FieldServer ENOTE

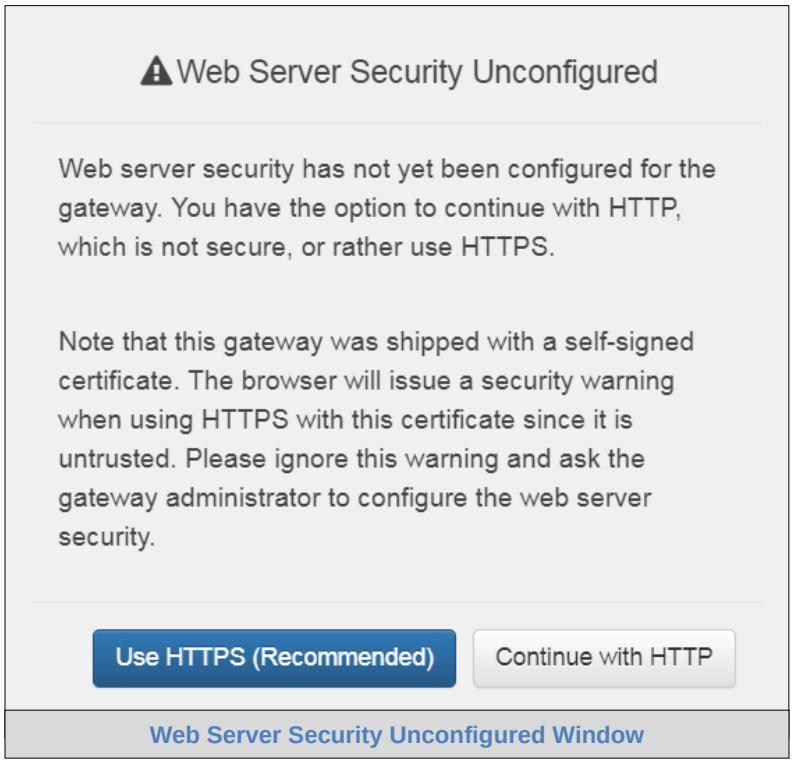
FieldSafe Secure FieldServer
Web Server Setup and
User Management Instructions

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

1 LOGIN TO THE FIELDSERVER

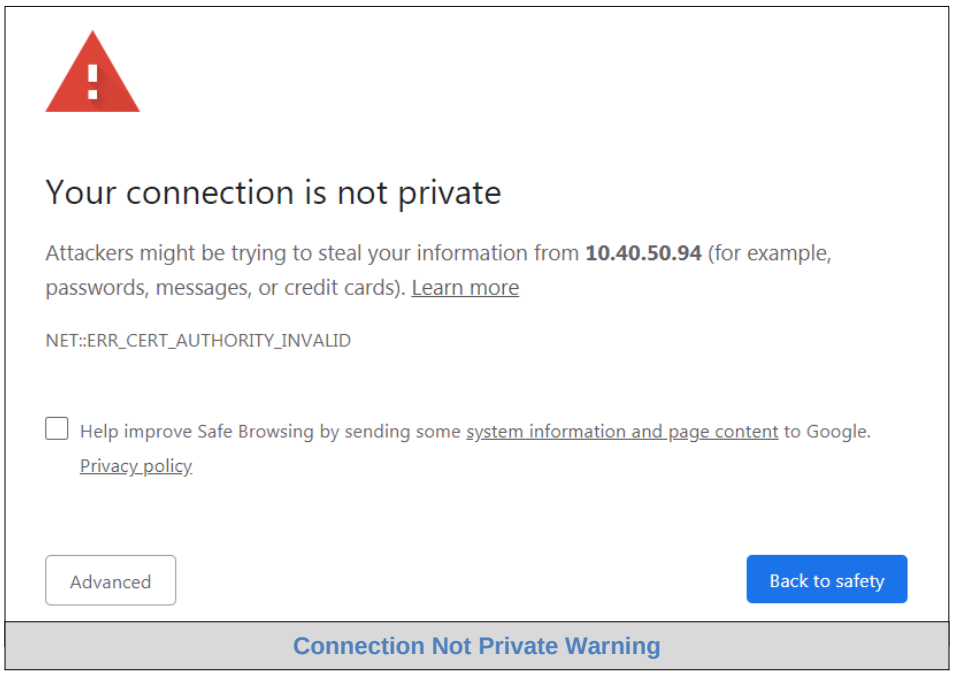
The first time the FieldServer GUI is opened in a browser, the IP Address for the gateway will appear as untrusted. This will cause the following pop-up windows to appear.

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



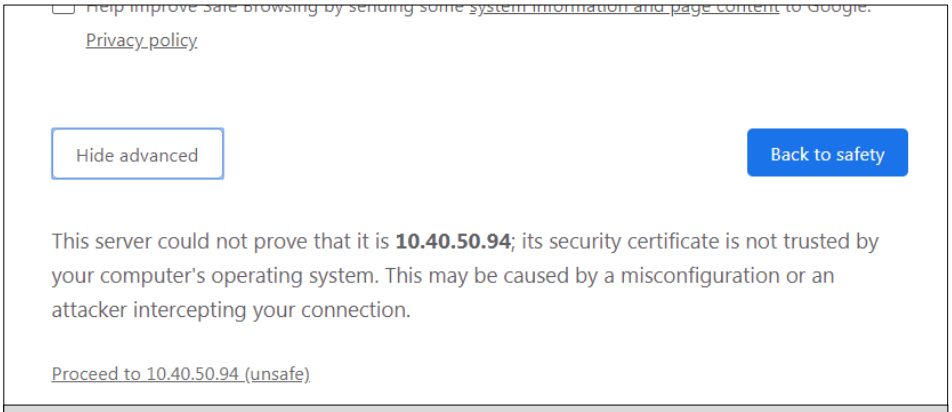
Web Server Security Unconfigured Window

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



Connection Not Private Warning

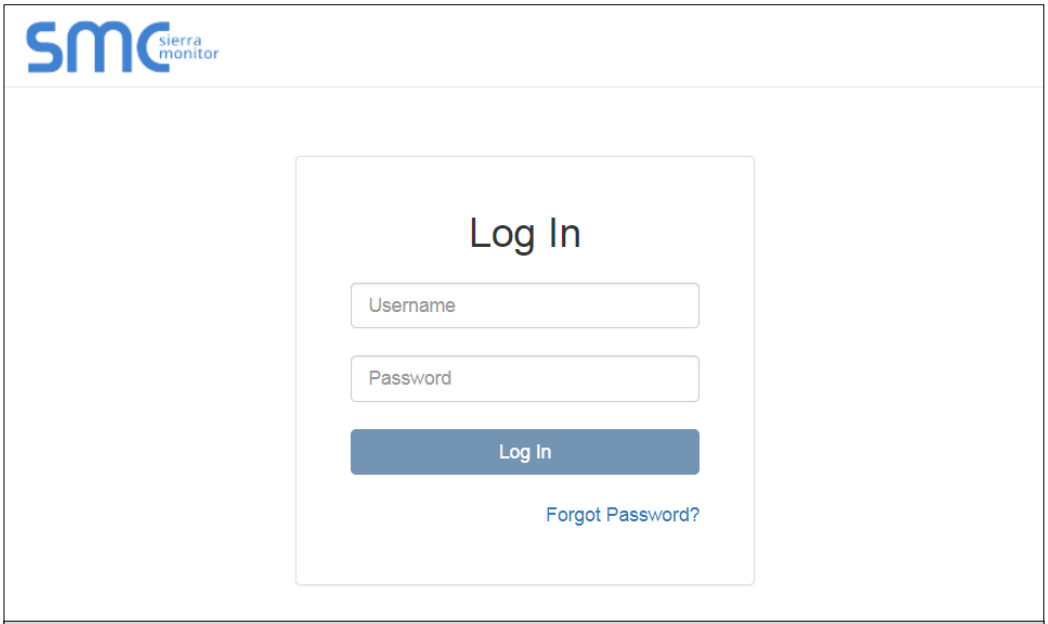
- Additional text will expand below the warning, click the underlined text "Proceed to 10.40.50.94 (unsafe)".



Warning Expanded Text

- 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.

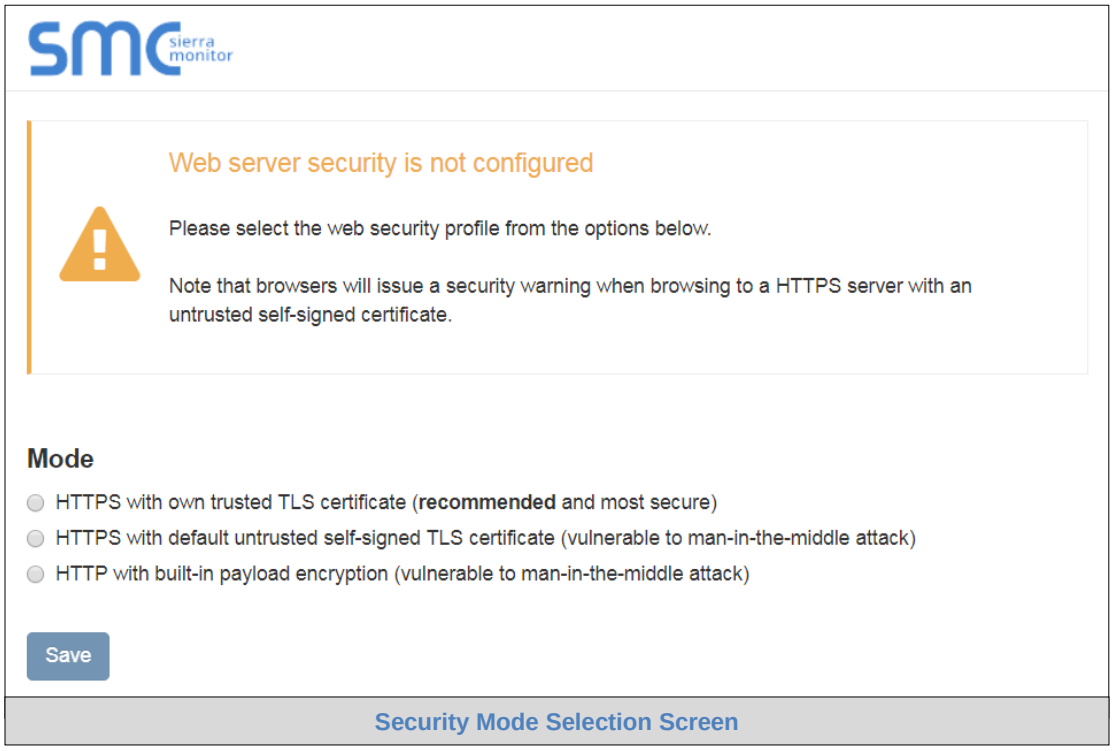


FieldServer Login

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.



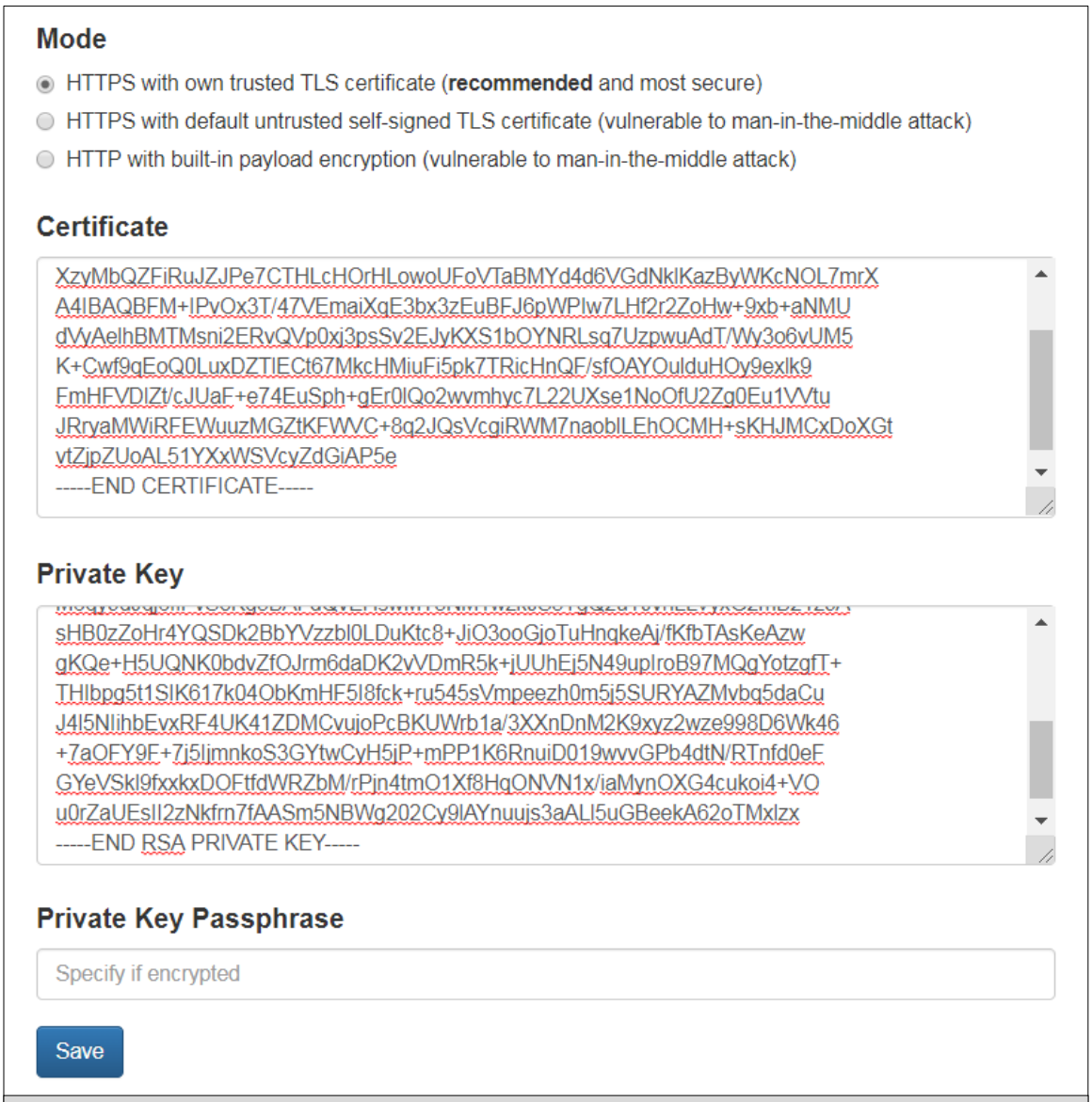
Security Mode Selection Screen

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.



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.

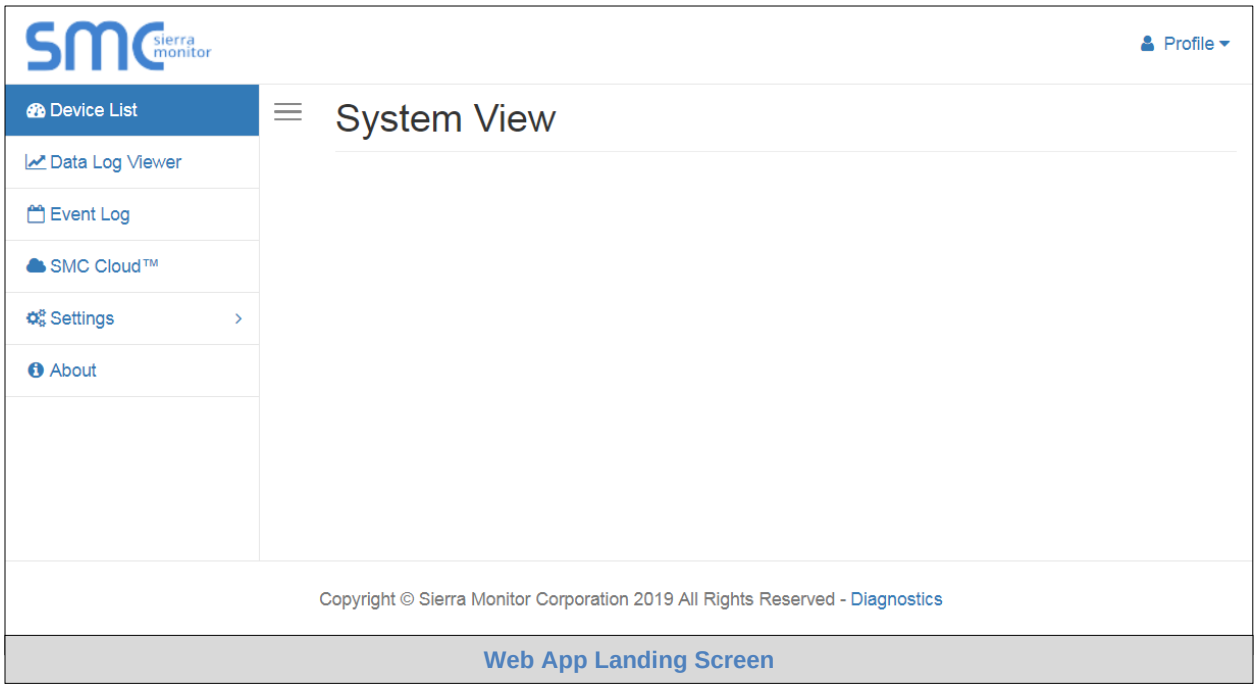
2.2 HTTPS with Default Untrusted Self-Signed TLS Certificate or HTTP with Built-in Payload Encryption

- 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

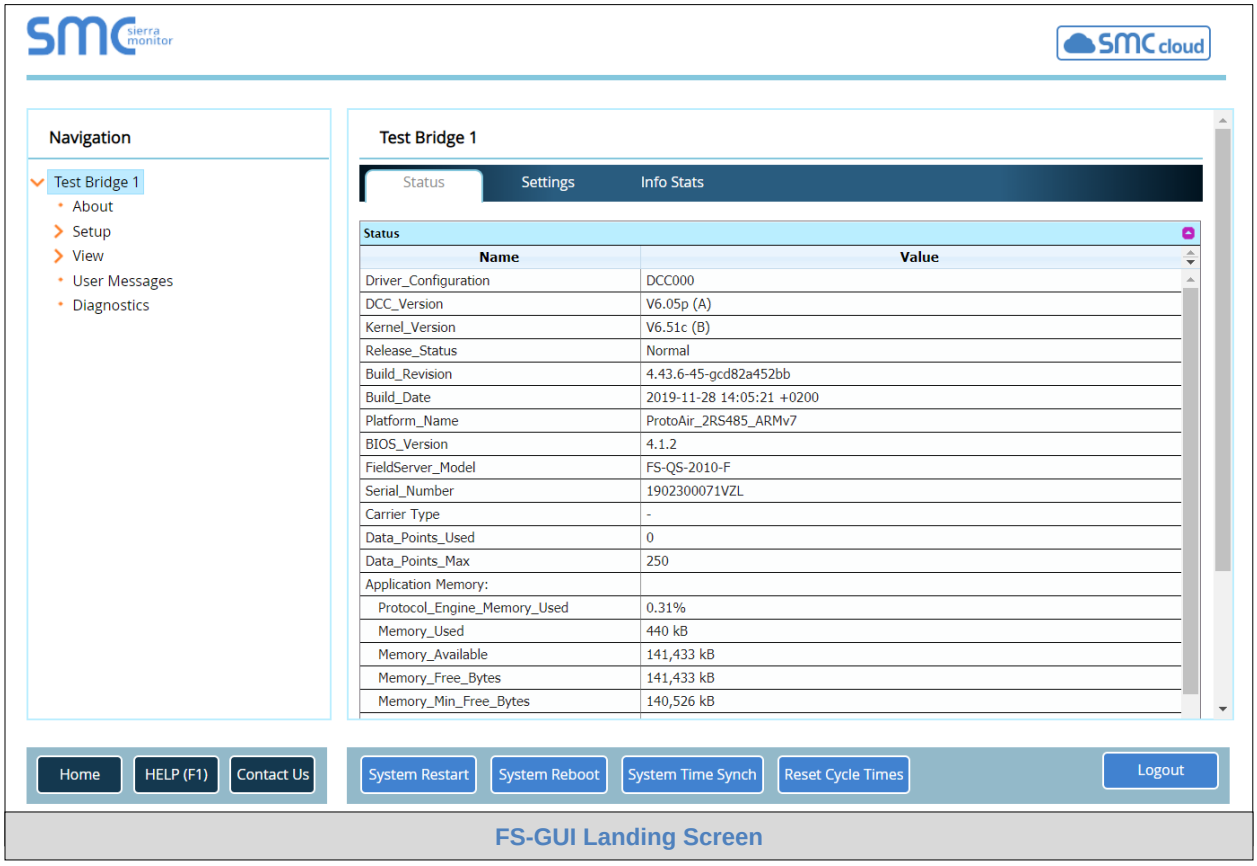
NOTE: Any changes will require a FieldServer reboot to take effect.

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



Web App Landing Screen

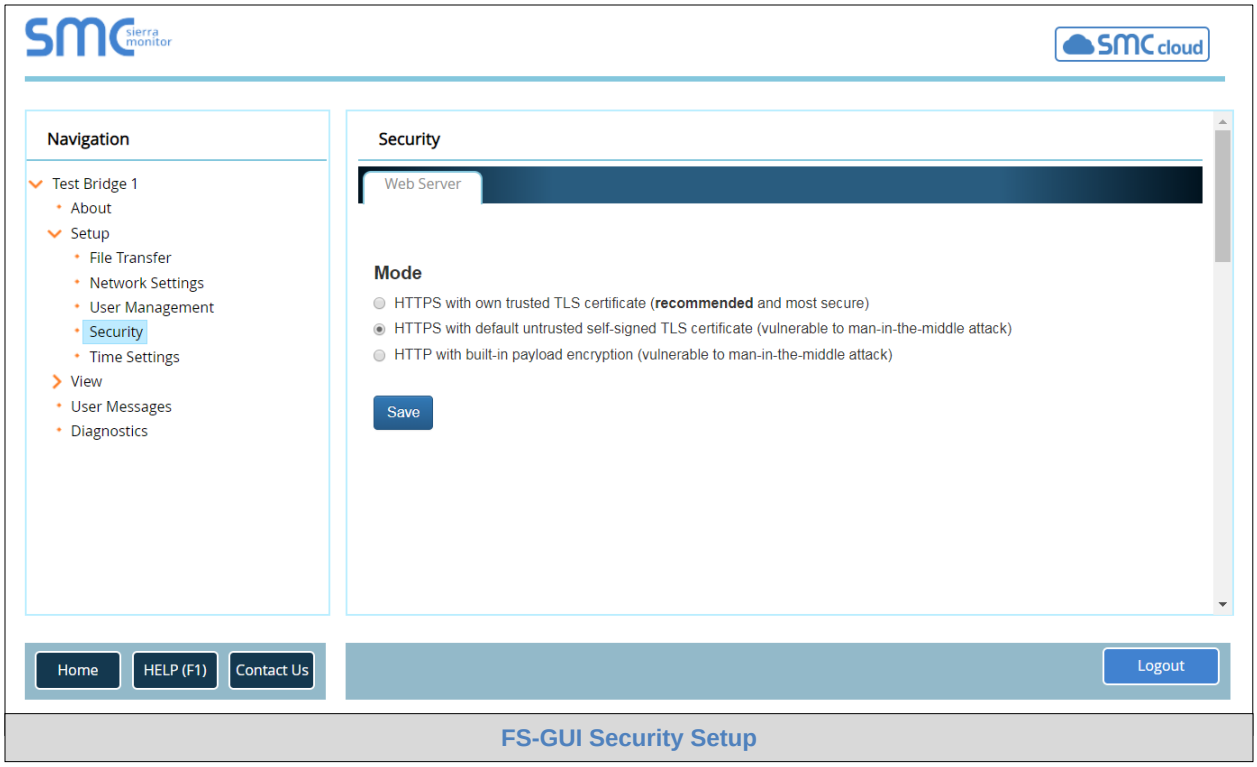
- Click Setup in the Navigation panel.



FS-GUI Landing Screen

3.1 Change Security Mode

- Click Security in the Navigation panel.



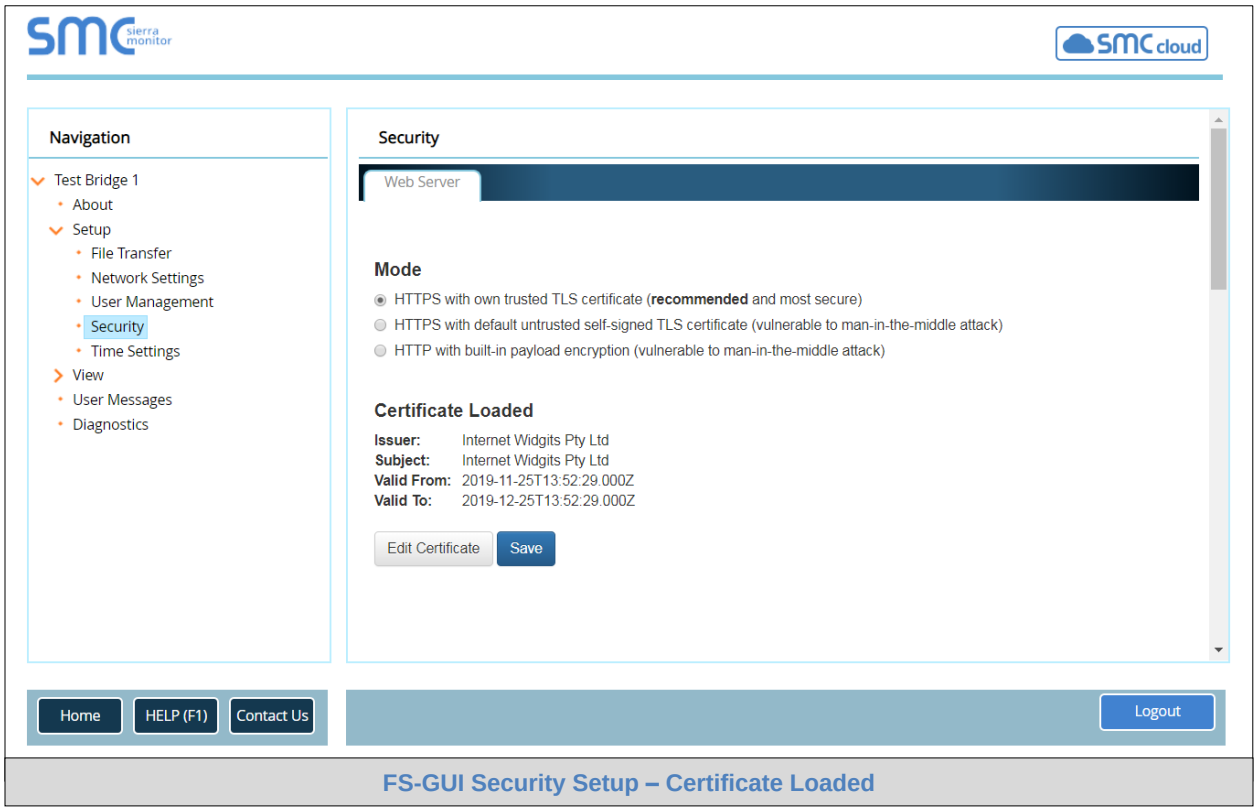
FS-GUI Security Setup

- 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.



FS-GUI Security Setup – Certificate Loaded

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

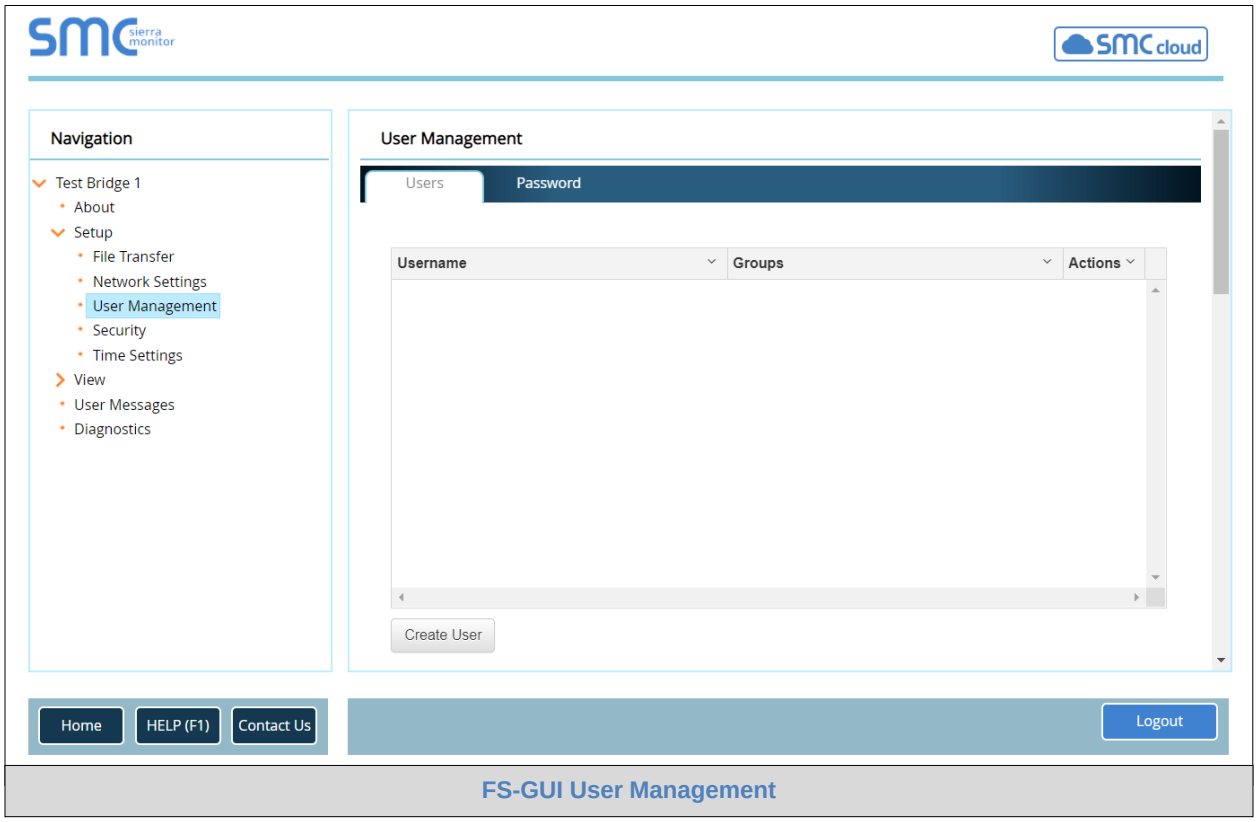
3.3 Change User Management Settings

- 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.



FS-GUI User Management

User Types:

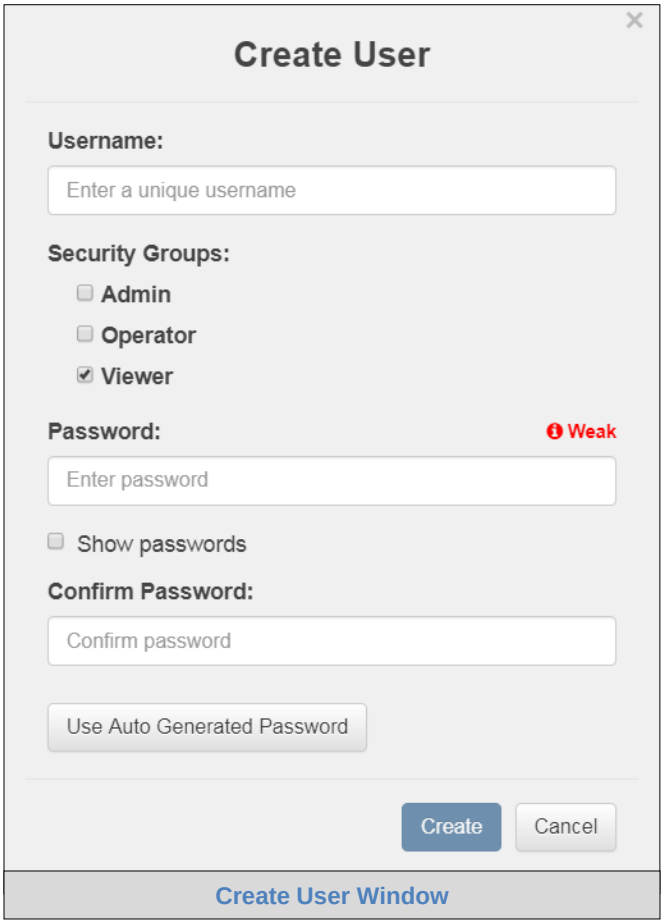
Admin – Can modify and view any settings on the FieldServer.

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 Window

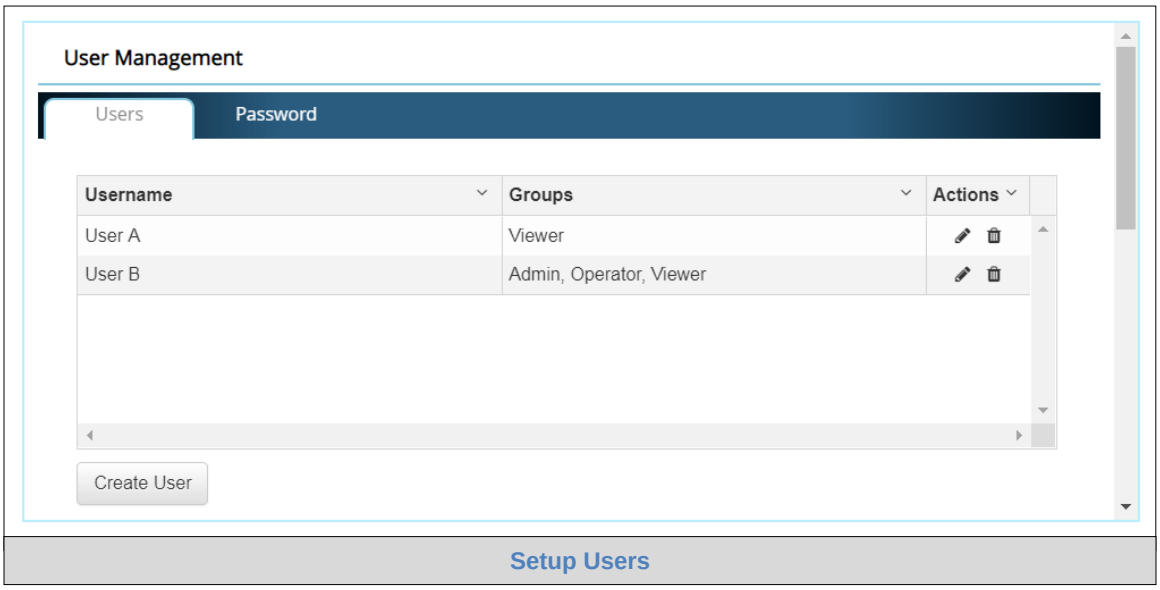
- Enter the new User fields: Name, Security Group and Password.

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.

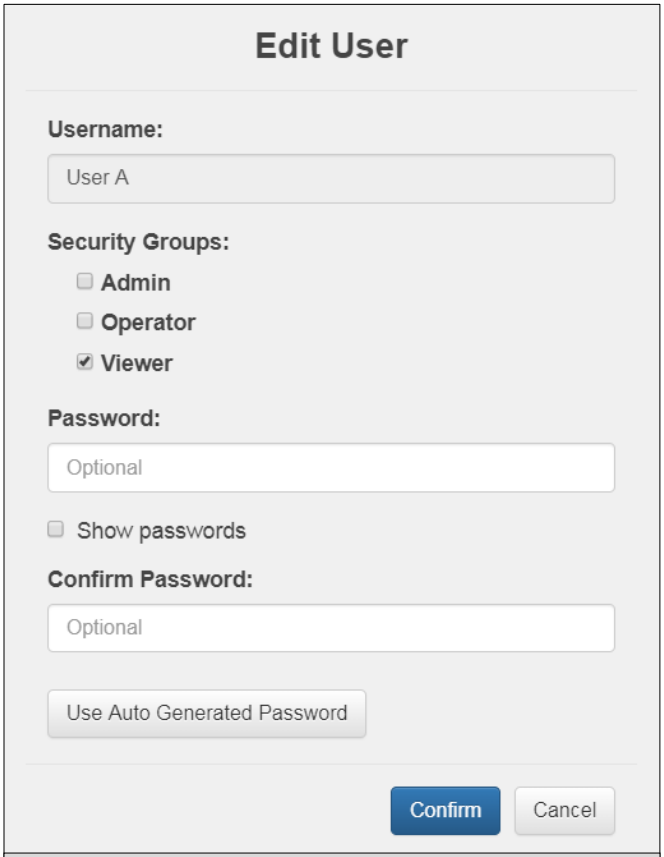
3.3.1.1 Edit Users

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



Setup Users

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

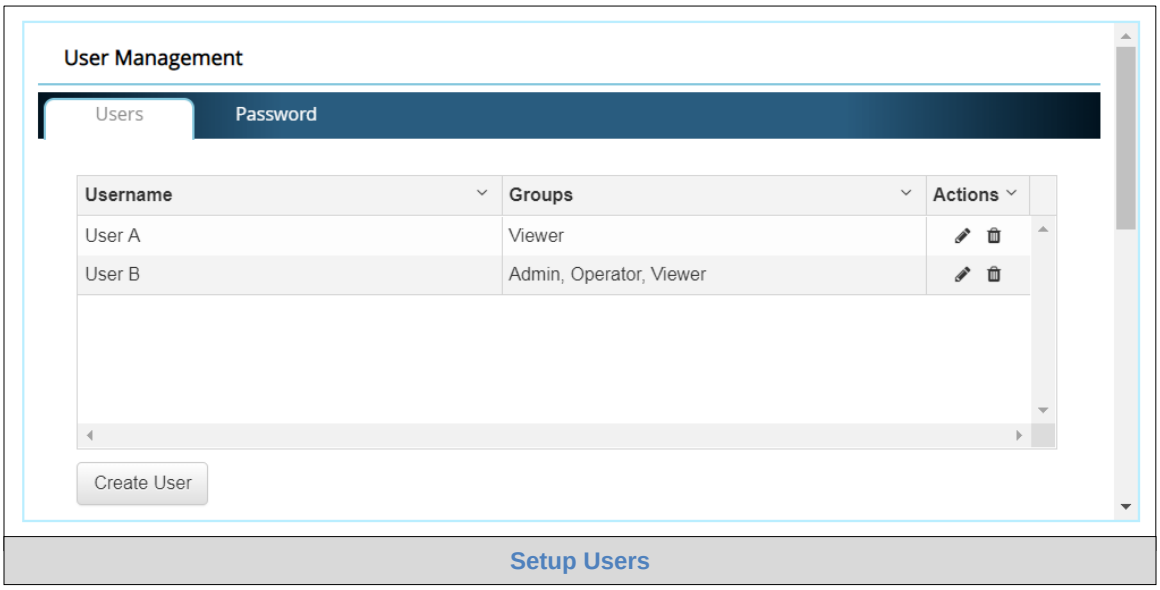


Edit User Window

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

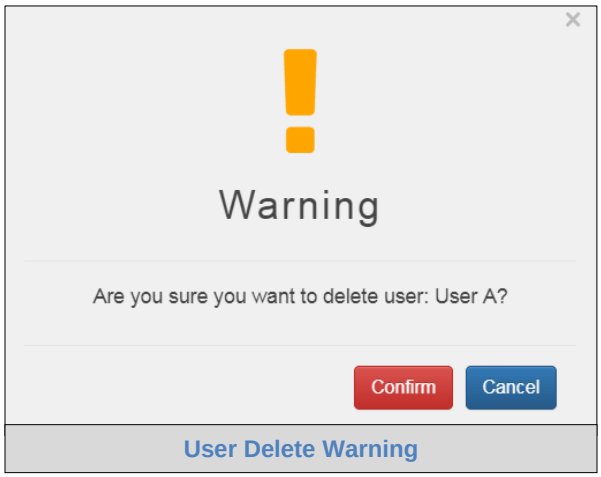
3.3.1.2 Delete Users

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



Setup Users

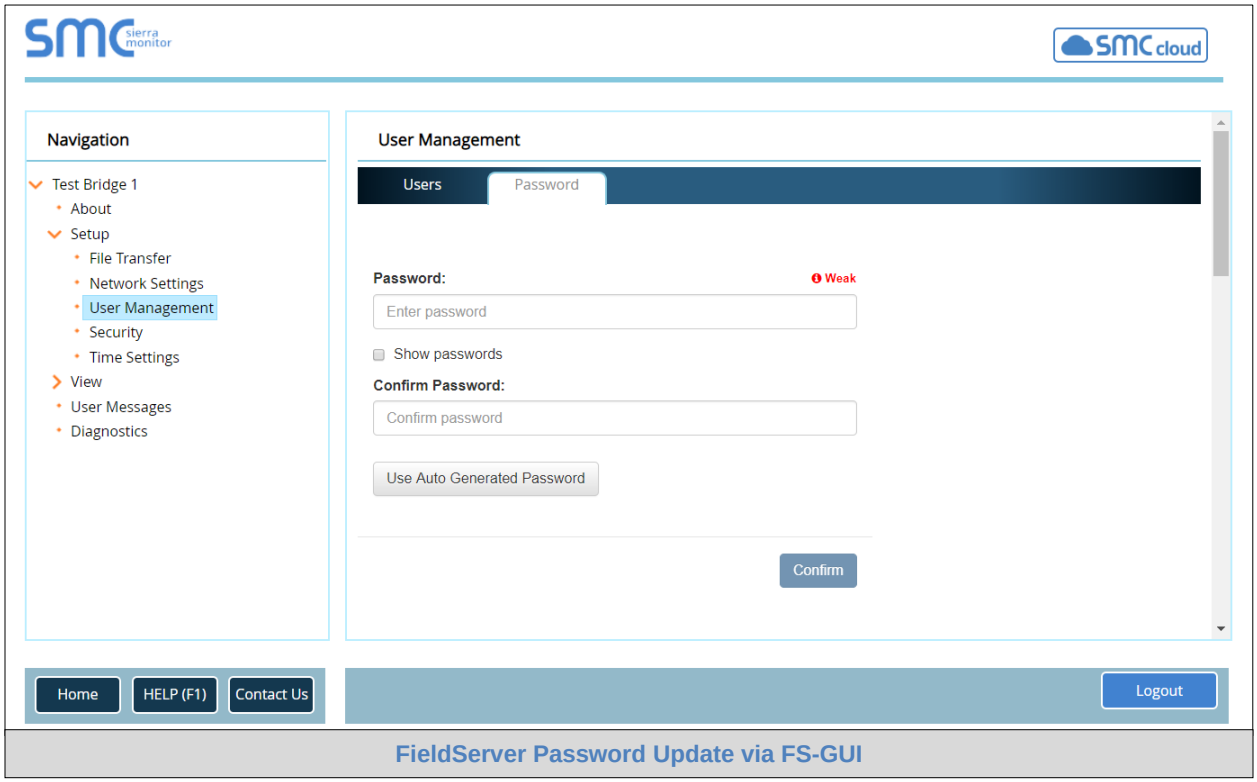
- When the warning message appears, click Confirm.



User Delete Warning

3.3.2 Change FieldServer Password

- Click the Password tab.



FieldServer Password Update via FS-GUI

- 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

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