Table of Contents

1 PINsafe Migration Path

Please see our Install / Upgrade page for information about upgrading PINsafe.

2 Upgrade from v3 to v4

3 Upgrading notes

This document tells the procedure of upgrading from version 3 to version 4 sentry Authcontrol using the CMI

4 Before upgrade : License considerations

To access the latest AuthControl Sentry V4.04 features you will need to upgrade your appliance as well as request a V4 license key and Site ID, please contact your local Swivel Secure representative who can arrange this for you.

Please note some features like Single Sign On are chargeable.
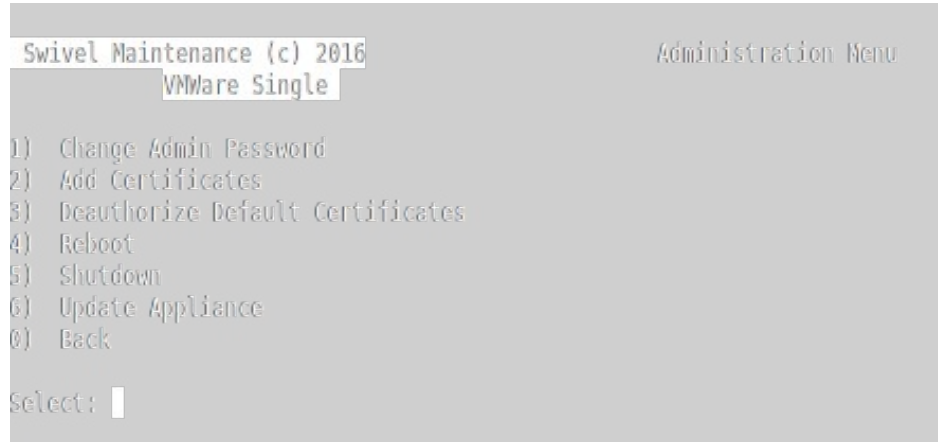
5 Upgrading procedure

- Updating v3 to v4

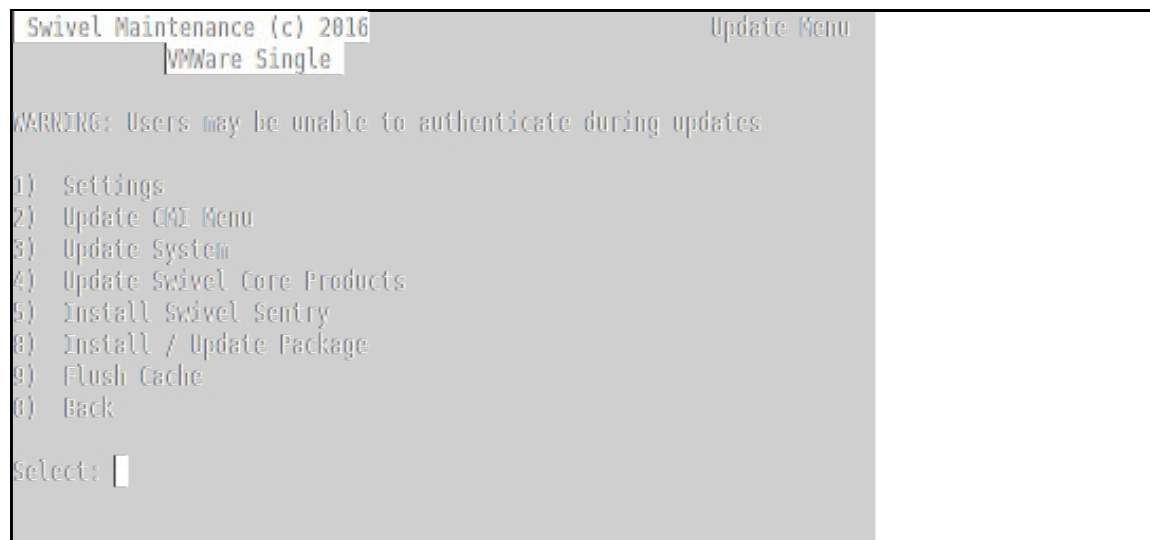1. Update swivel-cmi to at least 2214.

```
Update System or CMI from the update menu.
```

2. Logout.

3.Login into Administration Menu

```
Swivel Maintenance (c) 2016                    Administration Menu
          VMWare Single

1)   Change Admin Password
2)   Add Certificates
3)   Deauthorize Default Certificates
4)   Reboot
5)   Shutdown
6)   Update Appliance
0)   Back

Select: 
```

4. Select update menu and Select "Settings"

```
Swivel Maintenance (c) 2016                         Update Menu
          VMWare Single

WARNING: Users may be unable to authenticate during updates

1)   Settings
2)   Update CMI Menu
3)   Update System
4)   Update Swivel Core Products
5)   Install Swivel Sentry
8)   Install / Update Package
9)   Flush Cache
0)   Back

Select: 
```

5. Select "Upgrade to v4 Repository"

```
Swivel Maintenance (c) 2016                       Update Settings
          VMWare Single

1)   Enable External Repository Access
2)   Yum Proxy
3)   Upgrade to v4 Repository
0)   Back

Select: 
```
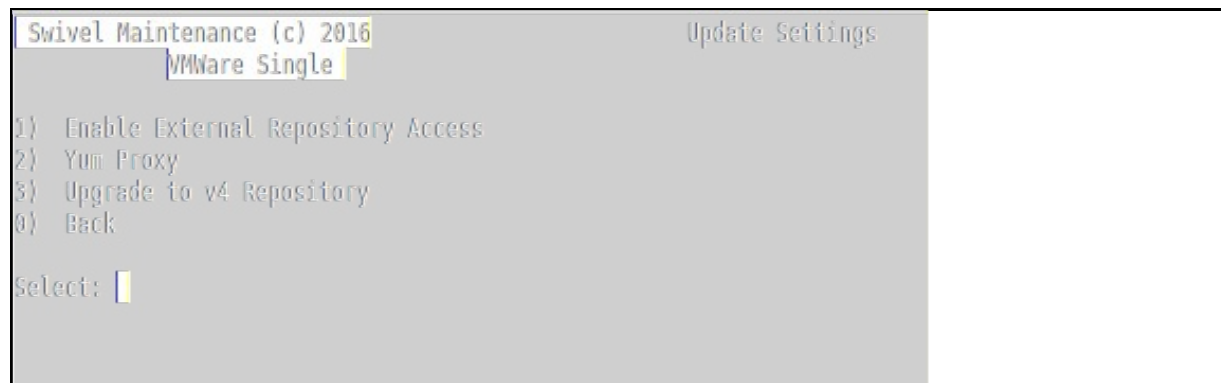
```
Select: 3
INFO: Changed to take updates from v4 repositories.
Press RETURN to continue: █
```

6. Update System, Swivel Core Products.

```
 Swivel Maintenance (c) 2016                          Update Menu
          VMWare Single

WARNING: Users may be unable to authenticate during updates

1)  Settings
2)  Update CMI Menu
3)  Update System
4)  Update Swivel Core Products
5)  Install Swivel Sentry
8)  Install / Update Package
9)  Flush Cache
0)  Back

Select: █
```

```
Resolving Dependencies
--> Running transaction check
---> Package swivel-cmi.noarch 0:3.0.2228-22 will be updated
---> Package swivel-cmi.noarch 0:4.0.2227-955 will be an update
---> Package swivel-mon.noarch 0:1.0.1841-16 will be updated
---> Package swivel-mon.noarch 0:1.0.2192-18 will be an update
---> Package swivel-mysql.noarch 0:1.0.2143-46 will be updated
---> Package swivel-mysql.noarch 0:1.0.2231-48 will be an update
---> Package swivel-release.noarch 0:1.0.1743-39 will be updated
---> Package swivel-release.noarch 0:4.0.1983-47 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package            Arch         Version             Repository        Size
================================================================================
Updating:
 swivel-cmi         noarch       4.0.2227-955        appliance        117 k
 swivel-mon         noarch       1.0.2192-18         appliance         21 k
 swivel-mysql       noarch       1.0.2231-48         appliance         20 k
 swivel-release     noarch       4.0.1983-47         appliance         21 k

Transaction Summary
================================================================================
Upgrade       4 Package(s)

Total download size: 179 k
Is this ok [y/N]: █
```

```
Dependencies Resolved

================================================================================
 Package            Arch        Version           Repository          Size
================================================================================
Updating:
 apache-tomcat      noarch      8.0.36-67         appliance-core       6.9 M
 swivel-PINsafe     noarch      4.0.4.5093-76     appliance-core        24 M
 swivel-proxy       noarch      1.6.2.4703-13     appliance-core        91 k
Installing for dependencies:
 jre1.8.0_121       x86_64      1.8.0_121-fcs     appliance-core        54 M
 swivel-ROOT        noarch      1.0.0-3           appliance-core       163 k

Transaction Summary
================================================================================
Install       2 Package(s)
Upgrade       3 Package(s)

Total download size: 86 M
Is this ok [y/N]: 
```

Select Y

7. Select "Install Swivel Sentry" in update Menu.

```
Swivel Maintenance (c) 2016                    Update Menu
          VMWare Single

WARNING: Users may be unable to authenticate during updates

1)   Settings
2)   Update CMI Menu
3)   Update System
4)   Update Swivel Core Products
5)   Install Swivel Sentry
8)   Install / Update Package
9)   Flush Cache
0)   Back

Select: 
```

8. (opt) Select "Install / Update Package", then enter "swivel-logviewer" without quotes.

6 Need more help?

Please contact your partner or create a support ticket in our support portal https://supportdesk.swivelsecure.com/dashboard

7 Upgrade PINsafe

7.1 Overview

Swivel upgrades and migration can be performed by following the below procedures. This document covers all Swivel 3.x versions. The Swivel license is compatible within major versions 3.1 to 3.2, etc, but a new license is required between versions 2.1 to 3.1. To determine your version see Version Information.

For information on upgrading the Swivel virtual or hardware appliance see Patch Appliance Install

See the following table for an overview on the options for an Upgrade

7.2 Prerequisites

1. What DB is Swivel using: Internal, MySQL, Other?

2. Is a Virtual IP being used?

3. Type of virtual or hardware appliance installation: Active/Active, Active/Passive, or Standalone.

4. Access to the virtual or hardware appliances using root oradmin. Referred to as ?Login? for the remainder of the document.

5. Test Transports and authentication are all working before the upgrade.

6. Create a directory under root called upgrade

7. New copy of pinsafe.war placed in /root. If using an virtual or hardware appliance see Copying appliance files How to Guide

8. In the case of HA configurations, both virtual or hardware appliances are working and functioning with the intended design.

9. Ensure Swivel is fully functional (check logs)

10. Put a freeze on Swivel administration changes and repository synchronisations during the upgrade (no PIN changes, account creations or deletions)

11. Turn off AD synchronisation on the server being upgraded

12. Ensure Swivel is fully backed up

13. Downloads

7.3 Upgrade Considerations

Ensure the OS/Appliance has the latest updates and patches see Patch Appliance Install

Where necessary schedule downtime

It is better to notify Swivel Secure in good time before an upgrade

Where necessary request professional services through your reseller

Where available carry out upgrade on test system prior to production system

Site specific customisations may need these customisations to be applied after the upgrade, these include Custom Transports and external databases are used such as MS SQL and Oracle the drivers located in pinsafe/WEB-INF/lib such as sqljdbc.jar, sqljdbc4.jar need to be copied see MS SQL Database How To Guide and Oracle Database How To Guide

To upgrade Swivel by copying data from one virtual or hardware appliance to another you may wish to use WinSCP, see WinSCP How To Guide

7.4 Swivel Version Specific Considerations

For information on Swivel features in each version see Versions FAQ. Swivel version prior to 3.6 may require a Java upgrade, see JAVA upgrade.

7.4.1 Swivel PINsafe 2.x

2.x uses a different database and direct upgrades are only possible through Swivel Secure Support. An upgrade from version 2.x to version 3.x will require a new license.

7.4.2 Swivel PINsafe 3.1

When upgrading from 3.1 it is not possible to directly copy the 3.1 config.xml file to higher versions. The configuration should be manually entered through the Swivel administration console.

Unfortunately, there are problems with upgrading the database from version 3.1 to 3.8 or 3.9. The workaround is to upgrade to version 3.2 first. You can get a copy of 3.2 from here.

As the upgrade to 3.2 is a temporary one, the recommended procedure is as follows. Note that the paths below assume you are upgrading a virtual or hardware appliance. If you are not using a virtual or hardware appliance, substitute the appropriate location of the Tomcat webapps folder:

- If you have not already done so, stop Tomcat on the existing virtual or hardware appliance, and take a copy of the database from /usr/local/tomcat/webapps/pinsafe/WEB-INF/db/. If you are using an XML repository, make sure you also copy repository.xml from /usr/local/tomcat/webapps/pinsafe/WEB-INF/data/.
- Extract pinsafe.war from the above zip file, and rename it to pinsafe32.war.
- Copy pinsafe32.war to the new virtual or hardware appliance inside /usr/local/tomcat/webapps/. Start Tomcat if it is not already running, and wait about a minute for pinsafe32 to deploy.
- Login to the 3.2 system, create the database and set the mode to synchronised and the repository option will appear then create a repository based on the original 3.1 data source using the following exact names. For Active Directory use **Active Directory** for XML use **XML**.
- Stop Tomcat and copy the saved database from version 3.1 into /usr/local/tomcat/webapps/pinsafe32/WEB-INF/db/.
- (virtual or hardware Appliance only) Set the owner and group of the database folder and all sub-folders to swivel.
- Restart Tomcat and log into the console at https://<pinsafe_address>:8080/pinsafe32. Use the username admin and PIN 1234.
- Set the mode to Synchronized and then set the active database to Internal. Set the repository type to match that of 3.1. If all goes well, the database will be upgraded to 3.2.
- Stop Tomcat and take a copy of the upgraded database.
- Deploy the latest version of PINsafe, if you have not already done so.
- Stop Tomcat and copy the 3.2 database to /usr/local/tomcat/webapps/pinsafe/WEB-INF/db/.
- If you are using an XML repository, copy repository.xml to /usr/local/tomcat/webapps/pinsafe/WEB-INF/data/.
- (virtual or hardware Appliance only) As before, make sure that the owner and group of the db folder and its contents, and also repository.xml if relevant, are set to swivel.
- Restart Tomcat.
- Follow the instructions to configure PINsafe, with the following provisos: it is important when creating your initial repository that you set the type to match the type of your original repository. Also, the step to change the database should be the LAST step you make, AFTER you have created the repository and set mode to Synchronized.

You should now have a working database. Carry on as usual.

7.4.3 Swivel PINsafe 3.2

This also applies to upgrading from 3.1.

Group membership is not included in the old database. Therefore, you need to run a user sync at least once after upgrade to set your group membership.

When upgrading from Swivel 3.2

1). Stop Tomcat

2). Backup /usr/local/tomcat/webapps/pinsafe

3). Start Tomcat

4). Remove the /usr/local/tomcat/webapps/pinsafe.war folder which should delete the /usr/local/tomcat/webapps/pinsafe folder

5). Install the new version of Swivel by copying in the pinsafe.war file to /usr/local/tomcat/webapps/ (version 3.8 is a good version to upgrade to)

6). In the Swivel Administration console, create a repository of the type used, e.g. Active Directory or XML, and give it the required name

7). Stop Tomcat

8). Copy from the backup the db folder to /usr/local/tomcat/webapps/pinsafe/WEB-INF/ ensure ownership and permissions are the same

9). Start Tomcat

10). Login and select Mode Synchronised, and set the database to internal. The user data should reside in the correct repository and data can be Migrated to another database type if required.

7.4.4 Swivel PINsafe 3.5

With External databases some new tables are added. There may be with issues with MySQL tables PINsafe upgrade fails on MySQL

If you are using session sharing, you will need to edit config.properties after upgrade, as described here. DO NOT copy the old config.properties file, as it will not be valid.

7.4.5 Swivel PINsafe 3.6

The animated security string requires JRE 1.6, the Java version may need upgrading (check PINSAFEK for correct value such as 3500)

Custom Transports used in 3.5 or earlier will not work in Swivel PINsafe 3.6 or later, contact support@swivelsecure.com for an updated transport

7.4.6 Swivel PINsafe 3.7

If RADIUS groups are being used, then these may need to be re-entered as the group configuration has moved from RADIUS/Server to RADIUS/NAS

7.4.7 Swivel PINsafe 3.8

- If you currently have 'Check Password with Repository' set to 'Yes' on the Policy -> Password screen, you will need to define this against each agent where it is required as this is now configured against each agent, rather than being a general setting;

- If you currently have 'Check Password with Repository' set to 'Yes' on the Policy -> Password screen, this will no longer take effect upon the Swivel Administration Console login;

- Mobile clients (Swivlet/iPhone iClient/Android) will need to be upgraded to versions that include 3.8 Mobile Device Provisioning to utilise the new features provided see Mobile Provision Code

- Swivel virtual or hardware appliances will need to have their proxy upgraded for the 3.8 Mobile device provisioning see Appliance Proxy Server Upgrade

- Self-provisioning for the mobile clients is conducted via the ResetPIN application. This needs to be upgraded when upgrading to Swivel PINsafe 3.8. See ResetPIN upgrade for PINsafe 3.8 How To Guide

7.4.8 Swivel PINsafe 3.9

WARNING: there is a known issue in the current release of 3.9 which means that some configuration items are not loaded properly after an upgrade. In particular, this affects transport attributes and repository group definitions.

The workaround is to stop and restart Tomcat after you have completed the upgrade process, before you do anything else: in particular, before you run a user sync.

7.4.9 Swivel PINsafe 3.9.1

Software release only. For Active/Passive appliances upgrading to 3.9.1 or higher contact Swivel support.

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Upgrade Appliance

Version 3.9.1 only allows one instance to be run under Tomcat. Multiple instances of older versions may still be run. Swivel will make an external copy of the required information, see Transient Data Storage. Note the Transient Data Storage may now need to be included in the backups.

When upgrading software only installations (not virtual or hardware appliances) from Swivel 3.9.1 to a higher version, the pinsafe.war file simply needs to be copied into the /webapps folder, except where custom transports are used and/or when not using the Internal, or MySQL DB, in this case backup the DB driver or custom transports need to be copied before upgrading Swivel, refer to the relevant sections below for details on the upgrade.

Note that, since user attributes are a new feature of 3.9.1, if you upgrade from an earlier version, you will need to configure the required attributes for the repositories and then run a user sync before they are available.

7.4.10 Swivel PINsafe 3.9.2 and later

For upgrading to Swivel virtual or hardware appliances to version 3.9.2 or higher see Patch Appliance Install

For non-appliance (software only) installations, the procedure is the same as for 3.9.1. For Active/Passive appliances upgrading to 3.9.1 or higher contact Swivel support. Note the Transient Data Storage may now need to be included in the backups.

For virtual or hardware appliances, you must upgrade the virtual or hardware appliance using the Patch Appliance Install. Please do so before attempting to upgrade to version 3.9.2. or later Once you have installed the virtual or hardware appliance patch, use the Patch Swivel Install procedure to install the 3.9.2 or later version.

7.5 Microsoft Windows Swivel Upgrade

The following article covers the Microsoft Windows Swivel Upgrade steps Upgrading PINsafe on Microsoft Windows

7.6 Swivel Upgrade on virtual or hardware Appliances

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Patch Appliance Install

For upgrading Swivel software **TO** version 3.2-3.9 follow the below

7.6.1 Virtual or hardware appliance System Preparation

Determine which version of the virtual or hardware appliance is being used, see Appliance types FAQ

The following steps are required for all Swivel upgrades on an virtual or hardware appliance.

Access the command line, and create a temporary backup area:

```
mkdir /root/upgrade
```

7.6.2 Upgrading Swivel Standalone virtual or hardware Appliances

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Patch Appliance Install

Login to the Swivel administration web interface on the virtual or hardware appliance.

Change Mode to ?Slave?, and change the Database to ?shipping?.

Login to the virtual or hardware appliance:

Stop Tomcat:

```
service tomcat5 stop
```

Now proceed with the upgrade process described below Upgrading from Versions 3.2-3.9 on the primary virtual or hardware appliance. After upgrading the primary virtual or hardware appliance repeat the process for the secondary virtual or hardware appliance.

7.6.3 Upgrading Swivel Active/Passive Appliances

Older Active/Passive appliances can only be upgraded to Swivel version 3.9. To upgrade beyond this version on Active/Passive appliances, contact Swivel support.

A HA A/P pair uses disk replication between two appliances, therefore upgrading the primary appliance will automatically upgrade the standby. However to prevent the cluster from switching over, the service that monitors Tomcat will need to be stopped.

Login to the Swivel administration web interface on the Primary appliance.

Change Mode to ?Slave?, and change the Database to ?shipping? (Swivel PINsafe 3.2 or later only).

Login to the Secondary appliance:

Stop Monitor and Heartbeat:

```
service mon stop
```

```
service heartbeat stop
```

This will prevent the Passive appliance taking over whilst Tomcat is stopped on the Active appliance.

Login to the Primary appliance:

Stop Monitor and Tomcat:

```
service mon stop
service tomcat5 stop
```

Do NOT stop heartbeat on the Primary appliance.

Now proceed with the upgrade process described below Upgrading from Versions 3.2-3.9 on the primary appliance.

7.6.4 Upgrading Swivel Active/Active virtual or hardware Appliances

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Patch Appliance Install

A HA A/A pair uses DB replication between two virtual or hardware appliances, therefore both appliances will require upgrading, as the Swivel configuration file is not part of the replication. However to prevent the cluster from switching over, the service that monitors Tomcat will need to be stopped.

When upgrading to Swivel PINsafe 3.5 or higher, ensure Swivel virtual or hardware appliance permissions are correct

Ensure databases are correctly synchronised between Swivel virtual or hardware appliances.

If a Virtual IP is NOT being used ignore all heartbeat related commands.

Login to the Swivel administration web interface on both virtual or hardware appliances.

Change the Mode to ?Slave?, and change the Database to ?shipping? (make a note of the DB currently being used).

Login to Standby virtual or hardware appliance:

Stop Monitor, Heartbeat and Tomcat:

```
service mon stop
service heartbeat stop
service tomcat5 stop
```

If the virtual or hardware appliances are using a virtual IP, this will prevent a fail-over taking place.

Login to the Primary virtual or hardware appliance:

Stop Monitor, Heartbeat and Tomcat:

```
service mon stop
service heartbeat stop
service tomcat5 stop
```

If the virtual or hardware appliances are using a virtual IP, this will prevent a fail-over taking place.

If MySQL is being used to replicate the DB, create a secure copy. If Oracle or another external DB is being used to provide Swivel DB replication ensure that a valid DB backup is taken.

Login to the Primary virtual or hardware appliance:

Backup MySQL replicated DB (enter command on one line):

```
mysqldump --single-transaction --flush-logs pinsafe_rep > /root/upgrade/mysql_rep_backup_$$.sql
```

Now proceed with the upgrade process described below Upgrading from Versions 3.2-3.9 on the primary virtual or hardware appliance. After upgrading the primary virtual or hardware appliance repeat the process for the secondary virtual or hardware appliance.

7.6.5 Upgrading Swivel DR virtual or hardware Appliances

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Patch Appliance Install

Login to the DR, virtual or hardware appliances and ensure Mode is et to ?Slave?, and change the Database to ?shipping?

Follow the Upgrading Swivel Generic Information

After the upgrade ensure Swivel has been upgraded as expected

Ensure Swivel is functioning as expected

Ensure Swivel servers are set back to the correct database type and Mode

7.7 Upgrading to Versions 3.9.1 or higher

For upgrading to Swivel Appliances to version 3.9.2 or higher see Patch Appliance Install

For upgrading to versions 3.9.1 and higher (excluding 3.9) the, the pinsafe.war file can be copied into the webapps folder as part of the upgrade, but make a copy of custom transports and the <database name>.jar file in WEB-INF/lib before upgrading and copy back in as below.

7.8 Upgrading to Versions 3.2-3.9

For upgrading to Swivel virtual or hardware Appliances to version 3.9.2 or higher see Patch Appliance Install

The WEB-INF directory is located under /usr/local/apache-tomcat-x.x/webapps/pinsafe

1. It is highly recommended that you take a copy of the entire ?/WEB-INF/ folder but specifically ensure steps 2-4, and 5-6 if relevant, are completed.

```
cp ?rp /usr/local/tomcat/webapps/pinsafe /root/upgrade/
```

2. Back up the PINsafe configuration by taking a copy of .../WEB-INF/conf/config.xml to a safe location.

```
cp ?p /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf/config.xml /root/upgrade
```

3. Back up the PINsafe ranges file by taking a copy of .../WEB-INF/conf/ranges.xml to a safe location.

```
cp ?p /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf/ranges.xml /root/upgrade
```

4. Back up the PINsafe ranges file by taking a copy of .../WEB-INF/conf/config.properties to a safe location.

```
cp ?p /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf/config.properties /root/upgrade
```

5. Back up the PINsafe User Repository by taking a copy of .../WEB-INF/data/repository.xml to a safe location.

```
cp ?p /usr/local/tomcat/webapps/pinsafe/WEB-INF/data/repository.xml /root/upgrade
```

6. Back up the PINsafe user data by taking a copy of everything under .../WEB-INF/db to a safe location. This is only relevant if you are using the Internal database.

```
cp ?rp /usr/local/tomcat/webapps/pinsafe/WEB-INF/db /root/upgrade
```

7. If you have any custom transport classes, note that classes from 3.5 or earlier are not compatible with 3.6 or higher. Check with Swivel Secure if there is an upgrade available. As a matter of principle, when Swivel Secure develops a custom transport class for a customer, it is included as a standard component in the next release of Swivel software. Please check with Swivel that your transport is available and/or still valid before upgrading.

8. Back up the Swivel logs by taking a copy of everything under .../WEB-INF/logs to a safe location. The upgrade will not fail if you do not backup logs, but you will not be able to view old log entries.

```
cp ?rp /usr/local/tomcat/webapps/pinsafe/WEB-INF/logs /root/upgrade
```

9. If the Internal, or MySQL DB is not being used, backup the DB driver file ../WEB-INF/lib (check with Swivel Secure the name of the driver file).

```
cp -p /usr/local/tomcat/webapps/pinsafe/WEB-INF/lib/<driver>.jar /root/upgrade
```

10. Remove the current Swivel installation by deleting the pinsafe.war file. Tomcat will remove the associated directory.

```
service tomcat5 start
rm ?f /usr/local/tomcat/webapps/pinsafe.war
service tomcat5 restart
```

11. Copy new pinsafe.war file to the webapps folder.

```
cp ?p /root/pinsafe.war /usr/local/tomcat/webapps
```

12. Stop the Tomcat service.

```
service tomcat5 stop
```

13. Restore the config.xml file to .../WEB-INF/conf/config.xml

```
cp ?p /root/upgrade/config.xml /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf
```

14. Restore the ranges.xml file to .../WEB-INF/conf/ranges.xml

```
cp ?p /root/upgrade/ranges.xml /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf
```

15. PINsafe 3.6 OR LATER ONLY: Restore the config.properties file to .../WEB-INF/conf/config.properties

```
cp ?p /root/upgrade/config.properties /usr/local/tomcat/webapps/pinsafe/WEB-INF/conf
```

NOTE: Step 15 is strictly only necessary if you are using session sharing. See note for upgrading from 3.5 if session sharing is enabled.

16. If an internal database is being used, restore the database.

```
cp -rp /root/upgrade/db/* /usr/local/tomcat/webapps/pinsafe/WEB-INF/db/
```

17. If an XML repository is being used restore the repository.xml file.

```
cp ?p /root/upgrade/repository.xml /usr/local/tomcat/webapps/pinsafe/WEB-INF/data
```

18. Restore your custom transport classes if relevant.

19. Restore the old log files.

```
cp ?rp /root/upgrade/logs/* /usr/local/tomcat/webapps/pinsafe/WEB-INF/logs
```

20. Restore the JDBC driver file if you backed it up (replace the name of the driver with the name used previously)

```
cp -p /root/upgrade/<driver>.jar /usr/local/tomcat/webapps/pinsafe/WEB-INF/lib/
```

21. Ensure that the ownerships and permissions on the files that have been restored are correct.

```
chown ?R swivel:swivel /usr/local/tomcat/webapps/pinsafe
chmod ?R 775 /usr/local/tomcat/webapps/pinsafe/WEB-INF/db
```

22. Start the Tomcat service.

```
service tomcat5 start
```

23. **PINsafe 3.9 only**: once the configuration has been successfully upgraded, restart the Tomcat service again (as described above).

```
service tomcat5 restart
```

7.8.1 Standalone virtual or hardware Appliance

Login to the Swivel administration web interface.

1. Test that the configuration has been correctly upgraded.

2. Configure the Swivel DB for use with Swivel by changing the Database back to the value prior to the upgrade. Check logs for errors.

3. Check users have been correctly migrated, and test a user can authenticate.

4. To start AD updates, change the Mode to ?Synchronized?.

7.8.2 Active/Passive Appliance

1. Test that the configuration has been correctly upgraded.

2. Configure the Swivel DB for use with Swivel by changing the Database back to ?internal?. Check the logs for any errors.

3. Check users have been correctly migrated, and test a user can authenticate.

4. To start AD updates, change the Mode to ?Synchronized? (Swivel PINsafe 3.2 or later only).

Login to the Primary virtual or hardware appliance:

Start Monitor:

```
service mon start
```

Login to the Secondary virtual or hardware appliance:

Start Monitor and Heartbeat:

```
service heartbeat start
service mon start
```

7.8.3 Active/Active virtual or hardware Appliance

If a Virtual IP is NOT being used ignore all heartbeat related commands.

Login to the Swivel administration web interface on the Primary virtual or hardware appliance.

1. Test that the configuration has been correctly upgraded.

2. Configure the Swivel DB for use with Swivel by changing the Database back to the value prior to the upgrade. Check logs for errors.

3. Check users have been correctly imported, and test a user can authenticate.

Login to the Swivel administration web interface on the Standby virtual or hardware appliance.

4. Test that the configuration has been correctly upgraded.

5. Change the Swivel DB for use with Swivel by changing the Database back to the value prior to the upgrade. DB will already have been updated by the Primary.

Check users have been correctly imported, and test a user can authenticate.

Before continuing ensure that the primary and standby virtual or hardware appliances have been upgraded to the correct version

6. To start AD updates, change the Mode to ?Synchronized? on the Primary virtual or hardware appliance, and then the Standby virtual or hardware appliance if required.

Login to Primary virtual or hardware appliance:

7. Start Heartbeat and Mon:

```
service heartbeat start
service mon start
```

Login to Standby virtual or hardware appliance:

8. Start Heartbeat and Mon:

```
service heartbeat start
service mon start
```

7.9 Additional Information

After upgrading you may see that any repository you had will exist on the new installation and it will be named after the associated hostname (or hostname followed by context in the case of the XML repository). Therefore if you had an AD repository in 3.2 you will have an XML repository in 3.3 named after the AD server's hostname (or IP address)

If you had an AD repository on your 3.2 installation you will now have the option to add an XML repository. It is recommended that you do this as this gives you the ability to create admin accounts whilst you are working on the installation

7.10 Troubleshooting

Upgrade to 3.9.1 fails on Swivel virtual or hardware appliance with Swivel settings not imported, and Swivel set to defaults. This can occur when Swivel is upgraded without installing the relevant patch, see https://kb.swivelsecure.com/wiki/index.php/Upgrade_PINsafe#Swivel_PINsafe_3.9.1. Restore Swivel from backup and carry out upgrade using patch.

Transports absent after upgrade

8 Why upgrade to v3

Upgrade to V3 Appliance

ASAP

Version 1.1 March 31, Updated March 2017

9 Introduction

This document referes to a general question about appliance upgrade.

9.1 Prerequisites

Appliance v2.X

10 Why shoud I upgrade?

The primary reason to upgrade to a version 3 appliance is that version 2 cannot support TLS versions higher than 1.0, which is now considered obsolete and insecure. Upgrading from version 2 to version 3 involves a complete rebuild, as the operating system is different. Version 4 will use the same operating system as version 3, so there will be an upgrade path.

10.1 EOL - When will it happen?

A grace period ending on 30-09-2017 can be applied to allow our VAD/VAR upgrade their customers to Appliances V3. x

SWIVEL SECURE going to generate download links for VIRTUAL Appliances has requested free of charge. For HARDWARE Appliance customer need to buy new appliances, because that old hardware don?t support V3.x

This operation is FREE OF CHARGE for VAD/VAR/CUSTOMERS if they manage all the upgrades without a need of a Solutions Engineer, in the case that is a request a analyse need to be performed by Solutions Engineer to identify the effort needed in PS days. (Sales Department, can request exceptions when exists a justification).

11 Additional Information

For assistance in the Swivel installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com