

Appliance Synchronisation

Contents

- 1 Overview
- 2 Prerequisites
- 3 Appliance Synchronisation
- 4 Testing
- 5 Known Issues
 - ◆ 5.1 Session sharing and Appliance Synchronisation
 - ◆ 5.2 SSL vulnerability updates stop Appliance Synchronisation working
 - ◆ 5.3 3.9.6 and 3.9.7 appliance session sync issue
- 6 Troubleshooting

Overview

Appliance synchronisation allows certain elements to be synchronised across appliances or another Swivel instance that is using a shared database. This method of sharing session information supersedes [Single Channel Session Cache](#) and [Session Sharing](#) and it is recommended to disable these if they have been enabled. By default session sharing and Appliance Synchronisation are not enabled.

Sessions that can be synchronised across appliances include:

- [Single Channel Sessions \(TURING, Pinpad\)](#)
- [SMS by On Demand Authentication](#) authentication
- [Mobile Provision Codes](#)

Prerequisites

Swivel 3.9.5 or later

Swivel Appliance 2.0.14 or later

Shared database between Swivel instances.

Where the older session sharing is used it is recommended to disable it before enabling the Appliance Synchronisation.

Appliance Synchronisation

From the Swivel Administration console select **Appliance Synchronisation**. Options available are:

Partner Appliance IP: The IP address or hostname of the partner appliance.

Context: The name of the Swivel installation, usually pinsafe.

Port: The port used for communication between appliances, usually 8080.

Ignore SSL Cert Errors: Options Yes/No. Ignore invalid certificates such as self-signed or expired.

Connection Timeout (ms): Default 3000. How long the server attempts to connect to the partner before stopping.

Use SSL: Options Yes/No. Select this if SSL is used on the appliances for the selected ports.

Shared Secret: Shared secret, also required on the other partner. For versions 3.9.6 and 3.9.7 the only shared secret that can be used is *secret*

Synchronise Sessions: Options: Yes/No. When enabled this will synchronise sessions between Swivel appliances. Sessions are used for Single Channel authentication images such as TURING and SMS on demand.

Testing

Enable the Appliance synchronisation. A single channel image generated for an admin user on one appliance should allow a login on the partner appliance (must allow a admin console login).

For each session sharing the following log message will be generated:

SESSION_UPDATE, `<SyncResponse><Session><Data Username="admin"/></Session></SyncResponse>`

Known Issues

Session sharing and Appliance Synchronisation

Disable [Session Sharing](#) where Appliance Synchronisation is used, as this may cause incompatibilities.

SSL vulnerability updates stop Appliance Synchronisation working

The following error may be displayed

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

This can be resolved by editing the file `/usr/local/tomcat/conf/server.xml` and changing both instances of `'sslProtocols='` or `'sslProtocol='` to be `'sslEnabledProtocols='`, i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

3.9.6 and 3.9.7 appliance session sync issue

Swivel versions 3.9.6 and 3.9.7 contain a bug that allows session sharing to a second Swivel instance but breaks it when a session is started on that second instance, to resolve this download the [Session Sync patch file](#) and copy the contents to the following locations:

LocalSessionManager.class to: `/usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/session`

SyncXML.class to: `/usr/local/tomcat/webapps/pinsafe/WEB-INF/classes/com/swiveltechnologies/pinsafe/server/sync`

For a software only install substitute `/usr/local/tomcat` with the Tomcat install path

This issue is fixed in Swivel 3.10 Resolution, use shared secret of secret or to upgrade to 3.10

Troubleshooting

Check the Swivel log.

Check connectivity by a Telnet from each Swivel server to the other:

```
Telnet 192.168.1.100
Trying 192.168.1.100
connected to standby@swivel.local (192.168.1.100).
Escape character is '^]'.
Connection closed by foreign host.
```

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: Received fatal alert: handshake_failure, Time out now 10

1. This can be resolved by editing the file `/usr/local/tomcat/conf/server.xml` and changing both instances of `'sslProtocols='` or `'sslProtocol='` to be `'sslEnabledProtocols='`, i.e. adding Enabled.

Restart Tomcat.

Test by generating an image and checking the logs.

2. The error is also seen on **Version 3 Appliances**, there you will need to enable TLSv1 either via the CMI menu (if available) or editing the `server.xml` from `sslEnabledProtocols="TLSv1.1,TLSv1.2"` To `sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2"` for both connector ports and restart Tomcat.

Appliance Synchronisation unavailable

If the appliance synchronisation is not available in the Administration console, it may be due to [Session Sharing](#). Disabling this will allow the appliance synchronisation to be selectable. Edit the `/home/swivel/.swivel/conf/config.properties` (path will be different for a non appliance) and change the following:

`SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.DistributedCacheSessionManager`

to

`SESSION_MANAGER = com.swiveltechnologies.pinsafe.server.session.LocalSessionManager`

Then restart Tomcat

SYNC_ERROR, 404: Not Found, Time out now 10

Synchronisation has failed between appliances. Check the IP/Hostname, port, context, network connectivity, SSL, SSL errors permitted, on each partner.

SYNC_ERROR_UNAUTHORIZED

The shared secrets do not match, re-enter them on both instances. for 3.9.6 and 3.9.7 the only available option for the shared secrets is *secret*

SYNC_ERROR Unknown Time out now 10

Swivel instance has failed to send the synchronisation data to the partner. Check all settings and network connectivity on each partner. If the appliances have http/https enabled then the settings need to be used for no SSL or SSL respectively.

SYNC_ERROR, java.net.UnknownHostException: standby-swivel-local-pinsafe, Time out now 30

The hostname is not known to the Swivel instance, check the hostname and DNS servers are correct, or try with the IP address.

SYNC_ERROR, javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target, Time out now 20

Certificate error in communication, used a valid certificate or use option to **Ignore SSL Cert Errors**:

SYNC_ERROR, Unexpected end of file from server, Time out now 60

Check to see if SSL or non SSL communications are used. On the Admin Console, navigate to Appliance > Appliance Synchronisation and check the setting Use SSL.

SYNC_ERROR, java.net.SocketTimeoutException: Read timed out, Time out now 20

Check Network connectivity between the Swivel instances.