

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.

Contents

- 1 Introduction
 - ◆ 1.1 Improvements over Version 2
 - ◆ 1.2 Benefits of upgrading
 - ◆ 1.3 Process Summary
- 2 Prerequisites
- 3 Upgrade your Version 2 Appliance prior to backup
- 4 Upgrade your Swivel Core application prior to backup
- 5 Backup your Version 2 Appliance
- 6 Retrieve the Version 2 backup files
- 7 Restore to your new Version 3 Appliance
 - ◆ 7.1 Post restore considerations
- 8 Troubleshooting

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.

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.

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.

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.

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.**

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.

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.

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.

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.

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.

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.

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.