

# Helpdesk Operations User Guide

## Contents

- 1 Overview
- 2 Prerequisites
- 3 Helpdesk login Guide
- 4 User Administration
  - ◆ 4.1 Help Desk Users
- 5 Helpdesk Operations Tasks
  - ◆ 5.1 Check user Status
  - ◆ 5.2 Check the Swivel log
  - ◆ 5.3 Send User a new PIN
  - ◆ 5.4 Reset a Users PIN
  - ◆ 5.5 Reset a Users Password
  - ◆ 5.6 Unlock an Account
  - ◆ 5.7 Disable or Enable an Account
  - ◆ 5.8 Send a security String
  - ◆ 5.9 View a users security String
  - ◆ 5.10 View a users transport
  - ◆ 5.11 Viewing User Attributes
  - ◆ 5.12 Purge Deleted Users
  - ◆ 5.13 Provision a mobile Phone Client
  - ◆ 5.14 View a users last login details
- 6 Known Issues
- 7 Troubleshooting User Issues
  - ◆ 7.1 User cannot login
  - ◆ 7.2 User is not receiving their security string
  - ◆ 7.3 User is not added to Swivel
  - ◆ 7.4 User forgets their PIN
  - ◆ 7.5 User must Change their PIN
  - ◆ 7.6 Loss/Replacement of Mobile Device
  - ◆ 7.7 User cannot provision a Mobile Device
  - ◆ 7.8 User deletes/loses their SMS security string
  - ◆ 7.9 User differences between Swivel instances
  - ◆ 7.10 Additional Symptoms

## 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.

## Prerequisites

Swivel 3.x

## 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](#)

## User Administration

### 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

admin	▲	✓	✓	✓	✓	✓	
Edit	Policy	Reset PIN	Reset Password	View Strings	Send String	Resend	
Reprovision	Lock	Delete	History				

# Helpdesk Operations Tasks

The following tasks are commonly carried out by helpdesk users

## 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.

## 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.

## 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.

## 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.

<b>Username</b>	graham
<b>New PIN</b>	<input type="text"/>
<b>Confirm New PIN</b>	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

## 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.

<b>Username</b>	graham
<b>New Password</b>	<input type="text"/>
<b>Confirm New Password</b>	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

## 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](#)

## 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.

## 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.

## 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](#)

## 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		Alert	
	Transport	Destination	Transport	
admin ▼	SMTP	support@swivelsecure.com	CM	00441234
graham ▼	CM	00441234567890	SMTP	g.field@sw
piduser ▼				

## Viewing User Attributes

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

Username	altusername	email	familyname	givenname
admin ▼				admin
graham ▼		g.field@swivelsecure.com	Field	Graham
support ▼		support@swivelsecure.com	Support	Swivel

## 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](#).

## 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.

## 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.

<b>Username:</b>	graham
<b>Created:</b>	12:02:30 16 July 2009
<b>Last login:</b>	12:10:12 16 July 2009
<b>Last PIN change:</b>	N/A
<b>Last self-reset:</b>	N/A
<b>Disabled:</b>	<input type="checkbox"/>
<b>Change PIN at first login:</b>	<input type="checkbox"/>
<b>PIN never expires:</b>	<input type="checkbox"/>
<div><div>Reset</div><div>OK</div><div>Apply</div><div>Cancel</div></div>	

## 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.

## Troubleshooting User Issues

### 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](#)

### 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](#)

## 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 synchronisation messages or messages that the license has been exceeded, see [Installing a license key](#).

See also [User Missing](#)

## 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](#)

## 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.

## 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](#)

## User cannot provision a Mobile Device

See [Mobile Phone Client](#)

## 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 single 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](#)

## 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).

## Additional Symptoms

The following additional [Symptoms](#) may occur