Swivel Core V4 Appliance Menu

Appliance Synchronisation

swivelsecure

Status
Log Viewer
▸ Server
▸ Policy
▸ Logging
▸ Messaging
▸ Database
▸ Mode
▸ Repository
▸ RADIUS
▸ Migration
▾ Appliance
› Appliance Synchronisation
▸ OATH
▸ Config Sync
▸ Reporting
User Administration
Save Configuration
Upload Email Images
Administration Guide
Logout

Appliance / Appliance Synchronisation

Defines what elements are synchronised with another Sentr

Partner Appliance IP:	lo
Context:	se
Port:	8(
Ignore SSL Cert Errors:	Y
Connection Timeout (ms):	3(
Use SSL:	N
Shared Secret:	
Synchronise Sessions:	N

[Apply] [Reset]

This screen allows you to determine how session data is to be shared between Swivel Appliances

If you purchased Swivel as a HA pair (Active-Active) the MariaDB database will be pre-configured with the required settings to replicate the data between the appliances.

If you also need to share session data between the appliances you can use this section to enable this. This configuration needs to be completed on both servers. Once enabled every session will be replicated via http(s) between appliances meaning that a user can authenticate to either server irrespective of from which server server they requested the security string.

- **Partner Appliance IP**: The IP address or hostname of the other Swivel Appliance.
- **Context**: The context in which the Swivel application is running in.
- **Port**: The port number the other appliance is listening on.
- **Ignore SSL Cert Errors**: Allows the replication to operate over https with invalid or self-signed certificates
- **Connection Timeout (ms)**: Allows to indicate the connection timeout on milliseconds.
- **Use SSL**: Whether to use secure-socket level (SSL) for replication

- **Shared Secret**: The same shared secret needs to be set on both appliances
- **Syncronise Sessions**: Indicates if the sessions synchronisation is enabled