Swivel Core V4 Server Menu

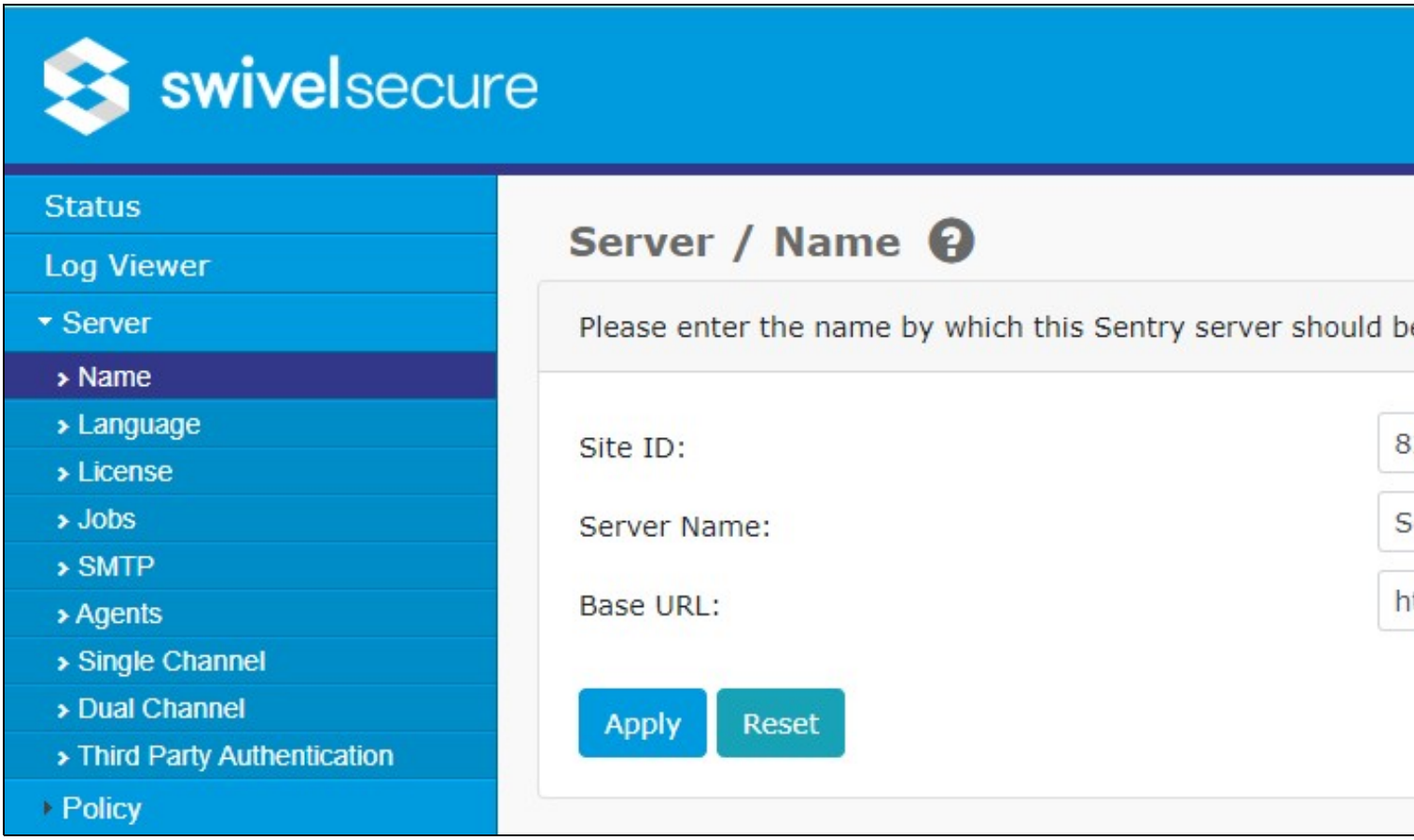
Contents

Server Menu

This menu consists of a number of pages which configure how the Swivel server works. A list of pages follows:

Name	Sets the server name and other details
Language	Sets the language for the menus
License	Allows you to install your Swivel licence
Jobs	Sets when certain regularly-scheduled jobs should run
SMTP	Configures the SMTP server used to send messages
Agents	Configures external devices that will interact with the Swivel server
Peers	Configures RADIUS peering
Single Channel	Configures how Single Channel authentication works
Dual Channel	Configures how Dual Channel authentication works
Third Party Authentication	Configures how external software interacts with the authentication mechanism
Voice Channel	Configures the gateway used for voice messaging

Server Name



On this page, you configure

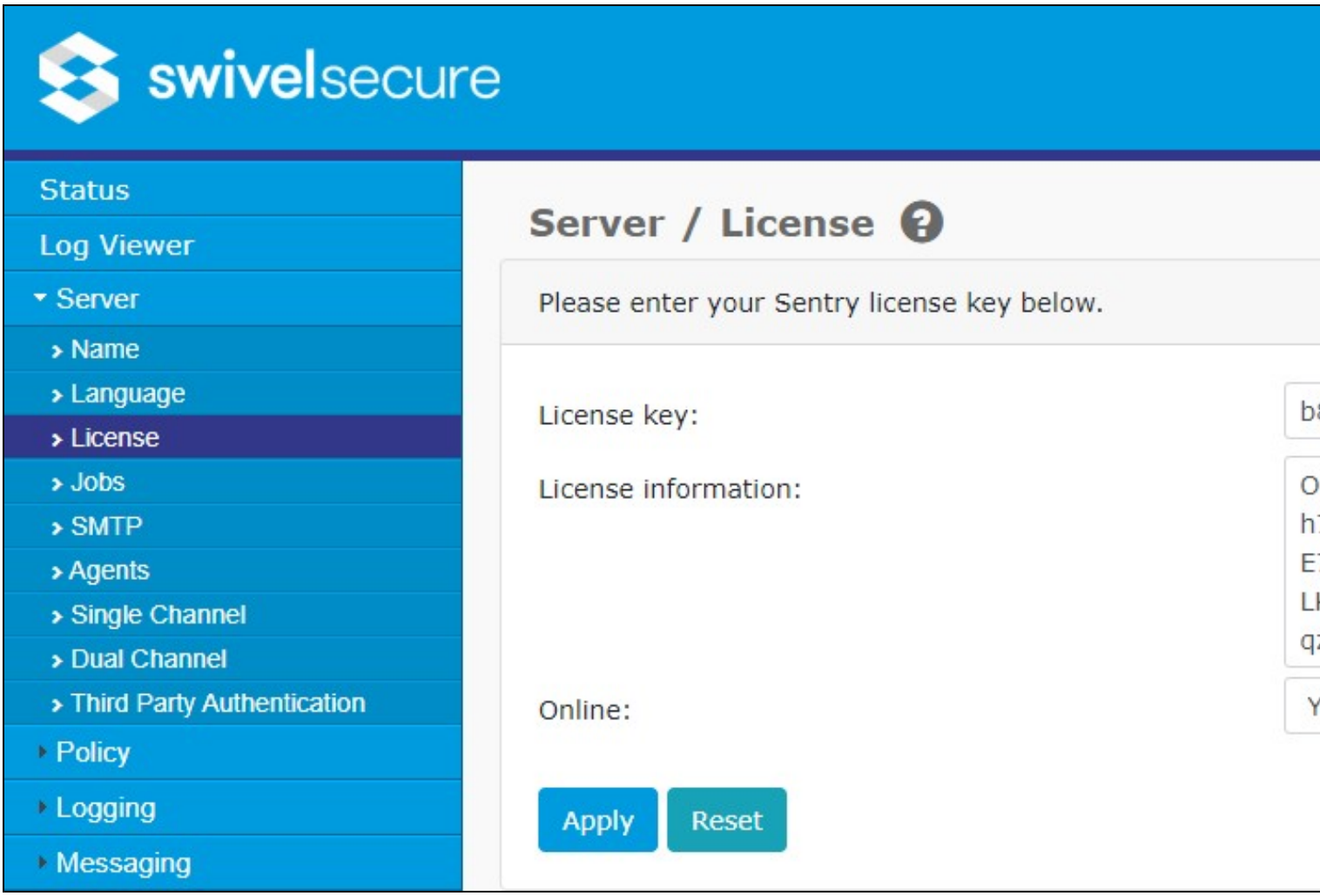
- **Site ID**: this will be given to you by your reseller, or direct from Swivel. It is unique to your site (multiple servers in a HA configuration use the same site ID).
- **Server Name**: this is a name that you give to the Swivel server. It is displayed at the top of all pages, so it is recommended that you use a different name for each server, to make it easy to distinguish them.
- **Base URL**: this is the public URL used in emails to serve images. This should be set to the public URL by which your users can access the auxiliary applications from the Swivel server. If you are not using this feature, there is no need to set it.

Language

On this page you configure

- **Language**: the language for console and error messages. Swivel only provides English language messages, so you should normally leave this as the default *en*. However, if you have a complete set of phrases in a different language, you can change this to the appropriate language.
- **Date format**: this configures the day/month/year order used in reports and in the log viewer start and end dates. The options are **dd/mm/yyyy**, **mm/dd/yyyy** and **yyy/mm/dd**.
- **Time offset (minutes)**: this is an attempt to fix a known issue where, if the time zone on a server is changed after users have been added, their credentials become invalid. We recommend that you do not change the timezone after adding users, and that all servers in a HA configuration are in the same time zone. Therefore, this should always be set to 0.

License



Before applying a license please revise that the Site ID attribute on Server > Name section has been defined.

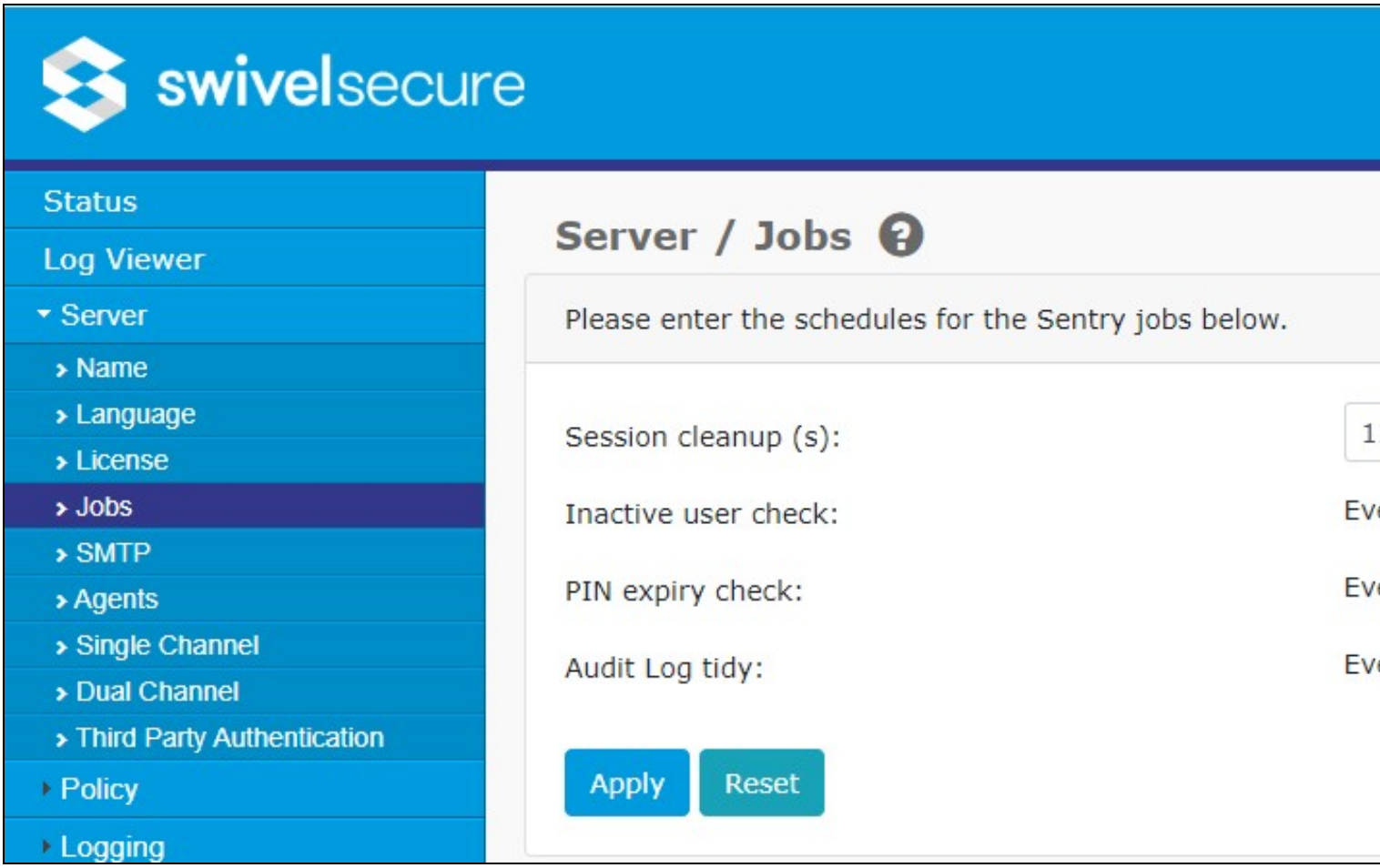
- **License Key:** A license key has the format xxxx-xxxx-xxxx-xxxx with that key Swivel Core requires to be able to contact Swivel License Server to get the license information. If you have the License Key you will need to set the Online to yes.
- **License Information:** That information will be automatically set when a correct license key is entered with Online mode set to yes. On the cases that the Swivel Core cannot connect to the License Server that information can be introduced manually and the Online mode needs to be set to No.
- **Online:** By default will be set to yes and indicates to the system that it needs to download the license information related with the license key introduce from the License Server.

When a license has been applied a information message will appear on the screen to indicate the expiration time of the license and the entitlements included on that license. Those entitlements will be the following:

- Core Users: Maximum of users allowed in the system
- Sentry: Allows the use of the AuthControl Sentry rules system
- SSO: Allows the use of the SSO on the AuthControl Sentry rules system.

The information related with the license entitlements will appear also on the Status screen.

Scheduled Jobs



All the settings on this page, apart from the first, use a time schedule. These work as follows:

Select from the first drop-down: **NEVER**, **custom...**, or one of the time periods to select how frequently the job runs. Depending on the frequency, other drop-down fields will appear to specify the time offset. For example, if the frequency is set to **day**, two drop-down fields are shown to set the hour and minute at which the event occurs. If you select **custom...**, you must specify the schedule using a valid cron string. If you are not familiar with cron strings, it is recommended you stick with the standard options.

- **Session cleanup**: this specifies how long a single-channel (TURing or PINpad) authentication session is valid. The default is 120 seconds, or 2 minutes.
- **Peer synchronisation**: this option is no longer required, and should be left as **NEVER**.
- **Inactive user check**: specifies when the job runs to check for users that have not logged in for some time.
- **PIN expiry check**: specifies when the job runs to check for PINs that have not been changed for some time.
- **Audit Log tidy**: specifies when the job runs to clear down old records in the user activity audit log.

It is recommended that these jobs are run at different times, and in particular, they are not run at the same time as User Sync jobs. If you have multiple servers using the same database (i.e. a HA solution), you should also consider offsetting the standby server schedule slightly.

SMTP Server

Use this section to configure an external SMTP server to send emails from the Swivel server. The default settings use localhost: the Swivel server has a built-in sendmail application, but that needs to be configured to connect to the outside world, so if you have an SMTP server, it may be more convenient to reference that directly.

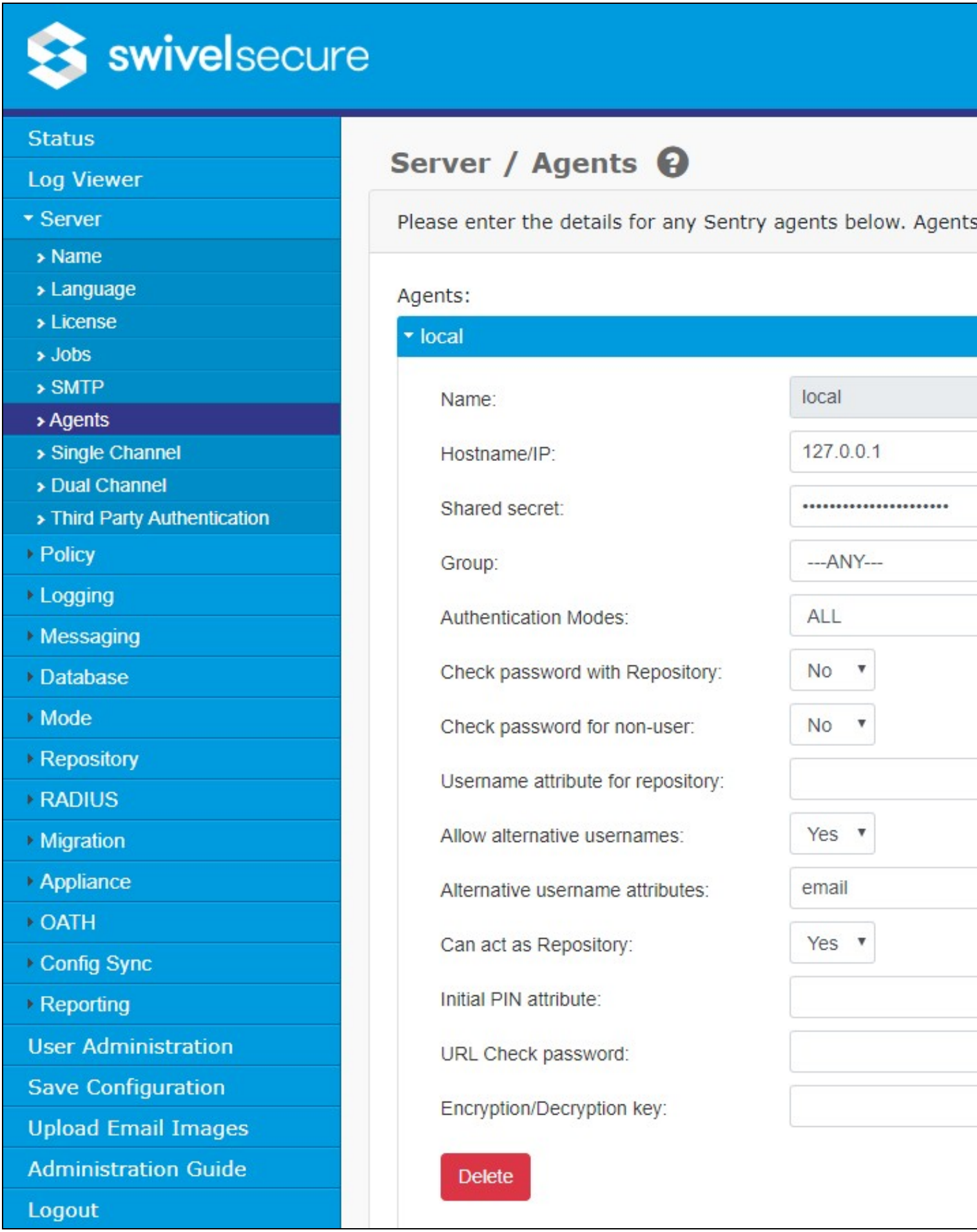
The first five settings specify the connection to the SMTP server. The remaining settings are used as follows:

- **Server Connection Timeout**: specifies how long to wait for a connection to the SMTP server.
- **Use Connection Pooling**: if **No**, then a separate connection is opened for each email that is sent, and subsequently closed. If **Yes**, the following two settings control how emails are bundled together.
- **Connection Idle Timeout**: specifies how long to wait between consecutive emails before closing the connection. It is recommended to keep this low - 1 or 2 seconds - or else the SMTP server may close the connection at the other end. This is not a problem, since the emails will still be sent, but it may cause small delays while the connection is tested and then rejected.
- **Max. No. Messages per Connection**: specifies the maximum number of messages that can be sent using a single connection. If you know that your SMTP server has a limit, make sure this limit is no greater than that.
- **Debug Enabled**: should only be used for testing. All SMTP communications will be logged in the Tomcat logs (not the Swivel logs).

Known Issues

Note that these server settings do not currently support SMTP over SSL. If you need to use a secure SMTP server, you should use the SecureSMTPTransport for messaging. This does mean that we do not currently support SMTP over SSL for logging or reporting.

Agents


swivelsecure
Status
Log Viewer
Server
Name
Language
License
Jobs
SMTP
Agents
Single Channel
Dual Channel
Third Party Authentication
Policy
Logging
Messaging
Database
Mode
Repository
RADIUS
Migration
Appliance
OATH
Config Sync
Reporting
User Administration
Save Configuration
Upload Email Images
Administration Guide
Logout
Server / Agents
Please enter the details for any Sentry agents below. Agents
Agents:
local
Name:
local
Hostname/IP:
127.0.0.1
Shared secret:
Group:
---ANY---
Authentication Modes:
ALL
Check password with Repository:
No
Check password for non-user:
No
Username attribute for repository:
Allow alternative usernames:
Yes
Alternative username attributes:
email
Can act as Repository:
Yes
Initial PIN attribute:
URL Check password:
Encryption/Decryption key:
Delete

You need to create an Agent entry for every device that needs to authenticate to Swivel using our proprietary AgentXML protocol. You do not need to create Agents for devices that authenticate using RADIUS - specify those in the RADIUS -> NAS page.

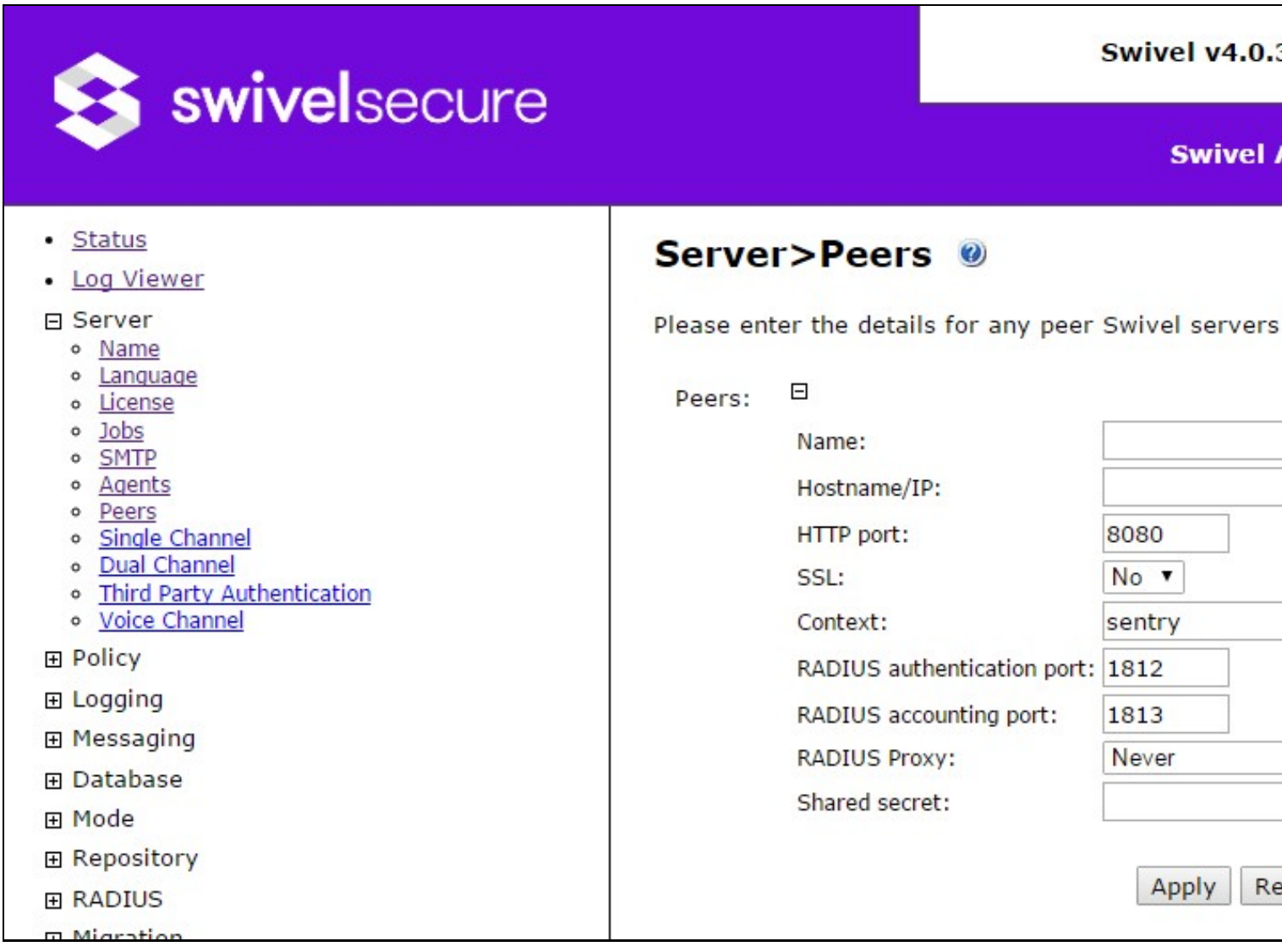
The example above shows the default Agent created for Localhost. You should not delete or modify this, as it is used by the auxiliary applications to communicate with the core.

You can create a new Agent simply by entering settings in the **New Entry** section. The settings are as follows:

- **Name**: the name of the agent. This can be anything, but should be unique among Agents.
- **Hostname/IP**: the hostname or IP address of the Agent.
- **Shared secret**: this is used as a mutual identifier between the Swivel Server and the Agent.
- **Group**: this drop-down allows you to specify that only members of a specific group can use this Agent. The default is **ANY**.
- **Authentication Modes**: specifies whether Single- or Dual-channel authentication is permitted through this Agent.
- **Check password with Repository**: if enabled, any password passed from the Agent is checked against the repository the user originates from - for example, their Active Directory password.
- **Check password for non-user**: if enabled, users not in the Swivel database can still authenticate, provided they are known to the repository, and their password is correct.
- **Username attribute for repository**: used with the previous option to identify users not in the Swivel database against the repository.
- **Allow alternative usernames**: if enabled, the username entered will be checked against other attributes in the Swivel database, not just the primary username.
- **Alternative username attributes**: used with the previous option to specify which attributes can be used to identify the user.
- **Can act as Repository**: if **Yes**, this Agent can use the Swivel AdminXML protocol to add, modify and delete users. In this case, a repository with the same name as the Agent will be created to contain the users. A consequence of this is that, if a repository already exists with the same name, the Agent can be used to manipulate users in that repository. Be aware, however, that running a user sync on that repository will overwrite all changes made by the Agent.
- **URL Check password**: If an agent can act as a repository, there may be a requirement to check a password via this agent. This URL specifies where to post the check password request for this repository. That is set automatically by the AD Agent.
- **Encryption/Decryption key**: As the password checking request will include the user?s password you can optionally supply a encryption key to add another layer of encryption on top of that supplied by https. The same value will need to be set on the AD Agent.

Peers

On new sentry version 4.1, this was moved to the RADIUS menu on the Administration Portal.



Peers are used to proxy authentication to other RADIUS servers. They are useful when moving from another authentication platform to Swivel: you can use them to pass the authentication request to the old RADIUS server if the account is not yet set up on Swivel.

The settings for each peer are as follows:

- **Name**: the name for the peer.
- **Hostname/IP**: the IP address or host of the peer.
- **HTTP port**: this setting is no longer used
- **SSL**: this setting is no longer used
- **Context**: this setting is no longer used
- **RADIUS authentication port**: the port on the peer server to use to proxy authentication.
- **RADIUS accounting port**: the port on the peer server to use to proxy accounting.
- **RADIUS Proxy**: the conditions under which to proxy authentication
- **Shared secret**: the RADIUS shared secret

Single Channel

swivelsecure

- Status
- Log Viewer
- Server
  - Name
  - Language
  - License
  - Jobs
  - SMTP
  - Agents
  - Single Channel
  - Dual Channel
  - Third Party Authentication
- Policy
- Logging
- Messaging
- Database
- Mode
- Repository
- RADIUS
- Migration
- Appliance
- OATH
- Config Sync
- Reporting
- User Administration
- Save Configuration
- Upload Email Images
- Administration Guide
- Logout

Server / Single Channel

Please specify how single channel security strings are delive

Allow session request by username:	Y
Allow alternative usernames:	Y
Alternative username attributes:	al
Multiple Authentications per String:	Y
Allow text Security Strings:	B
Image file:	tu
Background image file:	b
Text Alpha Value:	10
Only use one font per image:	Y
Image Rendering:	S
Jiggle characters within slot:	N
Add blank trailer frame to animated images:	N
Number of complete display cycles per image:	10
Inter-frame delay (1/100s):	25
No. Characters Visible:	1
Timeout to show turing image (in seconds):	0

Apply Reset

The settings on this menu configure how single channel authentication works.

- **Allow session request by username**: if **Yes**, then you can request a single-channel security string from any computer using the URL

```
http(s)://<swivel_server>:8080/sentry/SCImage?username=<username>
```

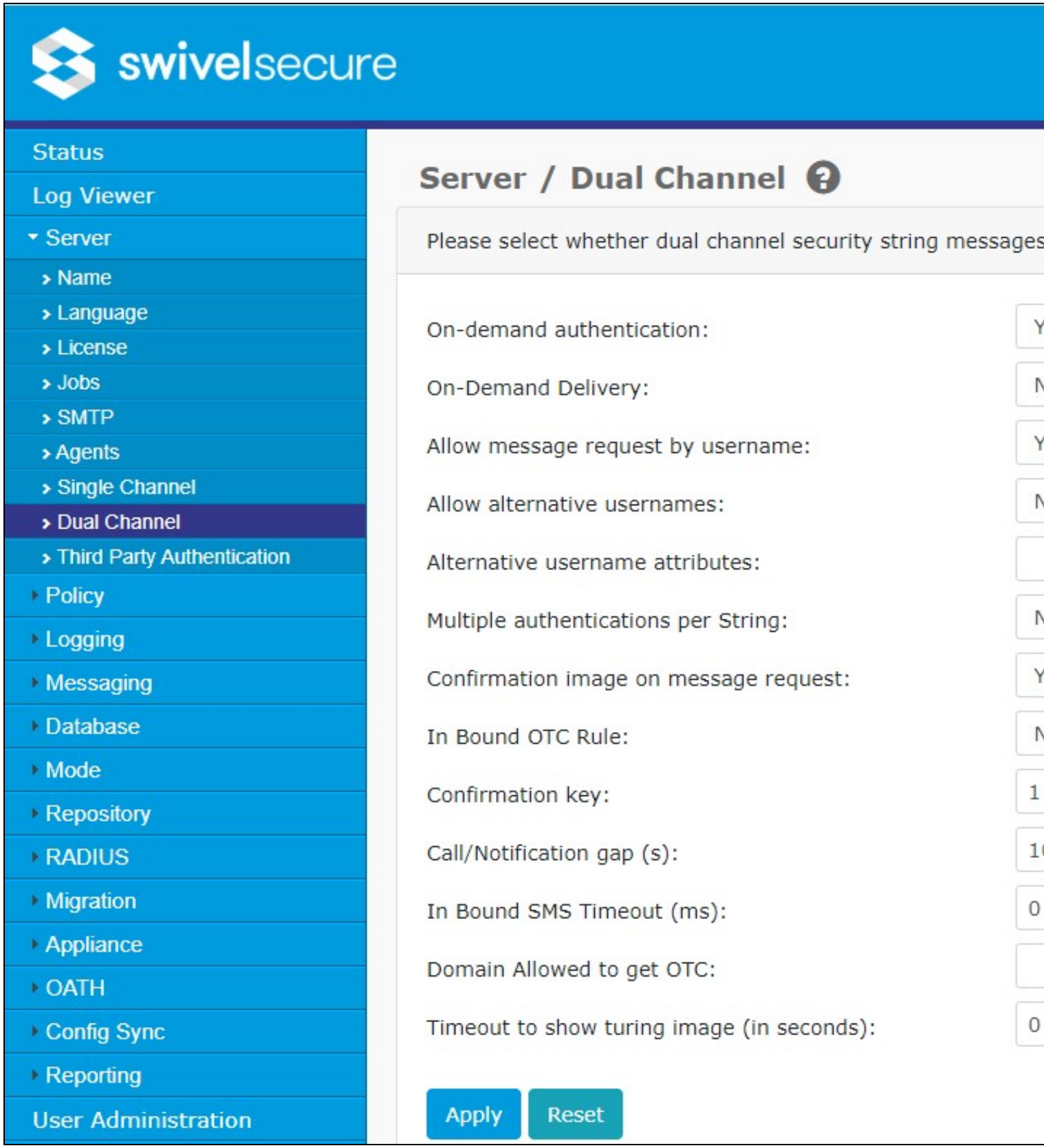
substituting the appropriate server address and username. If **No**, then you must initiate a session start and request the image by session ID. This can only be done from an Agent, so it restricts the use of single channel requests.

- **Allow alternative usernames**: if **Yes**, then single channel requests can be made using alternative attributes, not just username.
- **Alternative username attributes**: in conjunction with the previous option, specifies which Swivel attributes can be used to identify a user.
- **Multiple authentications per string**: if **Yes**, then a single-channel session is not removed once it has been used to authenticate, but can be re-used for the same user. The session remains valid until the normal session duration (default 2 minutes) has expired, the session is manually terminated, or a new session is created.
- **Allow text Security Strings**: If enabled allows security strings to be sent as plain text, using the "/SCText" servlet.
- **Image file**: specifies the image used for single channel strings. There are 4 types of image:
    - turing - this is the default. The characters are indexed 1-9 then 0 from left to right.
    - button
    - pattern
    - pattern2

In addition to the above images with a purple background, the same 4 types are available in orange.

- **Backgrounds file**: each file in this drop-down specifies a list of available background images. The default set contains background images in multiple colours. Alternatives are a set of orange and black backgrounds, and a set of black and white backgrounds.
- **Text Alpha value**: specifies the transparency of the digits: 100 is completely solid, while 0 is invisible.
- **Only use one font per image**: if **No**, then each character in the security string is rendered using a different font.
- **Image rendering**: specifies how the image is animated, if at all. The options are **Static**, **Ripple**, **Random** or **Fade Up**. Be aware that animation is not supported by certain integrations, for example, the Windows Credential Provider.
- **Jiggle characters within slot**: if **Yes**, then the characters' vertical position will vary across the string. If **No**, all characters will be centered vertically.
- **Add blank trailer frame to animated images**: if **Yes**, then the security string is invisible once each animation cycle is complete.
- **Number of complete display cycles per image**: the number of times the animation cycle is displayed.
- **Inter-frame delay**: the time, in milliseconds, between each animation frame.
- **No. characters visible**: the number of characters visible at the same time for each animation frame.
- **Timeout to show turing image (in seconds)** (Available from 4.0.5): Limit number of requests done by a user to Turing image requests in single channel to 1 every x seconds. Possible values are 0 (no timeout, default) and 1 to 86400 seconds. An error of "Too many requests" is returned before the time passes.

Dual Channel



The dual channel settings control how security strings are sent by email or SMS.

- **On-demand authentication**: if **Yes**, then security strings are only sent when explicitly requested using the URL

`http(s)://<swivel_server>:8080/sentry/DCMessage?username=<username>`

or

`http(s)://<swivel_server>:8443/proxy/DCMessage?username=<username>`

Additionally, the strings are session-based, and have the same validity period as single channel strings.

- **On-demand delivery**: if **Yes**, then security strings are sent in advance, as usual, but users can manually request a new string to be sent, using the above URL. This should not be selected at the same time as **On-demand authentication**.
- **Allow message request by username**: if **Yes**, and one of the above options is also enabled, then you can request a dual-channel security string from any computer using the URL above. If **No**, then you must initiate a session start and request the string by session ID. This can only be done from an Agent, so it restricts the use of dual channel requests.
- **Allow alternative usernames**: if **Yes**, then dual channel requests can be made using alternative attributes, not just username.
- **Alternative username attributes**: in conjunction with the previous option, specifies which Swivel attributes can be used to identify a user.
- **Multiple authentications per string**: if **Yes**, then a dual-channel session is not removed once it has been used to authenticate, but can be re-used for the same user. The string remains valid until a new string is requested or used, or if **On-demand authentication** is enabled, the normal session duration (default 2 minutes) has expired.
- **Confirmation image on message request**: if **Yes**, then a *Confirmed* image is displayed as a result of the DCMessage request.
- **Verification Mode**
- **In-bound OTC Rule**: The credentials that a user must supply as to complete a One Touch authentication is determined by this setting. The options are.

```
None:          One Touch is not supported
Match:         The user must supply a one-time code on both the OneTouch response and on the login form. (Just supported by Call Phone at t
Message:       The user must supply a one-time code via the One Touch response.  The login form needs to contain the session ID as the cred
               the moment)
Confirm Key:   The user need only respond with a single confirmation key.  The login form needs to submit the session ID as the credential.
               (Supported by Call Phone, Mobile App Push and RADIUS One Touch)
```

- **Confirmation key**: If the inbound rule is set to Confirm Key, this is the key the user must press in order to authenticate. This generally applies to the telephony implementation of OneTouch. The Mobile Client version the use will be merely prompted to confirm the authentication.

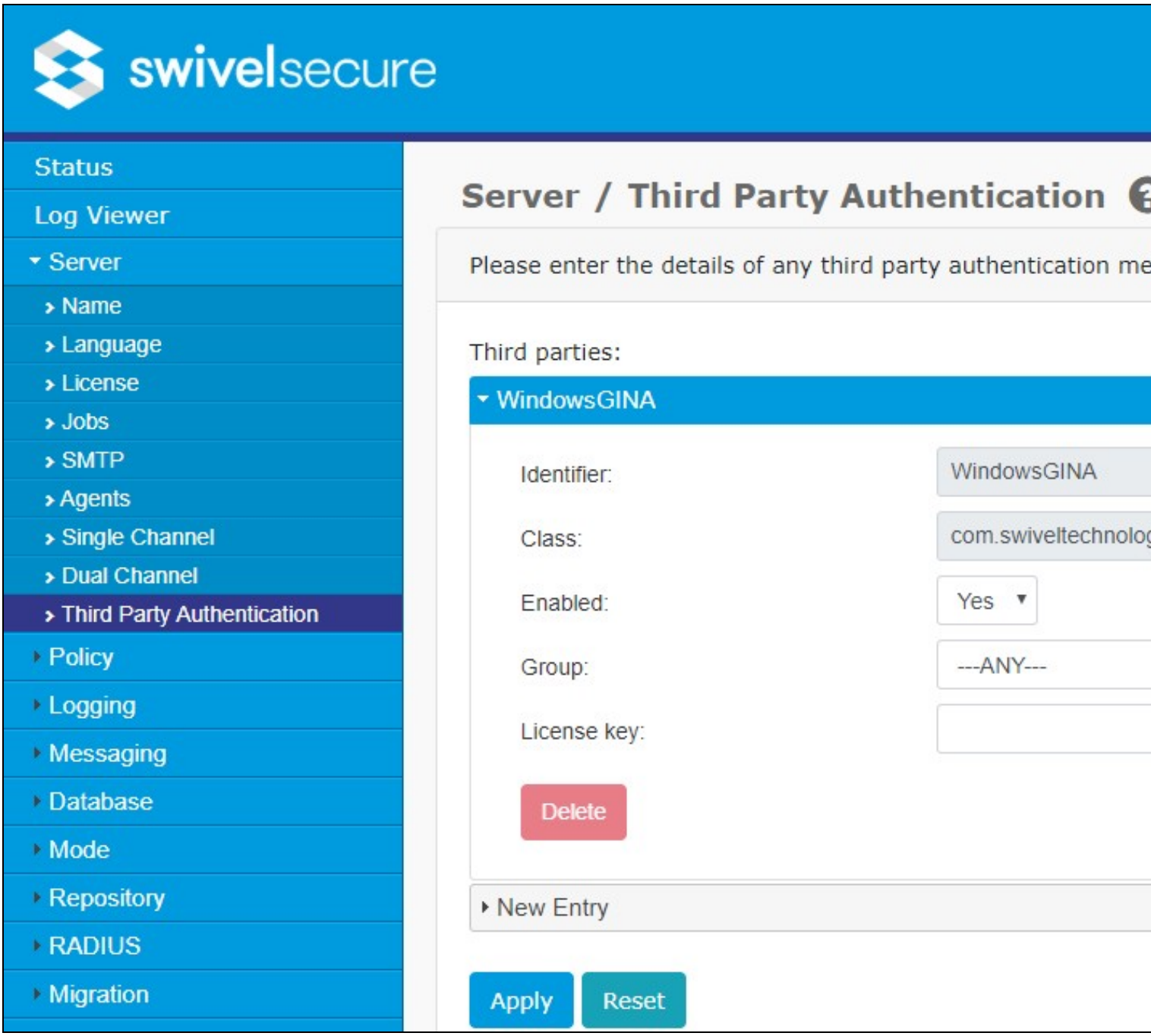
- **Call/Notification gap**: To prevent multiple repeated calls a call gap is defined. So if a call or message is requested for a user another call or message will not be sent until the call gap was expired. If another call is requested a new session is created and the user can use the first call to authenticate the subsequent session of that call is in progress.

- **In-bound SMS timeout**: In normal operation the login page will be able to be submitted only once the user?s One Touch response has been received. However if the login form is submitted before the user?s response has been received the Swivel core will wait until this timeout has expired for the user?s response.

- **Domain allowed to get OTC**: If javascript (Ajax) is used to poll the Swivel Core to determine when the user?s response has been received you may need to specify the domain of the login page. This is to handle the issue of browser security settings prevent cross domain posting. Domain needs to include full url of the login page, including port number.

- **Timeout to show turing image (in seconds)** (Available from 4.0.5): Limit number of requests done by a user to Turing image requests in dual channel to 1 every x seconds. Possible values are 0 (no timeout, default) and 1 to 86400 seconds. An error of "Too many requests" is returned before the time passes.

Third Party Authentication



The third-party authentication list allows custom classes to control the AgentXML authentication, and optionally receive data from the request, or insert additional data into the response.

Currently, there is only one third party authentication class: **WindowsGINA**. This is used by the Windows Credential Provider (GINA was the old name for the Credential Provider), to pass back security strings for offline use, and to store and retrieve encrypted passwords.

Voice Channel