MSA
The Safety Company

fieldserver

FieldServer ENOTE

FieldSafe Secure FieldServer Web Server Setup and User Management Instructions

Revision: 2.B

Print Spec: 10000005389 (F)

MSA Safety
1000 Cranberry Woods Drive
Cranberry Township, PA 16066 USA

U.S. Support Information:
+1 408 964-4443
+1 800 727-4377
Email: smc-support@msasafety.com

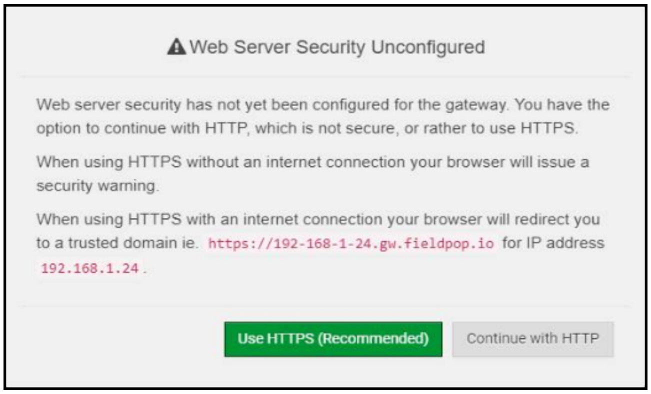
EMEA Support Information:
+31 33 808 0590
Email:
smc-support.emea@msasafety.com

For your local MSA contacts, please go to our website www.MSAsafety.com

1 Login to the FieldServer

The first time the FieldServer GUI is opened in a browser, the IP Address for the gateway will appear as untrusted. This will cause the following pop-up windows to appear.

- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



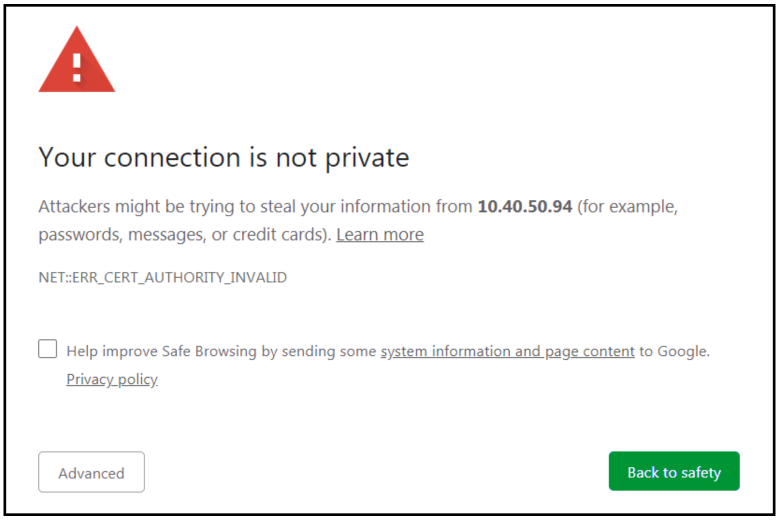
Web Server Security Unconfigured

Web server security has not yet been configured for the gateway. You have the option to continue with HTTP, which is not secure, or rather to use HTTPS.

When using HTTPS without an internet connection your browser will issue a security warning.

When using HTTPS with an internet connection your browser will redirect you to a trusted domain ie. `https://192-168-1-24.gw.fieldpop.io` for IP address `192.168.1.24`.

- When the warning that "Your connection is not private" appears, click the advanced button on the bottom left corner of the screen.



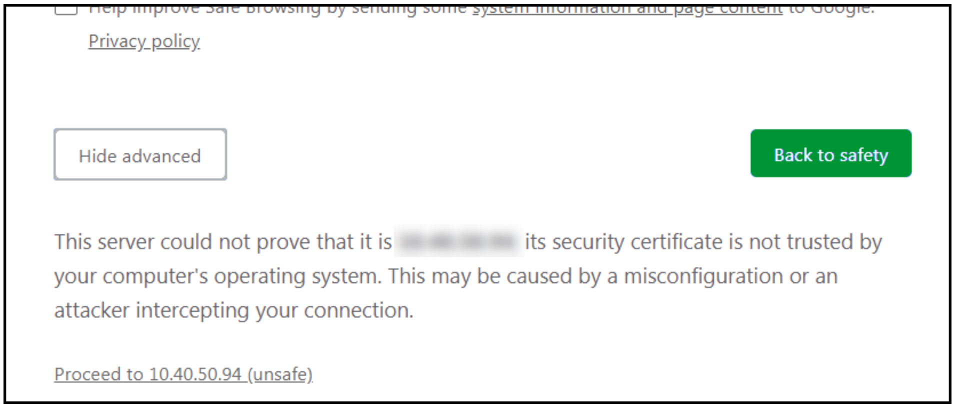
Your connection is not private

Attackers might be trying to steal your information from **10.40.50.94** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

- Additional text will expand below the warning, click the underlined text to go to the IP Address. In the example below this text is "Proceed to 10.40.50.94 (unsafe)".



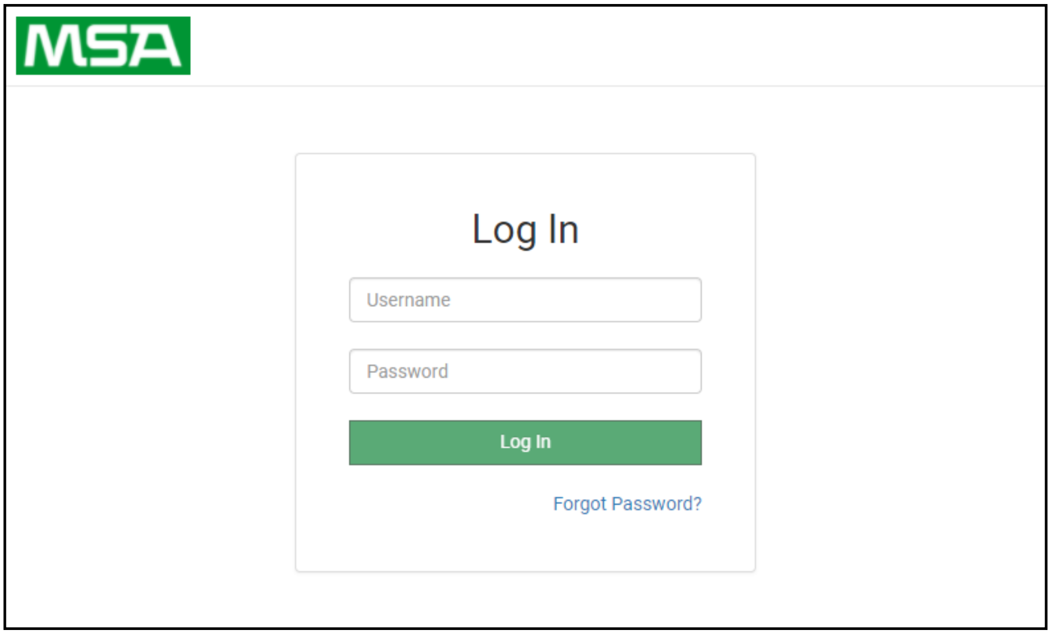
□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is [redacted] its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 10.40.50.94 (unsafe)

- When the login screen appears, put in the Username (default is "admin") and the Password (found on the label of the FieldServer).

NOTE: There is also a QR code in the top right corner of the FieldServer label that shows the default unique password when scanned.

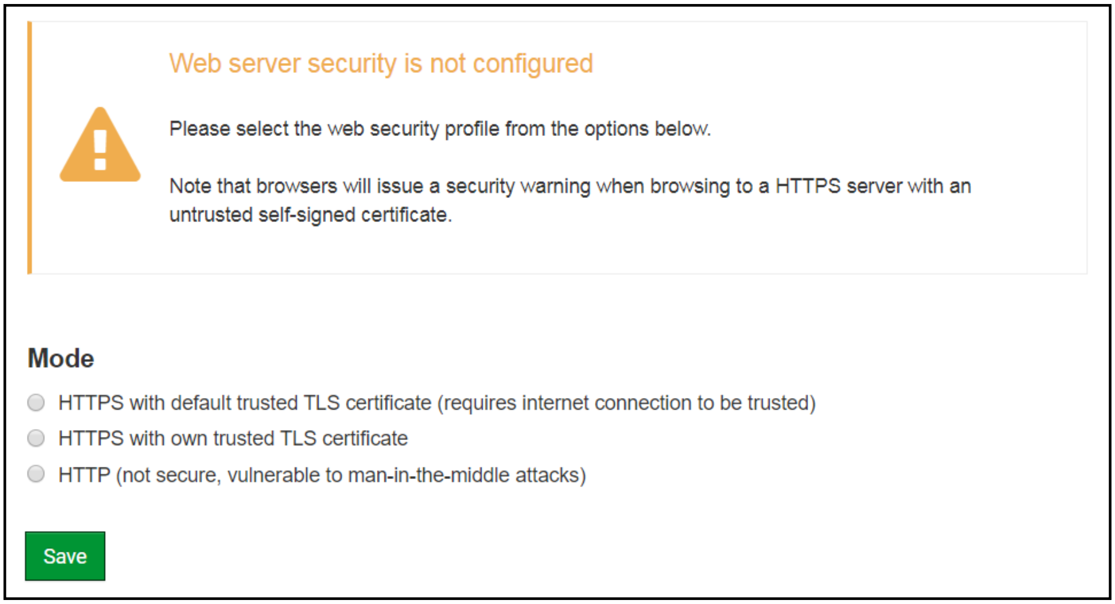


NOTE: A user has 5 attempts to login then there will be a 10-minute lockout. There is no timeout on the FieldServer to enter a password.

2 Select the Security Mode

On the first login to the FieldServer, the following screen will appear that allows the user to select which mode the FieldServer should use.

NOTE: Uses port 443.



Web server security is not configured

Please select the web security profile from the options below.

Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.

Mode

○ HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

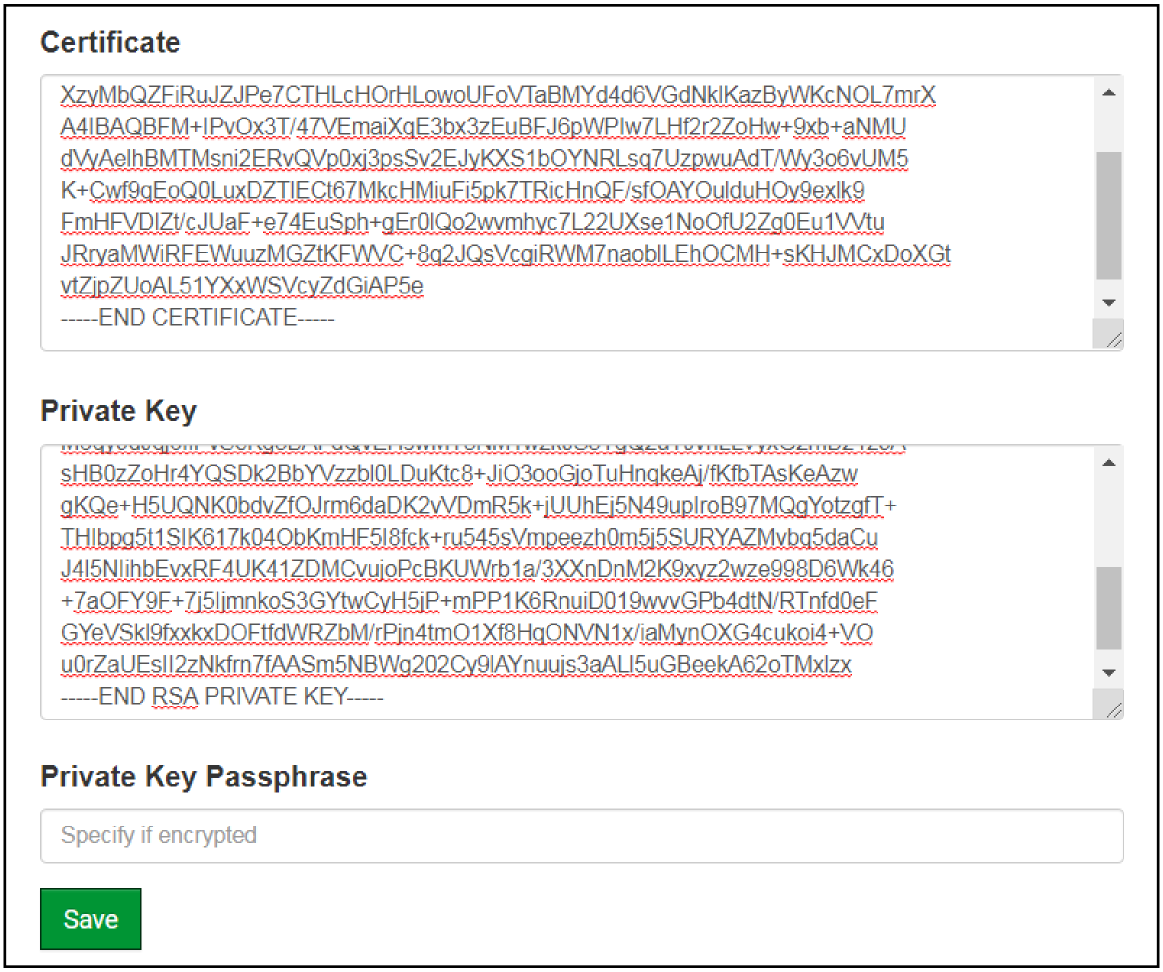
NOTE: Cookies are used for authentication.

NOTE: TLS version 1.3 is supported.

2.1 HTTPS with Own Trusted TLS Certificate

This is the recommended selection and the most secure. **Please contact your IT department to find out if you can obtain a TLS certificate from your company before proceeding with the Own Trusted TLS Certificate option.**

- Once this option is selected, the Certificate, Private Key and Private Key Passphrase fields will appear under the mode selection.



Certificate

```
XzyMbQZFiRuJZJPe7CTHLcHOrHLowoUFoVTaBMYd4d6VGdNkIKazByWKcNOL7mrX
A4IBAQBFM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPIw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTMsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LuxDZTIECt67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exIk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0IQo2wvmhyc7L22UXse1NoOfU2Zg0Eu1VVtu
JRryaMWiRFEWuuzMGZtKFWVC+8q2JQsVcgiRWM7naobILEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

Private Key

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fKfbTAsKeAzw
gKQe+H5UQNK0bdvZfOJrm6daDK2vVDmR5k+jUUhEj5N49upIroB97MQgYotzgfT+
THIbpg5t1SIK617k04ObKmHF5I8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4I5NIihbEvxRF4UK41ZDMCvujoPcBKUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOFY9F+7j5ljmnkoS3GYtwCyH5jP+mPP1K6RnuiD019wvvGPb4dtN/RTnfd0eF
GYeVSkI9fxxkxDOFtfdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9lAYnuujs3aALI5uGBeekA62oTMxIzx
-----END RSA PRIVATE KEY-----
```

Private Key Passphrase

Specify if encrypted

- Copy and paste the Certificate and Private Key text into their respective fields. If the Private Key is encrypted type in the associated Passphrase.
- Click Save.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

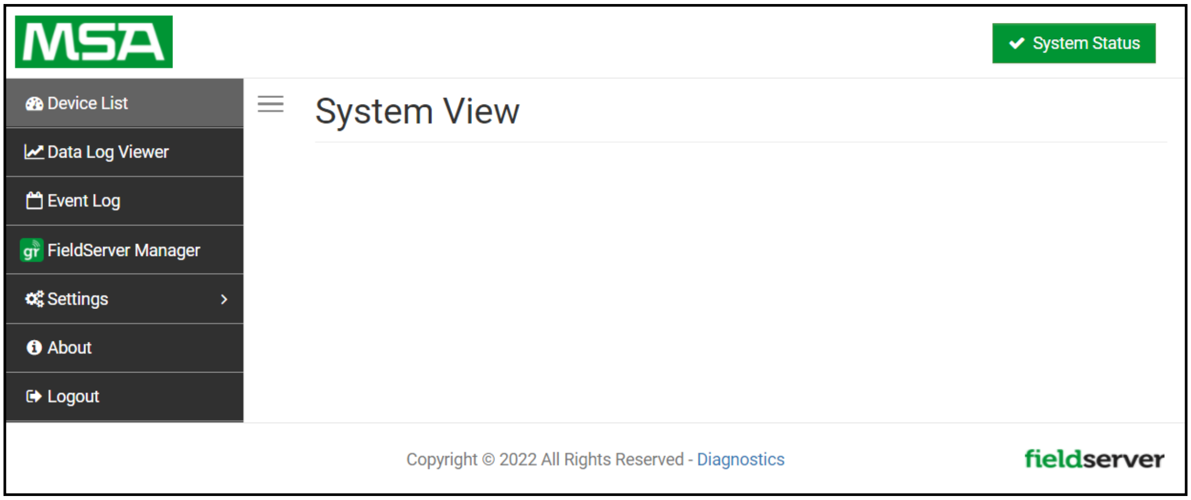
2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

- Select one of these options and click the Save button.
- A “Redirecting” message will appear. After a short time, the FieldServer GUI will open.

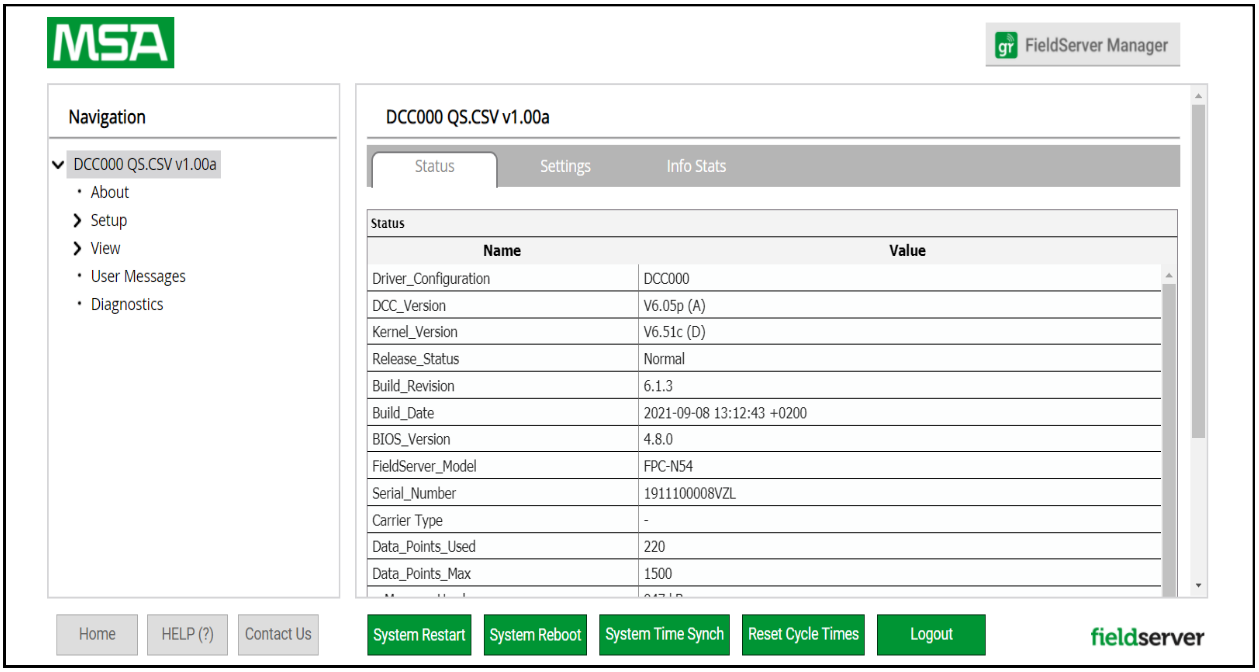
3 Change Web Server Security Settings After Initial Setup

NOTE: Any changes will require a FieldServer reboot to take effect.

- Navigate from the FieldServer landing page to the FS-GUI by clicking the blue “Diagnostics” text on the bottom of the screen.



- Click Setup in the Navigation panel.

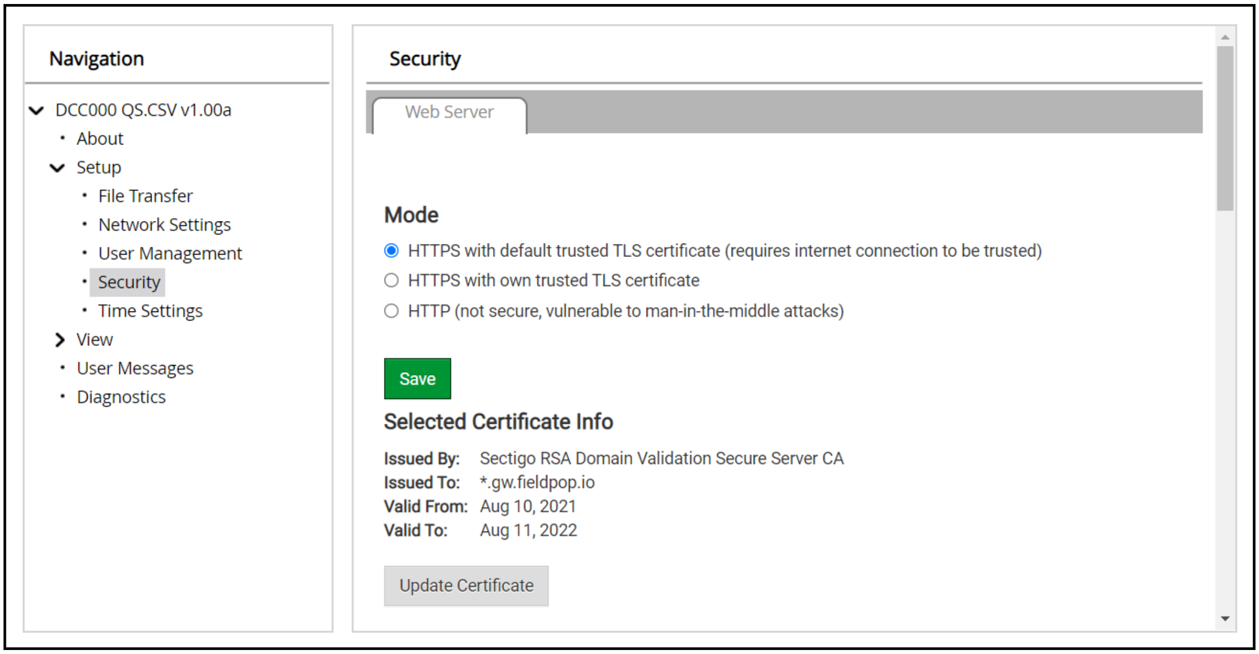


Status

Name	Value
Driver_Configuration	DCC000
DCC_Version	V6.05p (A)
Kernel_Version	V6.51c (D)
Release_Status	Normal
Build_Revision	6.1.3
Build_Date	2021-09-08 13:12:43 +0200
BIOS_Version	4.8.0
FieldServer_Model	FPC-N54
Serial_Number	1911100008VZL
Carrier Type	-
Data_Points_Used	220
Data_Points_Max	1500

3.1 Change Security Mode

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

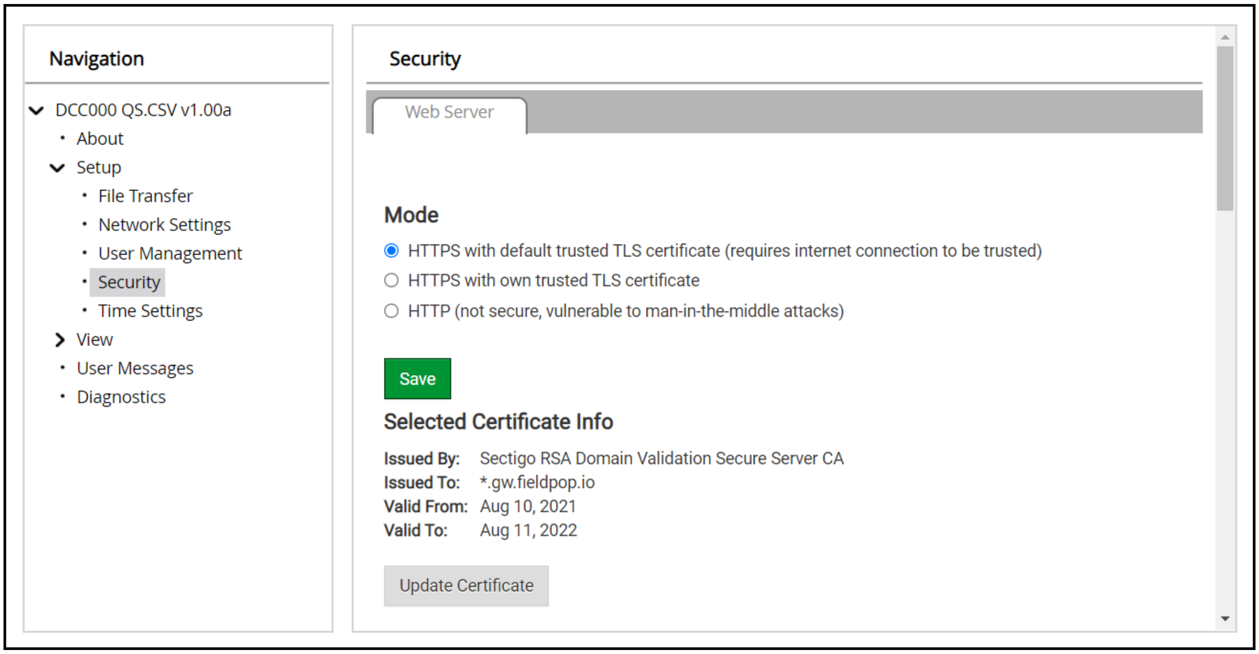
Issued By: Sectigo RSA Domain Validation Secure Server CA
Issued To: *.gw.fieldpop.io
Valid From: Aug 10, 2021
Valid To: Aug 11, 2022

- Click the Mode desired.
    - If HTTPS with own trusted TLS certificate is selected, follow instructions in **Section 2.1 HTTPS with Own Trusted TLS Certificate**
- Click the Save button.

3.2 Edit the Certificate Loaded onto the FieldServer

NOTE: A loaded certificate will only be available if the security mode was previously setup as HTTPS with own trusted TLS certificate.

- Click Security in the Navigation panel.



Mode

● HTTPS with default trusted TLS certificate (requires internet connection to be trusted)

○ HTTPS with own trusted TLS certificate

○ HTTP (not secure, vulnerable to man-in-the-middle attacks)

Selected Certificate Info

Issued By: Sectigo RSA Domain Validation Secure Server CA
Issued To: *.gw.fieldpop.io
Valid From: Aug 10, 2021
Valid To: Aug 11, 2022

- Click the Edit Certificate button to open the certificate and key fields.
- Edit the loaded certificate or key text as needed.
- Click Save.

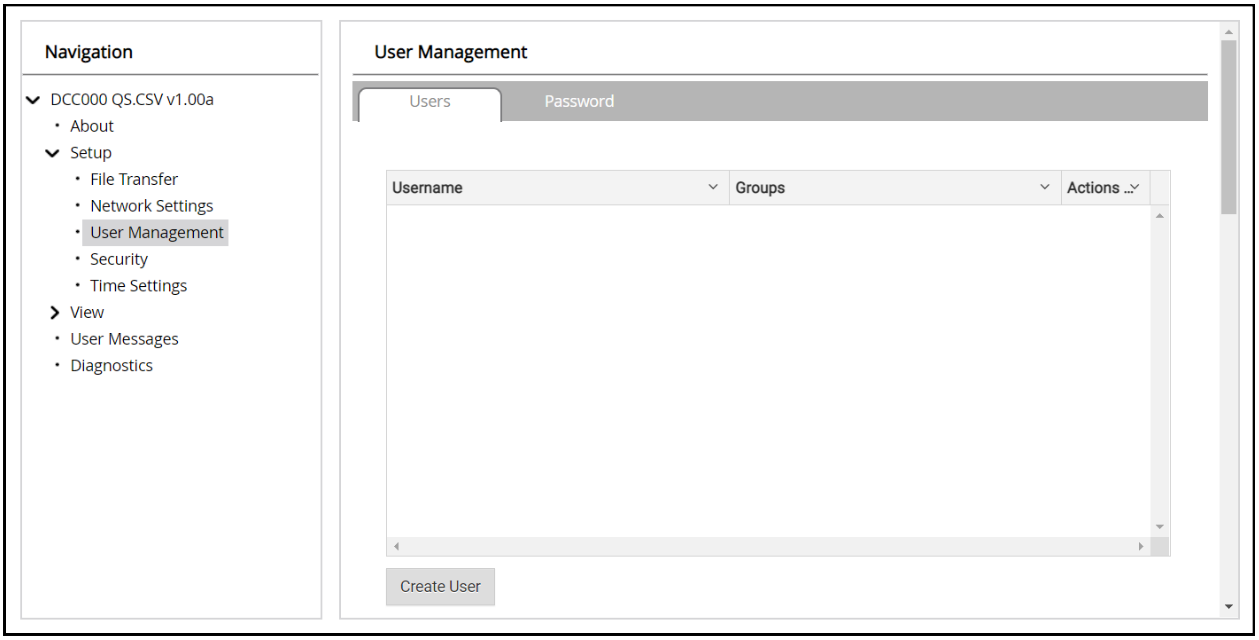
3.3 Change User Management Settings

- From the FS-GUI page, click Setup in the Navigation panel.
- Click User Management in the navigation panel.

NOTE: If the passwords are lost, the unit can be reset to factory settings to reinstate the default unique password on the label. For ProtoNode, ProtoCessor or ProtoCarrier recovery instructions, see the FieldServer Recovery Instructions document. For ProtoNode FPC-N54, ProtoNode FPC-N64 or ProtoAir recovery instructions, see the FieldServer Next Gen Recovery document. If the default unique password is lost, then the unit must be mailed back to the factory.

NOTE: Any changes will require a FieldServer reboot to take effect.

- Check that the Users tab is selected.



User Types:

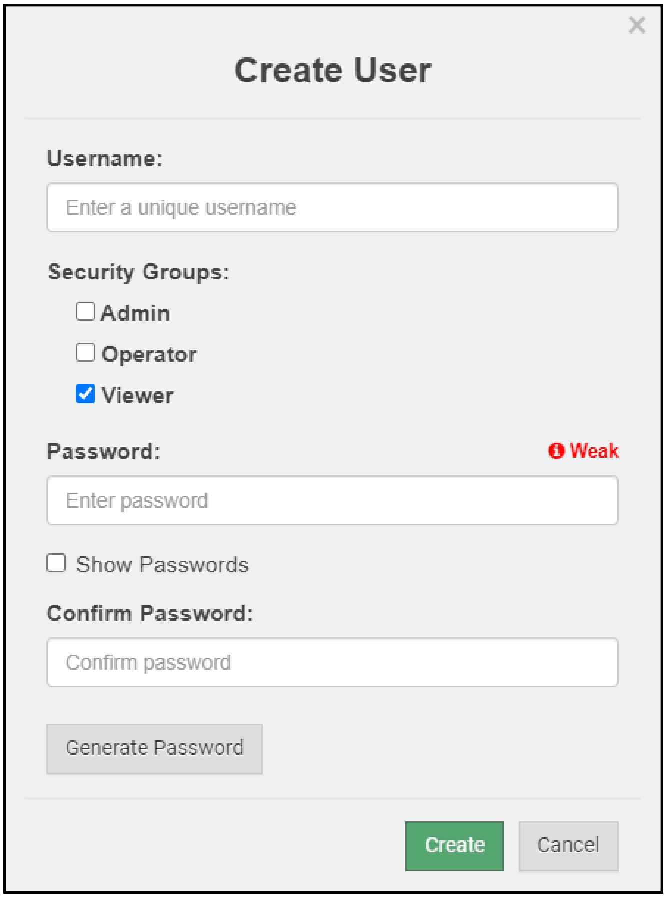
Admin – Can modify and view any settings on the FieldServer.

Operator – Can modify and view any data in the FieldServer array(s).

Viewer – Can only view settings/readings on the FieldServer.

3.3.1 Create Users

- Click the Create User button.



Create User

Username:

Enter a unique username

Security Groups:

□ Admin

□ Operator

☑ Viewer

Password: Weak

Enter password

□ Show Passwords

Confirm Password:

Confirm password

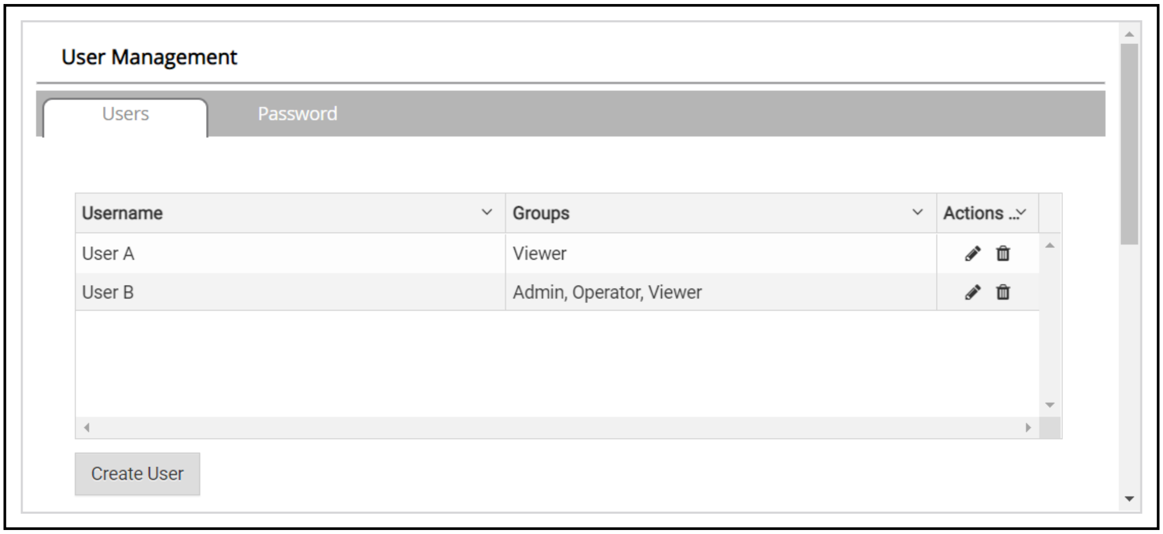
- Enter the new User fields: Name, Security Group and Password.
    - **User details are hashed and salted**

NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.

- Click the Create button.
- Once the Success message appears, click OK.

3.3.2 Edit Users

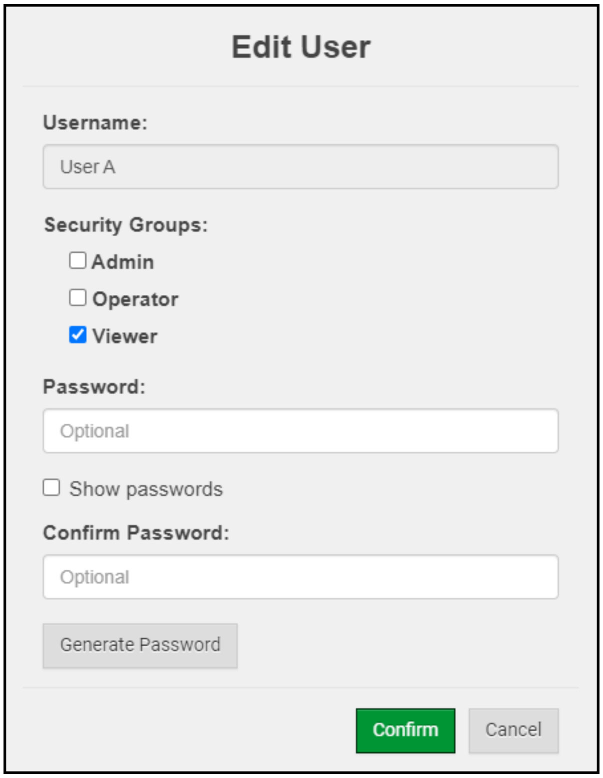
- Click the pencil icon next to the desired user to open the User Edit window.



User Management

Username	Groups	Actions
User A	Viewer	✎ 🗑
User B	Admin, Operator, Viewer	✎ 🗑

- Once the User Edit window opens, change the User Security Group and Password as needed.



Edit User

Username: User A

Security Groups:

☐ Admin

☐ Operator

☑ Viewer

Password: Optional

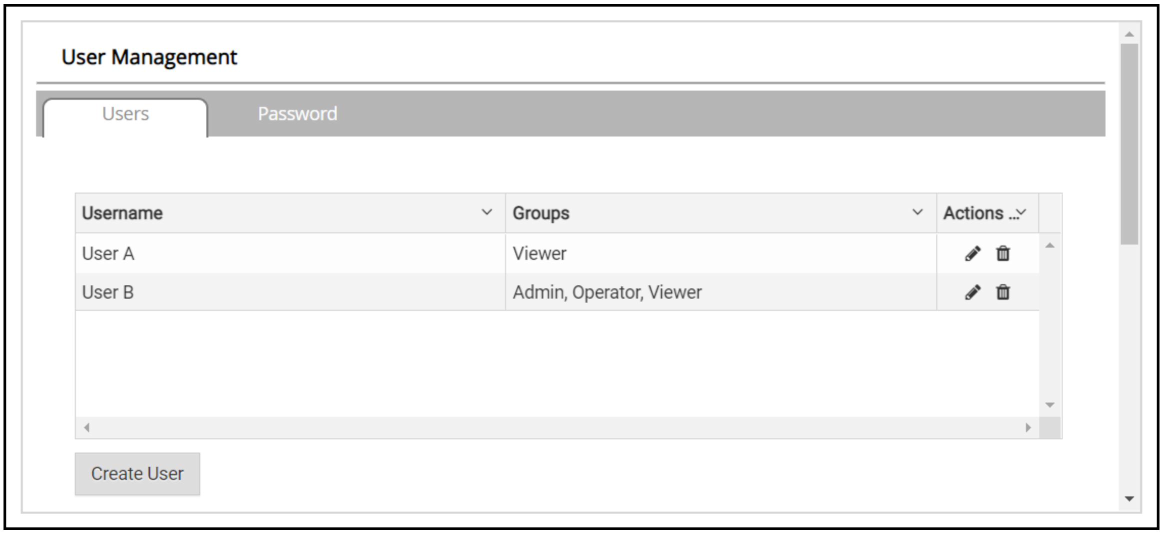
☐ Show passwords

Confirm Password: Optional

- Click Confirm.
- Once the Success message appears, click OK.

3.3.3 Delete Users

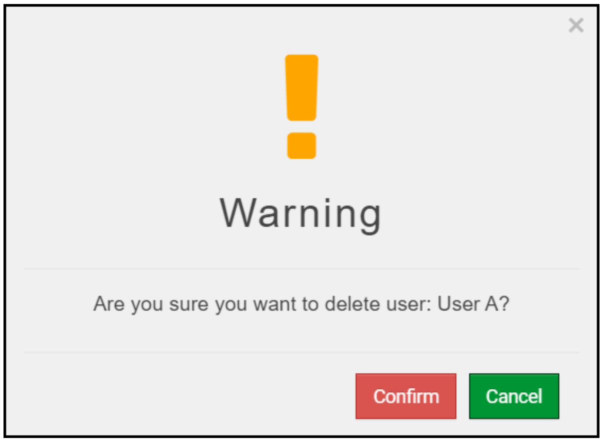
- Click the trash can icon next to the desired user to delete the entry.



User Management

Username	Groups	Actions ...
User A	Viewer	✎ 🗑
User B	Admin, Operator, Viewer	✎ 🗑

- When the warning message appears, click Confirm.

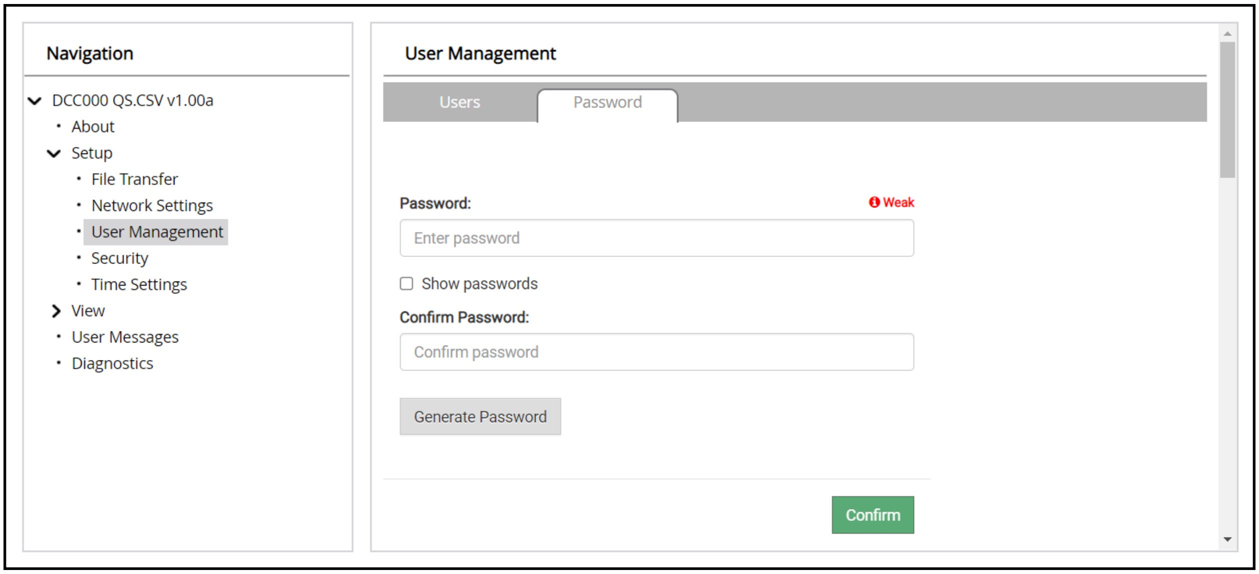


Warning

Are you sure you want to delete user: User A?

3.3.4 Change FieldServer Password

- Click the Password tab.



- Change the general login password for the FieldServer as needed.

NOTE: The password must meet the minimum complexity requirements. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.