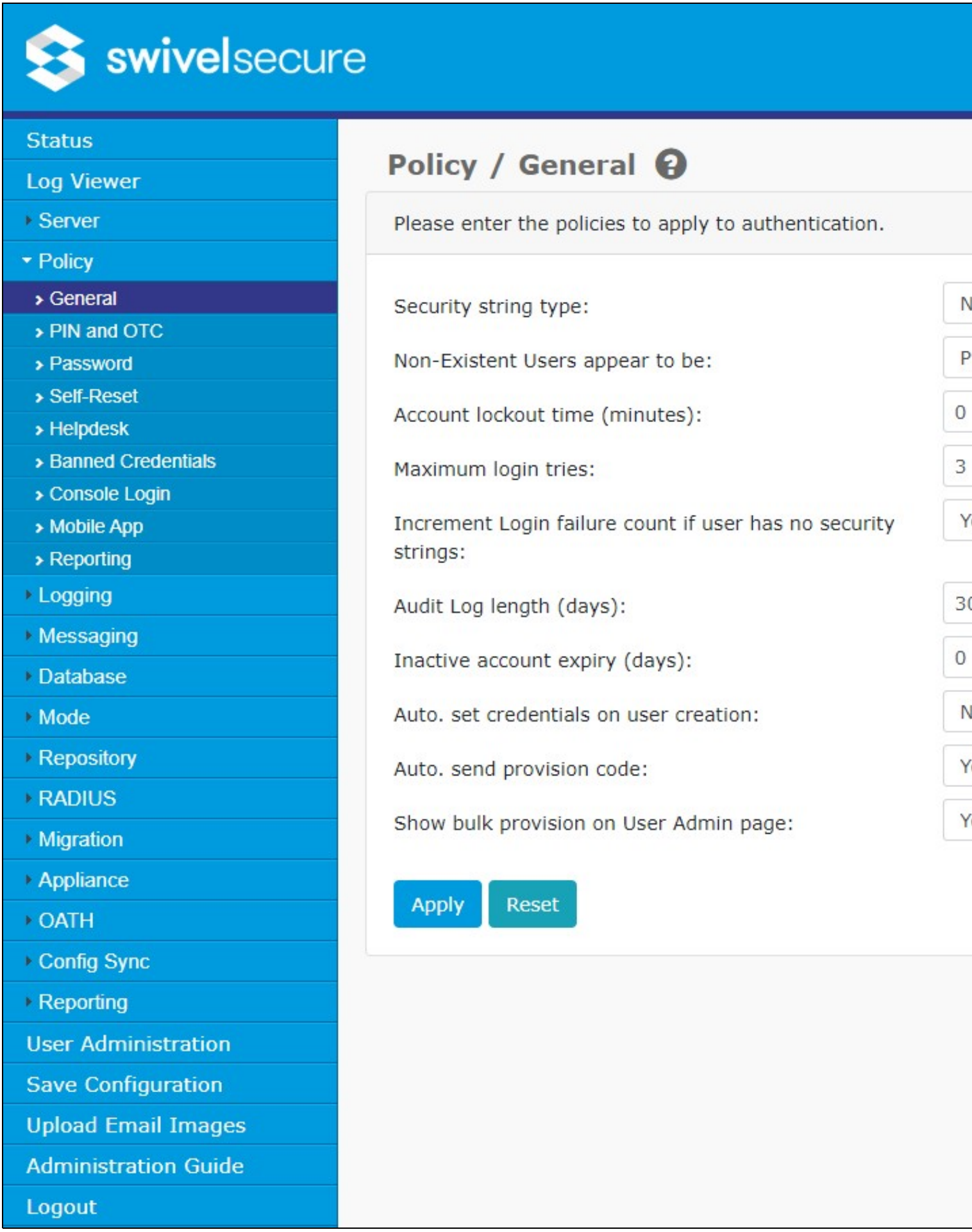
Swivel Core V4 Policy Menu

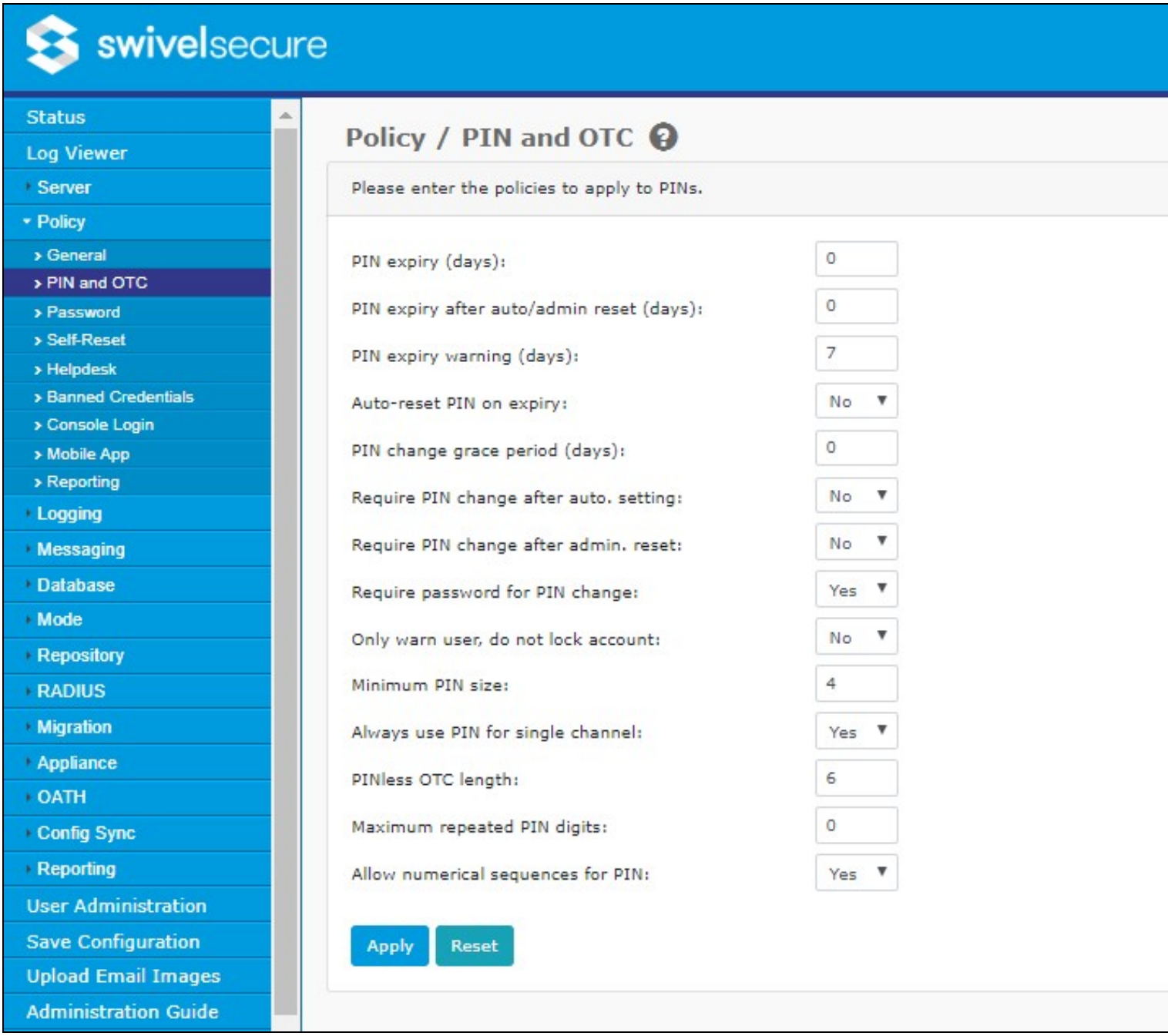
Contents

General


swivelsecure
Status
Log Viewer
Server
Policy
General
PIN and OTC
Password
Self-Reset
Helpdesk
Banned Credentials
Console Login
Mobile App
Reporting
Logging
Messaging
Database
Mode
Repository
RADIUS
Migration
Appliance
OATH
Config Sync
Reporting
User Administration
Save Configuration
Upload Email Images
Administration Guide
Logout
Policy / General
Please enter the policies to apply to authentication.
Security string type:
Non-Existent Users appear to be:
Account lockout time (minutes):
Maximum login tries:
Increment Login failure count if user has no security strings:
Audit Log length (days):
Inactive account expiry (days):
Auto. set credentials on user creation:
Auto. send provision code:
Show bulk provision on User Admin page:
Apply
Reset

- **Security string type**: Security strings can be comprised of numbers, upper case letters, lower case letter, mixed case letters or a mix of upper case letters and numbers.
- **Non-Existent Users appear to be**: When a TURing image is requested for a user that does not exist, Swivel will still produce an image. This is to prevent a hacker determining which usernames are valid accounts. You can specify the type of image that is presented when a image for a non-existent user is requested. Therefore if all your users have PINs you should set this to PINned. If all your users are PINless, this should be set to PINless and if you have a mixture of users you should set this value to mixed.
- **Account lockout time**: Specifies how long an account will be locked out in the event of too many failed authentications. The default is 0, which means the lock will remain until an administrator or helpdesk user unlocks the user. If a period is set then after that period the account will be usable again. Note, however, that the lock flag is not reset until the user attempts to authenticate, so users will still appear to be locked even after the lock time has expired.
- **Maximum login tries**: Maximum number of consecutive failed login attempts a user can make before their account is locked. Note that setting the maximum to a high value increases the risk of a brute force attack resulting in a successful authentication. It is not possible to enable infinite retries.
- **Increment Login failure count if user has no security strings**: This option effectively determines whether attempting a login without any valid security string counts as a failure.
- **Audit Log Length**: Swivel maintains an activity log for users. This setting determines how long this log is maintained. Entries older than this are removed by a scheduled job.
- **Inactive account expiry**: Maximum number of days for which an account may remain inactive before it will be automatically locked by the inactive user check job. 0 means that the account will never be locked due to inactivity.
- **Auto. set credentials on user creation**: Enable/disable the automatic creation and setting of user credentials when they are initially added to the user population. Note that users must be correctly associated with an alert transport in order for them to receive notification of their credentials.
- **Auto. send provision code**: If **Yes**, then new users will automatically be sent a provision code if they are configured as mobile app users and have a valid alert transport.
- **Show bulk provision on User Admin page**: This option controls whether the bulk provision feature is enabled. This feature will send a new provision code to everyone that is not currently provisioned or has a valid pending provision code, is configured a mobile user, and has a valid alert transport.

PIN and OTC



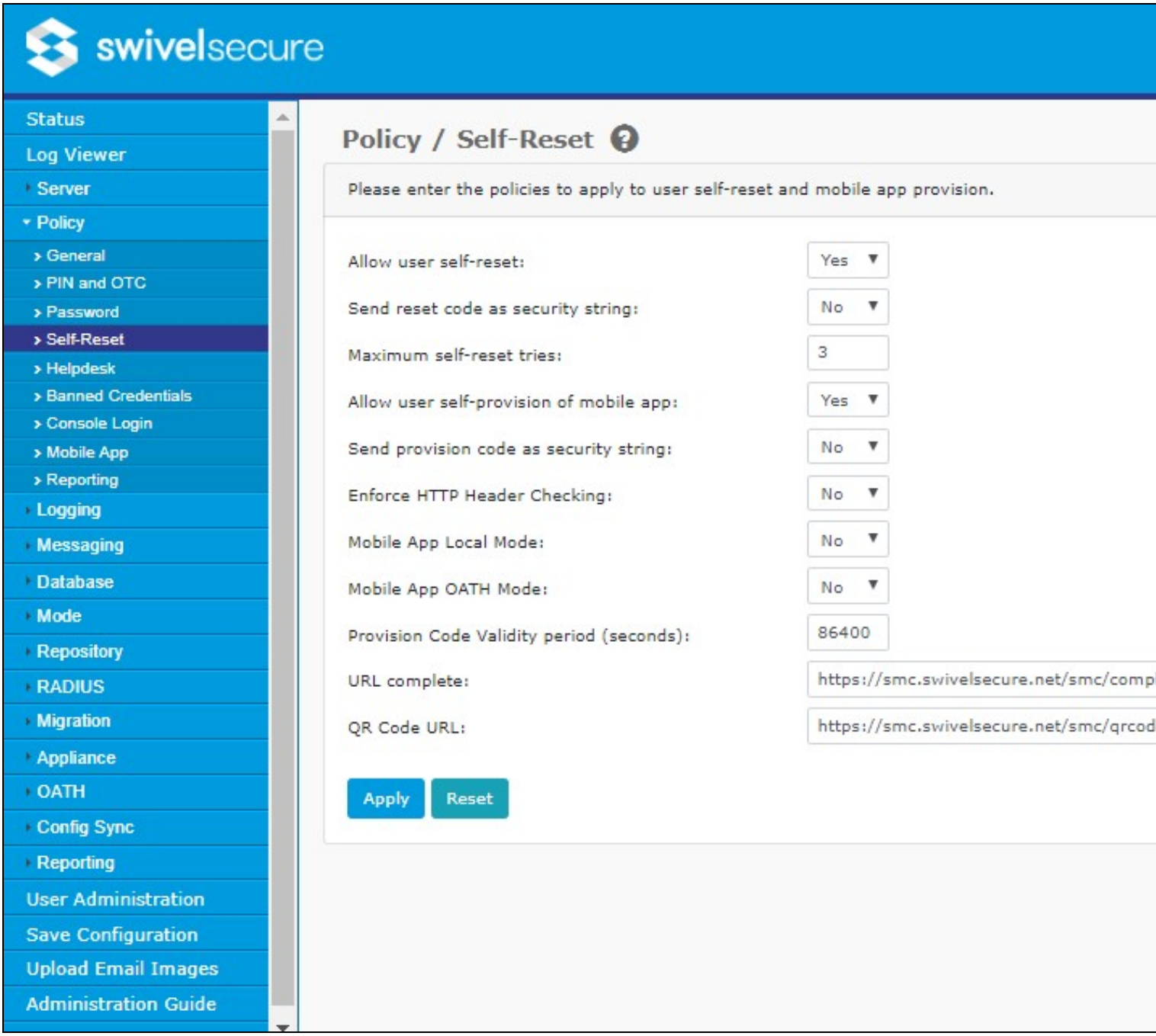
- **PIN expiry**: Maximum number of days for which a PIN may be used. This policy is enforced both at the point of authentication and by the PIN expiry check job. In both cases the account will be locked if the number of days since the PIN was set exceeds the maximum. 0 means that the PIN never expires.
- **PIN expiry after auto/admin reset**: this sets the length of time a user has to change their PIN after it has been set by an admin/helpdesk user, or reset automatically.
- **PIN expiry warning**: Number of days for which the user will be warned about the imminent expiry of their PIN. Users may be informed of the imminent expiry via alerts sent by the PIN expiry check job or by an agent that supports the display of warnings to the user.
- **Auto-reset PIN on expiry**: If **Yes**, then the user's PIN will automatically be reset at the time their PIN would expire, if the user has an alert transport configured. If this is set to **No**, the user's account will become locked when their PIN expires.
- **PIN change grace period**: This sets the length of time a user has to change their PIN after being unlocked. This only applies to PINs set by admin/helpdesk users.
- **Require PIN change after auto. setting**: Enable/disable 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.
- **Require PIN change after admin. reset**: Enable/disable the requirement for a user to change their PIN following a reset performed by an administrator. The user may be informed of this requirement via an alert or by an agent that supports the display of warnings to the user.
- **Require password for PIN change**: If **Yes**, and a Swivel password is set, then the user must provide their password when changing their PIN. If **No**, then the PIN can be changed knowing only the current PIN, even if the user has a password.
- **Only warn user, do not lock account**: If **Yes**, then users are never locked when policy dictates, they are only sent a warning message.
- **Minimum PIN size**: Minimum number of digits that a user's PIN must contain. Values between 4 and 10 inclusive are allowed.
- **Always use PIN for single channel**: If **Yes**, then even if a user is designated as PINless, they are allocated a PIN for single channel authentication. Only dual channel is PINless in this case.
- **PINless OTC length**: If a user has been configured to work without a PIN, this field dictates the length of the one-time code they are sent. Valid values are from 4 to 8.
- **Maximum Repeated PIN Digits**: This sets the policy for PINs and how many repeated digits are allowed. When set to 0 it means that the all digits in the PIN must be different. A setting of one means that a single repeat is allowed, e.g. 3783. If the number of repeated digits equals the PIN length then there is no restriction on repeated digits.

- **Allow numerical sequences**: This determines whether sequences such as 1234, 3579, 8642 are allowed as PINs.

Password

- **Require password**: Enable/disable the requirement for a user to have a static password in addition to their PIN. Note that enabling this setting only affects the automatic setting of credentials, where it will result in a password being created in addition to a PIN. Enabling this option when existing users do not have a password will not result in them failing subsequent authentications. However, once this policy is enabled, whenever a user subsequently changes their PIN, they will be required to set a password as well.
- **Password mask**: Mask that Swivel will use to create passwords. The password mask uses the following definitions, a = letter, d = digit, s = special character, x = any character. This is only used for automatic password generation - it does not impose the pattern on user-created passwords.
- **Show 'Reset Password' on User Admin page**: This option controls whether the **Reset Password** button is displayed for each user. As relatively few installations use Swivel passwords, the existence of this button has caused confusion for many customers, and it is a common occurrence that the user's Password is reset, rather than their PIN, resulting in authentication failures. Therefore, by default, this button is no longer shown. However, if this option is disabled, and any users have passwords, it will not be possible to change them using the admin console.

Self-Reset



- **Allow user self-reset**: Enable/disable the ability of users to perform a self-reset. When enabled, users given access to a suitable agent will be permitted to reset their PIN without the involvement of an administrator. Following submission of their username the user will be sent an alert containing a one-time reset code.
- **Send reset code as security string**: Alerts are typically sent via email (alert transport). However you may wish to restrict reset codes to a specific device by sending them to a specific device, like a security string.
- **Maximum self-reset tries**: Maximum number of consecutive failed self-reset attempts a user can make before their account is locked. Setting this value to '0' allows infinite attempts.
- **Allow user self-provision of mobile app**: Enable/disable the ability of users to perform a self-provision. When enabled users given access to a suitable agent will be permitted to reprovision their mobile by requesting a new mobile client provision code.
- **Send provision code as security string**: Alerts are typically sent via email (alert transport). However you may wish to restrict provision codes to a specific device by sending them to a specific device, like a security string.
- **Enforce HTTP Header Checking**: If **Yes**, then Swivel will check certain HTTP headers sent from the Mobile app, to confirm that request is sent from the same phone as previous requests.
- **Mobile App Local Mode**: If **Yes**, then the mobile app is sent a unique code that makes it capable of generating its own security strings, and so does not need to refer to the Swivel server to retrieve new strings.
- **Mobile App OATH Mode**: If **Yes**, then mobile apps will be provisioned with a unique OATH seed, allowing them to be used to perform OATH authentication. The phone then becomes a so-called "soft token".

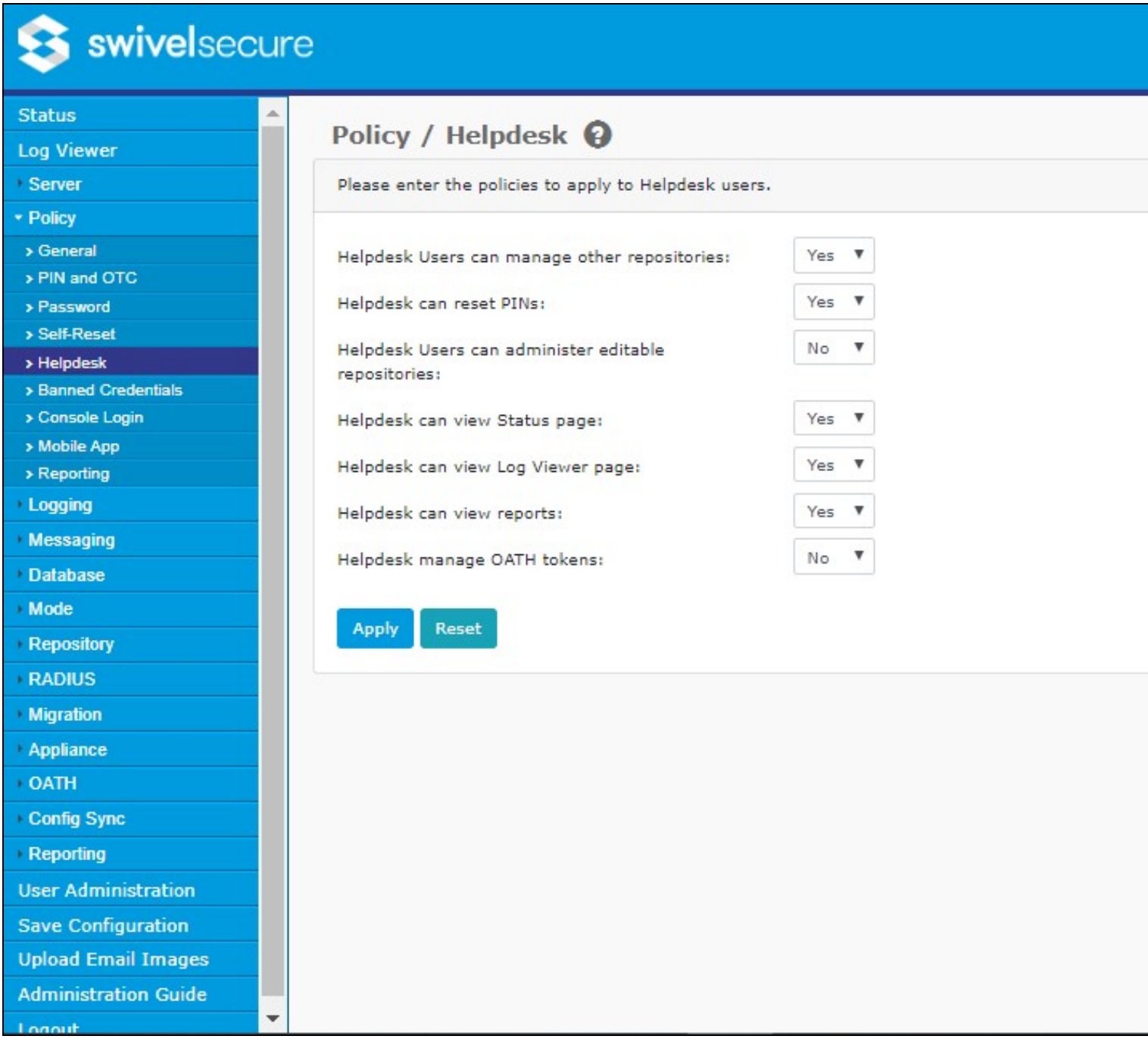
Allow user self-provision: Enable/disable the ability of users to perform a self-provision. When enabled users given access to a suitable agent will be permitted to reprovision their mobile by requesting a new mobile client provision code

- **Provision Code Validity period**: determines how long a provision code is valid. This value is measured in seconds, so the default of 86400 is equivalent to 1 day.
- **URL provisioning**: Contains the URL to the Swivel Mobile Connector application that allows automatic provision of the mobile app.
- **URL to get settings**: Contains the URL to the Swivel Mobile Connector application that allows the mobile app to get configuration settings automatically.

- **URL complete**: Contains the URL to the Swivel Mobile Connector application that allows both automatic provision of the mobile app and get configuration settings.
- **QR Code URL**: Contains the URL to the Swivel Mobile Connector application that generates a QR code.

NOTE: the last 4 URLs are set by Swivel, and should not be modified unless you are advised to do so by Swivel or your reseller.

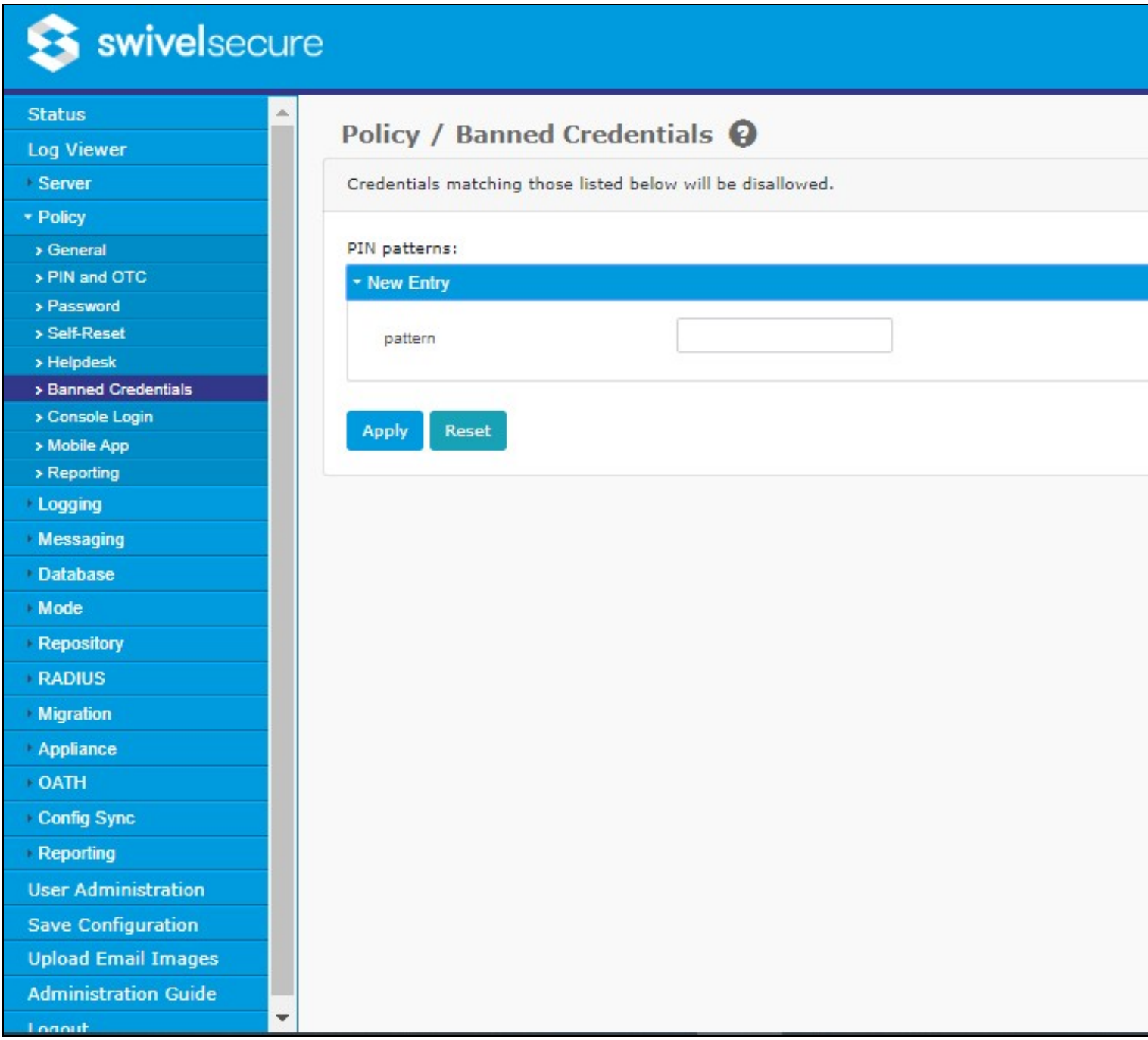
Helpdesk



These options determine what abilities helpdesk users (as opposed to administrators) have. Most of these options are self-explanatory, but some explanation may be useful in some cases:

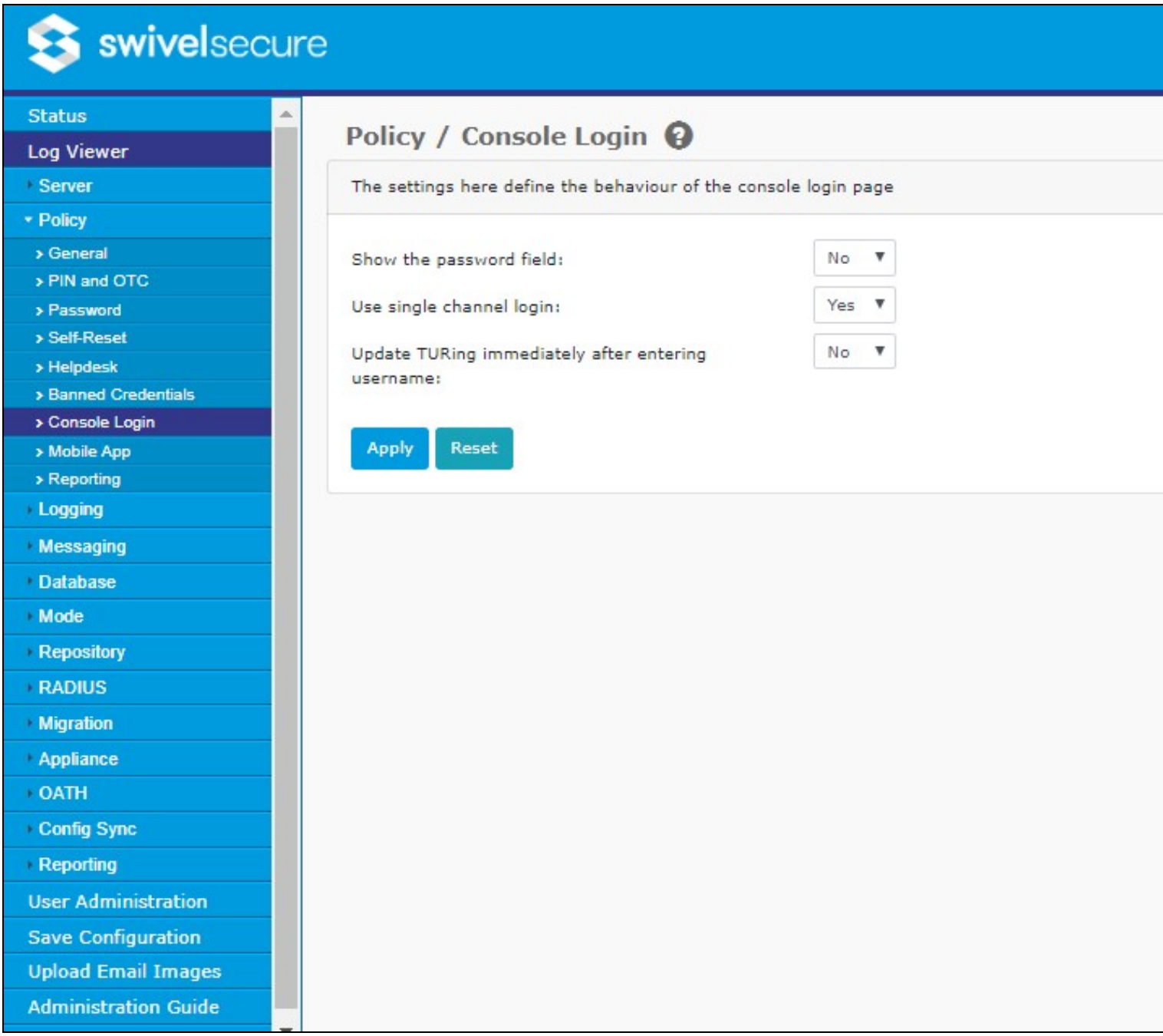
- **Helpdesk Users can manage other repositories**: If this is **No**, then helpdesk users can only manage users from the same repository as they belong to. If **Yes**, then helpdesk users can manage users from other repositories as well. Note that you can apply greater control over which helpdesk groups can manage which other groups by using the Repository Helpdesk Groups feature.
- **Helpdesk Users can administer editable repositories**: Editable repository types are XML, ADAM and Writeable LDAP. If this is enabled, then helpdesk users are allowed to create and delete users in these repositories. If not, they can only manage existing users.

Banned Credentials



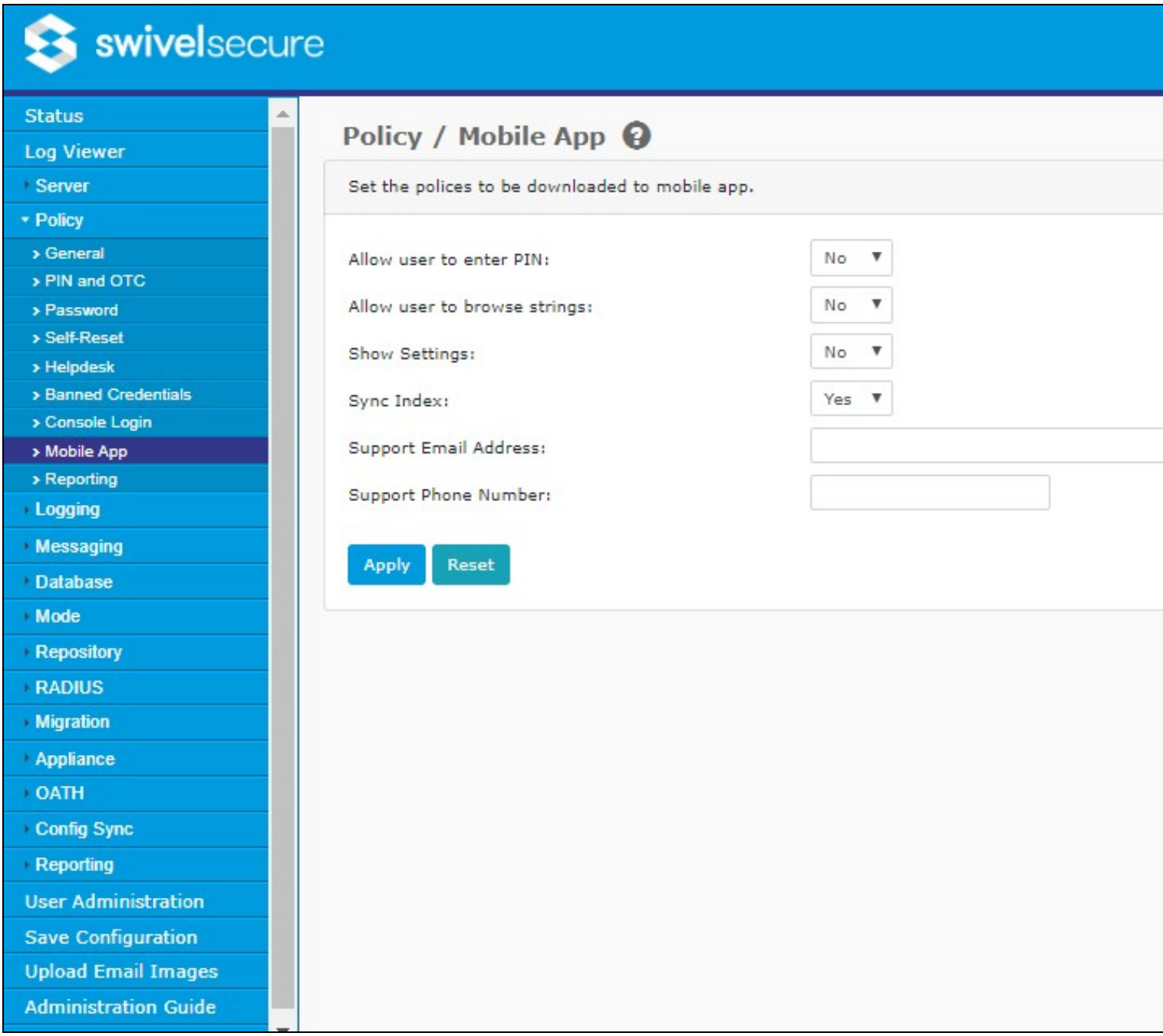
You can specify any number of PIN patterns that are not permitted. For example, *19??* will prevent users from specifying any year from the 20th century as a PIN.

Console Login



- **Show the password field**: Use this option to show or hide the password field on the Swivel administration console login page.
- **Use Single Channel login**: Use this option to show or hide the Start Session button, and hence the TURing image. If this option is set to **No**, it is assumed that you will be using dual channel security strings.
- **Update TURing immediately after entering username**: Use this option to enable or disable automatic display of TURing image after entering the username. The Single Channel option must also be enabled for this option to be effective. If this option is set to **No**, but Single Channel is enabled, you must click the "Start Session" button to display a TURing image.

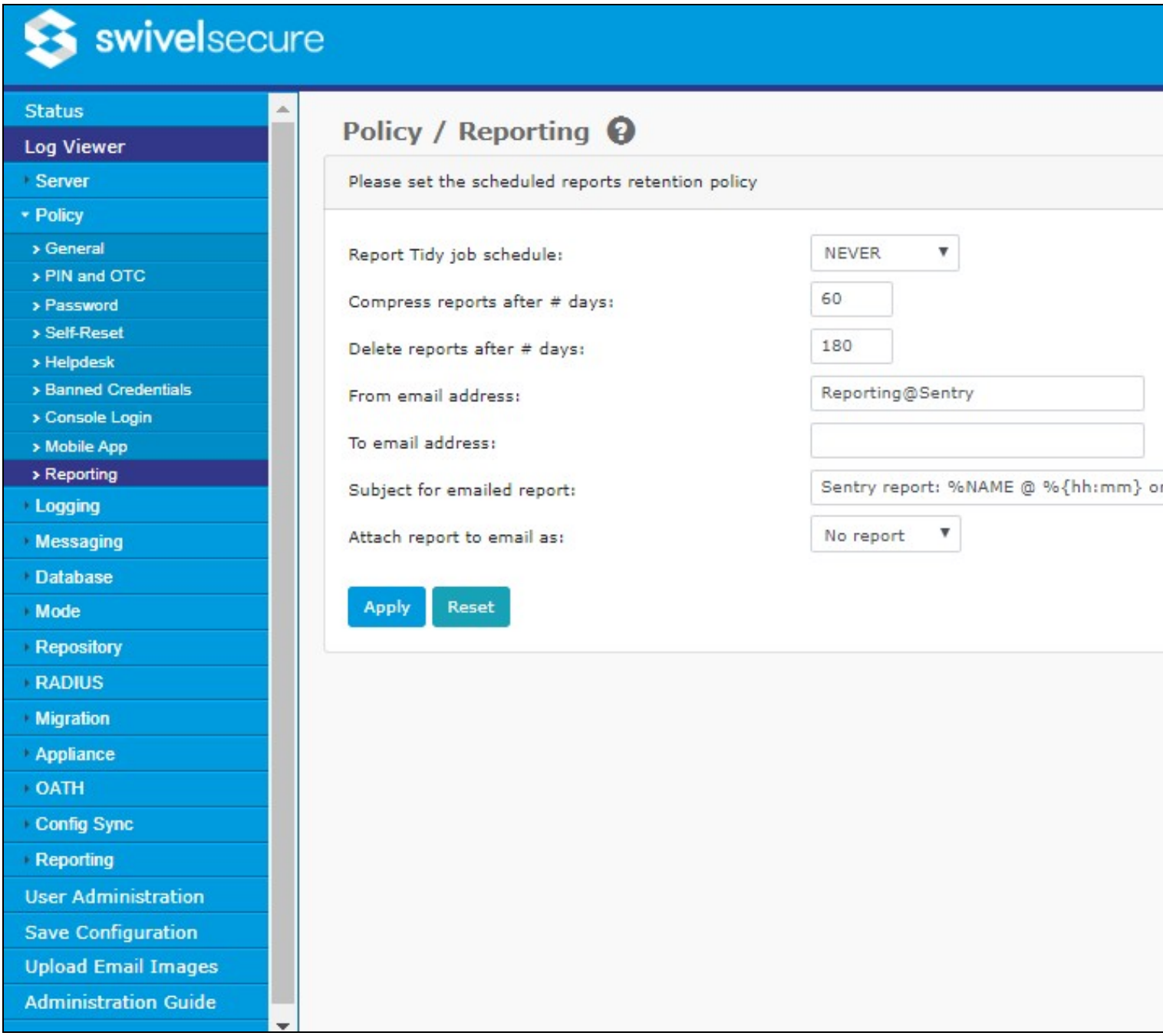
Mobile App



This page contains settings that relate to the Swivel Mobile App.

- **Allow user to enter PIN**: If **Yes**, then the user can enter their PIN directly in the mobile app, and it will display their required one-time code. If **No**, then the mobile app will display the next security string and the user must calculate their one-time code from that.
- **Allow user to choose how to extract OTC** (Deprecated since 4.0.5): If **Yes**, and the above option is also **Yes**, then the user has the choice of entering their PIN directly or viewing the one-time code.
- **Allow user to browse strings**: If **Yes**, then the mobile app will display buttons allowing the user to view previous or later security strings. If **No**, then only the current string will be shown.
- **Provision is numeric** (Deprecated since 4.0.5): If **Yes**, then the generated provision code will always be numeric. If **No**, the provision code will use the character set defined under Policy -> General. Since provisioning is usually automatic now, this option is largely irrelevant.
- **Show Settings**: Determines whether or not the mobile app allows the user to view and change their settings.
- **Sync Index**: If enabled, the mobile app automatically synchronizes the security string index with the Swivel server. This requires connection to the server.
- **Support Email Address**: if specified, the mobile app will display this email address for support from their company.
- **Support Phone Number**: if specified, the mobile app will display this phone number for support from their company.
- **VPN URL Scheme** (Deprecated since 4.0.5): this feature is not currently used.

Reporting



These settings determine how scheduled reports are managed.

- **Report Tidy job schedule**: determines when the job to clear down old reports is run. See Scheduled Jobs for more information on setting scheduled tasks.
- **Compress reports after # days**: when the report tidy job runs, determines how long reports are kept before being compressed (zipped).
- **Delete reports after # days**: when the report tidy job runs, determines how long reports are kept before being deleted.
- **From email address**: sets the email address that reports appear to come from.
- **To email address**: sets the email address that scheduled reports are sent to.
- **Subject for emailed report**: sets the subject line for emailed scheduled reports. The following place holders can be used:
  - *%NAME* - the name of the report.
  - *%{hh:mm}* - the time the report was generated.
  - *%{dd/MM/yyyy}* - the date the report was generated. Note that you can change the date format, and that month uses capital M, as opposed to lowercase m for minutes.
- **Attach report to email as**: determines how the report should be emailed: within the email body, as an attachment, or as a zipped attachment.