

SPS GNSS

VERSION 5.44/6.04 FIRMWARE

This document contains summary information on new features, late-breaking product information, updates, and troubleshooting tips not covered in the Trimble® SPS GNSS firmware documentation.

Introduction

These release notes describe the features and enhancements that are new in version 5.44 of the SPS GNSS firmware. This release is shown as Active Firmware Version 6.04 / Active Core Engine Version 5.44 in the SPS986 Web UI.

The following table shows the minimum firmware warranty date that you require to load the new firmware into your Trimble SPS GNSS receiver. Contact your Trimble Dealer/SITECH if an extended firmware warranty is required.

We advise users to connect their SPS GNSS to the Trimble Installation Manager (see below for details on Trimble Installation Manager) to load the 5.44/6.04 firmware. That method will automatically determine whether the receiver is currently able to load the firmware based on the receiver’s firmware warranty date.

SPS GNSS Model receiver	Firmware Warranty Date (min)
SPS855, SPS852	November 2018
Fugro 9205	November 2018
SPS985, SPS985L	November 2018
SPS986	November 2018
SPS356	November 2018
SPS585	November 2018
BX982	November 2018
BX992	November 2018

Please order firmware maintenance if required to upgrade to v5.44 firmware.

Version: 5.44
 Date: November 2019

Part Number	Description
EWHCC-FW	TPP - Firmware Maintenance - HCC SPS GNSS Receiver, SPS Smart Antenna or GPS Receiver
EWHCC-FW-RNST	TPP - Firmware Maintenance - HCC SPS GNSS Receiver, SPS Smart Antenna or GPS Receiver Reinstatement

For further support information, go to www.trimble.com/Support/

System support

System compatibility with this release of SPS GNSS firmware is detailed below.

Siteworks and SCS900 System compatibility

The current released version of Trimble Siteworks (v1.11) has been tested to be compatible with SPS GNSS firmware v5.43/v6.03 only, not the v5.44/6.04 release described in these release notes. Please refer to the most current Siteworks and SCS900 release notes for the currently supported GNSS firmware versions before upgrading.

New Security Legislation

Senate Bill 327 (SB 327) is a California (USA) law that will come into effect on January 1, 2020. The law will require manufacturers of devices that connect “directly or indirectly” to the internet to equip the devices with “reasonable” security features.

The law requires that depending on the nature and purpose of the device, if a device can be accessed outside a local area network then the password for the device needs to either be unique for each device OR force the user of the device to set their own password.

Although the law is currently specific to California, we have chosen to implement the changes to all affected devices shipped from Trimble before Jan 1, 2020.

Trimble GNSS Devices with enhanced security

This will be implemented in the GNSS receivers listed below that ship with the listed firmware (or greater) and factory security option installed.

GNSS receivers that ship with an earlier firmware version do not have the factory security option installed and will not include the enhanced security feature when upgraded to the listed firmware version.

Trimble GNSS Model	Firmware version	Downgrade limit
SPS855, SPS555H, Fugro9205	v5.44	v5.43

SPS986	v6.04	v6.01
SPS985L	v5.44	v5.03
SPS985	v5.44	v5.14
SPS585	v5.44	v5.00
SPS356	v5.44	v5.41
BX982	v5.44	v5.35
BX992	v5.44	v5.41

What's changed?

The first time you access the receiver WebUI you will need to perform additional steps to set up a new password for the 'admin' login. You will also be given the option to enable Wi-Fi access point security.

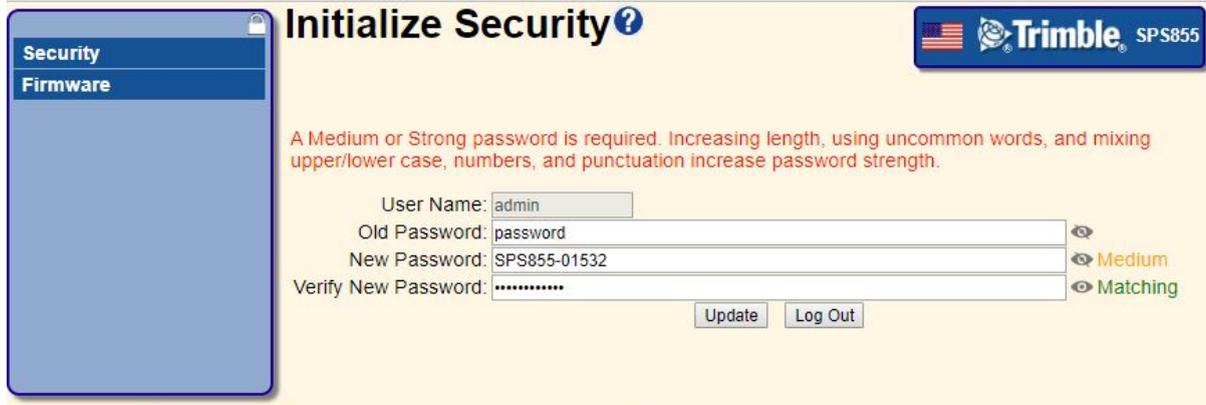
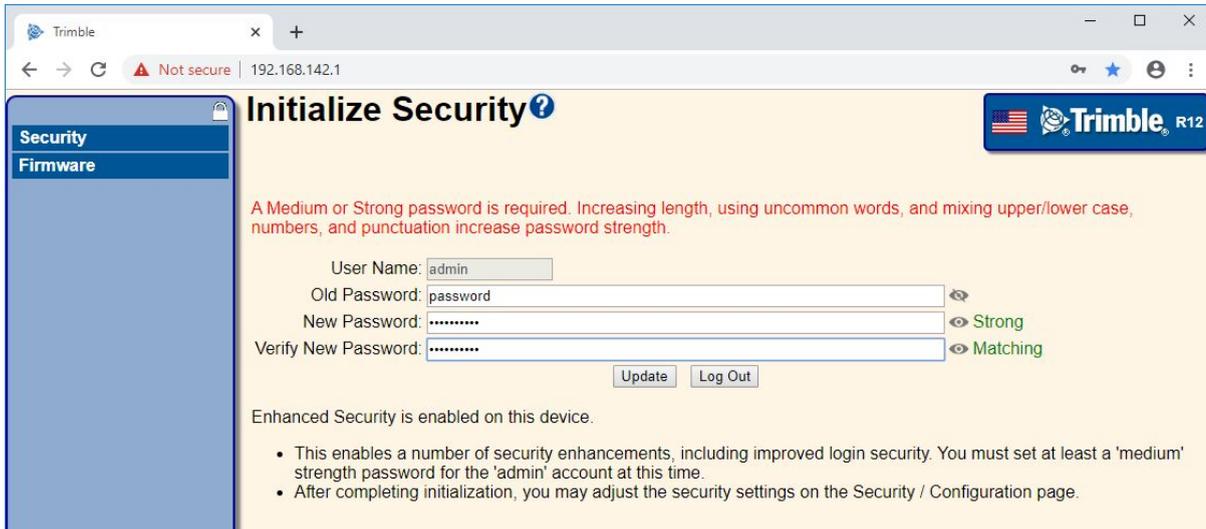
Connect to the receiver on Ethernet or via the Wi-Fi access point and open a web browser with the appropriate IP address to launch the WebUI. You will initially see that the list of menu options is limited to Security and Firmware. When prompted, enter the default login username and password.

By default, the username is **admin** and the password is **password**.



Next, you will be prompted to enter a new password. Use a combination of upper and lowercase letters, numbers, and punctuation in order to obtain a 'medium' or 'strong' password; a 'weak' password will be rejected. After verifying your new password, click "Update".

Make sure to record/remember the new password and be aware that it is no longer possible to clear this password without direct physical access to the receiver.



What do I do if I forget the password?

It is no longer possible to clear this password without direct physical access to the receiver.

The device can be reset by holding the power button for 35 seconds to return the unit to its default state.

For an SPS Modular device with a front panel display:

1. Hold down the Power button
2. The display shows a countdown timer.
3. When the display goes blank, continue to hold the Power button.
4. The display shows a countdown to clear the almanac and ephemeris.
5. When the counter reaches 0, continue to hold the Power button.
6. The display indicates a countdown to resetting the receiver.
7. When the counter reaches 0, release the Power button.

NOTE: The receiver will need to be reconfigured after the reset operation.

Any Options which have been installed will be unaffected by the reset.

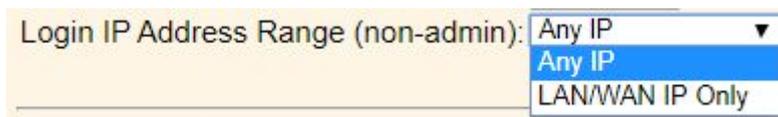
What if I am not connected to the Internet?

Security Configuration - LAN/WAN IP only

The Security Configuration page now includes a new option to allow weaker (or no) passwords to be used for non-admin accounts but with the restriction that accounts will only authenticate from WAN format IP addresses and not the Internet.

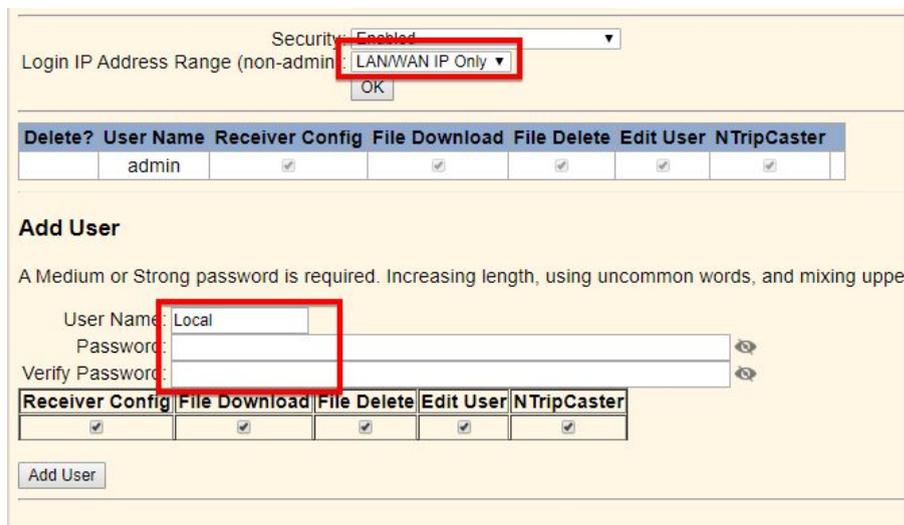
NOTE: First-time initialization of the “admin” account password is still required even if you are on a local network. The medium/strong requirement is maintained at all times for this account. The admin account always authenticates from any IP address.

Select “LAN/WAN IP Only” and create a new account.



The “Any IP” setting is the default, and there is no change in behavior. When “LAN/WAN IP Only” is selected, the user is allowed to use any strength password for accounts other than ‘admin’, but those accounts will only authenticate form from LAN/WAN IP addresses and not internet format addresses. Even a blank/empty password is allowed.

So a local user account could be set up without any password being required to allow anyone to access the receiver web UI from a LAN/WAN IP address.



Bluetooth Security

The Bluetooth module security has also been enhanced. Upon powering on the receiver a 5 minute pairing timer will begin, during which time the receiver’s Bluetooth is discoverable by other devices. Once the timer expires the receiver is no longer discoverable by external devices. In order to reset this timer the user can either power cycle the receiver or log into the webUI and restart the timer as shown in the image below.



Receiver specific changes

- SPS855: Field Radio- the status screen on the front panel of the SPS855 now indicates the radio link quality (%) when in Repeater mode.
- SPS855: Bluetooth connectivity between the TSC3 and the SPS855 has been improved to resolve the following issues:
 - Unable to complete SPS855 Base configuration using TSC3
- SPS585: Add expanded CSIB support. Geoid subgrid files of up to 128K can be integrated into the coordinate system (CSIB) file using the Configuration ToolBox application.

SPS986 with Trimble® ProPoint™ GNSS Technology

Trimble Civil Engineering and Construction is pleased to introduce Trimble® ProPoint™ GNSS Technology, a trademarked name for the GNSS engine contained within the Trimble SPS986 GNSS Smart Antenna. ProPoint allows users to measure points more quickly and with greater accuracy in certain challenging GNSS environments*. Flexible signal management enables the use of all available GNSS constellations and signals, resulting in higher satellite availability. When combined with advanced new proprietary noise modeling algorithms, ProPoint is better able to cope in situations where GNSS signals are obstructed or attenuated.

In one common example—positioning near or under tree canopy—GNSS satellites and signals may be lost or become unusable because of diffusion caused by leaves and branches. In urban environments, signals may reflect off of surfaces before reaching the GNSS receiver (multipath) or be obstructed entirely. These impediments limit the satellite data available to a GNSS receiver to produce a precise solution. The new Trimble ProPoint GNSS engine is able to take all of the usable signals available to it and use them to produce a survey-grade solution in many areas where other GNSS systems either can't provide a solution at all or which produce a solution with unreliable error estimates.

NOTE: This technology was available for all SPS986 receivers using receiver firmware 6.00 and higher since December 2018. Firmware versions 5.32 through 5.37 for the SPS986 do not utilize the ProPoint technology.

Version	Date	Benefit
5.40/6.00	Dec 2018	ProPoint and Dynamic Tilt
5.41/6.01	April 2019	ProPoint and Tilt Compensation
5.42/6.02	Jun 2019	ProPoint and Plumb Pole Routine
5.43/6.03	Oct 2019	ProPoint and Constellations Improvements.

**Results may vary depending on the user's geographic location, atmospheric activity, scintillation levels, GNSS constellation health and availability, and level of multipath.*

Trimble Installation Manager for SPS GNSS

- The [Product Bulletin](#) explains why Installation Manager should now be used for loading SPS GNSS firmware
- The following products can now be used with Installation Manager:
 - SPS986
 - SPS855, SPS555H
 - SPS985, SPS985L
 - Fugro 9205
 - SPS356
 - BX982
 - BX992
 - SPS585
- SPS GNSS Receivers that are not current products sold by Trimble today can not use Installation Manager.
- Other than the SPS986 and SPS785, Installation Manager can not load options, upgrades or the 450 MHz radio settings to SPS GNSS.

Upgrade procedure

1. There are 3 methods to upgrade firmware in a SPS GNSS receiver:
 - a. Web browser UI (Ethernet or WiFi)
 - b. WinFlash computer application (RS232 or USB)
 - c. Installation Manager (RS232 or USB)
2. Check the firmware warranty date on your SPS receiver is valid (see table in Introduction). If not, then you must purchase an extended warranty to be able to install v5.40 firmware.
3. Use the instructions in the SPS Help or Getting Started Guide to connect the computer to the receiver.
4. If using the Web UI method download the *.TIMG file from the Trimble support website http://www.trimble.com/Support/Support_AZ.aspx
5. See the online Guide: http://www.trimble.com/EC_ReceiverHelp/

Legal notices

Trimble Inc.
 Civil Construction & Engineering
 10368 Westmoor Drive
 Westminster, Colorado 80021
 USA

+1-800-361-1249 (toll free in USA)

+1-937-245-5154 Phone

www.trimble.com

Copyright and trademarks

© 2019, Trimble Inc. All rights reserved.

Trimble, the Globe & Triangle logo, CenterPoint, and OmniSTAR are trademarks of Trimble Inc., registered in the United States and in other countries. xFill is a trademark of Trimble Inc.

The Bluetooth word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Trimble Inc. is under license. All other trademarks are the property of their respective owners.

Release notice

This is the 5.44/6.04 2019 release (Revision B) of the Release Notes. It applies to version 5.44/6.04 of the SPS GNSS firmware.