TRIMBLE OEM GNSS

NEW CYBER SECURITY MEASURES FOR TRIMBLE GNSS RECEIVERS

The CA 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. This insures the highest security in all applications worldwide.

Affected Trimble GNSS Devices

Units received before January 1, 2020 are not affected by the following changes. Loading v5.44 or later firmware versions will not require you to update passwords to comply with the legislation.

Units received on or after January 1, 2020 will have the new behavior described below.

The following models are affected when they are received after January 1, 2020. They will have v5.44 or higher firmware installed.

Trimble GNSS Module	Firmware Version	Downgrade Limit
BD940	v5.44	v5.30
BD940-INS	v5.44	v5.33
BX940	v5.44	v5.30
BD970	v5.44	v5.34
BD982	v5.44	v5.35
BX982	v5.44	v5.35
BD990	v5.44	v5.37
BD992	v5.44	v5.37
BD992-INS	v5.44	v5.37
BX992	v5.44	v5.37

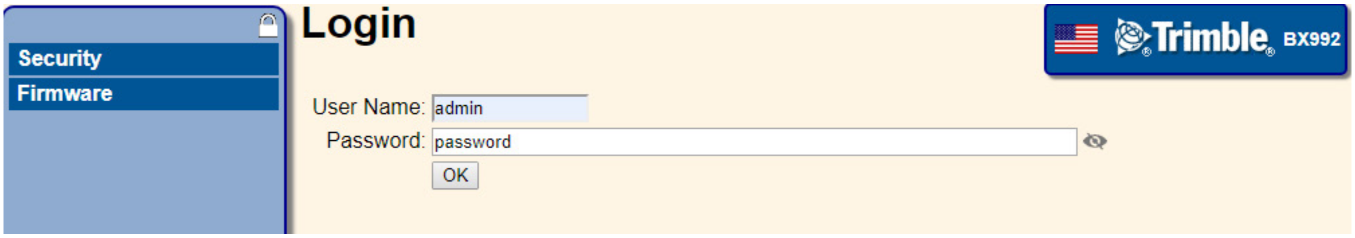
Note: These new security measures do not affect receivers that were shipped with a lower version of firmware(<5.44) and then choose to upgrade to 5.44 or above.

For information about the MB-Two and ABX-Two products, refer to this bulletin.

What’s changed on units shipped after Jan 1, 2020?

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.

Connect to the receiver on Ethernet 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**.



Login

BX992

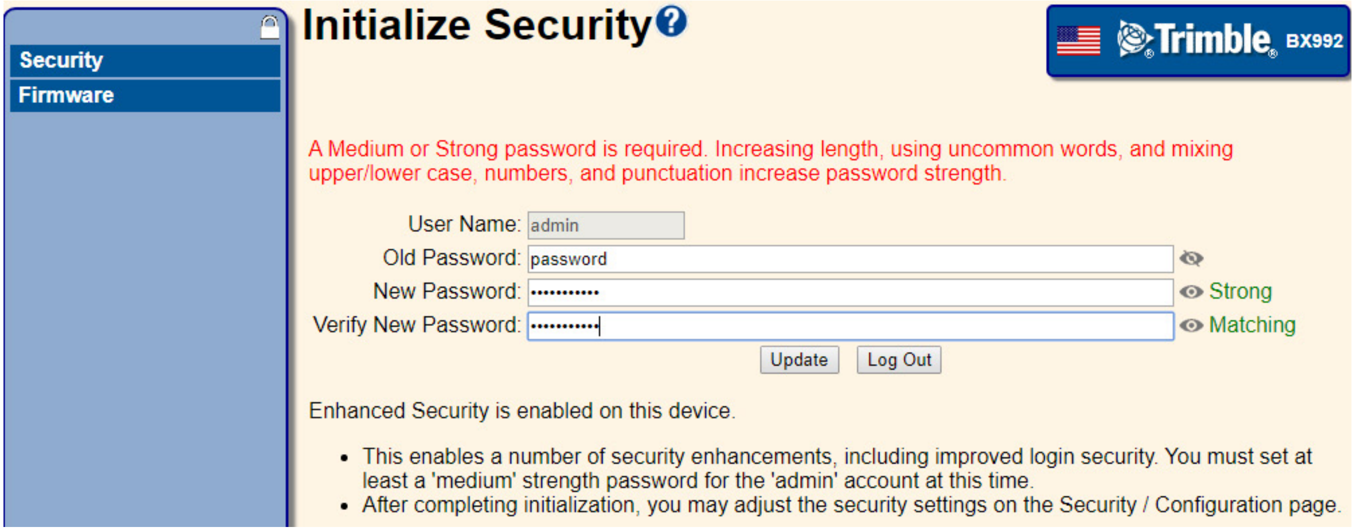
User Name: admin

Password: password

OK

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.



Initialize Security

BX992

A Medium or Strong password is required. Increasing length, using uncommon words, and mixing upper/lower case, numbers, and punctuation increase password strength.

User Name: admin

Old Password: password

New Password: ••••••••••• Strong

Verify New Password: ••••••••••• Matching

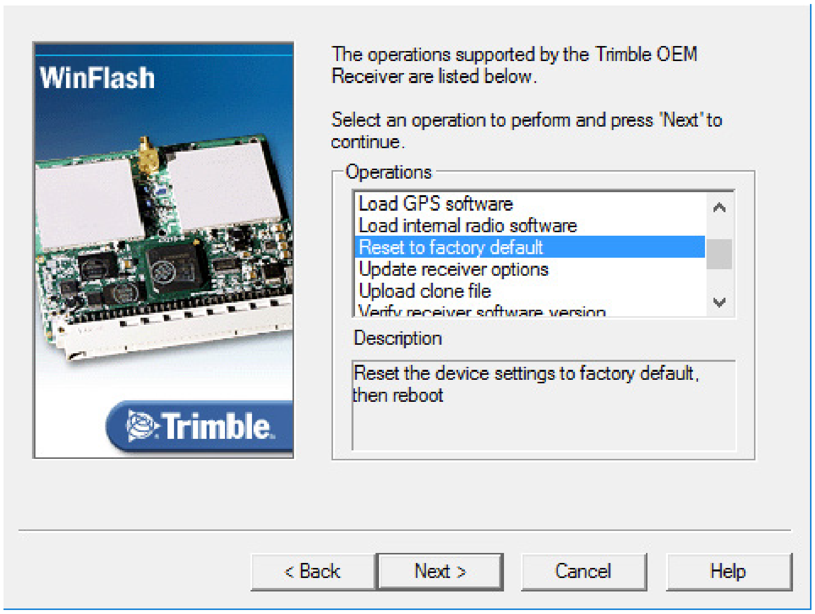
Update Log Out

Enhanced Security is enabled on this device.

- This enables a number of security enhancements, including improved login security. You must set at least a 'medium' strength password for the 'admin' account at this time.
- After completing initialization, you may adjust the security settings on the Security / Configuration page.

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.
Connect to the receiver using the WinFlash software and select "Reset to factory default". You will then have to repeat above steps starting with the username as **admin** and the password as **password.**



The operations supported by the Trimble OEM Receiver are listed below.

Select an operation to perform and press 'Next' to continue.

Operations

- Load GPS software
- Load internal radio software
- Reset to factory default
- Update receiver options
- Upload clone file
- Verify receiver software version

Description

Reset the device settings to factory default, then reboot

< Back Next > Cancel Help

Note: The receiver will need to be reconfigured after the reset operation.
Any Options which have been installed will be unaffected by the reset.

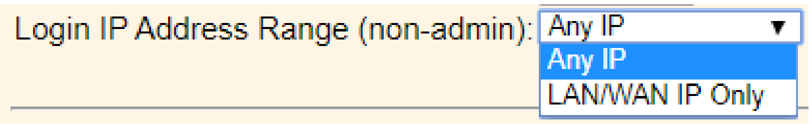
What if I am not connected to the Internet?

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 LAN/WAN 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 can always authenticate from any IP address.

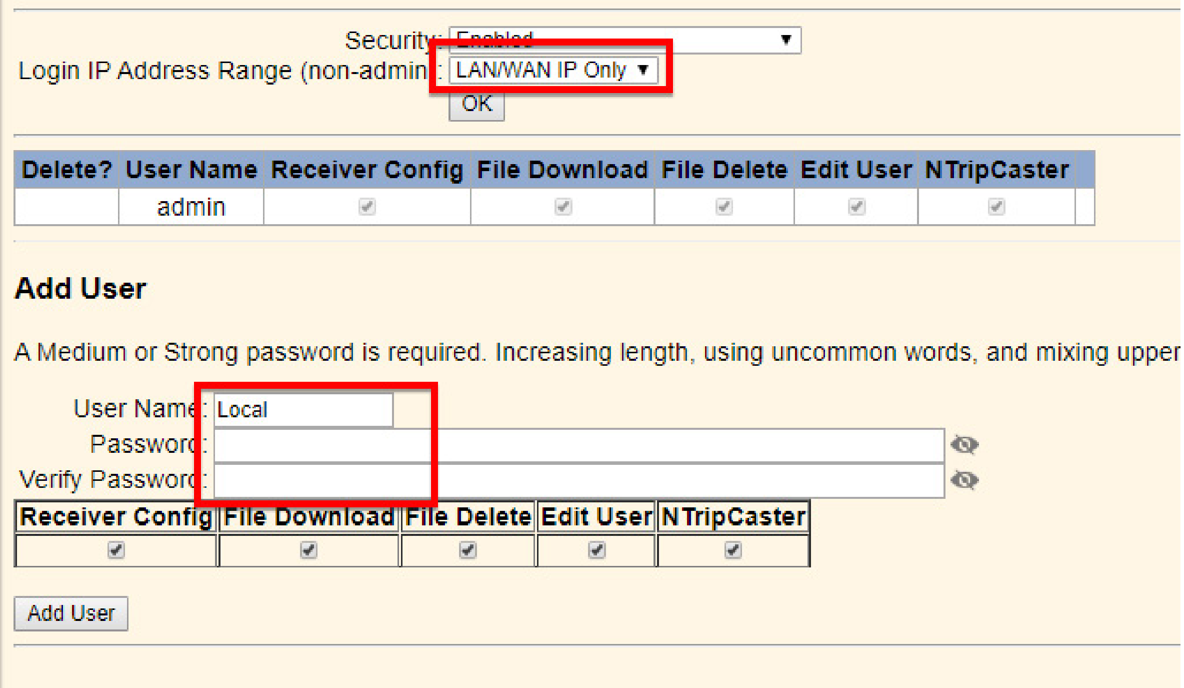
Select "LAN/WAN IP Only" and click OK.



Login IP Address Range (non-admin): Any IP ▼

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 from LAN/WAN IP 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.



Security: Enabled ▼
Login IP Address Range (non-admin): LAN/WAN IP Only ▼

Delete?	User Name	Receiver Config	File Download	File Delete	Edit User	NTripCaster
	admin	☑	☑	☑	☑	☑

Add User

A Medium or Strong password is required. Increasing length, using uncommon words, and mixing upper

User Name: Local
Password:
Verify Password:

Receiver Config	File Download	File Delete	Edit User	NTripCaster
☑	☑	☑	☑	☑