



## **FieldServer ENOTE**

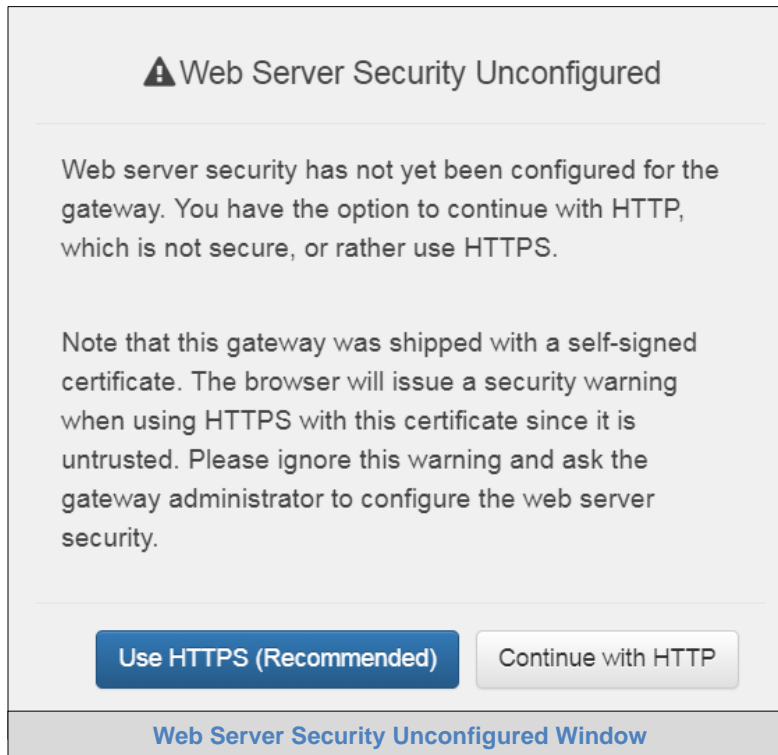
### **FieldSafe Secure FieldServer Web Server Setup and User Management Instructions**

Document Revision: 1.E  
Date: 6/20  
T18025

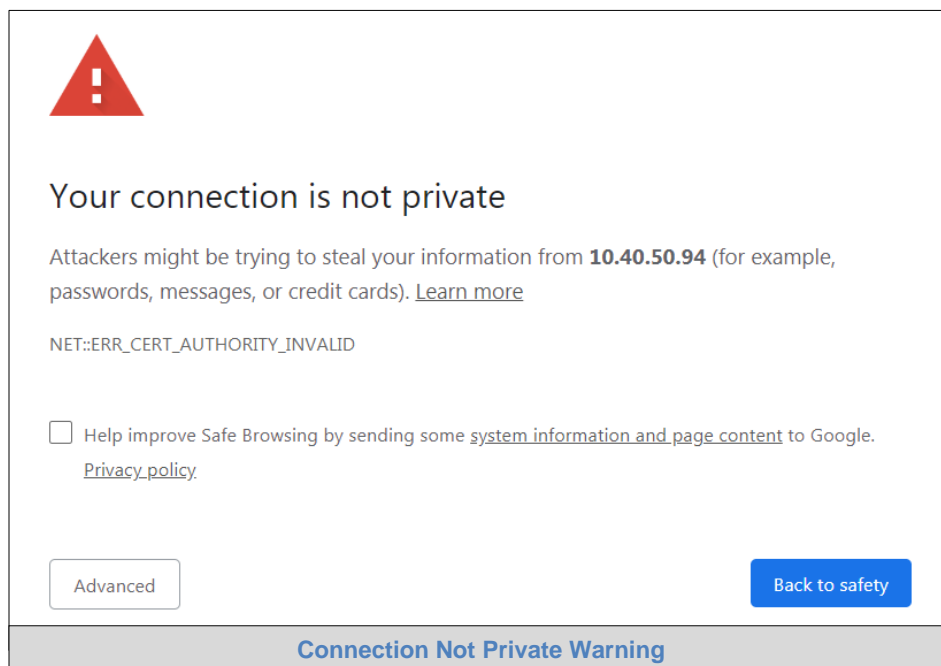
## 1 LOGIN TO THE FIELD SERVER

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.

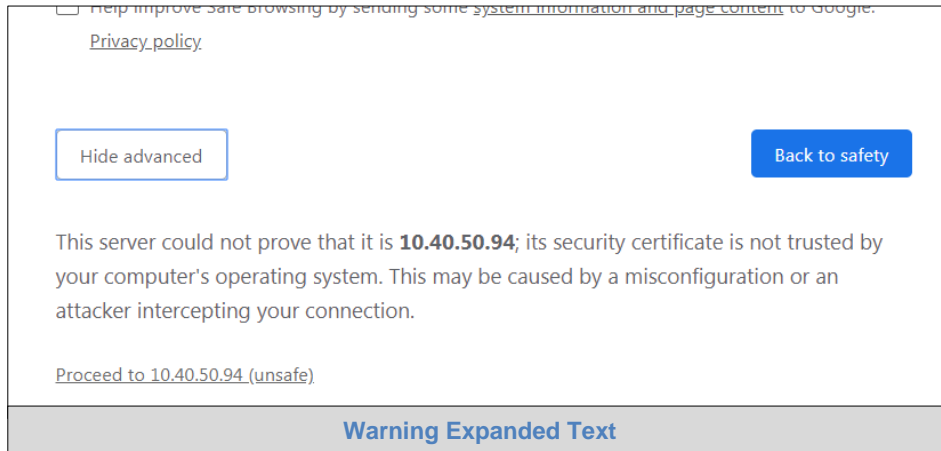
- When the Web Server Security Unconfigured window appears, read the text and choose whether to move forward with HTTPS or HTTP.



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

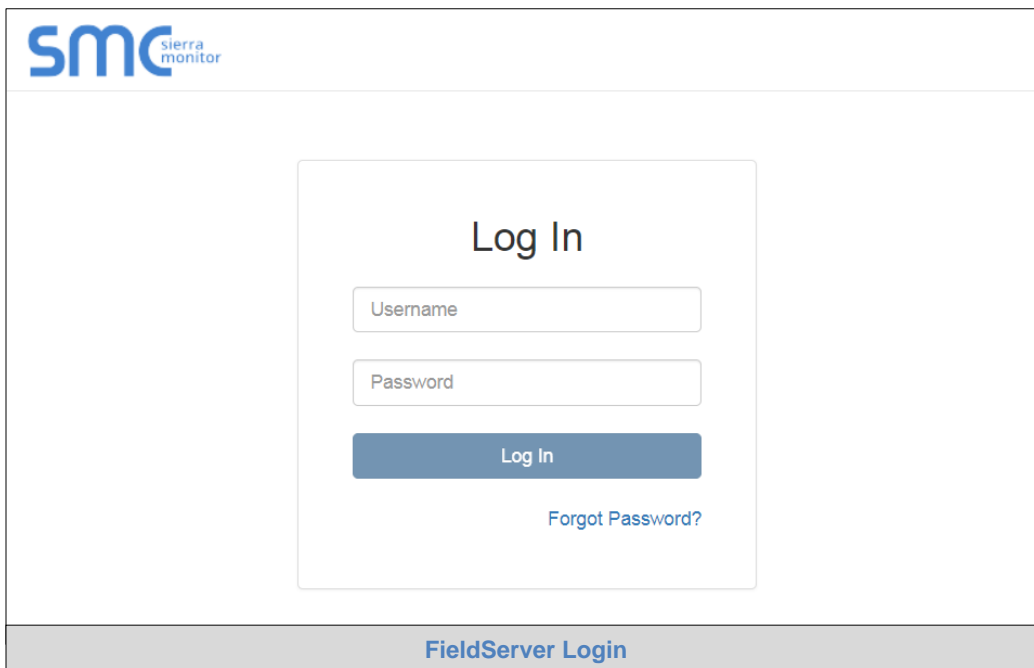


- Additional text will expand below the warning, click the underlined text “[Proceed to 10.40.50.94 \(unsafe\)](#)”.



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

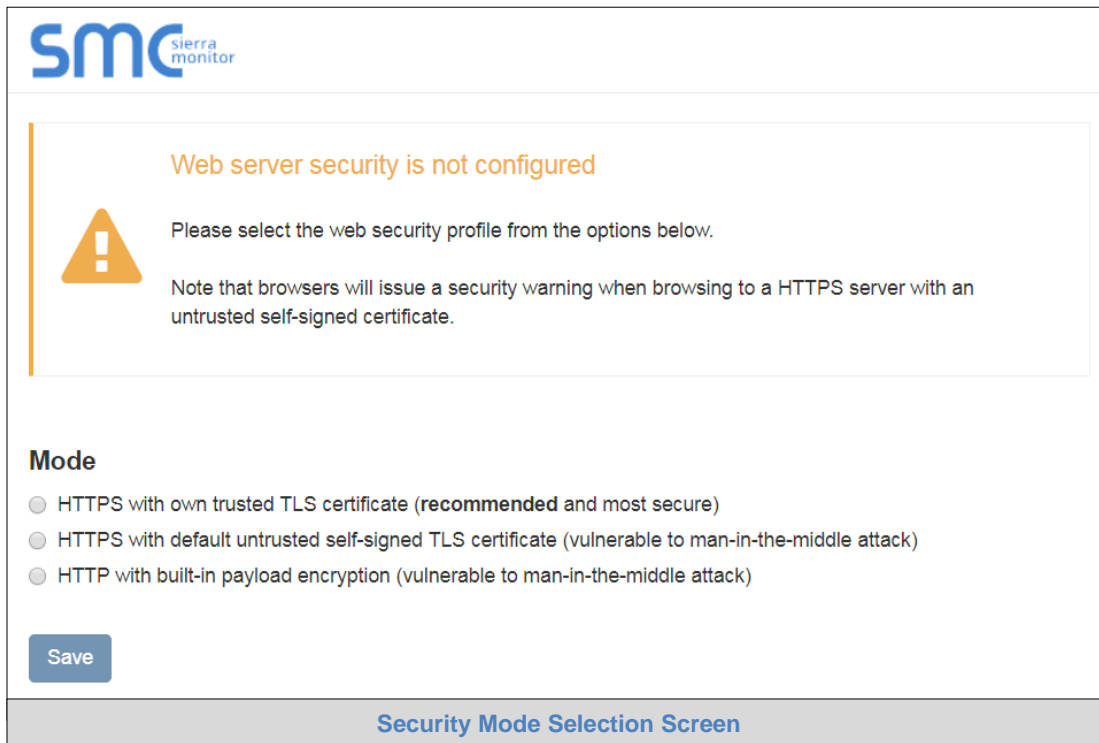
**NOTE:** There is also a QR code in the top right corner of the FieldServer label that shows the default unique password when scanned.



**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.



The screenshot shows the 'Security Mode Selection Screen' in the FieldServer interface. At the top left is the 'smc sierra monitor' logo. A central warning box contains a yellow triangle with an exclamation mark, the text 'Web server security is not configured', and instructions: 'Please select the web security profile from the options below.' and 'Note that browsers will issue a security warning when browsing to a HTTPS server with an untrusted self-signed certificate.' Below this, under the heading 'Mode', are three radio button options: 'HTTPS with own trusted TLS certificate (recommended and most secure)', 'HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)', and 'HTTP with built-in payload encryption (vulnerable to man-in-the-middle attack)'. A blue 'Save' button is located at the bottom left of the form area. The footer of the screen is a grey bar with the text 'Security Mode Selection Screen'.

**NOTE: Cookies are used for authentication.**

## 2.1 HTTPS with Own Trusted TLS Certificate

This is the recommended selection and the most secure.

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

**Mode**

HTTPS with own trusted TLS certificate (**recommended** and most secure)  
 HTTPS with default untrusted self-signed TLS certificate (vulnerable to man-in-the-middle attack)  
 HTTP with built-in payload encryption (vulnerable to man-in-the-middle attack)

**Certificate**

```
XzyMbQZFIRuJZJPe7CTHLcHORHLowoUFoVtaBMYd4d6VGdNklKazByWKcNOL7mrX
A4lBAQBfM+IPvOx3T/47VEmaiXqE3bx3zEuBFJ6pWPlw7LHf2r2ZoHw+9xb+aNMU
dVyAelhBMTmsni2ERvQVp0xj3psSv2EJyKXS1bOYNRLsq7UzpwuAdT/Wy3o6vUM5
K+Cwf9qEoQ0LUXDZTIEct67MkcHMiuFi5pk7TRicHnQF/sfOAYOulduHOy9exlk9
FmHFVDIZt/cJUaF+e74EuSph+gEr0IQo2wvmhyc7L22UXse1NoOfU2Zq0Eu1VVtu
JRryaMMwIRFEWuuzMGZtKFWVC+8q2JQsVcqiRWM7naoblLEhOCMH+sKHJMCxDoXGt
vtZjpZUoAL51YXxWSVcyZdGiAP5e
-----END CERTIFICATE-----
```

**Private Key**

```
sHB0zZoHr4YQSDk2BbYVzzbl0LDuKtc8+JiO3ooGjoTuHnqkeAj/fkfbTAsKeAzw
gKQe+H5UQNk0bdvZfOJrm6daDK2vVDmR5k+juUUhEj5N49upIroB97MQgYotzqfT+
THlbpq5t1SIK617k04ObKmHF5l8fck+ru545sVmpeezh0m5j5SURYAZMvbq5daCu
J4l5NlihbEvxRF4UK41ZDMCvujopCbkUWrb1a/3XXnDnM2K9xyz2wze998D6Wk46
+7aOfY9F+7j5ljmkoS3GYtwCyH5jP+mPP1K6RnuiD019wvGPb4dtN/RTnfd0eF
GYeVSkI9fxkxDOFtdWRZbM/rPjn4tmO1Xf8HqONVN1x/iaMynOXG4cukoi4+VO
u0rZaUEsII2zNkfrn7fAASm5NBWg202Cy9IAYnuujs3aAlI5uGBeekA62oTMxlzx
-----END RSA PRIVATE KEY-----
```

**Private Key Passphrase**

Specify if encrypted

Security Mode Selection Screen

- 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 and after a short period of time the FieldServer GUI will open.

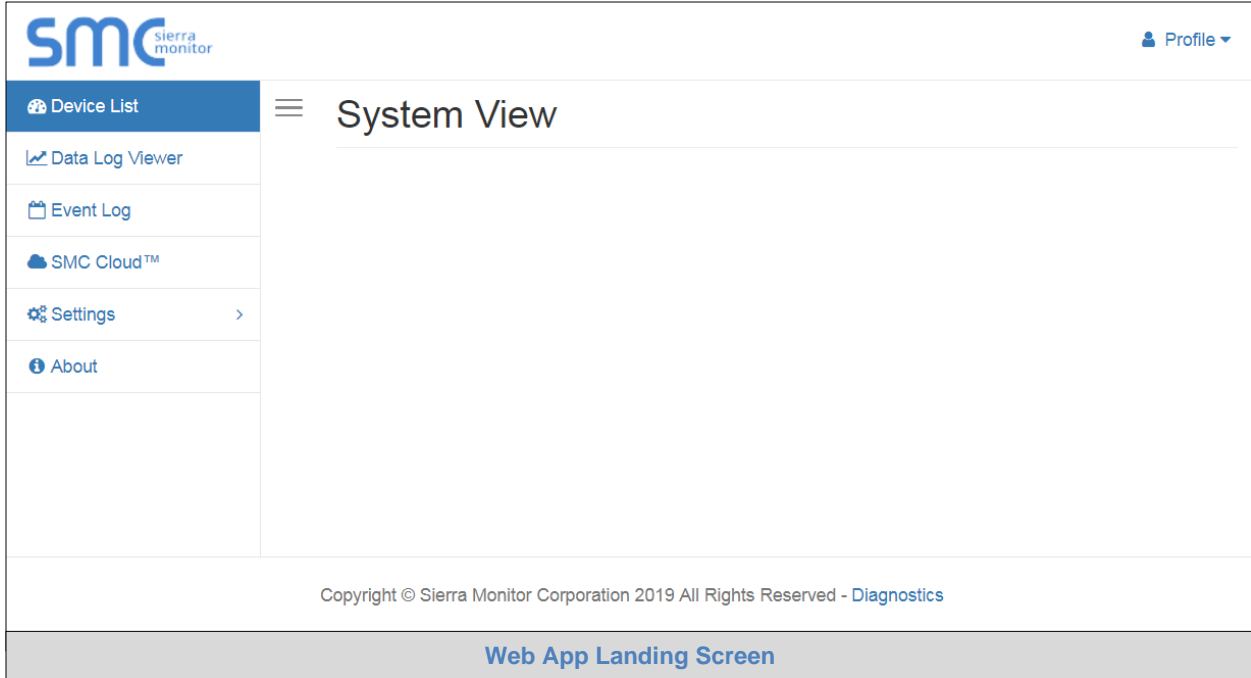
## 2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

- Simply select one of these options and click the Save button.
- A “Redirecting” message will appear and after a short period of time the FieldServer GUI will open.

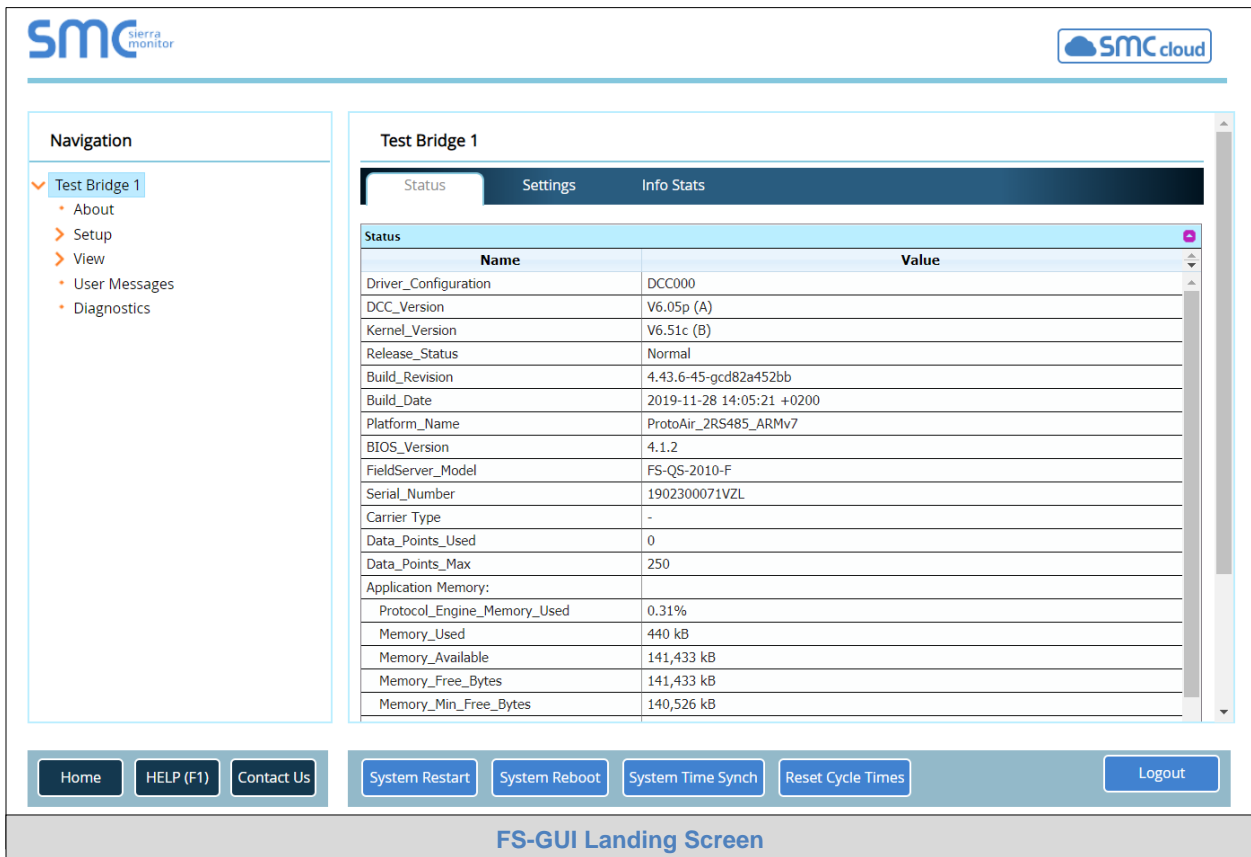
### 3 CHANGE SETTINGS AFTER INITIAL SETUP

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

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



- Click Setup in the Navigation panel.



### 3.1 Change Security Mode

- Click Security in the Navigation panel.



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

The screenshot shows the SMC GUI interface for editing a certificate. The navigation panel on the left includes 'Test Bridge 1', 'Setup', and 'View'. The 'Security' section is active, showing the 'Web Server' tab. The 'Mode' section has three radio buttons, with the first one selected. The 'Certificate Loaded' section displays the following information:

Issuer:	Internet Widgits Pty Ltd
Subject:	Internet Widgits Pty Ltd
Valid From:	2019-11-25T13:52:29.000Z
Valid To:	2019-12-25T13:52:29.000Z

At the bottom of the certificate details, there are two buttons: 'Edit Certificate' and 'Save'.

- 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

- 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 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.

#### 3.3.1 User Management

- Check that the Users tab is selected.

The screenshot displays the SMC GUI User Management interface. On the left is a navigation panel with a tree view under 'Test Bridge 1', including 'About', 'Setup' (with sub-items: File Transfer, Network Settings, User Management, Security, Time Settings), 'View', 'User Messages', and 'Diagnostics'. The 'User Management' section is active. The main content area has two tabs: 'Users' (selected) and 'Password'. Below the tabs is a table with columns for 'Username', 'Groups', and 'Actions'. A 'Create User' button is located at the bottom of the table area. The footer contains 'Home', 'HELP (F1)', 'Contact Us', and 'Logout' buttons. The title 'FS-GUI User Management' is centered at the bottom.

User Types:

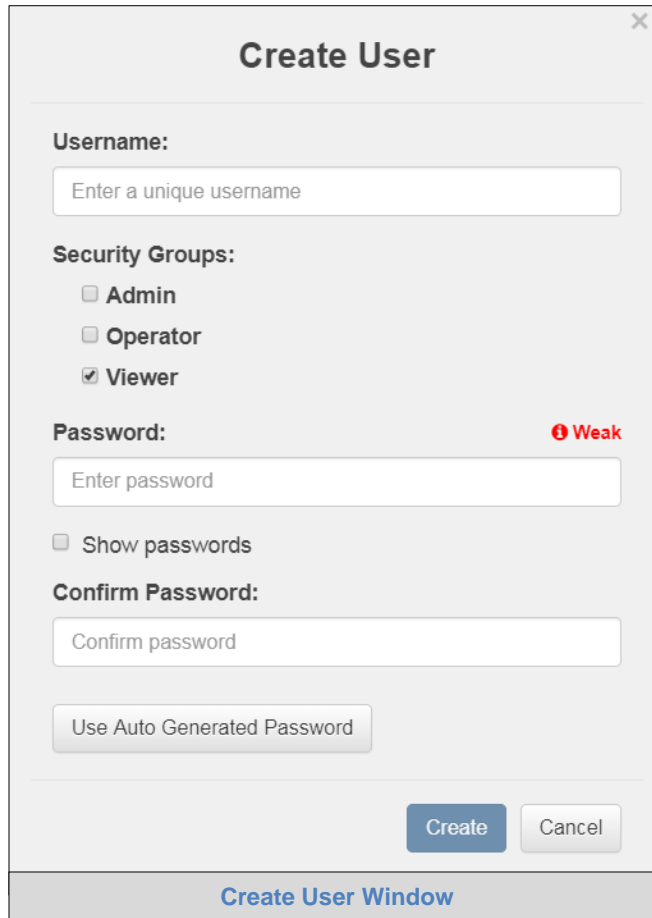
**Admin** – Can modify and view any settings on the FieldServer.

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

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

**Create Users**

- Click the Create User button.



**Create User**

**Username:**

**Security Groups:**

- Admin
- Operator
- Viewer

**Password:** Weak

Show passwords

**Confirm Password:**

Create User Window

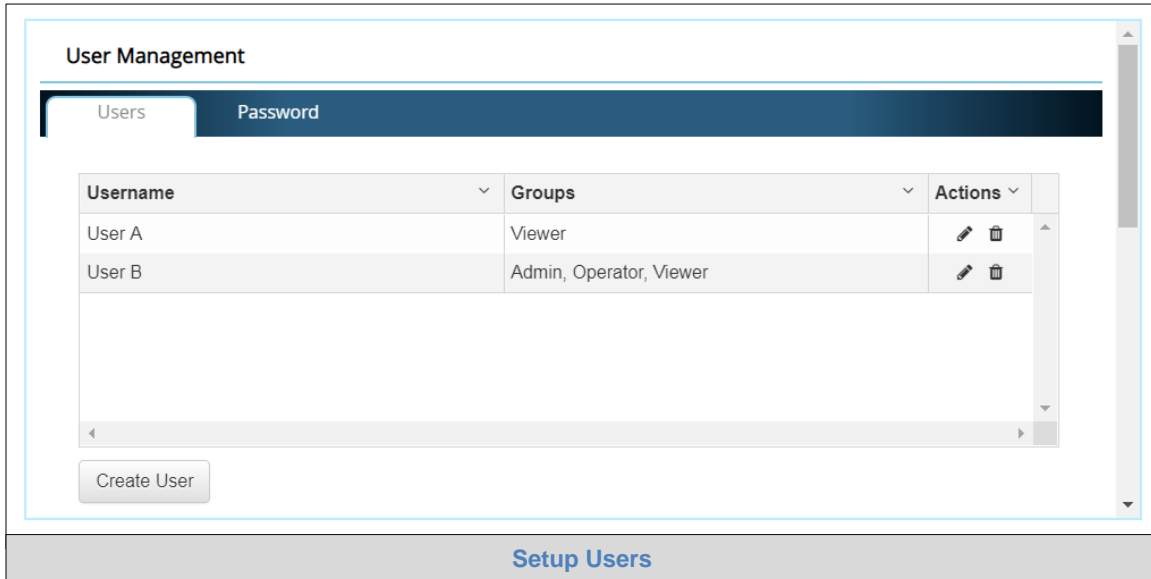
- Enter the new User fields: Name, Security Group and Password.

**NOTE: Passwords must be at least 10 characters long. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.**

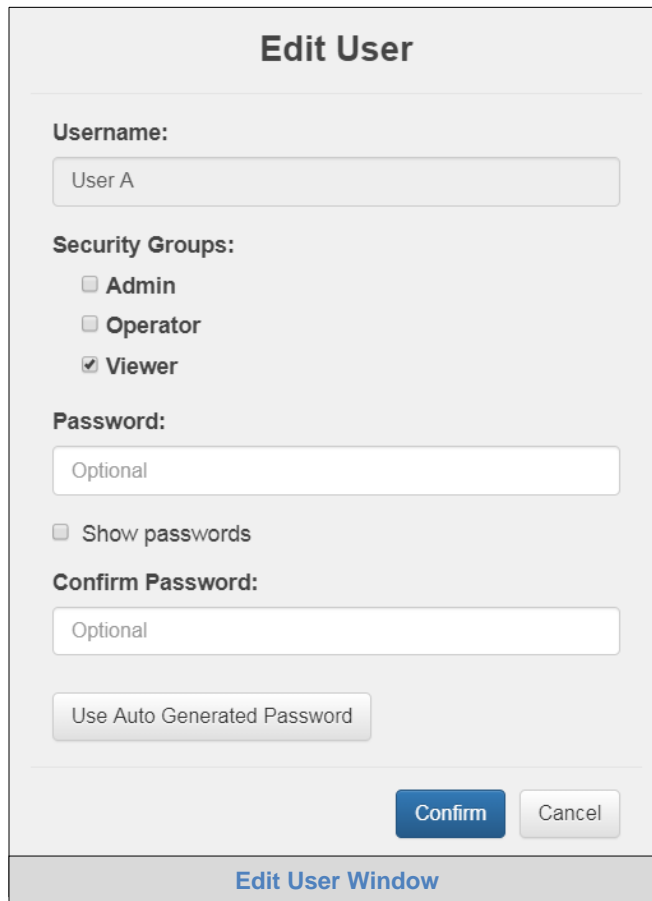
- **User details are hashed and salted.**
- Click the Create button.
- Once the Success message appears, click OK.

3.3.1.1 Edit Users

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



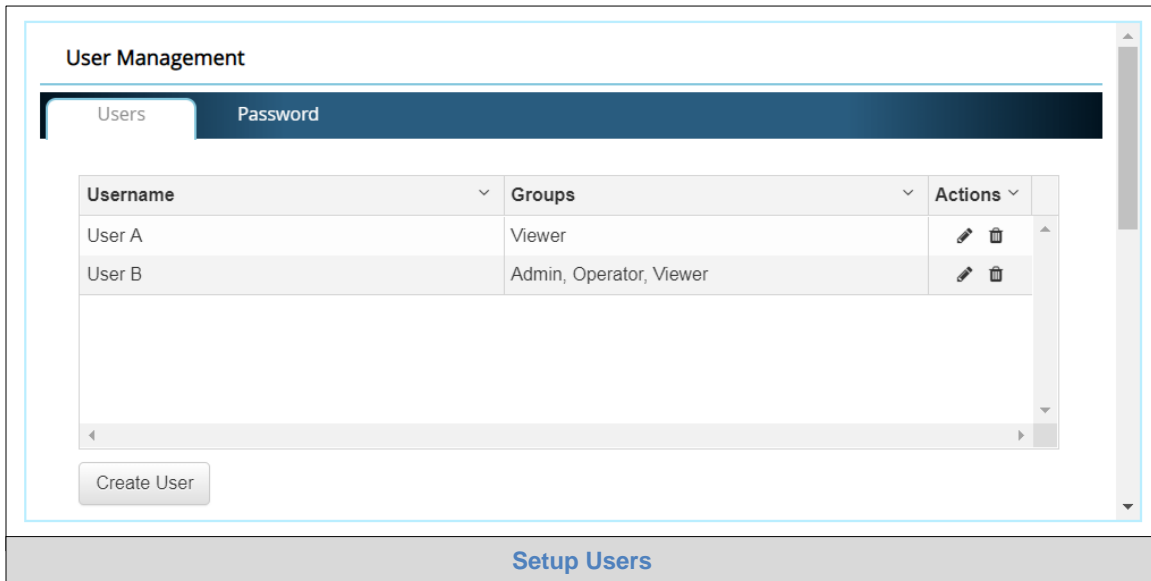
- Once the User Edit window opens, change the User Security Group and Password as needed.



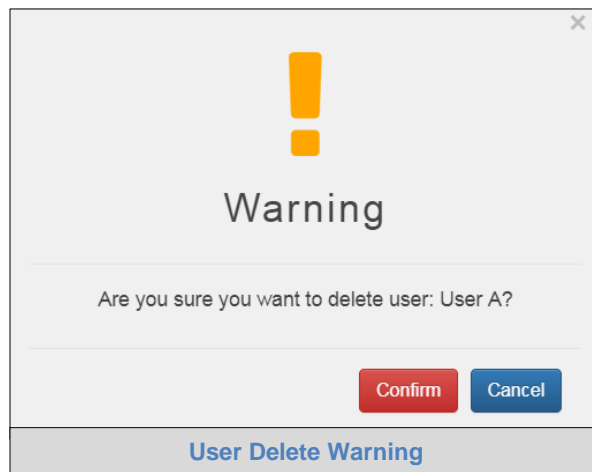
- Click Confirm.
- Once the Success message appears, click OK.

3.3.1.2 Delete Users

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

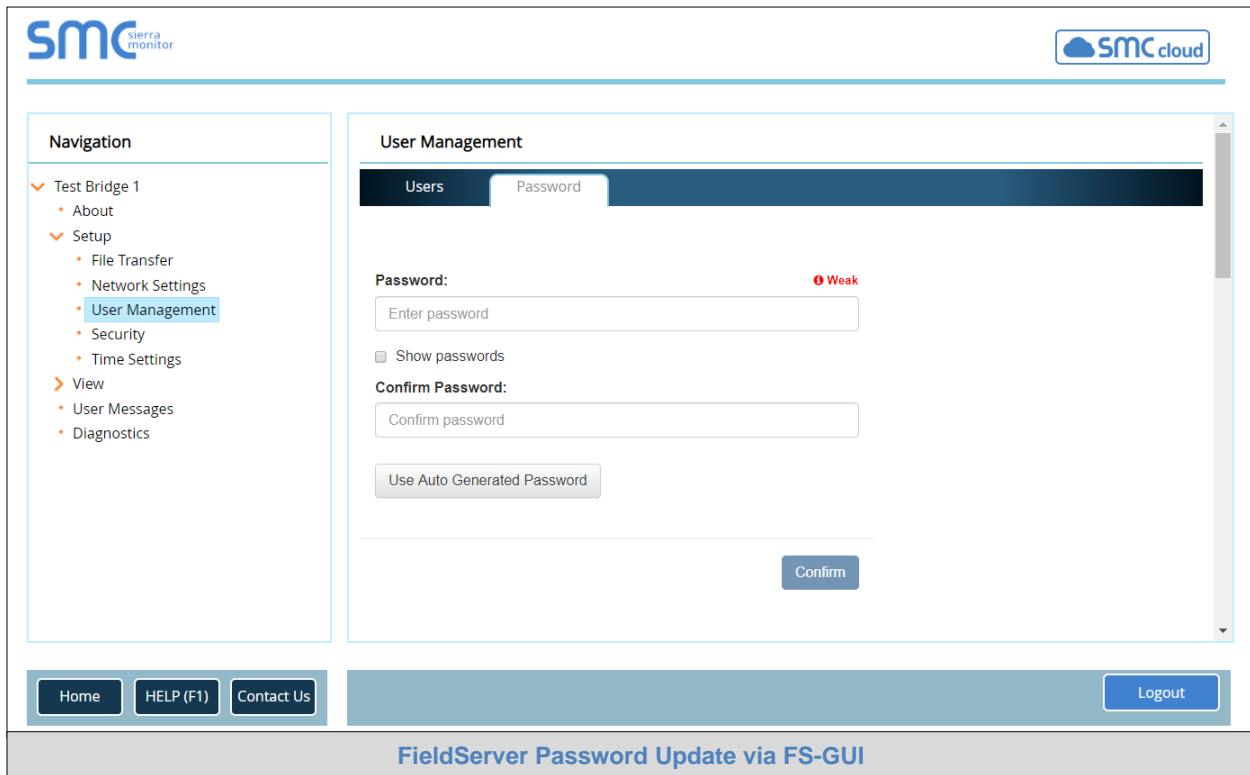


- When the warning message appears, click Confirm.



### 3.3.2 Change FieldServer Password

- Click the Password tab.



- Change the login password for the FieldServer as needed.

**NOTE: Passwords must be at least 10 characters long. An algorithm automatically checks the password entered and notes the level of strength on the top right of the Password text field.**

---

## Technical Support

Thank you for purchasing the FieldServer from MSA Safety.

Please call us for any technical support needs related to the FieldServer product.

MSA Safety  
1991 Tarob Court  
Milpitas, CA 95035

Website: [www.sierramonitor.com](http://www.sierramonitor.com)

U.S. Support Information:

+1 408 964-4443

+1 800 727-4377

Email: [smc-support@msasafety.com](mailto:smc-support@msasafety.com)

EMEA Support Information:

+31 33 808 0590

Email: [smc-support.emea@msasafety.com](mailto:smc-support.emea@msasafety.com)