SecureSync®

System Software

Version 5.9.2

Upgrade Instructions



Date: 24-March-2021

orolia.com

© 2021 Orolia. All rights reserved.

The information in this document has been carefully reviewed and is believed to be accurate and up-to-date. Orolia assumes no responsibility for any errors or omissions that may be contained in this document, and makes no commitment to keep current the information in this manual, or to notify any person or organization of updates. This Software Upgrade Instructions is subject to change without notice. For the most current version of this documentation, please see our web site at orolia.com.

Orolia reserves the right to make changes to the product described in this document at any time and without notice. Any software that may be provided with the product described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

End-user customers of Orolia products may, without the need for a written license from Orolia, reproduce and modify any Orolia product documentation accompanying such products, for distribution within their organization in order to use the products.

Orolia authorized partners, systems integrators, government contractors, and other similarly-situated third-party installers may, without the need for a written license from Orolia, reproduce Orolia product documentation (including media type changes) and create derivative works thereof in the form of compilations, for distribution to their end-users.

Except as described above, no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose without the written permission of Orolia.

Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Orolia USA, Inc.

• 45 Becker Road, Suite A, West Henrietta, NY 14586 USA
• 3, Avenue du Canada, 91974 Les Ulis, France

The industry-leading Spectracom products you depend on are now brought to you by Orolia, the global leader in Resilient Positioning, Navigation and Timing Solutions.

Do you have questions or comments regarding this Software Upgrade Instructions?

➔ E-mail: techpubs@orolia.com

Warranty Information

See the website:http://www.orolia.com/support/spectracom/warranty-information for a copy of Orolia's Limited Warranty policy.

Blank page.

CONTENTS

CHAPTER 1

Upgrade Preparations 5

1.1 Determining the Current System Software 6

1.1.1 Using Version 5.1.2 and Above 6

1.1.2 Using Version 5.0.2 and Below ("Old Style" Web UI) 6

1.2 Determining the Correct Upgrade Procedure 8

1.3 Determining Remaining Disk Life 9

1.3.1 Disk Health Check 9

1.4 Freeing up Disk Space 9

1.4.1 Determining Current Disk Usage 10

1.4.2 Archiving and Deleting Log Files 10

1.4.3 Deleting Old Update Files 11

1.4.4 Disk Cleanup Patch 12

1.5 Downloading the Upgrade Software Bundle 12

1.6 Hardware-Specific Steps 12

1.6.1 Trimble RES-SMT-GG Receiver and u-blox M8T Receiver 13

1.6.1.1 Determining the GNSS Receiver 13

1.6.2 Simulcast Option Card (Model 1204-14) 14

1.6.3 10/100 PTP Option Card (Model 1204-12) 14

1.6.4 Gigabit Ethernet Option Card (Model 1204-06) 15

CHAPTER 2

Upgrade Procedure 17

2.1 Upgrading from V. 5.0.2 to a Newer Version 18

2.1.1 Required Repeat of Upgrade Process 23

2.1.2 Confirming Successful Installation 24

2.1.3 Creating new Local Clock(s) 24

2.2 Upgrading from V. ≥5.1.2 to a Newer Version 24

2.2.1 Potential Need to Repeat Upgrade Process 30

2.2.1.1 u-blox M8T: Upgrading to Version 5.9.2: 30

2.2.1.2 RES-SMT-GG: Upgrading to Version 5.9.2: 31

2.2.2 Confirming Successful Installation 31

APPENDIX

Appendix ..... **i**

3.1 Upgrading via CLI ii

3.2 Saving/Restoring Configuration Files iii

3.3 Software Update Log Entries iii

3.4 Downgrading the SW to a Previous Version iii

3.5 “Upgrade Failure” (V. 5.0.2 to a Newer Version) vi

3.6 “Upgrade Failure” (V. ≥5.1.2 to a Newer Version) viii

3.6.1 Failure of Component Upgrades x

3.7 Technical Support xii

3.7.1 Regional Contact xii

CHAPTER 1

Upgrade Preparations

Chapter 1 guides you through the steps necessary to prepare the upgrade.

The following topics are included in this Chapter:

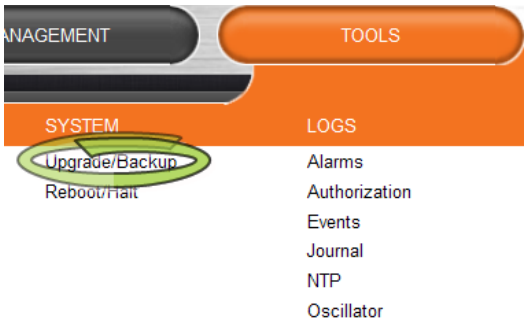
1.1 Determining the Current System Software 6
1.2 Determining the Correct Upgrade Procedure 8
1.3 Determining Remaining Disk Life 9
1.4 Freeing up Disk Space 9
1.5 Downloading the Upgrade Software Bundle 12
1.6 Hardware-Specific Steps 12

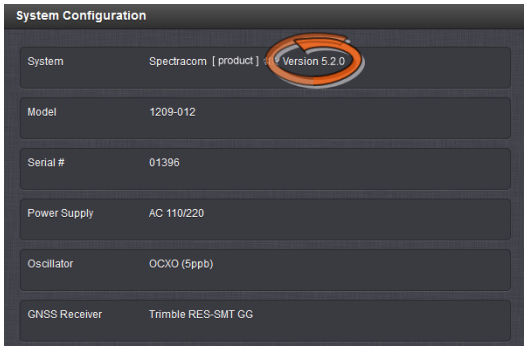
1.1 Determining the Current System Software

First, determine which system software version is currently installed on your SecureSync:

1.1.1 Using Version 5.1.2 and Above

1. In the SecureSync Web User Interface (Web UI), navigate to **Tools** > **System: Upgrade/Backup**.

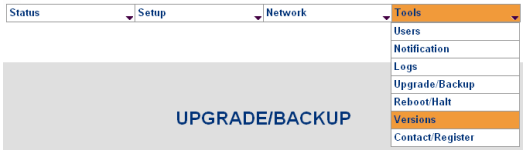


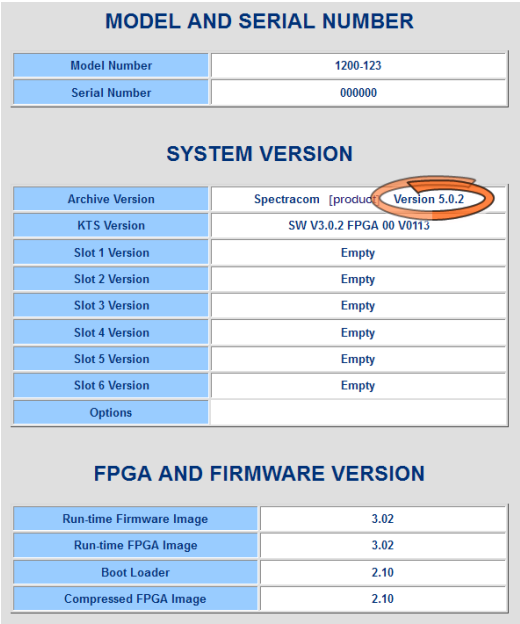


2. Take note of the system software version number.

1.1.2 Using Version 5.0.2 and Below ("Old Style" Web UI)

1. In the Web UI, navigate to **Tools** > **Versions**.





MODEL AND SERIAL NUMBER

Model Number	1200-123
Serial Number	000000

SYSTEM VERSION

Archive Version	Spectracom [produc Version 5.0.2
KTS Version	SW V3.0.2 FPGA 00 V0113
Slot 1 Version	Empty
Slot 2 Version	Empty
Slot 3 Version	Empty
Slot 4 Version	Empty
Slot 5 Version	Empty
Slot 6 Version	Empty
Options	

FPGA AND FIRMWARE VERSION

Run-time Firmware Image	3.02
Run-time FPGA Image	3.02
Boot Loader	2.10
Compressed FPGA Image	2.10

2. Take note of the Archive Version number.

1.2 Determining the Correct Upgrade Procedure

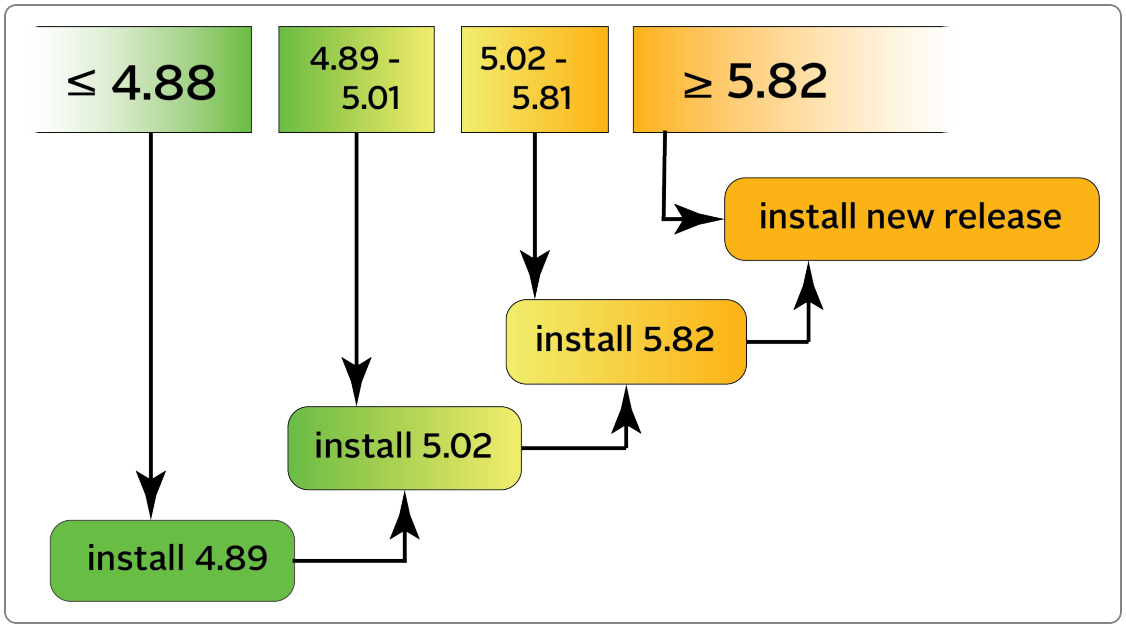
There are four possible upgrade scenarios:

I. If your currently installed software is Version 5.8.2 or higher, proceed to "Upgrade Procedure" on page 17.

II. If your currently installed software is Version 5.0.2 or higher and 5.8.1 or lower: You must install Version 5.8.2 first, and then the latest version. To download the 5.8.2 software bundle (includes instructions), navigate to http://spectracom.com/support/securesync-and-netclock-9400-support.

III. If your currently installed software is Version 5.0.1 or lower and 4.8.9 or higher: You must install Version 5.0.2 first,5.8.2 second, and then the latest version. To download the 5.0.2 and 5.8.2 software bundles (includes instructions), navigate to http://spectracom.com/support/securesync-and-netclock-9400-support.

IV. If your currently installed software is Version 4.8.8 or lower, you must install Version 4.8.9 first, 5.0.2 second, 5.8.2 third, and then the latest version. To download the 4.8.9, 5.0.2, and 5.8.2 software bundles (includes instructions), navigate to http://spectracom.com/support/securesync-and-netclock-9400-support.



With all four scenarios, before beginning with the actual software installation, you must first complete all necessary steps in CHAPTER 1.

If you download more than one file, the files will be bundled into one compressed file that you need to extract, once it has been downloaded. Thereafter, only upload the file `upda-texxx.tar.gz` (where xxx = software version) to the unit to be upgraded.

1.3 Determining Remaining Disk Life

SecureSync uses a Compact Flash (CF) memory card for storing logs, configurations and software. Certain rare conditions can reduce the disk life to the point where the unit is unable to upgrade. This condition is unrelated to the memory capacity; instead, the disk health is an expression of the length of time the CF card will continue to operate.

1.3.1 Disk Health Check

The Disk Health Check is available after SW V 5.8.5 or through an applied hotpatch.

In order to view the length of time remaining in the operation of your disk:

- Log on to the Web UI
- Navigate to TOOLS Upgrade/Backup
- The Disk Health panel is on the lower left of the screen

Disk Health Results

- **Health OK** - Healthy disks are capable of conducting a software upgrade and have more than three months of estimated operating "life" left. You are okay to upgrade if your Disk Health is listed as No Disk Maintenance Required.
- **Less than 1 year** - If your Disk Health is listed as less than one year but more than three months, you may conduct a software upgrade but do still need to contact Technical Support for more information.
- **Less than 3 months** - If your Disk Health is listed as less than three months, do not attempt a software upgrade. Contact Technical Support.

1.4 Freeing up Disk Space

SecureSync uses a Compact Flash (CF) memory card for storing logs, configurations and software. Over time, the Compact Flash card can contain many log entries and any previous software update files retained from earlier software updates.

If the CF card usage is higher than normal when a software update is performed, this can potentially result in the loss of some or all of the unit's configurations upon completion of the software update process or may prevent the update from being able to begin. It may be necessary for the unit's logs and previous update files to be deleted before performing software updates.

The logs can be backed-up to a single bundled fine and then extracted before deleting them, if required by your organization. The processes to easily delete logs and previous Update files before updating the software is described within.

> **Note:** An available CLI command (df –h) can be used to read what percentage of the CF card is currently in use, to determine if the logs and update files should be deleted. In general, if the CF card usage is more than around 70 % or so, the logs and any previous software update files should be deleted to ensure there is plenty of space in the CF card to persist the config files and to be able to perform the upgrade.

1.4.1 Determining Current Disk Usage

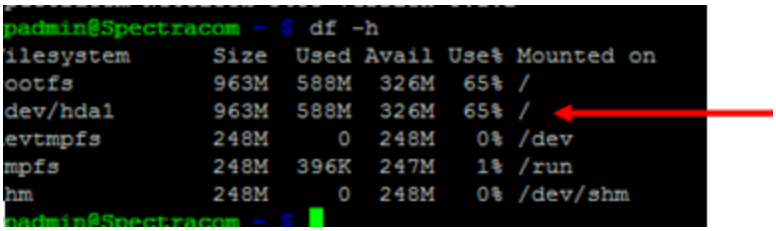
There are two ways to determine the usage, via the Web UI, or using the Command Line Interface (CLI):

Determining Disk Usage via the Web UI

1. In the Web UI, navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the **Disk Status** panel in the bottom-left corner of the screen, the **Percent** value indicates what percentage of disk space is currently used.

Determining Disk Usage via the CLI

Login to the CLI (telnet or ssh) and at the command prompt, type: df –h <enter> (as shown below). The "Use%" column in the "/dev/hda1" row will indicate the CF card usage (65 % in this example, which indicates the logs and any previous Update files do not need to be deleted before performing the update process.)



1.4.2 Archiving and Deleting Log Files

If the disk usage is higher than 70% (approximately), Spectracom recommends that you delete the **logs** and **update files** that may have been previously applied before performing the system software upgrade.

Archiving Logs

As an option, the logs can be archived (backed up) before deletion, by bundling them into a single file, and then transferring them to your PC, all from within the SecureSync Web UI.

To archive logs:

1. In the Web UI, navigate to **MANAGEMENT** > **OTHER: Log Configuration**.
2. Click on **Save and Download All Logs**. This will generate a single bundled file (`*.log`) of the logs. Select where to save this file on your PC.

Deleting Logs and Statistics

To delete log files and statistics files, in order to cleanup disk space:

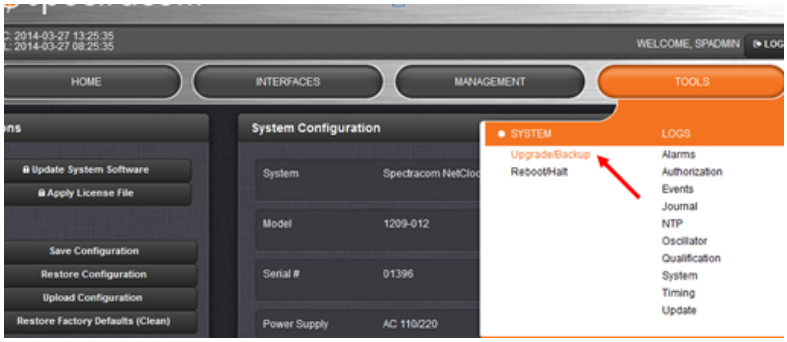
1. In the Web UI, navigate to **TOOLS > SYSTEM: Upgrade/Backup**.
2. In the bottom-left corner of the screen, take note of the Percent value, indicating how much disk space is currently used.
3. Then click on **Clear All Logs**, and then **Clear All Stats** below.
4. After completion of the process, the **Percent** value should show a smaller number, indicating how much disk space was cleared.

1.4.3 Deleting Old Update Files

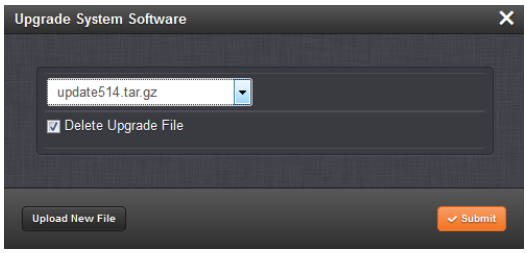
Update files used in previously executed software upgrades are stored in the `home/spectracom` directory. You can delete them individually via the Web UI (they are no longer used by the System, after the update has been applied).

To delete each update file:

1. In the Web UI, navigate to **Tools** > **Upgrade/Backup** (see illustration below):



2. Click on the button **Update System Software** in the top-left corner. The **Upgrade System Software** window will open (see illustration below):



3. The drop-down list will display each update file currently stored in the SecureSync Compact Flash Card. Select the file to be deleted, and check the **Delete Upgrade File** checkbox. Then click **Submit**.
4. Repeat this process to delete any other listed update file.

1.4.4 Disk Cleanup Patch

Under some circumstances, clearing logs and stats conventionally via the Web UI (as described above) will require a second step in order to achieve an optimum restoration of disk space.

To this end, Spectracom provides a **Disk Cleanup Patch** that can be downloaded with instructions from https://files.spectracom.com/public-downloads/updatecleaner-securesyncnetclock-9400, and run from within the Web UI. This Patch will clean items that are not user accessible otherwise.

1.5 Downloading the Upgrade Software Bundle

The new version system software upgrade (as well as previous versions, if needed) can be downloaded from the Spectracom Corporate website, see:

Spectracom Support page for SecureSync

» Download the file(s) onto your PC, and note the location. If you download more than one file, the files will be bundled in a compressed file that needs to be extracted after download. Then, only upload the file `updatexxx.tar.gz` to the unit to be upgraded (where xxx = software version).

1.6 Hardware-Specific Steps

With certain hardware configurations and option cards (see below), the corresponding procedures described below must be carried out when upgrading **from Versions 5.0.2 or**

higher to Version 5.9.2.

These instructions apply only, if one or several of these are installed:

- Trimble RES-SMT-GG Receiver
- Simulcast Option Card (Model 1204-14)
- 10/100 PTP Option Card (Model 1204-12)
- Gigabit Ethernet Option Card (Model 1204-06)

Please note that these option-card related procedures **must be carried out only once**, i.e. if you have previously upgraded your system from Version 5.0.2 to e.g., 5.1.5, you can skip this section.

1.6.1 Trimble RES-SMT-GG Receiver and u-blox M8T Receiver

Units shipped between 2Q 2014 and 3Q 2016 typically have a RES-SMT-GG GNSS receiver installed, while units built thereafter are equipped with a u-blox M8T receiver.

With either receiver, it may be necessary to **execute the installation procedure twice** in order to install not only the SecureSync system software update, but also a GNSS receiver firmware update:

a. If your unit has a RES-SMT-GG receiver, AND you are upgrading from a version less than 5.1.5 to a higher version (does not apply to SAASM GPS SecureSyncs).
   - When upgrading from version 5.0.2 to 5.1.5 or higher, see "Required Repeat of Upgrade Process" on page 23.
   - When upgrading from version 5.1.2 to 5.1.5 or higher, see "Potential Need to Repeat Upgrade Process" on page 30.

b. If your unit includes a u-blox M8T receiver, AND you are upgrading from version 5.5.0 or lower to 5.6.0 or higher.
   - See "Potential Need to Repeat Upgrade Process" on page 30.

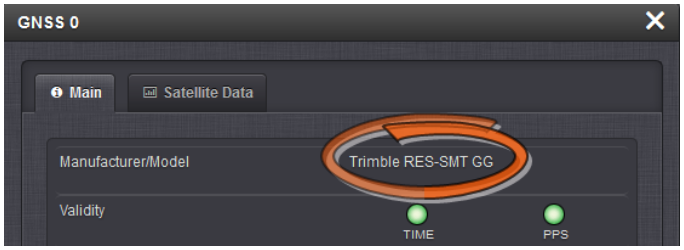
Note: In cases other than the ones described above, the firmware update will be skipped automatically.

1.6.1.1 Determining the GNSS Receiver

Next, you need to determine which type of GNSS receiver is installed in your SecureSync.

Note: If the default Web UI of your unit is blue/white (rather than dark grey), your unit has a Res-T receiver.

1. If your Web UI is dark grey (see illustration below), navigate to **Interfaces** -> **GNSS 0**. The first line item under the default **Main** tab will report the GNSS receiver Model that is installed in your SecureSync. The example shown in the illustration below shows a "RES-SMT GG" receiver.



2. Take note of the receiver type installed in your unit.

1.6.2 Simulcast Option Card (Model 1204-14)

Simulcast/CTCSS Option Cards (Model 1204-14) have one RJ-45 jack and should be identified with a small "14" label screened onto a corner of the metal plate of the Option Card itself).

Due to a software change in the version 5.1.2 update to address an issue with the 9600 baud output, the settings of this particular Option Card need to be "resubmitted" just one time, after applying the next subsequent update version beyond version 5.0.2. The issue with the 9600 baud output, if configured, will still be initially present after applying the version 5.1.2 or higher software update, until the configurations of this Option Card are "resubmitted" one-time.

To "resubmit" the settings, navigate to the "Interfaces" page of the browser and select the Simulcast Option Card. With the settings displayed, simply press the "Submit" button to refresh the settings. This will resolve the issue with the 9600 baud output. Note this additional step does not need to be performed again, after any subsequent software updates are applied.

1.6.3 10/100 PTP Option Card (Model 1204-12)

Note: Not applicable to the Gb PTP Option Card Model 1204-32.

10/100 PTP Option Cards (Model 1204-12) have one Ethernet jack and can be identified with a small "12" label screened onto a corner of the metal plate of the Option Card itself.

When there are software updates that need to be automatically applied to the 10/100 PTP Option Cards during the upgrade process, the upgrade process will take an additional 5 to 7 minutes longer, for each 10/100 PTP Option Card that is installed.

1.6.4 Gigabit Ethernet Option Card (Model 1204-06)

Note: This section is not applicable when previously upgrading from versions 5.1.2 and above and the Ethernet ports have already been enabled by a user.

Important Notices when upgrading from version 5.0.2

When updating from versions prior to 5.1.2 with this Option Card installed, Eth1, Eth2 and Eth3 will all be disabled (not accessible by the network) upon applying this software update. If you are connected to one of these three ports to perform the update process, the time server will not be accessible once the update has completed. Further below is information about two different methods to enable each of these three Interfaces as desired, after applying the software update.

Because the three interfaces are disabled once the software update has completed, the network settings will appear to have been lost during the update. However, the settings do actually persist through the update process. All of the settings will be present again, once each interface is individually enabled.

If the software was previously updated to versions 5.1.2 or higher, the three Ethernet ports will be in the same state (enabled or disabled) as they were before applying this update.

System software version 5.1.2 added a new feature which allows unused Ethernet interfaces (Eth1, Eth2 and/or Eth3) of the Model 1204-06 Gigabit Option Card, if installed, to be disabled via software for security purposes. Note this change does not apply to the base Ethernet port, "Eth0", which cannot be disabled.

After applying this software update from version 5.0.2, all three of these Ethernet interfaces will be disabled. If any or all three of these interfaces are currently being used, after applying the software update (or if it's desired to start using any of these three interfaces at a later date) the desired Ethernet interface(s) needs to be enabled. Until the interfaces have been enabled by a user, they will be inaccessible to the network.

Each of the three Ethernet interfaces can be enabled as desired, via either the web browser (using the "base" Ethernet interface "Eth0") or by issuing a specific command with a CLI connection (telnet or SSH).

Enabling each interface using a CLI connection

After creating a CLI connection (using either telnet or SSH) the command to enable each desired interface is as follows: portset x on (where x is the Ethernet interface number - 1, 2, or 3 - for the interface you wish to enable).

An example of enabling Interface "Eth1" is shown below:

```
padmin@Spectracom ~ $ portset 1 on
padmin@Spectracom ~ $
```

Enabling each interface using a web browser connection

To enable each desired Interface using the web browser, login to the browser using Eth0 (this interface is not disabled during the update). Navigate to the **Management** -> **Network** page of the Web UI. This will open a page displaying all four Ethernet interfaces (Eth0 through Eth3). The Status of Eth1 through Eth3 will be displayed as "DISABLED".

For each Interface you wish to enable, click on the corresponding **Gear** button (center of the three buttons in that row). In the next screen that opens, click on the checkbox at the top of the page (as shown below). Then press either the **Apply** or **Submit** button to enable the interface. The port will now have the previous configuration as before the update was applied and will be accessible to the network.



CHAPTER 2

Upgrade Procedure

After completion of all preparation steps, the actual upgrade will be performed.

Chapter 2 will guide you through this process.

Depending on which software version is currently installed in your SecureSync unit, proceed either to:

- "Upgrading from V. 5.0.2 to a Newer Version" on the next page,
- or to "Upgrading from V. ≥5.1.2 to a Newer Version" on page 24.

2.1 Upgrading from V. 5.0.2 to a Newer Version

Note: Depending on the software currently installed on your unit, upgrading to the latest version may be a multi-step process. See "Determining the Correct Upgrade Procedure" on page 8 for more information.

The software upgrade process is performed using a PC that is either on the same network as the SecureSync appliance, or is connected directly to the SecureSync via a network cable.

Note: In order to perform the software upgrade, the Web UI of the unit to be upgraded must be accessible from this particular PC.

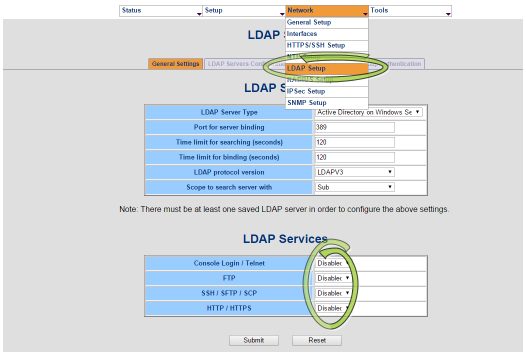
Once you downloaded the upgrade file onto a network PC, you can then transfer the file onto your SecureSync unit, using the unit's Web UI.

Note: Alternatively, you can also upgrade via Command Line Interface: In this case, the file must be transferred manually, using FTP/SFTP, to the SecureSync directory `home/spectracom`.

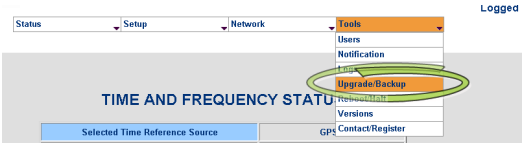
During the time that the file is being uploaded into SecureSync, the unit will remain fully functional and accessible for other network PC's.

Once the file transfer is complete, SecureSync is performing the software upgrade ("Upgrade System"), during which the unit is configured: Normally, all current SecureSync configurations are automatically saved and restored as part of the update process. During the “Upgrade System” process, the front panel LCDs will go blank, and the unit will not be operational until the upgrade process has completed.

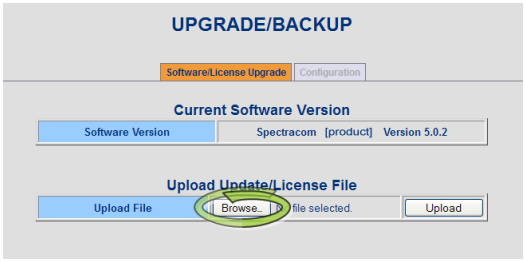
1. Local Clock: After updating from the "Classic" interface only SW Version (5.0.2) to a more recent version, you will have to create a new local clock, and apply it to the ports as desired. It is therefore advisable to write down any current Local Clock settings you may be using, before installing the new software.
2. Verify that LDAP has not been ENABLED inadvertently, by navigating to **Network > LDAP Setup**: If you are not using LDAP, DISABLE all services (if correctly configured, the services can remain ENABLED during the upgrade process).



3. Download the SecureSync upgrade file (`updateXXX.tar.gz`) from the Spectracom website—see also "Downloading the Upgrade Software Bundle" on page 12—to an accessible directory on your local Windows machine (such as `C:/Temp`).
4. Open the Web UI, and login. Then navigate to **Tools** > **Upgrade/Backup**.



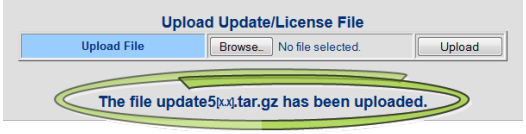
5. Ensure the **Software/License Upgrade** tab is orange (Orange indicates the tab is selected). Either click in the blank text box located next to **Upload File**, or select **Browse** to be able to select the update file (see illustration below).



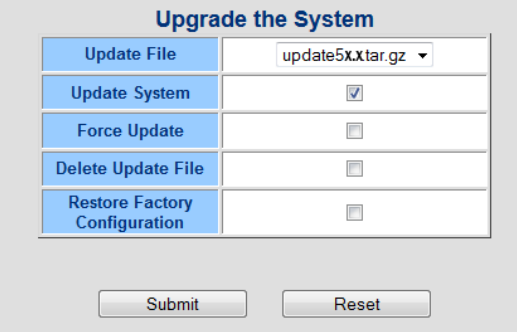
6. Use the Windows® Explorer to navigate to the location on your network PC where the update file (`updateXXX.tar.gz`) was stored earlier (such as `C:/Temp`), and select it. Once the path appears in the text field (see illustration below), click the **Upload** button.



7. The file upload process may take several minutes. Once the file has been uploaded, the message "The file updatexxx.tar.gz has been uploaded." (where xxx is the new version being applied) will be displayed underneath the field **Upload Update/License File**:



8. Now refer to the bottom of this page, under the title **Upgrade the System**. Ensure the correct file name (`updateXXX.tar.gz`) is selected in the box next to **Update File**.



9. Check the box next to **Update System** to install the software update.

Other available checkboxes:

Note: To perform the software update from an earlier software version to the latest version, only the checkbox next to Update System should be selected.

» Force Update: When checked, will force the software to install all packages, even if it is already at the current revision, or (for example, it is desired to install version 5.9.2, even though version 5.9.2 is already installed). The software will reinstall over the previously installed packages.

USE CASE: This checkbox must be selected if it is ever desired to downgrade to a previous software version.

» Delete Update File: When checked, will remove the Archive file that was uploaded into the unit. Note that this will not remove the file from your PC, just from SecureSync.

Note: If it is desired to remove the update file from the unit after completion of the upgrade process, note that the "Delete the Update File" checkbox should not be selected at the same time as the "Update System" checkbox. This process should be performed any time after the System Update process has been completed.

» Restore Factory Configuration: When checked, will return SecureSync to its original factory configuration.

USE CASE: This checkbox should be selected if it is ever desired to downgrade to a previous version (such as back to version 5.0.2, for instance).

During the System Upgrade you will see an analysis screen (as shown in the illustration below).

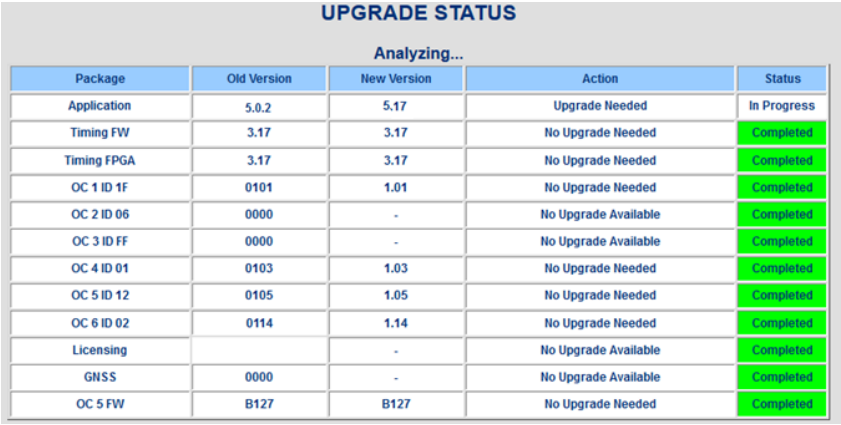
Note: If the unit has had any previous software updates applied and if any of the earlier upgrade files have not since been deleted from the unit, a Web UI screen may momentarily indicate the Upgrade process is "Complete". This does not affect the software update process and the analysis screen will be displayed shortly thereafter.

UPGRADE STATUS

Analyzing...

Package	Old Version	New Version	Action	Status
Application	5.1.5	-	-	Analyzing
Timing FW	3.17	-	-	Analyzing
Timing FPGA	3.17	-	-	Analyzing
OC 1 ID 1F HW 01	0101	-	-	Analyzing
OC 2 ID 06 HW 02	0000	-	-	Analyzing
OC 3 ID FF HW FF	0000	-	-	Analyzing
OC 4 ID 01 HW 01	0103	-	-	Analyzing
OC 5 ID 12 HW 01	0105	-	-	Analyzing
OC 6 ID 02 HW 01	0114	-	-	Analyzing
Licensing	-	-	-	Analyzing
GNSS	0000	-	-	-
OC 5 FW	B127	-	-	Analyzing

Note: "OC" being displayed in the bottom rows refers to OPTION CARDS which may or may not be installed in your unit.



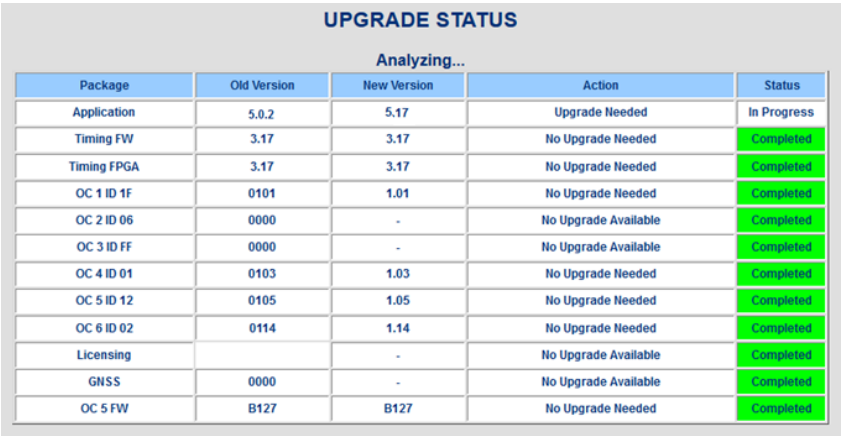
UPGRADE STATUS

Analyzing...

Package	Old Version	New Version	Action	Status
Application	5.0.2	5.17	Upgrade Needed	In Progress
Timing FW	3.17	3.17	No Upgrade Needed	Completed
Timing FPGA	3.17	3.17	No Upgrade Needed	Completed
OC 1 ID 1F	0101	1.01	No Upgrade Needed	Completed
OC 2 ID 06	0000	-	No Upgrade Available	Completed
OC 3 ID FF	0000	-	No Upgrade Available	Completed
OC 4 ID 01	0103	1.03	No Upgrade Needed	Completed
OC 5 ID 12	0105	1.05	No Upgrade Needed	Completed
OC 6 ID 02	0114	1.14	No Upgrade Needed	Completed
Licensing		-	No Upgrade Available	Completed
GNSS	0000	-	No Upgrade Available	Completed
OC 5 FW	B127	B127	No Upgrade Needed	Completed

Caution: Do not close the Web UI, or attempt to reboot the unit. The installation is in progress and may take several minutes to complete.

SecureSync will reboot itself during the update process, as shown in the following screenshot:



UPGRADE STATUS

Analyzing...

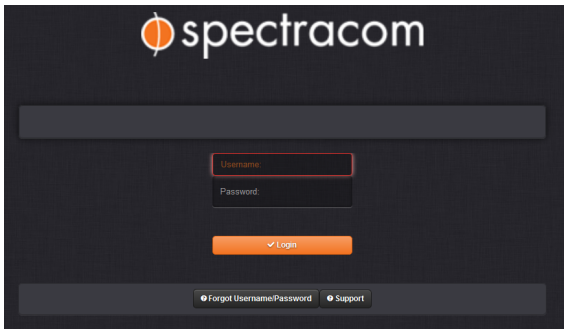
Package	Old Version	New Version	Action	Status
Application	5.0.2	5.17	Upgrade Needed	In Progress
Timing FW	3.17	3.17	No Upgrade Needed	Completed
Timing FPGA	3.17	3.17	No Upgrade Needed	Completed
OC 1 ID 1F	0101	1.01	No Upgrade Needed	Completed
OC 2 ID 06	0000	-	No Upgrade Available	Completed
OC 3 ID FF	0000	-	No Upgrade Available	Completed
OC 4 ID 01	0103	1.03	No Upgrade Needed	Completed
OC 5 ID 12	0105	1.05	No Upgrade Needed	Completed
OC 6 ID 02	0114	1.14	No Upgrade Needed	Completed
Licensing		-	No Upgrade Available	Completed
GNSS	0000	-	No Upgrade Available	Completed
OC 5 FW	B127	B127	No Upgrade Needed	Completed

Note: If using a DHCP assigned IP address (instead of having a statically assigned IP address), the unit's IP address may change once the update has completed (it may be re-assigned a different IP address by the DHCP server). Automatic Reloading of the Web UI will not work if the address has been changed by the DHCP server. Therefore, a new web browser connection using the newly assigned IP address will need to be opened.

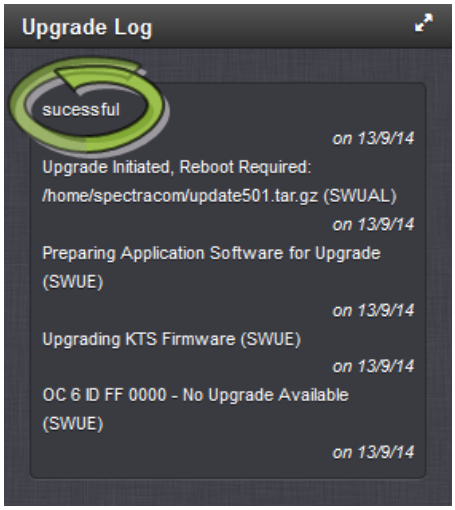
If the front panel LCD is configured to display network settings, the LCD window will show the newly assigned IP address.

When using a static-assigned IP address (or if the DHCP server did not assign a new IP address after the reboot), and as long the Web UI did not time-out during the update process (if it times-out, press the F5 key to refresh the connection), once the update is complete, you will now see the main page of the "new" Web UI design.

If you need to reconnect to the Web UI at any point, the login screen for the new Web UI design will now look like the following:



With the new Web UI design, the **Upgrade Log** with is located in the upper-right corner of the **Home** page. The top of this log should indicate “Successful”.



2.1.1 Required Repeat of Upgrade Process

IMPORTANT: The upgrade process must be performed a second time, if you are upgrading **from a software version 5.1.4** or lower (as described in this chapter) AND your unit is equipped with a **RES-SMT-GG** receiver.

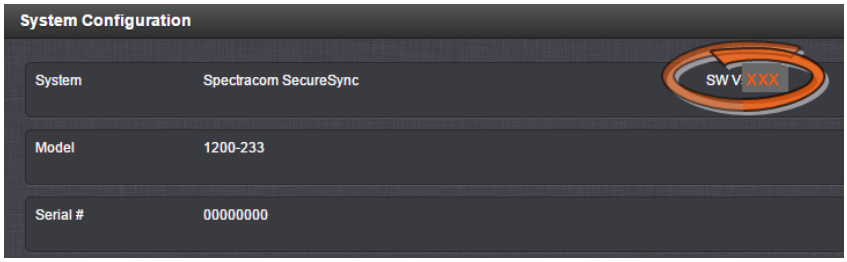
This is required to update the GNSS receiver firmware.

Caution: Note the second time performing the same update process does require the update file be uploaded into the unit again. The checkbox Force Update must NOT be checked.

With `updateXXX.tar.gz` in the update drop-down list after re-loading the update file, just select **Perform Upgrade** again and click **Submit**. The second time through the update process will be faster than the first time, as the receiver is the only item updated.

2.1.2 Confirming Successful Installation

Navigate to **Tools** > **Upgrade/Backup**. The following information should now be displayed:



2.1.3 Creating new Local Clock(s)

If you previously used a Local Clock (or several), manually re-generate these Local Clock (s), using the settings you wrote down in **Step 1** above. For instructions see the main **User Manual** under **MANAGING TIME > System Time >** Local Clock(s).

2.2 Upgrading from V. ≥5.1.2 to a Newer Version

Note: Depending on the software currently installed on your unit, upgrading to the latest version may be a multi-step process. See "Determining the Correct Upgrade Procedure" on page 8 for more information.

The software upgrade process is performed using PC that is either on the same network as the SecureSync appliance, or is connected directly to the SecureSync via a network cable.

Note: In order to perform the software upgrade, the Web UI of the unit to be upgraded must be accessible from this particular PC.

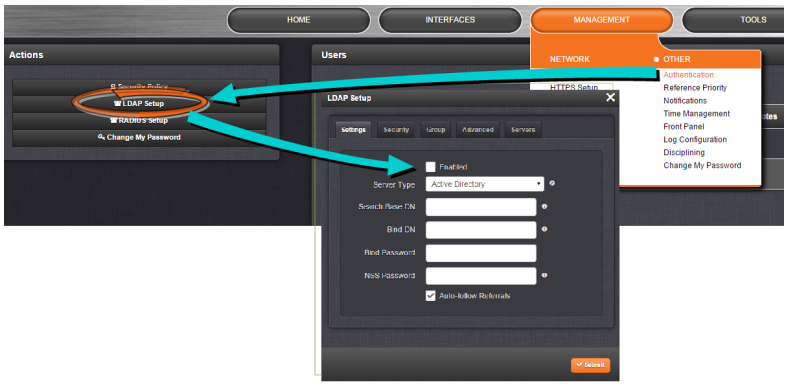
Once you downloaded the upgrade file onto a network PC, you can then transfer the file onto your SecureSync unit, using the unit's Web UI.

Note: Alternatively, you can also upgrade via Command Line Interface: In this case, the file must be transferred manually, using FTP/SFTP, to the SecureSync directory `home/spectracom`.

During the time that the file is being uploaded into SecureSync, the unit will remain fully functional and accessible for other network PC's.

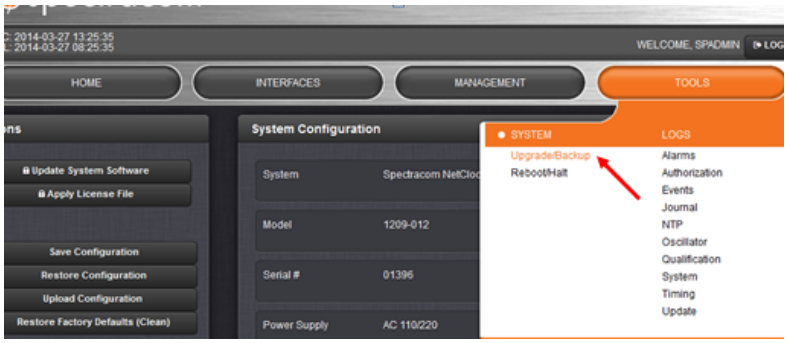
Once the file transfer is complete, SecureSync is performing the software upgrade ("Upgrade System"), during which the unit is configured: Normally, all current SecureSync configurations are automatically saved and restored as part of the update process. During the "Upgrade System" process, the front panel LCDs will go blank, and the unit will not be operational until the upgrade process has completed.

1. Verify that LDAP has not been ENABLED inadvertently, by navigating to **Management** > **Authentication** > **Actions: LDAP Setup**: If you are not using LDAP, DISABLE the service (if correctly configured, the services can remain ENABLED during the upgrade process).

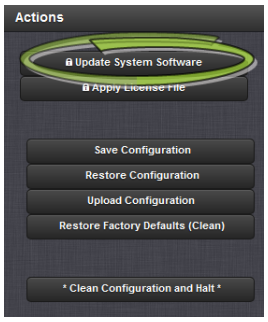


2. Download the SecureSync ugrade file (`updateXXX.tar.gz`) from the Spectracom website—see also "Downloading the Upgrade Software Bundle" on page 12—to an accessible directory on your local Windows machine (such as `C:/Temp`).

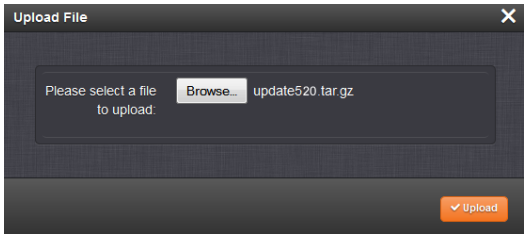
3. Open the Web UI, and login. Then navigate to **Tools** > **Upgrade/Backup**.



4. Click the button **Update System Software** in the top-left corner of the **Upgrade/Backup** page:

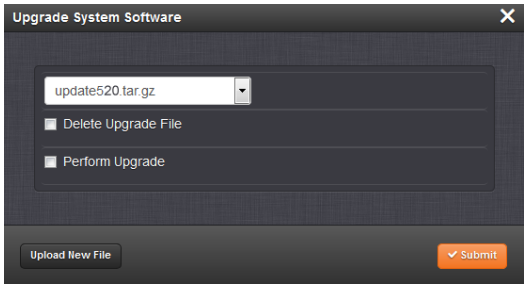


5. Click **Browse...**, and navigate to the location to which you previously saved the update file (`updateXXX.tar.gz`) on your PC (such as `C:/Temp`). Select the file. The file name will appear next to the **Browse...** button.
6. Click **Upload**.

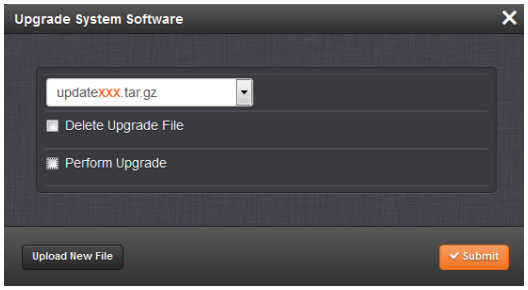


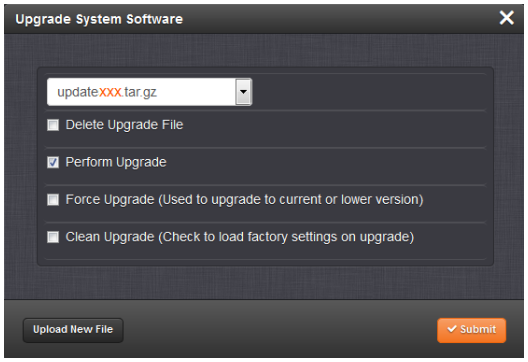
Note: When uploading files remotely via long distances, or when uploading multiple files via several browser windows simultaneously, the upload process may fail to complete. In this case, cancel the upload by clicking X, and go back to Step 2.

7. The file upload process may take several minutes. Once the file has been uploaded into your SecureSync, the directory of `updatexxx.tar.gz` (where xxx is the version) will be listed in the "File" dropdown, (The "down arrow" to the right-side of this field may need to be clicked, in order to see the file, if previous update files have been uploaded).



8. Ensure the correct file name (`updateXXX.tar.gz`)[1] is selected in the "File" dropdown field.
9. Check the box next to **Perform Upgrade** to install the software update (or to downgrade to an earlier version).
   Once this checkbox has been selected, two other checkboxes (**Force Upgrade** and **Clean Upgrade**) will become visible towards the bottom of the window. Note that these two checkboxes do not need to be selected for a standard upgrade to a newer version.





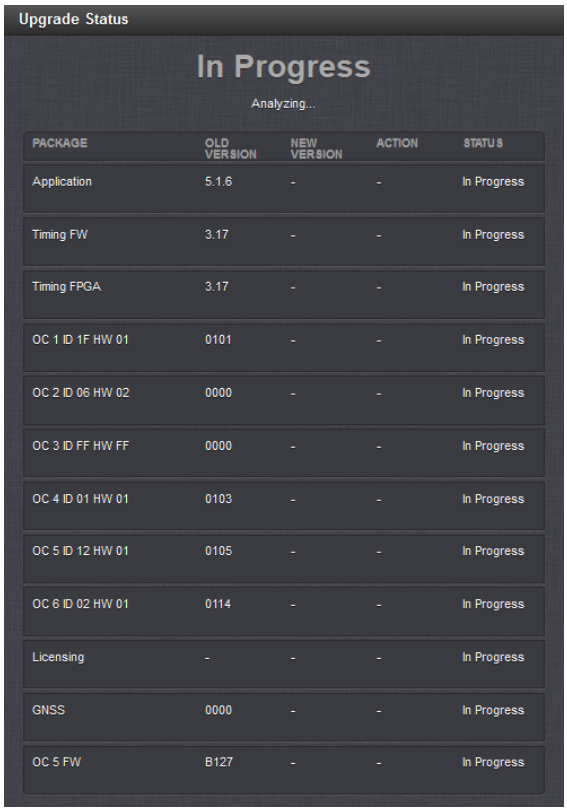
[1] XXX: Software Upgrade Version Number

- **Force Upgrade** — When checked, will force the software to install all update packages, even if it is already at the current revision, (for example, it is desired to install version 5.9.2, even though version 5.9.2 is already installed). The software will reinstall over the previously installed packages.

  USE CASE: This checkbox needs be selected if it is ever desired to downgrade to a previous version of Software.

- **Clean Upgrade** — When checked, will return the SecureSync to its original factory configuration for the version of software being installed. (The **Force Upgrade** checkbox will be automatically selected when the **Clean Upgrade** checkbox is selected.)

Note: To perform a standard software upgrade, i.e. from an earlier software version to the latest version, only the checkbox Perform Upgrade needs to be selected.



During the System Upgrade process, the **Upgrade Log** window on the right-side of the browser will periodically have new entries asserted, indicating the update process is progressing.

Caution: Do not close the Web UI, or attempt to reboot the unit. The installation is in progress and may take several minutes to complete.

The **Upgrade Status** window will remain displayed during the upgrade progress, as long the browser is not refreshed (such as by pressing the keyboard F5 key, for instance) or as long as the web browser background is not clicked. If the page happens to be refreshed or the background clicked during the next few minutes while the update is being performed (causing the **Status** window to disappear), this **Status** window cannot be re-opened. However, the software update will continue to be performed with the window closed (the **Upgrade Status** window and the Web UI being open are not required for the update to be performed). The **Status** window will periodically report status change updates.

Note: If using a DHCP assigned IP address (instead of the unit having a statically assigned IP address), the IP address may change once the update has completed (it may be re-assigned a different IP address by the DHCP server).

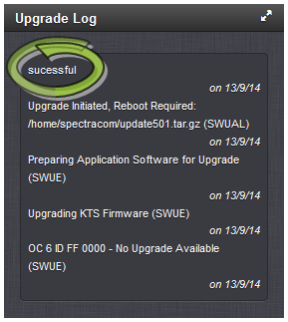
Automatic Reloading of the web page will not work if the address has been changed by the DHCP server. Therefore, a new web browser connection using the newly assigned IP address will need to be opened.

If the front panel LCD is configured to display network settings, the LCD window will show the newly assigned IP address.

When using a static-assigned IP address (or if the DHCP server did not assign a new IP address after the reboot), and as long the web browser didn't time-out during the update process (if it times-out, press the F5 key to refresh the connection), once the update is complete, you will now see the main page of the new web browser design.

Upgrade Log

The **Upgrade Log** is located in the upper-right corner of the **Tools** > **Upgrade/Backup** page of the Web UI. After completion of the upgrade process, the top of this log should indicate "Successful".



2.2.1 Potential Need to Repeat Upgrade Process

IMPORTANT: **The upgrade process must be performed a second time, if:**

a. your unit is equipped with a **RES-SMT-GG** receiver, and you are upgrading **from a software version 5.1.4** or lower

b. OR: If your unit is equipped with a **u-blox M8T** receiver, and you are upgrading from a software version **older than 5.5.0** .

This is required to update the receiver firmware.



Caution: Note the second time performing the same update process does require the update file be uploaded into the time server again. The check-box Force Update must NOT be checked.

With `updateXXX.tar.gz`[1] in the update drop-down list after re-loading the update file, just select **Perform Upgrade** again and click **Submit**. The second time through the update process will be faster than the first time, as the receiver is the only item updated.

2.2.1.1 u-blox M8T: Upgrading to Version 5.9.2:

1. Update to software version 5.9.2.
2. The final update status page after reboot will show the u-blox M8T failed to update to version 3.0.1 TIM 1.10.
3. Re-run the update again in order to update the u-blox M8T.

Should you see a version other than 3.0.1 TIM 1.10 displayed, the upgrade was not successful. Proceed as follows:

a. Reset the receiver from the Web UI: Navigate to **Interfaces > References: GNSS Reference**, and click the GEAR button next to the **GNSS Reference**. In the **GNSS 0** window, locate the **Reset Receiver** box, check it, and click Submit.

b. If the version persists, reboot SecureSync.

c. If it still persists, run the Release 5.9.2 update again.

[1] XYZ = New Software Version

2.2.1.2 RES-SMT-GG: Upgrading to Version 5.9.2:

1. Update to software version 5.9.2.
2. The final update status page after reboot will show the u-blox M8T failed to update to version 1.9.
3. Re-run the update again in order to update the RES-SMT-GG.

Should you see a version other than 1.9 displayed, the upgrade was not successful. Proceed as follows:

a. Reset the receiver from the Web UI: Navigate to **Interfaces > References: GNSS Reference**, and click the GEAR button next to the **GNSS Reference**. In the **GNSS 0** window, locate the **Reset Receiver** box, check it, and click Submit.

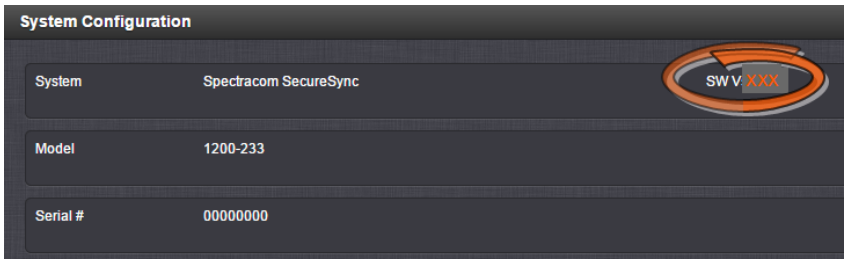
b. If the version persists, reboot SecureSync.

c. If it still persists, run the Release 5.9.2 update again.

2.2.2 Confirming Successful Installation

Note: You will need to log into the Web UI, using your login account information

Navigate to **Tools** > **Upgrade/Backup**. The new **System** software version should be displayed, and the new **GNSS Receiver** version should be displayed (Trimble RES-SMT-GG: **SW V1.9**; u-blox M8T: **SW V3.0.1 TIM 1.10.**)



BLANK PAGE.

APPENDIX

Appendix

The following topics are included in this Chapter:

3.1 Upgrading via CLI ii
3.2 Saving/Restoring Configuration Files iii
3.3 Software Update Log Entries iii
3.4 Downgrading the SW to a Previous Version . iii
3.5 "Upgrade Failure" (V. 5.0.2 to a Newer Version) vi
3.6 "Upgrade Failure" (V. ≥5.1.2 to a Newer Version) viii
3.7 Technical Support xii

3.1 Upgrading via CLI

It is possible perform a software upgrade via a Command Line Interface, rather than using the Web UI, for example for scripting software updates.

Starting in Archive software version 4.8.8, the software update can be initiated using a CLI command (issued via telnet, SSH or the front panel Serial port), instead of using the web browser, if desired. This entails performing an FTP/SCP transfer of the software update file into SecureSync's `/home/spectracom` directory and then issuing the sysupgrade CLI command to initiate the software upgrade.



Note: IMPORTANT: When transferring the update file using either FTP or SCP (instead of uploading it using the web browser), make sure the Update file is transferred using BINARY mode (SCP transfer is preferred, because it always transfers using Binary mode). Otherwise, this file will likely be altered during the file transfer, preventing the updater from being able to extract it. The following error message will be asserted into the Update log if the Update file is altered/can't be extracted: "ERROR (-1) - Failure while unpacking Upgrade Bundle (SWUE)".

The syntax for issuing the sysupgrade command is:

- Standard upgrade (Such as upgrading versions 4.8.8 to 4.8.9, for example): "sysupgrade" followed by the upgrade file name (Example: sysupgrade update489.tar.gz).
- Forced upgrade (Such as downgrading versions 4.8.9 to 4.8.8, for example, but can also be used with Standard upgrades, also): "sysupgrade force" followed by the upgrade file name (Example: sysupgrade force update489.tar.gz).
- Clean upgrade (Such as first performing a Forced upgrade from 4.8.8 to 4.8.9, for example. Then automatically resetting the NTP server back to factory default settings and deleting all log files): "sysupgrade clean" followed by the upgrade file name (Example: sysupgrade clean update489.tar.gz).

3.2 Saving/Restoring Configuration Files

Important note about restoring old configuration files

Due to fairly significant changes to the system configuration files from system software versions prior to version 5.9.2, it is not recommended to perform a configuration restore with 5.9.2 software installed, from a configuration save that was performed in a SecureSync with versions 4.8.9 or earlier installed. If a configuration restore from versions 4.8.9 or below software is performed on a version 5.x.x time server, a 'clean' will be required to be performed via the front panel keypad thereafter to reset the NTP server to the factory default settings for the installed version.

In general, due to possible changes to configuration files from one version to another, if you wish to have a configuration backup file saved, we recommend performing a new "configuration save" after each new software update is performed, to replace the earlier configuration bundle. This will ensure that if a configuration restore is performed, the configs in the captured file will be identical to the ones in the NTP server.

3.3 Software Update Log Entries

Software update log entries, such as upgrades that have already been performed, or an error occurring during the update process, are placed in the **Update** Log (**Tools** > **Logs** page of the Web UI). Please refer to this log if you have any problems with the software update process (such as if the message "Upgrade Failure" is displayed, for instance).

3.4 Downgrading the SW to a Previous Version

If desired, the software can be downloaded to previous versions 5.0.0 or higher (it is not recommended to downgrade to versions 4.8.9 or below from versions 5.0.0 and above). The downgrade process is the same as an upgrade, except an earlier version update bundle is selected during the process and the update needs to be "Force Updated" (to override the version checking that normally occurs).

Note: Due to incompatibilities between later and earlier configuration files, a "Clean Upgrade" is also required to be performed during the software "downgrade" process (the unit will need to be reconfigured as desired, once it's been downgraded to the desired, earlier version).

Note: You will not be able to apply a Saved configuration file from a later version of software to any earlier, downgraded version of software to restore the configurations. However, a saved config file previously performed when it was at the earlier version can be safely re-applied as desired to restore configs.

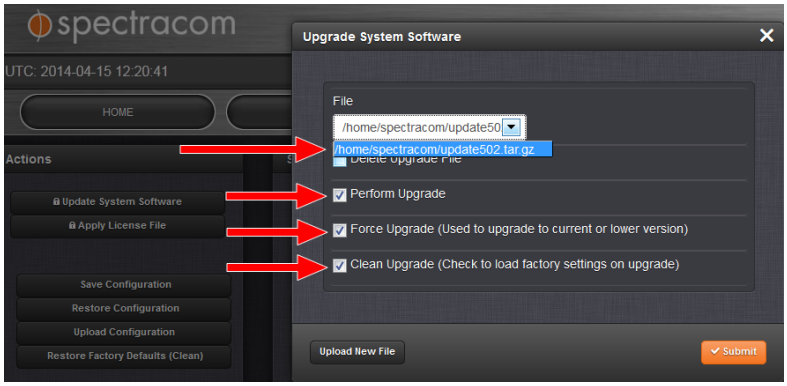
Downgrading to an earlier version using the newer (black/charcoal background) Web UI:

To simultaneously downgrade and 'Restore Factory Configuration":

1. Navigate to the **Tools** > **Upgrade/Backup** page.
2. Press **Update System software** (on the left side of the screen, under **Actions**).
3. Verify the desired update bundle you wish to downgrade to is in the **File** drop-down. If not, press **Upload New File** and browse to where the earlier update bundle is stored. Upload the bundle into the unit.
4. Select the **Perform Upgrade** checkbox in the menu that opens, which will expand the menu down to display two additional checkboxes.
5. Select the desired Update bundle version which you wish to downgrade to.
6. Select also the **Force Upgrade** and **Clean Upgrade** checkboxes, before clicking **Submit** (as shown in the screenshot below) to begin the downgrade. The Clean Upgrade checkbox resets all of the configurations back to factory default, as needed to occur when downgrading to an earlier software version.

   The software downgrade will take several minutes to complete.

Note: If the software was downgraded back to a version prior to version 5.1.0, the "classic interface" will be displayed after logging back in, once the downgrade has completed.



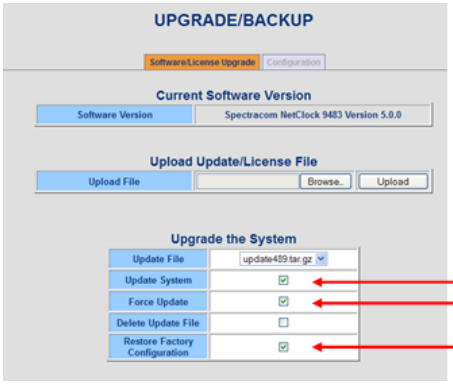
1. Once downgraded, reconfigure the unit's settings as desired, or restore a previously Saved config file from the version the software has been downgraded to.

Downgrading to an earlier version using the "classic interface" Web UI

To simultaneously downgrade and **Restore Factory Configuration**, in addition to selecting the **Update System**, and **Force Update** checkboxes, also select the **Restore Factory Configuration** checkbox before clicking **Submit** (as shown in the screenshot below). The software downgrade will take several minutes to complete.

The **Restore Factory Configuration** checkbox resets all of the unit's configurations back to the factory default settings.

Note: If the software was downgraded back to a version prior to version 5.1.2, the "classic" interface will be displayed after logging back in, once the downgrade has completed.



Select the "**Update System**", the "**Force Update**" and the "**Restore Factory Configuration**" check-boxes when downgrading to any previous version (such as downgrading from version 5.0.2 to version 4.8.9, for example).

Reconfigure the settings as desired, or restore a previously saved config file from the version the software has just been downgraded to.

3.5 "Upgrade Failure" (V. 5.0.2 to a Newer Version)

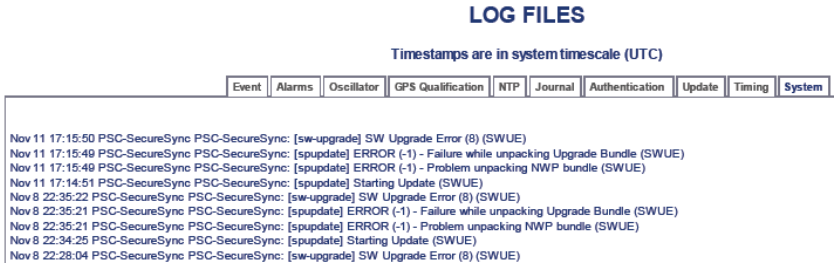
If the Update process returns "Upgrade Failure" (as shown below), the software update process was not successful.



If this happens, review the entries in the Update and System logs.

Applying the same version already installed or downgrading to an earlier version of software without select the "Force Update" checkbox, in addition to selecting the "Update System" checkbox can cause the upgrade to fail. Make sure to select "Force update when applying the same or earlier version of software.

The Update log may contain the following entry: "Error (-1) Failure while unpacking Upgrade Bundle" / "Problem unpacking NWP bundle" (as shown below):

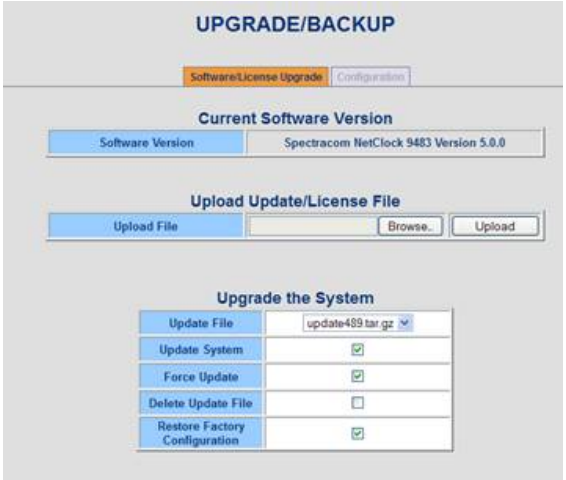


Likely causes for this error message in the Update log

- The update file may be corrupt (preventing it from being able to be extracted in the time server). Run MD5 checker against the update file to verify file integrity. Spectracom provides the MD5 file for each software update file.
- Too many Update Bundles are stored in the time server. Delete previous update bundles (such as update489, for instance).

Once a software update has been applied, the update bundle can be deleted (the bundles only need to be stored in the time server to alleviate the need to transfer them again to perform a software downgrade. Otherwise, they can be safely deleted without affecting the time server). Having too many upgrade files saved can prevent the update file being applied from being able to extract.

To delete earlier update files, select each one individually in the drop-down, check only the "Delete Update File" checkbox in the screen where you normally select "Update File". Then press Submit. This will delete the selected update file. Then run the update process again.



3.6 “Upgrade Failure” (V. ≥5.1.2 to a Newer Version)

If the Update process returns “Upgrade Failure” (as shown below), the software update process was not successful. Note that starting the update process again after it is already been started will result in an “upgrade failure” of the subsequent update process, while the first one is still being performed in the background.



If this happens, review the entries in the Update and System logs.

1. The time server may be retaining earlier upgrade bundle files which were applied and are no longer needed. Previous update bundles should be deleted. For more information, see "Deleting Old Update Files" on page 11.
2. Applying the same version already installed or downgrading to an earlier version of software without select the “Force Update” checkbox, in addition to also selecting both the “Force Upgrade” and “Clean Upgrade” checkboxes can cause the upgrade to fail. Make sure to select the “Perform Upgrade”, “Force Upgrade” and “Clean Upgrade” checkboxes when applying the same or earlier version of software.
3. The Update log may contain the following entry: “Error (-1) Failure while unpacking Upgrade Bundle” / “Problem unpacking NWP bundle”

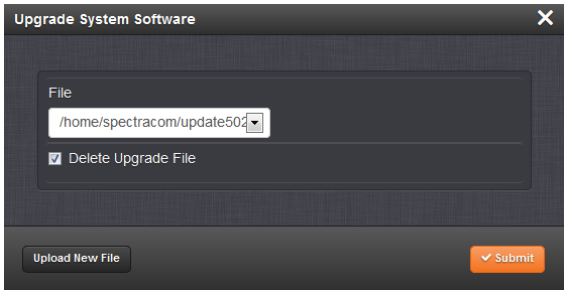
Likely causes for this error message in the Update log:

» The update file may be corrupt (preventing it from being able to be extracted in the time server). Run MD5 checker against the update file to verify file integrity. Spectracom provides the MD5 file for each software update file.

» Too many Update Bundles are stored in the time server. Delete previous update bundles (such as update489, for instance).

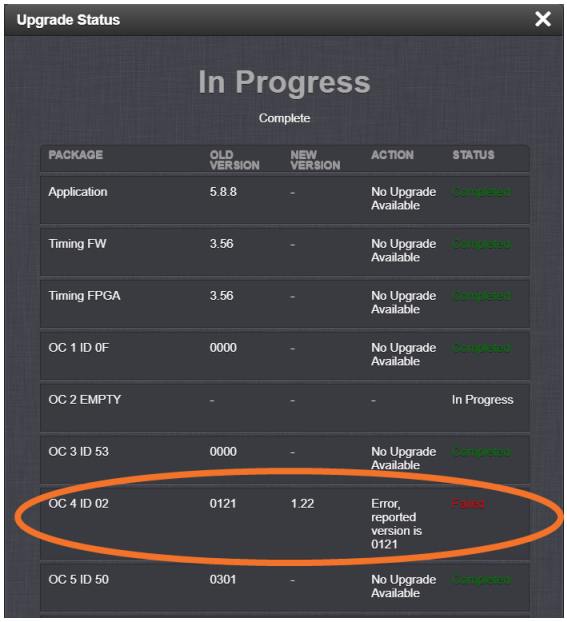
Once a software update has been applied, the update bundle can be deleted (the bundles only need to be stored in the time server to alleviate the need to transfer them again to perform a software downgrade. Otherwise, they can be safely deleted without affecting the time server). Having too many upgrade files saved can prevent the update file being applied from being able to extract.

To delete earlier update files, select each one individually in the drop-down, check only the checkbox **Delete Upgrade File** in the screen where you normally select "Update File". Then click Submit. This will delete the selected update file. Then run the update process again.



3.6.1 Failure of Component Upgrades

Certain conditions may cause your overall upgrade status to be listed as Complete, even though some components show Failed upgrades.



Note: One known cause of this problem is in units currently running software version 5.8.3 through 5.8.7 with option cards 1204-01, 1204-02, 1204-03, 1204-04, 1204-05, 1204-15, or 1204-23 installed and active, and upgrading to a newer version.

If a component such as an option card fails your first attempt at upgrade:

- Upload the upgrade file again
- Repeat upgrade
- Note component status

If all Failed messages have cleared, the update has been successful with all expected materials.

If you receive additional Failed messages, it is recommended that you contact Technical support for additional insturction or infomation.

3.7 Technical Support

To request technical support for your SecureSync unit, please go to the "Timing Support" page of the Orolia website (https://www.orolia.com/support/timing), where you can not only submit a support request, but also find additional technical documentation.

Phone support is available during regular office hours under the telephone numbers listed below.

To speed up the diagnosis of your SecureSync, please send us:

- the current **product configuration** (see "Option Card Identification" on page 1 to find out which option cards are installed in your unit), and
- the **events log** (see "Saving and Downloading Logs" on page 1).

Thank you for your cooperation.

3.7.1 Regional Contact

Orolia operates globally and has offices in several locations around the world. The Orolia (Spectracom) main offices are listed below:

Table 3-1: Orolia contact information

Country	Location	Phone	Address
France	Les Ulis	+33 (0)1 64 53 39 80	**Orolia France** Parc Technopolis – Bat. Sigma 3, Avenue du Canada 91974 Les Ulis Cedex
USA	West Henrietta, NY	+1 585 321 5800	**Orolia USA** 45 Becker Rd, Suite A West Henrietta, NY 14586

Additional regional contact information can be found on the Contact page of the Orolia website (https://www.orolia.com/contact-us).