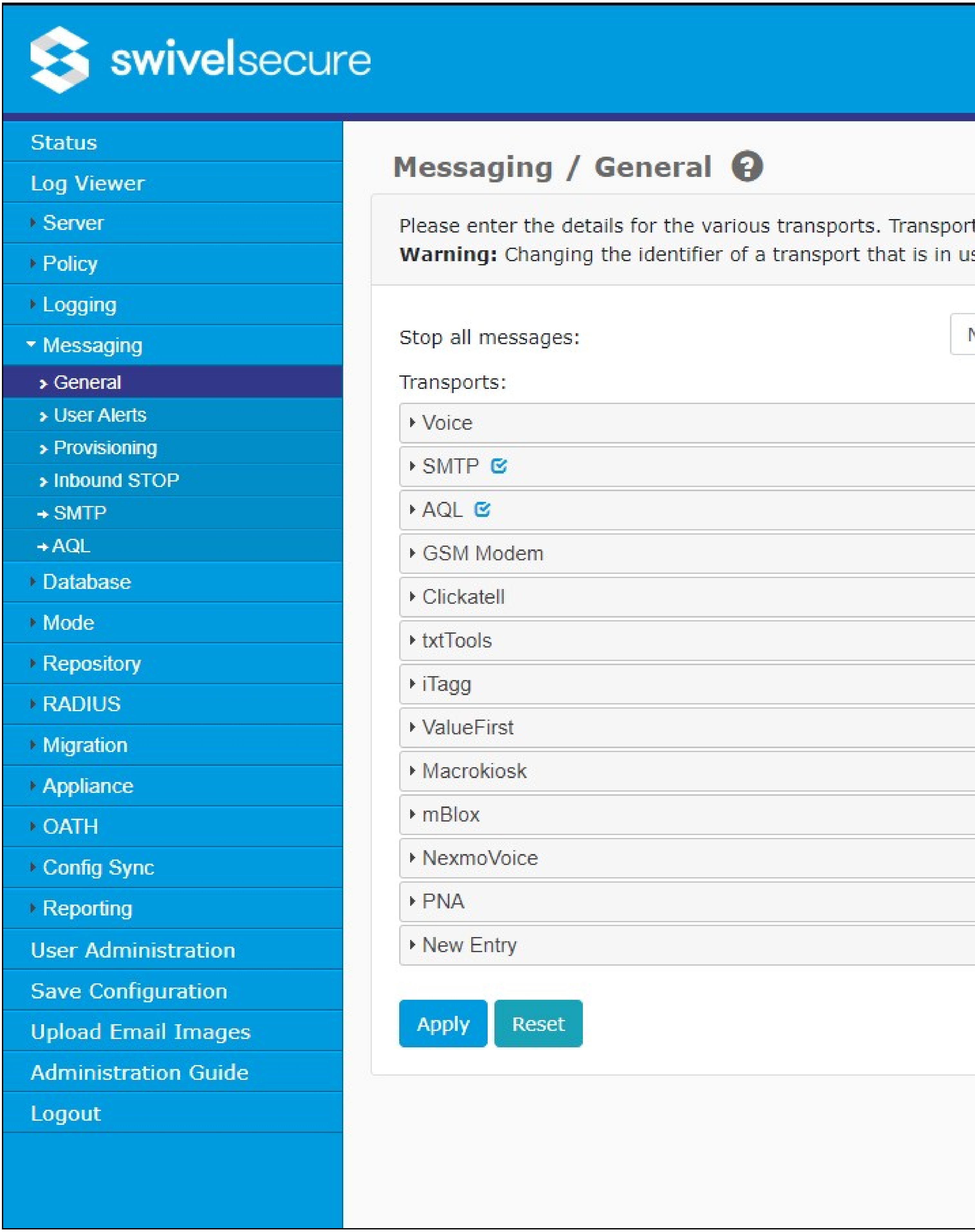
Table of Contents

1 Swivel Core V4 Messaging Menu

1.1 General



Messaging / General

Please enter the details for the various transports. Transport

Warning: Changing the identifier of a transport that is in us

Stop all messages: N

Transports:

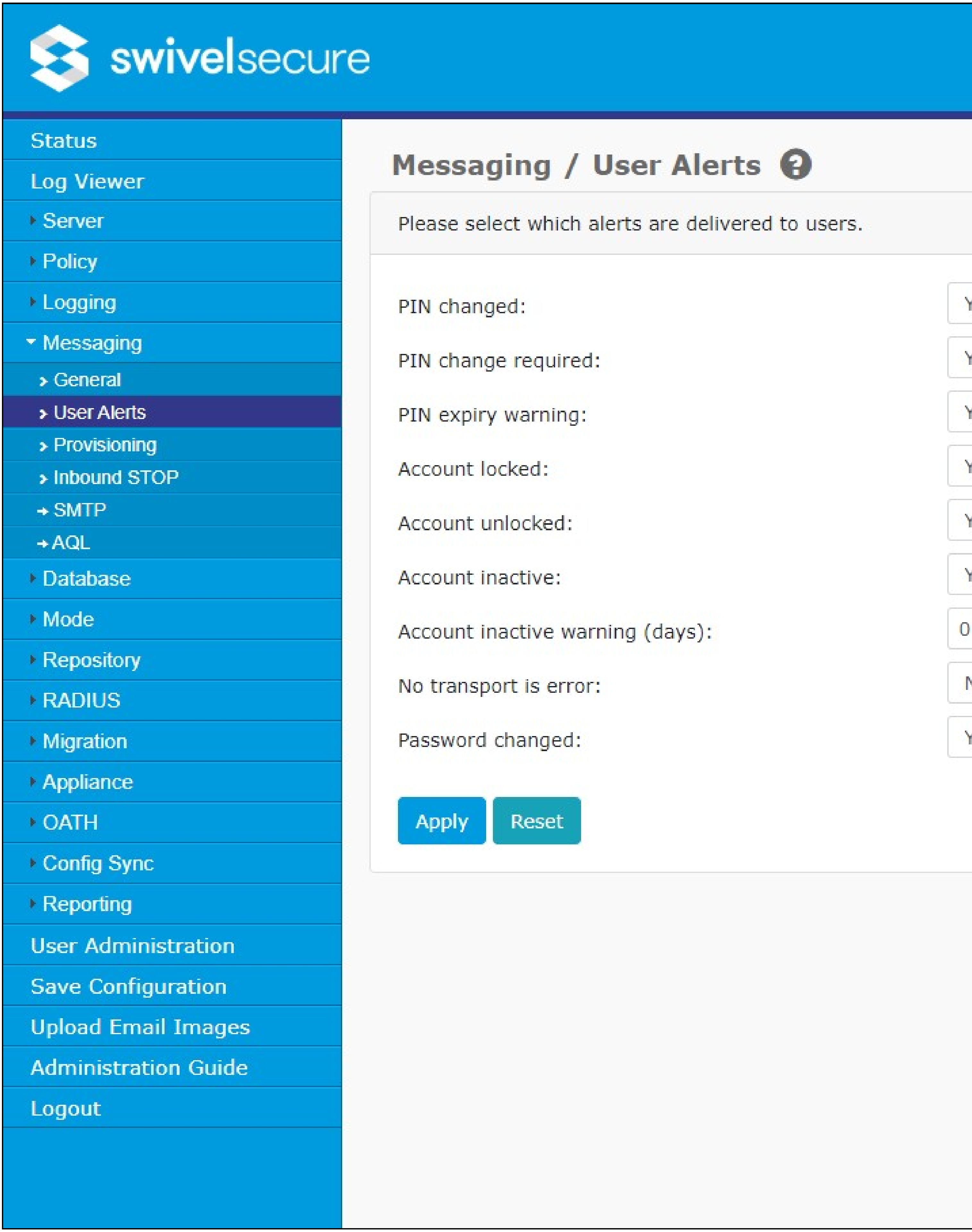
For each configured messaging type:

- **Identifier**: Friendly name to uniquely identify the messaging from others in the list.
- **Class**: Name of the Java class that implements the messaging type.
- **Strings per message**: Number of security strings that will be sent in each message. Copy to alert messaging This allows the security strings set using this Transport to be also copied to a users alert messaging. This is for deployments where users may need to be sent strings via one messaging in certain circumstances and another under other circumstances
- **Destination attribute**: User repository attribute to be used as the destination for messages sent via the messaging type. The destination attributes are defined for each repository on the Transports-Attributes screen.
- **Strings Repository group**: User repository group whose members will receive security strings messages via the messaging type. Users should only be a member of a single messaging repository group, as otherwise they may receive messages via different messaging types in an unpredictable manner.
- **Alert repository group**: User repository group whose members will receive alert messages via the messaging type. This may be the same as the repository group if it desired that users receive security strings and alerts via the same messaging type. Users should only be a member of a single alert repository group, as otherwise they may receive alert message via different messaging types in an unpredictable manner.
- **Push repository group**: User repository group whose members will receive Push messages via the messaging type.
- **Voice repository group**: User repository group whose members will receive interact Voice messages via the messaging type.

Multiple messaging types using a single class can be created by cutting and pasting the class name (e.g. com.swiveltechnologies.transport.SmtpTransport) to another entry and filling the remaining fields.

Configuration for individual messaging types will only become available in the left hand menu once it has been associated with a repository group.

1.2 User Alerts



Messaging / User Alerts

Please select which alerts are delivered to users.

PIN changed: Y

PIN change required: Y

PIN expiry warning: Y

Account locked: Y

Account unlocked: Y

Account inactive: Y

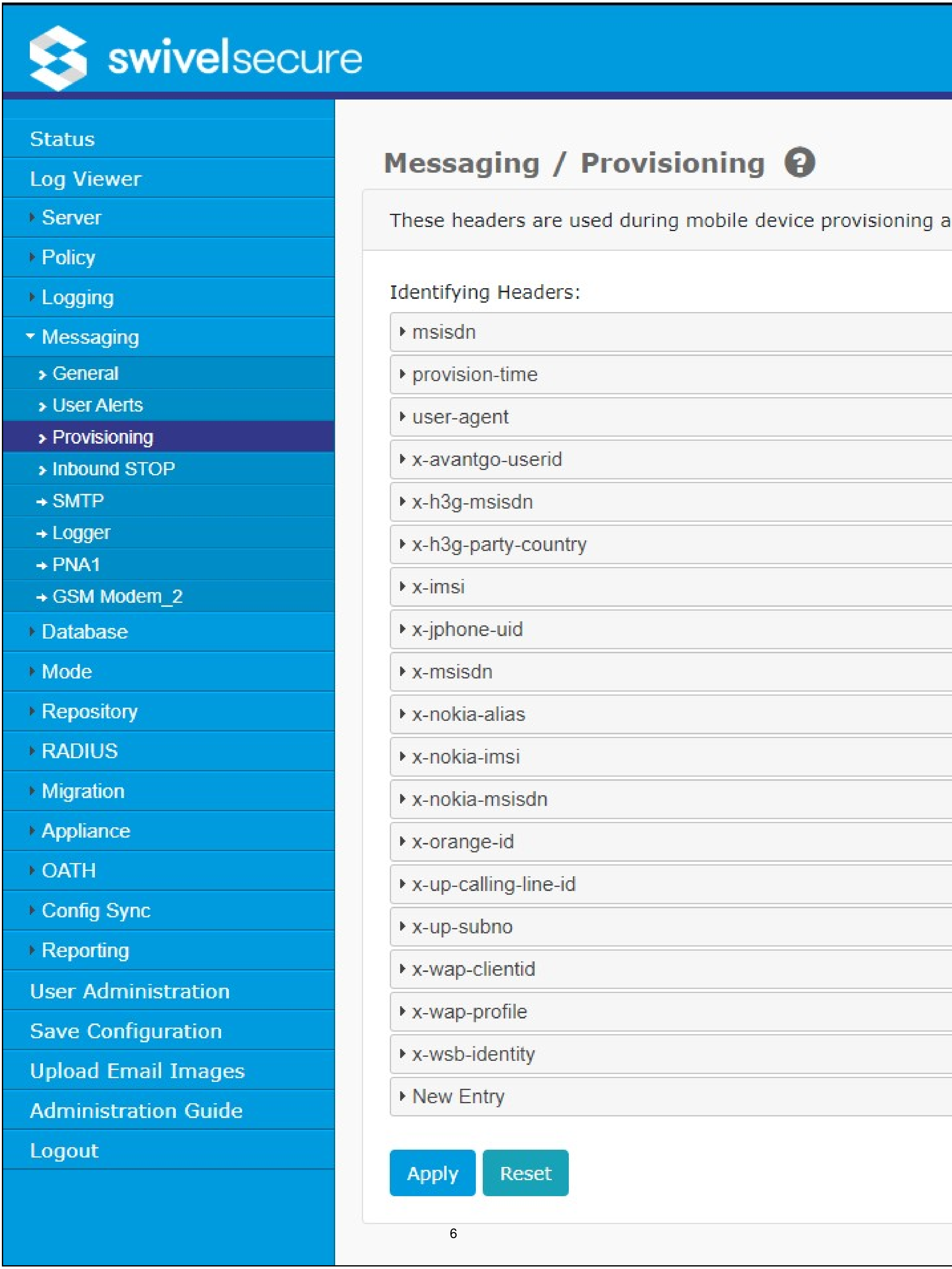
Account inactive warning (days): 0

No transport is error: N

Password changed: Y

- **PIN changed**: Enable/disable the sending of alerts informing users that their PIN has been changed.
- **PIN change required**: Enable/disable the sending of alerts informing a user that they must change their PIN before their next authentication.
- **PIN expiry warning**: Enable/disable the sending of alerts informing a user that their PIN is about to expire.
- **Account locked**: Enable/disable the sending of alerts informing a user that their account has been locked.
- **Account unlocked**: Enable/disable the sending of alerts informing a user that their account has been unlocked.
- **Account inactive**: Enable/disable the sending of alerts informing a user that their account has been inactive.
- **Account inactive warning(days)**: Enable/disable the sending of alerts informing a user that their account is going to get inactive in # days.
- **Device key allocated**: Enable/disable the sending of alerts informing a user of the allocation of a PositiveID device key.
- **No transport is error**: Normally, if a user has no transport attribute, it is logged as a warning. However, if that attribute is set to yes then it is logged as an error - mainly so it would trigger the audit report
- **Password changed**: Enable/disable the sending of alerts informing users that their Password has been changed.

1.3 Provisioning



Messaging / Provisioning

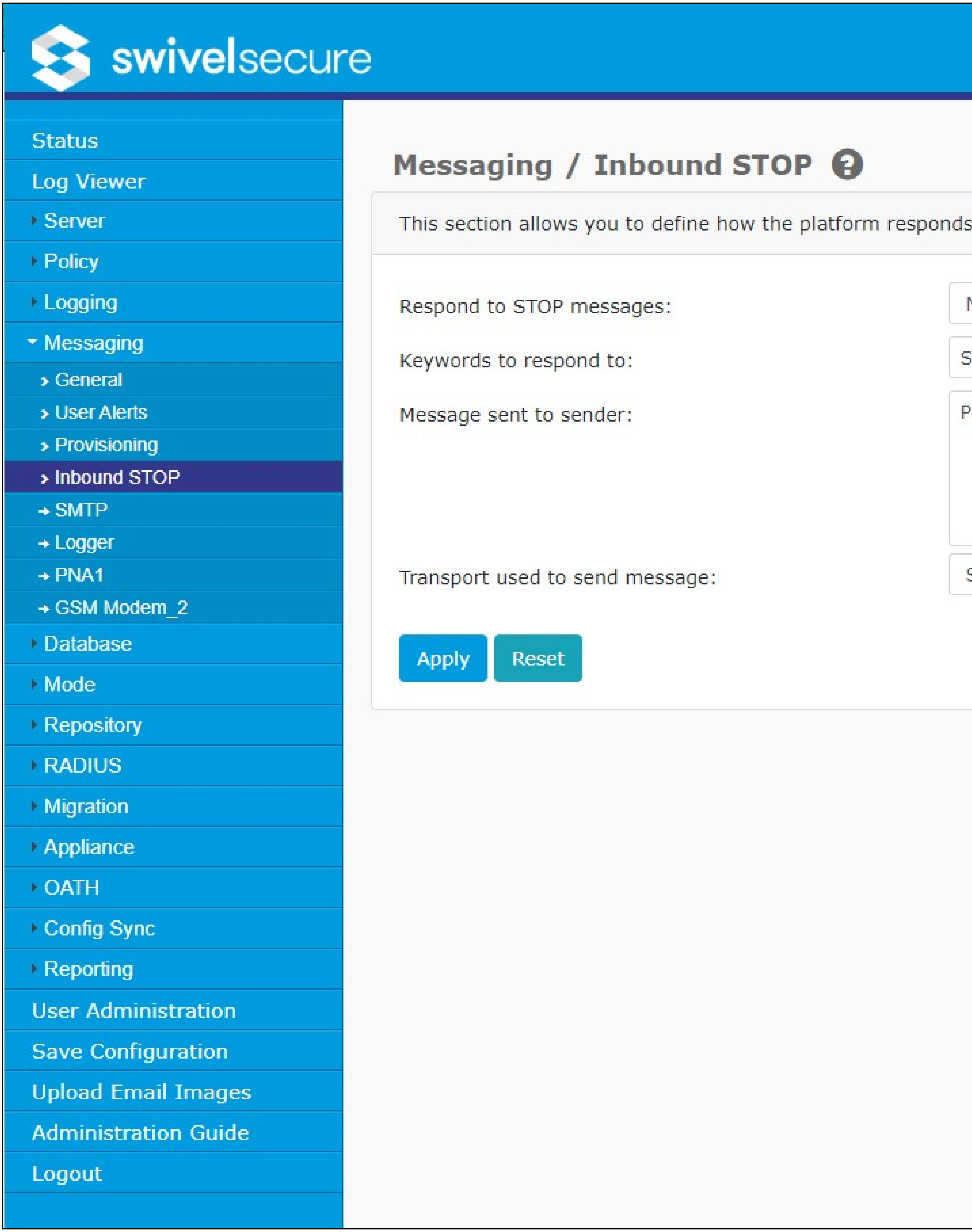
These headers are used during mobile device provisioning a

Identifying Headers:

- msisdn
- provision-time
- user-agent
- x-avantgo-userid
- x-h3g-msisdn
- x-h3g-party-country
- x-imsi
- x-jphone-uid
- x-msisdn
- x-nokia-alias
- x-nokia-imsi
- x-nokia-msisdn
- x-orange-id
- x-up-calling-line-id
- x-up-subno
- x-wap-clientid
- x-wap-profile
- x-wsb-identity
- New Entry

These headers are used during mobile app provisioning and on the updating keys process just if the policy 'Enforce HTTP Header Checking' on Self-Reset section is set to yes. These headers help to uniquely identify a particular mobile device.

1.4 Inbound STOP



Messaging / Inbound STOP

This section allows you to define how the platform responds

Respond to STOP messages: N

Keywords to respond to: S

Message sent to sender: P

Transport used to send message: S

- **Respond to STOP messages**: Indicates if the platform needs to respond when it receives a message with the keyword indicated on the next attribute.
- **Keywords to respond to**: Allows to define the keyword by default is set to STOP.
- **Message sent to sender**: Message that will be sent as a respond of those kind of messages
- **Transport used to send message**: SMTP

1.5 Messaging Common Attributes

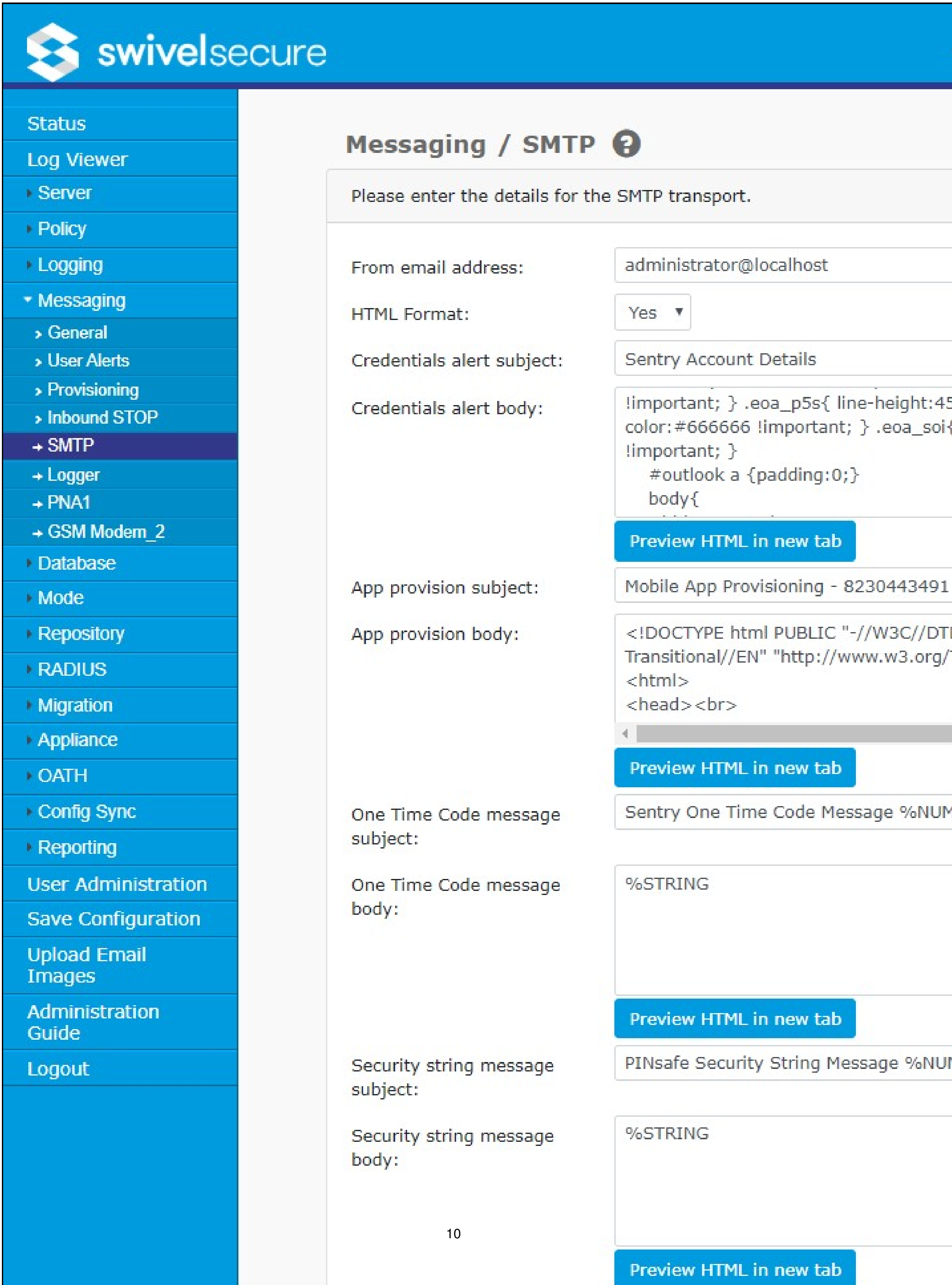
Once a messaging type has been allocated to a group, the specific messaging can be configured. Configuration items will be specific for each transport but some are common across most or all transports and those are related to how the messages will be formatted.

- **Credentials alert message**: Text to use for new credential alert messages sent to users. If the text contains "%NAME" this will be replaces with the user's username. If the text contains "%PASSWORD" this will be replaced with the user's new password. If the text contains "%PIN" this will be replaced with the user's new PIN.
- **App Provision Message**: Text to use for provisioning the mobile app sent to users. If the text contains "%CODE" this will be replaces with the provisioning code. If the text contains "%URL_COMPLETE%SITE_ID/%NAME/%CODE" this will be replaced with URL to provision the device automatically.
- **Security string message header**: Text to use as the header at the beginning of security string messages. If the text contains "%NUMBER" this will be replaced with the number of the security string message, which is useful for user identification of the most recent message received from Swivel.
- **String Delimeter**: An optional character or characters that can be used to separate the individual characters within a security string, for example "->"

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

- **Vertical Strings**: Allows strings to be displayed vertically, this makes them easier to read on certain smart phones
- **PIN expiry alert message**: Text to use for PIN expiry alert messages. If the text contains "%DAYS" this will be replaces with the number of days until the PIN will expiry.
- **PIN change required alert message**: Text to use for PIN change required alert messages.
- **PIN changed alert message**: Text to use for PIN changed alert messages. If the text contains "%TIME" this will be replaced with the time and date at which the change occured.
- **Account locked alert message**: Text to use for account locked alert messages. If the text contains "%TIME" this will be replaced with the time and date at which the lock occured.
- **Account inactive alert message**: Text to use for account inactive alert messages.
- **Account lock warning**: Text to use for account lock warning alert messages. If the text contains "%DAYS" this will be replaced with the days when the user account will get inactive.
- **Reset code alert message**: Text to use for reset code alert messages. If the text contains "%CODE" this will be replaced with the self-reset code.

1.6 SMTP



Messaging / SMTP

Please enter the details for the SMTP transport.

From email address: administrator@localhost

HTML Format: Yes

Credentials alert subject: Sentry Account Details

Credentials alert body:

```
!important; } .eoa_p5s{ line-height:45
color:#666666 !important; } .eoa_soi{
!important; }
   #outlook a {padding:0;}
   body{
```

App provision subject: Mobile App Provisioning - 8230443491

App provision body:

```
<!DOCTYPE html PUBLIC "-//W3C//DTI
Transitional//EN" "http://www.w3.org/
<html>
<head><br>
```

One Time Code message subject: Sentry One Time Code Message %NUM

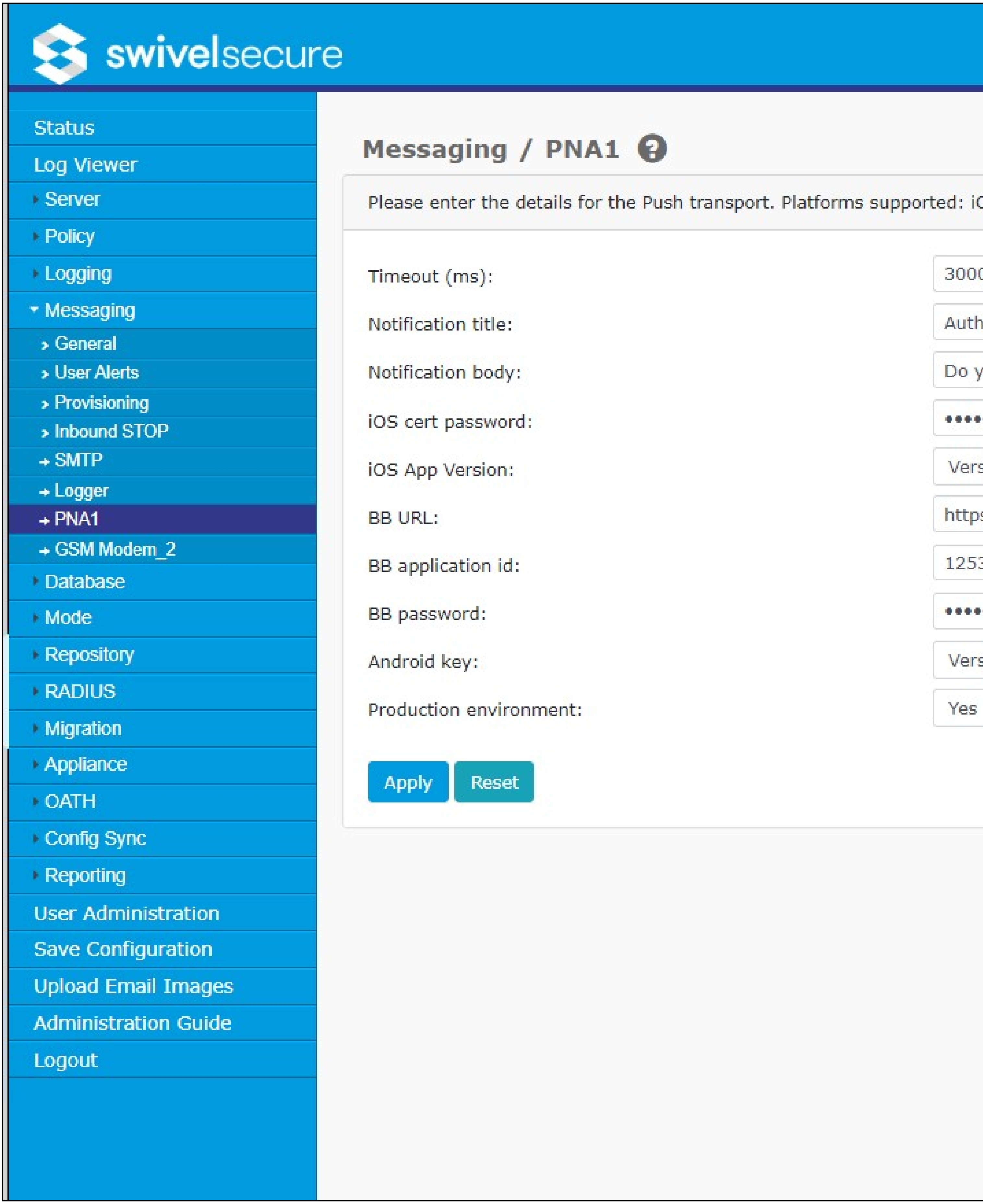
One Time Code message body: %STRING

Security string message subject: PINsafe Security String Message %NUI

Security string message body: %STRING

Please go to Messaging Common Attributes section to revised the different kind of messages that can be sent. SMTP also allows you to specify the email subject and the email from address. In addition it allows to indicate if the format is HTML. Credential and Provisioning App messages for SMTP have been defined with HTML templates by default so that attribute needs to be set to yes to be able to display them correctly. The images used on the SMTP templates can be updated from the Upload Email Images menu. To link a image on the SMTP template the attribute %BASE_URL is used. This attribute will be replaced by the value defined on the Base URL attribute on Server > Name section.

1.7 PNA



Messaging / PNA1

Please enter the details for the Push transport. Platforms supported: iO

Timeout (ms): 3000

Notification title: Auth

Notification body: Do y

iOS cert password: ••••

iOS App Version: Vers

BB URL: https

BB application id: 1253

BB password: ••••

Android key: Vers

Production environment: Yes

- **Timeout (ms)**: 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.

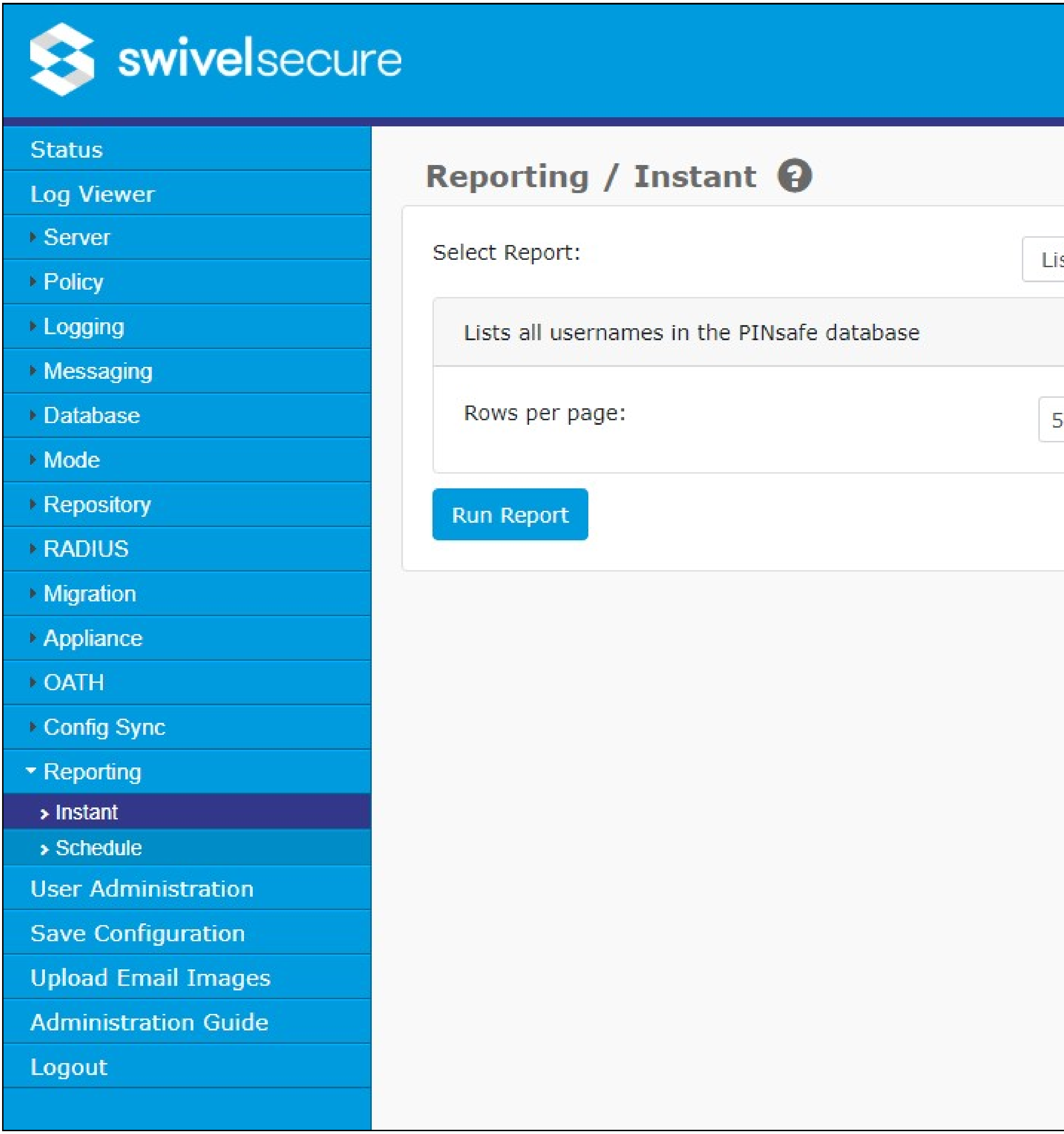
- **Notification title**: Text displayed on the device notification.
- **Notification body**: Text displayed on the authentication screen of the Swivel Mobile App.
- **iOS cert password**: iOS certificate password which should correspond with the kind of certificate that is being used: production or 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.

2 Swivel Core V4 Reporting Menu

Swivel Core has the ability to run reports against the user database to help manage the Swivel userbase. There are a number of in-built reports including

- **List all users**: simply list all the user in the database
- **List all idle users since date**: allows you to specify a date and list all the users that have not used Swivel since that date
- **User fail count and reset count**: list all users and how many authentication failures they have had
- **Latest connections for all users**: Lists the creation time and last login time for all users
- **Users that have never logged in**: Lists all users that have never successfully logged into PINsafe
- **Allocated OATH tokens**: Lists all users allocated OATH tokens, the token ID and the date allocated
- **Tokens and import date**: Lists tokens imported before a specified date
- **Number of logins for each user**: Lists the number of times each user has successfully logged in within the audit period

The results of the report are displayed on the screen and can be exported as in xml or csv formats



Reporting / Instant

Select Report: Lis

Lists all usernames in the PINsafe database

Rows per page: 5