

Table of Contents

1 V3 & V4 Appliance Quick Start.....	1
1.1 Quick Start.....	1
1.2 Accessing Appliance Menus.....	1
1.3 Updating Appliance.....	1
1.4 Webmin.....	2
1.5 Setting Hostname IP Address.....	2
1.6 Starting and Stopping Tomcat.....	2
1.7 Accessing the Swivel Applications.....	2
2 V3 Appliance Alerts.....	3
2.1 Alerts.....	3
2.2 Configure the Alerts menu options.....	3
3 V3 Appliance Backup and Restore.....	4
4 Backup and Restore.....	5
4.1 Retrieving Backups from the Appliance.....	5
4.2 Taking a Backup.....	5
4.3 Restoring from a Backup.....	5
4.4 Purging Old Backups.....	6
5 V3 Appliance Bootable Media.....	7
5.1 Introduction.....	7
5.2 Prerequisites.....	7
5.3 Backup your appliance.....	7
5.4 Creating the Bootable Media.....	7
5.5 Connect your appliance to a console.....	8
5.6 Insert the DVD and boot it up.....	8
5.7 Restoring the V3 Factory build.....	8
5.8 Updating the appliance.....	8
5.9 Restore your Appliance Backup.....	9
6 V3 Appliance Database Sync.....	10
6.1 Introduction.....	10
6.2 Database Replication Basics.....	10
6.3 Perform a Manual Sync.....	10
7 V3 Appliance Insufficient Permissions.....	11
8 WinSCP and Insufficient Permissions.....	12
8.1 Commandline access.....	12
9 V3 Appliance Migrate From V2.....	14
9.1 Introduction.....	14
9.2 Prerequisites.....	14
9.3 Upgrade your Version 2 Appliance prior to backup.....	14
9.4 Upgrade your Swivel Core application prior to backup.....	14
9.5 Backup your Version 2 Appliance.....	15
9.6 Retrieve the Version 2 backup files.....	15
9.7 Restore to your new Version 3 Appliance.....	15
9.8 Troubleshooting.....	15
10 V3 Appliance Reference.....	17
10.1 Introduction.....	17
10.2 Main Menu.....	17
10.3 Tomcat Menu.....	17
10.4 Network Menu.....	18
10.5 Appliance Menu.....	19
10.6 Backup and Restore.....	20
10.7 Tools.....	21
10.8 Admin.....	21
10.9 High Availability (HA).....	22
10.10 Version Information.....	23
11 V3 Appliance Retrieve Logs.....	24
11.1 How To: Retrieve Logs.....	24
12 V3 Appliance SSL Certificate.....	25
13 Adding a SSL Certificate.....	26
13.1 Prerequisites.....	26
13.2 Import existing Swivel keystore file.....	26
13.3 Generate new local certificate.....	26
13.4 Generate a self-signed certificate.....	29
13.5 Apply the changes - Restart Tomcat.....	30
13.6 Troubleshooting.....	31
14 V3 Appliance Update.....	32
15 Introduction.....	33
16 Get to the Update Menu.....	34

Table of Contents

17 Update Swivel Core Products.....	35
18 Update CMI Menu.....	36
19 Update System.....	37
20 Install Swivel Sentry.....	38
21 Install / Update Package.....	39
22 Flush Cache.....	40
23 V3 Setup HA Pair.....	41
24 Setting Up a High Availability (HA) Pair.....	42
24.1 What is a HA Pair?.....	42
24.2 Minimum setup required.....	42
24.3 Configure the High Availability menu options.....	42
25 Version 3 Appliance.....	44
25.1 Introduction.....	44

1 V3 & V4 Appliance Quick Start

1.1 Quick Start

```
Swivel Maintenance (c) 2019      Main Menu      VMware Single
Hostname      : test.single.name
Interface : eth8      : 192.168.0.25
Tomcat Status : Running

WARNING: Password still default. This can be changed in Administration
WARNING: No alert email set. This can be set in Tools -> Alerts

1) Tomcat
2) Network
3) Appliance
4) Backup and Restore
5) Tools and Utilities
6) Administration
8) System Status
9) Version Information
0) Exit

Select: _
```

This guide is a quick start guide to the **Version 3 and 4** Swivel Secure Appliances.

A reference guide that describes the meaning for all the menus is also available [here for version 3](#) and [here for version 4](#).

The appliance will come with a pre-configured IP address depending on appliance type:

Stand-alone (192.168.0.35)

HA Primary (192.168.0.36)

HA Standby (192.168.0.37)

Amazon/Cloud (DHCP)

If this IP address is compatible with your network you can plug an ethernet cable into eth0 (labelled Gb1) and access the appliance via SSH.

Alternatively you can access by plugging in an ethernet cross-over cable into eth0

1.2 Accessing Appliance Menus

To access the appliance menus you secure-shell onto the appliance. From a Windows machine you can use a terminal emulator capable of SSH connections, such as putty. From a Linux machine you can simply use the ssh command. SSH access is via the standard port 22.

When you access the appliance you will be prompted for a username and password. The default settings for this are:

- V3 and V4.0 appliances:

username:admin

password:lockbox

- V4.1 and later appliances:

username:admin

password:securebox

Once you have logged on you will be presented with the top level menu. Sub-menus are accessed by simply pressing the number of the item required followed by <Enter>

On certain actions you will be asked to enter Y to continue. Entering any other character or just entering return will cause the action to be cancelled. To maintain compatibility with v2, entering ?yes? will also work.

NOTE Refer to our [PuTTY How To Guide](#) for detailed instructions and screenshots.

1.3 Updating Appliance

Important You should update an appliance prior to installation to ensure it is running the optimum versions and settings

A [reference guide that details the options available for Appliance updating](#) is available.

1.4 Webmin

You can find the [Webmin guide here](#).

1.5 Setting Hostname IP Address

If you are using an Cloud-based appliance, IP addresses must be set by DHCP.

You will need to set the IP address(es) of the appliance. To do this use the access the Network Menu and do the following

1. Use the change hostname to set the hostname. Recommended to make this a meaningful, eg swivel.yourcompany. If this appliance is part of an HA installation include the appliance type eg primary.swivel.yourcompany.
2. Set the Network settings for ETH0. This is the main interface, you may not need to change the ETH1 settings as this is used for database replication (ref Setting up HA)
3. Set DNS servers. This may not be required at this stage but will be required if the Swivel Appliance will need to perform DNS resolution, eg for sending emails or SMS messages via named hosts.

1.6 Starting and Stopping Tomcat

Swivel applications run within Tomcat so you will only be able to access them when Tomcat is running. Tomcat will start automatically when the appliance starts and the status of Tomcat is shown on the main screen and on the Tomcat menu screen.

Should you need to manually start or stop Tomcat, this is possible from the Tomcat menu.

1.7 Accessing the Swivel Applications

With the ETH0 address set to <IP Address> you will be able to access the following applications from a browser:

Swivel Core admin console <https://<IP Address>:8080/pinsafe>. For version 4, this should be <https://<IP Address>:8080/sentry>.

Swivel User (Self Service) Portal <https://<IP Address>:8443/userportal>

Swivel Proxy <https://<IP Address>:8443/proxy>

- The Swivel Proxy has no user interface but acts as a proxy for image and message requests e.g. <https://<IP Address>:8443/proxy/SCImage?username=test> should result in a TURING image being displayed.



2 V3 Appliance Alerts

2.1 Alerts

You can use the built in Alerts feature to setup and receive Disk Space Alerts. The feature is accessible from the **Main Menu -> Tools and Utilities -> Alerts** menu.

To access the Tools and Utilities Menu, login to the Appliance using **PuTTY**.

Each partition can be configured to have a different disk space warning level (%) at which point you will receive an email alert. It's also possible to Add and Remove other disks to be monitored by the Alerts feature.

2.1.1 Minimum setup required

- The mailserver must be configured beforehand, from the **Main Menu -> Appliance -> SMTP Server menu** option. Or via the **.. Alerts -> SMTP Server Menu** menu option;
- An alerts email address must be configured via the **.. Alerts -> Change Alert Email** menu option;
- At least one disk must be configured (default settings will suffice).

2.2 Configure the Alerts menu options

2.2.1 SMTP Server Menu

Use this menu option to enable/disable and configure the system wide SMTP Server settings.

Bear in mind that this requires that you have a mailserver on the network and the ability to relay email from the Swivel appliance, which will likely be located within your network DMZ.

Change Alert Email

You will be prompted to set the Alert Email destination when selecting this menu option.

Change From Address

You will be prompted to set the From Address when selecting this menu option.

2.2.2 Show Disk Space Menu

Status - This menu option is the equivalent of running the `df -h` command on the command line and lists the partition status output in human readable format.

Change Disk Space Warning Levels - You are prompted to choose a particular partition that you want to change the Warning Levels for. The disk space warning level can then be entered as a percentage (e.g. 10%) or a byte amount in human readable format (e.g. 100M).

If the available disk space falls below the disk space warning level, an alert email will be sent.

Add New Disk to Check - This option will prompt you for the name of a mount point of the disk or partition to check. The mount point name you enter should include the forward slash preceding it (e.g. enter `/support` instead of `support`)

Remove Disk from Check - You are prompted to choose a particular partition that you want to remove from the disk space check.

Restore to Default - All partitions and their alert levels will be restored to default settings.

3 V3 Appliance Backup and Restore

4 Backup and Restore

The appliance Backup and Restore menu option can be found on the Main Menu of the Appliance Console Management Interface (CMI). To access the Backup and Restore menu, login to the Appliance using [PuTTY](#).

By default, full backups are made daily on each Swivel appliance at 4 a.m. This section details how to retrieve backups, how to produce various backup types manually and how to restore backups from both this version of the appliance and older versions.

4.1 Retrieving Backups from the Appliance

Backups can be retrieved either manually or automatically from the appliance.

4.1.1 Using WinSCP

Connect to the IP address or hostname of the appliance using the default credentials of Username: admin and Password: lockbox (unless you've changed the default password in which case use your new password)

Once connected you will be in the /home/admin/ directory. From here, navigate up to the /backups directory in the root of the disk (/).

From here you can Download the backup files. Daily backups are stored in /backups/swivel

4.1.2 Using FTP

From the Backup and Restore Menu, select ?Configure FTP?. Enter the server, username, password and destination directory as prompted. Selecting ?Forcibly Send Latest Backup Over FTP? sends the latest backup to your entries and can be used to confirm you have entered them correctly. If an FTP server is provided here, the daily backup will attempt to send the just-made backup to your FTP server just after it creates it.

4.2 Taking a Backup

4.2.1 Full Backup

From the Backup and Restore Menu, select ?Backup?, then ?Full Backup?. This backup type backs up the Tomcat config, Keystore, Webapps, External Database, Swivel home, Swivel config, networking, webmin, mon, heartbeat, sendmail, scripts, drbd, ssh, snmp, profile, user home, database config, tomcat logs.

4.2.2 Application Only Backup

From the Backup and Restore Menu, select ?Backup?, then ?Application Only Backup?. This backup type backs up the Tomcat config, the keystore, Swivel home, Webapps and the database.

4.2.3 System Only Backup

From the Backup and Restore Menu, select ?Backup?, then ?System Only Backup?. This backup type backs up the Tomcat config, the keystore, Swivel config, networking, webmin, mon, heartbeat, sendmail, scripts, drbd, ssh, snmp, profile, user home, database config and tomcat logs. Essentially, the full backup without the application-only items (but with the Tomcat configuration and keystore).

4.2.4 Create Restore Point

From the Backup and Restore Menu, select ?Backup?, then ?Create Restore Point?. This is the same as a full backup, but has a given name, is never purged, and is stored in the /backups/restore folder.

4.3 Restoring from a Backup

4.3.1 Full Restore

From the Backup and Restore Menu, select ?Restore?, then ?Full Restore?. This can attempt to restore from FULL backups stored in /backups/swivel. It tries to restore everything.

4.3.2 Application Only Restore

From the Backup and Restore Menu, select ?Restore?, then ?Application Only Restore?. This can attempt to restore from FULL or APP backups stored in /backups/swivel. It tries to restore only the Tomcat config, the keystore, Swivel home, Webapps and the database.

4.3.3 System Only Restore

From the Backup and Restore Menu, select ?Restore?, then ?System Only Restore?. This can attempt to restore from FULL or SYS backups stored in /backups/swivel. It tries to restore only the Tomcat config, the keystore, Swivel config, networking, webmin, mon, heartbeat, sendmail, scripts, drbd, ssh, snmp, profile, user home, database config and tomcat logs.

4.3.4 Restore Point Restore

From the Backup and Restore Menu, select ?Restore?, then ?Restore Point Restore?. This can attempt to restore from backups stored in /backups/restore. It tries to restore everything.

4.3.5 Restore from older version

Obtain a backup from the v2 appliance you wish to restore from, and place it in /backups/old (e.g. by using [WinSCP](#)).

Next, from the Backup and Restore Menu, select ?Restore?, then ?Restore from Older Version?.

The process will:

- Attempt to restore the Swivel Home, the keystore, the database, mon, heartbeat, snmp, drbd, the relevant items from pinsafe.conf, ssh, some networking items.
- Give you the option to replace the version of Swivel with the one found in the backup, although this is not recommended, since you may as well upgrade at this point.

4.3.5.1 For a HA Appliance Pair with ?Appliance? or ?MySQL 5? database type

Restore the backup from each appliance as above, but be sure to perform a DB Sync via the Database CMI menu afterwards. Give the machine a reboot prior to finish the restore process.

4.3.5.2 For a DR Appliance with ?Appliance? or ?MySQL 5? database type

Restore the backup as above, but be sure to perform a DB Sync with the Primary unit via the Database CMI menu afterwards. Give the machine a reboot prior to finish the restore process.

4.3.5.3 For a Single Appliance with ?Internal? database type

Restore the backup as above. Give the machine a reboot prior to finish the restore process.

4.3.5.4 For a Enterprise HA Appliance Pair with ?Appliance? or ?MySQL 5? database type

Restore the backup from each appliance as above, but be sure to perform a DB Sync via the Database CMI menu afterwards. Give the machine a reboot prior to finish the restore process.

4.4 Purging Old Backups

From the Backup and Restore Menu, select ?Purge Old Backups?. Purging will get rid of any backups older than the number of days you specify to keep. You will be presented with the local system time and date. If the current date shown is wrong, you should proceed carefully as deletion of these backup archives cannot be undone.

5 V3 Appliance Bootable Media

5.1 Introduction

This article is a reference guide detailing the process of restoring a factory build of the V3 appliance to existing customer hardware. The hard disk of the appliance will be wiped during this process so the previous appliance Operating System and data will be unrecoverable.

5.2 Prerequisites

IMPORTANT: These prerequisites are absolutely essential for a successful installation process. If not followed correctly your Swivel appliance may enter an unusable state and you may not be entitled to support. Please read the prerequisites very carefully.

- Your Swivel appliance must be less than five years old;
- A Swivel hardware warranty must be in place before undertaking this restoration process;
- You will need to have an existing Swivel Maintenance Agreement;
- You must perform a backup of your appliance configuration, Swivel configuration and data from your existing appliance CMI menu;
- Your backup must then be copied off the appliance to a safe place, ideally on your Workstation, for restoration later;
- If migrating from a Version 2 appliance to a Version 3 appliance, please observe the prerequisites for the restoration process which is detailed in a separate article [V3 Appliance Migrate From V2](#);
- You must contact your Swivel Reseller in the first instance to obtain the Version 3 appliance Bootable Media ISO file. This is not available for public download and requires a Swivel Maintenance Agreement;
- It is essential for a reliable restore process that Physical DVD media is created from the ISO file;
- You must not only burn the ISO file to a DVD, but also validate the disc after burning;
- Any failed attempt using Virtual Media via the DRAC or any other means other than a Physical DVD inserted into the disc drive of the appliance will not be supported;
- The restoration process is only supported against compatible hardware listed below;
- Physical access is required to insert the DVD or configure DRAC networking (for Keyboard and Monitor). You may need to connect a KVM or Keyboard and Monitor to configure the DRAC networking from the BIOS if this has not already been done. Please verify that you have DRAC access already setup before proceeding.

5.2.1 Prerequisite: Compatible hardware

The below hardware is only compatible for Swivel supplied hardware. You may need to remove the orange Swivel steel faceplate to determine whether the appliance is DELL branded or OEM DELL (unbranded).

- DELL branded PowerEdge R210
- OEM DELL (unbranded) PowerEdge R210
- DELL branded PowerEdge R220
- OEM DELL (unbranded) PowerEdge R220

5.3 Backup your appliance

IMPORTANT: Be sure to copy the backup off the appliance to a safe place, ideally on your Workstation, for restoration later.

5.3.1 Backup Version 2

If backing up an existing Version 2 appliance with the intention of migrating to Version 3, please follow the backup process listed in the [V3 Appliance Migrate From V2](#) article. **This is very important because you will likely need to update your Version 2 appliance to very specific build numbers listed in the article, in order to have a robust and supported migration process, prior to taking a backup of your Version 2 appliance.**

5.3.2 Backup Version 3

If backing up an existing Version 3 appliance, please be sure to take a 'Full Backup' using the CMI menu options provided.

NOTE: Once you have completed the backup be sure to return to this article to begin the process of restoring a Factory build of the Version 3 appliance to your Hardware.

5.4 Creating the Bootable Media

IMPORTANT: Any attempt at using the ISO as Virtual Media via DRAC, USB drive or any other means will not be supported. A physical DVD must be created, validated and inserted into the appliance DVD drive.

You must contact your Swivel Reseller in the first instance to obtain the Version 3 appliance Bootable Media ISO file. This is not available for public download and requires a Swivel Maintenance Agreement.

The ISO file is approximately 2.87GB in size so we recommend downloading this well in advance of any scheduled work taking place.

It is essential for a reliable restore process that Physical DVD media is created from the ISO file.

You must not only burn the ISO file to a DVD, but also validate the disc after burning.

When using the media to restore a Factory build of the Version 3 appliance, the disc must be inserted into the DVD drive. Any attempt at using the ISO as Virtual Media via DRAC, USB drive or any other means will not be supported.

The supported method to burn the disc is Windows 7/8/10 shell menu extension. When you have downloaded the ISO file, right click the file and select 'Burn disc image' to run the 'Windows Disc Image Burner' program. **You must click the 'Verify disc after burning' checkbox to ensure that the burn is validated before using the disc.**

If the burn validation fails you must discard the disc and dispose of it to ensure that it is not accidentally used.

Only one DVD is required during this process as the disc is capable of restoring all of the Version 3 appliance variants: Single, DR, Primary, Standby.

Once a physical DVD has been created you can proceed to the next section.

5.5 Connect your appliance to a console

In order to view and carry out the on-screen instructions after inserting the disc, the appliance must have access to either a KVM with keyboard and monitor leads or a physical keyboard and monitor. Alternatively you may receive monitor output and give keyboard input via the DRAC (Dell Remote Access Controller) but this requires prior networking setup via the BIOS, so may yet still require a physical keyboard and monitor to the appliance.

- The monitor will require a standard 15-PIN VGA RGB connector. The port is located at the rear of the unit;
- The keyboard will require a USB connector. USB ports are available at the front and rear of the unit.

Alternatively if using DRAC:

- The DRAC ethernet port is located to the rear of the appliance and is often denoted with a spanner/wrench symbol;
- Remember: You will need to have configured the DRAC via the BIOS to have a specific network IP prior to attempting to gain access to it from your web browser.

5.6 Insert the DVD and boot it up

The DVD drive is built into the appliance and is a standard component that ships with all compatible hardware listed in the pre-requisites section. Located at the front of the unit, the drive is of slim-line form factor.

To open the drive:

- The appliance must be powered on;
- The button to open the drive is located on the plastic bezel of the tray itself, similar to a DVD drive you might find on a laptop.

After pressing the button, the green status light may flash and the tray should pop out after a short delay. You will need to pull the tray fully out before inserting the disc.

After inserting the disc, close the tray until it clicks shut. Reboot the machine. Be ready to hit the F11 key when prompted, to get to the Boot Options menu.

If you don't hit the key in time, you may need to reboot the appliance again to make another attempt. You should receive confirmation at the top right of the screen if your keypress has been accepted. If you are not registering any key presses from a physical keyboard, you may need to try the keyboard in another USB port.

Select the DVD drive as the boot option and proceed to the next section.

5.7 Restoring the V3 Factory build

NOTE: The hard disk will not be wiped by this process until after the RESTORE command has been issued and the appliance variant you wish to restore has been selected.

After successfully booting the DVD you will see some loading take place. You should be presented with a command prompt.

Please do not proceed unless you have taken a backup as detailed in the previous section [Backup your appliance](#). On the command line, type the word RESTORE in uppercase and press Enter to continue.

NOTE: If you need to back out of this process at this point simply reboot then eject the disc immediately.

If you are able to proceed with the RESTORE command, after some loading you should be presented with a list of appliance variants e.g.: Single, DR, Primary, Standby.

Select the appliance variant that you are entitled to restore. This will invoke the restoration process. If you restore the wrong appliance variant then your appliance will not be supported and your license may be invalidated.

After the restore has completed you should be prompted to reboot the appliance.

5.8 Updating the appliance

It is critical to update the appliance via the Internet after using this restore disc. This is because the disc contents are not always going to be up to date.

If you intend to restore from a Version 2 backup then you will need to manually update some packages to some very specific versions in order to have a successful migration. This is detailed in the below subsection.

5.8.1 Updating for appliance Version 2 migration

If you have taken a backup from an up to date Version 2 appliance, you can use the following instructions to update your Version 3 appliance to the correct packages required in order to have a robust and successful restore of your Version 2 appliance backup.

After the appliance has booted up, login to the CMI using the default credentials of:

- **Username:** admin
- **Password:** lockbox

By entering the menu numbers and pressing Enter, navigate from the "Main Menu" to the "Administration -> Update Appliance" screen.

- Select the "Flush Cache" option to flush the package manager cache. Return to the menu;
- Select the "Install / Update Package" menu option;
- When prompted, enter the package name **swivel-cmi-3.0.1869-881** being careful to enter this exactly as shown. Press Enter to proceed with the update;
- When prompted, enter the package name **apache-tomcat-7.0.59-43** being careful to enter this exactly as shown. Press Enter to proceed with the update;
- When prompted, enter the package name **swivel-PINsafe-3.10.5.3022-35** being careful to enter this exactly as shown. Press Enter to proceed with the update;

5.9 Restore your Appliance Backup

IMPORTANT: The Version 3 appliance should be updated to some specific package versions prior to restoring your Version 2 appliance backup. This is necessary to ensure a successful migration. If you have skipped ahead to this section, please review [Updating for appliance Version 2 migration](#)

If restoring an appliance Version 2 backup that you created earlier you can pickup the [Restore to your new Version 3 Appliance](#), section of the Version 2 migration article to proceed with the Restore of your Version 2 backup.

6 V3 Appliance Database Sync

6.1 Introduction

Prior to performing a database sync you will need to follow the ?Setting Up a High Availability (HA) Pair? section to ensure that your HA Pair is setup correctly.

If your HA Pair is already setup then you can follow this guide to perform a manual sync of the Database.

6.2 Database Replication Basics

When a database is set to replicate the changes that are made on one server (Master) are copied across to the other (Slave) server.

The process for doing this is that when the Master writes a change to the database it logs the change made to a BIN Log.

The Slave copies across that BIN log and makes a local copy of that log file called a Relay Log.

The Slave then processes the transactions in that Relay Log thus making the same changes to the local slave database that were made on the Remote Master database.

A Master server can have many Slaves but a Slave can only have one Master.

6.2.1 Master-Master Replication

A server can be both a Master and a Slave so if they are, as in a Swivel HA Pair, as peers, one is both a Master and Slave to the other so replication works both ways between the two servers.

For replication to work The Master must be set up as a Master so that it creates the BIN Logs Slave must have permission on the Master to read BIN logs Slave IO must be running, this reads the BIN logs across to create RELAY logs Slave MySQL must be running to process RELAY logs.

6.3 Perform a Manual Sync

To access the High Availability Menu, login to the Appliance using PuTTY.

Select the menu option High Availability -> Database Replication.

From this menu you are able to check the replication status and repair replication.

6.3.1 Check the Status

From the .. Database Replication -> Status screen, select the IP of the appliance that you want to check the status of. Any replication errors that need to be addressed prior to a successful repair will be listed here.

6.3.2 Repair Replication

From the .. Database Replication -> Repair Replication screen, select the Peer IP of the appliance that you want to repair replication for.

You will then be prompted to confirm which way you want to synchronise the data.

For example if you select the Local database as the canonical (correct) database, then the Local database will be synced with the Peer you selected.

However if you select the Peer database as the canonical database, the Peer database will be synced to the Local machine that you're logged into.

After selecting which database you want to sync, you will be asked to confirm.

If the sync worked as expected you will receive an ?INFO: Sent database to peer? message.

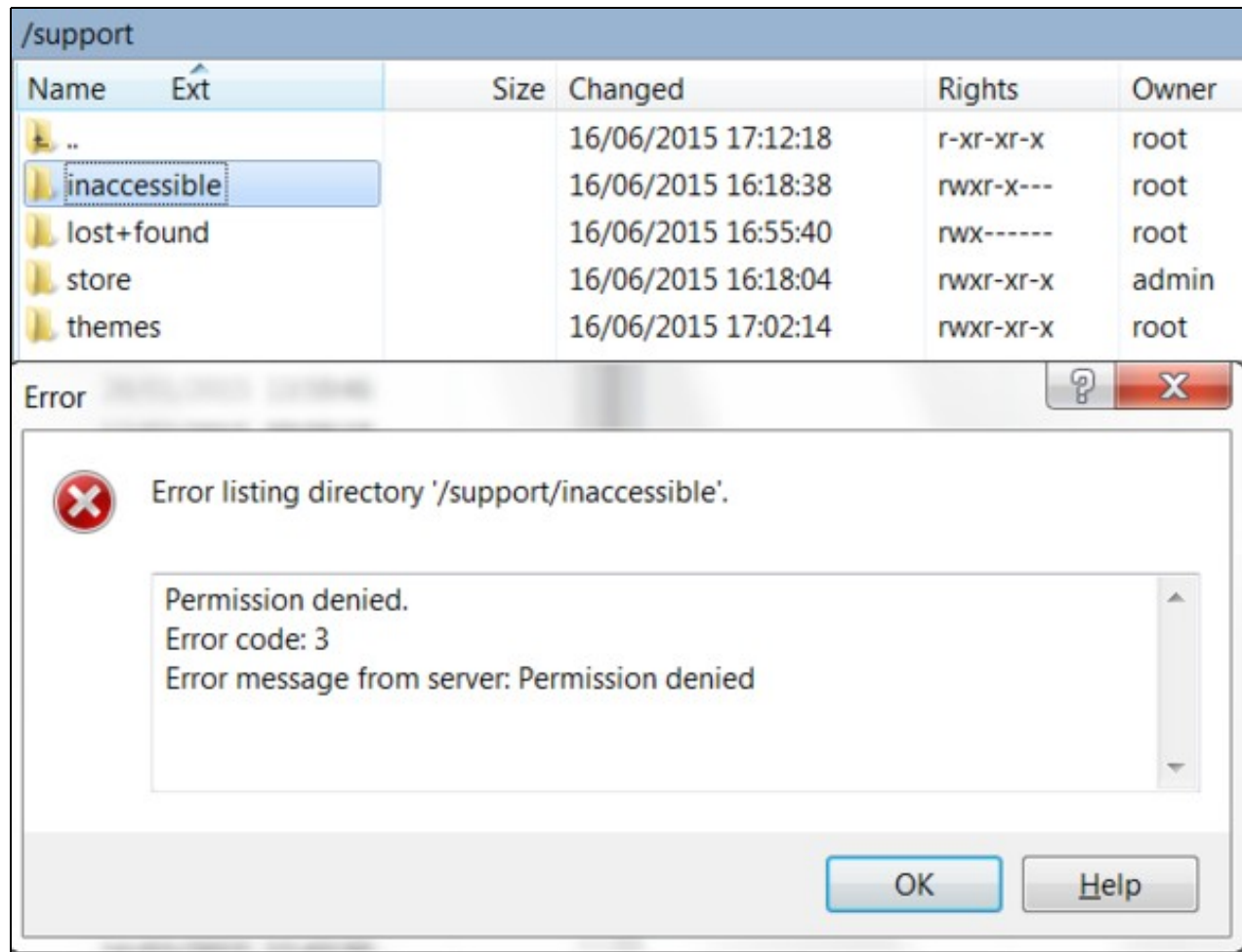
7 V3 Appliance Insufficient Permissions

8 WinSCP and Insufficient Permissions

In versions prior to V3, arbitrary files could be accessed (or replaced) using WinSCP. In V3, this has changed, and the admin user needs the relevant permissions to access or replace files. Most files should still be accessible from WinSCP as usual, but some may require special methods.

8.1 Commandline access

Any file can be recovered using WinSCP using commandline access and a storage space, /support/store. This space is owned by the admin user, and can be used for storing files to WinSCP out.



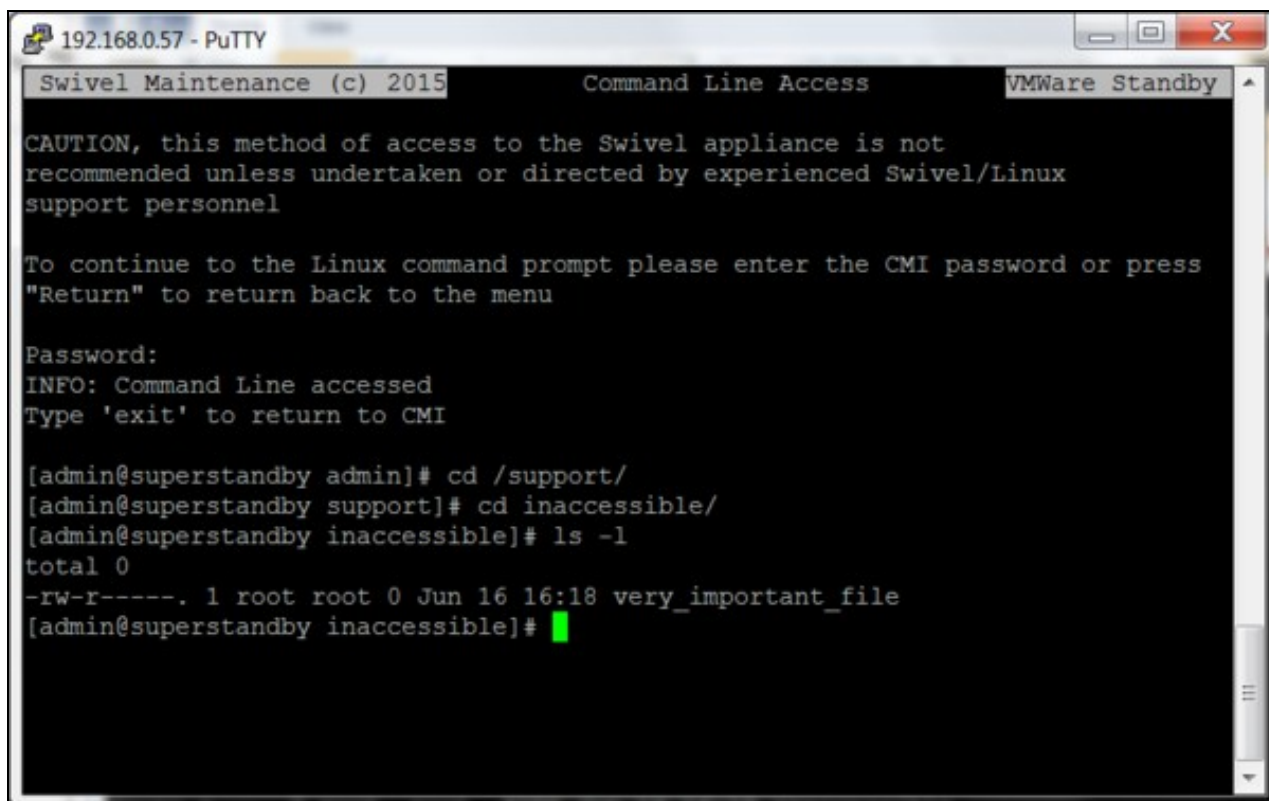
The screenshot shows the WinSCP interface with a directory listing for the /support directory. The listing includes columns for Name, Ext, Size, Changed, Rights, and Owner. The 'inaccessible' folder is highlighted. Below the listing, an error dialog box is displayed with the message: 'Error listing directory '/support/inaccessible'. Permission denied. Error code: 3. Error message from server: Permission denied'. The dialog box has 'OK' and 'Help' buttons.

Name	Ext	Size	Changed	Rights	Owner
..			16/06/2015 17:12:18	r-xr-xr-x	root
inaccessible			16/06/2015 16:18:38	rwxr-x---	root
lost+found			16/06/2015 16:55:40	rwX-----	root
store			16/06/2015 16:18:04	rwxr-xr-x	admin
themes			16/06/2015 17:02:14	rwxr-xr-x	root

Error listing directory '/support/inaccessible'.
Permission denied.
Error code: 3
Error message from server: Permission denied

OK Help

Suppose we wish to access a file within the folder inaccessible, which the admin user does not have access to. We cannot gain privileges from within WinSCP, so we log on to the CMI using a separate instance, and access the command line using Tools -> Commandline. We can then access ?inaccessible?.



```
192.168.0.57 - PuTTY
Swivel Maintenance (c) 2015      Command Line Access      VMWare Standby

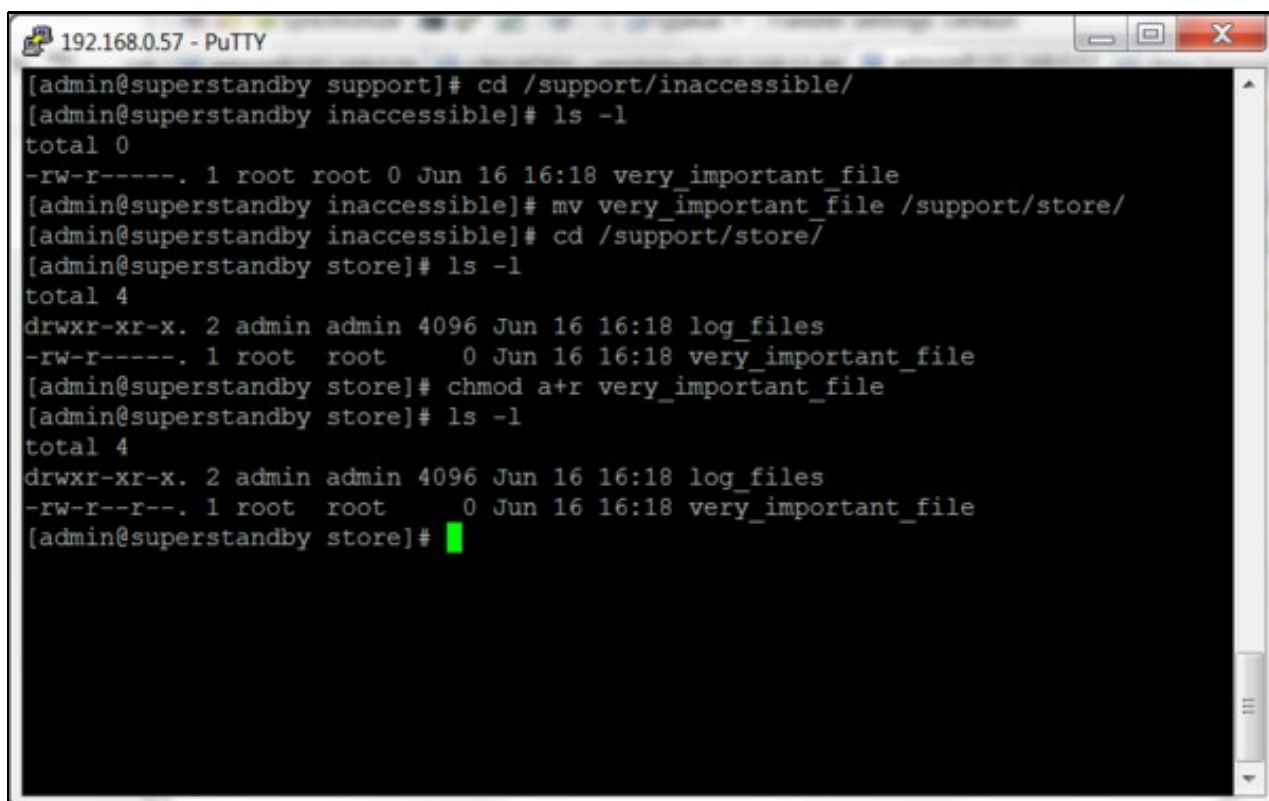
CAUTION, this method of access to the Swivel appliance is not
recommended unless undertaken or directed by experienced Swivel/Linux
support personnel

To continue to the Linux command prompt please enter the CMI password or press
"Return" to return back to the menu

Password:
INFO: Command Line accessed
Type 'exit' to return to CMI

[admin@superstandby admin]# cd /support/
[admin@superstandby support]# cd inaccessible/
[admin@superstandby inaccessible]# ls -l
total 0
-rw-r-----. 1 root root 0 Jun 16 16:18 very_important_file
[admin@superstandby inaccessible]#
```

We can then copy `very_important_file` into `/support/store` (so that the admin user can see it) and give the admin user read permissions (so that we can WinSCP it out).



```
192.168.0.57 - PuTTY

[admin@superstandby support]# cd /support/inaccessible/
[admin@superstandby inaccessible]# ls -l
total 0
-rw-r-----. 1 root root 0 Jun 16 16:18 very_important_file
[admin@superstandby inaccessible]# mv very_important_file /support/store/
[admin@superstandby inaccessible]# cd /support/store/
[admin@superstandby store]# ls -l
total 4
drwxr-xr-x. 2 admin admin 4096 Jun 16 16:18 log_files
-rw-r-----. 1 root root 0 Jun 16 16:18 very_important_file
[admin@superstandby store]# chmod a+r very_important_file
[admin@superstandby store]# ls -l
total 4
drwxr-xr-x. 2 admin admin 4096 Jun 16 16:18 log_files
-rw-r--r--. 1 root root 0 Jun 16 16:18 very_important_file
[admin@superstandby store]#
```

9 V3 Appliance Migrate From V2

IMPORTANT: The following process should only be undertaken by an Accredited partner, with current and specific training relating to the migration process.

Migrations that are attempted, without using a certified technical resource, are outside of normal support cover.

9.1 Introduction

This article is a reference guide detailing the process of migration from Version 2 of the Swivel Appliance to Version 3. It also applies to upgrading to version 4.

Note that you cannot upgrade a version 2 appliance, hardware or virtual, in place. For virtual machines, you must acquire a new image from Swivel Secure, which is free of charge, provided you have a current support contract. For hardware, you can get an ISO image to upgrade the appliance. Note that the hardware appliance must have 4GB RAM for the upgrade to succeed, and the disk is completely reformatted during the upgrade process, so be sure to take your backup before booting from the ISO image.

9.1.1 Improvements over Version 2

- Newer Linux Operating System based on CentOS 6 as opposed to Red Hat 4;
- YUM package management replaces the old proprietary patching system for Swivel applications;
- RPMs are now produced by our Development Team for all Swivel applications and rolled out as YUM updates;
- Now running Java 7 as opposed to Java 6 (Java 8 on version 4.0.5);
- Now running Apache Tomcat 7 as opposed to Apache Tomcat 5 (Tomcat 9 on version 4.0.5);
- Now running MariaDB 5.5 as opposed to MySQL 5.0.

9.1.2 Benefits of upgrading

- Easier installation of updates to Swivel applications due to dependencies being managed at the package level;
- Quicker access to fixes for potential security exploits to the Operating System or Application Server components.

9.1.3 Process Summary

- Update your old Version 2 appliance to build 2.0.16;
- Update your old Version 2 appliance Swivel Core to build 3.10.4 or later;
- Take a Full backup of your old Version 2 appliance;
- Update Appliance on V3/4 to get the latest CMI options;
- Restore the backup to your new Version 3/4 appliance with the same Timezone (timezone cannot be changed);
- Perform further configuration upon your new Version 3/4 appliance (as detailed in this article) if necessary.

9.2 Prerequisites

IMPORTANT: These prerequisites are absolutely essential for a successful migration process.

The migration process utilises the existing Backup process on the Version 2 appliance. Prior to initiating a manual backup as detailed in later sections, you must:

- Upgrade your Version 2 Appliance prior to backup;
- Upgrade your Swivel Core application prior to backup.

These steps are detailed in the below article sections.

Your Version 2 appliance will need to be running **Appliance Build version 2.0.16** and a **Swivel Core build 3.10.4** or later in order to make the transition to the Version 3 appliance as smooth as possible.

Since upgrading your Version 2 appliance may have an impact on your Authentication it is also important to **test that Authentication continues to function** after the upgrade of your Version 2 appliance and **prior to migration to Version 3**.

You must be able to reach the YUM management tool in order to perform the automated updates from yum.swivelsecure.net, which must be allowed access via the firewall to the Swivel servers.

NOTE: If you are upgrading your existing appliance using Bootable Media then you will need to fulfil all of the Prerequisites of the [Version 3 Appliance Bootable Media article](#). **This includes updating the swivel-cmi package on the destination Version 3 appliance to ensure that restore process will work correctly.**

9.3 Upgrade your Version 2 Appliance prior to backup

- The **Appliance Build version 2.0.16** download is available on request from Swivel Secure to customers with current support contracts. The instructions for installing the patch are available at [Patch Swivel Install](#). This will need to be performed first;
- If your Appliance build is older than 2.0.12 then you will need to install 2 patch files in order to get to the latest version;
- After the upgrade, be sure to perform a reboot;
- Test that Authentication still works for your users.

9.4 Upgrade your Swivel Core application prior to backup

You must have at least software version 3.10.4 to perform this upgrade. If you have 3.10.4 or later on your old appliance, you can skip this step.

- The **Latest Swivel Core build, 3.11.5.4741** download is available from Swivel Secure to customers with a current support contract. The instructions for installing it are at [Patch Swivel Install](#). This will need to be performed after the Appliance 2.0.16 update above;
- After the upgrade, be sure to perform a reboot;
- Test that Authentication still works for your users.

NOTE: If you are currently running on a version of Swivel that is below 3.8 then you cannot upgrade directly to v3.10.5.3030 or later. Please contact support@swivelsecure.com for further guidance on how to upgrade.

NOTE: If you have an HA environment, after successfully completing the process on one appliance, do the same on the other.

9.5 Backup your Version 2 Appliance

IMPORTANT: It is currently recommended that a Full Backup is used for the migration due to issues with the Partial Backup only being able to restore the Swivel Core database and not the Swivel Core configuration.

Version 2 appliances have two options for manual backup:

- Full Backup (the "Full backup, including appliance config and Swivel" menu option): which includes the Swivel Core configuration, database, keystore (SSL certificate), proxy configuration. Also includes the Appliance networking, DNS, Mon config, Heartbeat config, SNMP config, DRBD config, hosts file and appliance configuration;
- Partial Backup (the "Backup Swivel, and Swivel configuration files" menu option): which includes the Swivel Core configuration, database, keystore (SSL certificate), proxy configuration.

Login to the Version 2 appliance using **PuTTY**. From the **Main Menu**, select **Backup & Restore Options**. You will then be presented with the above two options.

9.6 Retrieve the Version 2 backup files

You will need to copy the manual backup file you created from the Version 2 appliance file system to your Workstation. You can use **WinSCP** for this task.

- Login to the Version 2 appliance using the **WinSCP** application;
- Navigate to the directory **/backups** (you may need to traverse to the root of the file system first);
- Order the backups by modified date;
- You should be able to find your latest backup based on the time and date;
- Copy the backup file to your Workstation. The backup file has a **.tar.gz** extension, you do not need the file with the **.info** extension of the same name.

9.7 Restore to your new Version 3 Appliance

NOTE: On the Version 3 appliance there is a dedicated menu option (**Restore from v2 Appliance**) and file system directory (**/backups/old**) for restoring a backup from a Version 2 appliance

IMPORTANT: If you are restoring to a Version 3 appliance you have created from Bootable Media recovery disc then you need to update some packages first. Please be sure to review the **Updating the appliance** section of the Version 2 migration article prior to restoring your Version 2 backup.

You now need to copy the manual backup file you created from your Workstation to the Version 3 appliance. You can use **WinSCP** for this task.

- Login to the Version 3 appliance using the **WinSCP** application;
- Navigate to the directory **/backups/old** (you may need to traverse to the root of the file system first);
- (Do not confuse this for **/backups/restore!** **This is for Version 3 backups only!**);
- Copy the backup file with the **.tar.gz** extension to **/backups/old**.

The next steps involve using the CMI menu of the Version 3 appliance. You will need to login to the appliance using **PuTTY**:

- Login to the Version 3 appliance using the **PuTTY** application;
- From the **Main Menu** select **Backup and Restore**;
- From the **Backup and Restore** menu select **Restore**;
- From the **Restore** menu select **Restore from v2 Appliance**; *If the menu option says "Restore from older version" - you must perform an 'Update Appliance' first.*

NOTE: If you have not placed the backup files into the correct directory **/backups/old** then the menu will complain at this point!

- The backup you placed into **/backups/old** will be listed as a Restore option;
- Select the backup to restore from, you will be prompted to accept a warning;
- You will then be prompted to select the type of Restore you want to perform:
 - ◆ Restore Full backup archive;
 - ◆ Restore Swivel Core, proxy and user portal configs, DB and .keystore;
 - ◆ Restore Swivel DB only;

NOTE: After restoring your data using the Full backup archive option, a reboot is recommended.

9.7.1 Post restore considerations

For the 'Full backup restore' option you will notice that the IP address is not restored until after a reboot, hence why the reboot is recommended. On a HA pair you will need to perform a DB sync to the other peers via the 'High Availability' menu option.

The 'Swivel Core, proxy and user portal configs, DB and .keystore' restore option will not affect the appliance configuration and does not require a reboot. On a HA pair you will need to perform a DB sync to the other peers via the 'High Availability' menu option.

After restoring a 'Swivel DB only' option you will find that the database is available immediately. On a HA pair you will need to perform a DB sync to the other peers via the 'High Availability' menu option.

9.8 Troubleshooting

The backup .tar.gz not appearing in the CMI after placing the file within /backups/old

You must select a backup .tar.gz that has a date/time stamp as a filename. If you use latest.tar.gz, this will not be read by the CMI.

When performing an 'Update Appliance' or 'Update Swivel Core': Could not retrieve mirrorlist

<http://yum.swivelsecure.net/centos/6/mirrors-webmin> error was 14: PYCURL ERROR 6 - "Couldn't resolve host 'yum.swivelsecure.net'"

Ensure that a DNS server is configured under Network > DNS. Additionally, you must ensure that the Swivel server is allowed access to yum.swivelsecure.net on the firewall in order to perform the automated updates via the YUM management tool.

Could not retrieve mirrorlist <http://yum.swivelsecure.net/centos/6/mirrors-webmin> error was 14: PYCURL ERROR 6 - "Couldn't resolve host 'puias.math.ias.edu/data/puias/computational'"

Please contact supportdesk@swivelsecure.com as the mirrors are trying to read from the external YUM repositories rather than yum.swivelsecure.net.

10 V3 Appliance Reference

10.1 Introduction

This is a reference guide for Version 3 of the Swivel Appliance. It describes the function of each menu.

It should be used in conjunction with the How to guides and quick start guide.

10.2 Main Menu

1	Tomcat
2	Network
3	Appliance
4	Backup and Restore
5	Tools and Utilities
6	Administration
7	High Availability
8	System Status
9	Version Information
0	Exit

Most of the items on this menu have sub-menus described below. The exception are:

Version Information: Lists versions of the installed software on this appliance.

Exit: Logs out of the Console. **0** will always return to the previous menu from all sub-menus.

Note that the High Availability menu is not shown on stand-alone appliances.

10.3 Tomcat Menu

1	Start/Stop	Start or Stop Tomcat as required
2	Restart	If Tomcat is running it will be stopped and the restarted. If Tomcat is not running, it will be started
3	HTTPS	Sub menu that allows you to Enable or Disable https on either port 8080 or 8443 as required. Requires Tomcat Restart to take effect
4	Certificates	Opens a menu for managing certificates
5	SSL Protocols	Opens a menu to enable or disable SSL protocols

10.3.1 HTTP(s) Menu

1	Enable/Disable HTTPS on Port 8080	Enables or disables HTTPS for Swivel Core (port 8080)
2	Enable/Disable HTTPS on Port 8443	Enables or disables HTTPS for Sentry and auxiliary applications (port 8443)

10.3.2 Certificates Menu

1	Create Local Certificate	Use this option to Generate a Local Certificate, which can then be signed by a Certificate Authority.
---	--------------------------	---

2	Generate CSR	Generate a Certificate Signing Request from an existing certificate alias
3	Import to New/Existing Alias	Sub-menu to import a Certificate Response from a Certificate Authority on top of the existing alias that the Certificate Signing Request was generated from, or to import a trusted root certificate.
4	View Keystore	View the contents of the Keystore, either by selecting one alias in particular or choose to view everything.
5	Delete Certificate from Keystore	Delete a certificate from the Keystore by selecting a particular alias name.
6	Generate Self-Signed Certificate	Use this option to Generate a Self-Signed Certificate.
7	Clone Certificate	This option can be used to clone a Certificate by specifying the alias name of the certificate you wish to clone and providing a new alias name for the clone. This is useful for backing up aliases prior to making changes such as importing responses
8	Import / Roll Back to Previous Keystore	Each time a change is made to a Keystore, a backup is created. This option allows you to rollback to one of those backups and they are labelled according to date and time. You can also use this option to import from an external keystore.
9	Change Keystore Password	Use this option to change the password for the certificate keystore

10.3.2.1 Import Menu

1	Import to New Alias	Import a trusted root certificate
2	Import Response to Existing Alias	Import a certificate response to an alias that has previously been used to generate a CSR

NOTE:

- All trusted root certificates **MUST** be imported **before** the response which they have been used to sign.
- Certificates must be uploaded to /backups/upload prior to using this menu.

10.3.3 SSL Protocols Menu

1	Enable/Disable TLSv1.0
---	------------------------

As the caption for this menu states, TLSv1.0 is deprecated and insecure, but is required by some legacy applications. Use this option under advice from your reseller or Swivel Secure support.

10.4 Network Menu

1	Change Hostname	Set the hostname of the appliance.
2	Change IP address	Displays a sub-menu to change the IP address of either of the network interfaces
3	Change Default Gateway	Change the default gateway IP address
4	NIC Settings	Allows for the setting of the bit rate negotiation for the network interfaces. Default is Auto-Negotiation
5	DNS	Allows for the adding and removal of DNS servers for the appliance to use for domain-name resolution.
6	HTTP Proxy	If the Swivel Appliance has to make outbound http connections via an http proxy, those proxy settings can be set here. This includes proxy IP Address, Port and username/password if required.
7	NTP Servers	The Swivel appliances run an NTP Daemon. This menu allows you to edit the list of NTP servers that this daemon will use to keep the Appliance server time accurate.
8	Route Configurations	This allows you to create custom routes, see below

9	Restart Interfaces	Restart the Network interfaces. This may be required to allow new settings to take effect
---	--------------------	---

10.4.1 Route Configurations Menu

1	Show Route Table	This displays the default rules for routing traffic. Typically it will show that the default route (for destination IP 0.0.0.0) to be routed via the gateway defined under the Network menu
2	Add Route	By default outbound traffic will be routed via the defined gateway. You can specify exceptions to this rule by adding custom routes to the routing table. For example if you require traffic to IP addresses 12.19.19.xxx to be routed via the gateway 172.1.1.1 you would create the route IP address 12.19.19.0 Netmask 255.255.255.0 Gateway 172.1.1.1
3	Delete Route	You can delete one or all of the custom routes that you have added. This will have no effect on the default routing table.

10.5 Appliance Menu

1	Default running services	The default running services are those services that will start automatically when the appliance boots. It is recommended that you only start the services your required as starting non-configured services can increase boot times.
2	Start/Stop Services	Manually start or stop any of the Appliance services
3	SMTP Server	Configure an SMTP server to which to send Appliance alerts
4	Set Database to Shipping	Sets the Swivel Core database to Shipping Mode to allow access using default credentials. A Tomcat restart is required

10.5.1 Default Running Services

	Service	Description	Default
1	Tomcat	Host server for Swivel Applications	ON
2	Sendmail	Required to use Appliance as a mail relay server	ON
3	SNMP	For Network Management (if required)	OFF
4	Database	Appliance Database service	ON
5	Webmin	Web based GUI alternative for Appliance management	OFF
6	Heartbeat	Use for HA installations to determine status of peer appliance	OFF
7	Database	Use for HA installations to determine status of peer application server	OFF

10.5.2 Start/Stop Services

	Service	Description
1	Tomcat	Host server for Swivel Applications
2	Sendmail	Required to use Appliance as a mail relay server

3	SNMP	For Network Management (if required)
4	Database	Appliance Database service
5	Webmin	Web based GUI alternative for Appliance management
6	Heartbeat	Use for HA installations to determine status of peer appliance
7	Database	Use for HA installations to determine status of peer application server

10.5.3 SMTP Server

1	Enable/Disable SMTP	Enable or Disable the sending of alerts via email
2	Change SMTP server	Select this option to enter a hostname or IP address of the SMTP server you wish to relay email to, from the appliance.

10.6 Backup and Restore

1	Backup	This option takes you to the Backup submenu. From here you can choose from a multitude of manual Backup types.
2	Restore	This option takes you to the Restore submenu. From here you can choose from a multitude of Restore types.
3	Purge Old Backups	Use this option to get to the Purge menu. Here you can define how many days to retain backups and manually purge them
4	Configure FTP	Use this option to define your FTP server details. You can also manually send the latest backup to your FTP server.

10.6.1 Backup Menu

1	Full Backup	This option takes a full backup of the Swivel Application including the Swivel configuration, database, Tomcat certificate keystore. The Appliance settings are also backed up.
2	Application Only Backup	This option takes a backup of the items necessary to restore the application. the Tomcat configuration and keystore, the Swivel home folder contents, and the Tomcat webapps and the database.
3	System Only Backup	This option takes a backup of the items more central to the system than the application. Effectively, it's everything in the full backup that isn't in the application backup (and the tomcat config and keystore).
4	Create Restore Point	This option takes a full backup which is never purged and has an assigned name.

10.6.2 Restore Menu

1	Full Restore	This option lets you restore from any full backup present in /backups/swivel.
2	Application Only Restore	This option lets you restore only appliance-level files from any full or appliance backup present in /backups/swivel.
3	System Only Restore	This option lets you restore only system-level files from any full or system backup present in /backups/swivel.
4	Restore Point Restore	This option lets you restore from any restore point backup present in /backups/restore.

5	Restore from Older Version	This option lets you restore from v2 backups present in /backups/old
---	----------------------------	--

10.6.3 Configure FTP Menu

1	Modify FTP Server	Modify the features of the assigned FTP server: server, destination folder, user, password
2	Delete FTP Server	Delete the assigned FTP server, and stop sending backups using FTP.
3	Forcibly Send Latest Backup Over FTP	Send backups to the FTP server manually. If backups aren't being sent, the error message from this command could be helpful in debugging the problem.

10.7 Tools

1	Ping	Allows you to ping a hostname or IP address to test DNS and network connectivity
2	NS Lookup	Perform a DNS lookup on a hostname
3	Telnet	Attempt a telnet session to a remote host and port
4	Trace-Route	Lists the hops between the appliance and a remote host
5	Command Line	Allows access to the command line, requires command line password, contact support@swivelsecure.com
6	Email logs	Collects log information and sends to an email address, requires SMTP server to be set
7	Alerts	This allows to enable an email alert to be sent if there is a disk space warning. (See Disk Space)

10.7.1 Disk Space

1	Status	Shows the current usage of the Appliance disk partitions
2	Change Warning Levels	Allows you to set the level at which a warning will be sent indicating that the partition has gone above capacity expected for normal operation
3	Add Disk to Check	Allows you to add a new partition to be have its usage monitored
4	Remove a Disk from Check	Remove a disk from the list to be checked
5	Restore to Defaults	Restores the partition usage thresholds back to their default settings.
6	Email logs	Collects log information and sends to an email address, requires SMTP server to be set
7	Alerts	This allows to enable an email alert to be sent if there is a disk space warning. (See Disk Space)

10.8 Admin

1	Change Admin Password	Changes the password required to access the Appliance Menus. If you do change this password please keep a secure record . if you lose this password Swivel Secure may not be able to regain access to the appliance
2	Add Certificate	It is possible to use certificate based authentication to access the Appliance. This menu allows you to add that certificate

3	Deauthorise Default Certificates	Remove the ability to log on to the appliance using the default certificates stored in /root/.ssh. Ensure you have some other way of logging in before doing this!
4	Reboot	Reboots the appliance.
5	Shutdown	Shutdown the appliance, use with caution if remote from appliance
6	Update Appliance	The appliance will contact Swivel Secures servers and install any applicable upgrades.

10.9 High Availability (HA)

1	Set Peer IP	<p>In an HA configuration there are two servers that act as peers and possibly others that act as Disaster Recovery. Peer servers replicate data between each other (Master-Master replication)</p> <p>This menu option allows you to set the details of the appliance that is the peer appliance in the HA pair.</p> <p>You can set</p> <p>The Peer Hostname Needs to match the setting set on the peer appliance</p> <p>Peer IP addresses for ETH0 and ETH1</p> <p>By default the database replication traffic is routed via eth1. If required it can be routed of ETH0 by using the change replication interface option</p>
2	Set DR IP	<p>A DR Appliance has Master-Slave replication. This means changes made on this appliance will be replicated across to the DR Appliance but changes made on the DR appliance will not be reflected back.</p> <p>This menu allows you to add a DR Appliance to this Appliance so that database replication logs will be available to the configured DR Appliance.</p> <p>You can add up to 2 DR Appliances.</p> <p>All that is required is to enter the IP address of the DR appliance</p>
3	Database Replication	Start and Stop replication and view the status. see Database Replication
4	Virtual IP	<p>An HA pair can share a virtual IP address. If this is enabled then by default primary server will respond to that IP address. In the event that the primary server goes off-line the standby server will respond. The switchover is initiated via Mon or Heartbeat services. See Virtual IP</p>
5	Advanced	<p>Change hostnames, IPs for HA. Not usually required as defaults will usually be ok or changes will be made when setting Peer IP address in HA menu</p>

10.9.1 Database Replication

1	Status	<p>Replication will take place between peers and between peers and DRs. This menu will allow you to view the status of replication between this appliance and its peer or its DR</p> <p>The status will show if the Remote Appliance is reading the database changes made locally and (in the case of a peer) vice-versa</p>
2	Start/Stop Reading updates	Starts or stops the reading of updates from the remote peer. Equivalent to starting and stopping the slave.
3	Database Replication	Start and Stop replication and view the status. see Database Replication
4	Repair Replication	<p>If replication stops (or has never started) this option allows the databases to be brought into to line and for replication to start. To do this select the database that you want to be the version to use. This data will be copied to both servers and replication will be re-started.</p>

10.9.2 Virtual IP

1	Set Email Address	An email alert will be sent in the event of a failover of the VIP from one server to the other (requires SMTP server to be set up). This sets the destination email address for this alert
2	Change Virtual IP	This sets the value for the virtual IP. This needs setting on both peer appliances.
3/4	Add/Remove Ping Nodes	One way that will be used to determine which Appliance should be responding on the virtual IP is to compare how many ping nodes each server can ping. The default gateway is usually a ping node but others can be added. The same number of ping nodes should be set on both appliances
5	Start/Stop Mon	Mon monitors whether the Swivel core is running on the peer appliance
6	Start/Stop Heartbeat	Heartbeat monitors whether the peer appliance is contactable via either network interface

10.10 Version Information

Lists version numbers of installed software on the appliance.

11 V3 Appliance Retrieve Logs

11.1 How To: Retrieve Logs

In the event that you need to retrieve logs for support or diagnostic purposes, there are a number of methods available:

1. Use the built in wizard to generate a tar.gz file containing all system diagnostics. This can be forwarded to a support representative;
2. Retrieve the log files using a third party tool called WinSCP (drag and drop over port 22 / secure copy);
3. As a last resort you could also simply view the logs via a console session (SSH port 22).

11.1.1 Using the Built-in Wizard

You can use the built in **Collect Support Logs** wizard to generate a tar.gz file. The wizard is accessible from the **Tools and Utilities Menu** which is available from the Main Menu.

To access the Tools and Utilities Menu, login to the Appliance using PuTTY (see [PuTTY How To Guide](#)).

This feature will give you the option to either:

- Generate a file containing the support logs in a specific location (which you will retrieve yourself using WinSCP).
- Have the support logs emailed to you. However, this requires that you have a mailserver on the network and the ability to relay email from the Swivel appliance, which will likely be located within your network DMZ.

The mailserver can be configured beforehand, from the **Main Menu -> Appliance -> SMTP Server** menu option.

The email subject line will be: ?Swivel Appliance Logs?

11.1.2 Using WinSCP

If you know the filename of the particular log file that you wish to retrieve, you can retrieve it manually using WinSCP (see [WinSCP How To Guide](#)). Please be aware however that the latest version of the appliance is more restrictive. See [Appendix B](#) for more information about the changes which will likely result in you having insufficient permissions that in previous versions.

11.1.3 Viewing Logs via Console

Whilst this is possible, it's not recommended as it requires command line access. Should you not be in a position to retrieve logs via the other methods mentioned, please contact your Swivel Support Representative for further assistance.

12 V3 Appliance SSL Certificate

13 Adding a SSL Certificate

If you have an existing keystore on an older Swivel appliance that you wish to repurpose on a newer Swivel appliance, then it is possible to import it using the menu in the new Swivel appliance. See the section [Import existing Swivel keystore file](#).

If you don't have an existing keystore to import, you can generate a new certificate to be signed by a Certificate Authority. See the section [Generate new local certificate](#).

If you just want a self-signed certificate for testing purposes then you can either use the default self-signed certificate that ships with the appliance by default, or generate a new self-signed certificate with a custom Common Name (CN) / sitename e.g. acme.customersite.com. See the section [Generate a self-signed certificate](#).

13.1 Prerequisites

- Public DNS record for the Swivel instance, usually resolving to a Public IP address;
- Certificate Authority to sign a Certificate Signing Request (CSR);
- Full appliance backup or copy of the /home/swivel/.keystore file, in case things don't go to plan;

13.2 Import existing Swivel keystore file

A backup of the original keystore will be taken as part of the process, named with the date that you tried to replace the keystore. This can be restored using the 'Roll Back' option in the menu, provided that not too much time has passed.

Using WinSCP (see [WinSCP How To Guide](#)) copy the keystore you wish to import to /backups/upload. From the Certificate Menu, select 'Import / Roll Back to Previous Keystore?', then 'Import Keystore?'

```
Swivel Maintenance (c) 2015          Certificate Menu          VMWare Primary

PrivateKeyEntry      : selfsigned

#####
Upload your keystore
to /backups/upload
#####

Contents of /backups/upload
1) .keystore.20150630141122
2) .keystore
3) REFRESH DIRECTORY
0) Cancel

Select filename: 1
Revert keystore to /backups/upload/.keystore.20150630141122
Enter Y to confirm: y
INFO: Replaced current keystore with uploaded
This will require a tomcat restart to take effect
Do this now?
Enter Y to confirm: y
INFO: tomcat was stopped
.....
```

Select the keystore you wish to restore to and restart tomcat as prompted. The keystore will be renamed and given the appropriate permissions.

13.3 Generate new local certificate

If you don't have an existing keystore to import, as per the above instructions, you can generate a new certificate.

In summary, the process is as follows:

- Create a new local certificate on the appliance;
- Generate a Certificate Signing Request (CSR) for the new local certificate;
- Submit the CSR to your chosen Certificate Authority (CA) online, for signing;
- The CA will provide a response which contains the signed certificate, possibly some Intermediate *Certificates and a Root certificate;
- Import the CA Root Certificate to the Keystore;
- Import any CA Intermediate Certificates (there may be multiple Intermediates and they go by various names depending on the CA e.g. Primary and Secondary Intermediates);

The process is now described in detail:

13.3.1 Create Local certificate

From the Certificate Management menu, select the **Create Local Certificate** option.

```
6) Delete Certificate from Keystore
7) Generate Self-Signed Certificate
8) Clone Certificate
9) Roll Back to Previous Keystore
0) Back
```

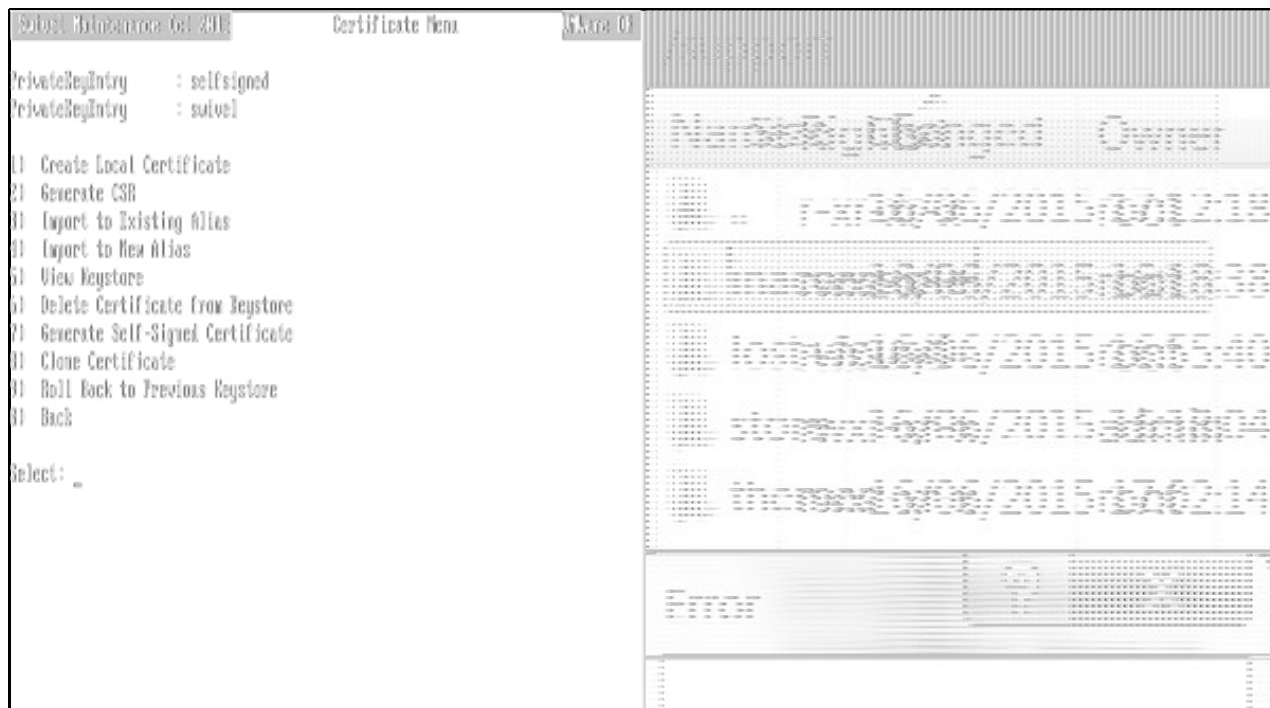
Select: 7

Example:

```
Domain Name      : pinsafe.swivelsecure.com
Company Name     : Swivel Secure Ltd
Department       : IT Department
City             : Wetherby
County          : West Yorkshire
Country Code     : GB
```

```
Enter domain, or press RETURN to use default (Unknown): test.domain.com
Enter Company Name, or press RETURN to use default (Unknown): Example Company
Enter Department, or press RETURN to use default (Unknown): IT Department
Enter City, or press RETURN to use default (Unknown): London
Enter County, or press RETURN to use default (Unknown): Westminster
Enter Country, or press RETURN to use default (Unknown): GB
INFO: Certificate created, alias selfsigned
Press RETURN to continue: _
```

A new alias of ?swivel? will appear in the certificate list as a ?PrivateKeyEntry?:



At this point, you can delete the ?PrivateKeyEntry? named ?selfsigned? that shipped with the appliance (using the **Delete Certificate from Keystore** option), otherwise this will conflict with the new alias that you have created.

13.3.2 Generate Certificate Signing Request

Before generating a Certificate Signing Request (CSR), you must create a local certificate as detailed in the previous section.

To generate a CSR from the new local certificate, select the **Generate CSR** menu option from the Certificate Management menu screen.

Note: If you haven't yet deleted the ?selfsigned? alias you will be prompted to delete it now.

Select the ?swivel? alias from the list:



The CSR will be created as a text file named swivel.csr. You can retrieve the file from the appliance using WinSCP (see [WinSCP How To Guide](#)). As the screenshot suggests, the location of the file is:

/backups/upload/swivel.csr

13.3.3 Submit the CSR to your chosen Certificate Authority (CA)

The contents of the ?csr? file can be submitted to your chosen CA. Assuming that this is a commercial Certificate Authority, then usually they will respond within 24 hours.

You will usually have to paste the contents of the CSR file into the CA's web page. Notepad or a similar text editor e.g. Notepad++ is most appropriate for copying the text.

The response, typically by email after purchase through a website, may include:

- Download links to the generic CA Root Certificates;
- Download links to the generic CA Intermediate Certificates;
- You may be provided with a ?certificate bundle? containing the CA Root and CA Intermediates bundled into one certificate - we would recommend avoiding this and instead importing the certificates as separate aliases, since bundles have not always been reliable;
- The unique, signed response of the certificate you generated, which you will import on top of the ?swivel? alias at the end of the import process;

Note: You may not receive Download Links by email or indeed any information pertaining to the Root and Intermediate certificates, from the CA. If this is the case, you will need to visit the CA website to obtain them prior to importing the signed response into the Keystore. This is because if they aren't imported prior, you will receive an error ?Could not establish chain from reply?. Your signed response is essentially useless without them.

The Download Links provided by the Certificate Authority to the Root and Intermediate(s), may provide links to alternative Root and Intermediate certificates which do not apply to the SSL Certificate product you purchased. Hence you need to be careful to download only those Root and/or Intermediates that apply to the product you purchased in order for the import to be successful.

13.3.4 Import the Certificates

The certificates need to be imported in a specific order:

1. Import the Root certificate, with a unique alias name, e.g. ?root?. By importing this first, all the subsequent imports will be able to establish a chain from it. You may find that you are told that this is already imported into the ?system-wide keystore? which is separate to the keystore you are working with. That's OK, but it's probably wise to import it into this keystore anyway if prompted - so that the keystore and entire certificate chain is self contained should you migrate systems later;
2. Import the Intermediate certificate(s), with unique alias names e.g. ?intermediate1? and ?intermediate2?. There may only be one Intermediate depending on your Certificate Authority and how they operate. Once an Intermediate is imported, then your unique signed certificate will be able to establish a chain from it (and the Root certificate imported earlier);
3. Once the above certificates are in place, you can import the signed certificate onto the ?swivel? alias. The ?swivel? alias is the default alias name when you create a new local certificate. You should receive a success message at this point such as ?Certificate was added to keystore?. Alternatively you may receive a failure message such as ?Failed to establish chain from reply?. In this situation it is wise to check that you have imported the correct Root and Intermediate certificates prior, that are relevant to the SSL/TLS product you purchased. If you are

not sure, contact your CA support who will be able to confirm.

Now you have imported the Certificates, see the section [Apply the changes - Restart Tomcat](#) to make the changes take effect.

13.4 Generate a self-signed certificate

If you need to create a self signed certificate, do not wish to use a commercial certificate signed by a Certificate Authority and have no need for the default self-signed certificate that ships with the appliance, then you can generate your own.

13.4.1 Prerequisites

- Prior to doing this you will need to delete the existing self-signed certificate.

See the section [Delete the existing self-signed certificate](#).

- It's advisable to ensure that you have taken a Backup first.

See the section [Taking a Backup](#).

13.4.2 Delete the existing self-signed certificate

From the Certificate Menu, select the ?Delete Certificate from Keystore? option. Select the certificate aliases you want to delete until there are no more entries left.

13.4.3 Generate Self-Signed Certificate

From the Certificate Menu, select the ?Generate Self-Signed Certificate? option. You will be prompted to enter various attributes to create the certificate:

```
6) Delete Certificate from Keystore
7) Generate Self-Signed Certificate
8) Clone Certificate
9) Roll Back to Previous Keystore
0) Back

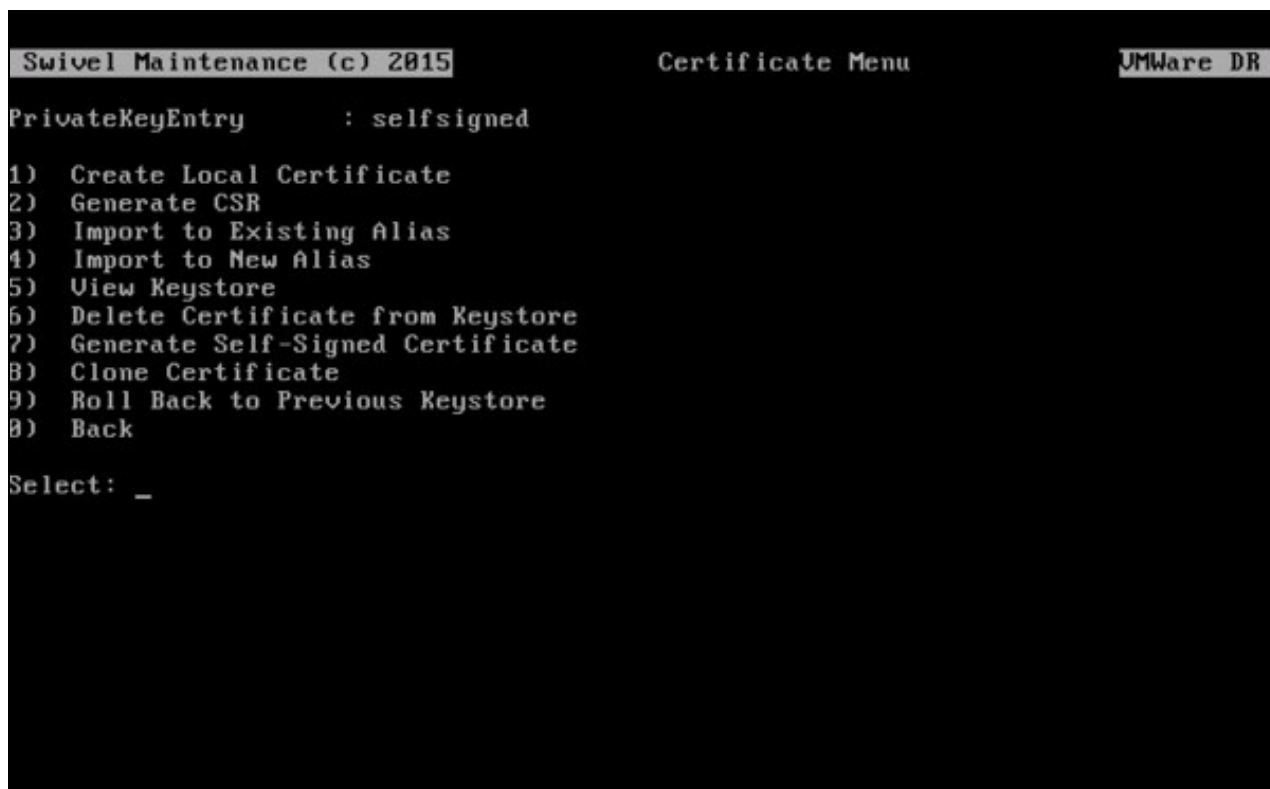
Select: 7

Example:

Domain Name      : pinsafe.swivelsecure.com
Company Name     : Swivel Secure Ltd
Department       : IT Department
City             : Wetherby
County          : West Yorkshire
Country Code     : GB

Enter domain, or press RETURN to use default (Unknown): test.domain.com
Enter Company Name, or press RETURN to use default (Unknown): Example Company
Enter Department, or press RETURN to use default (Unknown): IT Department
Enter City, or press RETURN to use default (Unknown): London
Enter County, or press RETURN to use default (Unknown): Westminster
Enter Country, or press RETURN to use default (Unknown): GB
INFO: Certificate created, alias selfsigned
Press RETURN to continue: _
```

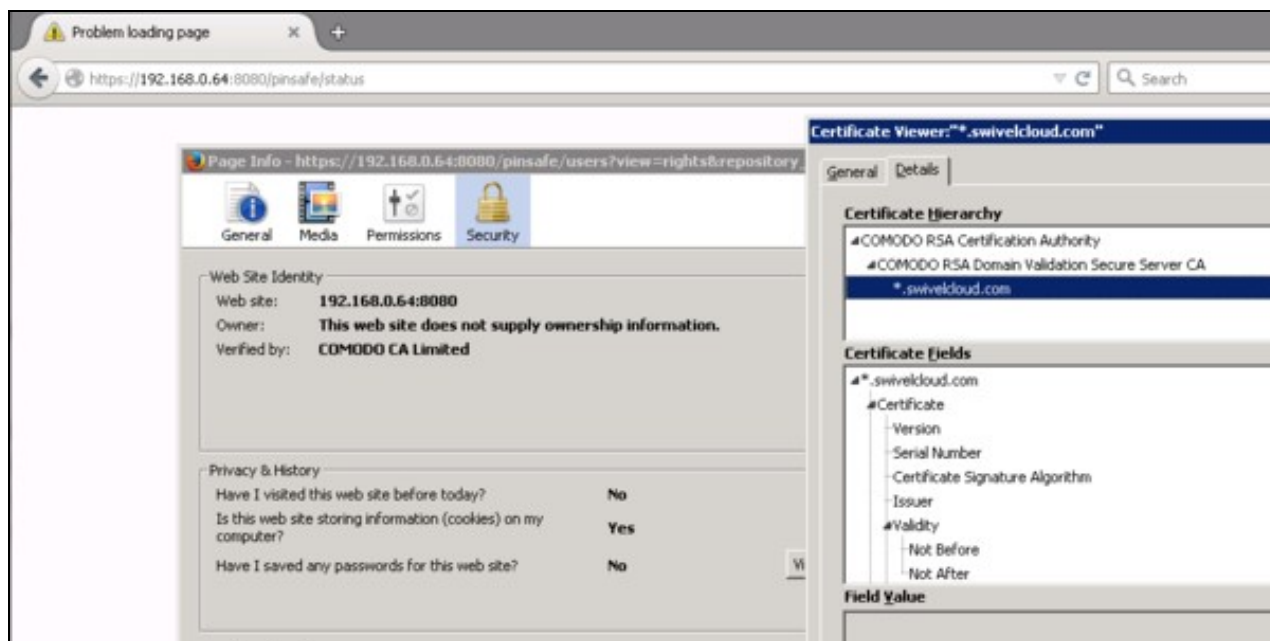
Once created, the certificate will appear as a PrivateKeyEntry alias named ?selfsigned?:



Now you have generated the Self-Signed Certificate, see the section [Apply the changes - Restart Tomcat](#) to make the changes take effect.

13.5 Apply the changes - Restart Tomcat

Once you restart the Tomcat service, the new keystore contents will be loaded. After the restart you can check the Certificate using a web browser. When the Swivel Core is operating in HTTPS mode, you can inspect the certificate padlock icon in the web browser address bar to reveal more information about the sitename or Common Name (CN). You should also be able to see the certificate chain/hierarchy when you view the certificate, containing all the certificates you imported (see the Certificate Hierarchy in the picture below).



Note: When you view the certificate in the browser, it's wise to enter the actual Fully Qualified Domain Name into the browser address bar, matching the site name of the certificate.

As an example, assuming that the Public DNS record is active and resolving, and the sitename/Common Name (CN) of the certificate was core.swivelsecure.com then you would visit:

<https://core.swivelsecure.com:8080/pinsafe>

If you don't use the sitename as above and instead use the local or public IP address as shown in the picture above, then this will cause the web browser to report that the certificate is 'invalid'. This is because the sitename of the certificate will not match the IP address in the address bar. Only until the hostname in the address bar matches the Common Name (CN) of the certificate, will you resolve the 'invalid' certificate issue.

If you still get an invalid certificate after eliminating the FQDN/CN mismatch issue above, then it is likely that you have not successfully established the certificate chain.

When you view the keystore you need to be sure that the alias for your unique certificate is definitely a PrivateKeyEntry and not TrustedCertEntry. If it is a TrustedCertEntry then it's likely that you've somehow deleted the original Local Certificate that you generated, containing the private key - and have just imported the response from the Certificate Authority into a new alias. It is important that the response from the CA for your unique certificate is imported back on top of the PrivateKeyEntry in order to sign the Private Key. Root and Intermediate certificates can be a TrustedCertEntry without issue.

13.6 Troubleshooting

If you have any problems after the Import and Restart then see the Troubleshooting section of the SSL Guide on the Knowledgebase. A good place to start if Tomcat will not run, or the Swivel Core is inaccessible is to review the Catalina.out log file (/var/log/tomcat/catalina.out). Look towards the bottom of this file to see the latest errors since Tomcat was restarted. A common problem can be permissions on the .keystore file itself, especially when copied from another appliance.

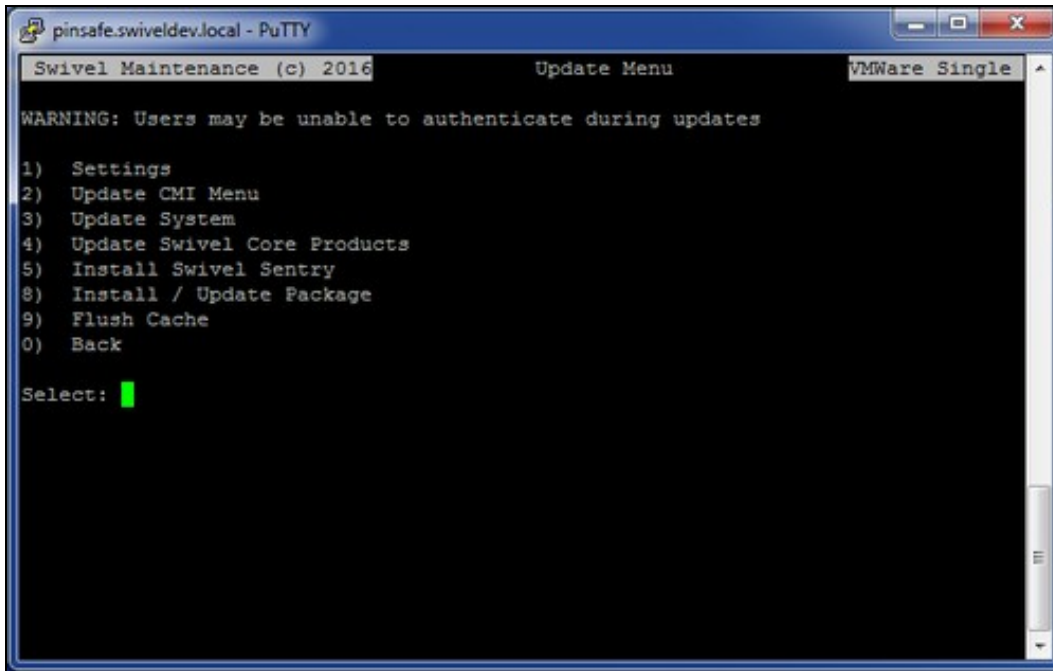
14 V3 Appliance Update

15 Introduction

As of Version 3 of the Swivel appliance (released October 2015), the popular automated package maintenance tool Yum, is now used to update the Swivel software and Operating System.

The Yum update mechanism automatically calculates dependencies and will download exactly what is needed to install new packages. It will also allow for quicker patching of security vulnerabilities.

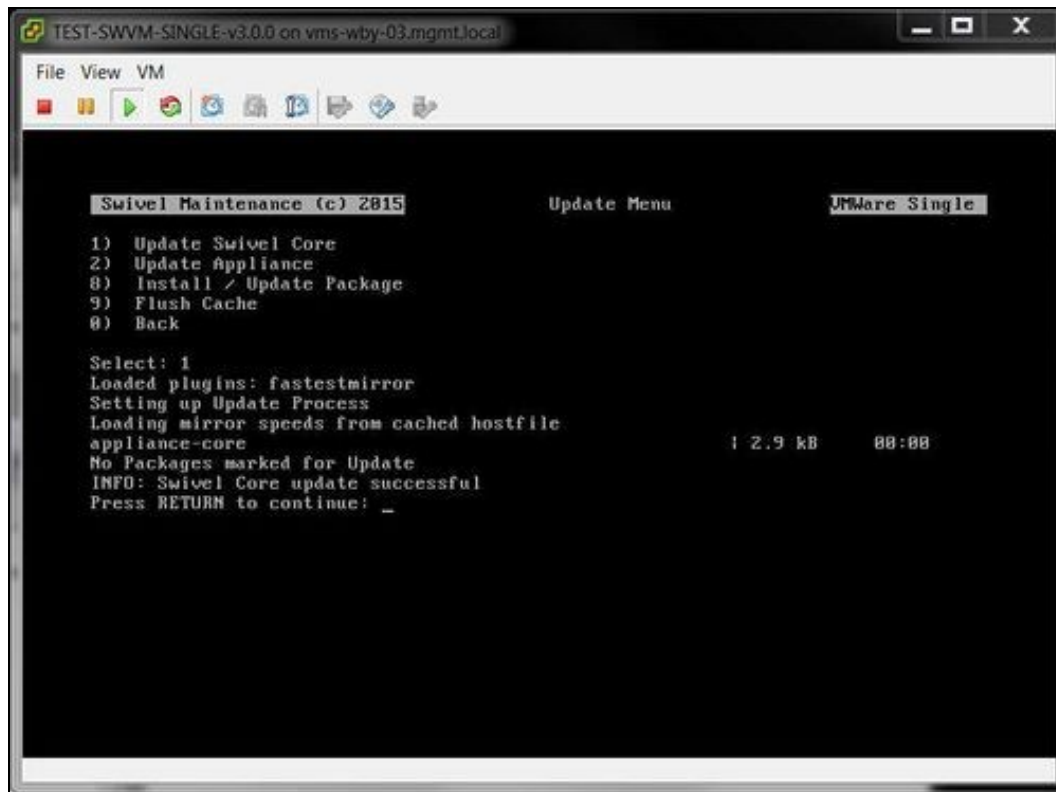
16 Get to the Update Menu



The Update Menu is located in the Console Management Interface of the Swivel Appliance. Please see the [PuTTY How To Guide](#) for guidance on connecting to the appliance via SSH. From the Main menu, select the **Administration** menu, then **Update Appliance**.

Each node in an Active/Active pair must be updated independently. Updating the Swivel Core Products will restart Tomcat at the end of the process. At the end of performing the updates, you must log out of the CMI and back in for the changes to take effect, this is namely for the Appliance and CMI Menu updates.

17 Update Swivel Core Products



Selecting this option from the Update Menu will attempt to update the Swivel Core to the latest version.

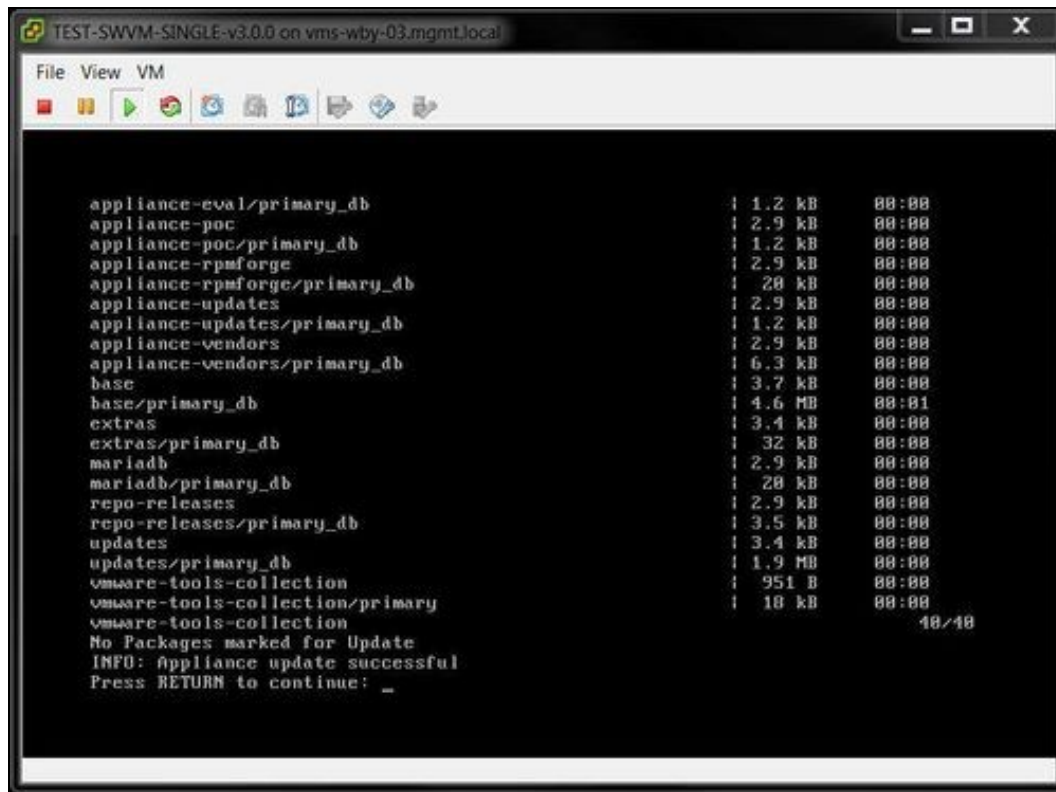
- If an update is available you will be prompted to install the new packages with a y/n (yes or no) response.
- If the packages are not currently installed, you will be prompted to install them with a y/n (yes or no) response.
- If the packages are up to date, then no updates will be available to install.

18 Update CMI Menu

Selecting this option from the Update Menu will attempt to update the console menu interface to the latest version.

- If an update is available you will be prompted to install the new packages with a y/n (yes or no) response.
- If the packages are not currently installed, you will be prompted to install them with a y/n (yes or no) response.
- If the packages are up to date, then no updates will be available to install.

19 Update System



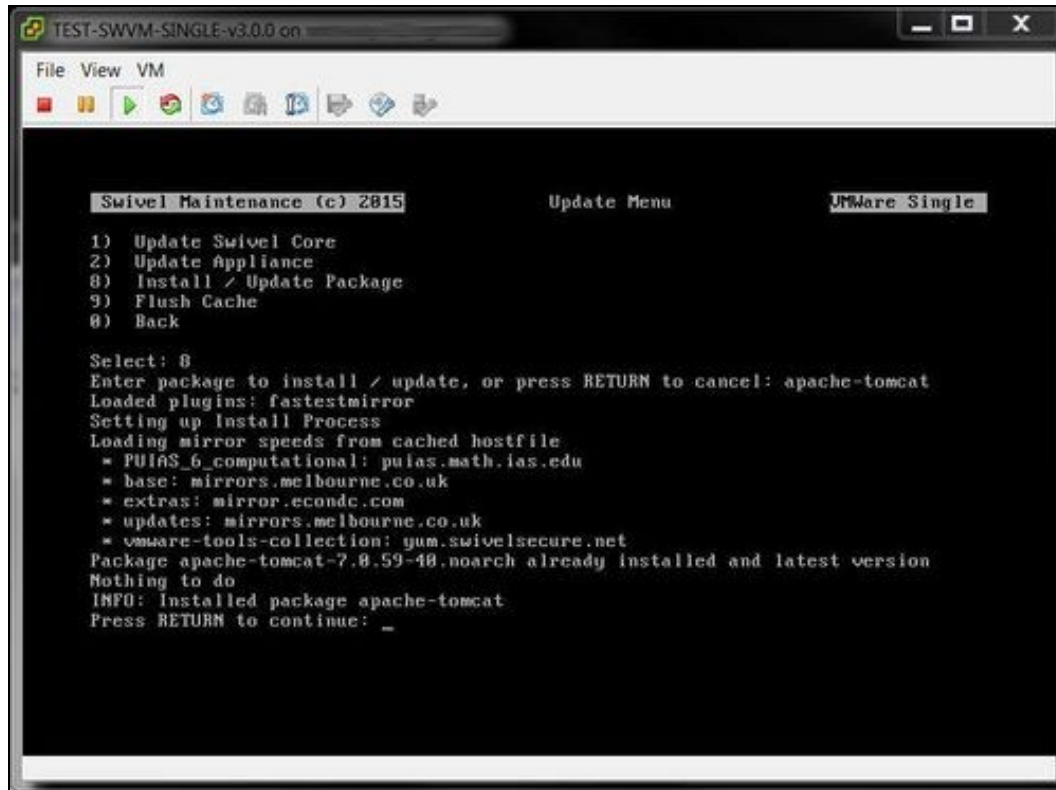
Selecting this option from the Update Menu will attempt to update the Appliance Operating System packages to the latest versions.

- If an update is available you will be prompted to install the new packages with a y/n (yes or no) response.
- If the packages are not currently installed, you will be prompted to install them with a y/n (yes or no) response.
- If the packages are up to date, then no updates will be available to install.

20 Install Swivel Sentry

Selecting this option from the Update Menu will attempt to install Swivel's Adaptive Authentication product, Sentry. If it has already been installed...

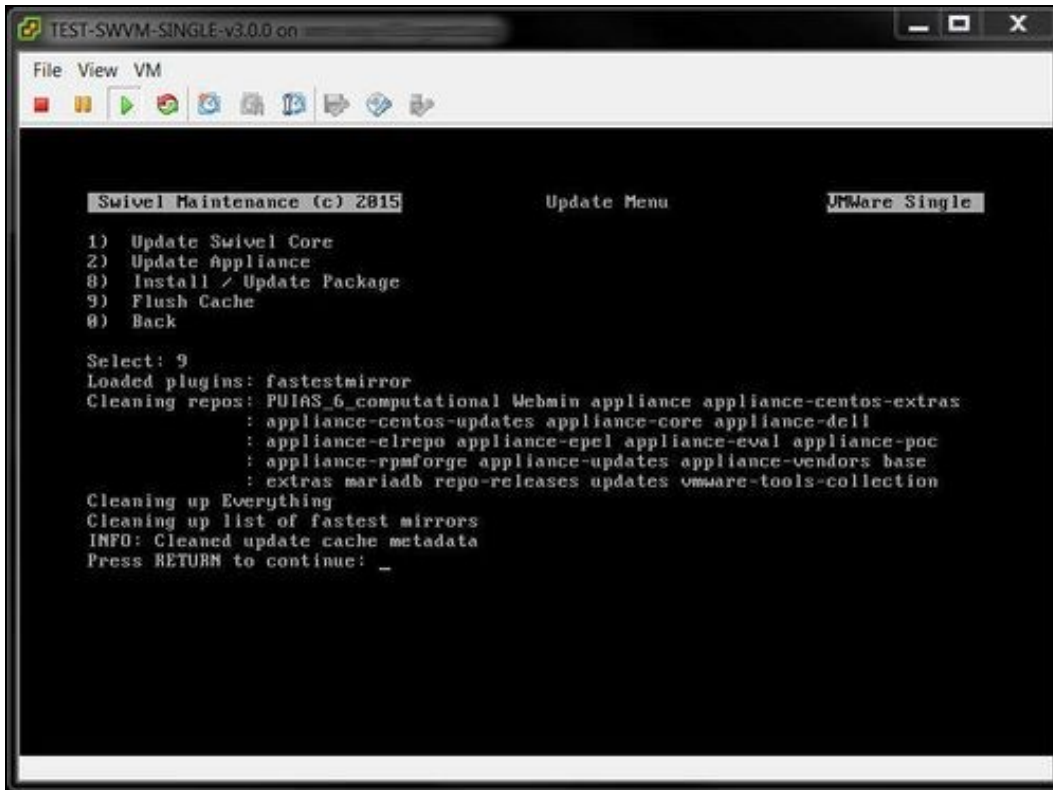
21 Install / Update Package



Selecting this option from the Update Menu will prompt you to enter a package name for update.

After entering the package name the Yum installation process will attempt to find the latest package version to see if the package needs updating. It also calculates any dependencies that may require other packages to be installed simultaneously.

22 Flush Cache



```
TEST-SWVM-SINGLE-v3.0.0 on
File View VM

Swivel Maintenance (c) 2015      Update Menu      VMware Single

1) Update Swivel Core
2) Update Appliance
8) Install / Update Package
9) Flush Cache
0) Back

Select: 9
Loaded plugins: fastestmirror
Cleaning repos: PUIAS_6_computational Webmin appliance appliance-centos-extras
                : appliance-centos-updates appliance-core appliance-dell
                : appliance-elrepo appliance-epel appliance-eval appliance-poc
                : appliance-rpmsforge appliance-updates appliance-vendors base
                : extras mariadb repo-releases updates vmware-tools-collection
Cleaning up Everything
Cleaning up list of fastest mirrors
INFO: Cleaned update cache metadata
Press RETURN to continue: _
```

Yum will retain packages and package data files that it downloads, so that they may be used again in future installation processes without the need to download them again.

If you are experiencing problems with the update process when selecting any of the update options, then try flushing the Yum packages cache using the Flush Cache option.

Next time an update option is selected the Yum process will then be forced to contact the package server to obtain package files instead of using local copies. This might just solve any problems where the cache has become corrupted or an installation package has become invalid.

23 V3 Setup HA Pair

24 Setting Up a High Availability (HA) Pair

24.1 What is a HA Pair?

This is a pair of Swivel appliances named **Primary Master** and **Secondary Master** that are able to provide authentication simultaneously for resilience purposes. Features include:

- **Dedicated Replication Interface:** User information is usually replicated across a dedicated network interface. On hardware appliances, a crossover cable is used on network interface eth1. This provides the maximum resilience, since there are no network devices between the appliances that can fail. Replication traffic may also be directed to run over network interface eth0 instead, with the loss of some resilience capability;
- **Replicated Database:** Out of the box, the Swivel appliances can replicate the Swivel Core database with one another. Transactions will be replicated both ways instantaneously. For example, this means that if a user changes their PIN on one Swivel appliance, the other appliance will receive the change and be able to authenticate with the new PIN immediately;
- **Config Sync:** Since the replicated database does not replicate the configuration of the Swivel Cores between the appliances, you will need to consider the use of the Config Sync feature. This is particularly useful when you have a lot of RADIUS entries for third party devices and need to ensure that any config changes are synced;
- **Virtual IP Address:** this is to allow a floating IP address to be attached to a Swivel appliance, which in the event of a Swivel appliance failure, can move to a second Swivel appliance on the same subnet. The VIP is bound to network interface eth0. The VIP is typically used to provide resilience for the Image based Swivel authentication method;
- **Appliance Sync:** (formerly Session Sharing) this allows an Image based security string to be requested from one appliance and an authentication request to hit the other. A session register is shared between the appliances to facilitate this;
- **RADIUS Proxy:** Where ?Appliance Sync? is not in operation this can be used to refer a RADIUS authentication request to another Swivel appliance, where the session may have originated from.

You may not take advantage of all of these features immediately, but as you integrate the Swivel appliances with more third party products, the need for these features will become apparent.

24.2 Minimum setup required

Before undertaking any High Availability configuration, you should ensure that you have setup the Network configuration for both the eth0 and eth1 network interfaces. You will need to allocate network addresses for:

- Primary eth0 interface
- Primary eth1 interface
- Secondary eth0 interface
- Secondary eth1 interface
- Virtual IP

Note: The 172.16.0.x default addresses for the eth1 interfaces can remain as they are if using a crossover cable between the eth1 interfaces that does not clash with your eth0 network.

As a minimum requirement when not using Image Based authentication you should setup both the **Replicated Database** and the **Config Sync** features. This will enable user data and configuration to synchronise between the appliances.

Where Image Based authentication is being used you should also setup **Virtual IP address** and **Appliance Sync** if you intend to be able to serve images from both appliances simultaneously or have some resilience (failover) for serving images.

24.3 Configure the High Availability menu options

To access the High Availability menu, login to the Appliance using PuTTY. This option is available from the Main Menu.

To configure the High Availability functionality we will start from the top menu item in the High Availability menu and work downwards.

As a bare minimum for a HA Pair you will need to do the following (in this order):

- Ensure that the secondary ethernet network interfaces are connected together (by crossover cable on Physical appliances or a dedicated vSwitch arrangement on Virtual Machines);
- Set the Peer IPs for on both the Primary and Standby appliances so that they can find each other on the network;
- Perform the initial Database sync if it has not synced automatically after setting the Peer IPs.

Detailed below are the configuration options on the High Availability menu.

24.3.1 Set Peer IP

These settings assume that you have already configured the Networking and Hostnames of the appliances. If you have not already configured the Networking and Hostnames then please do so before you proceed.

The ?Peer? appliance would simply be the alternate appliance in the HA Pair. So if you are logged into the Primary Console Management Interface, the ?Peer? would be the Secondary appliance.

Set Peer Hostname - If you are logged into the Primary appliance, you would enter the Secondary appliance hostname assuming that the Standby is the Peer you want to replicate against.

Change Replication Interface - This menu option provides the ability to toggle between using network interface eth0 or eth1 for replication of the database. By default this is set to eth1.

Set Peer eth0 IP - If you are logged into the Primary appliance, you would enter the Secondary eth0 IP.

Set Peer eth1 IP - If you are logged into the Primary appliance, you would enter the Secondary eth1 IP.

24.3.2 Set DR IP

These settings assume that you have already configured the Networking and Hostnames of the appliances. If you have not already configured the Networking and Hostnames then please do so before you proceed.

Add DR IP - If you are logged into the Primary appliance, you would enter the DR appliance IP assuming that the DR is the appliance you want to replicate data to, from the Primary. Multiple DR IPs can be added here - however this is not recommended. Any extra DRs would need to be configured manually using Webmin or the Command Line.

Remove DR IP - Select the item number of the DR IP that you wish to remove from the list of DRs.

24.3.3 Database Replication

After you have configured the Network IPs, Hostnames, Peers and DRs you should check the Status of the Database Replication with each of the Peers and if necessary perform an initial sync.

Status - This option presents you with a list of Peer and DR IPs. Select the Peer IP you want to check Replication Status against

Start Reading Updates from Peer - As described when selected this feature will begin reading database updates from the Peer appliance

Repair Replication - This option prompts you to select the canonical (valid) database to sync to the alternate appliance during the repair operation

24.3.4 Virtual IP

Set Email Address - Enter an email address for Virtual IP alerting emails

Change Virtual IP - Enter a new virtual IP or replace the current one

Add Ping Node - This is vital to provide the HA failover mechanism with the ability to know if it can contact something else on the network or not. Typically this would be a router or a gateway. Multiple entries can be added and will appear above the menu options in a list.

Remove Ping Node - Select the number pertaining to a particular Ping Node to remove it.

Start Mon - This is an alternating menu option. It will appear as either Start Mon or Stop Mon depending on the current service status. If you select Start Mon the Mon service will be started. If you select Stop Mon the Mon service will be stopped.

Stop Mon - This is an alternating menu option. It will appear as either Start Mon or Stop Mon depending on the current service status. If you select Start Mon the Mon service will be started. If you select Stop Mon the Mon service will be stopped.

Start Heartbeat - This is an alternating menu option. It will appear as either Start Heartbeat or Stop Heartbeat depending on the current service status. If you select Start Heartbeat the Heartbeat service will be started. If you select Stop Heartbeat the Heartbeat service will be stopped.

Stop Heartbeat - This is an alternating menu option. It will appear as either Start Heartbeat or Stop Heartbeat depending on the current service status. If you select Start Heartbeat the Heartbeat service will be started. If you select Stop Heartbeat the Heartbeat service will be stopped.

24.3.5 Advanced

These settings are for an engineer to be able to view the contents of the ha.cf, haresources and mon.cf files. They are to be used for advanced purposes and diagnostics only. It is not recommended that you use this menu option if setting up your appliances for the first time.

Modify Hostnames - You will be prompted to enter both the Primary and Standby hostnames. The HA configuration files will be modified with the hostnames you provide.

Modify IPs - This option sets the IP for the network interface you select or replaces the current IP.

Modify VIP - This option sets the VIP or replaces the default VIP of 192.168.0.38.

25 Version 3 Appliance

25.1 Introduction

```
Swivel Maintenance (c) 2015           Main Menu           VMware Single
Hostname      : test.single.name
Interface    : eth0      : 192.168.8.25
Tomcat Status : Running

WARNING: Password still default. This can be changed in Administration
WARNING: No alert email set. This can be set in Tools -> Alerts

1) Tomcat
2) Network
3) Appliance
4) Backup and Restore
5) Tools and Utilities
6) Administration
8) System Status
9) Version Information
0) Exit

Select: _
```

Version 3 of the Swivel Appliance is a completely new version of the Appliance, redeveloped in order to:

1. Move to more up to date OS and Applications;
2. Move to a more structured and easier support development environment for the menu system;
3. Create an appliance that is easier to upgrade and patch after deployment.

25.1.1 Key Differences

- New Base Operating System based on Centos;
- New Appliance Database (based on MariaDB);
- Newer Versions of Java and Tomcat;
- Access to YUM type updates.

25.1.1.1 New Features

- New alerts for issues such as disk space;
- More diagnostics available without the need to drop to command line.

There is a [Quick Start Guide](#) available and a [Reference Guide](#) that lists the menus and their meanings.

There is also a number of How To articles to explain specific features that are listed [here](#)