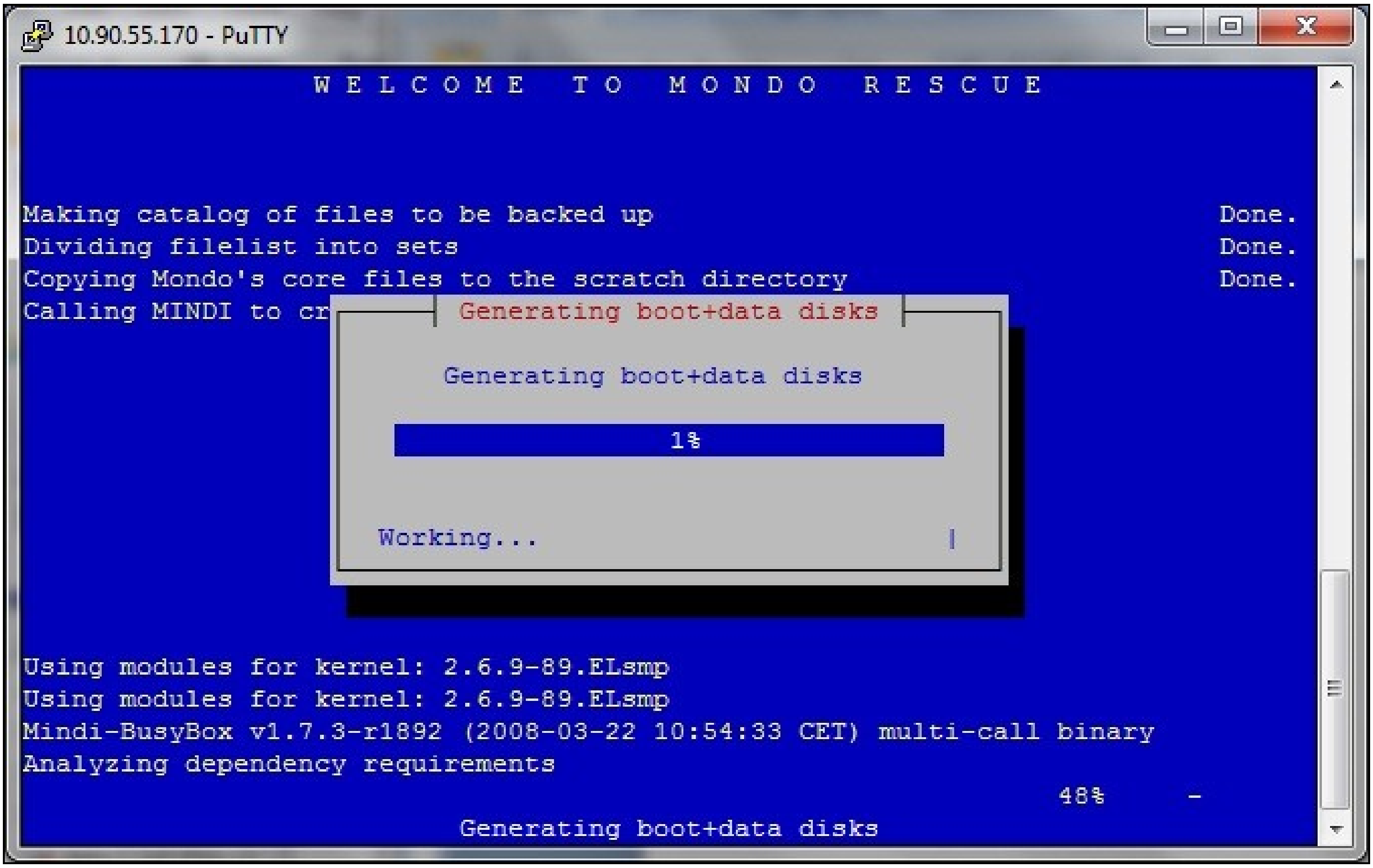
449.3 Creating the Recovery CD

449.3.1 Create the ISO image

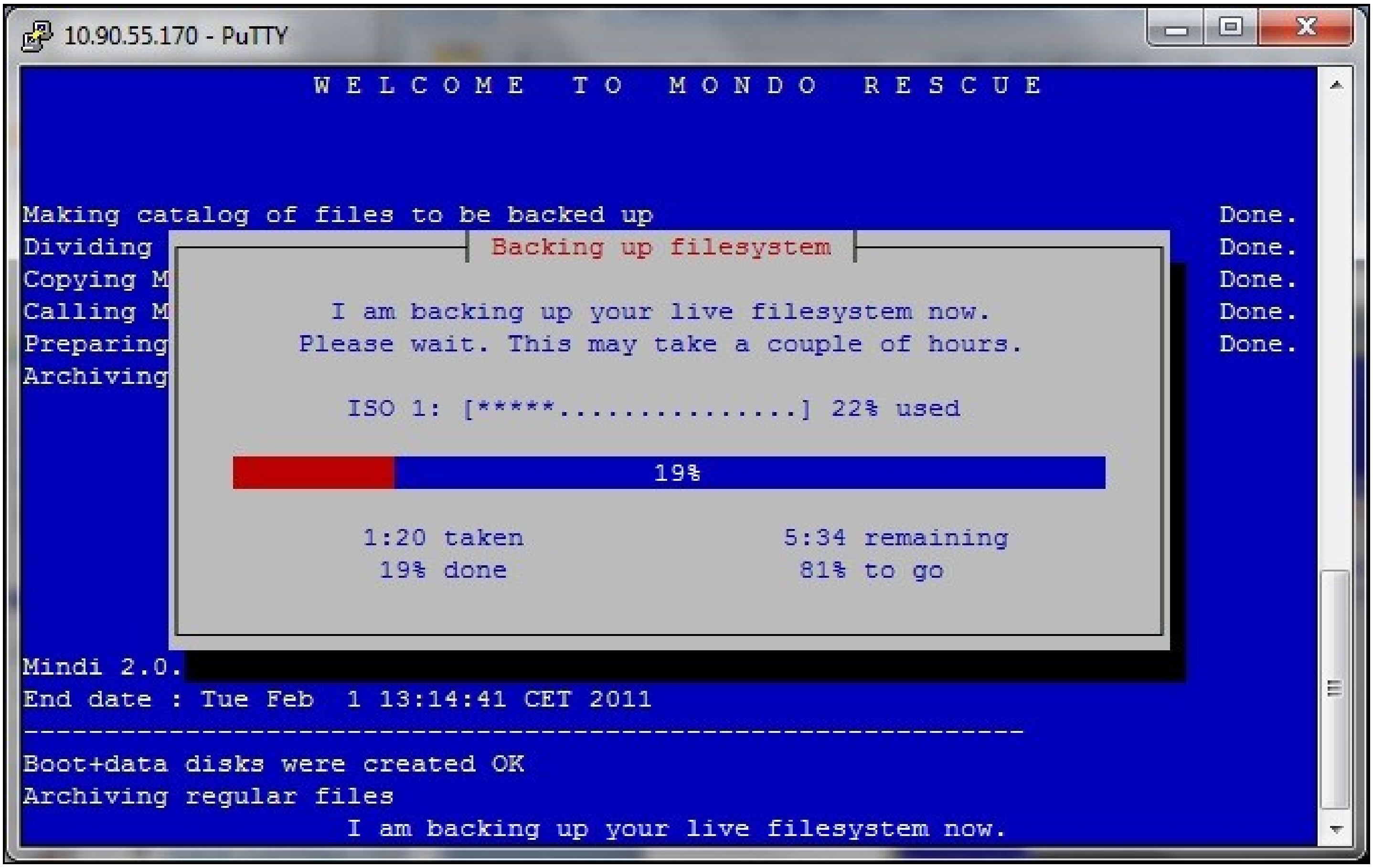
From the PINsafe CMI select the Option for 'Backups and Restore Options', then navigate to the create ISO image option. At the prompt *Are you sure? (Yes/No):* enter *y*



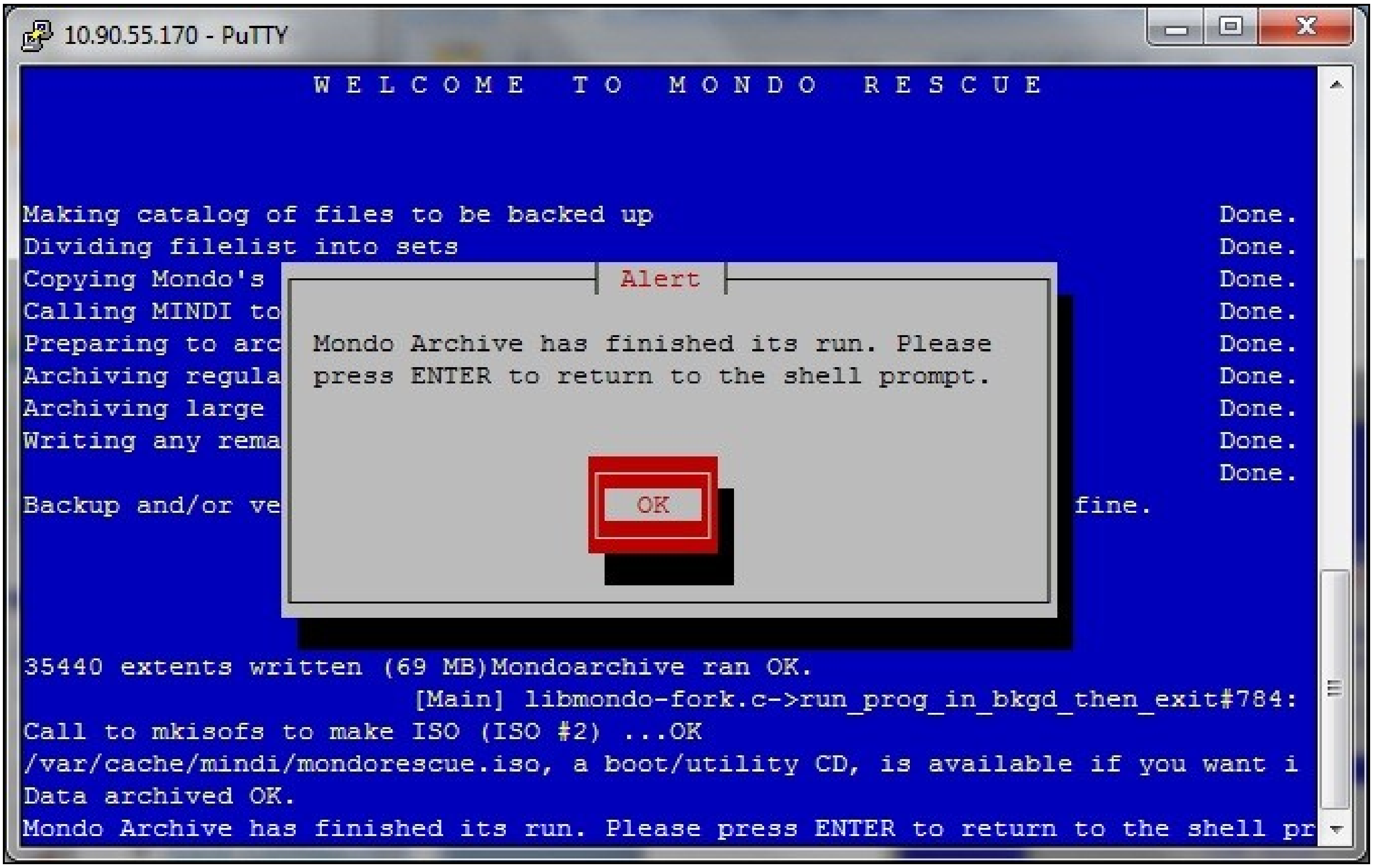
```
                  W E L C O M E   T O   M O N D O   R E S C U E



Making catalog of files to be backed up                               Done.
Dividing                 Backing up filesystem                        Done.
Copying M                                                             Done.
Calling M        I am backing up your live filesystem now.            Done.
Preparing      Please wait. This may take a couple of hours.          Done.
Archiving





                  1% done                       99% to go


Mindi 2.0.
End date : Tue Feb  1 13:14:41 CET 2011
--------------------------------------------------------------
Boot+data disks were created OK
Archiving regular files
                    I am backing up your live filesystem now.
```



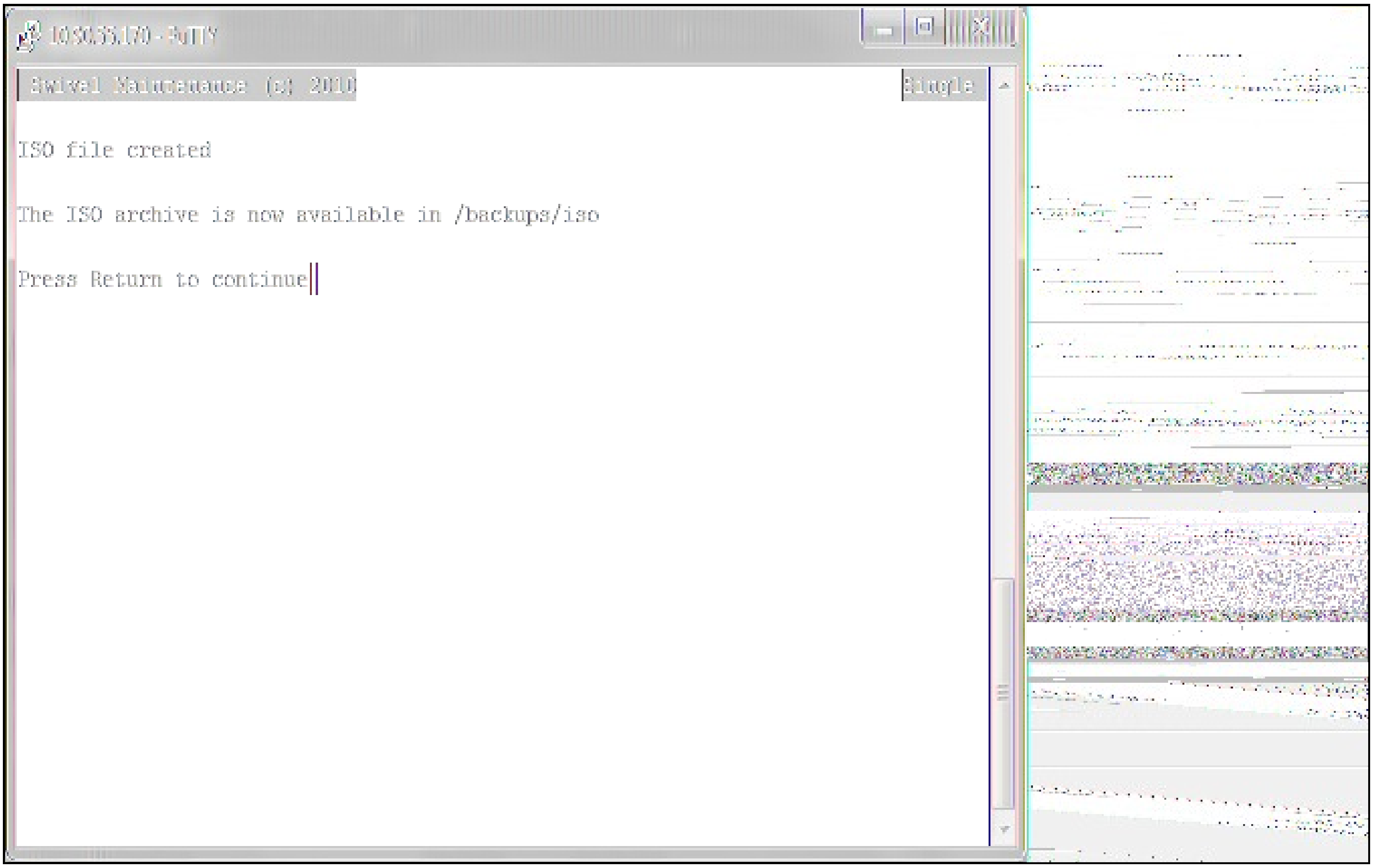
```
                    W E L C O M E   T O   M O N D O   R E S C U E


Making catalog of files to be backed up                                        Done.
Dividing filelist into sets                                                    Done.
Copying Mondo's core files to the scratch directory                            Done.
Calling MINDI to cr ------| Generating boot+data disks |------

                             Generating boot+data disks

                         [                1%                  ]


                         Working...                          |


Using modules for kernel: 2.6.9-89.ELsmp
Using modules for kernel: 2.6.9-89.ELsmp
Mindi-BusyBox v1.7.3-r1892 (2008-03-22 10:54:33 CET) multi-call binary
Analyzing dependency requirements
                                                                      48%      -
                                 Generating boot+data disks
```



```
                    W E L C O M E   T O   M O N D O   R E S C U E


Making catalog of files to be backed up                                        Done.
Dividing  ------------------| Backing up filesystem |-----------------         Done.
Copying M                                                                      Done.
Calling M              I am backing up your live filesystem now.               Done.
Preparing            Please wait. This may take a couple of hours.             Done.
Archiving
                       ISO 1: [*****...............] 22% used

              [                        19%                        ]

                        1:20 taken                 5:34 remaining
                         19% done                   81% to go


Mindi 2.0.
End date : Tue Feb  1 13:14:41 CET 2011
--------------------------------------------------------------
Boot+data disks were created OK
Archiving regular files
                     I am backing up your live filesystem now.
```



```
                  W E L C O M E   T O   M O N D O   R E S C U E



Making catalog of files to be backed up                               Done.
Dividing filelist into sets                                           Done.
Copying Mondo's                                                       Done.
Calling MINDI to                                                      Done.
Preparing to arc      Mondo Archive has finished its run. Please      Done.
Archiving regula      press ENTER to return to the shell prompt.      Done.
Archiving large                                                       Done.
Writing any rema                                                      Done.
                                                                      Done.
Backup and/or ve                                                fine.




35440 extents written (69 MB)Mondoarchive ran OK.
                        [Main] libmondo-fork.c->run_prog_in_bkgd_then_exit#784:
Call to mkisofs to make ISO (ISO #2) ...OK
/var/cache/mindi/mondorescue.iso, a boot/utility CD, is available if you want i
Data archived OK.
Mondo Archive has finished its run. Please press ENTER to return to the shell pr
```



```
Swivel Maintenance (c) 2010                                   Single

ISO file created

The ISO archive is now available in /backups/iso

Press Return to continue
```

449.3.2 Copy the ISO images off of the Appliance

Copy the ISO images off of the hardware appliance from /backups/iso. See Copying appliance files How to Guide. There are usually two ISO images for each hardware appliance.

449.3.3 Burn ISO image

Use your preferred CD recording software to create a CD of the ISO image. (Ensure that the ISO image itself is not burnt onto CD but the file structure within the ISO image). Label the recovery disks as Recovery CD 1 and Recovery CD 2 as appropriate.

449.3.4 Repeat Process for Each hardware Appliance

Each Swivel hardware appliance will have a different configuration. Also Swivel HA Primary, HA Standby, Standalone and DR appliances have different builds so recovery CD's should be created for each appliance.

449.3.5 Testing Recovery CD

Ensure Recovery CD can be read.

449.4 Restoring from a Recovery CD

449.4.1 Install new Hardware

Install the new hardware appliance. A USB or PS2 keyboard and VGA monitor are required to view the console and select the boot options.

449.4.2 Boot from Recovery CD

Note: This process will overwrite any existing data on the Appliance

Insert Recovery CD 1 and power on the appliance.

The following message will appear:

```
Warning: this will restore the data from the recovery disks and overwrite existing data on the PINsafe Hardware Appliance
```

Wait for command prompt of ?boot:? Type RESTORE Press enter

```
boot: RESTORE
```

Observe install and follow any instructions. The process would normally take around 15 minutes.

449.4.3 Restore from latest backup

Use the CMI options to restore the PINsafe server from the latest backup. See Restore Appliance

449.5 Known Issues

The VMware image does not contain the create Recovery ISO image option. Use VMware backups and snapshots as appropriate.

449.6 Troubleshooting

If the ISO image creation terminates early, or the end **OK** button cannot be selected, then the Mondo file creation may appear at the CMI login. Pressing the RETURN key should allow the CMI to be accessible. To remove this message delete the file /tmp/iso.creation

450 Remote Sync Agent

451 Overview

The remote Sync Agent is installed on a repository server such as Active Directory and sends repository information to the Swivel instance.

This document is in development

452 Prerequisites

453 How to Guide

454 Testing

455 Known Issues

456 Troubleshooting

457 Repository

458 Overview

Configuration and use of the Swivel Repository

459 Configuration Considerations

During initial configuration, it is recommended to use an Internal XML repository, this can be removed later if required.

When using an external database such as MySQL, ensure all Swivel servers are set to the same timezone before installation of Swivel, and once set that timezone should not be altered as it will invalidate the PIN number decryption. When setting the time zone restart the database i.e. for internal restart Swivel or MySQL for appliances.

460 What is a Repository?

A repository is a data source of information. Each set of repositories must have a unique name and contain unique usernames. The various forms of repository are:

XML Repository: A data source stored and entered on the Swivel server. Swivel 3.9 onwards supports multiple XML repositories, earlier versions support only one XML repository on each Swivel server

Active Directory Repository: AD groups can be configured as data sources. Multiple AD servers and groups can be configured, the Global Catalogue can also be used.

LDAP Repository: LDAP groups can be configured as data sources. Multiple LDAP servers and groups can be configured.

SQL Repository: SQL groups can be configured as data sources. Multiple SQL servers can be configured. Swivel needs to know in which fields the data is stored, so a java class is written to read the database, see SQL as a data source How To Guide.

ADAM Repository ADAM (AD-LDS) can be used as a data source, this has the potential to be writable source.

LDAP Writeable Repository LDAP can be used as a data source, this has the potential to be writable source.

461 Repostory Options

Delete users with server: Yes/No, default: No. If set to Yes and the repository is deleted, then users will be deleted as well. If set to No, then the associated users will not be deleted.

Allow user repository to change: Yes/No, default No. If set to yes then it will allow users whose repository changes, to change their repository in Swivel. If set to No, the user will remai in the existing repository.

Server to use to attempt to authenticate non-users: This provides a drop down list of repositories against which non Swivel users can be checked for authentication.

462 Removing a Repository?

A repository is removed when all the members of that repository have been deleted and then the repository is deleted. If users are left in the repository then the repository will be visible in the User Administration. If the repository is deleted with users remaining, then it will still be visible in the User Administration as an orphaned repository.

To remove the Repository completely on the Swivel Administration Console:

- Select Repository/Servers and set the Delete Users with Server to Yes

To remove an orphaned repository:

- Recreate the repository with exactly the same name and then remove it with the set the Delete Users with Server to Yes

463 Working with Active-Active Configurations

In an Active-Active configuration the data is written into an external database or Data Store. It is recommended that only one Swivel server reads the repository data source at any one time. Each **repository** and **username** must be unique, *for example an admin user cannot exist on the XML database in both the primary and secondary Swivel servers.* Below is a recommended configuration for Active-Active-DR-DR Swivel servers using internal repositories, to avoid confusion it is suggested that only one local XML repository be used for XML user data:

Server	Repository Name	Admin name
Primary Swivel server	primary_local	primary_admin
Standby Swivel server	standby_local	standby_admin
DR1	dr1_local	dr1_admin
DR2	dr2_local	dr2_admin

XML users should be added onto the Primary Swivel server, and with an external data store they can be viewed on all Swivel servers. If the primary Swivel server is to be removed or taken down for a lengthy period then users can be added to the secondary server.

464 Known Issues

Swivel 3.10 and 3.10.1, 3.10.2, 3.10.3 A user with an '_' in their name cannot bel deleted from the XML repository. Upgrade to 3.10.4.

465 Troubleshooting

- Q. On the User Administration screen, I cannot select a repository. I can only see the text "repository_all" where the Repository drop down menu should be.
    - A. Ensure that you have not got the Shipping database selected on the Database -> General screen.

466 ResetPIN How To Guide

466.1 Overview

For the ResetPIN user guide see ResetPIN User Guide For information on the AGENT-XML ResetPIN see AuthenticationAPI#Reset and the Helpdesk AGENT-XML HelpdeskAPI#Reset

The ResetPIN utility version 4038 includes a Mobile Provision Code utility. For information and using and configuring this see: Mobile Re-Provision How to Guide. Virtual or hardware Appliances 2.0.12 and earlier include the old version of ResetPIN, see below for upgrade information.

ResetPIN may be used by a user to receive a new PIN. The user is directed to a web page where they enter their username and click on request code. They are sent to their mobile phone a request code which they enter into the web page. If this is correctly entered the user is sent a new PIN number to their transport. **It is not possible to perform a self reset if the user is locked**. If a user has been locked out due to too many incorrect logins, they must contact the helpdesk to be unlocked. Self reset can be used if the user has forgotten their PIN, but has not tried too many times to authenticate. For security reasons the PIN Reset Application does not tell a user their current PIN number.

- ResetPIN can be used with dual channel (SMS or email) authentication, the Reset code and PIN is sent to the users Alert Channel, see Transport Configuration.
- ResetPIN uses XML authentication not RADIUS to authenticate to the Swivel server.
- ResetPIN uses session ID rather than username for authentication, so Allow session request by username is not required.
- Changes to the ResetPIN application may be applied by restarting Tomcat.
- Additionally there is a IIS version of the ResetPIN application.

ResetPIN has a timeout value and is located under Server -> Jobs -> Session Cleanup (this value also sets the the validity of single channel images and dual channel On Demand security strings).

466.1.1 ResetPIN and Password

ResetPIN will also reset a users Swivel password to a blank value. It will not reset a users AD or LDAP password.

466.2 ResetPIN software

The ResetPIN software can be downloaded from the Software download page

To upgrade the ResetPIN software see ResetPIN upgrade for PINsafe 3.8 How To Guide

466.3 Installing ResetPIN

Virtual or hardware appliances: ResetPIN is already installed on the Appliances in the webapps2 folder

Software Install (Non Appliances): To install extract from the zip file and copy the resetpin.war file to the <path to Tomccat>/webapps folder. It will automatically deploy when Tomcat is running.

466.4 Connecting to ResetPIN

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

software install: http://IP:8080/resetpin

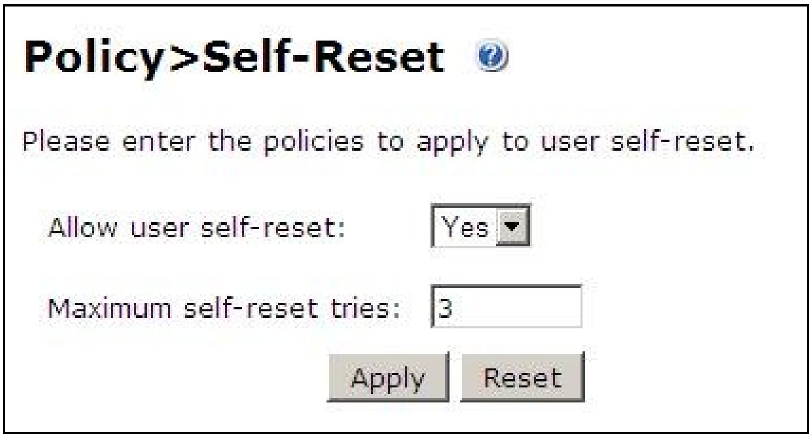
or for the new version

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

software install: http://IP:8080/reset

466.5 Configuring Swivel to allow ResetPIN

Swivel must be configured to allow the ResetPIN utility. On the Swivel Administration console select Policy/Self-Reset and set the Allow user self-reset to Yes.



Policy>Self-Reset

Please enter the policies to apply to user self-reset.

Allow user self-reset: Yes

Maximum self-reset tries: 3

Send reset code as security string: Yes/No. If set to Yes, then the users reset code will be sent by their security string transport instead of their Alert transport.

466.6 Default Configuration files

The configuration file settings.xml file located at:

Virtual or hardware appliance: /usr/local/apache-tomcat-5.5.20/webapps2/resetpin/WEB-INF/settings.xml

Windows Software <path to Tomcat>/webapps/resetpin/WEB-INF/settings.xml

The configuration of ResetPIN is in the file settings.xml with the following default values

```
<?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="secret">secret</entry>
<entry key="redirect">http://www.swivelsecure.com</entry>
</properties>
```

ResetPIN version 4038 path is reset/WEB-INF/settings.xml and has the following default configuration file:

```
<?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.google.com</entry>
</properties>
```

466.7 ResetPIN options explained

ssl: true/false, for communication between ResetPIN and the Swivel server

server: the Swivel server hostname for IP address, for communication between ResetPIN and the Swivel server

port: the port used to communicate with the Swivel server for IP address, for communication between ResetPIN and the Swivel server. For a Swivel virtual or hardware appliance this should be 8181, for a software install it should be 8080

context: the install name of the Swivel application, usually Swivel for IP address, for communication between ResetPIN and the Swivel server

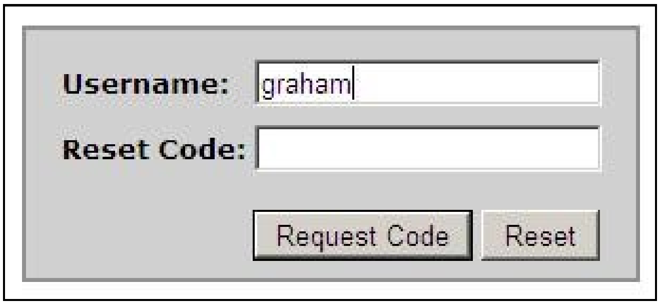
secret: the shared secret, must also be entered under Server/Agent on the Swivel console for IP address, for communication between ResetPIN and the Swivel server

redirect: redirects on completion of ResetPIN, remove the line for no redirect, this must be an address uses can get to

Additionally the ResetPIN has a limited time in which the Reset Code must be entered. By default this is two minutes, but can be changed the the required value on the Swivel administration console by selecting Server/Jobs, and setting the Session Cleanup value.

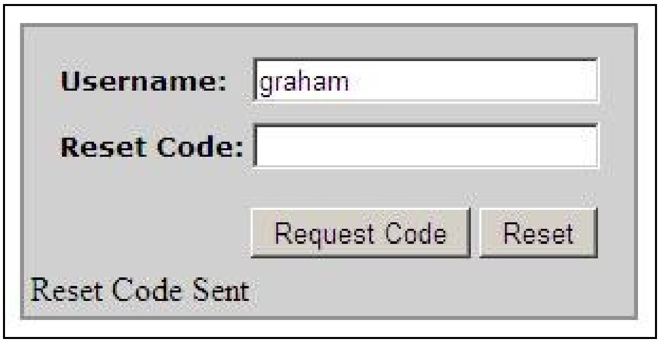
466.8 ResetPIN Sample

Entering the ResetPIN request Page


Username: graham

Reset Code:

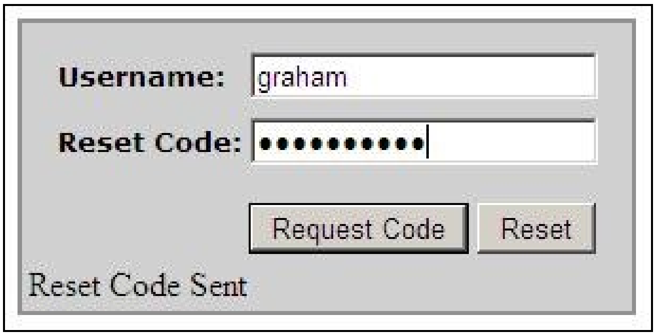
ResetPIN request


Username: graham

Reset Code:

Reset Code Sent

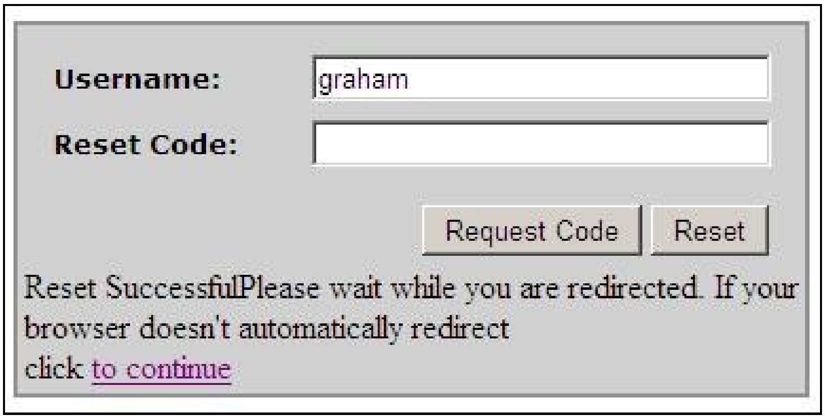
ResetPIN Code sent


Username: graham

Reset Code: ●●●●●●●●●●

Reset Code Sent

ResetPIN request Successful


Username: graham

Reset Code:

Reset SuccessfulPlease wait while you are redirected. If your browser doesn't automatically redirect
click to continue

466.9 Bulk ResetPIN

It is possible to change large number of users PIN numbers using a list of usernames that you wish to reset in bulk and prepare some XML for the Admin API. Please see the following article section:

http://kb.swivelsecure.com/wiki/index.php/AdminAPI#Reset

466.10 Known Issues

If self-reset is enabled, then users who fail the requisite number of login tries are not actually marked as locked, although they are not permitted to log in, so are effectively locked. The reason for this is so that they can use self-reset to unlock themselves.

Unfortunately, because they are not marked as locked, they don't get a message telling them that they have failed login too many times.

Note that users who were locked BEFORE reset pin was enabled WILL be marked as locked, and so won't be able to use reset pin.

If resetPIN is enabled then the automated time based automated account unlock will be disabled.

466.11 Troubleshooting ResetPIN

Check the Swivel logs

If the resetPIN fails when installed on a virtual or hardware appliance when using a self signed certificate, verify the port used is 8181 and not 8080.

ResetPIN will not function for PINless users as they have no PIN.

466.11.1 ResetPIN log messages

Swivel ResetPIN Code sent to user

```
Message sent to user: graham, destination:
```

ResetPIN incorrect code entered

```
Self-reset failed for user: graham.
```

ResetPIN entered correctly

```
Self-reset code request successful for user: graham
```

User requests a ResetPIN code

```
Self-reset code created for user: graham
```

ResetPIN correcly entered ans a new PIN has been generated for the user

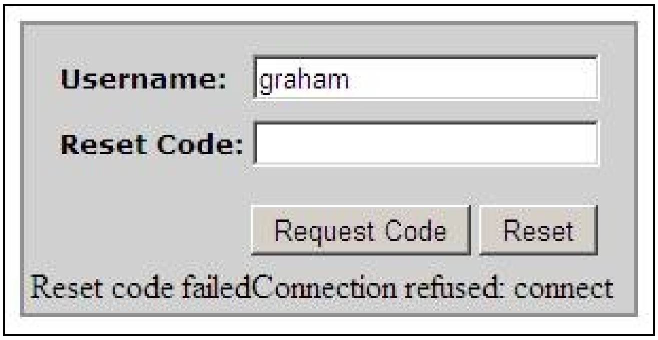
```
PIN created for user: graham
```

466.11.2 ResetPIN error messages

Reset code failed Connection refused: connect

Note: The resetPIN error message given is *Reset code failedConnection refused: connect*

Incorrectly configured ResetPIN due to wrong Swivel IP or port



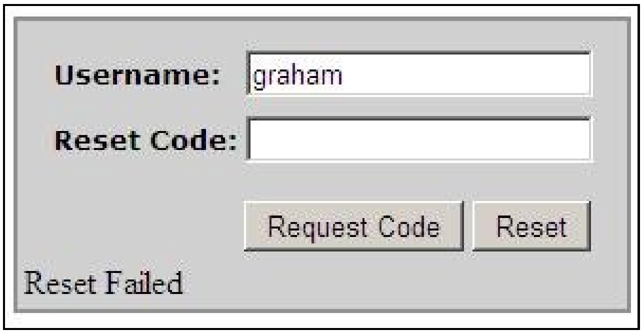
Username: graham

Reset Code:

Reset code failedConnection refused: connect

Reset Failed

Incorrect code entered



Username: graham

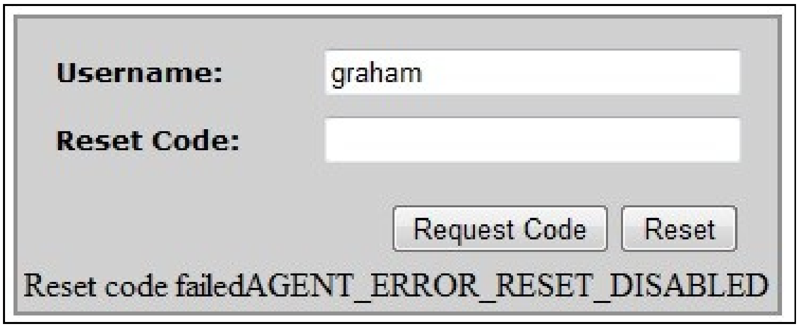
Reset Code:

Reset Failed

Reset code failed AGENT_ERROR_RESET_DISABLED

Self-reset code request failed for user: graham, error: User self-reset is disabled.

reset pin has not been enabled. To enable the reset pin on the Swivel Administration console select reset pin and change Allow user self-reset: to Yes.


Username: graham

Reset Code:

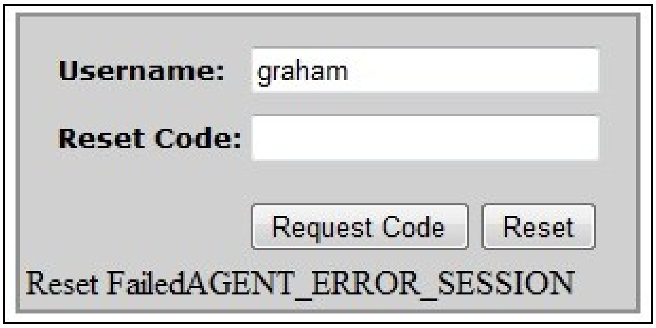
Reset code failedAGENT_ERROR_RESET_DISABLED

Reset Failed AGENT_ERROR_SESSION

Self-reset failed for user: graham, error: A valid session could not be loaded or created for the user.

Note: The resetPIN error message given is *Reset FailedAGENT_ERROR_SESSION*

The reset pin value has time out. User must use the Reset Code within the session cleanup time. For further information see Session Cleanup


Username: graham

Reset Code:

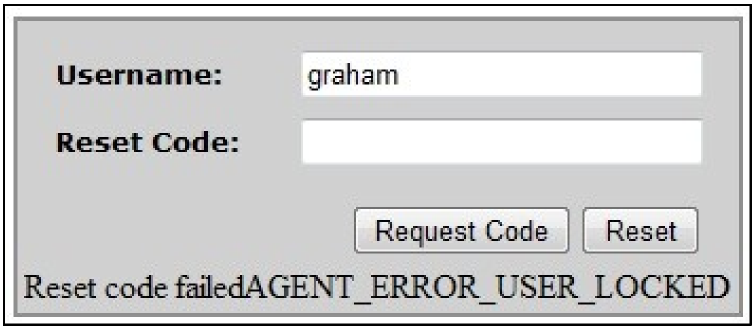
Reset FailedAGENT_ERROR_SESSION

Reset code failed AGENT_ERROR_USER_LOCKED

Self-reset code request failed for user: graham, error: The user account is locked

Note: The resetPIN error message given is *Reset code failedAGENT_ERROR_USER_LOCKED*

The user account has been locked and a reset pin cannot be performed until the account has been unlocked.


Username: graham

Reset Code:

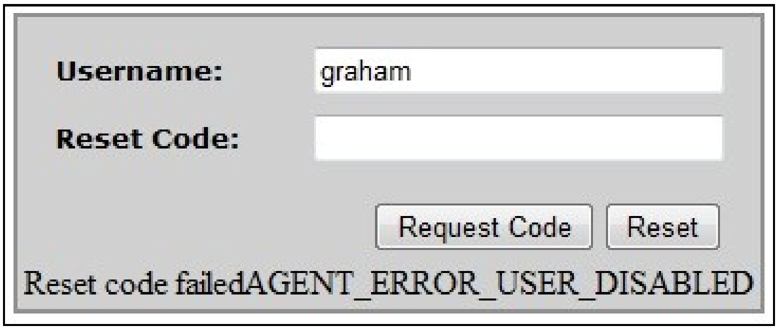
Reset code failedAGENT_ERROR_USER_LOCKED

Reset code failed AGENT_ERROR_USER_DISABLED

Self-reset code request failed for user: graham, error: The user account is disabled.

Note: The resetPIN error message given is *Reset code failedAGENT_ERROR_USER_DISABLED*

The user account has been disabled and a reset pin cannot be performed until the account has been enabled.



Username: graham

Reset Code:

Reset code failedAGENT_ERROR_USER_DISABLED

467 Retrieving PINsafe backup files using Webmin

468 Overview

Before changing Swivel configuration settings it is suggested that you take a backup of the current configuration. This will allow the application to be restored to its current state in the event of a problem. One benefit being that the configuration may also be copied to a different appliance, in the event of an appliance being exchanged due to a fault.

- This article contains a step-by-step process to copy a backup file from the appliance to a PC.
- This article is intended for an intermediate user.

If you've not yet taken a backup of your appliance(s), please see the following articles:

- Backup Appliance
- Backup PINsafe on a Active/Active appliance
- Backup PINsafe on a Active/Passive appliance

For further information on copying files with appliances see: Copying appliance files How to Guide and Automated SCP Backups.

469 Solution

It is possible to take a range of back-ups from Swivel via the CMI. It is now possible on newer appliances to automate retrieval of backups using FTP, see the Automated FTP Backups article. However it may be required to retrieve these backup images manually from the Swivel server.

This article explains the various manual options available.

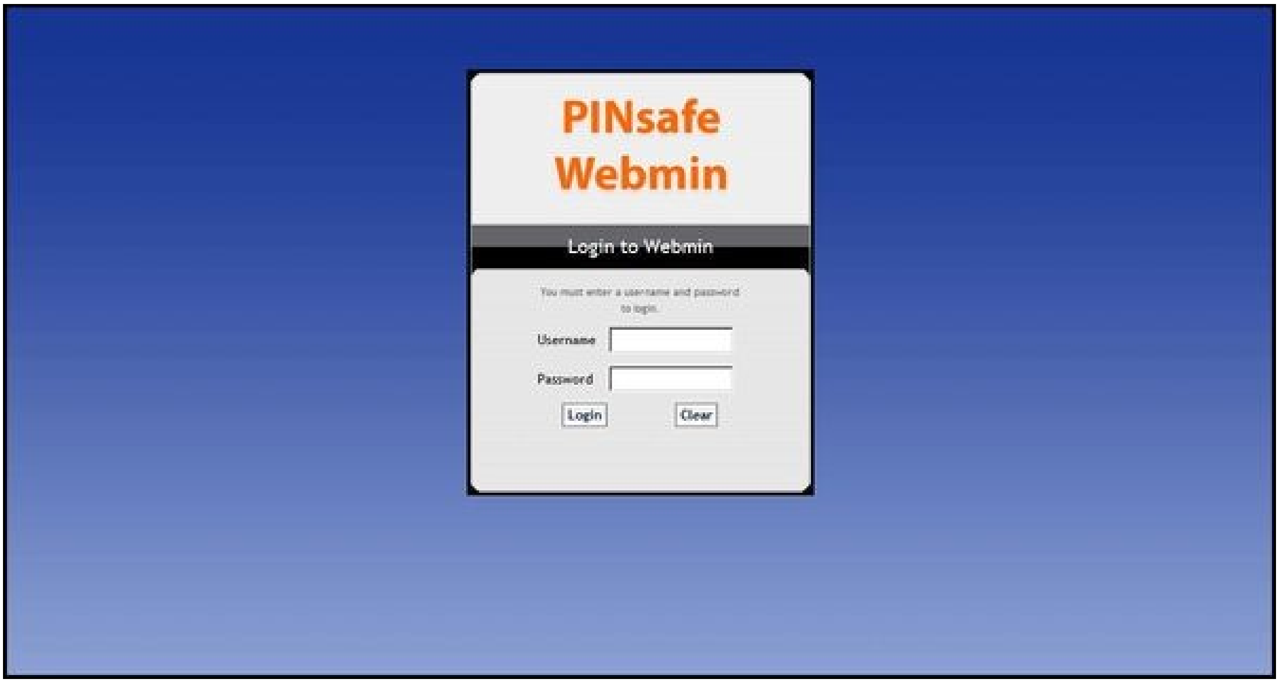
469.1 Copy a backup file from the appliance using Webmin

Login to the Webmin console via the following URL:

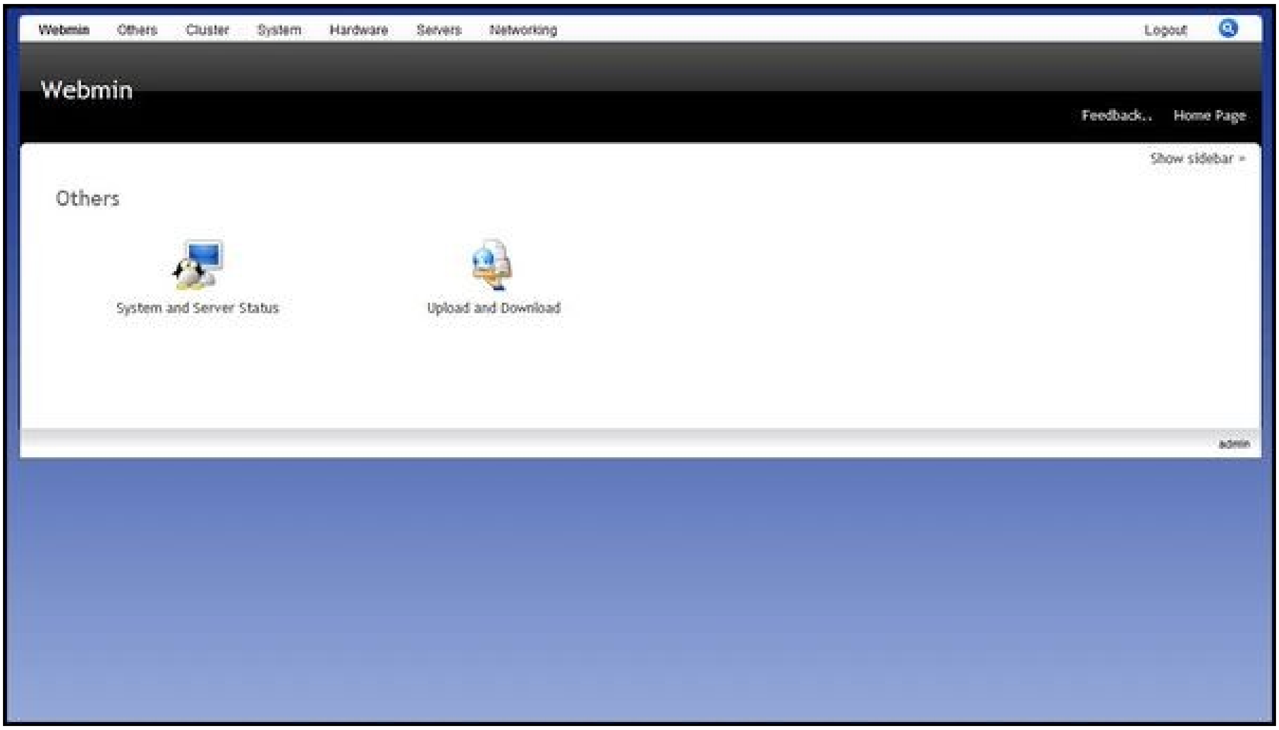
- https://ApplianceIP:10000/

The Login page will be displayed. The default credentials are:

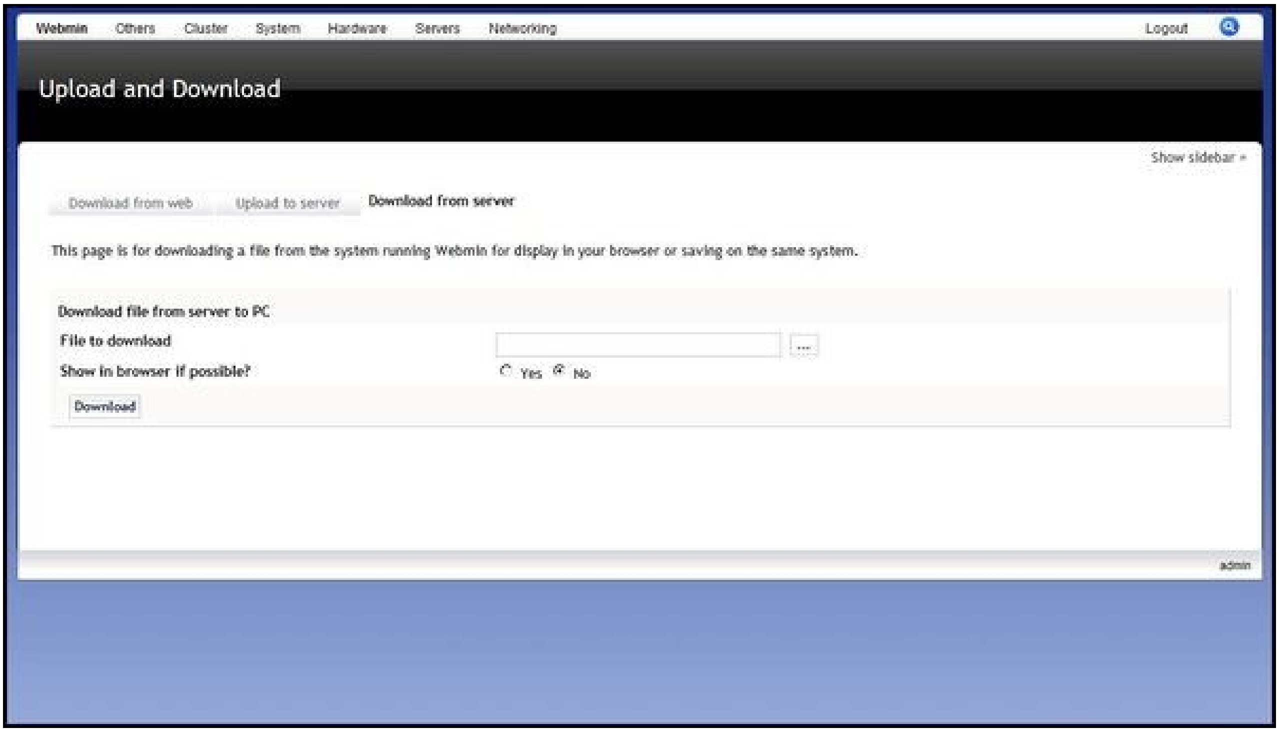
- Username: admin
- Password: lockbox



Once you've logged in, select the 'Others -> Upload and Download' option from the menu bar:



Select the tab entitled "Download from server":



This page is for downloading a file from the system running Webmin for display in your browser or saving on the same system.

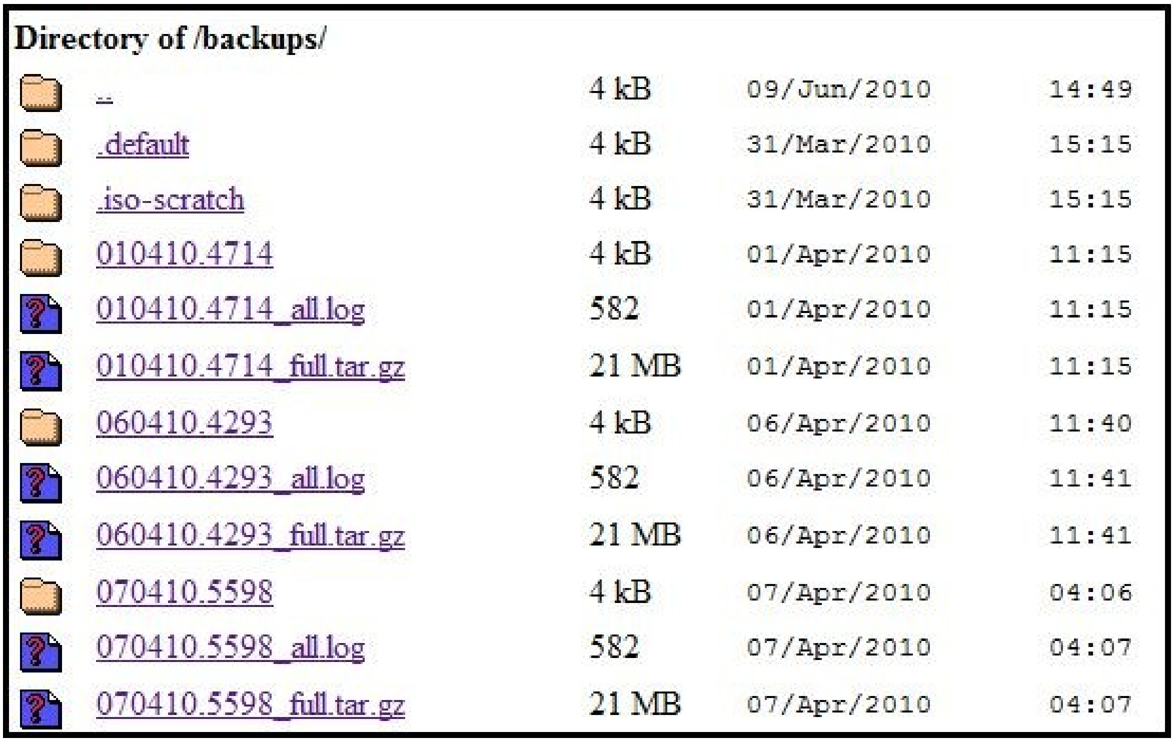
Download file from server to PC

File to download

Show in browser if possible? ○ Yes ● No

Download

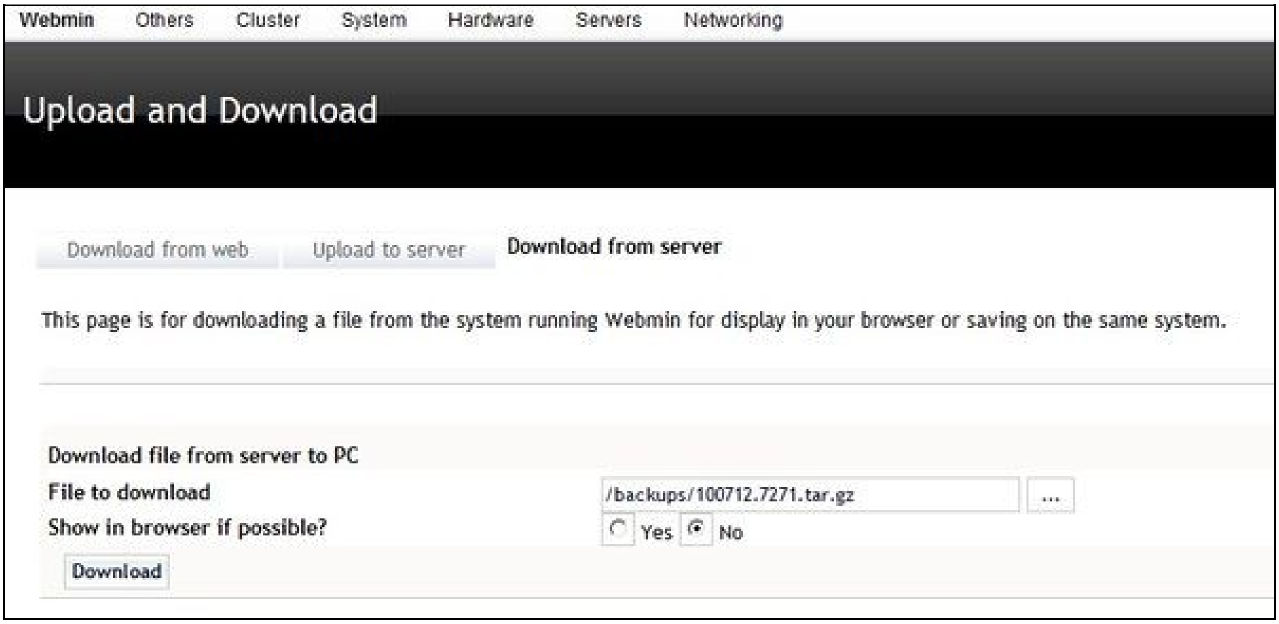
Click the button to the right of the "File to download" dialogue box:



Directory of /backups/

```
..                        4 kB    09/Jun/2010   14:49
.default                  4 kB    31/Mar/2010   15:15
.iso-scratch              4 kB    31/Mar/2010   15:15
010410.4714               4 kB    01/Apr/2010   11:15
010410.4714_all.log       582     01/Apr/2010   11:15
010410.4714_full.tar.gz   21 MB   01/Apr/2010   11:15
060410.4293               4 kB    06/Apr/2010   11:40
060410.4293_all.log       582     06/Apr/2010   11:41
060410.4293_full.tar.gz   21 MB   06/Apr/2010   11:41
070410.5598               4 kB    07/Apr/2010   04:06
070410.5598_all.log       582     07/Apr/2010   04:07
070410.5598_full.tar.gz   21 MB   07/Apr/2010   04:07
```

- Traverse the filesystem by double clicking the links
- Navigate to: /backups
- Select the backup file you wish to download
- Click OK, the required file should be listed



Upload and Download

This page is for downloading a file from the system running Webmin for display in your browser or saving on the same system.

Download file from server to PC

File to download: /backups/100712.7271.tar.gz

Show in browser if possible? ○ Yes ● No

- Click Download to download the required backup

469.2 Copy a backup file from the appliance using WinSCP

See WinSCP How To Guide

Keywords: appliance, backup, webmin

470 Schedule

471 Schedule

Swivel uses scheduling for several of its jobs, and from version 3.5 onwards, they are in a user friendly format with a drop down menu, but may still be customised for specific requirements. This document covers the customised format.

Schedules and custom schedules may be used in the following ways:

- Data source Synchronisation such as Active Directory and LDAP
- Reporting
- Inactive user check
- PIN Expiry Check
- Audit Log Tidy

472 Prerequisites

Swivel 3.x

473 Custom Scheduling

A cron expression is a string comprised of 6 or 7 fields separated by white space. The 6 mandatory and 1 optional fields are as follows:

Custom Scheduling

Field Name:	Seconds	Minutes	Hours	Day-of-month	Month	Day-of-week	Year (Optional) empty
Allowed Values:	0-59	0-59	0-23	1-31	1-12 or JAN-DEC	1-7 or SUN-SAT	1970-2099
Allowed Special Character	, - * /	, - * /	, - * /	, - * ? / L W C	, - * /	, - * ? / L C #	, - * /

The * character is used to specify all values. For example, "*" in the minute field means "every minute".

The **?** character is allowed for the day-of-month and day-of-week fields. It is used to specify 'no specific value'. This is useful when you need to specify something in one of the two fields, but not the other. See the examples below for clarification.

The **-** character is used to specify ranges For example "10-12" in the hour field means "the hours 10, 11 and 12".

The **,** character is used to specify additional values. For example "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".

The / character is used to specify increments. For example "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". Specifying '*' before the '/' is equivalent to specifying 0 is the value to start with. Essentially, for each field in the expression, there is a set of numbers that can be turned on or off. For seconds and minutes, the numbers range from 0 to 59, for hours 0 to 23, for days of the month 0 to 31, and for months 1 to 12. The "/" character simply helps you turn on every "nth" value in the given set. Thus "7/6" in the month field only turns on month "7", it does NOT mean every 6th month, please note that subtlety.

The **L** character is allowed for the day-of-month and day-of-week fields. This character is short-hand for "last", but it has different meaning in each of the two fields. For example, the value "L" in the day-of-month field means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing results.

The **W** character is allowed for the day-of-month field. This character is used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.

The **L** and **W** characters can also be combined for the day-of-month expression to yield **LW**, which translates to "last weekday of the month".

The **#** character is allowed for the day-of-week field. This character is used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means the third Friday of the month (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month.

The **C** character is allowed for the day-of-month and day-of-week fields. This character is short-hand for "calendar". This means values are calculated against the associated calendar, if any. If no calendar is associated, then it is equivalent to having an all-inclusive calendar. A value of "5C" in the day-of-month field means "the first day included by the calendar on or after the 5th". A value of "1C" in the day-of-week field means "the first day included by the calendar on or after sunday".

The legal characters and the names of months and days of the week are not case sensitive.

Here are some full examples:

Expression Meaning

"0 0 12 * * ?" Fire at 12pm (noon) every day

"0 15 10 ? * *" Fire at 10:15am every day

"0 15 10 * * ?" Fire at 10:15am every day

"0 15 10 * * ? *" Fire at 10:15am every day

"0 15 10 * * ? 2005" Fire at 10:15am every day during the year 2005

"0 * 14 * * ?" Fire every minute starting at 2pm and ending at 2:59pm, every day

"0 0/5 14 * * ?" Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day

"0 0/5 14,18 * * ?" Fire every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day

"0 0-5 14 * * ?" Fire every minute starting at 2pm and ending at 2:05pm, every day

"0 10,44 14 ? 3 WED" Fire at 2:10pm and at 2:44pm every Wednesday in the month of March.

"0 15 10 ? * MON-FRI" Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday

"0 15 10 15 * ?" Fire at 10:15am on the 15th day of every month

"0 15 10 L * ?" Fire at 10:15am on the last day of every month

"0 15 10 ? * 6L" Fire at 10:15am on the last Friday of every month

"0 15 10 ? * 6L" Fire at 10:15am on the last Friday of every month

"0 15 10 ? * 6L 2002-2005" Fire at 10:15am on every last Friday of every month during the years 2002, 2003, 2004 and 2005

"0 15 10 ? * 6#3" Fire at 10:15am on the third Friday of every month

"0 0 11 1-31/2 * ?" Fire on odd days at 11.00

"0 0 11 2-31/2 * ?" Fire on even days at 11.00

Pay attention to the effects of **?** and ***** in the day-of-week and day-of-month fields!

474 Testing

475 Known Issues

476 Troubleshooting

477 SCText How To Guide

478 Overview

The SCText servlet allows security strings to be requested by using a text string. It is disabled by default and if required must be explicitly enabled.

479 Prerequisites

PINsafe 3.x

480 How to Guide

480.1 Enabling SCText

To enable the SCText servlet, edit web.xml on the PINsafe web application (under <Tomcat_root>\pinsafe\WEB-INF). Check if the following lines exists:

```
<servlet>
  <servlet-name>SCText</servlet-name>
  <servlet-class>com.swiveltechnologies.pinsafe.server.session.SCText</servlet-class>
</servlet>
```

Insert them if they do not, next to the other servlet definitions. The other section will almost certainly be missing:

```
<servlet-mapping>
     <servlet-name>SCText</servlet-name>
     <url-pattern>/SCText</url-pattern>
</servlet-mapping>
```

Insert this section next to the other <servlet-mapping> entries.

Save web.xml and restart Tomcat.

480.2 Making SCText requests by username

You should now be able to make requests as follows to receive text security strings:

For a Software install:

http://<pinsafe>:8080/pinsafe/SCText?username=test

For an Appliance

https://<pinsafe>:8080/pinsafe/SCText?username=test

Example output:

1234567890

4507826913

480.3 Making SCText requests by SessionID

If "Allow session start by username" is disabled, you need to execute a session start request, retrieve the session ID and use the following format:

For a Software install:

http://<pinsafe>:8080/pinsafe/SCText?sessionid=<sessionid>

For an Appliance

https://<pinsafe>:8080/pinsafe/SCText?sessionid=<sessionid>

481 Testing

482 Known Issues

483 Troubleshooting

484 Security Strings

485 Overview

A Swivel Security String is a PIN protected One Time Code. A user carries out a simple extraction of the One Time Code OTC based upon their PIN number.

486 Prerequisites

Swivel authentication server

487 One Time Code Extraction

See PINsafe User Guide

488 Testing

489 Known Issues

490 Troubleshooting

491 Seed

492 Overview

Swivel supports the use of OATH HOTP such as used with the Swivel Token, and software tokens with a valid seed can be used to authenticate Swivel users. Hardware tokens are supplied with seeds each one for a specific hardware token, and do not need a seed generated.

493 Prerequisites

Swivel 3.9.6

494 Swivel OATH Seeds

Swivel OATH seeds for Swivel hardware Tokens are sent by email in an encrypted file, with the password sent by SMS text message and can then be imported. A seperate seed does not need to be generated.

495 Generating an OATH seed

The following command generates a Hexadecimal (base 16) seed for a software token authentication, it is possible to run this on the command line of a Swivel appliance through the CMI.

```
head -10 /dev/urandom | md5sum | cut -b 1-30
```

Example:

e0b10ee3a4bb2598c0575539529f33

This seed should be assigned a serial number and can be imported into the Swivel administration console. It may be used with an appropriate software token such as Google Authenticator.

Different length seeds may be generated, for example using sha1sum (SHA1-HMAC is used for Google Authenticator):

```
head -10 /dev/urandom | sha1sum | cut -b 1-40
```

496 Importing Token Seeds

There are two types of OATH Tokens: Event Based (HOTP) and Time Based (TOTP) Tokens. Before importing, you must confirm which type of Token is being used. From the Swivel Admin Console, under OATH > OATH Policies > Token Type, set this to HOTP or TOTP - this must be set BEFORE importing the Token Seeds.

Next, under OATH > OATH Tokens, you would click the 'Import' button and select the File Format from the dropdown menu or Browse to the file that contains the Token Seeds.

For further information on the token import options see Token.

497 Testing

498 Known Issues

499 Troubleshooting

500 Self Reset

See ResetPIN How To Guide

501 Sendmail

502 Overview

Sendmail is used on Swivel appliances to send out emails. It is configured through the CMI. Sendmail is used by the following processes:

Audit scripts

Mon

VIP on PINsafe Appliances

503 Prerequisites

Swivel Hardware or Virtual Appliance

SMTP gateway

DNS entry for Swivel hostname

504 Configuring Sendmail

On the CMI select Sendmail

Select Configure

Enter the Hostname for the SMTP server

Stop then start Sendmail

505 Testing

To test Sendmail use from the command line mail <email@domain>. Enter the subject, content, then enter a '.' on a new line, it will them prompt for a CC address, press enter and the email should be sent. Example:

```
mail support@swivelsecure.com
Subject: test
test
.
Cc:
```

check the /var/log/maillog for sent email

```
tail /var/log/maillog
```

Sample output

```
Oct 24 14:40:09 single sendmail[27940]: s9ODe9om027938: to=<support@swivelsecure.com>, ctladdr=<root@gswiveltest.swivelsecure.net> (0/0), de
```

506 Known Issues

507 Troubleshooting

On Swivel hardware and Virtual appliances sendmail emails are logged under /var/log/maillog, to view the logs use;

```
 tail /var/log/maillog
```

Ensure Sendmail was restarted after configuring it.

507.1 Error Messages

Sender address rejected: Domain not found

The source source DNS is not configured correctly, i.e. the Swivbel server needs a DNS record for a reverse DNS lookup.

508 Sentry

Sentry is the new context for Swivel Secure appliances. Before it used to be Pinsafe for v2 and v3 appliances.

509 Session Cleanup

509.1 Overview

This document outlines the use of the session cleanup located on the PINsafe Administration Console under Server/Jobs. The session cleanup periodically goes through the PINsafe running processes and clears out sessions that are longer than the defined value, this is by default 2 minutes. Changing this value will impact a number of PINsafe applications that use this.

509.2 Prerequisites

PINsafe 3.x

509.3 Session Cleanup Value

Session cleanup (s): (value in seconds) Default: 120. Minimum: 1, Maximum 9999999999

509.4 Where is Session Cleanup used

The following are dependant on the value of session cleanup:

- Single Channel Graphical Images
- SMS on Demand
- ResetPIN request code

509.5 Known Issues

509.6 Troubleshooting

510 Shutdown and Power Off Procedure

510.1 Overview

This document covers the shutdown procedure for PINsafe appliances, both hardware and software.

510.2 Prerequisites

PINsafe appliance

510.3 Considerations

If the appliance is part of an Active/Active Cluster verify that the other appliances are fully functional, this can be verified by logging into each PINsafe Administration Console, also the Virtual IP address can be checked, see VIP Status

Review the PINsafe logs for any errors

510.4 Shutdown and Power off Guide

1. Login to the PINsafe Command Management Interface (See Getting Started Basic CMI configuration)

2. Select Advanced Menu

3. Select Admin Menu

4. Select Power off Appliance

5. Wait several minutes for the appliance to shutdown, to verify the hardware appliances is shutdown, check the power light, to verify a Virtual Machine check the systems status.

510.5 Known Issues

510.6 Troubleshooting

511 Site ID

When creating a Site ID the customer will be asked to provide some information on how they intend to use Swivel Secure: see SSD

Other features are directly linked to the use of AuthControl Mobile App and its available options:

· PUSH (One Touch) authentication.

· PIN indicates whether or not the user enters their PIN in the mobile app and is shown the OTC, or has to extract the OTC from the security string.

· LOCAL - security strings are generated in the mobile app using TOTP, and are not requested from the appliance.

· OATH means that the mobile app generates one-time codes using TOTP.

512 SMPP How to guide

513 Overview

Swivel supports the use of the Short Message Peer-to-Peer (SMPP) protocol for authentication. This document outlines how to configure the Swivel server for SMPP authentication.

514 Prerequisites

Swivel 3.6 or higher

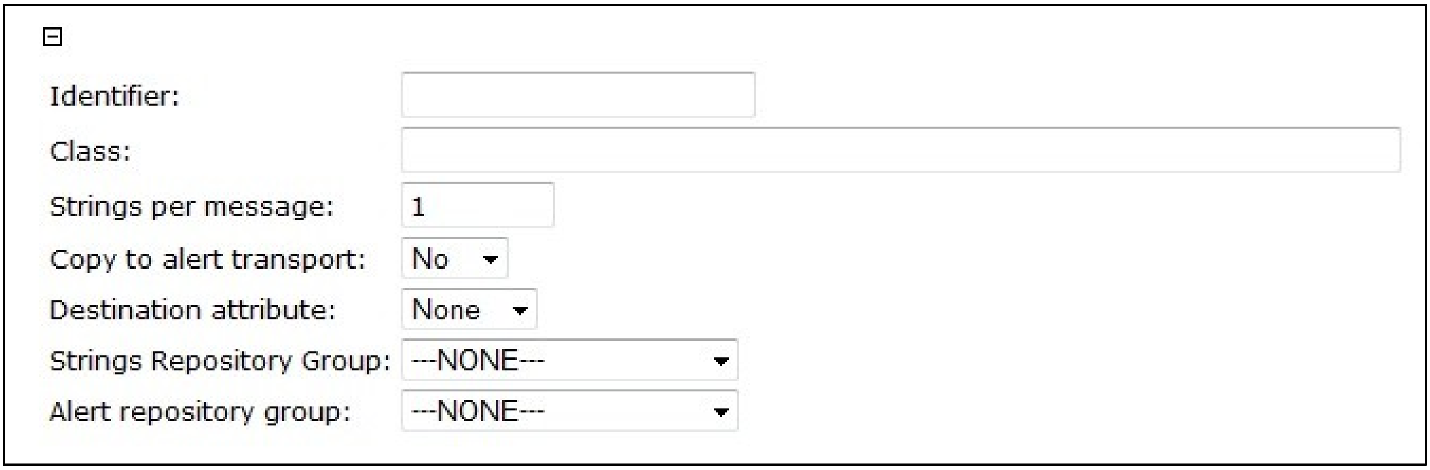
515 Baseline

Swivel 3.6 has been tested against SMPP version 3.4

516 Swivel Configuration

516.1 Transport General Configuration

On the Swivel Administration Console select Transport then General, and click on New Entry.



Identifier:

Class:

Strings per message: 1

Copy to alert transport: No

Destination attribute: None

Strings Repository Group: ---NONE---

Alert repository group: ---NONE---

Enter the required information for the Transport as below;

For the setting values see Transport Settings

Identifier: SMPP

Class: com.swiveltechnologies.pinsafe.server.transport.SMPPTransport

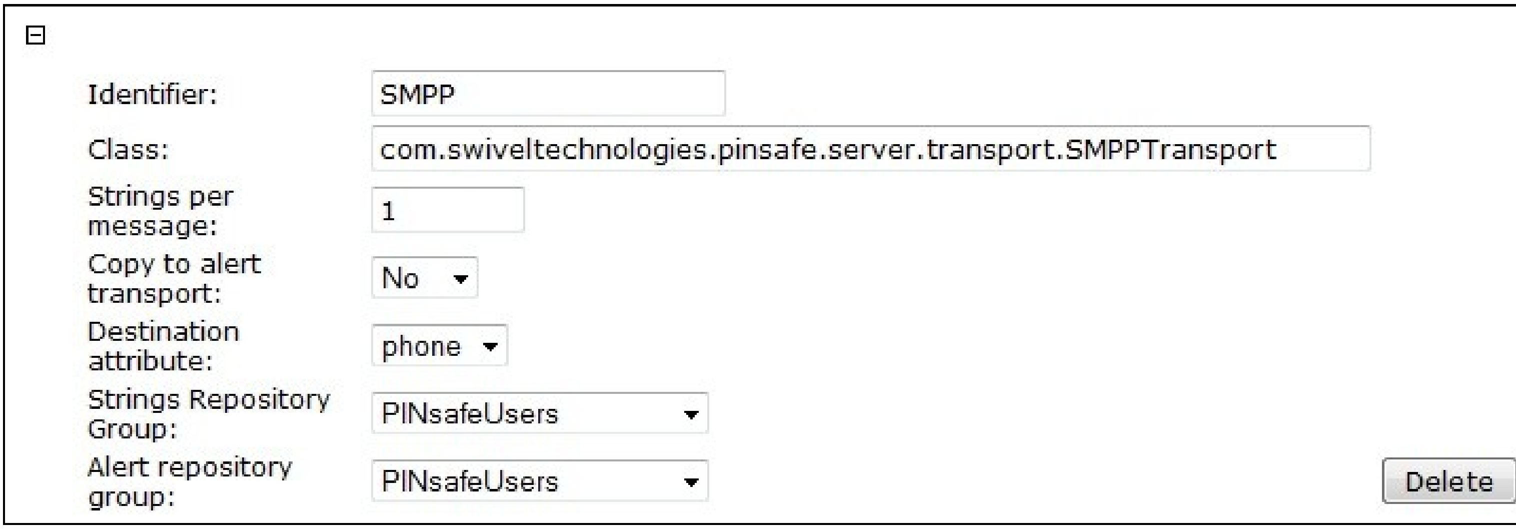
Strings per message: 1

Copy to alert transport: No

Destination attribute: phone

Strings Repository Group: PINsafeUsers (or other required group, can only have one transport entry for Strings Repository Group)

Alert repository group: PINsafeUsers (or other required group, can only have one transport entry for Alert repository group)



Identifier: SMPP

Class: com.swiveltechnologies.pinsafe.server.transport.SMPPTransport

Strings per message: 1

Copy to alert transport: No

Destination attribute: phone

Strings Repository Group: PINsafeUsers

Alert repository group: PINsafeUsers

When complete click Apply to save the settings, and a new entry should appear under Transport in the Administration console which can be edited as below.

516.2 Transport SMPP Configuration

Click on the name of the Identifier created above, located under Transport. The following will need to be configured.

Server: IP or Hostname of the SMPP server

Port: Port used by the SMPP server, default 2775

System Type: SMPP type, default pcsms

Username: SMPP server username (you are not allowed an e-mail address in the Username field)

Password: SMPP server password

Source Address:

Source TON: default 5 (see below)

Source NPI: default 0 (see below)

Destination TON: default 1 (see below)

Destination NPI default 0 (see below)

Keep Alive: default No, Options Yes/No

Keep Alive Time: default 30000

516.2.1 TON settings

Unknown = 0

International = 1

National = 2

Network Specific = 3

Subscriber Number = 4

Alphanumeric = 5

Abbreviated = 6

516.2.2 NPI settings

Unknown = 0

ISDN/telephone numbering plan (E163/E164) = 1

Data numbering plan (X.121) = 3

Telex numbering plan (F.69) = 4

Land Mobile (E.212) =6

National numbering plan = 8

Private numbering plan = 9

ERMES numbering plan (ETSI DE/PS 3 01-3) = 10

Internet (IP) = 13

WAP Client Id (to be defined by WAP Forum) = 18

517 Testing

518 Known Issues

519 Troubleshooting

519.1 Error Messages

Exception while processing message: ie.omk.smpp.message.InvalidParameterValueException: Bad service type

The SMPP SYSTEM TYPE is invalid, try with the default pcsms

520 SMS

521 Overview

Swivel can use Short Messaging Service (SMS) Text message to send users a One Time Code (OTC) for authentication, using the mobile phone as a device for two factor authentication. Swivel supports the following:

- SMS sent in Advance
- SMS sent on Demand

As an alternative to SMS text messaging see Mobile Phone Client. For alternative authentication see Authentication Methods.

521.1 SMS sent in Advance

When the user account is created the user is sent their first One Time Code. This helps to overcome network delivery issues as the user has an OTC on their mobile phone ready for authentication. If a user passes or fails an authentication, then they are sent their next OTC. If the message is deleted, the user can request a new text message.

This method also allows multiple OTC's to be sent in a single text message, see Mobile Security String Index

521.2 SMS sent on Demand or Request

When the user is making an authentication the user requests an SMS text message to be sent to them. The user then has a limited time to login using the OTC within the Text Message. This is On Demand Authentication and the length of time that the SMS is valid for is configurable, with a default of two minutes. The text message is usually requested by the following methods:

- Button on the login page
- Challenge and response, where user enters a username and Password
- Taskbar utility

521.2.1 Flash SMS

Some SMS gateways support the use of Flash SMS, which appears on the screen immediately upon arrival and unless it is saved, it is deleted. Flash SMS is usually used for On Demand authentication.

522 Integrating with SMS

522.1 Integrating the login

Integration of login portals is usually straight forward with SMS, although if TURing and Pinpad images are used, then these should not be automatically generated as a login will be expected using those methods. When using Challenge and response with RADIUS, then no changes to the login page may be required.

522.2 Sending SMS messages

SMS messages are usually sent through an SMS Gateway, although it is possible to use a GSM Modem.

523 SMS Security

SMS may be vulnerable to the below attacks. To overcome these PINsafe Protocol may be used to protect the OTC, see PINsafe User Guide.

- SMS Forwarding, particularly on Smart Phones
- Physical theft of the phone
- SIM cloning
- SMS eavesdropping
- Shoulder surfing

524 SMS Gateway Integration

525 Overview

When an SMS message is to be sent, Swivel can connect to an SMS gateway to send the SMS text messages. It may be possible to use an existing protocol for integration, or one may need to be modified.

526 Prerequisites

Swivel 3.x

SMS Gateway

527 Supported Transports

For a list of currently supported SMS and other transports see Transport Configuration. Some of these offer SMS for testing purposes.

528 SMS Integration

The following protocols are supported by Swivel. Other protocols could be integrated, but may be chargeable.

528.1 SMPP

SMPP can be used, see SMPP How to guide

528.2 SMTP to SMS

SMTP to SMS can be used, see SMTP to SMS

528.3 HTTP/HTTPS

HTTP/HTTPS integration, this will usually require a new transport class for that provider and may be chargeable. The following information is useful in testing this:

- API for gateway integration
- Account details for testing, including, gateway address, Username, Password, port

529 Testing

530 Known Issues

531 Troubleshooting

Error seen with PSWin Transpoort:

```
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target
```

The resolution is outlined below:

http://erikzaadi.com/2011/09/09/connecting-jenkins-to-self-signed-certificated-servers/

532 SMTP Credential Change How to Guide

532.1 Overview

PINsafe can connect to an SMTP gateway to send email messages for user alerts, security strings, and system messages. This document outlines how and where to change the SMTP Username and Password Credentials on the PINsafe Administration Console. For information on configuring Alert and security strings see Transport Configuration

532.2 Prerequisites

PINsafe 3.x

532.3 Changing SMTP Credentials

532.3.1 SMTP Server details

On the PINsafe Administration Console select Server/SMTP. The IP/Hostname, and if required authentication enabled or disabled and the Username and Password an be changed.

Repeat the SMTP credentials change on each PINsafe instance/appliance.

532.4 Testing

To test the SMTP credentials, force the system to send an email, such as resending a PIN on a test account that uses SMTP as its transport class. Observe the PINsafe logs for any errors.

532.5 Known Issues

532.6 Troubleshooting

533 Software Only Installation

534 Overview

Software Only installas are managed by Swivel customers and partners, for further information see Software Install advantages and disadvantages.

This document outlines the setup of a Swivel Software only installation and the settings required that differ from a Swivel Hardware Appliance or Virtual Appliance

535 Prerequisites

Swivel software Versions FAQ (installed on Tomcat and Java)

OS

536 Ports

536.1 Swivel Management

Swivel is managed by default on port 8080 by specifying the following URL:

http://IP_address:8080/pinsafe

If a valid SSL certificate is installed then this will be an https connection:

https://IP_address:8080/pinsafe

If this port is also shared for access for other services, then it should be protected using an IP address filter and sufficiently strong authentication, see Filter IP How to Guide. Swivel recommend the use of a Hardware Appliance or Virtual Appliance with its proxy port so that the management port does not need to be made available for other services.

536.2 Swivel Single Channel Images

Only a software only install the swivel TURing and Pinpad images are served up using port 8080, (this differs from Swivel hardware and virtual appliances that use port 8443/proxy).

http://IP_address:8080/pinsafe

If a valid SSL certificate is installed then this will be an https connection:

https://IP_address:8080/pinsafe

537 Testing

537.1 Testing Single Channel

To test a single channel image, the following URL can be used:

http://IP_address:8080/pinsafe/SCImage?username=test

If a valid SSL certificate is installed then this will be an https connection:

https://IP_address:8080/pinsafe/SCImage?username=test

537.2 Testing Dual Channel

To test a dual channel image, the following URL can be used:

http://IP_address:8080/pinsafe/DCIndexImage?username=test

If a valid SSL certificate is installed then this will be an https connection:

https://IP_address:8080/pinsafe/DCIndexImage?username=test

538 Known Issues

539 Troubleshooting

540 SSD

541 Overview

Swivel Mobile Clients allow security strings to be provided for remote authentication. The Swivel server details can be automatically configured through the use of a **Site ID or Server ID** which will then pull the settings for their Swivel server from the Swivel Server Details (SSD) allowing them to enter their username and a Mobile Provision Code. This service is provided to all Swivel customers with a valid maintenance agreement.

542 Prerequisites

Swivel Mobile Phone Client with Server ID option.

Swivel > 3.9.6

In order for the Security Strings or OTC to be downloaded from the Swivel server then the Swivel server needs to be accessible usually through a Network Address Translation or Proxy.

543 SSD server settings

543.1 Requesting a Site ID

To configure the SSD server the following information must be provided to Swivel Secure Support (supportdesk@swivelsecure.com):

Attribute	Example Settings
Instance Name	Your Company Name
Hostname	Public IP/Hostname
SSL	Yes
Port	443
Context	proxy
Push	Yes

Instance Name A descriptive name, example *Acme Company*

Hostname The Webservice URL, being Swivel Server hostname as accessible by mobile clients, example swivel.acme.com

SSL If SSL is enabled or not. A typical test install may have a self signed certificate, so may need to set the Swivel server to use a non SSL connection with HTTP over port 443 or 8443.

Port The web service port used by the client to connect to the Swivel server. For a Swivel virtual or hardware appliance this is usually 8443, for a software install it is usually 8080. Port address translation may allow different ports to be used. For Port Address Translation on Swivel hardware or virtual appliances see PAT

Context The installation name of the Swivel application, the web service context. For a Swivel virtual or hardware appliance this is usually proxy, for a software install it is usually pinsafe.

Push This is used by mobile clients to use the OneTouch Mobile, if it isnot specified then it will default to No.

You will then receive a Site ID which can be sent to users to automatically enter these fields on their Mobile Phone Client.

543.2 Configuring the Swivel Server

After submitting the SSD settings to Swivel, enter the returned Site ID under Server/Name

543.3 Sending the Site ID to users

Swivel version 3.9.6 onwards allows the Site ID to be sent to the users as part of an automated provisioning service, and can be sent as a number or as a link, see Provision URL.

The Site ID can be sent to the user upon account creation or as part of their Provision process.

543.3.1 Transport Message settings

Each transport has the following fields from Swivel version 3.9.7 onwards for Provisioning and may be edited as required:

Site Id subject: The Site Id subject

Site Id body: The Site Id message body

The default message is:

```
Server Id: %SITE_ID
```

```
To get the server settings automatically click the following URL: %URL_SETTINGS%SITE_ID
```

Where %SITE_ID is the site ID information and %URL_SETTINGS the Site ID URL for the Provision URL.

For older versions prior to 3.9.7, it can be entered manually.

The **Credentials alert message:** or **Mobile Provision Message:** can be configured to add the Site ID. Also the URL for the Mobile Provision Code could be added, see Mobile Re-Provision How to Guide

Use %SITE_ID to specify the Site ID entered into the Swivel server.

```
Your new PINsafe credentials are:%CR%LFUsername: %NAME%CR%LFPassword: %PASSWORD%CR%LFPIN: %PIN %CR%LFSite ID %SITE_ID
```

```
Site ID 1234567890 %CR%LF Mobile provision code: %CODE
```

For version 3.9.5 the Site ID must be entered manually

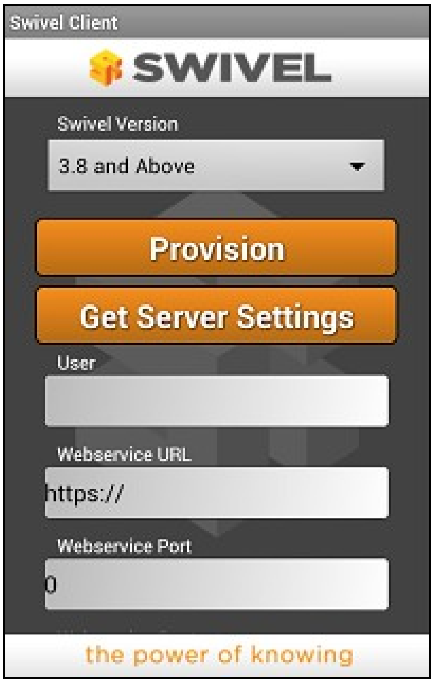
```
Your new PINsafe credentials are:%CR%LFUsername: %NAME%CR%LFPassword: %PASSWORD%CR%LFPIN: %PIN %CR%LFSite ID 1234567890
```

```
Site ID 1234567890 %CR%LF Mobile provision code: %CODE
```

544 Mobile Phone Clients

544.1 SSD Client Server ID

On the Mobile Phone client select **Settings**, ensure the Swivel version is *3.8 and above*, then select **Get Server Settings** and enter the **Server ID**, then click on Done.

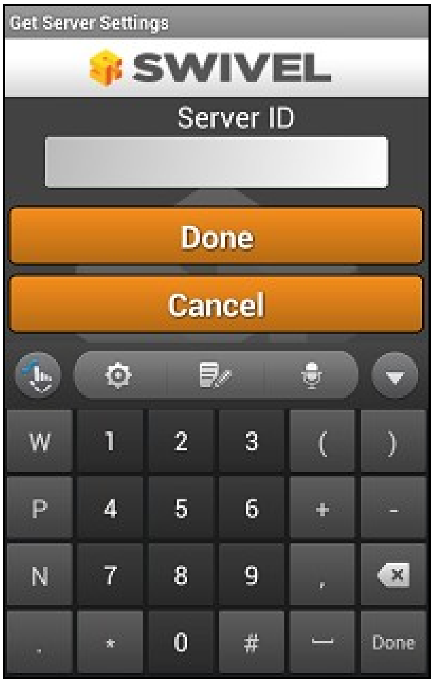


Swivel Version: 3.8 and Above

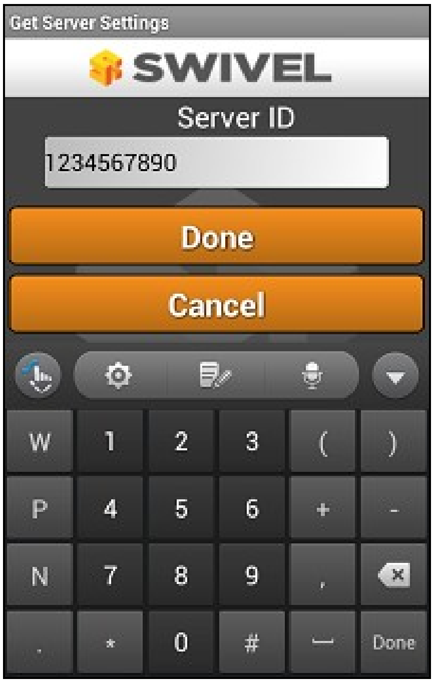
User

Webservice URL: https://

Webservice Port: 0



Server ID:



Server ID: 1234567890

545 Testing

Enter Server ID information into mobile phone client, and ensure server details are correct.

546 Known Issues

547 Troubleshooting

Is the provision request reaching the Swivel server, check the Swivel logs.

Is a SSL connection being specified for a non SSL sever, this can be verified using tcpdump and monitoring the connection:

```
tcpdump -i eth0 port 443
```

```
tcpdump -i eth0 port 8443
```

548 SSL Disabling On Appliance

548.1 Overview

This article explains how to disable SSL on a PINsafe appliance, so that pages can be accessed using http, rather than https.

NOTE: carrying this out is a security risk. Allowing users to access PINsafe without SSL encryption is inherently insecure. In particular, it is not recommended to allow http access to a production environment over the internet. This solution is only advised for pre-production testing, or if the PINsafe appliance is only accessible on the internal network. If you are implementing this change simply to avoid problems with certificate errors, the correct solution is to get a commercial SSL certificate for production use.

548.2 Prerequisites

These instructions assume you have a PINsafe appliance with Webmin. Otherwise, the instructions apply to all versions of PINsafe.

548.3 How to Guide

NOTE: this process involves restarting Tomcat, so PINsafe services will be unavailable for a short time.

Open webmin in a web browser (https://<pinsafe_server>:10000). Replace <pinsafe_server> with the name or IP address of your PINsafe server. You will need to log in, so make sure you know the administrator password for your PINsafe appliance.

Select **Servers** from the top menu, then **PINsafe**.

Select **Edit Tomcat Config File**.

Assuming you want to disable SSL only for the applications on port 8443 (proxy, changepin, reset), locate the line that starts as follows:

```
<Connector address="0.0.0.0" port="8443" scheme="https"
```

Delete everything from **scheme** up until the end marker: **/>**. The line should now look like this:

```
<Connector address="0.0.0.0" port="8443" />
```

If you also want to disable SSL for the pinsafe application (not recommended), then locate the line starting

```
<Connector address="0.0.0.0" port="8080" scheme="https"
```

and carry out the same procedure.

Click the Save button to return to the menu.

Finally, restart Tomcat to implement the changes. Most versions of PINsafe have the option to restart Tomcat on the webmin page you just returned to. However, this is not available on all versions, in which case you will have to restart Tomcat from the CMI menu on the appliance console.

548.4 Known Issues

Note that if you enable http in order to display a TURing image without certificate errors, and the image is embedded into a page that is using https, you may get warnings about mixing secure and non-secure elements on a web page. Read the warning carefully before choosing which button to click, as the response for Internet Explorer (IE) in particular has changed. In older versions of IE (6 or earlier), you selected "Yes" to allow mixed content. In newer versions, you select "No" to allow mixed content: "Yes" means show only secure content.

549 SSL Internal Certificate Authority

550 Overview

This document covers using an Internal Certificate Authority (CA) in Swivel deployments. See also SSL Certificate PINsafe Appliance How to Guide and SSL Solutions.

551 Prerequisites

Swivel 3.x

552 Using an Internal CA

Q). Can use certificates issued by our internal CA

A). In order for the certificates to be recognized without certificate problems arising, the CA certificate must be installed in the trusted root certificates store of any client machine.

- The host name by which the server is referenced must match the host name in the certificate, or an alternate name stored in the certificate.
- The certificate must be within its validity period.
- The certificate must be trusted by the client machine, either directly, or more commonly, by trusting the root CA certificate.

Where the request is proxied such as OWA, ADFS Proxy then this server is the client and needs to have the CA certificate which must be installed in the trusted root certificates store on that server, but users connecting in do not need to.

Where the request is made directly to the Swivel server or through a NAT then the user's PC is the client, and would need to have the certificate installed. In such situations a valid public certificate assigned to the public hostname of the Swivel server NAT is usually more appropriate.

Some browsers and access devices permit certificate errors to be ignored, but creating such a scenario may not be the most secure option.

553 Testing

554 Known Issues

555 Troubleshooting

556 Static Routes How to Guide

557 Overview

The Swivel appliance CMI allows one static route to be added, however subsequent static routes may need to be added manually. This is why you only see the Display Route option available on the appliance CMI if you already have a route configured.

558 View the routing table

From the CMI, select Advanced Menu > Admin > Networking > IPs & Routing > Diagnostics > Routing table

559 Add a Static Route

Swivel appliance 2.0.14

From the CMI, select Advanced Menu > Networking > IPs & Routing > Change Appliance Routing > Add a route

The following information is required:

- Address : The destination address
- Netmask : The network subnet mask for the address e.g. 255.255.255.0
- Gateway : The gateway address to be used

Press return when complete

To view a current route select Display route.

560 Multiple static routes

This option should only be used when multiple static route are required. Connect to the Swivel appliance using WinSCP How To Guide.

Then navigate to the following file on the appliance using WinSCP:

/etc/sysconfig/network-scripts/route-eth0

Edit this file by right clicking on it and selecting Edit.

You should see the route that you've already defined exists under the ADDRESS0, NETMASK0, GATEWAY0 entries. Add another set of values underneath as provided in the example below using ADDRESS1, NETMASK1, GATEWAY1 entries:

```
ADDRESS0=10.10.10.0

NETMASK0=255.255.255.0

GATEWAY0=192.168.0.1

ADDRESS1=172.16.1.0

NETMASK1=255.255.255.0

GATEWAY1=192.168.0.1
```

Save the file and restart networking through the command line or CMI

```
service network restart
```

561 Static Routes on different interfaces

create a routing file for the required network e.g. route-eth1, route-eth2

```
cd /etc/sysconfig/network-scripts
```

```
touch route-eth1
```

Edit the file with vi or WinSCP with the required parameters, for example:

ADDRESS0=192.168.0.0

NETMASK0=255.255.255.0

GATEWAY0=192.168.0.1

Save the file and restart networking through the command line or CMI

```
service network restart
```

562 Create a static route on a separate interface

create a routing file for the required network e.g. route-eth1 or route-eth2

```
cd /etc/sysconfig/network-scripts
```

```
touch route-eth1
```

Edit the file with vi or WinSCP with the required parameters, for example:

ADDRESS0=0.0.0.0

NETMASK0=0.0.0.0

GATEWAY0=192.168.0.1

Save the file and restart networking through the command line or CMI

```
service network restart
```

563 Verifying routes

the following commands are of use in verifying routes

```
route
```

```
netstat -r
```

to test if a route can be reached using traceroute

```
traceroute 192.168.0.1
```

564 Known Issues

If the delete route option is run from within the CMI menu, all routes are deleted.

565 Troubleshooting

View the /var/log/messages file as this may include network issues such as invalid format for the route or of the network is unreachable.

566 Support Ticket How To Guide

566.1 Overview

Below we outline the methods of raising a support ticket and the information required.

When a support ticket is raised, you will receive an automated response. If no response is received, please check the size of any attachments you have sent.

Note: The helpdesk is not monitored 24 hours a day. Customers who have paid for 24x7 Support must use their emergency out of hours contact details.

566.2 Check the Knowledgebase first

Lots of articles are available which contain solutions to common issues: http://kb.swivelsecure.com

566.3 Gathering information

Supply as much relevant information as possible as it will save us coming back to ask further questions.

As a minimum we ask that you supply the following::

- Customer Name (so we can look at previous support history and check their support entitlement)
- Swivel version
- Hardware Platform/Appliance/VMware
- Operating System
- Patch/Service Pack
- Severity: System down high priority?, low priority?
- Detailed Description (Key points: Does the issue affect all users; Is it repeatable?)
- Include any relevant logs or use the appliance log reporting feature, see App support logs
- What has changed recently?
- New installation or established system?
- What is Swivel integrated with? (Access devices)

566.4 Contacting Support

Support is available in UK office hours 09:00-17:00 Monday to Friday.

The best method is to include the above information in the support submission form or by email, where a Support Ticket number will be issued for tracking the problem. You are welcome to ask questions about Swivel through support:

Submit a support ticket through our online form

Alternatively, email us via supportdesk@swivelsecure.com

Please ensure that you've raised a support ticket by the above methods before attempting to contact us via telephone.

566.5 24 Hour Support

This is available only to those those who have purchased the 24 hour support option from Swivel Secure. An engineer will attempt to resolve high priority issues impacting authentication of users. Those who are receiving 24 hour support will have received the emergency contact details as part of the purchase of the 24x7 Support.

566.6 Resolving The Problem

566.6.1 Reply to Support Query

An engineer will reply to the support ticket to hopefully resolve the issue as quickly as possible, or request further information.

566.6.2 Remote Access

An engineer may request remote access to the relevant system to troubleshoot the problem. Swivel have their own remote access tools through desktop and application sharing in a web session. If this is not possible we can attempt to access through your remote access solutions.

566.7 Support Ticket Issues

No email confirmation

If the file attachments are too large, then they may be rejected by the mail gateway. If pictures are used then reduce the image size, or send an initial request and reply to the ticket with the required files across several emails.

567 Swivel Deployment

568 Swivel Deployment Overview

This document details the considerations to be made in the positioning of Swivel in a network.

569 Prerequisites

Swivel 3.x

570 Workflow

Initially a user is provisioned from a data source and may be automatically provisioned with a PIN and possibly a One Time Code, commonly the data source is Active Directory, and this provision process is fully automated. The user can be provisioned with a variety of authentication methods.

A user may connect in a variety of methods such as with their web browser or client software. The user then will be required to enter their username, password (if required), and One Time Code. Swivel supports an OTC that is pre-sent to the user, or on Demand and sent to the user when requested, or an OTC generated at the point of authentication such as with a hardware Token.

The Username, and password where required, and OTC are checked and authentication allowed or denied. If the authentication is in advance, the user is sent their next OTC. Depending on the integration Swivel may check the Username/OTC and Password, or the setup may be with primary/secondary authentication servers in a chained authentication.

Some variations exist on this such as where authentication uses Swivel as an Identity Provider (IDP) and is redirected to the Swivel IDP such as with Google or Two Stage authentication where the user is asked for a password and if correct the user can then enter their OTC.

Swivel supports the following Authentication Methods

571 Deployment Scenarios

Swivel needs to communicate with various services such as DNS servers and data sources such as Active Directory or LDAP, or have Single Channel Images requested by clients for authentication, and these may make an influence on where to deploy Swivel. For a list of ports and services required for a deployment see Swivel Install Information Notes for Engineers

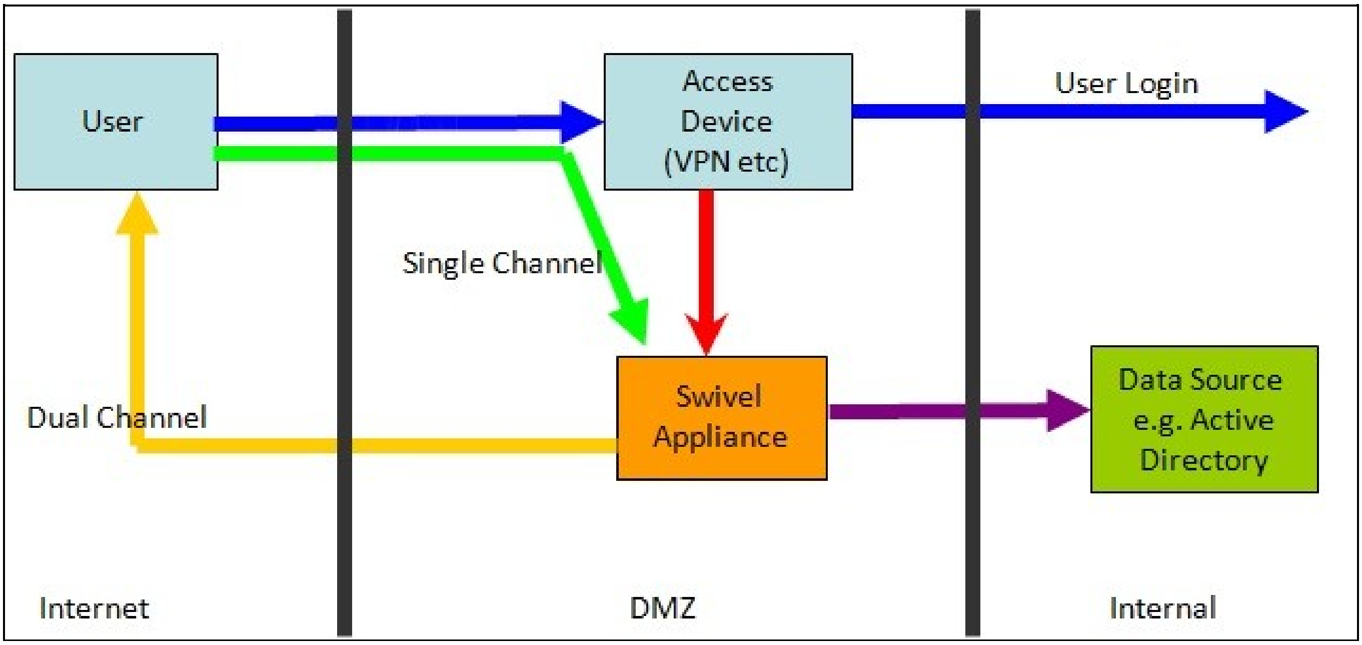
571.1 DMZ

Integrations may require clients external to an organisation, to make a request from the Swivel server or appliance, for security reasons Swivel is therefore usually deployed in the DMZ. Swivel appliances employ additional security by only allowing external connections to a proxy port. Reasons for making an external connection to the Swivel server include:

- TURing
- Pinpad
- Request a new SMS
- Security String Index
- Dual Channel Confirmed Message
- Taskbar
- ResetPIN
- Mobile Phone Clients

An exception to this is where the integration includes a device that proxies the request to the Swivel server so that there is no direct connection, this includes integrations such as OWA, ISA, TMG, Citrix Web Interface.

For security, by default Swivel appliances provide desperation between management on port 8080 and external requests using port 8443, although this can also be configured to accept requests on port 443 (see Using Port Address Translation (PAT) on the Swivel hardware or virtual appliance).



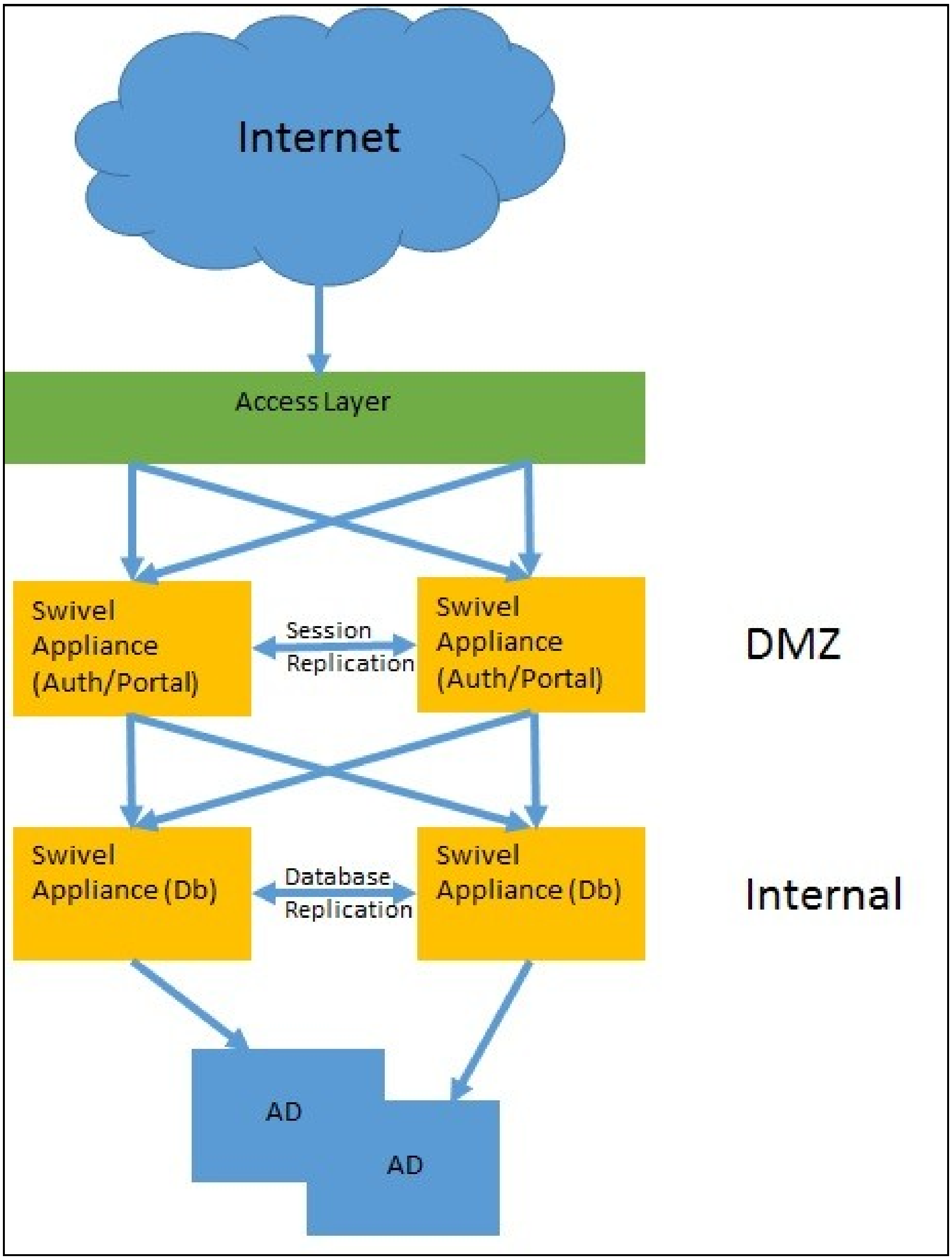
571.2 Internal

The general security principle for networks is that there should never be a connection from an external (untrusted) network to an internal (trusted) network. Where the Swivel server is used only for SMS authentication possibly using a GSM Modem or more commonly an SMS Gateway, using a hardware Token, or the clients are all located internally, it may be acceptable to place Swivel in the internal network.

Also where RADIUS responses are used for authentication such as using Challenge and Response new SMS requests can be made without the client making a direct request to Swivel.

571.3 Authentication and Database separation

For requirements where no data is to be stored within the DMZ, it is possible to separate the Authentication from the database using two Swivel A/A pairs, one pair for authentications and the second pair to hold the user data. The DMZ has Swivel Virtual or hardware Appliances as Authentication servers connecting to Swivel virtual or hardware Appliances acting as Database servers, or to use a database external to the Swivel appliance.



- VIP on Authentication servers provides resilience for single channel and Agent-XML authentication as well as security strings for mobile apps and User Portal functions such as ChangePIN Reset PIN
- RADIUS authentication is made using the real IP addresses of the DMZ Swivel virtual or hardware appliances
- Session replication provides resilience for sessions made on each authentication server
- VIP on Swivel database servers provides database resilience
- Swivel virtual or hardware appliances handle Database replication for resilience of data
- Swivel virtual or hardware appliances as Database servers import data into Swivel database from external data sources
- Two servers to import data from data source such as AD for resilience

Each Swivel server is configured with the same repositories, groups and transports. The Authentication servers define the Database servers as their database and not their local database.

572 Swivel OATH HOTP Hardware Token

573 Overview

Swivel provide tokens for authentication, below are the details of the Swivel OATH compliant HOTP token, see also Swivel OATH TOTP Hardware Token. Each time the button is pressed a number is displayed for use as a One Time Code in authenticating a user. For provisioning tokens see Token. A Swivel hardware token consists of the following:

- Serial Number to identify the hardware token
- Seed associated with the serial number, the seed is used to generate the OTC. The seed is sent separately from the token
- One Time Code, generated on the hardware token when the button is pressed.

574 Technical Specification

Swivel Hardware Token Specification

Platform	Specification
User Interface	Up to 8-characters high contrast LCD display, Built-in button, OTP displayed for 10 seconds S 3 and later. Approx. size: 0.5Mb
Security Algorithms	OATH compliant event-based HOTP
Memory Type	Random Access Memory (RAM)
Endurance	More than 14,000 clicks
Battery Lifecycle	4 years
Power Consumption	Less than 0.005mW
Operating Temperature	(-4°F ~ 158°F) (-15.6 degC ~ 70 degC)
Humidity	0% ~ 100% without condensation
Security	Tamper evident, IP54 ingress
Warranty	4 Years

575 Customization

Please contact Swivel for a quote if customization or other features/functionality is required.

576 Determining between a Swivel HOTP and a TOTP token

The Swivel OATH HOTP Hardware Token is similar to the Swivel OATH TOTP Hardware Token but there are some differences to tell them apart:

- When the button is pressed the HOTP token displays an OTC for about 12 seconds, the TOTP token 60 seconds.
- The HOTP token OTC can be used consecutively regardless of time, the TOTP token OTC has to be used within a very short time period.
- The Administrator can check the Serial Number against the list of purchased tokens.

577 Testing

578 Known Issues

579 Troubleshooting

If the Token seed will not import see Token

If the token will not sync ensure that HOTP has been selected at time of import. If it has been imported incorrectly, remove the token and reimport.

For further issues and token returns contact support@swivelsecure.com

580 Swivel OATH TOTP Hardware Token

581 Overview

Swivel provide tokens for authentication, below are the details of the Swivel OATH compliant TOTP token, see also Swivel OATH HOTP Hardware Token. Each time the button is pressed a number is displayed for use as a One Time Code in authenticating a user. For provisioning tokens see Token. A Swivel hardware token consists of the following:

- Serial Number to identify the hardware token
- Seed associated with the serial number, the seed is used to generate the OTC. The seed is sent separately from the token
- One Time Code, generated on the hardware token when the button is pressed.

582 Technical Specification

Swivel Hardware Token Specification

Platform	Specification
User Interface	Up to 8-characters high contrast LCD display, Built-in button, OTP displayed for 60 seconds Approx. size: 0.5Mb
Security Algorithms	OATH compliant event-based TOTP
Memory Type	Random Access Memory (RAM)
Endurance	More than 14,000 clicks
Battery Lifecycle	4 years
Power Consumption	Less than 0.005mW
Operating Temperature	(-4°F ~ 158°F) (-15.6 degC ~ 70 degC)
Humidity	0% ~ 100% without condensation
Security	Tamper evident, IP54 ingress
Warranty	4 Years

583 Customization

Please contact Swivel for a quote if customization or other features/functionality is required.

584 Determining between a Swivel HOTP and a TOTP token

The Swivel OATH TOTP Hardware Token is similar to the Swivel OATH HOTP Hardware Token but there are some differences to tell them apart:

- When the button is pressed the HOTP token displays an OTC for about 12 seconds, the TOTP token 60 seconds.
- The HOTP token OTC can be used consecutively regardless of time, the TOTP token OTC has to be used within a very short time period.
- The Administrator can check the Serial Number against the list of purchased tokens.

585 Testing

586 Known Issues

587 Troubleshooting

If the Token seed will not import see Token

If the token will not sync ensure that TOTP has been selected during import. If it has been imported incorrectly, remove the token and reimport.

For further issues and token returns contact support@swivelsecure.com

588 Swivel Remote Sync Client

589 Overview

The Swivel Secure AD Agent (AD Agent) allows data from a data source (e.g. Active Directory) to be pushed to a Swivel Server. The AD Agent can be used with a Swivel Secure instance deployed within the Cloud. Users are added to the appropriate repository and appear in the User Administration on AuthControl Sentry. The AD Agent runs under Tomcat and requires JAVA. The Windows installer contains all the required software elements and configures the software to run.

590 Prerequisites

AD Agent Installer.exe file from the Downloads page

Windows OS with Java or Swivel appliance

591 Swivel Configuration

591.1 Configuring the Server Agent

On the AuthControl Sentry Administration console configure the Server Agent, see Agents How to Guide. The following settings need to be configured:

Name

Hostname/IP of the AD Agent

Shared Secret: same value entered on AD Agent server

Can Act as Repository: Yes

URL Check Repository: https://IP_of_the_SRSC_server:8080/adagent/adminxml

Encryption/Deccryption key: same value entered on AD Agent server

591.1.1 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.

592 AD Agent Installation

592.1 Windows Installation

Download the AD Agent installer to where the AD Agent is to be run from, and run the installer.

592.2 AD Agent Settings

Run the AD Agent configuration program, and enter in the Cloud details supplied by Swivel.

592.3 AD Agent Administration security

The AD Agent Administration console can be protected by IP source. Edit the file .swivel/srsc/security.properties. After editing, Tomcat will need to be restarted, or on Windows quit and restart the console.

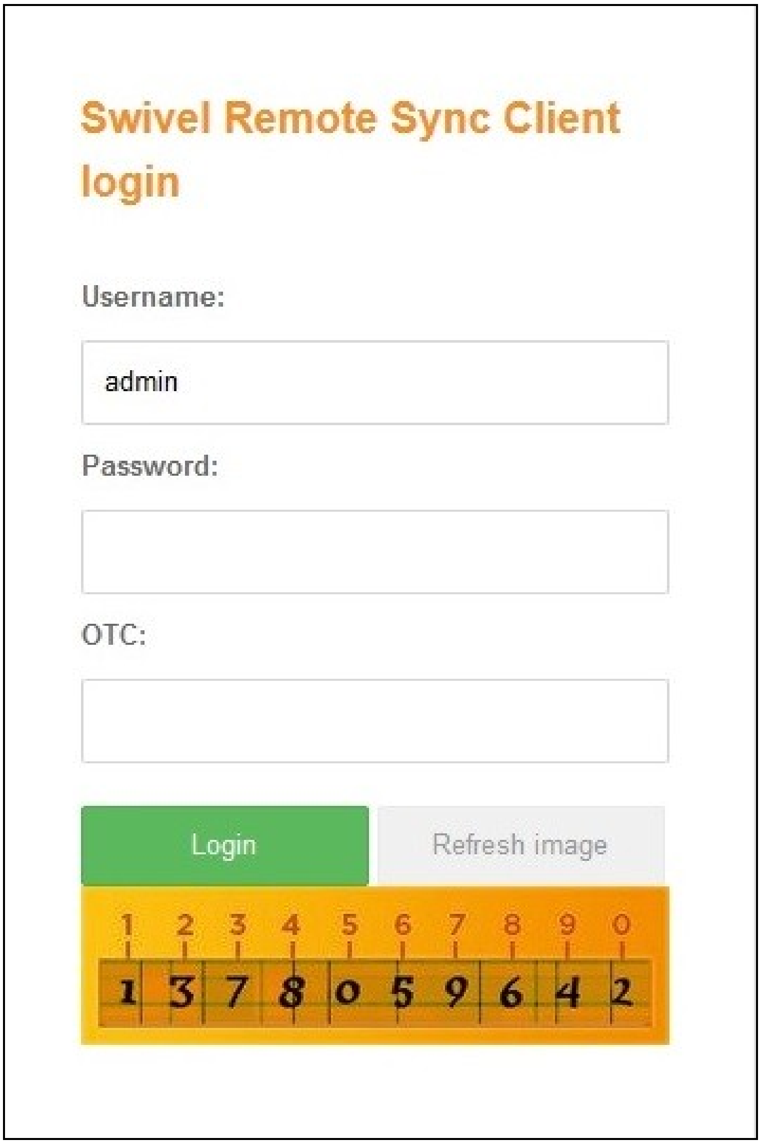
To allow access from any IP use 0.0.0.0/0

To specify a range of IP's or a specific IP specify the IP and netmask

```
admin.iprange=192.168.11.0/24
core.iprange=192.168.11.115
```

592.4 AD Agent Login

In a web browser connect to http://local_server_ip:8080/adagent, a login screen should appear, allowing login from a Swivel Administrative user account.



Swivel Remote Sync Client login

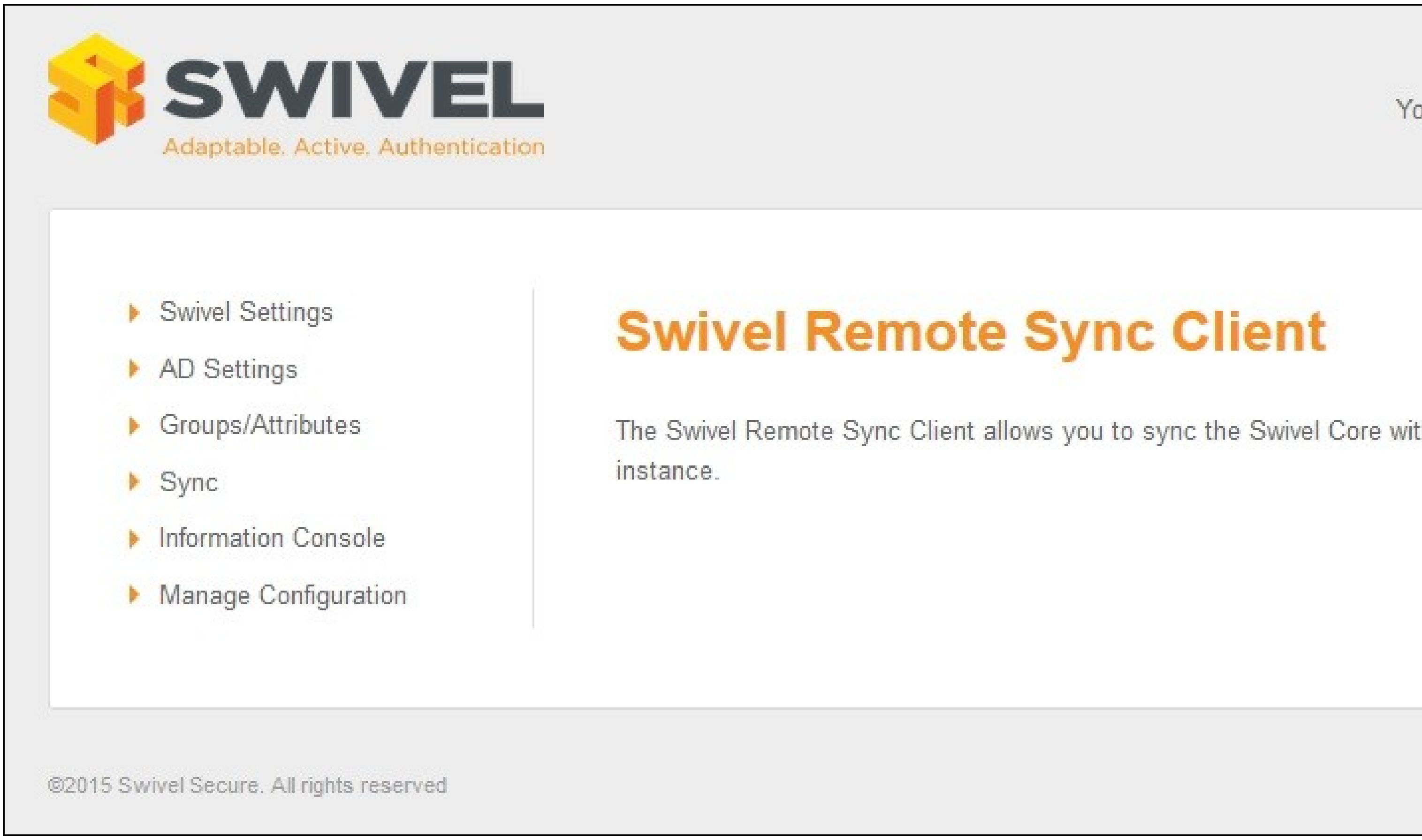
Username: admin

Password:

OTC:

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

A Successful login brings up the configuration options:



Swivel Remote Sync Client

The Swivel Remote Sync Client allows you to sync the Swivel Core wit instance.

©2015 Swivel Secure. All rights reserved

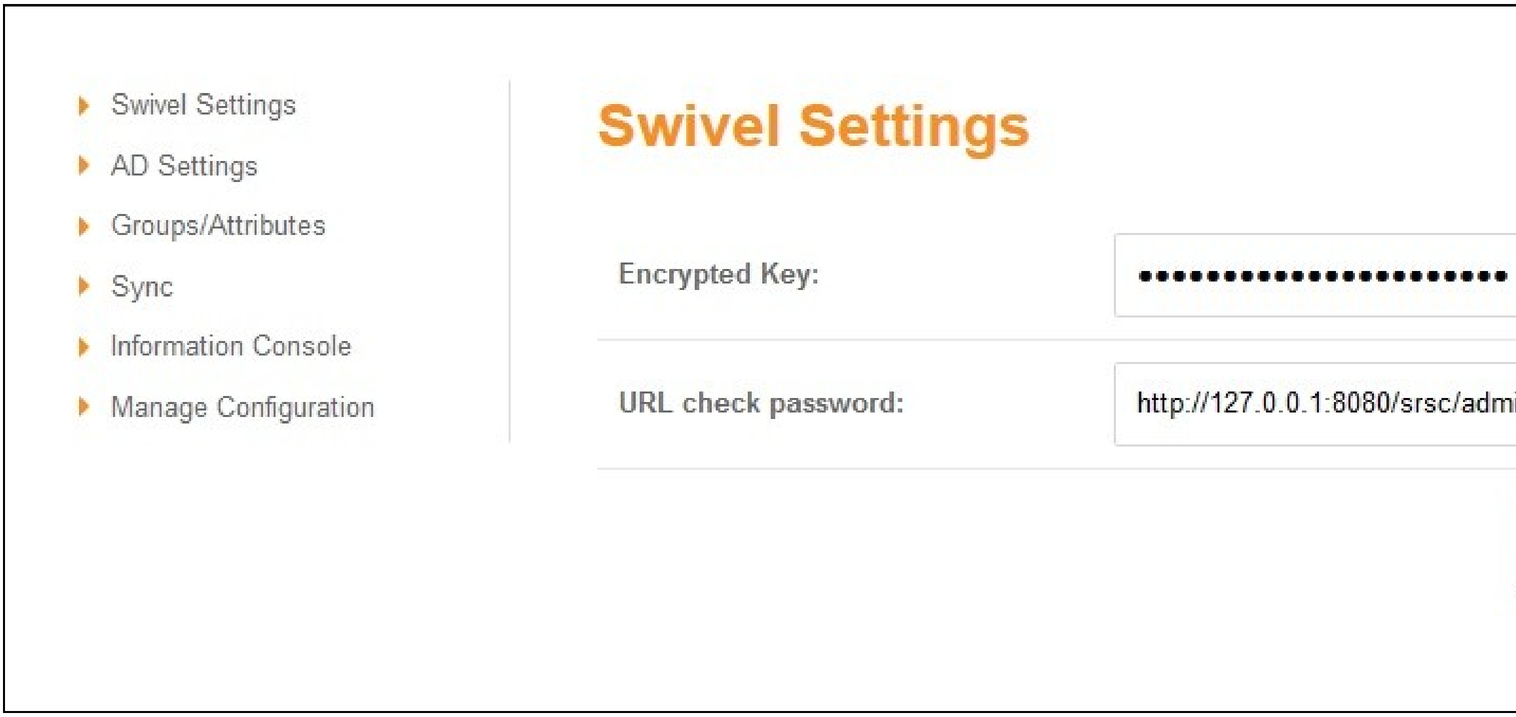
592.4.1 AD Agent Configuration - Swivel Settings

Encrypted Key: Indicates if the messages sent/received will be encrypted/decrypted. The value has to be the same as the encrypted key configured in the Agent. If empty the messages won?t be encrypted/decrypted.

URL check password: indicates the URL where the SRSC is listening for requests to check password

Note on Check Password

In the Swivel Settings screen there is a field to indicate the URL of SRSC that is listening requests. This parameter is sent in the ?Get Config? message to the Core, and is saved as information of the Agent. NOTE: if this value is changed directly in the Core when a synchronisation is done or a get config message is sent, it will be changed again with the value sent by AD Agent. That URL is used by the Core to check the password of the users created through this Agent ONLY if the Agent XML or RADIUS has been configured as ?Check password with repository?



Encrypted Key: ••••••••••••••••••••••

URL check password: http://127.0.0.1:8080/srsc/admi

592.4.2 AD Agent Configuration - AD Settings

Allows settings to configure ctive Directory data source

Server: IP/Hostname where the AD is running.

Port: Port where the AD is running.

Username: AD administrator username

Password: AD administrator password

SSL: Checked if the connection is SSL, unchecked otherwise.

Self-Signed Certs: If checked indicates that in a SSL connection self-signed certs are accepted.

Username attribute: Indicates the username?s name attribute. By default: sAMAccountName

Base DN: Indicate the BaseDN, if empty will be root.

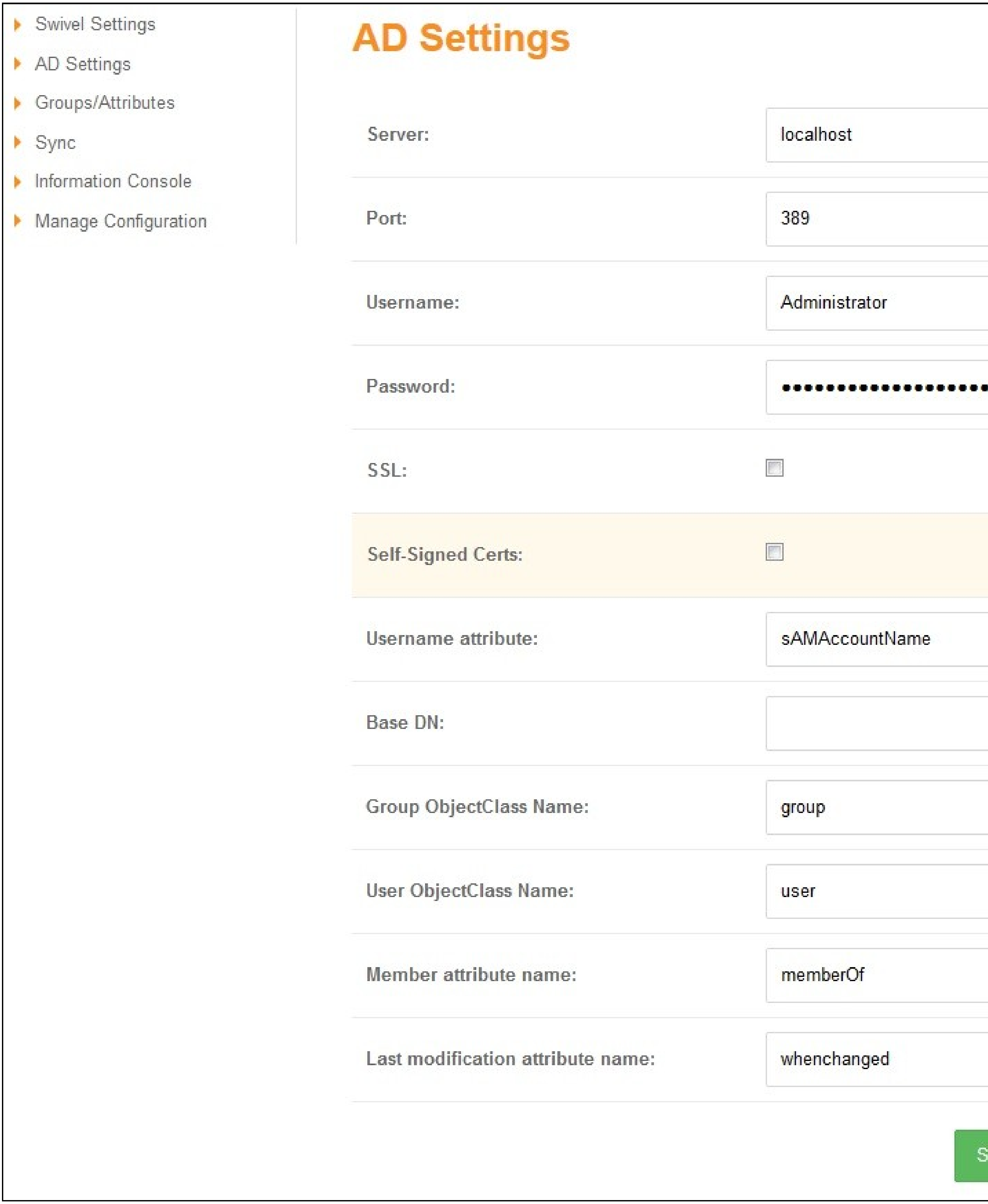
Group ObjectClass Name: Indicates the group object class name attribute. By default: group

User ObjectClass Name: Indicates the group object class name attribute. By default: user

Member attribute name: Indicates the member?s name attribute. By default: memberOf

Last modification attribute name: Indicates the last modification?s name attribute. By default: whenchanged

NOTE: Currently AD Agent gets only no disabled users, and to do that a rule has been added: ?!UserAccountControl:1.2.840.113556.1.4.803:2? this rule works for AD and it is something not configurable by the user in the application. This rule maybe is different for an OpenLDAP. So the good working is at the moment only covered for an AD.

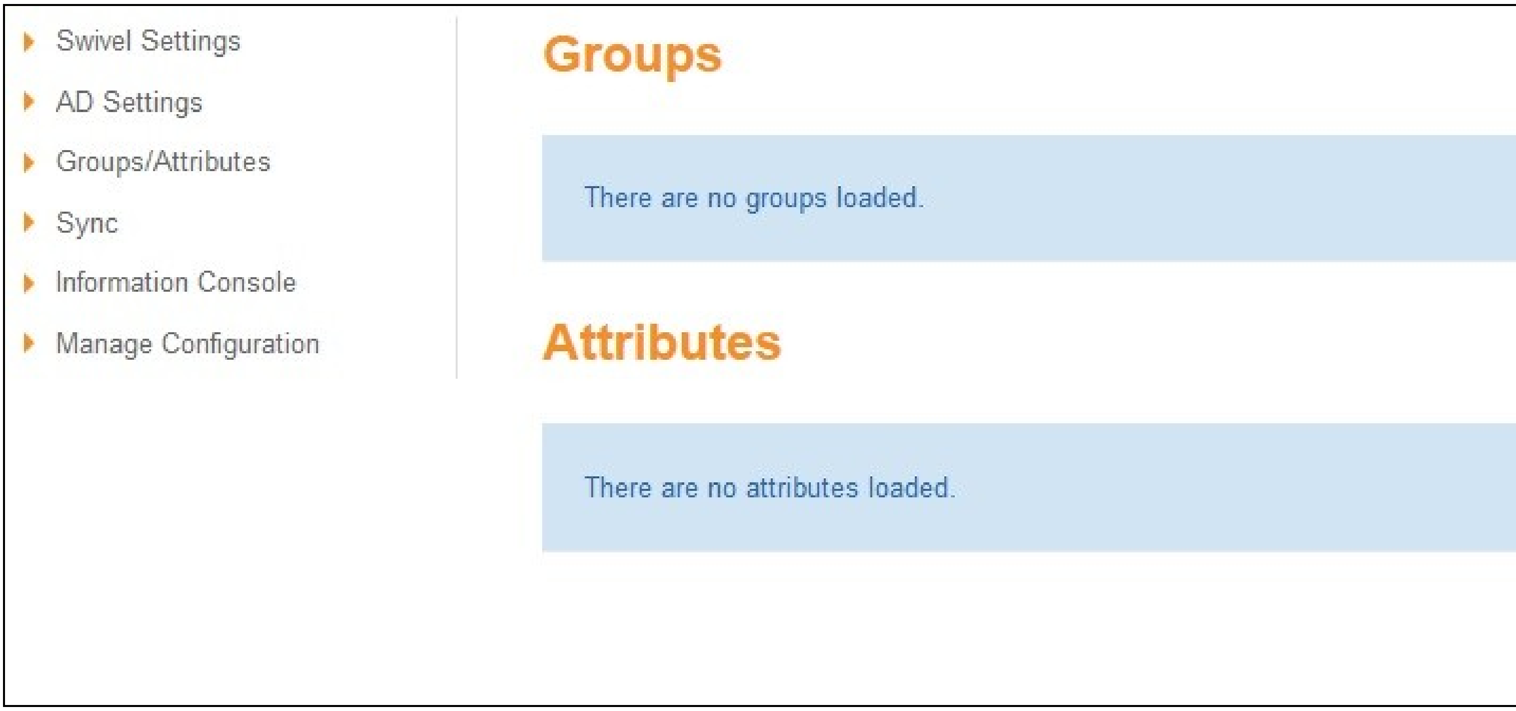


AD Settings

Server:	localhost
Port:	389
Username:	Administrator
Password:	•••••••••••••••••••
SSL:	□
Self-Signed Certs:	□
Username attribute:	sAMAccountName
Base DN:	
Group ObjectClass Name:	group
User ObjectClass Name:	user
Member attribute name:	memberOf
Last modification attribute name:	whenchanged

592.4.3 AD Agent Configuration - Groups/Attributes

Get Config connects to the configured Swivel instance and loads the Groups and Attributes available.



There are no groups loaded.

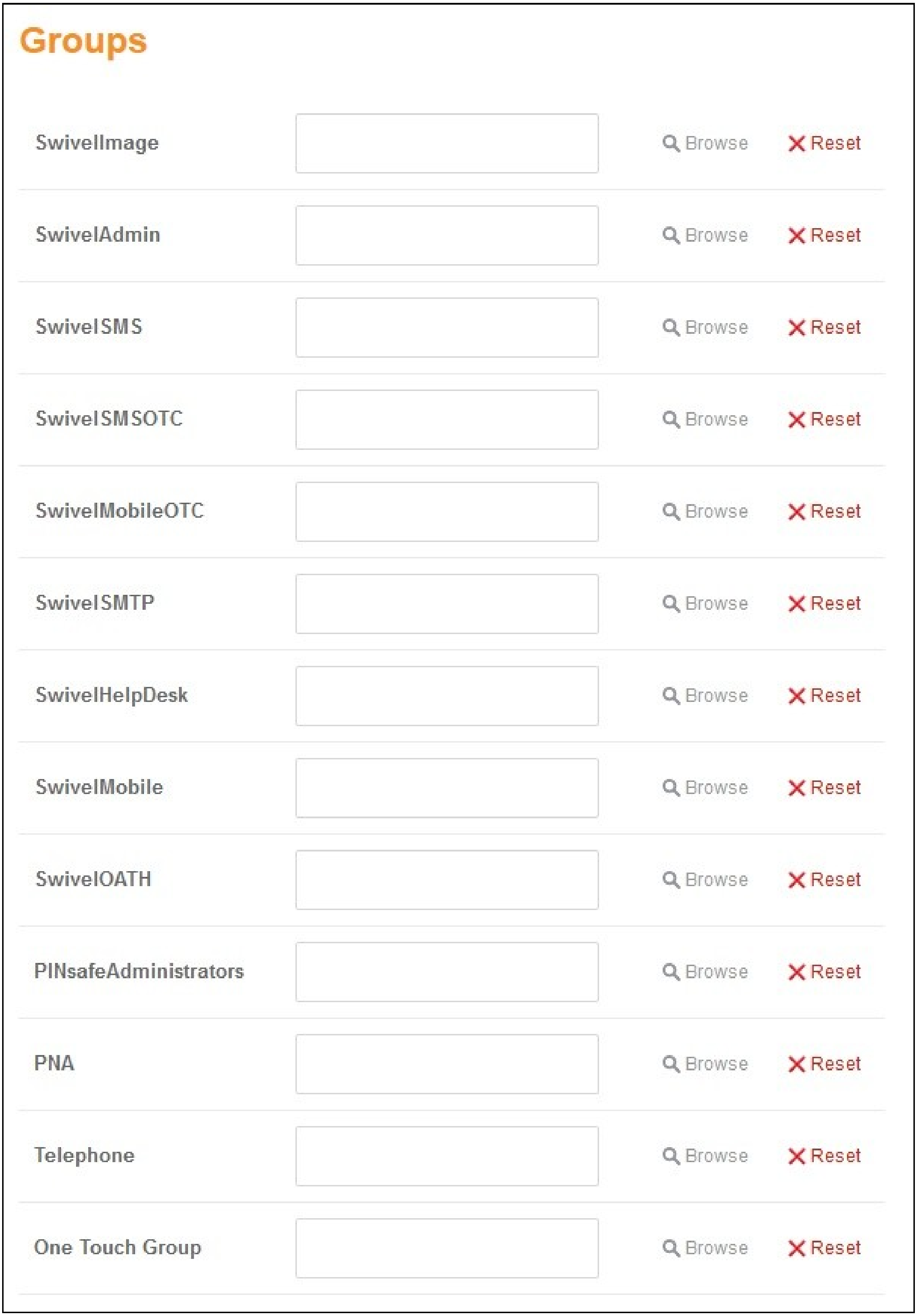
There are no attributes loaded.

The **Browser** screen shows the current AD Path, the name of the group that the user wants to assign a value on and a list of Groups and Subcontainers of the current path. When an AD group is selected it is automatically assigned to the group.

The second section on the Group/Attributes screen shows the attributes.

IMPORTANT: To save all the changes done in that screen ?Save? button has to be clicked.

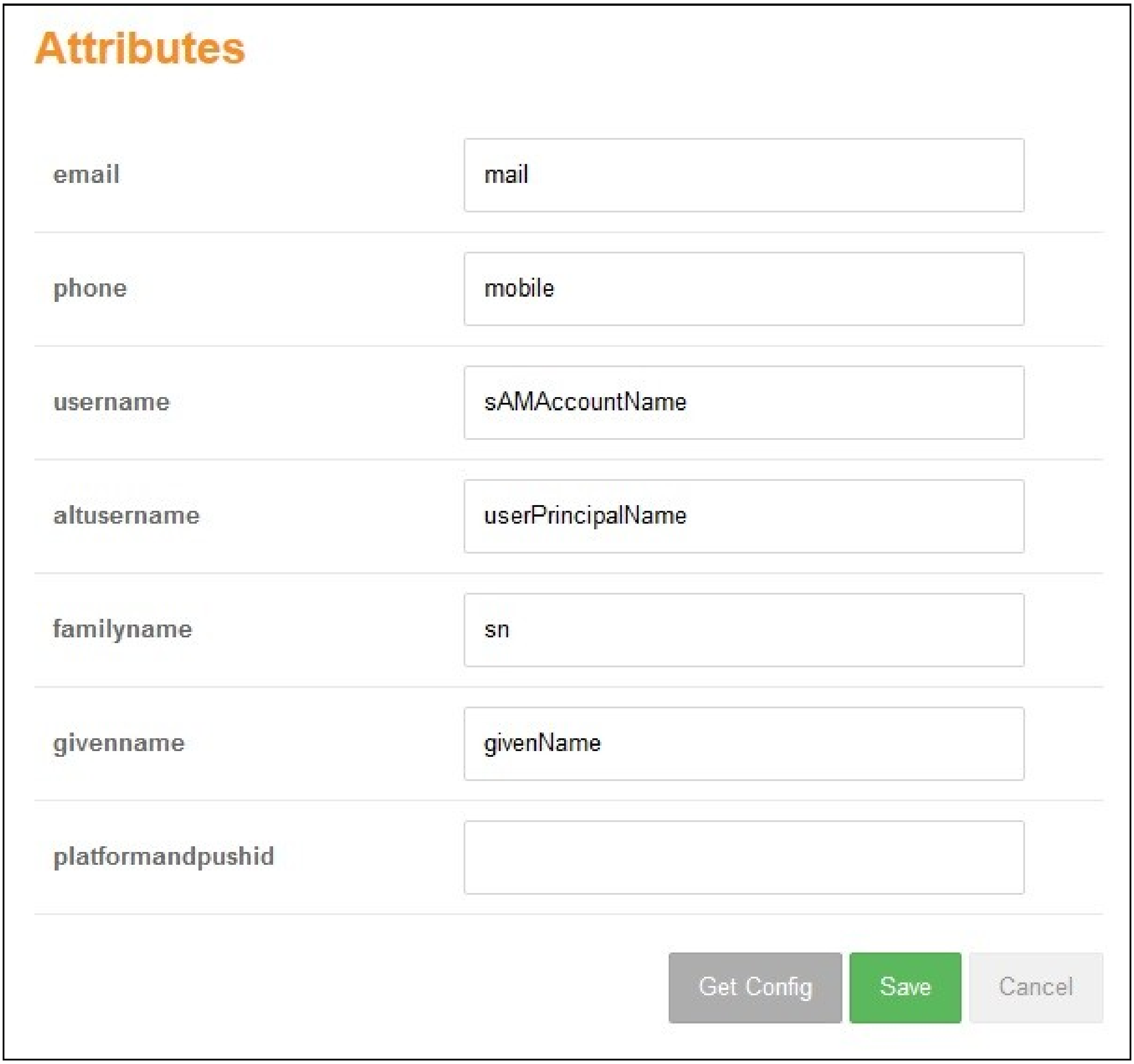
Browser Groups (imported from Swivel, values will depend n the Swivel setup)



Groups

SwivelImage		🔍 Browse	✕ Reset
SwivelAdmin		🔍 Browse	✕ Reset
SwivelSMS		🔍 Browse	✕ Reset
SwivelSMSOTC		🔍 Browse	✕ Reset
SwivelMobileOTC		🔍 Browse	✕ Reset
SwivelSMTP		🔍 Browse	✕ Reset
SwivelHelpDesk		🔍 Browse	✕ Reset
SwivelMobile		🔍 Browse	✕ Reset
SwivelOATH		🔍 Browse	✕ Reset
PINsafeAdministrators		🔍 Browse	✕ Reset
PNA		🔍 Browse	✕ Reset
Telephone		🔍 Browse	✕ Reset
One Touch Group		🔍 Browse	✕ Reset

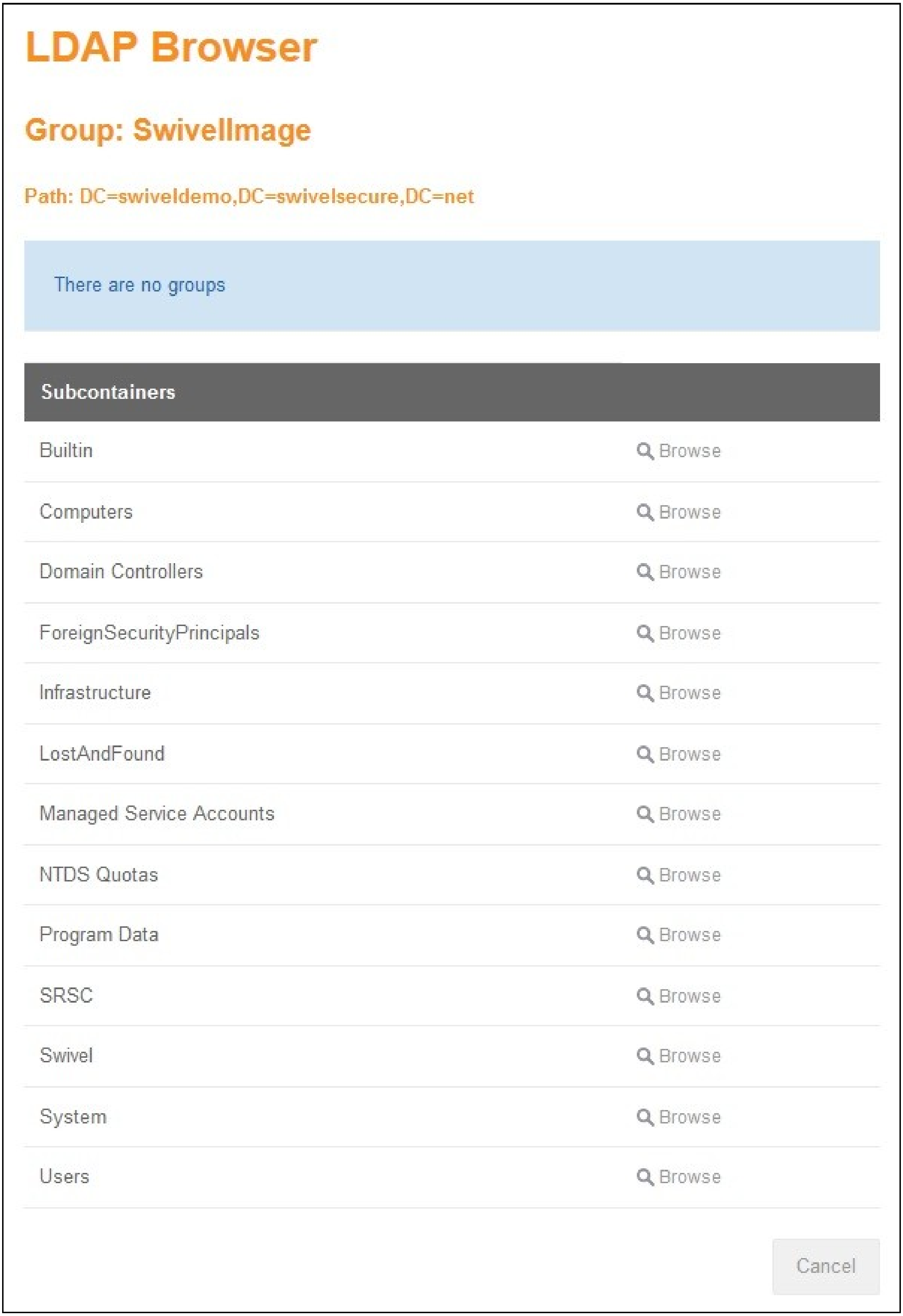
Browser Attributes (imported from Swivel, values will depend n the Swivel setup)



Attributes

email	mail
phone	mobile
username	sAMAccountName
altusername	userPrincipalName
familyname	sn
givenname	givenName
platformandpushid	

Browsing to the groups



LDAP Browser

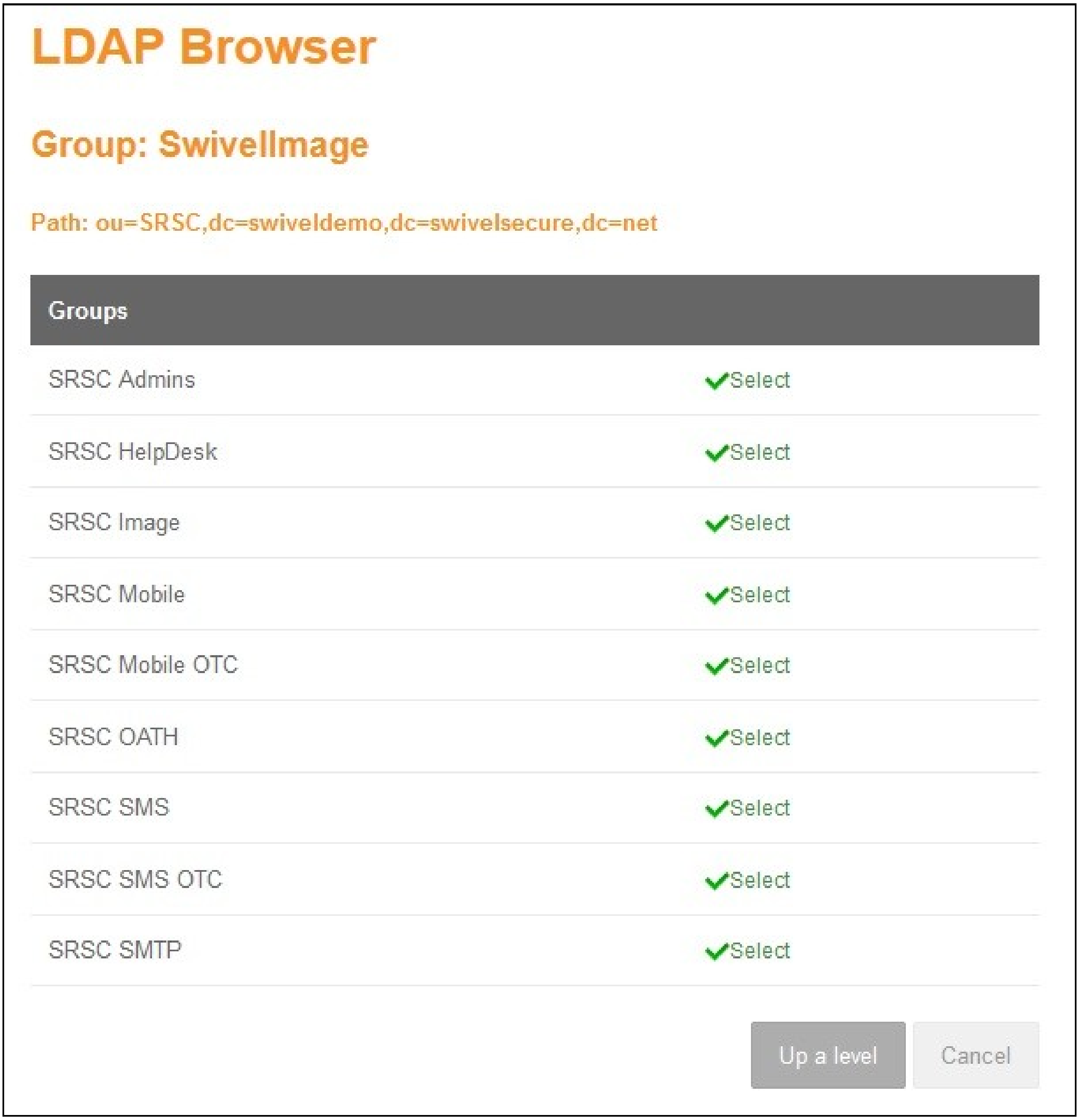
Group: SwivelImage

Path: DC=swiveldemo,DC=swivelsecure,DC=net

There are no groups

Subcontainers	
Builtin	Browse
Computers	Browse
Domain Controllers	Browse
ForeignSecurityPrincipals	Browse
Infrastructure	Browse
LostAndFound	Browse
Managed Service Accounts	Browse
NTDS Quotas	Browse
Program Data	Browse
SRSC	Browse
Swivel	Browse
System	Browse
Users	Browse

Selecting the Groups



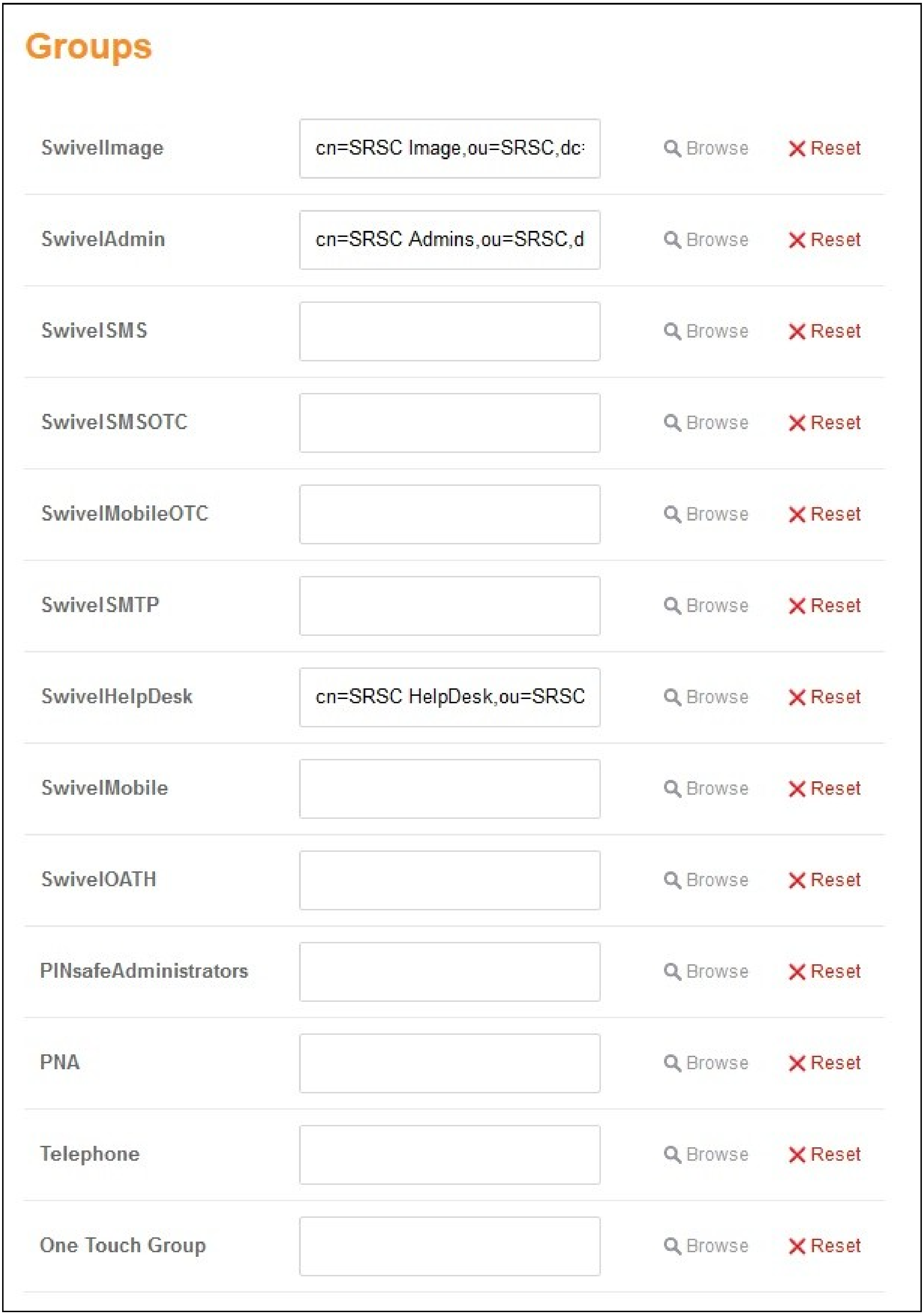
LDAP Browser

Group: SwivelImage

Path: ou=SRSC,dc=swiveldemo,dc=swivelsecure,dc=net

Groups	
SRSC Admins	✓Select
SRSC HelpDesk	✓Select
SRSC Image	✓Select
SRSC Mobile	✓Select
SRSC Mobile OTC	✓Select
SRSC OATH	✓Select
SRSC SMS	✓Select
SRSC SMS OTC	✓Select
SRSC SMTP	✓Select

Selected Groups



Groups

SwivelImage	cn=SRSC Image,ou=SRSC,dc:
SwivelAdmin	cn=SRSC Admins,ou=SRSC,d
SwivelSMS	
SwivelSMSOTC	
SwivelMobileOTC	
SwivelSMTP	
SwivelHelpDesk	cn=SRSC HelpDesk,ou=SRSC
SwivelMobile	
SwivelOATH	
PINsafeAdministrators	
PNA	
Telephone	
One Touch Group	

592.4.4 AD Agent Configuration - Sync

In the synchronisation screen, the user can indicate the maximum number of users that will be sent per message. If the number is 0 or less it will indicate that is not limit defined. Furthermore, the user can decide to do a Manual Sync clicking the corresponding button and/or define a scheduler for an automatic synchronisation. Also, there is a button to resync all the users.

The sync process involves the exchange of different types of messages as follows:

- AD Agent Request - Get Config / Response - Get Config (Groups and Attributes)

- AD Agent:

Groups not defined: Request - Error Groups / Response - Error Groups

All groups defined: No message

- AD Agent:

Get users members of the groups defined from AD

If there are users that have to be sync, the number of messages will depend of the maximum number of users per message

Request - Sync Users / Response - Sync Users

Update users last sync data if no error

No users to sync: no message sent

Information about the last synchronization (Manual or Scheduled) is shown. The information is as follows:

- Last sync date: date and time of last sync

- Type: Manual/Scheduled

- If there are groups not defined: Name of the groups not defined

- Created or updated users: number of OKs, number of FAILs

- Deleted users: number of OKs, number of FAILs

When a user has been synced with the Core, the next synchronization will not be update again unless:

- Data of that user has been updated in the AD after last sync, e.g. whenChange > lastSyncTime

NOTE: clocks of AD server and the SRSC has to be synchronized.

- There has been a change in the groups/attributes screen after last sync so next sync all the users will be updated.

Scheduled sync

To define a scheduled sync, set the field ?Scheduled sync activated?, when this field is checked a new field/s appear under this field to defined the scheduler. When the scheduler is defined the user has to click ?Save?, in than moment a job of synchronization will be started and executed every time that meet the time defined in the scheduler. If the job is already started and the user edit the scheduled time and press ?Save?, automatically the job will be rescheduled but if the user set unchecked the activated field the job will be stopped.

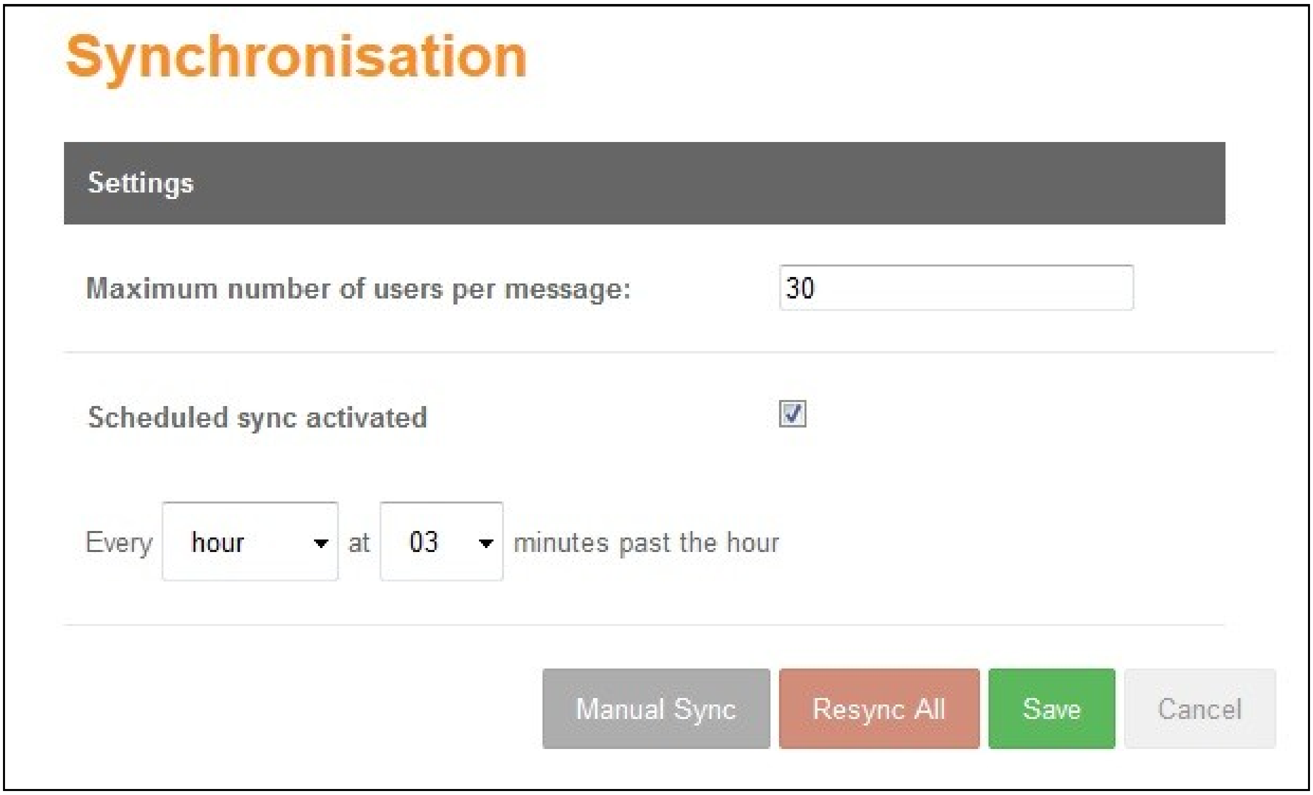
Manual Sync

When the user clicks ?Manual Sync? a confirmation dialog is shown, then if the user has accepted, a spinner overlap will be shown. That is useful to indicate to the user that the synchronization is working, mainly in synchronizations with a large amount of users that usually need more time and in addition, to avoid that the user clicks again Manual sync.

Resync All

This action allows to the user resync all the users independently of they were synced before or not.

NOTE: If the rights of the groups are changed in the Core those changes are not communicate to the AD Agent and the users won?t be updated. The next AD Agent synchronization won?t update the users of those groups if the data on the AD for that users has not be modified. In that case the resync all action has to be done to update the rights.



Synchronisation

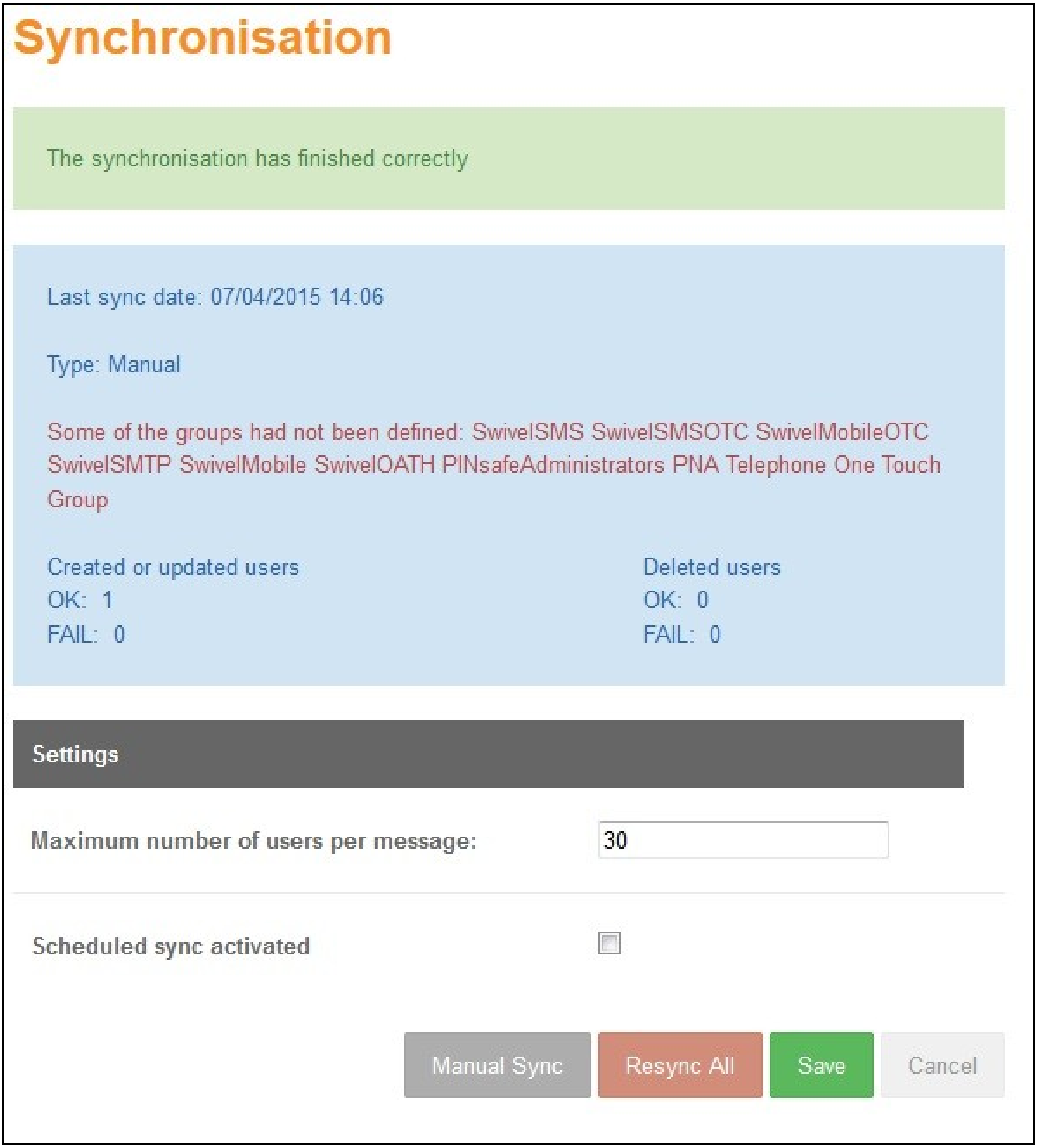
Settings

Maximum number of users per message: 30

Scheduled sync activated ☑

Every hour at 03 minutes past the hour

Manual Sync



Synchronisation

The synchronisation has finished correctly

Last sync date: 07/04/2015 14:06

Type: Manual

Some of the groups had not been defined: SwivelSMS SwivelSMSOTC SwivelMobileOTC SwivelSMTP SwivelMobile SwivelOATH PINsafeAdministrators PNA Telephone One Touch Group

Created or updated users
OK: 1
FAIL: 0

Deleted users
OK: 0
FAIL: 0

Settings

Maximum number of users per message: 30

Scheduled sync activated □

592.4.5 AD Agent Configuration - Information Console

This shows the information about the messages exchanged between AuthControl Sentry and AD Agent. The messages can be deleted automatically using a schedule job that will be executed every day at 19:00. That configuration could be changed in the file distpatcher-servlet.xml if it was needed. The user can customize the deletion indicating the number of days that the info message has to have to be considered old and the next execution of the job it will be deleted. If the number the days is less than 0 all the messages will be deleted.

Example: Number of days 1 - the messages previous to the current day will be deleted.

592.4.6 AD Agent Configuration - Manage Configuration

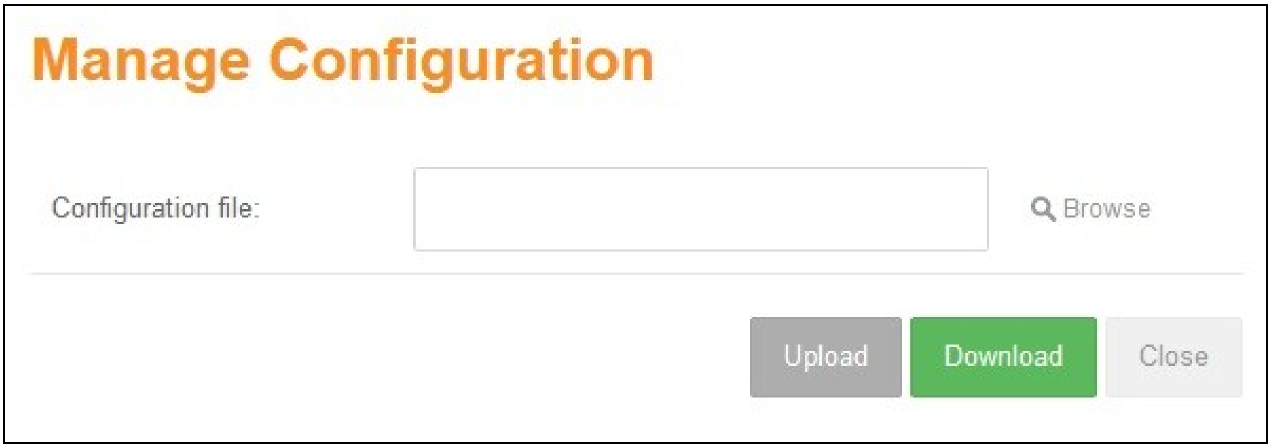
The application allows download the current configuration or upload a configuration previously stored.

The configuration exported contains the following:

- Swivel Settings

- AD Settings

- Groups/Attributes
- Sync settings
- Information Console settings.



593 Testing

594 Known Issues

595 Troubleshooting

AD Agent:Message encrypted

Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

Message decrypted

Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

Searching encryption key for the IP: 192.168.12.110, agent name found: AD Agent

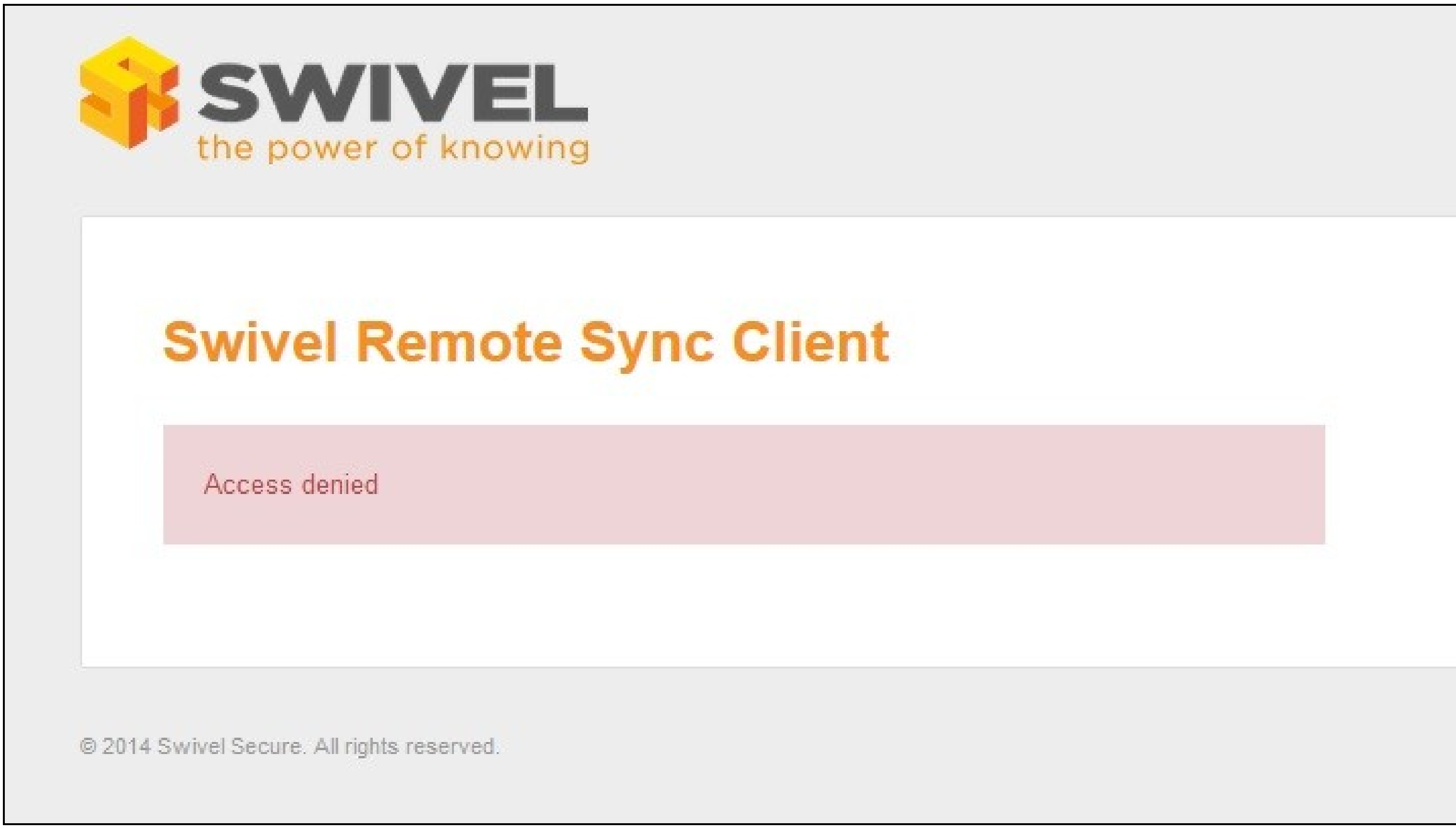
Message seen on the Swivel Core Log Viewer for communication with the AD Agent.

ERROR RestTemplateServiceImpl:72 - [MTD] sendPostMessage [MS G] Error: org.springframework.web.client.ResourceAccessException: I/O error on POST reques t for "https://192.168.12.111:8443/proxy/AdminXML": hostname in certificate didn't match: <192.168.12.111> != <*.swivelsecure.com>; nested exception is javax.net.ssl.SSLException: hostname in certificate didn't match: <192.168.12.111> != <*.swivelsecure.com>

Error seen in the AD Agent console for a certificate not matching the hostname. Select Self-Signed Certs.

ERROR ConfigurationController:81 - [MTD] getConfigRequest [MSG] Connection error

Error seen in the AD Agent console, unable to connect to the Swivel core.



SWIVEL
the power of knowing

Swivel Remote Sync Client

Access denied

© 2014 Swivel Secure. All rights reserved.

Access Denied

If trying to access the login page goes straight to Access Denied, check the IP security filter addresses.

There was an error getting configuration In the AD Agent console

Response: Parse Error In the SRSC log

Check the AD data source configuration.

The '*Encrypted Key:* needs to be configured with the Swivel core to match that under Sever/Agents for the correspoding AD Agent.

ERROR EncryptionUtility:103 - [MTD] initCiphers [MSG] Error: javax.crypto.BadPaddingException: Given final block not properly padded in the AD Agent program console.

The '*Encrypted Key:* needs to be configured with the Swivel core to match that under Sever/Agents for the correspoding AD Agent.

AD Connection error in the AD Agent Administration console.

2015-04-07 12:57:18 ERROR ConfigurationController:148 - [MTD] ldapBrowser [MSG] Error: org.springframework.ldap.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1]; nested exception is javax.naming.AuthenticationException: [LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9, comment: AcceptSecurityContext error, data 52e, v1db1] **in the SRSC program console.**

Use username@fqdn for the AD Settings

596 Telephone Authentication

597 Overview

Voice authentication allows a telephone number (Mobile or landline) to be called by the Swivel server to let the user authenticate by:

- Pressing # or other defined characters on phone keypad
- Enter OTC on phone keypad. The OTC may be from a security string or PINless

For other forms of authentication see: Transports How To Guide

597.1 Technical explanation

Login page starts a session and retrieves a session ID.

The login page then displays the TURing image for that sessionid using a TCImage request, for example https://hostname:8443/TCImage?username=test.

This causes the core platform to initiate the call.

The user answers the call and types the OTC.

The telephony provider posts the OTC to the Swivel core.

The Swivel Core works out who the user is from the phone number, updates the session by injecting the OTC into it.

The login page polls the core platform to see if the session has been updated. When it has the login page is submitted.

The login page actually submits the username and the session ID (if the mode is match, this means the OTC submitted by the form must match that type on the phone, in this mode the OTC is submitted not the sessionID).

The Swivel Core looks up the session id, reads the OTC from the session and processes the authentication as usual.

598 Prerequisites

Swivel 3.10 onwards

Nexmo Account

599 Swivel configuration

599.1 Add an Agent

On the Swivel Administration console select Server/Agents, and ensure that an Agent exists to allow communication to the Swivel server. On Swivel virtual and hardware appliances a local agent will exist by default.

See Agents How to Guide

599.2 Configure Dual Channel settings

On the Swivel Administration console select Server/Dual Channel and ensure the below settings are configured:

Set On-Demand Delivery: to Yes

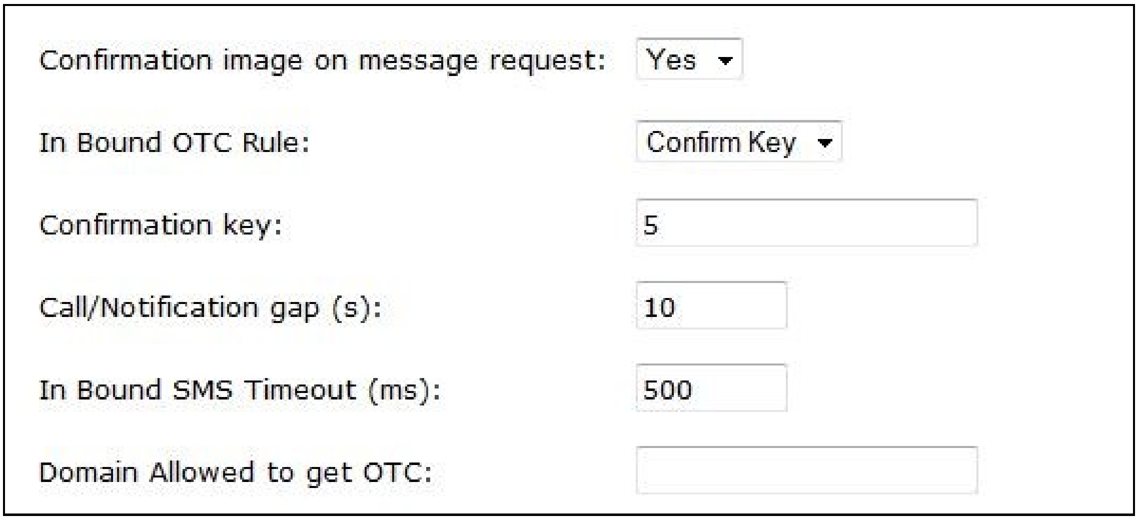
Set Allow message request by Username: to Yes

In Bound OTC Rule:

- None - No inbound
- Match - Must be the same on the telephone keypad as in the login
- Message - OTC comes from phone only
- Confirm key - enter the digits defined under Confirm Key to authenticate

Confirmation key (may be shown as [server_dualchannel_inboundconfirmkey]): The key(s) to be pressed to confirm authentication

Call/Notification gap (s) (may be shown as [server_dualchannel_inboundcallgap]):

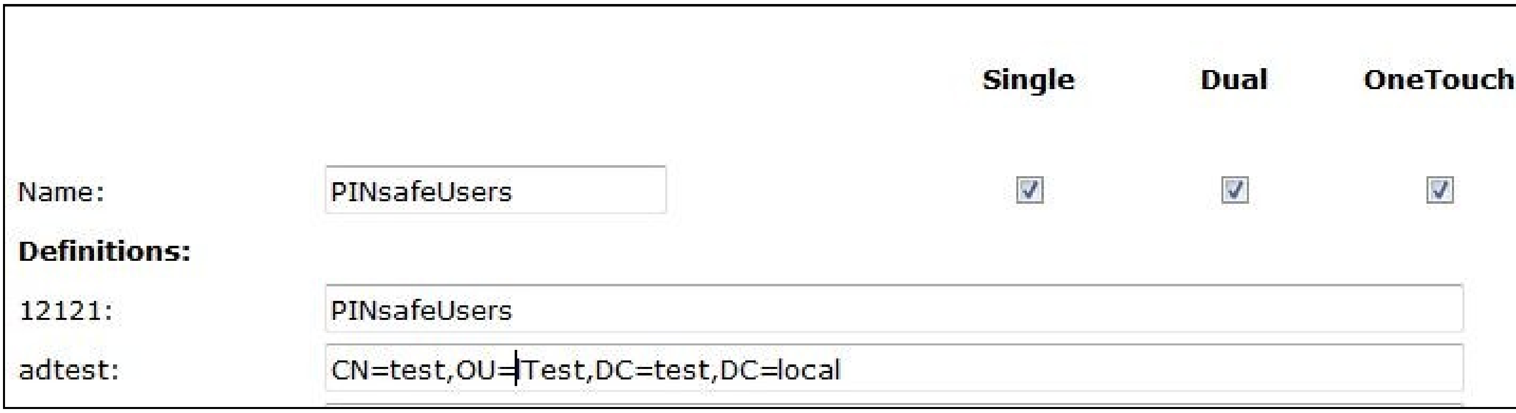


Confirmation image on message request:	Yes
In Bound OTC Rule:	Confirm Key
Confirmation key:	5
Call/Notification gap (s):	10
In Bound SMS Timeout (ms):	500
Domain Allowed to get OTC:	

NOTE: The Server -> Voice Channel page is not required any more. The options on this page are replaced by the Dual Channel and NexmoVoice options.

599.3 Define a group of Telephony Users

On the Swivel Administration console, select a group of users that will be using Telephony authentication and ensure that the Telephony box is ticked then click Apply.



		Single	Dual	OneTouch
Name:	PINsafeUsers	☑	☑	☑
Definitions:				
12121:	PINsafeUsers			
adtest:	CN=test,OU=Test,DC=test,DC=local			

599.4 Define a Telephone Transport

On the Swivel Administration console, select or create a voice Transport such as NexmoVoice

Identifier: NexmoVoice

Class: com.swiveltechnologies.pinsafe.server.transport.NexmoVoiceTransport

Strings per message: 1

Copy to alert transport: Yes No

Destination attribute: None

Strings Repository Group: NONE

Alert repository group: NONE

[transport_general_classes_twowaygroup]: The Telephony group defined above e.g. PINsafeUsers

599.5 Configure a Telephone Transport

On the Swivel Administration console select the created Transport then enter the configuration details (note the default URL has changed from rest to api):

[transport_nexmo_timeout]: 180000

[transport_nexmo_prompt]: Enter your one-time code:bye

[transport_nexmo_nexmomessageurl]: https://api.nexmo.com/tts/xml

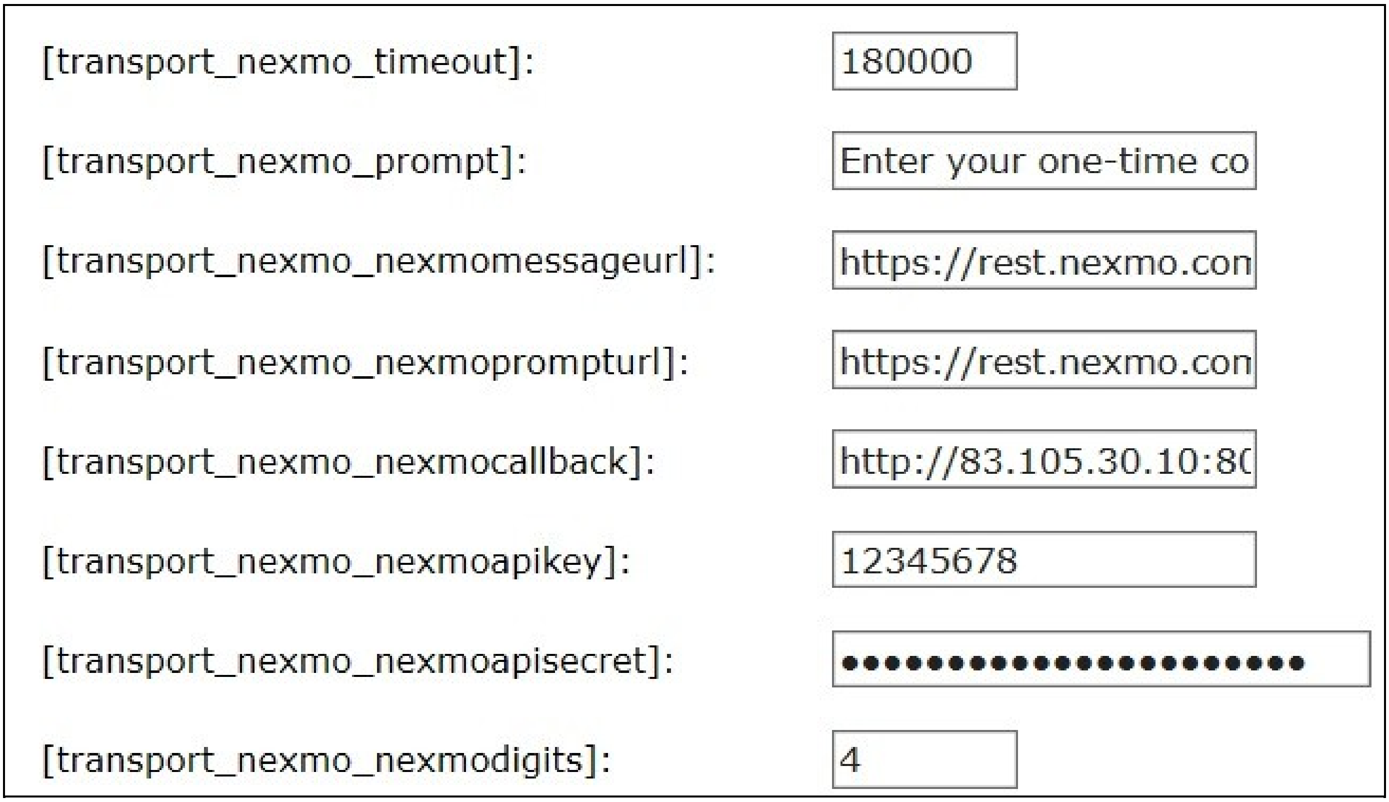
[transport_nexmo_nexmopprompturl]: https://api.nexmo.com/tts-prompt/xml

[transport_nexmo_nexmocallback]: http://83.105.30.10:8080/pinsafe/nexmoinbound

[transport_nexmo_nexmoapikey]: Your Nexmo account key

[transport_nexmo_nexmoapisecret]: Your Nexmo account password/secret

[transport_nexmo_nexmodigits]: 4 (to match the OTC length)



[transport_nexmo_timeout]:	180000
[transport_nexmo_prompt]:	Enter your one-time co
[transport_nexmo_nexmomessageurl]:	https://rest.nexmo.con
[transport_nexmo_nexmoprompturl]:	https://rest.nexmo.con
[transport_nexmo_nexmocallback]:	http://83.105.30.10:8(
[transport_nexmo_nexmoapikey]:	12345678
[transport_nexmo_nexmoapisecret]:	●●●●●●●●●●●●●●●●●●●●●●
[transport_nexmo_nexmodigits]:	4

600 Testing

The Swivel Telephony can be configured to work with a an authentication portal. For testing it is possible to use the User Portal.

600.1 Configuring the User Portal

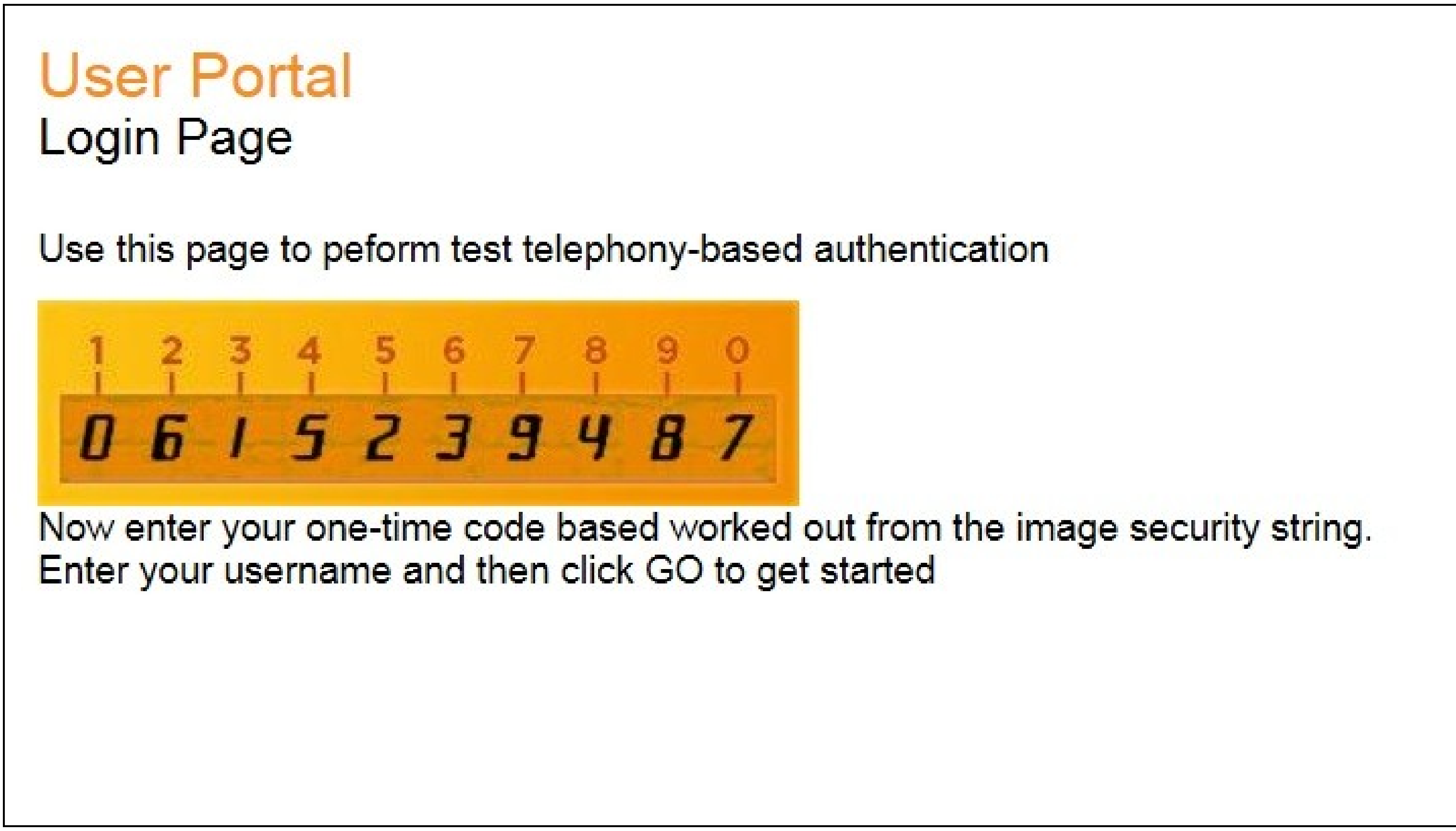
Edit the userportal/js/ajax.js file and make sure the top line has the serverContext variable set

var serverContext = https://localhost:8080/pinsafe

If it is installed on a different server then a Hostname or IP address will need to be specified. If HTTP is used instead of HTTPS then this may need to be changed.

600.2 Testing with the User Portal

Browse to https://IP_Hostname:8443/userportal/telephonylogin this will present the user with a Username and OTC field. Enter the Username then click Go. The user should be displayed a TURING image and receive a call. The User can enter on the Telephone using the keypad, and then also in the OTC field on screen, if they are set to match. If both are correct the authentication succeeds.



User Portal

Login Page

Use this page to peform test telephony-based authentication

Now enter your one-time code based worked out from the image security string.
Enter your username and then click GO to get started

601 Known Issues

602 Troubleshooting

Check the Swivel logs for error messages

Try with the country code

If a phone number is not receving calls, check the Swivel logs

Nexmo have a number of error Codes on their website which may be returned: What are Nexmo delivery error codes?

602.1 Error Mesages

LOG_HTTP_TRANSPORT_ERROR, https://rest.nexmo.com/tts-prompt/xml

LOG_HTTP_TRANSPORT_ERROR, 404 Not Found

The Nexmo transport has changed, use https://api.nexmo.com/tts-prompt/xml

603 Testing PINsafe Installations

603.1 Overview

This documents covers some simple tests that can be used to verify PINsafe installations and may be used as part of a Installation Acceptance Test.

A copy of the test plan can be downloaded in Word format from here PINsafe Test Plan.zip

603.2 Prerequisites

PINsafe 3.x

603.3 PINsafe Implementation Test Plan

603.3.1 Test Results

- Yes: Positive
- No: Negative
- NA: Not Applicable
- TBC: To be Confirmed

603.3.2 Network Test

603.3.2.1 Network connectivity test

Ping Gateway

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.2.2 DNS test

NSlookup to verify DNS

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.2.3 NTP test

(Successful installation of NTP verifies on appliance)

Ping Gateway from Appliances

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.3 Administration test

603.3.3.1 Administration Console test

Connect to PINsafe Administration Console, port 8080

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.3.2 Webmin test (for appliances)

Connect to PINsafe Webmin, port 10000

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.3.3 Proxy port test (for appliances)

TURing Image Request from port 8443

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.3.4 ChangePIN test

Connect to the ChangePIN page and change a users PIN

Primary appliance result:

Standby appliance result:

Connect to the ChangePIN page and verify failure if incorrect PIN is used to change a users PIN

Primary appliance result:

Standby appliance result:

603.3.3.5 ResetPIN test

Connect to the ChangePIN page and change a users PIN

Primary appliance result:

Standby appliance result:

Connect to the ResetPIN page and verify failure if an incorrect CODE is used

Primary appliance result:

Standby appliance result:

603.3.4 Database Replication Test (For MYSQL)

603.3.4.1 User Synchronisation test

Create a user on Primary and another on Standby, verify users exist

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.4.2 Data Synchronisation test

Verify MySQL status are in synchronisation

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.5 VIP Failover (For PINsafe VIP installs)

603.3.5.1 VIP moves to Standby test

Shutdown Primary appliance and authenticate on Standby/DR appliance using VIP

Standby appliance result:

603.3.5.2 VIP moves to Primary test

Shutdown Standby appliance and authenticate on Primary/DR appliance

Primary appliance result:

603.3.6 Transport test

603.3.6.1 User Security String test

Send PINsafe user a security String

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.6.2 User Alert test

Send PINsafe user an Alert

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.6.3 Admin user Security String test

Send PINsafe Admin user a security String

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.6.4 Admin user Alert test

Send PINsafe Admin user an Alert

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.6.5 Helpdesk user Security String test

Send PINsafe Helpdesk user a security String

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.6.6 Helpdesk user Alert test

Send PINsafe helpdesk user an Alert

Primary appliance result:

Standby appliance result:

DR appliance result:

603.3.7 Authentication Test

603.3.7.1 Test Authentication Succeeds

From Integrated Access device test authentication succeeds as expected

603.3.7.2 Test Authentication Fails as expected

From Integrated Access Client test authentication fails as expected

Repeat for each integrated device

604 Timezone

605 Timezone Overview

Each Swivel database will use the Timezone of the Swivel server that writes data into it. **All instances of Swivel that use the same database should be set to the same Timezone**: credentials set using one timezone are not valid in another. The Timezone should be set before configuring the Swivel application, and a restart made of the database.

The Swivel appliances are by default set to use GMT with daylight savings (BST).

To change the Timezone after adding users obliges to reset pins for those users.

606 Prerequisites

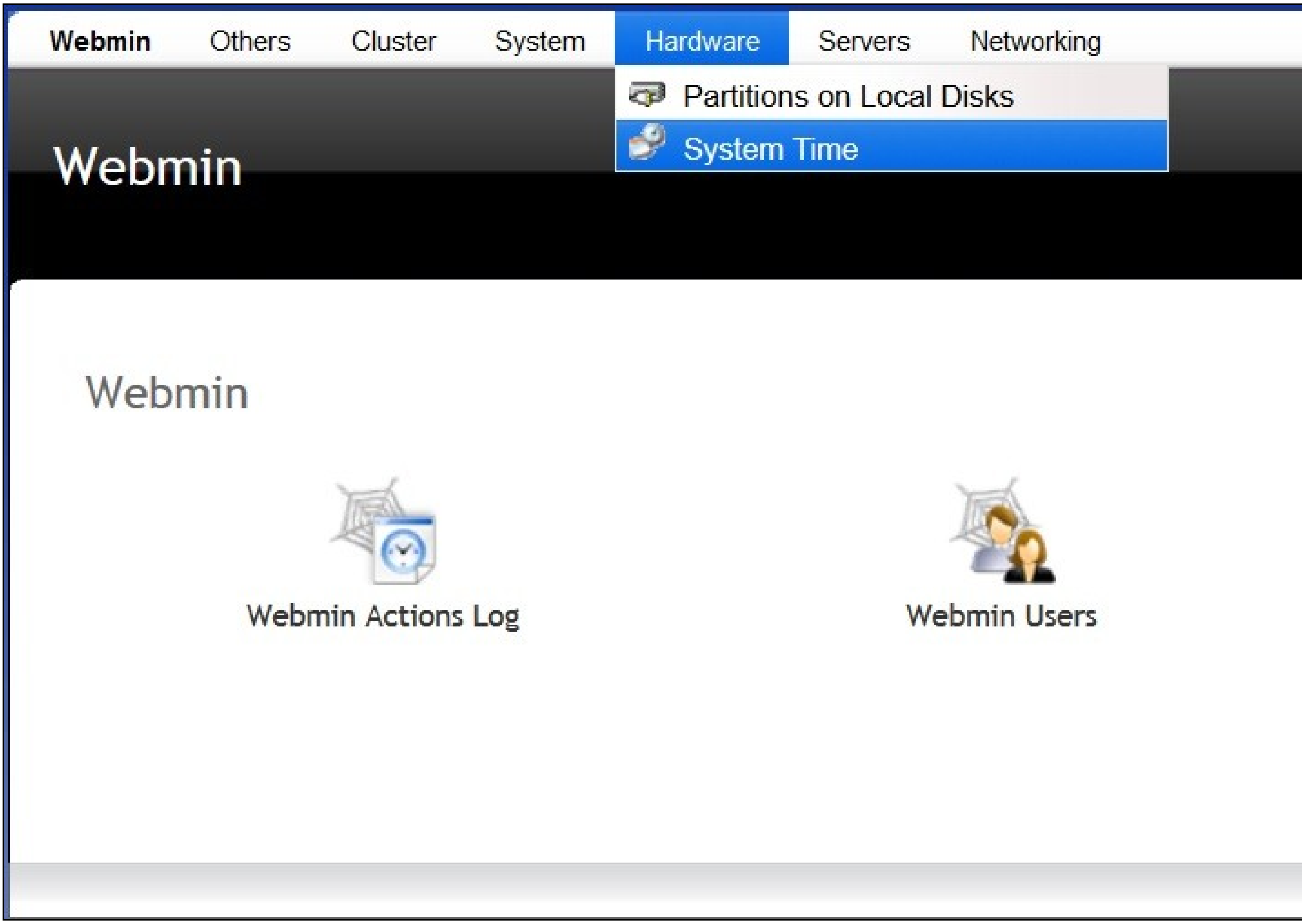
Swivel 3.x

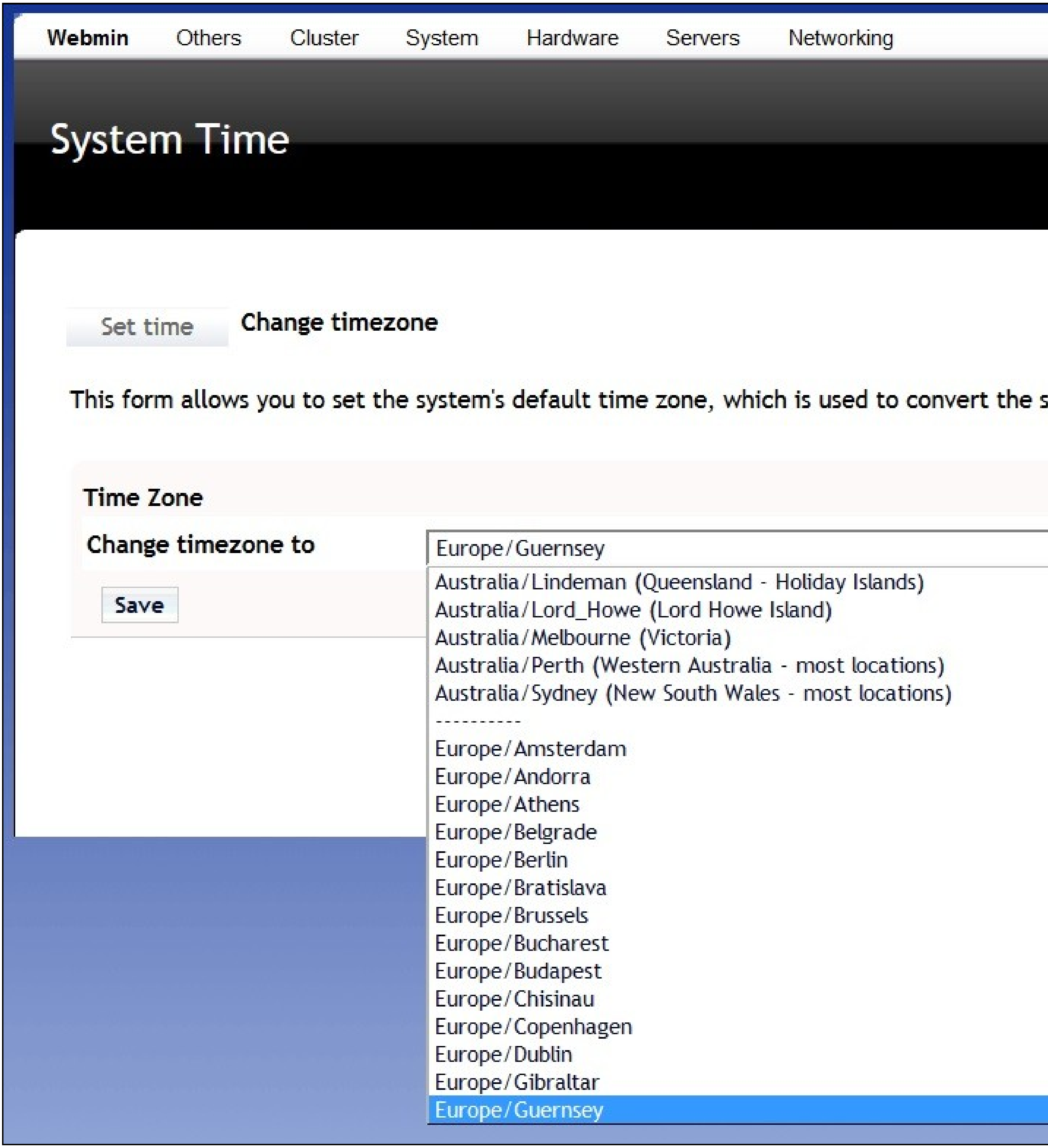
607 Swivel appliance Timezone change

Changing the Timezone on a Swivel appliance is done through the Webmin.

On each of the Swivel appliances set the timezone to be the same timezone, from the Webmin select Hardware, then System Time and then the tab for Change timezone. Select the required timezone then click save. It is not recommended to have Swivel instances on different timezones.

Restart the database after setting the timzone, for internal restart Tomcat, for MySQL restart MySQL on each Swivel instance after the change is made.





System Time

This form allows you to set the system's default time zone, which is used to convert the s

Time Zone

Change timezone to: Europe/Guernsey

Australia/Lindeman (Queensland - Holiday Islands)
Australia/Lord_Howe (Lord Howe Island)
Australia/Melbourne (Victoria)
Australia/Perth (Western Australia - most locations)
Australia/Sydney (New South Wales - most locations)

Europe/Amsterdam
Europe/Andorra
Europe/Athens
Europe/Belgrade
Europe/Berlin
Europe/Bratislava
Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Chisinau
Europe/Copenhagen
Europe/Dublin
Europe/Gibraltar
Europe/Guernsey

608 Testing

609 Known Issues

After a migration the error message: "The user does not have a PIN set" might mean a Timezone configuration issue between the backup version and the newer one.

610 Troubleshooting

For migration issues check the Timezone configurations.

611 Token

612 Overview

Swivel supports the use of hardware tokens for authentication and can be used as **"something you have"** in Two Factor Authentication. The Swivel OATH HOTP Hardware Token and Swivel OATH TOTP Hardware Token provide a value that is a One Time Code (OTC) which can be used to authenticate a user, other compatible tokens may also be used. For other forms of authentication see Transports How To Guide.

- Each user can be assigned a single token.
- Each token can be assigned to a single user.
- A Swivel installation can use HOTP, TOTP and OCRA tokens
- The token can be a software token or a hardware token as in the picture below

613 Prerequisites

Swivel 3.9.6 onwards

OATH HOTP compatible Token such as the Swivel OATH HOTP Hardware Token, Yubikey

Swivel 3.10.1 onwards

OATH TOTP compatible Token such as the Swivel OATH TOTP Hardware Token

Swivel 3.10.2 onwards

OATH OCRA compatible Token such as the Swivel OATH OCRA Hardware Token

614 Configuring tokens

Each token has a serial number and an associated seed. The Serial number and seed are entered into the Swivel database and then associated with a single user. Hardware tokens usually have a serial number on the back of the token. The seed is usually sent separately from the token.

614.1 Tokens and PIN numbers

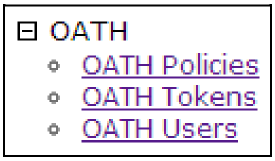
If the feature to allow a PIN to be is used with the Token is enabled, the OTC is entered first from the hardware token, then the PIN number.

<OTC><PIN>

For example for a token OTC of 111111 and a PIN of 0000, then enter 1111110000.

It is also possible to use a Token with an additional One Time Code (PINless), if the PINless code is more than six digits to differentiate it from the Token code.

614.2 OATH Menu



A new menu entry can be found on the left hand side of the Swivel Administration Console. This is where the tokens are added and then assigned to users.

614.3 Adding tokens

On the Swivel Administration Console select OATH then OATH Tokens, enter the serial number and seed. Large numbers of tokens can be imported through a CSV (Comma Separated Values) file. The format for the CSV file is:

```
Serial,Seed
Serial,Seed
Serial,Seed
```

One per line, entries after the first two per line are ignored.

The seed format Swivel is expecting is in HEX, 40 Characters long is the standard. The OATH standard generates a numeric One Time Code.

614.3.1 Hardware Tokens

Compatible tokens can be used with Swivel, for details on the Swivel token see Swivel OATH HOTP Hardware Token. Hardware tokens are supplied with a unique seed and serial number that is valid only for the specified hardware token.

614.3.2 Software Tokens

Software tokens may be used with an appropriate seed, and may be used with an appropriate software token such as Google Authenticator.

614.4 Configuring users with tokens

Hardware and Software tokens can be used with Swivel using a compatible seed.

On the Swivel Administration Console select OATH then OATH Users, for the required user click on Assign token, then select the required token serial number. The user must be a member of a Swivel Group that contains the permission to allow tokens.

614.5 OATH configuration

The following options may be configured for OATH.

Token Type: HOTP

OTP Length:, default 6, the Swivel OATH HOTP Hardware Token is a six digit token.

Error Window (Events):, default 5. If the difference between the number of button presses that the server has recorded and the actual number of button presses on the token is less than the error-windows, the authentication is allowed

Sync Windows (Events):, default 10. If the difference between the number of button presses that the server has recorded and the actual number of button presses on the token is greater than the error window but less than the Sync window, the authentication will fail but the server button-press count on the server is updated. This means if the user attempts to authenticate again, the next authentication will succeed.

Append PIN (if user has one) after OTP: , default No, Options Yes/No. If set to Yes the user must enter their PIN directly after the OTC generated by the token, without any decoration (i.e. ?,?).

615 Administering Tokens

Tokens can be synchronized for use.

Either from the OATH Tokens or the OATH Users list click on Re-sync for the required token or user. Enter the value displayed by the token, and then enter the next value for that token (must be the next value).

616 User Self Help for Synchronizing Tokens

Users may synchronize tokens themselves through the User Portal.

617 Integrating with Tokens

Integration of login portals is usually straight forward with Tokens, although if TURing and Pinpad images are used, then these should not be automatically generated as a login will be expected using those methods.

618 Testing

Add a token and ensure that it can be used for authentication.

An Administrator or Helpdesk user can test a token by logging into the Swivel Administration console if they have OATH and Admin or Helpdesk permissions, and do not generate a TURing image, if a TURing image is generated, then it will expect that to be used for authentication for the length specified under Server/Jobs/Session Cleanup (default 2 minutes).

619 Known Issues

Swivel 3.9.6 and 3.9.7 Oath seeds are not moved when a Swivel database is migrated. Workaround: Upgrade to 3.10 or re-import seeds into new database

Swivel 3.9.6 using PIN and Token fails. Upgrade to Swivel 3.10 or later.

620 Troubleshooting

Check the Swivel logs.

Token is out of synchronization, re-synchronize as described above.

On the User Administration for the user click on Reset Password, and reset it, but leave the password fields blank.

Are you using PIN entry with the Token? When a PIN is used with the Token, the OTC is entered first from the hardware token, then the PIN number. For example for a token OTC of 111111 and a PIN of 0000, then enter 1111110000

Is the serial number correct for the token?, Was the seed entered automatically or manually? Try re-entering it

620.1 Error Messages

Unable to synchronize OATH Token

Note - This error appears on-screen if the OATH Token fails to synchronise. Namely, with Time based (TOTP) tokens, there may be a time drift on the Swivel Server. From the Command Line, run the command: date

Ensure that the time stamp is correct and it has not drifted over 5 minutes.

Servlet.service() for servlet SyncOathToken threw exception

Incorrect seed entered for token

Token autosynced for user gfield

This message is logged when the Sync Windows (Events) is matched and the token is resynced. The login fails but the next login will succeed.

AgentXML request failed, error: The XML request sent from the agent was malformed

This has been seen when using the User Portal with Swivel version 3.10. Upgrade the User Portal.

TOKEN_BAD_SEED

The seed used is incorrect or in the wrong format

621 Transient Data Storage

622 Transient Data Storage Overview

From version 3.9.1 user and configuration data (Transient data) is stored separately from the Swivel application. Transient data includes Configuration files, data, XML repository, logs and reports are stored externally to the Swivel application.

Note this does not include java class files, such as those for transport classes or database drivers, these may need to be copied/moved/restored manually.

623 Prerequisites

Swivel 3.9.1 onwards

624 Transient Storage Guide

624.1 Transient Data Storage Default path

The data will be contained in folders within <user.home>/.swivel

In Linux based systems the default will be /home/<username>/.swivel

If Tomcat is run as a service in Windows then the transient data may be located in c:\.swivel

In Windows 7 the default will be c:\users\<username>\.swivel

Note: Windows naming of files. You cannot create file or folder in Windows Explorer starting with . but you can using the Windows command line. Create a folder swivel, then from the Windows command line use *move swivel .swivel*

624.2 Transient Data Storage Custom Path

Each Swivel instance from version 3.9.2 onwards may have a defined transient data storage path and this may be of use where several Swivel instances are installed on Tomcat.

The transient data storage can be modified at the time of install or modifying an existing installation.

624.2.1 Installation/upgrade transient data default storage path

To define the data storage path open the pinsafe.war archive and edit the file WEB-INF\web.xml, see below for what to edit. When Swivel is installed it will be installed with this transient data path. When upgrading from a version of Swivel prior to 3.9.1, the data will be copied from the pinsafe folder to the new transient data store.

624.2.2 Existing installation data default storage path

stop Tomcat

Edit the following file <path to Tomcat install>/pinsafe/WEB-INF/web.xml

For appliances this is /usr/local/tomcat/webapps/pinsafe/WEB-INF/web.xml

See below for what to edit.

The transient data should be copied from the old location to the new location.

start tomcat

624.2.3 Editing the Custom transient data storage Path

look for the following section:

```
   <env-entry>
        <description>If non empty value, will be the root for all the data - takes precedence over default and environment variable</descript
     <env-entry-name>swivelHome</env-entry-name>
     <env-entry-type>java.lang.String</env-entry-type>
     <env-entry-value></env-entry-value>
    </env-entry>
 </web-app>
```

change the line <env-entry-value></env-entry-value> to reflect the required path

Example 1:

```
   <env-entry-value>c:\Users\gfield\swivel</env-entry-value>
```

Example 2:

```
  <env-entry-value>c:\ProgramData\swivel</env-entry-value>
```

624.2.4 Appliance custom transient data store considerations

Ensure that the custom Transient data store is contained within an area that is backed up.

624.3 Transient Data Storage Custom Path system Environment Variable

Another option is to define a system variable for the transient data storage path. To use a different path:

Create an environment variable called SWIVEL_HOME and assign a path to it.

In Linux based systems for example:

```
 export SWIVEL_HOME="/home/swivel"
```

In Windows 7: ? Click Start, right-click Computer, and select Properties. Select Advanced System Settings. You might need to confirm a UAC prompt. Then, click the Environment Variables button. ? Under System Variables click ?New? ? Enter SWIVEL_HOME as the variable name then the desired path for the value

Note that the new location for these files can be seen near the bottom of the Swivel Administration Console Status page with the heading ?Data Storage Root?.

Note also to ensure that any processes external to PINsafe, for example backup processes, point to the new external locations.

624.4 Appliance Transient Data Storage

The Swivel patches should handle the Transient data storage for Swivel appliances.

If this needs to be altered from the pre Swivel version 3.9.1 to the new Transient storage location edit /etc/profile.d/swivel.sh and change

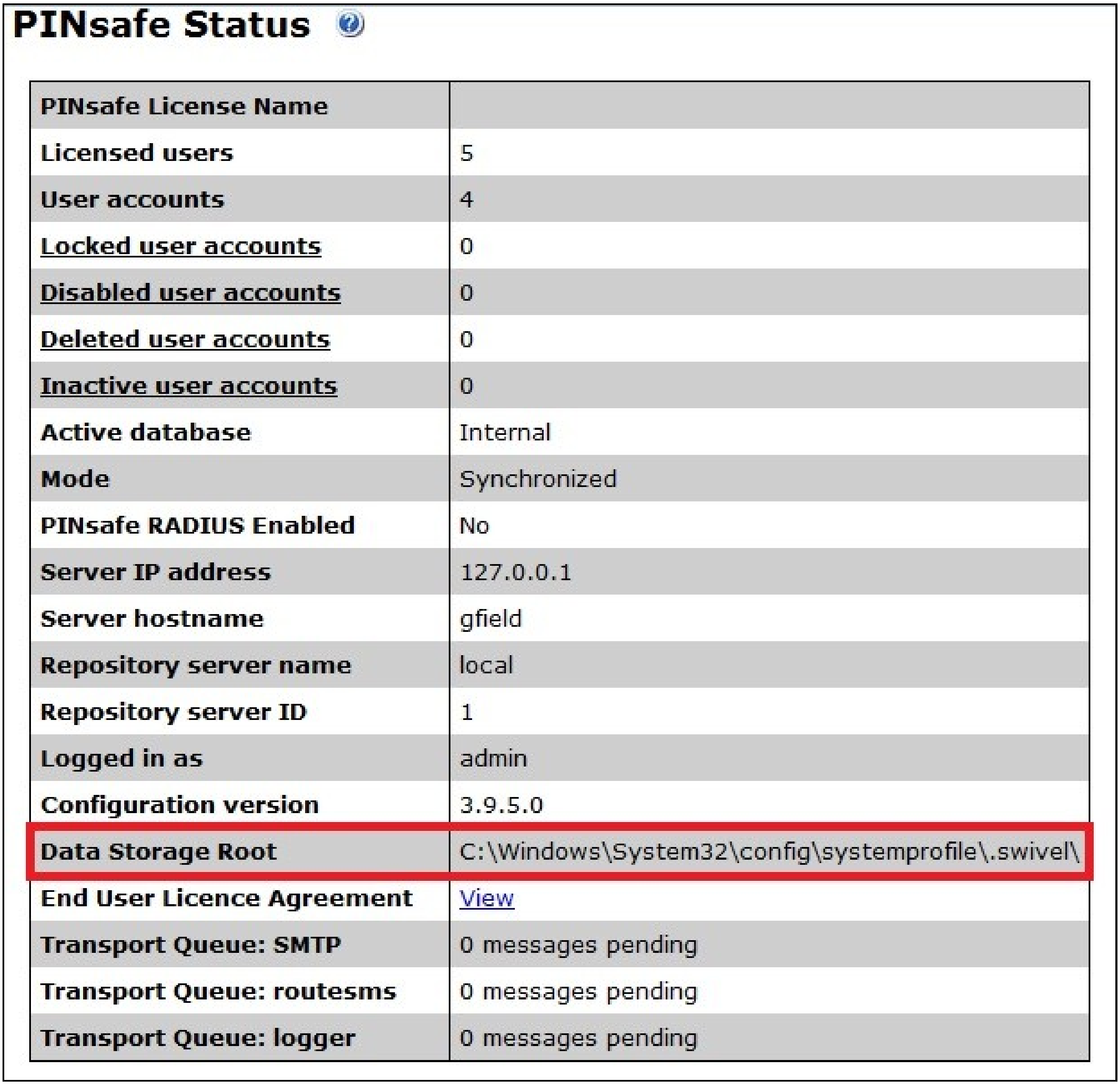
```
export SWIVEL_HOME=/usr/local/tomcat/webapps/pinsafe/WEB-INF
```

```
to
```

```
export SWIVEL_HOME=/home/swivel/.swivel
```

625 What is the Data Storage Path

The Data storage path is where the transient data is stored. It can be seen from the Status page on the swivel Administration console. If you are unsure where the transient data is stored then viewing this location will give its location.

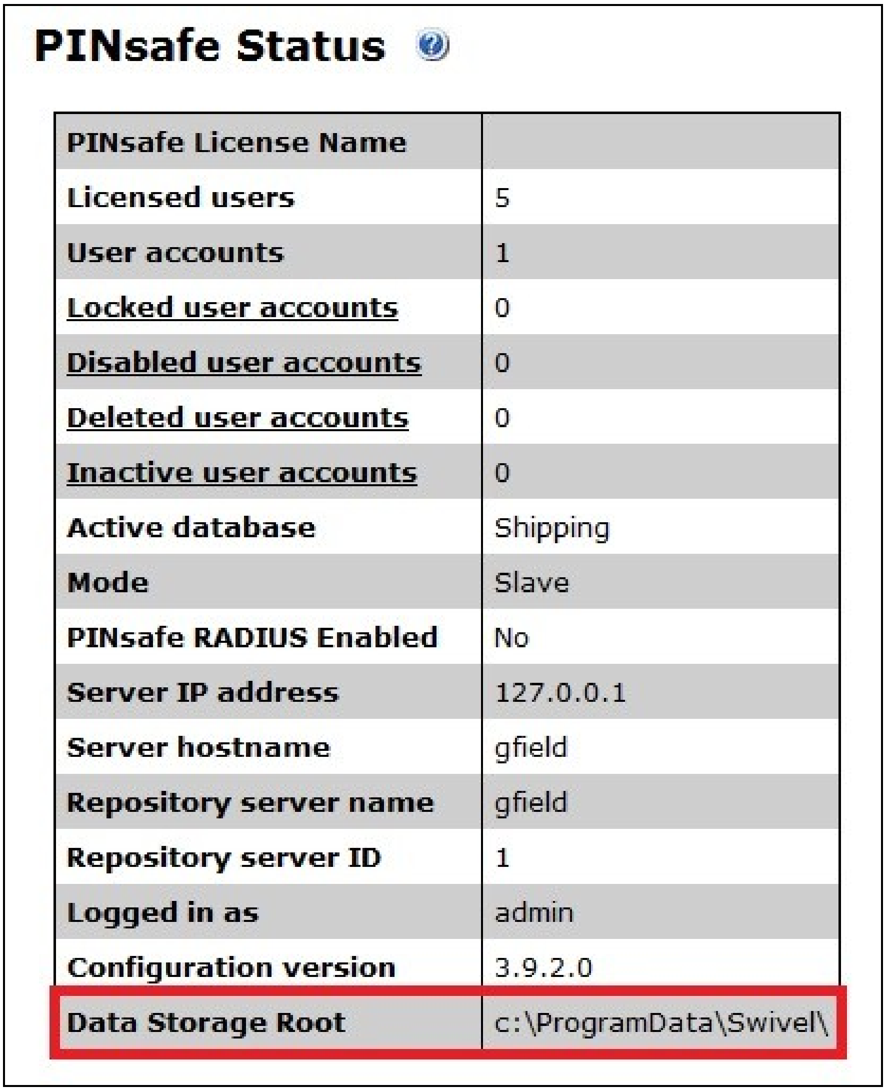


PINsafe Status

PINsafe License Name	
Licensed users	5
User accounts	4
Locked user accounts	0
Disabled user accounts	0
Deleted user accounts	0
Inactive user accounts	0
Active database	Internal
Mode	Synchronized
PINsafe RADIUS Enabled	No
Server IP address	127.0.0.1
Server hostname	gfield
Repository server name	local
Repository server ID	1
Logged in as	admin
Configuration version	3.9.5.0
Data Storage Root	C:\Windows\System32\config\systemprofile\.swivel\
End User Licence Agreement	View
Transport Queue: SMTP	0 messages pending
Transport Queue: routesms	0 messages pending
Transport Queue: logger	0 messages pending

626 Testing

The transient data storage location is listed under the Status page.



PINsafe Status

PINsafe License Name	
Licensed users	5
User accounts	1
Locked user accounts	0
Disabled user accounts	0
Deleted user accounts	0
Inactive user accounts	0
Active database	Shipping
Mode	Slave
PINsafe RADIUS Enabled	No
Server IP address	127.0.0.1
Server hostname	gfield
Repository server name	gfield
Repository server ID	1
Logged in as	admin
Configuration version	3.9.2.0
Data Storage Root	c:\ProgramData\Swivel\

627 Known Issues

628 Troubleshooting

If the transient data storage path is not correctly listed then the left hand menus may be absent.

628.1 Error Messages

Error occurred copying application data: java.io.IOException: Destination '/usr/share/tomcat5/.swivel/data' directory cannot be created

This error has been seen in the catalina.out log file for a CentOS install. Change the permissions on the CATALINA_HOME variable to allow Tomcat to create and write to the folder.

Data Storage Root:\Users\gfield\swivel\

log4j:ERROR No output stream or file set for the appender named [null].

Warning: java.io.FileNotFoundException: \\Users\gfield\swivel\conf\config.xml (The network path was not found)

Incorrectly specified transient data storage.

java.lang.NullPointerException

com.swiveltechnologies.pinsafe.server.filter.AdminConsoleFilter.doInitialization(AdminConsoleFilter.java:201)

com.swiveltechnologies.pinsafe.server.filter.AdminConsoleFilter.doFilter(AdminConsoleFilter.java:118)

filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:125)

This can be seen in the administration console login page where the transient data storage path is incorrect

629 Transport HTML

630 Overview

The Swivel Transports allow the use of HTML, to create rich formatting.

-

  New User HTML
-

  Quick Mobile Provisioning HTML

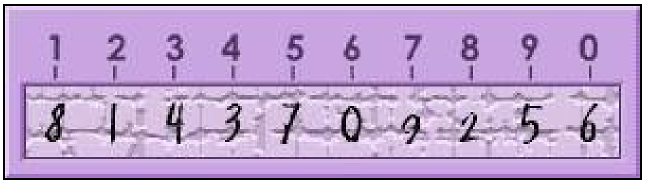
631 Sample Files

Sample Files.

632 TURing

633 Overview

TURing uses the PINsafe protocol to provide a One Time Code for authentication. TURing is often used as a stronger authentication method over a static password. Each image is unique for that session. If the user cannot read the image then they can request a new one. The length of time that the TURing is valid for is configurable, with a default of two minutes. For other methods of authentication see Authentication Methods.



634 Viewing the TURing image

The TURing image may be presented to the user in the following ways:

- Automatically after entering username with a login
- Generated by a button at the login page
- Taskbar utility

635 Configuration

See Single Channel How To Guide

636 Customisation

See Single Channel Customisation How to Guide

637 Security of TURing

The Turing authentication offers stronger authentication than a username and password since it introduces a One Time Code. However to increase security it should be used in combination with a static password.

638 Two Factor Authentication

639 Overview

Single Factor authentication consists of one of the below, Two Factor Authentication (2FA), sometimes also called Multi Factor Authentication, consists of two of the below:

- Something you know (e.g. PIN, Password)
- Something you have (e.g. Mobile Phone, Hardware Token)
- Something you are (e.g. Fingerprint, retina scan)

Two or Multi Factor authentication cannot consist of two of the same type, for example PIN and Password.

640 Further Information

See Transports How To Guide

641 Upgrade

642 Upgrade Overview for Swivel virtual or hardware Appliances

Install Type	virtual or hardware Appliance Type	Current appliance version	Current Swivel version	Appliance upgrade required before Swivel upgrade	Swivel upgrade
Hardware or VM Appliance	Standalone, Active/Active, DR	2.0.15 onwards	3.9.1 onwards	No	Swivel Patch?
Hardware or VM Appliance	Standalone, Active/Active, DR	2.0.14	3.9.1 onwards	Yes?	Swivel Patch?
Hardware or VM Appliance	Standalone, Active/Active, DR	2.0.14	3.8, 3.9.0	Yes?	Swivel Patch?
Hardware or VM Appliance	Standalone, Active/Active, DR	2.0.9a-2.013	3.2-3.9	Yes?	Swivel Patch?
Hardware or VM Appliance	Standalone, Active/Active, DR	2.0.8-2.09	3.2-3.9	Upgrade to 2.0.12? then apply Appliance Patch?	Swivel Patch?
Hardware or VM Appliance	Active/Passive	2.0.14 onwards	3.8 onwards	Yes?	Swivel Patch?
Hardware or VM Appliance	Active/Passive	2.0.8-2.12	3.2-3.9	Contact Swivel support	Contact Swivel support

643 Upgrade Overview for Swivel Software Only installs

Please Note - Swivel is NOT compatible with Java Version 8.

Install Type	Current Swivel version	Swivel upgrade
Software Only	3.2 to latest	Swivel Software upgrade
Software Only	3.1	Upgrade to 3.2, see Swivel Software upgrade

644 Help

What is my current Swivel version and Appliance version and Type?

645 Upgrading from Swivel 3-9 and Earlier on Microsoft Windows

646 Overview

This document covers upgrading Swivel on Microsoft Windows and supplements the article Upgrade PINsafe which should be used with this article. For Swivel appliance upgrades see the relevant patch files.

647 Prerequisites

- Existing Swivel installation version 3.9.4900 or earlier on Microsoft Windows Server 2000-2012, Windows XP, Windows Vista, Windows 7 or Windows 8 (including 8.1)
- Latest Swivel software to be installed
- Latest Swivel backup (requires the Tomcat service to be stopped if the internal DB is used) See Backup PINsafe on a Software Only Install
- To upgrade past Swivel 3.8 or later, you need Java 1.6.
- Swivel is compatible with versions of Tomcat versions 5.5 to 7.

If an external database such as MySQL or MSSQL is used make a backup of the database, since it may be modified if it was upgraded and you may need to go back to the previous version database state should something go wrong.

647.1 Upgrading from versions 3.2 to 3.9

647.1.1 Copy data

- Stop the Apache Tomcat service;
- It is highly recommended that you take a copy of the entire <path to Tomcat>\webapps\pinsafe\WEB-INF\ folder. DO NOT copy the files within the Tomcat folder, as this might cause multiple instances of Swivel to run. Make sure the backup is outside the Tomcat root folder, and preferably on a different computer altogether for safety.

Specifically the files you will need are:

<path to Tomcat>\webapps\pinsafe\WEB-INF\conf\config.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\conf\ranges.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\conf\config.properties <path to Tomcat>\webapps\pinsafe\WEB-INF\data\repository.xml

- If using the database "Internal" you will need:

<path to Tomcat>\webapps\pinsafe\WEB-INF\db

- If using an external database such as MySQL or MSSQL or Oracle, ensure you take a complete backup of the database
- If you have any custom transport classes, note that classes from 3.5 or earlier are not compatible with 3.6 or 3.7. Check with Swivel Secure if there is an upgrade available. When upgrading from 3.6 to 3.7, back up any custom transports as follows:

<path to Tomcat>\webapps\pinsafe\WEB-INF\classes\com\swiveltechnologies\pinsafe\server\transport

- If the Internal, or MySQL DB is not being used, backup the DB driver file you are using from <path to Tomcat>\webapps\pinsafe\WEB-INF\lib

647.1.2 Remove the old instance of Swivel

(This is only necessary if you are upgrading on the same server. Ensure your backup has been made).

- Ensure that the Tomcat service is started.
- Delete the current pinsafe.war in <path to Tomcat>\webapps
- Wait for the pinsafe folder to disappear. If the folder still remains after 30 seconds, you may need to delete it manually, as follows:
- If the pinsafe folder has not completely gone, stop Tomcat, delete the folder and then restart Tomcat.

647.1.3 Install a new instance of Swivel

Note: If moving to a new Microsoft Windows server, carry out the following install steps on the new server.

- Ensure that the Tomcat service is started.
- Copy the latest pinsafe.war file into the webapps folder and wait for the pinsafe folder to deploy;
- Once the new Swivel instance has deployed (the pinsafe folder has been created within webapps), verify that the Swivel service can be connected to and displays the new PINsafe version, from the local host use:

http://127.0.0.1:8080/pinsafe

If you have changed the Tomcat connector settings, use https and/or the modified port as appropriate.

- Login to Swivel admin (the DB is shipping) using the default credentials
- Check the location of the Data Storage Root folder from the Status screen.
- Stop Tomcat
- From the earlier backup, copy the conf, data and db directories to the Data Storage Root location, as previously written down

<path to Tomcat backup>\webapps\pinsafe\WEB-INF>

- Restore any custom classes or database libraries previously backed up.
- Start Tomcat, Swivel will startup and begin to upgrade the database configured in the config.xml

647.2 Testing

Verify that the Swivel service can be connected to, from the local host use:

http://127.0.0.1:8080/pinsafe

Verify that the new version is listed.

647.3 Known Issues

647.4 Troubleshooting

Transports absent after upgrade

648 Upgrading from Swivel 3-9-1 on Microsoft Windows

649 Overview

This document covers upgrading Swivel on Microsoft Windows and supplements the article Upgrade PINsafe which should be used with this article. For Swivel appliance upgrades see the relevant patch files. For a new Windows installation, see PINsafe Windows Installation.

650 Prerequisites

- Existing Swivel installation version 3.9.1.4908 or later on Microsoft Windows Server 2000-2012, Windows XP, Windows Vista, Windows 7 or Windows 8 (including 8.1)
- Latest Swivel software to be installed.
- Latest Swivel backup (requires the Tomcat service to be stopped if the internal Db is used) See Backup PINsafe on a Software Only Install
- To upgrade past Swivel 3.8 or later, you need Java 1.6.
- Swivel 3.8 is compatible with versions of Tomcat versions 5.5 to 7.

If an external database such as MySQL or MSSQL is used make a backup of the database, since it may be modified if it was upgraded and you may need to go back to the previous version database state should something go wrong.

650.1 Upgrading from versions 3.9.1 onwards to latest version

650.1.1 Copy data

- Log into the Swivel admin console and note the current setting for *Data Storage Root*.
- Stop the Apache Tomcat service
- It is highly recommended that you take a copy of the entire <path to Tomcat>\webapps\pinsafe\ folder. DO NOT copy the files within the Tomcat folder, as this might cause multiple instances of Swivel to run. Make sure the backup is outside the Tomcat root folder, and preferably on a different computer altogether for safety.
- If you have any custom classes not part of the original installation, check with Swivel support whether the latest version includes the customisation. If not, you will need to take copies of the custom classes to restore later on. You will also need to check with Swivel support if your custom classes are still compatible with the latest version.
- Take a backup of the Data Storage Root folder you noted earlier.
- If using an external database such as MySQL or MSSQL or Oracle, ensure you take a complete backup of the database
- If the Internal, or MySQL DB is not being used, backup the DB driver file you are using from <path to Tomcat>\webapps\pinsafe\WEB-INF\lib

650.1.2 Remove the old instance of Swivel

(This is only necessary if you are upgrading on the same server. Ensure your backup has been made).

- Ensure that the Tomcat service is started.
- Delete the current pinsafe.war in <path to Tomcat>\webapps
- Wait for the pinsafe folder to disappear. If the folder still remains after 30 seconds, you may need to delete it manually, as follows:
- If the pinsafe folder has not completely gone, stop Tomcat, delete the folder and then restart Tomcat.

650.1.3 Install a new instance of Swivel

Note: If moving to a new Microsoft Windows server, carry out the following install steps on the new server.

- Ensure that the Tomcat service is started.
- Copy the latest pinsafe.war file into the webapps folder and wait for the pinsafe folder to deploy;
- Once the new Swivel instance has deployed (the pinsafe folder has been created within webapps), verify that the Swivel service can be connected to and displays the new PINsafe version, from the local host use:

http://127.0.0.1:8080/pinsafe

If you have changed the Tomcat connector settings, use https and/or the modified port as appropriate.

- If you are upgrading in place, your existing configuration should still be in place, and you can log in using existing administrator credentials.
- If you are upgrading to a new server:
- ♦ Login to Swivel admin (the DB is shipping) using the default credentials
- ♦ Check the location of the configuration files from the status screen (write down the location)
- ♦ Stop Tomcat
- ♦ From the earlier backup, copy the conf, data and db directories to the new configuration location, as previously written down
- ♦ Start Tomcat, Swivel will startup and begin to upgrade the database configured in the config.xml

650.2 Testing

Verify that the Swivel service can be connected to, from the local host use:

http://127.0.0.1:8080/pinsafe

Verify that the new version is listed.

650.3 Known Issues

650.4 Troubleshooting

Transports absent after upgrade

651 Upgrading PINsafe on Microsoft Windows

652 Overview

This document covers upgrading Swivel on Microsoft Windows and supplements the article Upgrade PINsafe which should be used with this article. For Swivel appliance upgrades see the relevant patch files.

653 Prerequisites

- Existing Swivel installation on Microsoft Windows, 2000, 2003, 2008, XP, Vista, Win7
- Latest Swivel software
- Latest Swivel backup (requires the Tomcat service to be stopped if the internal Db is used) See Backup PINsafe on a Software Only Install
- To upgrade to Swivel 3.8 or later, you need Java 1.6. It is recommended that you update to the latest version of Java anyway.
- Swivel 3.8 is compatible with versions of Tomcat versions 5.5 to 7.

If an external database such as MySQL or MSSQL is used make a backup of the database, since it may be modified if it was upgraded and you may need to go back to the previous version database state should something go wrong.

654 Moving Swivel to another server

The steps detailed here can be used to move Swivel to another Microsoft Windows Server. As an overview the steps required are:

- Make a copy of the Swivel data;
- Install new instance of Swivel, on a new server;
- Copy configuration and data files, to new Swivel server.

See below specific information on each of these steps.

655 Upgrading Swivel on the same server

The steps detailed here can be used to upgrade an existing Swivel instance on the same Microsoft Windows Server. As an overview the steps required are:

- Make a copy/backup of the Swivel data;
- Remove the old instance of PINsafe;
- Install new instance of PINsafe;
- Copy configuration and data files, to new Swivel instance.

See below specific information on each of these steps.

656 Microsoft Windows Swivel Upgrade steps

656.1 Upgrade Java if required

Check what version of Java you are running. If you are on 1.5, upgrade to 1.6 or 7 - you should be able to download the latest version from the Oracle website: http://www.oracle.com/technetwork/java/javase/downloads/index.html.

If you upgrade Java, make sure that Tomcat is reconfigured to use the new version. The simplest way to do this is through the Tomcat Control Panel. If this is not already running, select Monitor Tomcat from the start menu. You may need to right-click and select Run As Administrator. Right-click on the taskbar icon and select Configure. Select the Java tab, and make sure that Use default is checked.

656.2 Upgrading from Versions of Swivel Earlier Than 3.9.1

Follow this procedure if you are upgrading from a version of Swivel PINsafe numbered 3.9.4900 or earlier to any subsequent version.

Upgrading_from_Swivel_3-9_and_Earlier_on_Microsoft_Windows

656.3 Upgrading from Versions of Swivel From 3.9.1.4908 Onwards

Follow this procedure if you are upgrading from a version of PINsafe numbered 3.9.1.4908 or later to any subsequent version.

Upgrading from Swivel 3-9-1 on Microsoft Windows

656.4 Upgrading versions 3.2 to 3.9

Use this section if you are upgrading **TO** a version of Swivel PINsafe numbered 3.9.4900 or earlier from a still earlier version. This section is provided for reference only - you are generally advised to upgrade to the latest version.

Upgrading Swivel 3-2 to 3-9 on Microsoft_Windows

656.5 Testing

Verify that the PINsafe server can be connected to, from the local host use:

http://127.0.0.1:8080/pinsafe

Verify that the new version is listed.

656.6 Known Issues

656.7 Troubleshooting

Transports absent after upgrade

657 Upgrading Swivel 3-2 to 3-9 on Microsoft Windows

658 Overview

This document covers upgrading Swivel on Microsoft Windows and supplements the article Upgrade PINsafe which should be used with this article. For Swivel appliance upgrades see the relevant patch files.

659 Prerequisites

- Existing Swivel installation on Microsoft Windows, 2000, 2003, 2008, XP, Vista, Win7
- Latest Swivel software
- Latest Swivel backup (requires the Tomcat service to be stopped if the internal Db is used) See Backup PINsafe on a Software Only Install
- To upgrade to Swivel 3.8 or later, you need Java 1.6. It is recommended that you update to the latest version of Java anyway.
- Swivel 3.8 is compatible with versions of Tomcat versions 5.5 to 7.

If an external database such as MySQL or MSSQL is used make a backup of the database, since it may be modified if it was upgraded and you may need to go back to the previous version database state should something go wrong.

659.1 Upgrading versions 3.2 to 3.9

659.1.1 Copy data (3.2-3.9)

For upgrading from versions 3.9.1 and higher (excluding 3.9) the, the pinsafe.war file can be copied into the webapps folder as part of the upgrade, but make a copy of custom transports and the <database name>.jar file in WEB-INF/lib before upgrading and copy back in as below. Note from Swivel 3.9.1 the location of the Transient Data Storage.

- Stop the Apache Tomcat service;
- It is highly recommended that you take a copy of the entire <path to Tomcat>\webapps\pinsafe\WEB-INF\ folder. DO NOT copy the files within the Tomcat folder, as this might cause multiple instances of PINsafe to run. Make sure the backup is outside the Tomcat root folder, and preferably on a different computer altogether for safety.

Specifically the files you will need are:

<path to Tomcat>\webapps\pinsafe\WEB-INF\conf\config.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\conf\ranges.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\conf\config.properties <path to Tomcat>\webapps\pinsafe\WEB-INF\data\repository.xml

- If using the database "Internal" you will need:

<path to Tomcat>\webapps\pinsafe\WEB-INF\db

- If using an external database such as MySQL or MSSQL or Oracle, ensure you take a complete backup of the database
- If you have any custom transport classes, note that classes from 3.5 or earlier are not compatible with 3.6 or 3.7. Check with Swivel Secure if there is an upgrade available. When upgrading from 3.6 to 3.7, back up any custom transports as follows:

<path to Tomcat>\webapps\pinsafe\WEB-INF\classes\com\swiveltechnologies\pinsafe\server\transport

- If the Internal, or MySQL DB is not being used, backup the DB driver file you are using from <path to Tomcat>\webapps\pinsafe\WEB-INF\lib

659.1.2 Remove the old instance of PINsafe (3.2-3.9)

(This is only necessary if you are upgrading on the same server. Ensure your backup has been made).

- Ensure that the Tomcat service is started.
- Delete the current pinsafe.war in <path to Tomcat>\webapps
- Wait for the pinsafe folder to disappear. If the folder still remains after 30 seconds, you may need to delete it manually, as follows:
- If the pinsafe folder has not completely gone, stop Tomcat, delete the folder and then restart Tomcat.

659.1.3 Install a new instance of PINsafe (3.2-3.9)

Note: If moving to a new Microsoft Windows server, carry out the following install steps on the new server.

- Ensure that the Tomcat service is started.
- Copy the latest pinsafe.war file into the webapps folder and wait for the pinsafe folder to deploy;
- Once the new Swivel instance has deployed (the pinsafe folder has been created within webapps), verify that the PINsafe server can be connected to and displays the new PINsafe version, from the local host use:

http://127.0.0.1:8080/pinsafe

- Stop Tomcat

659.1.4 Copy configuration and data files (3.2-3.9)

- Copy the previously made copies of the following files and folders to the new instance of Swivel.

Note: If moving to a new Microsoft Windows Server copy from the backup to location to the new server.

<path to Tomcat>\webapps\pinsafe\WEB-INF\conf\config.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\conf\ranges.xml <path to Tomcat>\webapps\pinsafe\WEB-INF\data\repository.xml

- If using the database "Internal" you will need:

<path to Tomcat>\webapps\pinsafe\WEB-INF\db

- Start Tomcat, pinsafe will startup and begin to upgrade the database configured in the config.xml

659.2 Testing

Verify that the PINsafe server can be connected to, from the local host use:

http://127.0.0.1:8080/pinsafe

Verify that the new version is listed.

659.3 Known Issues

659.4 Troubleshooting

Transports absent after upgrade

660 User Alerts

661 User Alerts

User Alerts are global settings which determine what messages users are sent through the users **Alert** transport. The alert transport group is a transport method that can be configured for a group of users, see also Transport Configuration.

662 Prerequisites

Swivel 3.x

663 User Alert Options

PIN expiry warning: Options Yes/No, default Yes, users are notified when their PIN will expire.

PIN change required: Options Yes/No, default Yes, users are notified when a PIN change is required.

PIN changed: Options Yes/No, default Yes, users are notified when their PIN has changed.

Account locked: Options Yes/No, default Yes, users are notified when their account has been locked.

Device key allocated: Options Yes/No, default Yes, users are notified when a PositiveID device key has been allocated.

Account inactive: Options Yes/No, default Yes, users are notified when their account has been locked due to inactivity.

Account inactive warning (days): Options time in days, default 0, users are notified the given number of days in advance of their account being locked due to inactivity.

No transport is error: Options Yes/No, default No, this raises the logging error level when a user has no transport defined so that administrators can receive them as higher priority.

Account unlocked: Options Yes/No, default Yes, users are notified when their account has been unlocked.

664 Testing

665 Known Issues

666 Troubleshooting

667 User Attributes How To

668 Overview

This document summarises the use of additional user attributes, available in Swivel since version 3.9.1.

User attributes have been used since version 3.4 to define destinations for transports. However, this facility has now been extended to allow the use of alternative attributes for authentication (from version 3.9.1) and searching (since 3.9.2). For each attribute field, Swivel will import one entry, if multiple entries are used, only the first is imported. To import multiple attributes, multiple Swivel attributes can be created.

669 Prerequisites

Swivel 3.10.4 for initial, synchronised or local attributes

Swivel 3.9.2 or higher for attribute search

Swivel 3.9.1 or higher

670 User Attribute uses

User Attributes can be used for the following purposes:

- Transport destinations (e.g. email address, phone number)
- Alternative usernames for authentication (e.g. Active Directory userPrincipalName)
- User searching (e.g. by surname)
- User identification (e.g. surname, given name)
- Including in messages

670.1 User Attributes Synchronisation

By default the Attributes are taken from the users repository. From Swivel version 3.10.4 onwards, this can be changed so that the value may be imported initially or from a local value:

Synchronised: Read its value from the repository and update

Initialised: Only read the value from the repository when the account is created

Local: Never read the value from the repository (e.g. it will be set via an API call)

670.2 Importing Additional Attributes From Repositories

Important: if you make any changes to the attribute definitions, you must perform a User Sync before these attributes are available.

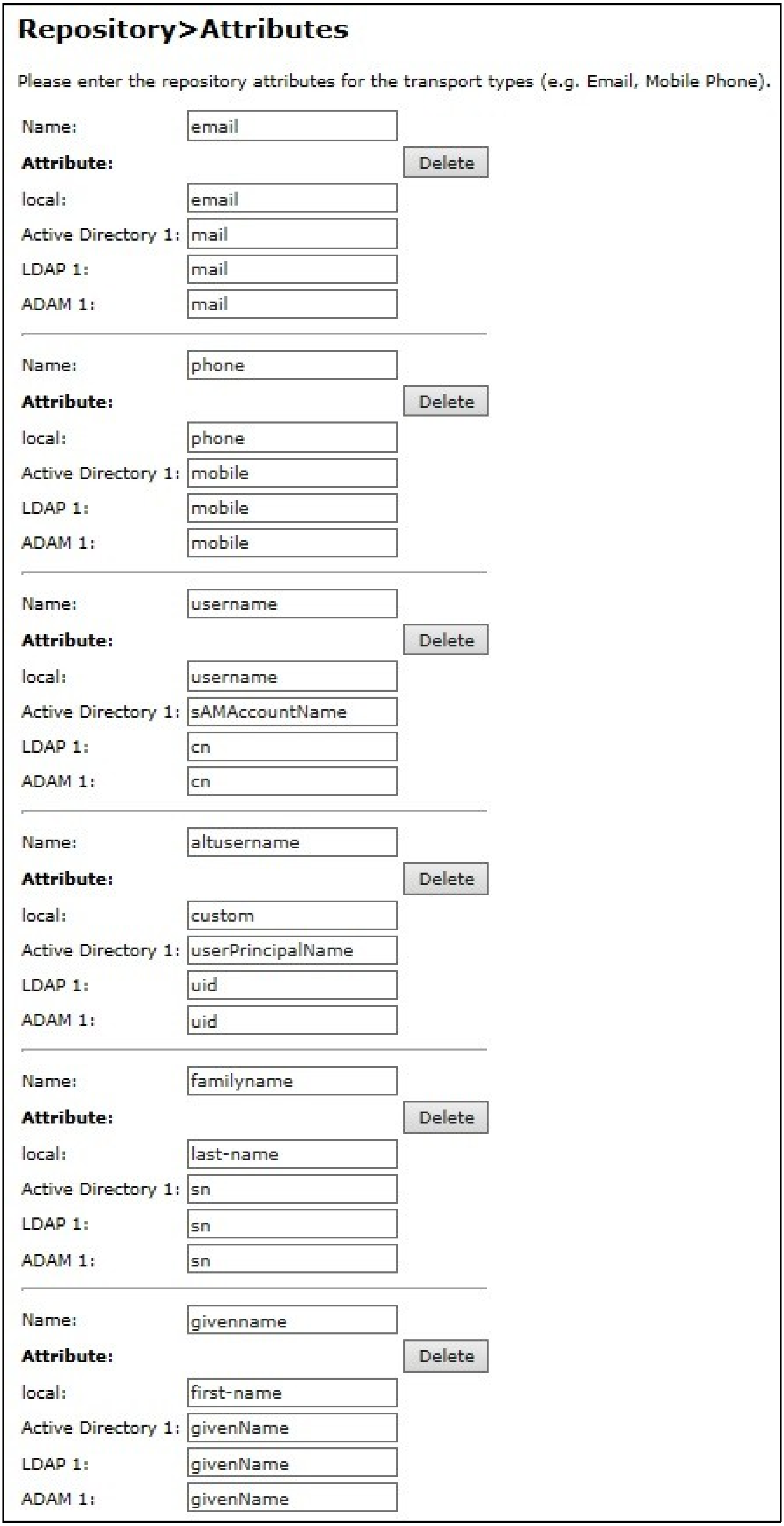
In order to make use of additional attributes, you need to define these attributes, and specify how they are imported from your repositories from the Repository -> Attributes menu. (For version 3.9.1 it is located under Transport -> Attributes menu).

Create a new attribute by entering a unique name for it in the Name field of the blank entry at the bottom of the page, and then for each Repository, enter the name of the attribute from that repository that should be imported.

Check the schema for your repository to determine what the correct attributes are. Most LDAP schemas provide at least the following attributes:

- **mail** - email address
- **mobile** - mobile telephone number
- **sn** - surname
- **givenName** - given (first, or christian) name

Additionally, to provide alternative usernames for authentication, Active Directory provides **userPrincipalName** and **sAMAccountName**. Most other LDAP implementations provide **uid** and **cn**. Note that it is not necessary to include the main username attribute as a user attribute, but there is no problem in doing so.



Repository>Attributes

Please enter the repository attributes for the transport types (e.g. Email, Mobile Phone).

Name: email

Attribute:

local: email

Active Directory 1: mail

LDAP 1: mail

ADAM 1: mail

Name: phone

Attribute:

local: phone

Active Directory 1: mobile

LDAP 1: mobile

ADAM 1: mobile

Name: username

Attribute:

local: username

Active Directory 1: sAMAccountName

LDAP 1: cn

ADAM 1: cn

Name: altusername

Attribute:

local: custom

Active Directory 1: userPrincipalName

LDAP 1: uid

ADAM 1: uid

Name: familyname

Attribute:

local: last-name

Active Directory 1: sn

LDAP 1: sn

ADAM 1: sn

Name: givenname

Attribute:

local: first-name

Active Directory 1: givenName

LDAP 1: givenName

ADAM 1: givenName

670.2.1 XML Repository Attributes

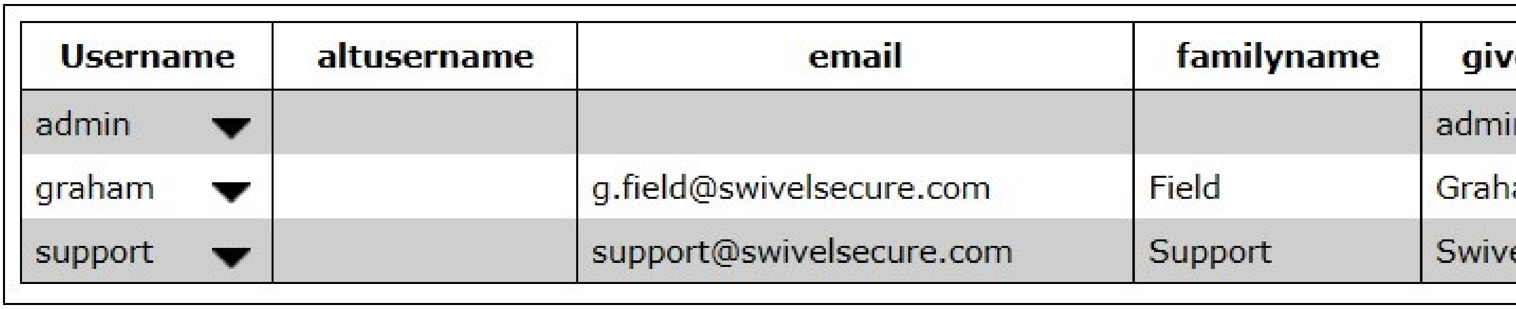
When using the built-in XML repository (or multiple repositories), the list of attribute names that you can use is given below:

Default Attributes

Attribute	**Local XML**	**LDAP**	**Active Directory**	**ADAM**
email	email	mail	mail	mail
phone	phone	phone	mobile	mobile
username	username	cn	sAMAccountName	cn
altusername	custom	uid	userPrincipalName	uid
familyname	last-name	sn	sn	sn
givenname	first-name	givenName	givenName	givenName

670.3 Viewing User Attributes

To view current user attributes, simply select the drop-down next to **View:** and select **Attributes**.



Username	altusername	email	familyname	giv
admin ▼				admi
graham ▼		g.field@swivelsecure.com	Field	Graha
support ▼		support@swivelsecure.com	Support	Swive

670.4 Authenticating Using Alternative Attributes

Authentication is configured per-Agent, or RADIUS NAS. New fields have been added to enable this feature, as follows:

- **Allow alternative usernames** - set to **Yes** to enable alternative usernames.
- **Alternative username attributes** - a list of permissible username attributes (see below).

Additionally, if you are using the **Check Password with repository** feature, the following enhancement is available:

- **Username attribute for repository** - specify the attribute to use as the repository username (see below).

When checking Swivel authentication, you can specify a number of attributes that can be used to identify the user to authenticate. List the names of the attributes as entered in the **Name** field of the Repository -> Attributes list, *NOT* the repository attribute name (if they are different). You can separate the individual names with commas, semi-colons or pipe (vertical bar) characters. *DO NOT* leave spaces before or after the separator, and *DO NOT* add a trailing separator. You do not have to include the primary username attribute in this list: Swivel will always check that anyway.

When you specify alternative attributes, Swivel will search for the entered username value first against the primary username. If there is no match for this, it will check against all permitted attributes. If this results in multiple matches, it will return the first match, but log a warning. So long as the matches all refer to the same user, this is not a problem, but you should take care when specifying alternative attributes for authentication that the values are unique over the entire database. So, for example, it is OK to have userPrincipalName and mail as authentication attributes, as typically they are unique, and if both attributes return the same value for a particular user, that doesn't matter, as the correct user is identified. However, it is not a good idea to use surname as an authentication attribute, as this is unlikely to be unique.

NOTE: currently it is not possible to create composite user attributes, as you can by adding a prefix or suffix to the primary username.

When checking the repository password, you can specify which attribute to send to the repository with the password. For example, suppose you normally enter sAMAccountName as the primary username, but when checking against Active Directory, you need to provide userPrincipalName. You can now manage this by specifying **userPrincipalName** as the **Username attribute for repository**. Then no matter what username is entered to authenticate to Swivel, the identified user's userPrincipalName attribute will be sent to Active Directory for authentication.

670.5 Session Requests

Session requests are Single Channel image requests such as the TURing or Dual Channel SMS requests for On Demand Authentication. Attributes can be defined for these on the Swivel Administration Console under:

Server/Single Channel

Server/Dual Channel

set the following:

Allow alternative usernames: Options: Yes/No, default No, set to Yes to allow alternative attributes.

Alternative username attributes: Enter an attribute name to use for sessions requests

670.6 Searching Using Alternative Attributes

To enable searching by attributes, the Username search on User Administration has been extended.

NOTE: If you are viewing an editable repository (e.g. an XML repository), make sure that the **Database** user set is selected in order to enable this feature.

Instead of a fixed Username search, there is now a drop-down containing all the user attributes. If you have included the username as an alternative attribute, this will appear twice, as Username is always the first entry. Simply select the attribute you want to search by, then enter the attribute value, or part-value, to search for.

670.7 Transport Destinations

This aspect of user attributes has been available since version 3.4. It refers to the ability to import transport destinations from the repository. By "Transport Destination", we mean typically email address or telephone number, depending on the nature of the transport.

To make a Transport active, you need to do 2 things:

- Select a group which uses that transport, either for security strings or alerts (or both).
- Select a user attribute to use as the destination.

In most cases, the transport attribute is pre-selected: for the SMTP transport, the "mail" attribute is chosen; for all other transports, "phone" is pre-selected, on the assumption that most transports are SMS gateways. However, if you have multiple phone numbers, or your phone number attribute is not called "mail", then you will need to select the appropriate attribute from the drop-down list for the appropriate transport on the Transport -> General page.

Be aware that you must run a User Sync after making any changes to the transport destination, even if that attribute has already been imported. The destination value for individual users is not automatically updated when the attribute changes.

670.8 Using Attributes in Messages

You can insert attribute values in alert messages sent to users, by inserting the placeholder %{attrname}, where attrname is the name of the attribute as defined under Repository -> Attributes. For example, if a user has a custom attribute "given_name" with the value "Tom", and the attribute "family_name" with the value "Smith", then the following message template:

```
Dear ${given_name} ${family_name}
```

Will result in the sent message:

```
Dear Tom Smith
```

671 Known Issues and Limitations

Swivel will import the first entry in each attribute only.

672 Troubleshooting

Ensure that the session request (single and/or dual channel) have multiple attributes enabled as well as the authentication (Agent or RADIUS).

673 User Portal

674 Overview

The user portal version 3 places all the self-service application in one place and allows the customer to decide what pages to make available to users and how those pages are to be used. This can replace the current changepin , resetpin and proxy applications.

The following applications are available.

- Change PIN
- Reset PIN (The ResetPIN needs to be enabled on the Swivel Administration console). See also ResetPIN How To Guide
- Provision a Mobile device
- Sync a Token

675 Prerequisites

For v4, see User Portal Administration Guide and User Portal User Guide:

Swivel v3.9.5 to v3.11.5.

Appliance v2.0.16 onwards.

QR Code Provision Provisioning 3.10.4 onwards.

Token See link for Token prerequisites.

Swivel appliance with user portal see Downloads.

676 Upgrading User Portal

The combined appliance patch gives the option to uninstall previous versions of the User Portal.

To manually remove it, backup the old user Portal, then with Tomcat running remove the /usr/local/tomcat/webapps2/userportal.war or whatever it has been called, this should remove the userportal folder. If using WinSCP refresh the folder to see if it has been removed.

677 User Portal Installation

If the User Portal is not installed on a Swivel appliance, it can be installed on an appliance running Swivel 3.9.1 onwards. WinSCP can be used to install this, see WinSCP How To Guide.

Copy the userportal.war file to /usr/local/tomcat/webapps2

678 User Portal Configuration

Config files are located in: /home/swivel/.swivel/user-portal/ (or .swiveluser-portal on some versions)

678.1 settings.properties

Communication settings for a local Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=127.0.0.1
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
imagessl=true
imageserver=YourSwivelURL.com
imagecontext=proxy
imageport=8443
```

Communication settings for a remote Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=RemoteSwivelIP or VIP
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8080
imagessl=true
imageserver=YourSwivelURL.com
imagecontext=proxy
imageport=8443
```

678.2 portalconfig.properties

Controls the behavious of changePIN. Restart Tomcat after making any changes.

```
#valid settings: directEntry turingEntry pinpadEntry
changepin.page=turingEntry
```

679 Language files

These are located in /usr/local/tomcat/webapps2/userportal/WEB-INF/classes

679.1 messages_en.properties

This file contains the text and language which may be customised

680 User Portal Menu options

The options available to portal users can be edited to remove menus that are not required. Edit the file /usr/local/apache-tomcat/webapps2/userportal/WEB-INF/view/template/leftpanel.jsp

To remove an item, add at the start '' example

The following removes the ChangePIN link

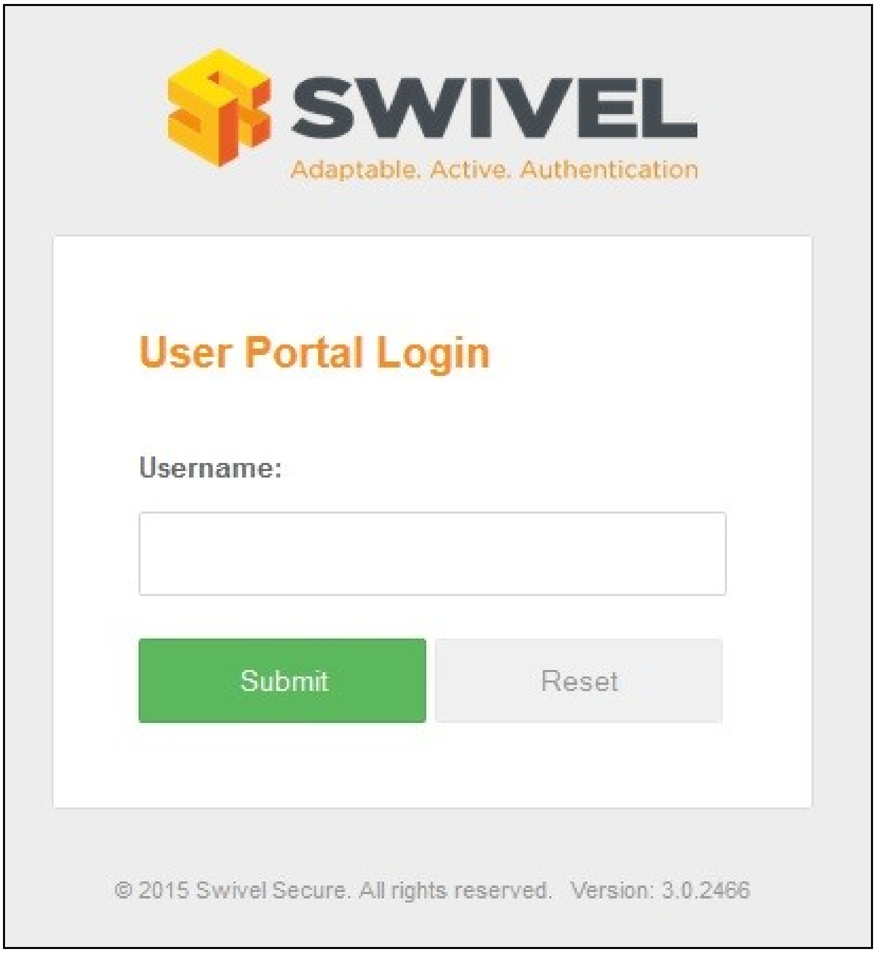
```
<li><a href="${mobileProvisioningUrl}"><spring:message code = "mobile_provisioning.title" /></a></li>
<li><a href="${selfResetUrl}" onclick="return confirmDialog(event);"><spring:message code = "reset.title" /></a></li>

<li><a href="${tokenManagementUrl}"><spring:message code = "tokenmanagement.title" /></a></li>
```

681 User Portal Usage

Navigate to the userportal page; https://IP:8443/userportal The userportal should be displayed.

681.1 User Portal Login

Here you can enter a user name and click [submit to access the User Portal.



SWIVEL

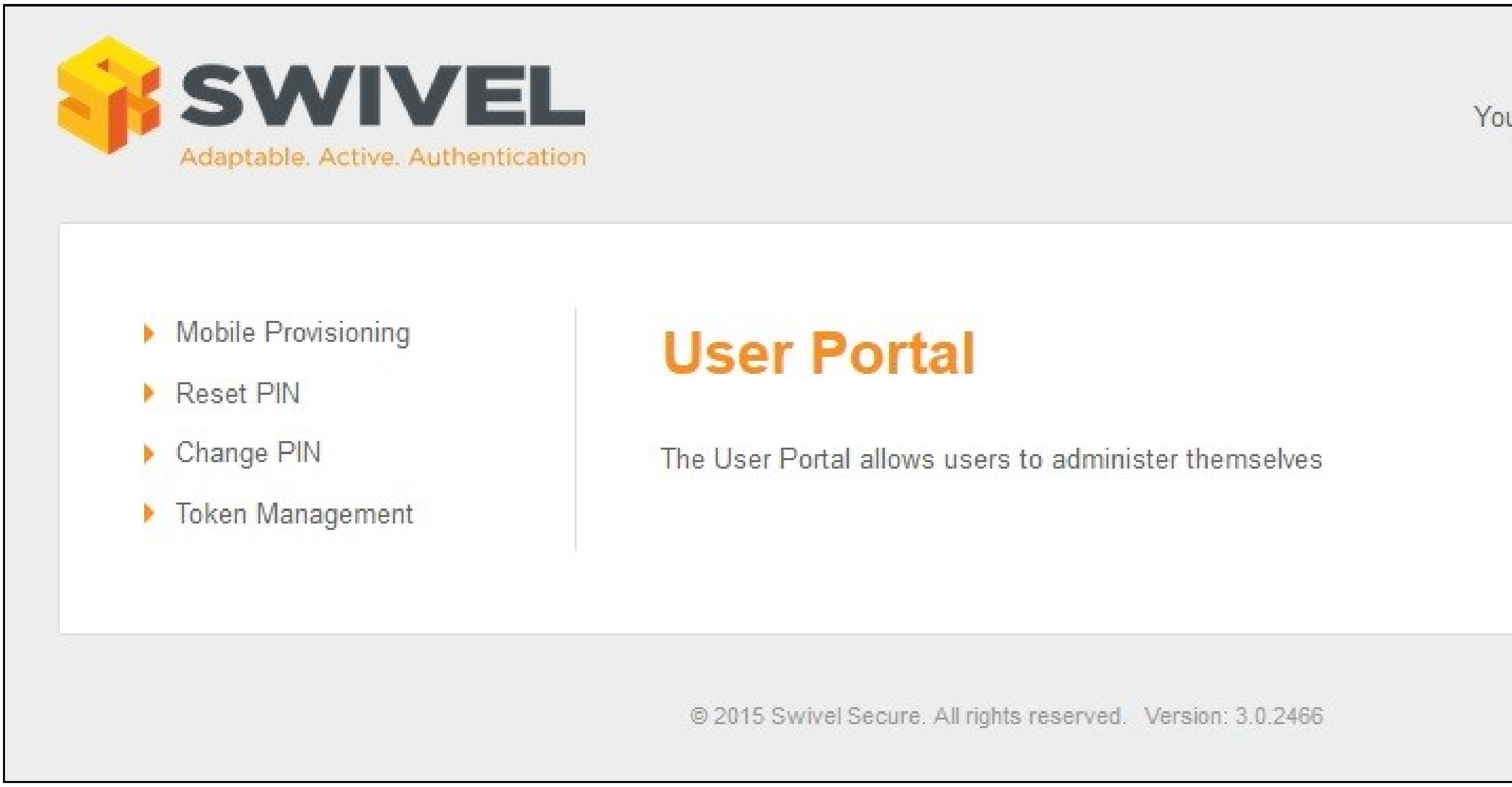
Adaptable. Active. Authentication

User Portal Login

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.2 User Portal Menu

The below screen will show once the username has been submitted.



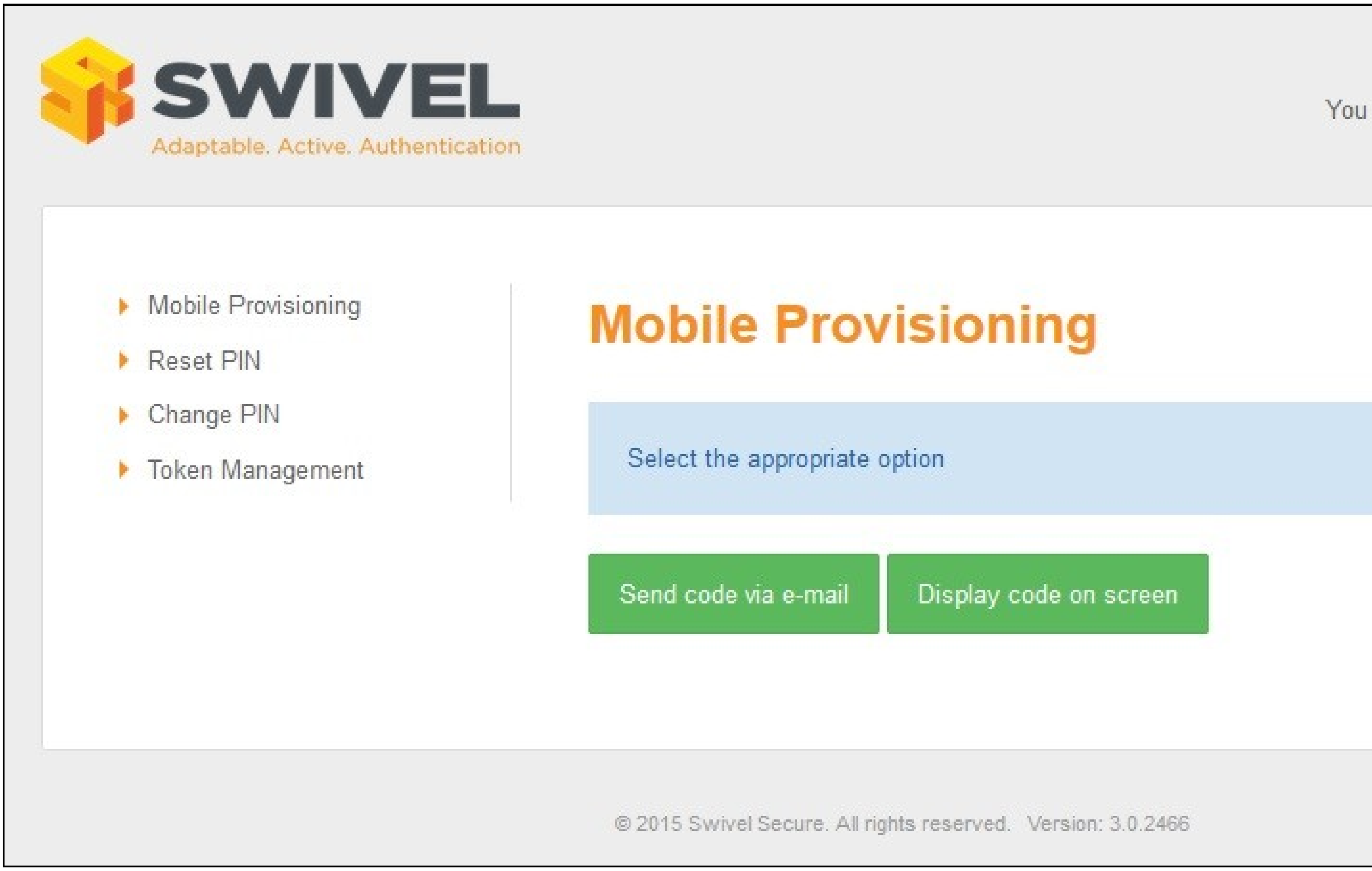
User Portal

The User Portal allows users to administer themselves

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.3 User Portal Mobile Provision

The Mobile provision option allows a message to be sent to the user or to use QR Code Provision.



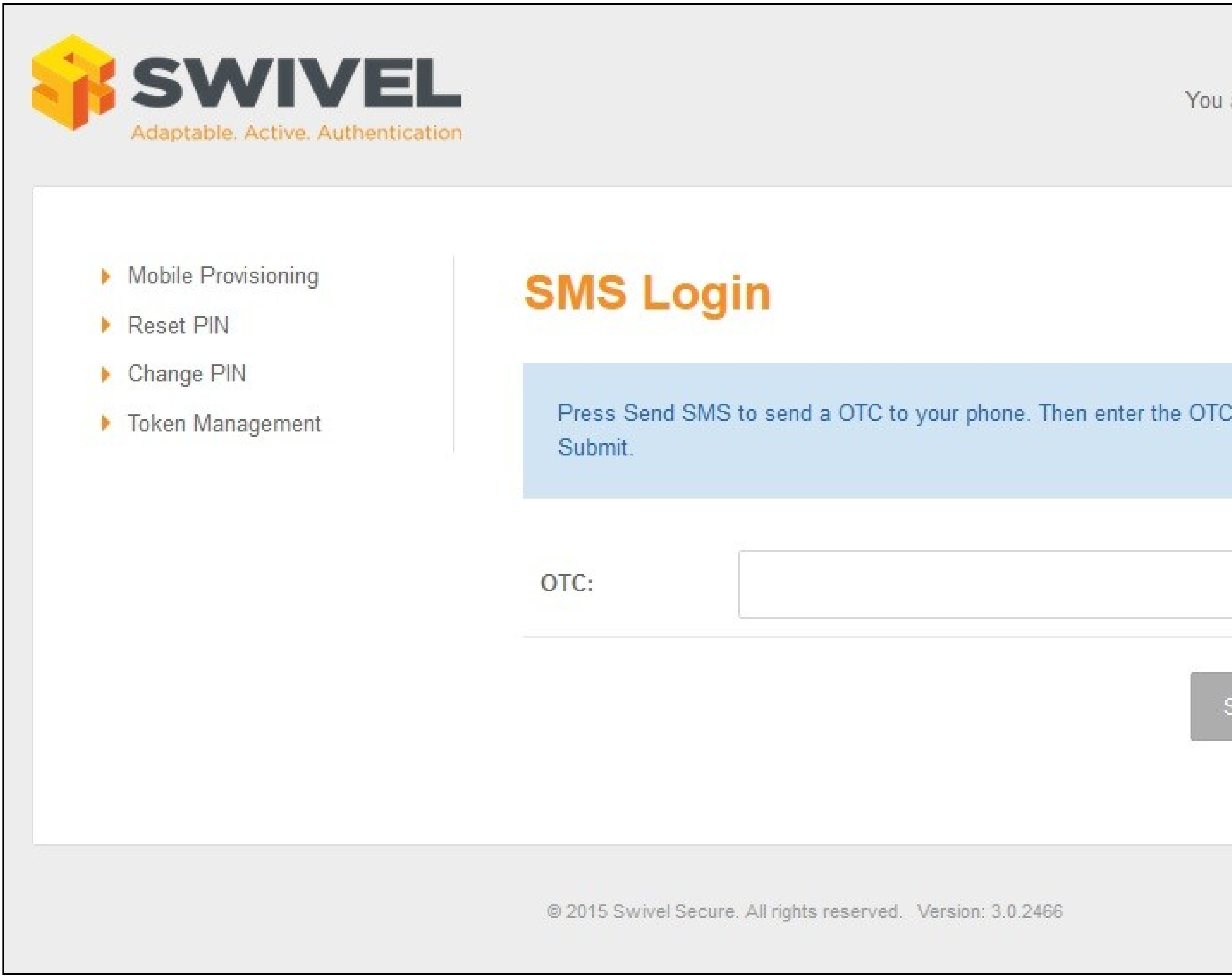
Mobile Provisioning

Select the appropriate option

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.4 User Portal Mobile Provision On Screen

To use the QR Code Provision the user needs to authenticate by entering an OTC, this screen allows the SMS to be sent to the user.



SMS Login

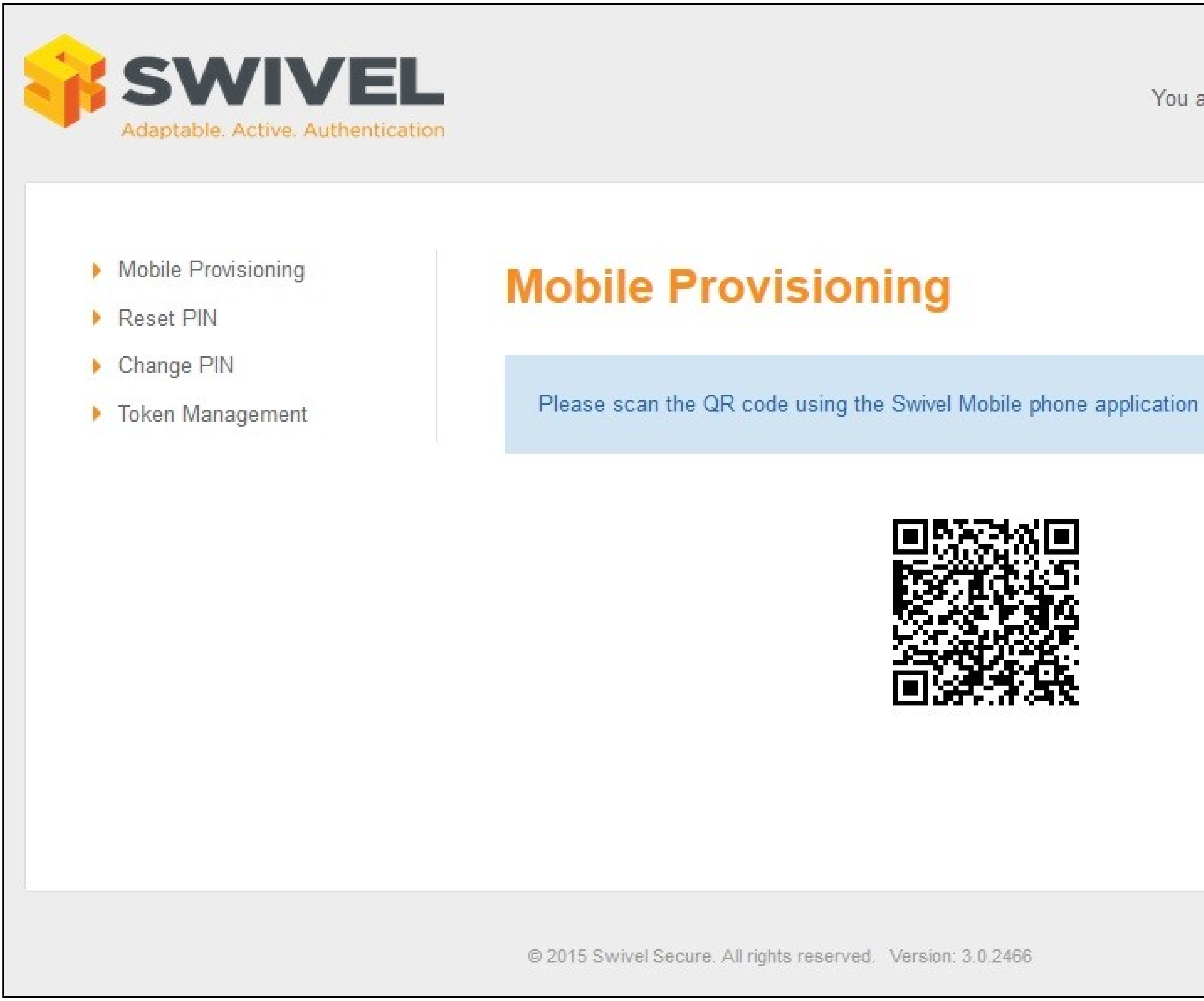
Press Send SMS to send a OTC to your phone. Then enter the OTC
Submit.

OTC:

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.5 User Portal Mobile Provision by QR Code

A valid OTC will display the QR Code Provision.



SWIVEL

Adaptable. Active. Authentication

You a

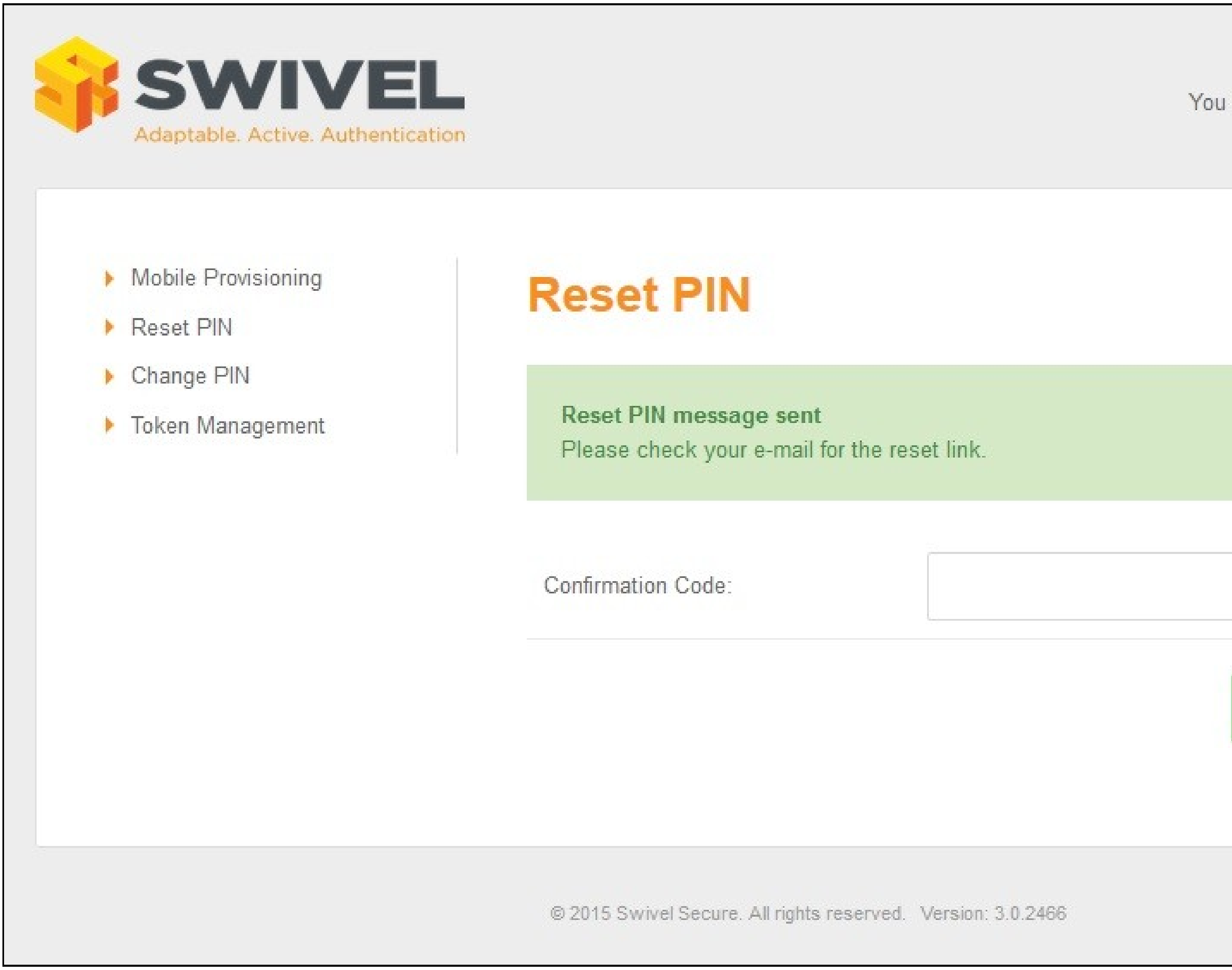
Mobile Provisioning

Please scan the QR code using the Swivel Mobile phone application

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.6 User Portal ResetPIN

ResetPIN allows a user to be sent a new PIN number. The user is sent a reset code to enter into the below page, which if correct when submitted will create a new PIN and send it to the user.



Reset PIN

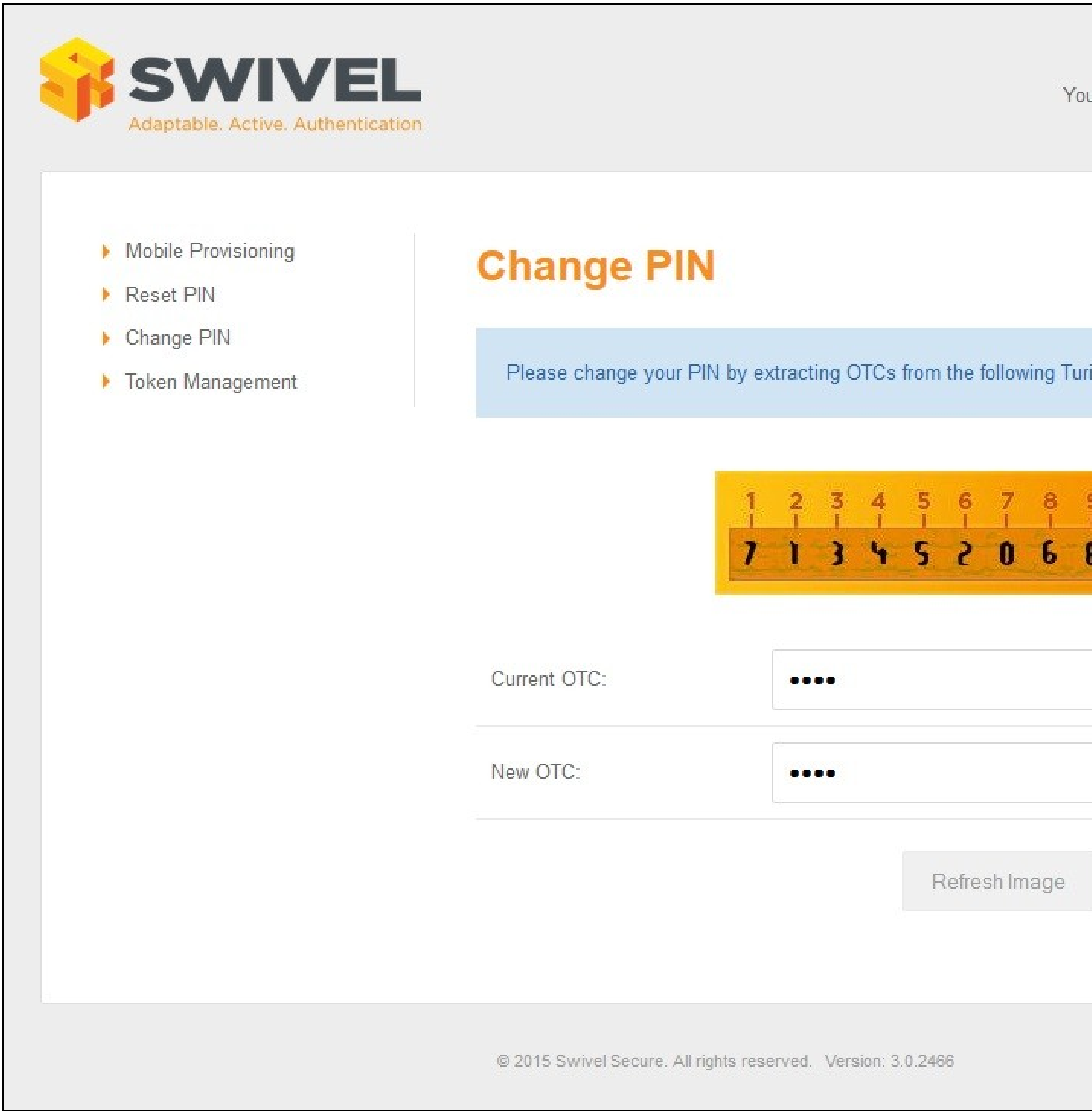
Reset PIN message sent
Please check your e-mail for the reset link.

Confirmation Code:

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.7 User Portal ChangePIN

ChangePIN allows a user to change their PIN number. Different options such as by using he TURing or Pinpad or direct entry of the PIN are available by modifying the configuration files above.



Change PIN

Please change your PIN by extracting OTCs from the following Turi

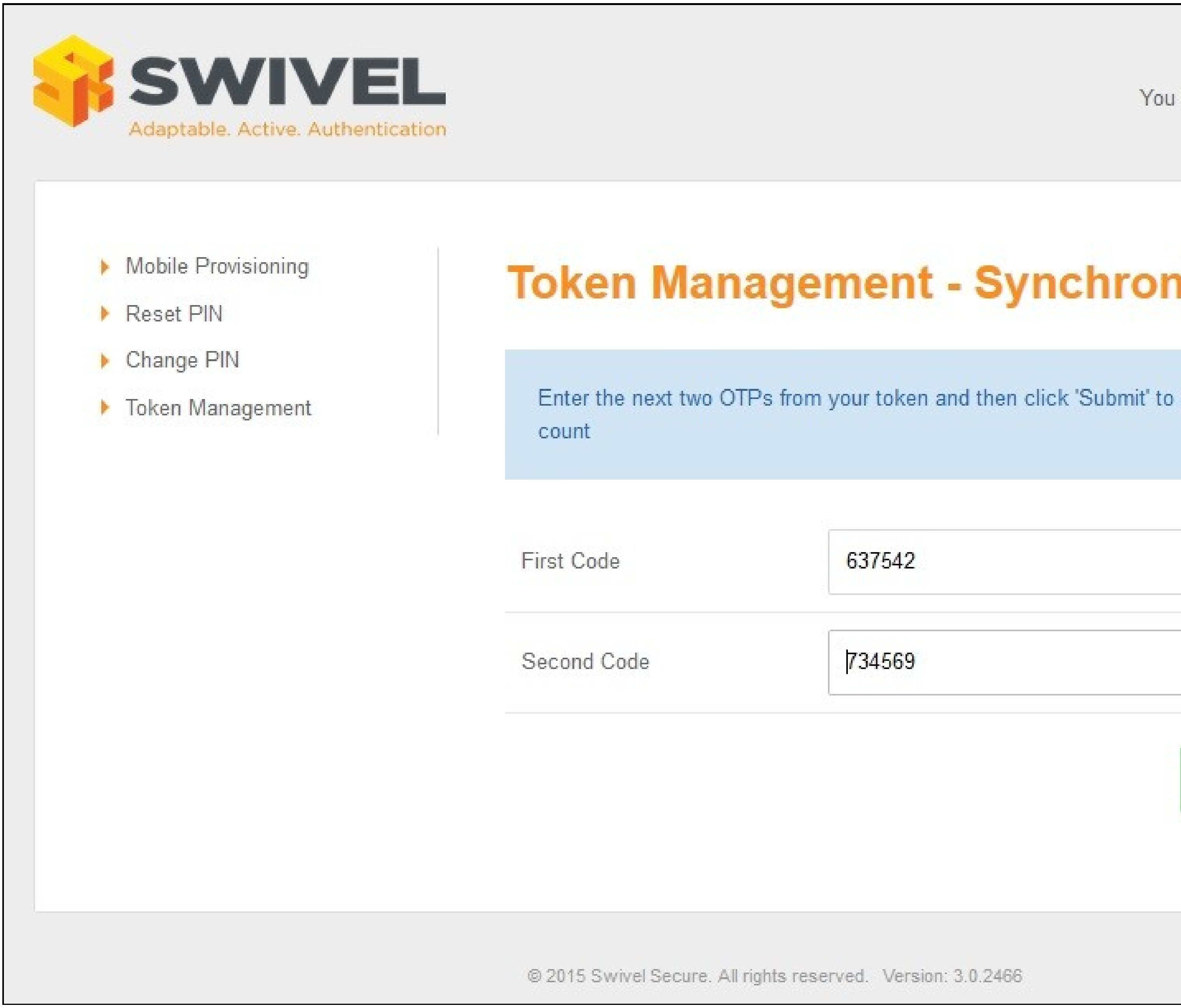
Current OTC: ••••

New OTC: ••••

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

681.8 User Portal Token Sync

Token Sync allows a user to synchronise a new or existing token by entering two consecutive OTC from the token.



Token Management - Synchron

Enter the next two OTPs from your token and then click 'Submit' to
count

First Code 637542

Second Code 734569

© 2015 Swivel Secure. All rights reserved. Version: 3.0.2466

682 Additional Configuration options

682.1 Creating a URL redirect from the root level

See Redirect link

682.2 Using 443 instead of 8443

See How to run PINsafe on non-default ports

682.3 Changing the logo

You can change the User Portal logo by navigating to /usr/local/tomcat/webapps2/userportal/img and there is an image called swivel-logo.png (Not to be mistaken for swivel_logo.png). Import the required image and rename it to swivel-logo.png.

683 Known Issues

The User Portal ONLY supports the UTF-8 Character Code Set.

684 Troubleshooting

A Reset code could not be requested.

The Swivel server does not allow Account Resets

The ResetPIN needs to be enabled on the Swivel Administration console.

684.1 Changes to xml files do not take effect

684.1.1 Cached files

You may find you need to clear the cached compiled files for User Portal before the new settings will take effect. You can find these in /usr/local/tomcat/work/Catalina-proxy/localhost/userportal. 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.

684.1.2 File locations

Ensure the correct locations are being edited: Config files will be stored in ~/.swivelportal/conf or as stated by stated in env variable SWIVEL_PORTAL_HOME or web.xml ?portalHome"

Editing the configuration files under <path to Tomcat>\webapps2\userportal\WEB-INF (Example: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps2\userportal\WEB-INF) will not be used.

684.2 Error Messages

There was an error please check your username and pin code if the problem persists contact your systems administrator.

Contact the Administrator to see verify the error. This error should be logged on the Swivel server that the User Portal uses.

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

The user is required to use a static Password

Change PIN failed for user: graham, error: The one-time code was missing or malformed.

Incorrect OTC entered

In the Swivel log viewer

AgentXML request failed, error: The XML request sent from the agent was malformed.

and in the User Portal

Something went wrong. Please try again or contact your system administrator.

This can be seen when a token is synced and the token is already synched.

Dual channel message request failed, error: On-demand dual channel delivery is disabled

When sending an SMS/Email to a user the On-demand dual channel delivery needs to be enabed on the Swivel Administration console under Server/Dual Channel.

685 User Portal - old

686 Overview

This version has been superceded by User Portal

This page discusses the User Portal version 2. The user portal places all the self-service application in one place and allows the customer to decide what pages to make available to users and how those pages are to be used. This can replace the current changepin , resetpin and proxy applications.

The following applications are available.

- View Security String
- Request a Security String Message (as defined by the transport, usually SMS or email). This can be password protected.
- Login presents a login page to the user, useful for testing but also used to protect user provision screen if required.
- Change PIN
- Reset PIN (The ResetPIN needs to be enabled on the Swivel Administration console). See also ResetPIN How To Guide
- Provision a Mobile device. This can be password protected.

687 Prerequisites

Swivel 3.9.1 onwards

Swivel appliance with user portal pre-installed or userportal.war file, see Downloads.

688 Upgrading User Portal

Download the User Portal, extract the userportal.war file and overwrite the existing userportal.war file (see below for file location). This will automatically upgrade the User Portal.

689 User Portal Installation

If the User Portal is not installed on a Swivel appliance, it can be installed on an appliance running Swivel 3.9.1 onwards. WinSCP can be used to install this, see WinSCP How To Guide.

Create a folder /home/swivel/.swivelportal/conf, ensure it has user and group permissions of swivel.

Copy the userportal.war file to /usr/local/tomcat/webapps2. It is possible to install into /usr/local/tomcat/webapps, but the installation will only work using HTTP, and SSL must be disabled for port 8080 through the CMI.

Copy the below files from /usr/local/tomcat/webapps2/userportal/resources/conf to /home/swivel/.swivelportal/conf

- portalsettings.xml
- settings.xml

690 User Portal Configuration

Config files will be stored in ~/.swivelportal/conf or as stated by stated in env variable SWIVEL_PORTAL_HOME or web.xml ?portalHome", see Transient Data Storage.

690.1 User portal communication with appliance settings

The file settings.xml defines how the user portal will communicate with the Swivel Appliance. Generally the only setting that needs editing is the shared secret that will need to match the one set on the Swivel Appliance, leave the other settings at their default.

Appliance webapps2 settings

```
<?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="secret">secret</entry>
<entry key="selfsigned">true</entry>
<entry key="codepage">UTF-8</entry>
<entry key="proxypinpad">false</entry>
</properties>
```

Appliance webapps settings (Non SSL only)

```
<?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="secret">secret</entry>
<entry key="selfsigned">true</entry>
<entry key="codepage">UTF-8</entry>
<entry key="proxypinpad">false</entry>
</properties>
```

690.2 User portal home page application settings

The file portalsettings.xml determines how the portal will perform

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="login">pinpad</entry>
<entry key="securitystring">pinpad</entry>
<entry key="changepin">pinpad</entry>
<entry key="secureprovision">true</entry>
<entry key="messagepassword">true</entry>
<entry key="redirect">./index.jsp</entry>
</properties>
```

690.2.1 Portalsettings.xml options

login: Default: pinpad Options: turing, pinpad. What image will be used on the login page.

securitystring: Default: pinpad, Options: turing, pinpad. What image will be used on the Security String page.

changepin: Default: pinpad, Options: turing, pinpad, explicit (PIN is entered directly). What image will be used on the changepin page.

secureprovision: Default true, Options true, false. Determines if a user must authenticate to the portal before they are allowed to request provision code.

messagepassword: Default: true, Options true, false. Determines if a user must supply a valid password before they can receive a dual channel message.

redirect: Default: ./index.jsp, Options index.jsp, or other URL. Where a user is redirected after completing a changepin or authentication.

After making a change restart Tomcat

691 Additional User Portal Customisation

691.1 User portal Images

The default image is at the below location, if a different image is required then this can be backed up and a new file of the same name used, or alternatively each page can be edited for the new image file.

<path to Tomcat>/userportal/images/swivel_logo.png

For Swivel appliances: /usr/local/tomcat/webapps2/userportal/images/swivel_logo.png

691.2 Changing Authentication Method

If you want the authentication changing from PinPad to Turing and vice versa, you need to navigate to home/swivel/.swivelportal/conf, then to portalsettings.xml. Under ?login?, ?securitystring? and ?changepin?; change the type of authentication to the desired method, i.e PinPad or Turing.

691.3 User Portal Menu options

The options available to portal users can be edited to remove menus that are not required. Edit the file \usr\local\tomcat\userportal\WEB-INF\pages\menu.jsp

To remove an item, add at the start '' example

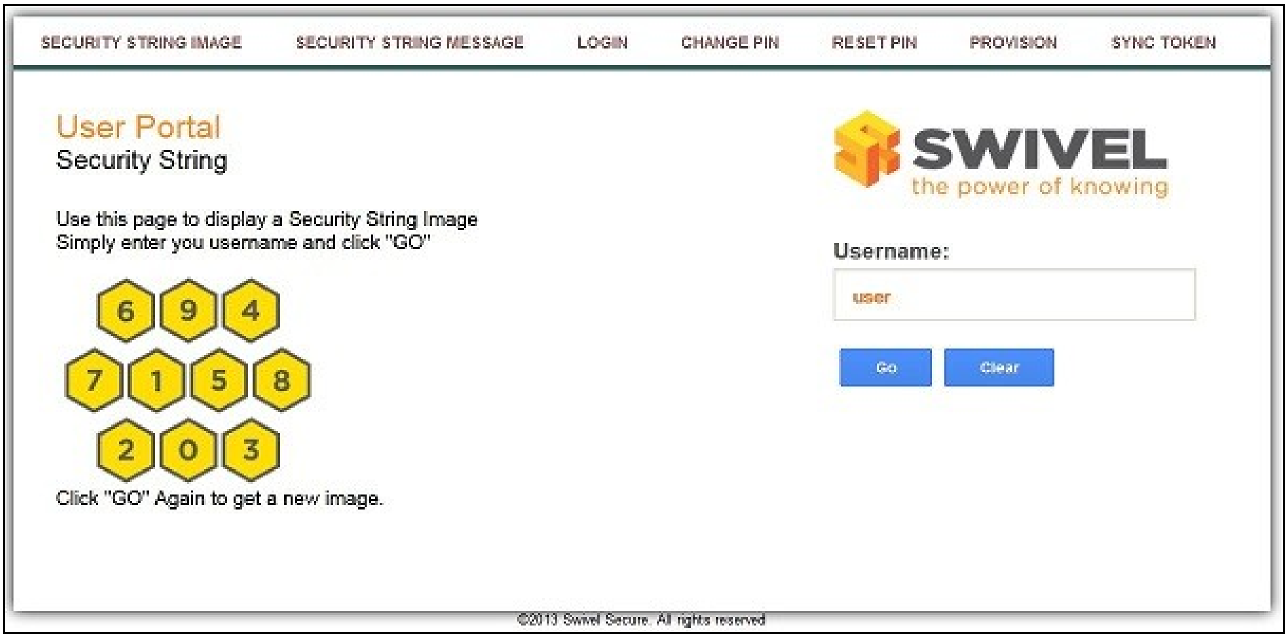
The following removes all but the ChangePIN and ResetPIN links

```
<div id='cssmenu'>
 <ul>



    <li><a href="change"><span>Change PIN</span></a></li>
    <li><a href="reset"><span>Reset PIN</span></a></li>


 </ul>
</div></nowiki>
```

692 Testing

Navigate to the userportal page; https://IP:8443/userportal The userportal should be displayed.

692.1 User Portal Security String Image



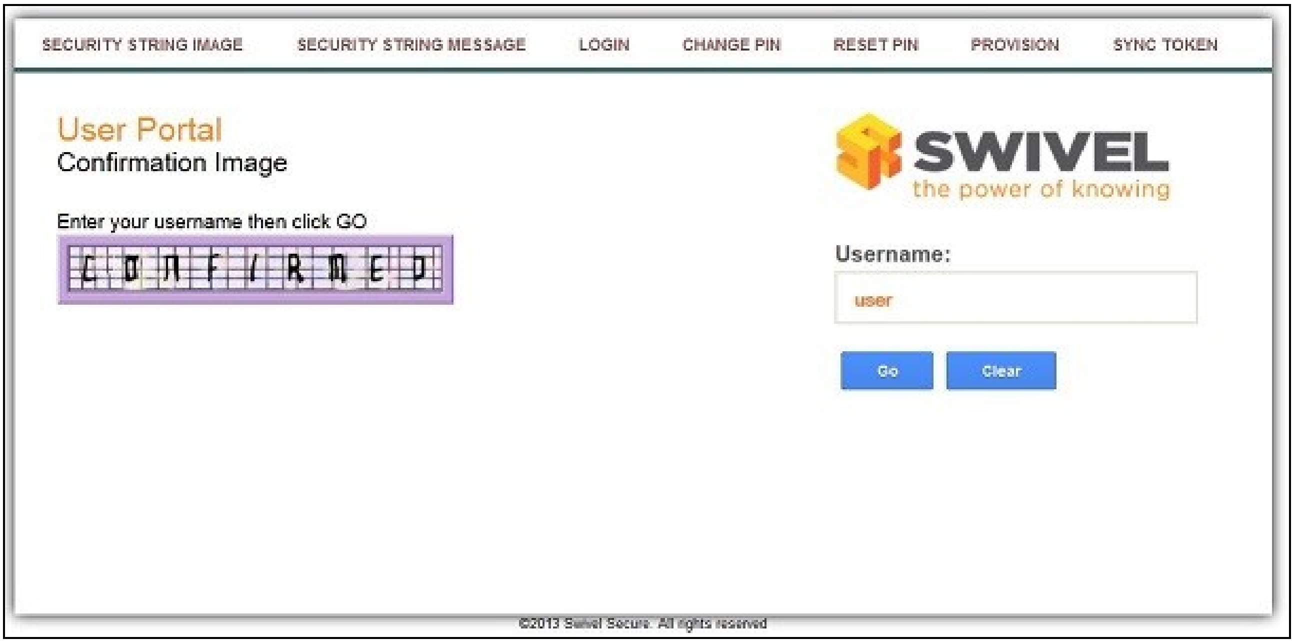
Use this page to display a Security String Image
Simply enter you username and click "GO"

Click "GO" Again to get a new image.

©2013 Swivel Secure. All rights reserved

Here you can enter a user name and click [Go] and the Security String image will update. If you press [Go] again, it will update the image once again.

692.2 User Portal Security String Message



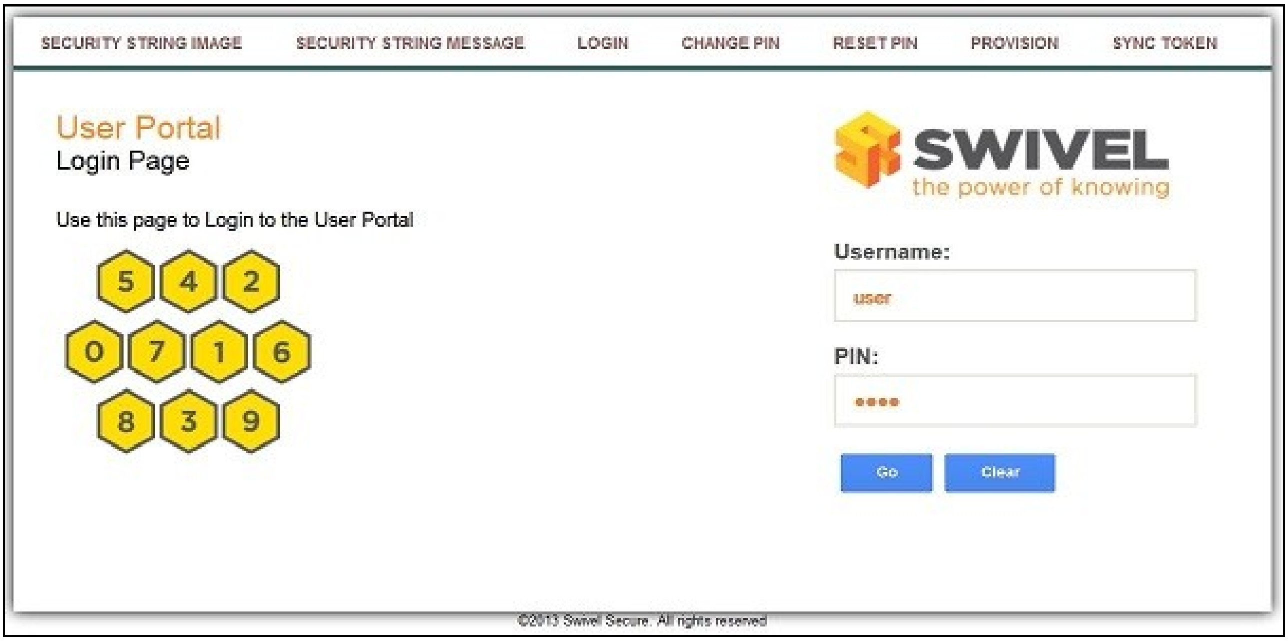
Enter your username then click GO

©2013 Swivel Secure. All rights reserved

Once you have entered a Username and clicked [Go], the ?Confirmed? TURing image will appear. Additionally, if you press [Go] again, it will update the image.

692.3 User Portal Login

The user portal login allows a user to verify that their login works with Swivel.



User Portal

Login Page

Use this page to Login to the User Portal

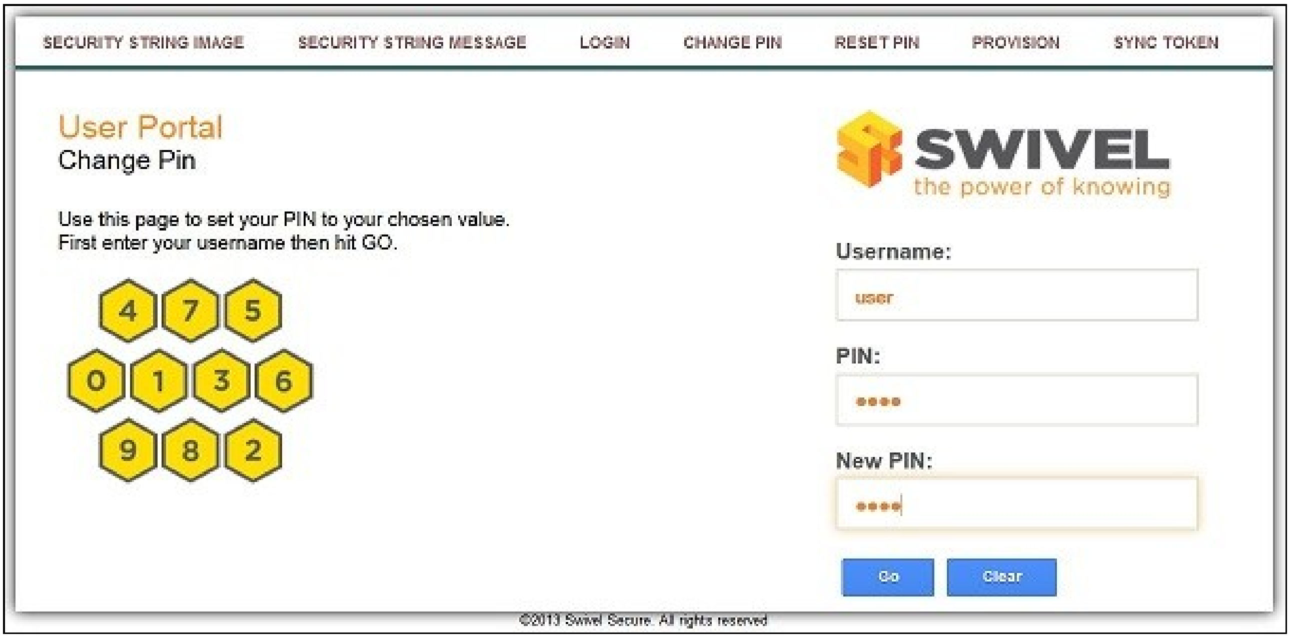
Username: user

PIN: ••••

©2013 Swivel Secure. All rights reserved

692.4 User Portal Change PIN

The user portal allows the user to Change their PIN.



User Portal

Change Pin

Use this page to set your PIN to your chosen value.
First enter your username then hit GO.

Username: user

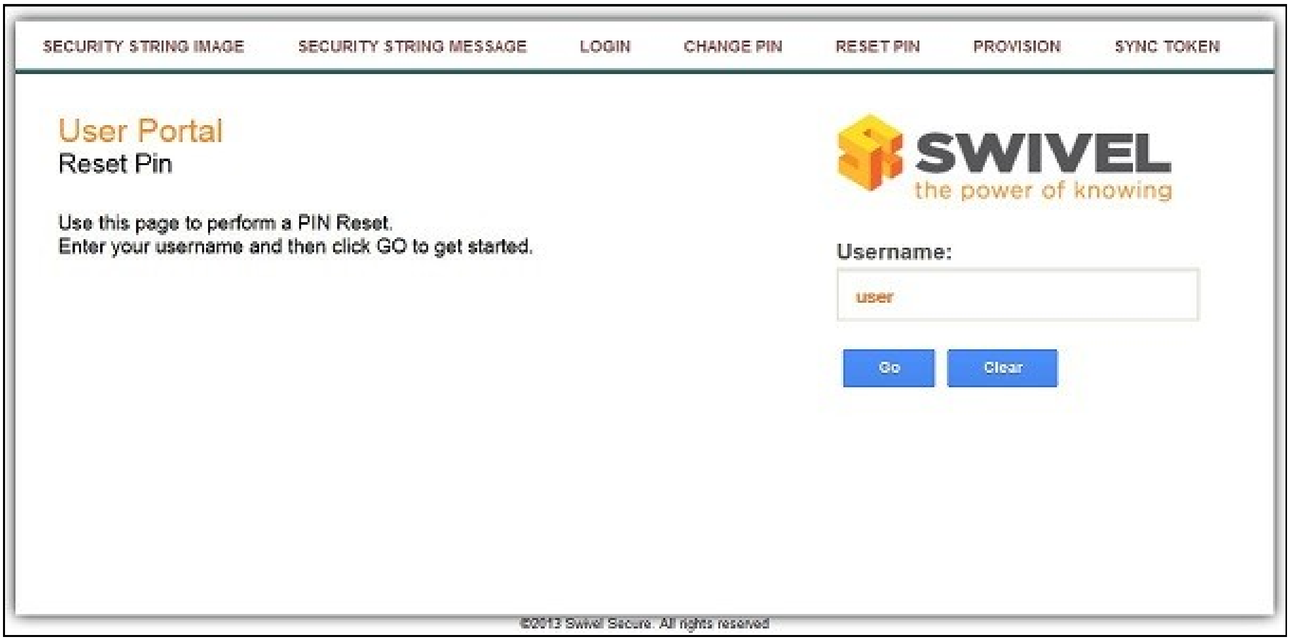
PIN: ••••

New PIN: ••••

©2013 Swivel Secure. All rights reserved

692.5 User Portal Reset PIN

The user portal Rset PIN allows a user to reset a forgotten PIN (It will not unlock an account)



User Portal

Reset Pin

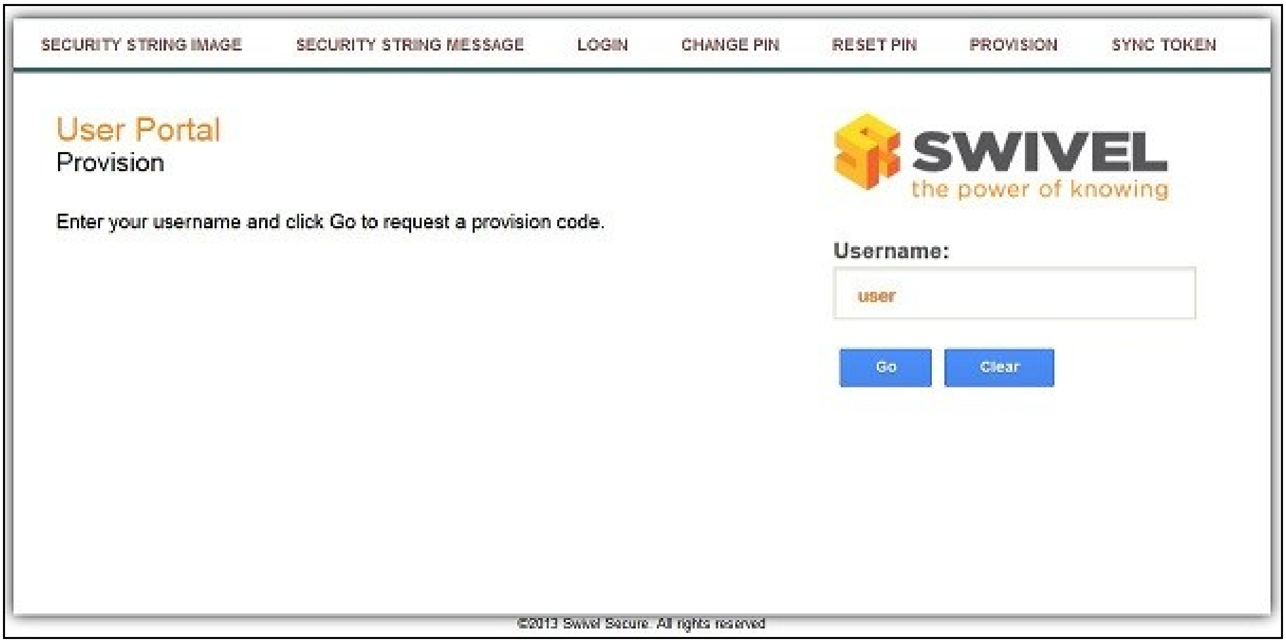
Use this page to perform a PIN Reset.
Enter your username and then click GO to get started.

Username: user

©2013 Swivel Secure. All rights reserved

692.6 User Portal Provision

The user portal allows a user to provision their Mobile Phone for authentication.



User Portal

Provision

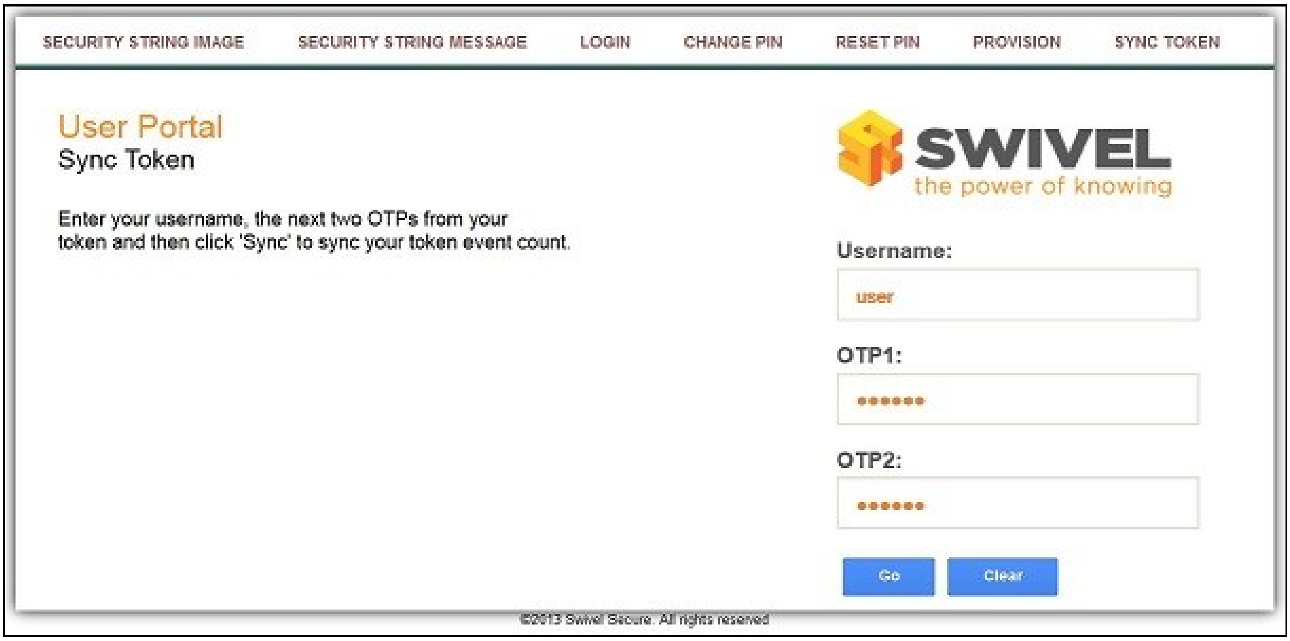
Enter your username and click Go to request a provision code.

Username: user

©2013 Swivel Secure. All rights reserved

692.7 User Portal Sync Token

The user portal allows a user to Synchronise their Token.



User Portal

Sync Token

Enter your username, the next two OTPs from your token and then click 'Sync' to sync your token event count.

Username: user

OTP1: ●●●●●●

OTP2: ●●●●●●

©2013 Swivel Secure. All rights reserved

693 Additional Configuration options

693.1 Creating a URL redirect from the root level

See Redirect link

693.2 Using 443 instead of 8443

See How to run PINsafe on non-default ports

694 Known Issues

The standard install of the user portal with an appliance is in the webapps2 folder with HTTPS but may also run under HTTP. An install in the webapps folder will only work with HTTP and not HTTPS.

695 Troubleshooting

A Reset code could not be requested.

The Swivel server does not allow Account Resets

The ResetPIN needs to be enabled on the Swivel Administration console.

695.1 Changes to xml files do not take effect

695.1.1 Cached files

You may find you need to clear the cached compiled files for User Portal before the new settings will take effect. You can find these in /usr/local/tomcat/work/Catalina-proxy/localhost/userportal. 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.

695.1.2 File locations

Ensure the correct locations are being edited: Config files will be stored in ~/.swivelportal/conf or as stated by stated in env variable SWIVEL_PORTAL_HOME or web.xml ?portalHome"

Editing the configuration files under <path to Tomcat>\webapps2\userportal\WEB-INF (Example: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps2\userportal\WEB-INF) will not be used.

695.2 Error Messages

There was an error please check your username and pin code if the problem persists contact your systems administrator.

Contact the Administrator to see verify the error. This error should be logged on the Swivel server that the User Portal uses.

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

The user is required to use a static Password

Change PIN failed for user: graham, error: The one-time code was missing or malformed.

Incorrect OTC entered

In the Swivel log viewer

AgentXML request failed, error: The XML request sent from the agent was malformed.

and in the User Portal

Something went wrong. Please try again or contact your system administrator.

This can be seen when a token is synced and the token is already synched.

696 User Portal Administrator User Guide

696.1 Overview

The user portal version 3 and 4 places all the self-service application in one place and allows the customer to decide what pages to make available to users and how those pages are to be used. This can replace the current changepin , resetpin and proxy applications.

The following applications are available.

- Change PIN
- Reset PIN (The ResetPIN needs to be enabled on the Swivel Administration console). See also ResetPIN How To Guide
- Provision a Mobile device
- Sync a Token

696.2 Prerequisites

User Portal

Swivel v3.9.5 onwards.

Appliance v2.0.16 onwards.

QR Code Provision Provisioning 3.10.4 onwards.

Token See link for Token prerequisites.

696.3 User Portal Configuration

Config files are located in: /home/swivel/.swivel/user-portal/ (or .swiveluser-portal on some versions)

settings.properties

Communication settings for a local Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=127.0.0.1
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8181
```

Communication settings for a remote Swivel instance. Restart Tomcat after making any changes.

```
pinsafessl=false
pinsafeserver=RemoteSwivelIP or VIP
pinsafecontext=pinsafe
pinsafesecret=secret
pinsafeport=8080
```

The following attribute indicates if on the ResetPIN screen the user can choose if the Password needs to be reset with the PIN or not. By default it is set to false.

```
showresetpasswordfield=false
```

From 4.0.5, the following attribute indicates if authentication in user portal requires a confirmation code. By default it is set to false.

```
showconfirmationcode=false
```

portalconfig.properties

Controls the behavious of changePIN. Restart Tomcat after making any changes.

```
#valid settings: directEntry turingEntry pinpadEntry
changepin.page=turingEntry
```

696.4 Language files

These are located in /usr/local/tomcat/webapps2/userportal/WEB-INF/classes

messages_en.properties

This file contains the text and language which may be customised

696.5 User Portal Menu options

The options available to portal users can be edited to remove menus that are not required. Edit the file \usr\local\tomcat\userportal\WEB-INF\view\template\leftpanel.jsp

To remove an item, add at the start '' example

The following removes the ChangePIN link

```
<li><a href="${mobileProvisioningUrl}"><spring:message code = "mobile_provisioning.title" /></a></li>
<li><a href="${selfResetUrl}" onclick="return confirmDialog(event);"><spring:message code = "reset.title" /></a></li>

<li><a href="${tokenManagementUrl}"><spring:message code = "tokenmanagement.title" /></a></li>
```

696.6 Additional Configuration options

Creating a URL redirect from the root level

See Redirect link

Using 443 instead of 8443

See How to run PINsafe on non-default ports

Changing the logo

You can change the User Portal logo by navigating to /usr/local/tomcat/webapps2/userportal/img and there is an image called swivel-logo.png (Not to be mistaken for swivel_logo.png). Import the required image and rename it to swivel-logo.png.

For v4 the available option is the logo-mark--purple.png which is the logo on top of the Username.

696.7 Known Issues

The User Portal ONLY supports the UTF-8 Character Code Set.

696.8 Troubleshooting

A Reset code could not be requested.

The Swivel server does not allow Account Resets

The ResetPIN needs to be enabled on the Swivel Administration console.

696.9 Changes to xml files do not take effect

Cached files

You may find you need to clear the cached compiled files for User Portal before the new settings will take effect. You can find these in /usr/local/tomcat/work/Catalina-proxy/localhost/userportal. 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.

File locations

Ensure the correct locations are being edited: Config files will be stored in ~/.swivelportal/conf or as stated by stated in env variable SWIVEL_PORTAL_HOME or web.xml ?portalHome"

Editing the configuration files under <path to Tomcat>\webapps2\userportal\WEB-INF (Example: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps2\userportal\WEB-INF) will not be used.

Error Messages

There was an error please check your username and pin code if the problem persists contact your systems administrator. Contact the Administrator to see verify the error. This error should be logged on the Swivel server that the User Portal uses.

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

Change PIN failed for user: graham, error: The one-time code was missing or malformed. Incorrect OTC entered

In the Swivel log viewer

AgentXML request failed, error: The XML request sent from the agent was malformed.

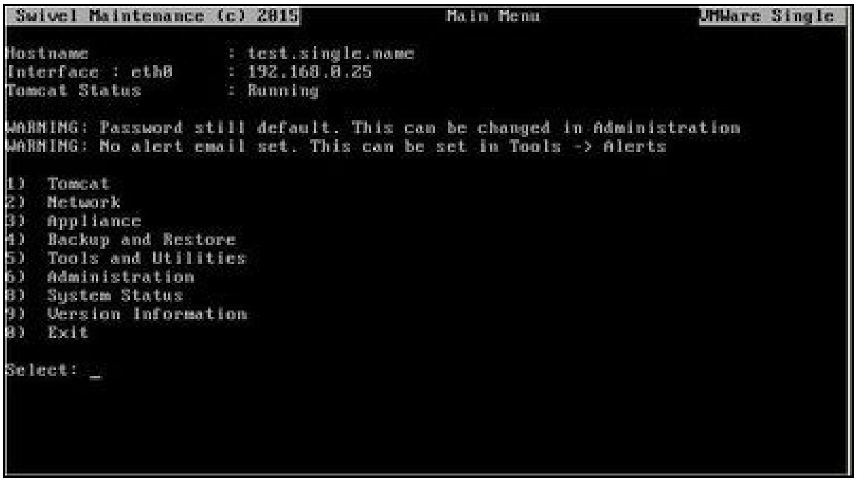
and in the User Portal

Something went wrong. Please try again or contact your system administrator. This can be seen when a token is synced and the token is already synched.

Dual channel message request failed, error: On-demand dual channel delivery is disabled When sending an SMS/Email to a user the On-demand dual channel delivery needs to be enabed on the Swivel Administration console under Server/Dual Channel.

697 V3 & V4 Appliance Quick Start

697.1 Quick Start



```
 Swivel Maintenance (c) 2015                Main Menu                VMWare Single

Hostname               : test.single.name
Interface : eth0       : 192.168.0.25
Tomcat Status          : Running

WARNING: Password still default. This can be changed in Administration
WARNING: No alert email set. This can be set in Tools -> Alerts

1)  Tomcat
2)  Network
3)  Appliance
4)  Backup and Restore
5)  Tools and Utilities
6)  Administration
8)  System Status
9)  Version Information
0)  Exit

Select: _
```

This guide is a quick start guide to the **Version 3 and 4** Swivel Secure Appliances.

A reference guide that describes the meaning for all the menus is also available here for version 3 and here for version 4.

The appliance will come with a pre-configured IP address depending on appliance type:

Stand-alone (192.168.0.35)

HA Primary (192.168.0.36)

HA Standby (192.168.0.37)

Amazon/Cloud (DHCP)

If this IP address is compatible with your network you can plug an ethernet cable into eth0 (labelled Gb1) and access the appliance via SSH.

Alternatively you can access by plugging in an ethernet cross-over cable into eth0

697.2 Accessing Appliance Menus

To access the appliance menus you secure-shell onto the appliance. From a Windows machine you can use a terminal emulator capable of SSH connections, such as putty. From a Linux machine you can simply use the ssh command. SSH access is via the standard port 22.

When you access the appliance you will be prompted for a username and password. The default settings for this are:

- V3 and V4.0 appliances:

username:admin

password:lockbox

- V4.1 and later appliances:

username:admin

password:securebox

Once you have logged on you will be presented with the top level menu. Sub-menus are accessed by simply pressing the number of the item required followed by <Enter>

On certain actions you will be asked to enter Y to continue. Entering any other character or just entering return will cause the action to be cancelled. To maintain compatibility with v2, entering ?yes? will also work.

NOTE Refer to our PuTTY How To Guide for detailed instructions and screenshots.

697.3 Updating Appliance

Important You should update an appliance prior to installation to ensure it is running the optimum versions and settings

A reference guide that details the options available for Appliance updating is available.

697.4 Webmin

You can find the Webmin guide here.

697.5 Setting Hostname IP Address

If you are using an Cloud-based appliance, IP addresses must be set by DHCP.

You will need to set the IP address(es) of the appliance. To do this use the access the Network Menu and do the following

1. Use the change hostname to set the hostname. Recommended to make this a meaningful, eg swivel.yourcompany. If this appliance is part of an HA installation include the appliance type eg primary.swivel.yourcompany.
2. Set the Network settings for ETH0. This is the main interface, you may not need to change the ETH1 settings as this is used for database replication (ref Setting up HA)
3. Set DNS servers. This may not be required at this stage but will be required if the Swivel Appliance will need to perform DNS resolution, eg for sending emails or SMS messages via named hosts.

697.6 Starting and Stopping Tomcat

Swivel applications run within Tomcat so you will only be able to access them when Tomcat is running. Tomcat will start automatically when the appliance starts and the status of Tomcat is shown on the main screen and on the Tomcat menu screen.

Should you need to manually start or stop Tomcat, this is possible from the Tomcat menu.

697.7 Accessing the Swivel Applications

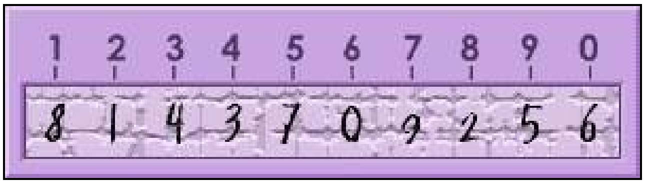
With the ETH0 address set to <IP Address> you will be able to access the following applications from a browser:

Swivel Core admin console https://<IP Address>:8080/pinsafe. For version 4, this should be https://<IP Address>:8080/sentry.

Swivel User (Self Service) Portal https://<IP Address>:8443/userportal

Swivel Proxy https://<IP Address>:8443/proxy

- The Swivel Proxy has no user interface but acts as a proxy for image and message requests e.g. https://<IP Address>:8443/proxy/SCImage?username=test should result in a TURing image being displayed.



698 Version Information

699 Overview

This article can help you determine the version of Swivel Core and the underlying Appliance Version if you use an appliance. To see Swivel version details see Versions FAQ and also appliance type see Appliance General FAQ.

700 Prerequisites

- Swivel 3.x
- Appliance version 2.x with CMI

701 Version Information via the CMI

Login to the appliance using the PuTTY How To Guide.

From the main menu, select Advanced Options -> Version Information. You will be presented with the following information:

```
Swivel Maintenance (c) 2012                                            Single

Appliance and software versions

CMI             : 0.12
CMI Backup      : 0.16
CMI Restore     : 0.16
CMI Certs.      : 0.10
CMI Diags.      : 0.6
Appliance Build : 2.0.14
Swivel Version  : 3.9.7.996
Tomcat Version  : 5.5.28
Java Version    : 1.6.0_18
Webmin Version  : 1.510

Press Return to continue
```

- **Swivel Version** is the version of the Swivel Core software installed in Webapps;
- **Appliance Build** is the appliance version.

702 Version information from the command line

Check the login message from the console.

run the following command

```
grep APPLIANCE_VERS /etc/pinsafe.conf|cut -d\= -f2
```

If not, inspect the /etc/pinsafe.conf file manually.

Other components can be found from the following commands on older appliances:

Apache Tomcat:

```
ls /usr/local|grep apache|cut -d\- -f3
```

Java:

```
ls /usr/java|grep jre|cut -d\e -f2
```

MySQL (if used):

```
mysql --version|cut -d\  -f6|cut -d\, -f1
```

Webmin:

```
cat /etc/webmin/version
```

703 What appliance do I have? Am I running standalone, Active/Passive, Active/Active, or a DR?

A). A lot of installs appear to be the same from the external view, and may require command line access to determine the type.

Standalone: Running on its own using the internal Swivel data store. A Standalone appliance may be Hardware or VMware.

Active/Passive: These are only hardware appliances and a VMware is not available. HA pair with a cross over cable between the secondary interface, it uses a Virtual IP address that switches from the Active machine to the standby machine when it is fails over and file replication to share data between systems, using a process called drbd. In this configuration there is only one Swivel instance to configure, the entire file system including the Swivel application automatically fails over. This system may not scale to more than two Swivel servers. To see if this system is running enter:

```
cat /proc/drbd
```

Expected Results:

primary

```
drbd driver loaded OK; device status:
version: 0.7.14 (api:77/proto:74)
SVN Revision: 1989 build by buildcentos@build-i386, 2006-03-18 19:03:54
 0: cs:Connected st:Primary/Secondary ld:Consistent
    ns:8492552 nr:22716 dw:8515268 dr:284982 al:106 bm:2286 lo:0 pe:0 ua:0 ap:0
```

secondary

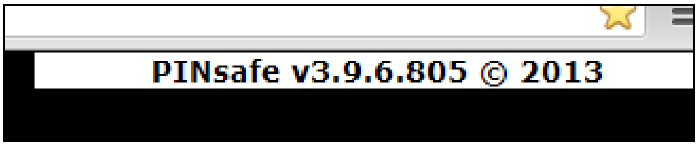
```
drbd driver loaded OK; device status:
version: 0.7.14 (api:77/proto:74)
SVN Revision: 1989 build by buildcentos@build-i386, 2006-03-18 19:03:54
 0: cs:Connected st:Secondary/Primary ld:Consistent
    ns:22716 nr:10565672 dw:10588388 dr:36158 al:20 bm:128 lo:0 pe:0 ua:0 ap:0
```

Active/Active: These may be hardware or VMware. Each Swivel appliance is able to receive authentication requests regardless of the state of the other. On the appliance this will be used with a MySQL database, although it would be possible to use another external Database. Using the Virtual IP address is optional. To verify it is in active/active mode, check from the Swivel Administration console to see if the MySQL database is being used and mode is synchronised.

DR or **Slave**: These may be hardware or VMWare. Here each Swivel appliance is able to receive authentication requests regardless of the state of the other. The appliance may appear to be Active/Passive if the deployment scenario directs all authentication requests to one Swivel appliance, although it is an Active/Active deployment. On the appliance a MySQL database is used, although it would be possible to use another external Database. To verify it is in DR or slave mode and not an Active server, check from the Swivel Administration console to see if the MySQL database is being used and mode is slave.

704 Software only installation - Swivel Core

When you visit the Swivel Administration Console on port 8080, in the top right hand corner you will see the version number of the Swivel Core. **Note that this is not the version of the underlying appliance.**



PINsafe v3.9.6.805 © 2013

705 View Security Strings How To Guide

705.1 Overview

PINsafe has a number of alternative methods to allow authentication should difficulties arise. This document outlines how to use the View Strings function for troubleshooting and as a backup authentication method.

705.2 Prerequisites

PINsafe 3.7 onwards

705.3 View Security Strings Guide

To view a users security string that they have been sent by email or SMS, on the PINsafe Administration Console, select User Administration, then click on the required user (search or filter as necessary to find the required user), then click on View Strings.

Single Channel Options Show, generates a single Channel authentication, valid for 2 minutes by default. Note generating a Single Channel image will prevent use of other authentication methods in the default time period until the expected single channel authentication is made. A new unique string is generated each tie the image is refreshed, rendering the previous image invalid.

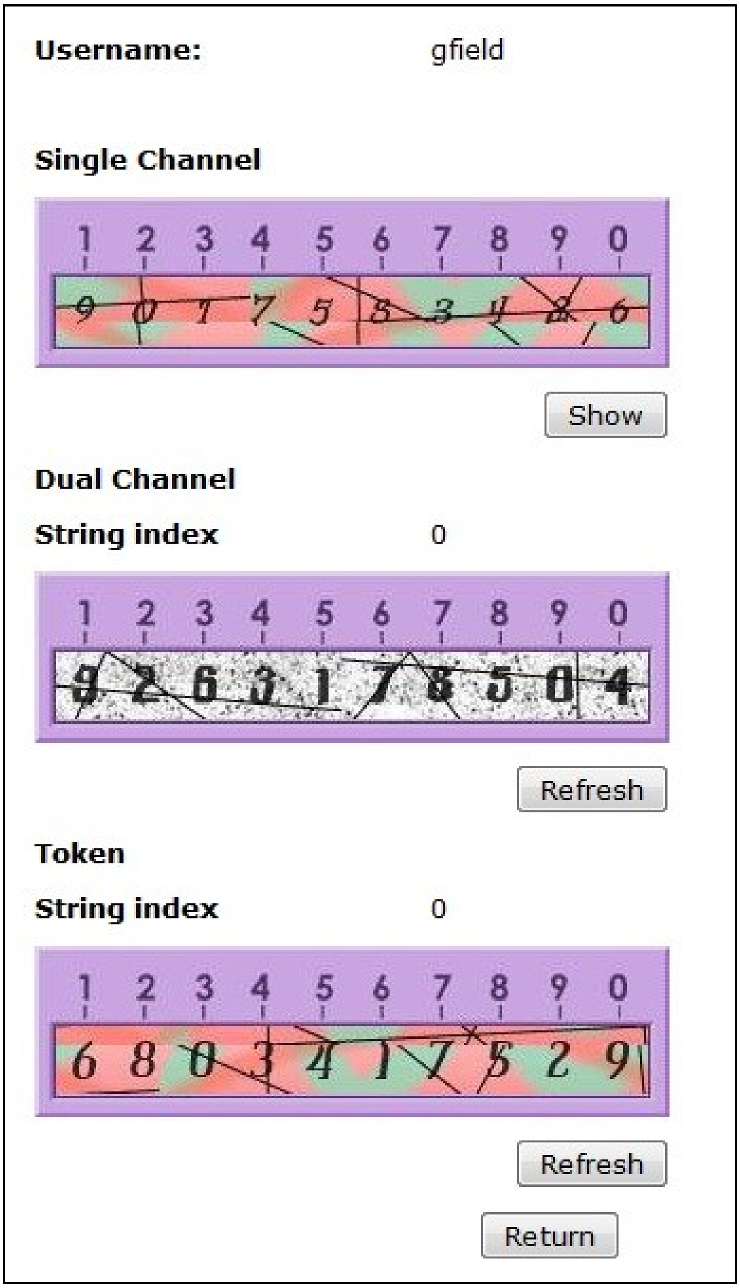
Dual Channel Shows the last dual channel security string sent to the user and any string index where multiple security strings are used, to tell the user which security string to use. If no Dual Channel message has been sent to the user then the following message is displayed **No Dual Channel strings available**

Note: On the PINsafe Administration console it is viewed as a single channel image, but for the user it will be sent by their transport method.

Token Shows the token/mobile Phone Client security expected any string index where multiple security strings are used, to tell the user which security string to use. If no Dual Channel message has been sent to the user then the following message is displayed **No Token strings available**

Note: On the PINsafe Administration console it is viewed as a single channel image, but for the user it will be sent by their transport method.

Oath Token (from v4.0.5 onwards) Shows the current OATH TOTP Token, to tell the user which security string to use.



Username: gfield

Single Channel

Dual Channel

String index 0

Token

String index 0

705.4 Using View Strings as a Backup Authentication

If a user loses their mobile device and needs authenticating before a replacement can be provisioned, cannot receive an SMS message, or view the single Channel TURing image, then the View Strings can be used to provide the user with a valid security string.

Other alternatives are:

- Use mobile Phone Client where no SMS is being received
- SMS where security strings cannot be downloaded to the mobile phone Client
- Enable Single Channel TURing authentication for the user

Security Note: It may not be appropriate to use Single Channel backup authentications where two factor authentication is mandatory.

The View Strings Backup authentication process is given below.

User calls helpdesk by landline

User Provide Username

Helpdesk View Strings for user

Helpdesk provide the required security string for the user

Call ends

User calculates OTC using their own PIN

User Authenticates

If further user authentication is required to determine the user please contact your Swivel Secure Sales representative to discuss additional options.

705.5 Testing

705.6 Known Issues

PINsafe 3.8.4256 has an error whereby On demand authentication security strings do not match those in the View Security strings. An authentication attempt will produce the error messages:

RADIUS: <0> Access-Request(1) LEN=192.168.0.1:1001 Access Request by username Failed: AccessRejectException: AGENT_ERROR_NO_SECURITY_STRINGS

and

Login failed for user:username, error: The user does not have any security strings suitable for the authentication.

705.7 Troubleshooting

706 VIP on PINsafe Appliances

707 Overview

This document covers the use of the VIP (Virtual IP Address) on Swivel appliances to provide redundancy in the event of a failure of one of the Swivel servers. The VIP is usually used for providing resilience to the single channel TURing image, but may also be used for Dual Channel message requests and the Security String index.

The VIP is often used with the Mon process, so when a monitored process fails, the VIP provides resilience to that process, see

The VIP is controlled by the heartbeat process.

707.1 What is a VIP?

The VIP is a Virtual IP address that can be bound to an Ethernet interface (ETH0) as a second IP address but can MOVE from one Swivel appliance to another. Swivel appliances are usually configured with an IP address on ETH0, and another IP address is assigned as the VIP. The VIP usually resides on the primary appliance and if there is a problem it is unbound from the Primary server and started on the standby server. Control of the VIP is by the Heartbeat process, which uses the Mon process to determine if the VIP should move from one appliance to another. The VIP IP must be on the same subnet as the Primary and Standby appliances ETH0 IP.

The VIP adds resilience to the appliances, and all traffic will be directed to one server. There is no session affinity.

708 Heartbeat Explained

Heartbeat regularly sends a UDP datagram on port 694 to the multicast address 225.0.0.1 announcing it is up and running and owns the VIP address. If the appliance it is running on shuts down for any reason, this stream of packets from the primary master stops and after a predetermined timeout, the standby master becomes master and assumes the VIP address. Through the webmin, Heartbeat can be configured to monitor certain resources on the appliance and give up the address if some conditions are met, see also MON Service Monitor How to guide.

Heartbeat uses gratutious ARP to announce the changing of the MAC address. (Unlike VRRPd which replaces the MAC address of the active machine with a virtual one).

709 Prerequisites

Swivel A/A appliances, see also High Availability with PINsafe

710 VIP deployment considerations

- Each Swivel appliance will need to be configured both for networking and Swivel configuration options.
- The VIP must be deployed on a pair of Swivel appliances within the same subnet.
- Three IP addresses within the subnet are required for ETH 0: Primary, Standby and VIP
- The Swivel appliances must be able to ping each other and the gateway IP address to ensure that each other is available and detect network failures. If the gateway is a firewall, then a rule may need to be created to allow the ping.
- Heartbeat status requires the appliances to be able to SSH each other. Verify that each appliance can ssh to the other by using ssh admin@hostname.
- Swivel A/A appliances use the cross over cable connection on ETH 1 directly between two appliances to detect that the difference between a network failure and the failure of a Swivel appliance. the **heartbeat** process monitors the network and controls where the VIP should be. The **mon** process monitors the VIP and provides alerting. If the cross over cable is not used, then communication for multicast traffic on UDP port 694 must be permitted between the appliances.
- Where the VIP is used to obtain a graphical TURing image, the real IP address of the Swivel appliance should be used for a RADIUS request since the Swivel appliance will respond with its real IP address which may cause the access device to drop the response as it will have come from a different IP. Primary and Secondary RADIUS servers may be configured. To overcome the possibility of the single channel image coming from one server and the RADIUS request going to another server one of the following should be enabled on the Primary Master and Standby Master:

Session Sharing

RADIUS Proxy see PINsafe RADIUS Proxy

710.1 VIP Configuration

The VIP should be configured from the CMI. The networking section allows the IP address of the Primary Master, Standby Master and VIP to be entered on each appliance.

To activate the VIP the heartbeat should be configured to start on system boot on the Primary Master and Standby Master, by selecting in the CMI Advanced, then Default Running Services, select Heartbeat so that it displays ON. To manually start heartbeat, in the CMI select Heartbeat then start.

Please Note: Do NOT use the VIP address as the RADIUS server address.

710.2 VIP Alerting

The Mon process monitors the Swivel Appliance Tomcat and can allow failover but also the Swivel appliance can be configured to send an email when a fail over occurs.

Note: using Webmin on older versions of the appliance, a semi colon may be added onto the end of the configuration which renders it useless.

Make a backup of /etc/ha.d/haresources

Edit /etc/ha.d/haresources

using command line, or by editing the file using WinSCP see WinSCP How To Guide, or a recent version of the Webmin and alter the first instance of root@localhost to be the new monitoring email address.

Default Primary haresources file

```
# Swivel Appliance Build primary haresources File
#
# Use this line if you are going to use mysql replication method.
primary.swivel.local 172.16.1.98 MailTo::root@localhost::PINsafePrimary
# primary.swivel.local 172.16.1.98 drbddisk::webapps Filesystem::/dev/drbd0::/dr bd::ext3 tomcat5 MailTo::root@localhost::PINsafePrimary

################################################################################
######################
standby.swivel.local MailTo::root@localhost::PINsafeStandby
```

Default Standby haresources file

```
# Swivel Appliance Build standby haresources File
#
# Use this line if you are going to use mysql replication method.
primary.swivel.local 172.16.1.98 MailTo::root@localhost::PINsafePrimary
# primary.swivel.local 172.16.1.98 drbddisk::webapps Filesystem::/dev/drbd0::/drbd::ext3 tomcat5 MailTo::root@localhost::PINsafePrimary

######################################################################################################
standby.swivel.local MailTo::root@localhost::PINsafeStandby
```

To see email alerts sent see, /var/log/maillog

cat /var/log/maillog

710.2.1 VIP Alerting destination email address

The VIP alerting is sent by the appliance email system. To specify a different email server edit the file /etc/mail/sendmail.cf and look for the line

```
"smart" relay host
DS
```

Edit this to add the email server, for example

```
"smart" relay host
DSmail.swivelsecure.net
```

Restart Sendmail from the CMI or from the command line *service sendmail restart*

Also consider the use of MON for monitoring Tomcat see MON Service Monitor How to guide

710.3 VIP Status

To verify the VIP status on a Swivel appliance see VIP Status

711 Testing

712 Known Issues

The VIP should primarily be used for the TURing image single channel authentication. RADIUS requests should be directed against the real IP address of the appliance rather than the VIP. Requests to the VIP will be returned by the appliance on the real IP address and the access device may reject the RADIUS response as the source and destination IP addresses do not match.

713 Troubleshooting

Heartbeat will not start, see Heartbeat issues

714 VIP Status

715 Overview

This document details how to check the VIP Status on a Swivel appliance. For information on VIP configuration see VIP on PINsafe Appliances, for further information on Swivel HA see High Availability with PINsafe.

716 Prerequisites

Swivel appliance

717 Heartbeat Status

717.1 PINsafe VIP Status Check through the CMI

On each Swivel Appliance in the cluster (Primary Master, Standby Master, but not DR)

1. Login to the PINsafe Command Management Interface (See CMI).

2. Select Heartbeat

3. Select Status

4. Check VIP is on the expected server (usually always on the primary

If the Primary appliance is shutdown, the VIP should fail across to the Standby appliance.

717.2 Swivel VIP status check through the command line

From the command line run the following:

```
service heartbeat status
```

- If it's not started you'll get something like:

```
[admin@standby ~]# service heartbeat status heartbeat is stopped. No process
```

- If it is started you'll get something like:

```
[admin@standby ~]# service heartbeat status heartbeat OK [pid 6855 et al] is running on standby.swivel.local [standby.swivel.local]...
```

718 Testing

Shutdown Primary Master, observe VIP on Standby, start Primary Master, observe VIP on Primary and Standby

719 Known Issues

Running multiple Swivel HA clusters without a cross over cable, on the same network may cause issues as they use multicast on port 694 UDP by default.

719.1 Troubleshooting

Heartbeat will not start see Heartbeat issues

Check the /var/log/messages on each appliance for error messages related to heartbeat, see Troubleshooting Files FAQ

720 Voice Authentication

See Telephone Authentication

721 Yubikey

722 Overview

Yubikey supports the use of OATH HOTP such as used with the Swivel Token, or software tokens with a valid Seed can be used to authenticate Swivel users.

723 Prerequisites

Swivel 3.9.6

Yubico Yubikey token

Yubico Yubikey programming tool

724 Configure the Yubico Yubikey

Programming Tool Video

Insert the Yubikey and run the Yubikey programming tool. Select the following settings:

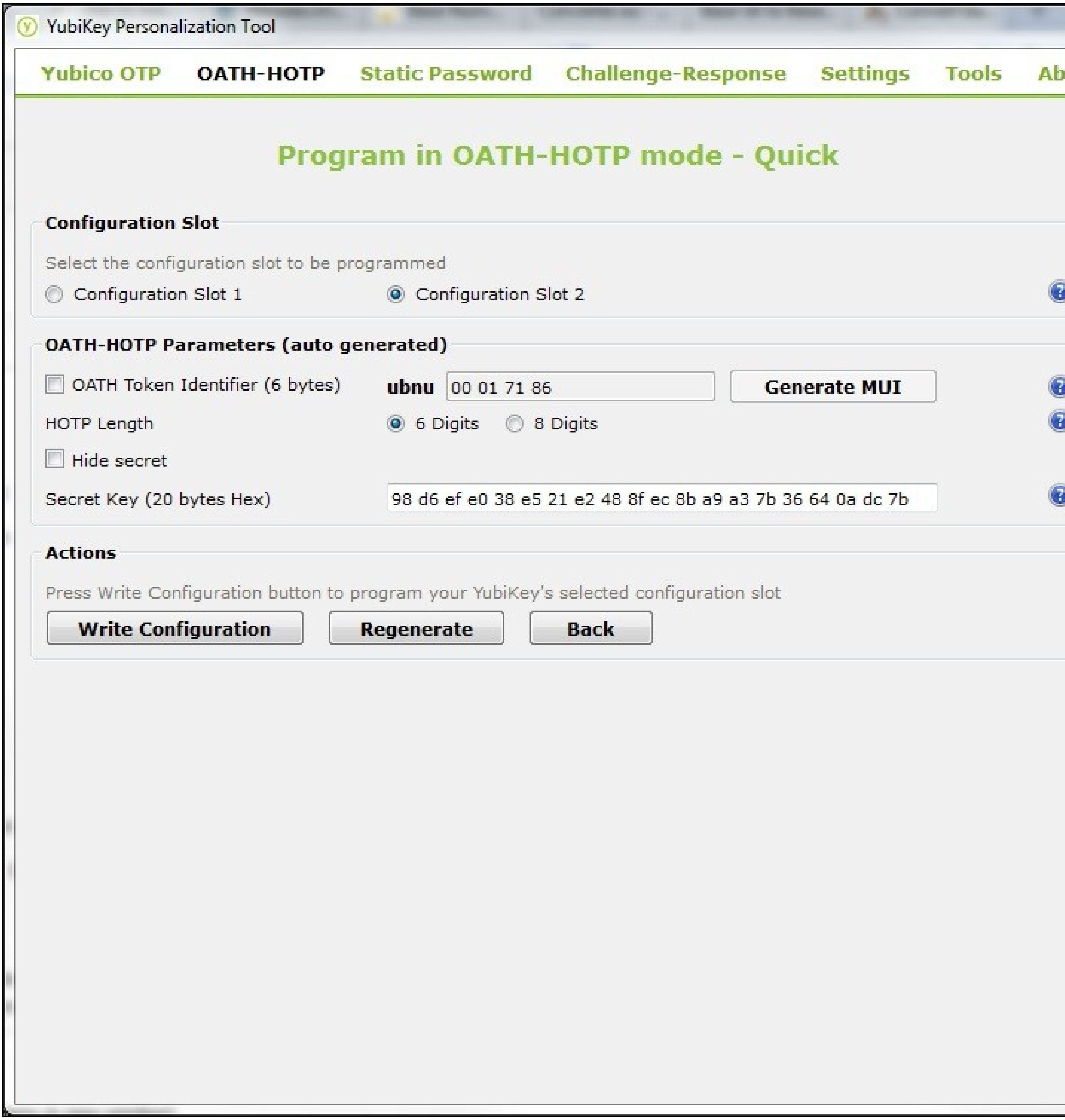
Configuration slot Configuration Slot 2

Oath-Token Identifier (6 bytes) uncheck

HOTP Length 6 digits

Hide Secret uncheck to copy seed

Then select the Action, Write Configuration



Program in OATH-HOTP mode - Quick

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

OATH-HOTP Parameters (auto generated)

□ OATH Token Identifier (6 bytes) **ubnu** 00 01 71 86

HOTP Length ● 6 Digits ○ 8 Digits

□ Hide secret

Secret Key (20 bytes Hex) 98 d6 ef e0 38 e5 21 e2 48 8f ec 8b a9 a3 7b 36 64 0a dc 7b

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

725 Configure the Swivel User

Swivel uses a Hexadecimal seed, generated on the yubikey programming tool. Copy the Seed from the programming tool, remove any spaces and add the seed as a hardware or software HOTP token on the Swivel Administration console, see Token.

When the seed has been assigned to a user, open a text editor such as Notepad, and press when the green light on the Yubikey is pressed, an OTC is generated on the Notepad. Generate two OTC to synchronise the token.

726 Testing

Open a text editor such as Notepad, and press when the green light on the Yubikey is pressed, an OTC is generated on the Notepad. The OTC can be used to test a user authentication.

727 Known Issues

728 Troubleshooting

TOKEN_BAD_SEED

Ensure spaces are removed when importing a seed.