SIEMENS

J2INNOVATIONS
A Siemens Company

CFG3.F200

Install Guide

A6V12893144_en--_a

2022-02-24

Smart Infrastructure

Edition notice

Technical specifications and availability subject to change without notice.

Edition: 2022-02-24

Document ID: A6V12893144_en--_a

Copyright

Table of Contents

Cybersecurity disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under https://www.siemens.com/cert/en/cert-security-advisories.htm.

1 About this Document

1.1 Scope

This guide provides an overview of the F200 and instructions for configuring it to control your building automation system.

1.2 Target reader

The target reader of this document has networking knowledge and can answer the following questions:

- Is your network in a single location or distributed?
- Are static IP address necessary for your system? If so, what are they?
- What is the subnet mask?
- What is the gateway?
- What is the DNS server?

2 Setting up the F200

This section will cover the installation, network choice, and log-in credentials for the F200.

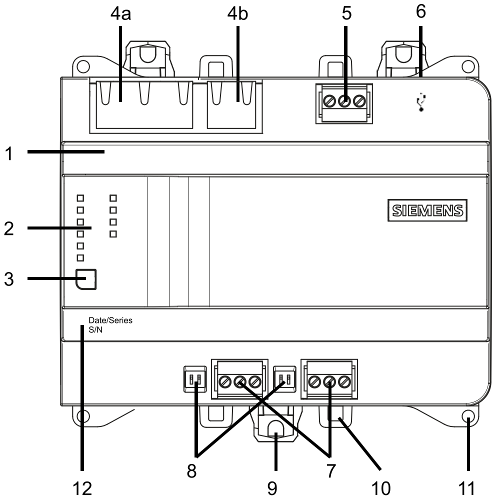
There are two ways to access the configuration user interface:

1. Connect the 2-port Ethernet switch (4a) to a DHCP server and open a new browser window. The DHCP server will automatically be assigned an IP address.
2. Connect the 2-port Ethernet switch (4a) to your computer. Press the SVC button (3) and wait for the SVC LED to illuminate red. In the browser address bar, type the following IP address: **169.254.169.254**.

   ⇨ The network patching configuration should look as follows:

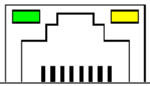
   – **Single network mode (combined):** WAN in in 2-port Ethernet switch (4a).

> Only the 2-port Ethernet switch (4a) supports a local connection to the F200. LAN and WAN in different networks must have different subnets.



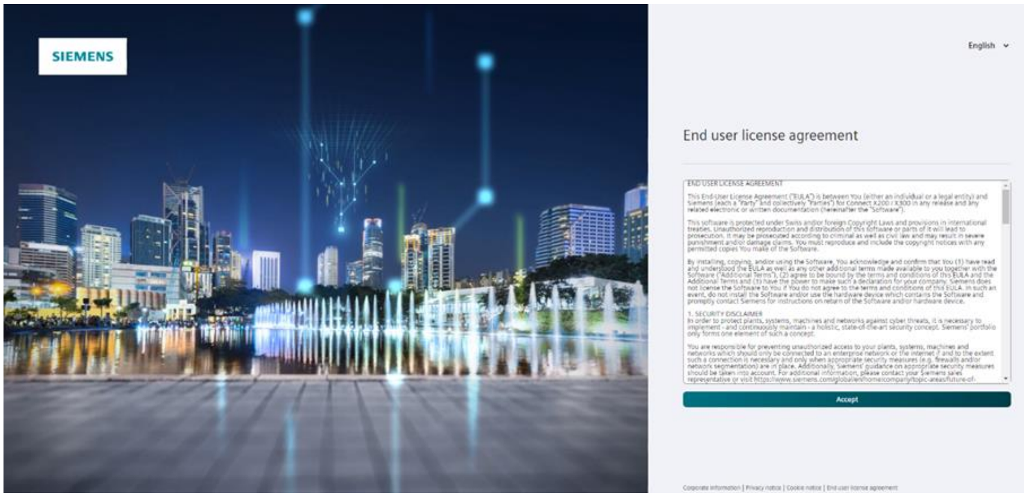
1	Plastic housing
2	LEDs for communication and status
3	Service button
4a	2-port Ethernet switch with 2 LEDs per port
4b	1-port Ethernet interface with 2 LEDs for WAN (Internet access)
5	Plug-in terminal blocks with screw terminals Power supply
6	USB interface for 4G dongles
7	Not supported (for future release)
8	Not supported (for future release)
9	Slider for mounting on standard mounting rails
10	Eyelets for cable ties
11	Holes for wall mounting
12	Date / Series and Serial number

There are multiple LED lights on the F200. The table below outlines each light's function:

Activity	LED / Interface	Color	Activity	Function
	Ethernet 1…3	Green	Continuously ON	Link active
			Continuously OFF	No connection

			Flashing	Network traffic
		Yellow	Continuously ON	Link 100 Mbps
			Continuously OFF	Link 10 Mbps
🟩RUN 🟦☁ □SVC	RUN	Green	Continuously ON	Device operational
			Continuously OFF	Device not operational
			Flashing	Start-up or program halted
		Red	Continuously ON	OK
			Continuously OFF	HW or SW fault – power off and on the F200
			Rapid flashing	Firmware or application missing/corrupted
	☁	Blue	Continuously ON	Connection to the cloud OK
			Flashing	No connection to the cloud Onboarding to cloud not finished or device certificates not updated
	SVC	Red	Continuously OFF	IP address not assigned to LAN port
			Continuously ON	IP address assigned to LAN port
□ SVC	Service button		First, power off device. Then, hold the button for up to 20 seconds.	Factory reset All configuration data and installed apps are deleted If RUN LED is constantly green, factory reset was successful
			Short press	IP address 169.254.169.254 will be assigned to LAN port for 15 minutes.

1. In the FIN Stack landing page, select **Accept** to verify you've acknowledged the end user license agreement.



End user license agreement

END USER LICENSE AGREEMENT

This End-User License Agreement ("EULA") is between You (either an individual or a legal entity) and Siemens (each a "Party" and collectively "Parties") for Connect X200 / X300 in any release and any related electronic or written documentation (hereinafter the "Software").

This software is protected under Swiss and/or foreign Copyright Laws and provisions in international treaties. Unauthorized reproduction and distribution of this software or parts of it will lead to prosecution. It may be prosecuted according to criminal as well as civil law and may result in severe punishment and/or damage claims. You must reproduce and include the copyright notices with any permitted copies You make of the Software.

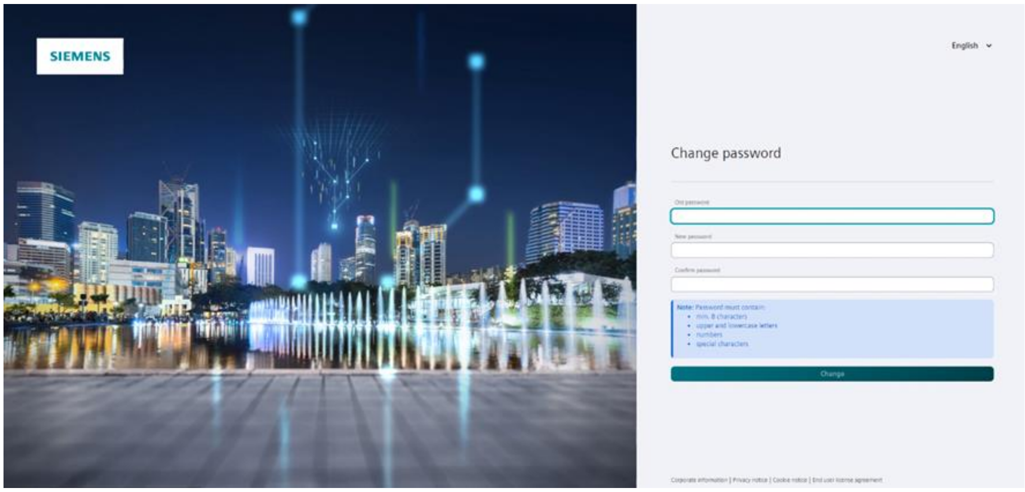
By installing, copying, and/or using the Software, You acknowledge and confirm that You (1) have read and understood the EULA as well as any other additional terms made available to you together with the Software ("Additional Terms"), (2) agree to be bound by the terms and conditions of this EULA and the Additional Terms and (3) have the power to make such a declaration for your company. Siemens does not license the Software to You if You do not agree to the terms and conditions of this EULA. In such an event, do not install the Software and/or use the hardware device which contains the Software and promptly contact Siemens for instructions on return of the Software and/or hardware device.

1. SECURITY DISCLAIMER
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit https://www.siemens.com/global/en/home/company/topic-areas/future-of-

Accept
Corporate information | Privacy notice | Cookie notice | End user license agreement

2. Next, enter the following credentials in the fields provided:
   - **Password:** admin (case-sensitive)
3. Next, complete the prompt to change the default password. This password is specific to the device you are logged in to. Select a password that complies with the following guidelines:
   - At least 8 characters
   - Uppercase and lowercase letters
   - Numbers
   - Special characters
4. Select **Change Password** when finished.


SIEMENS
English
Change password
Old password
New password
Confirm password
Change
Corporate information | Privacy notice | Cookie notice | End user license agreement

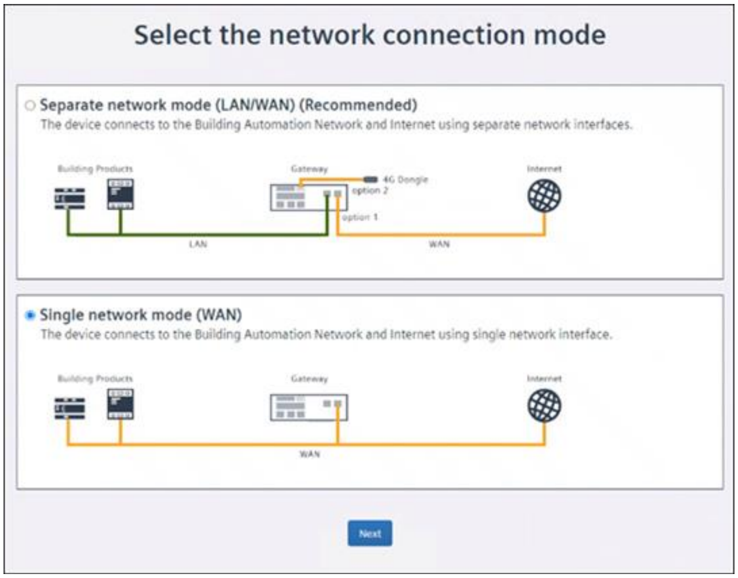
Note: Password must contain:
- min. 8 characters
- upper and lowercase letters
- numbers
- special characters

5. Sign in again with the newly created password.

3 Choosing a network and activating the F200

After you sign in to the F200 device, complete the following instructions:

1. Select a network connection mode.
   - If you plan to use distributed architecture features, spanning multiple subnets, then you must select **Single network mode**.
   - If you do not plan to use distributed architecture features and your building controls network is isolated from your internet access, then you must select **Separate network mode**.



Select the network connection mode

○ Separate network mode (LAN/WAN) (Recommended)

The device connects to the Building Automation Network and Internet using separate network interfaces.

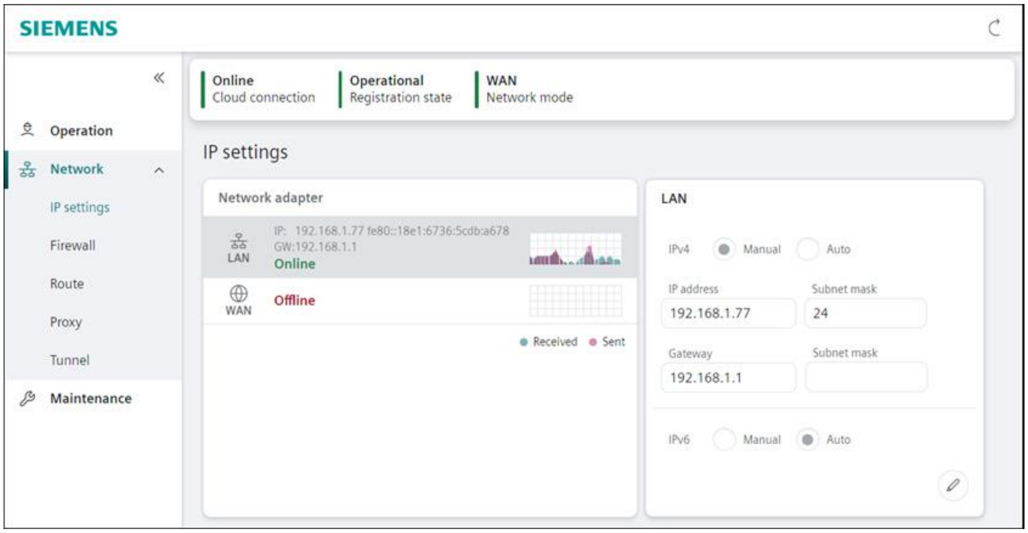
● Single network mode (WAN)

The device connects to the Building Automation Network and Internet using single network interface.

⚠ CAUTION	
⚠	This selection is not reversible. Verify your building's network connection mode before making a selection. A configuration reset is required to change this selection, which will result in loss of existing network configuration and project data.

⚠ CAUTION	
⚠	**Single network mode and cybersecurity** If you select **Single network mode**, you are responsible for securing your network with proper protection mechanisms.

2. To configure alternative IP and proxy settings, click the **IP settings** tab under the **Network** tab.
   NOTE: To configure the **Subnet mask**, define the number of masked bits. See **Appendix A** for more information.



Online Cloud connection | Operational Registration state | WAN Network mode

IP settings

Network adapter

LAN — IP: 192.168.1.77 fe80::18e1:6736:5cdb:a678 GW:192.168.1.1 Online

WAN — Offline

LAN

IPv4 ● Manual ○ Auto

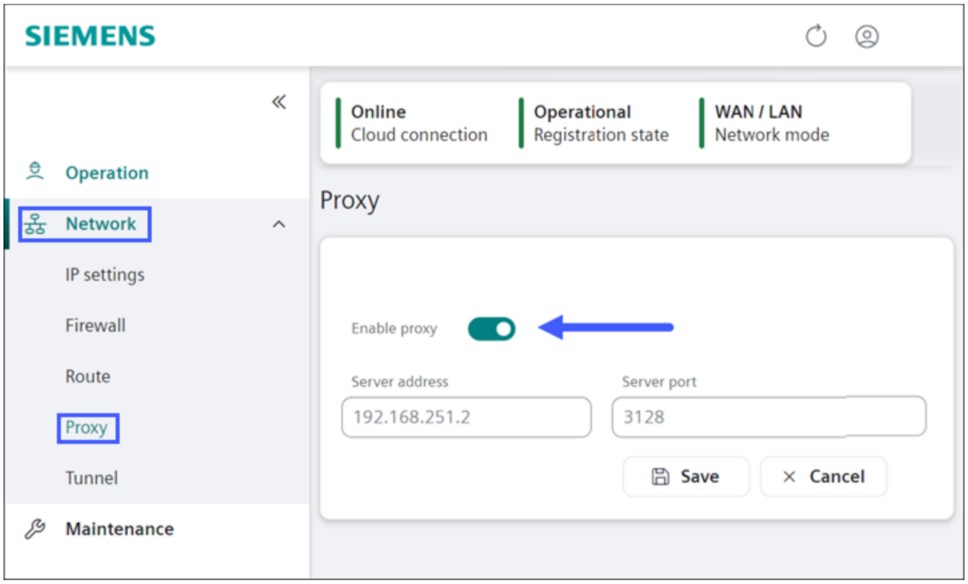
IP address: 192.168.1.77 Subnet mask: 24

Gateway: 192.168.1.1 Subnet mask:

IPv6 ○ Manual ● Auto

3. *(Optional)* If you need to configure a proxy setting for an alternative WAN IP address, do so by clicking the **Network** tab, then **Proxy**.

4. *(Optional)* Toggle on the proxy server button. Then type to enter the appropriate values in the spaces provided.



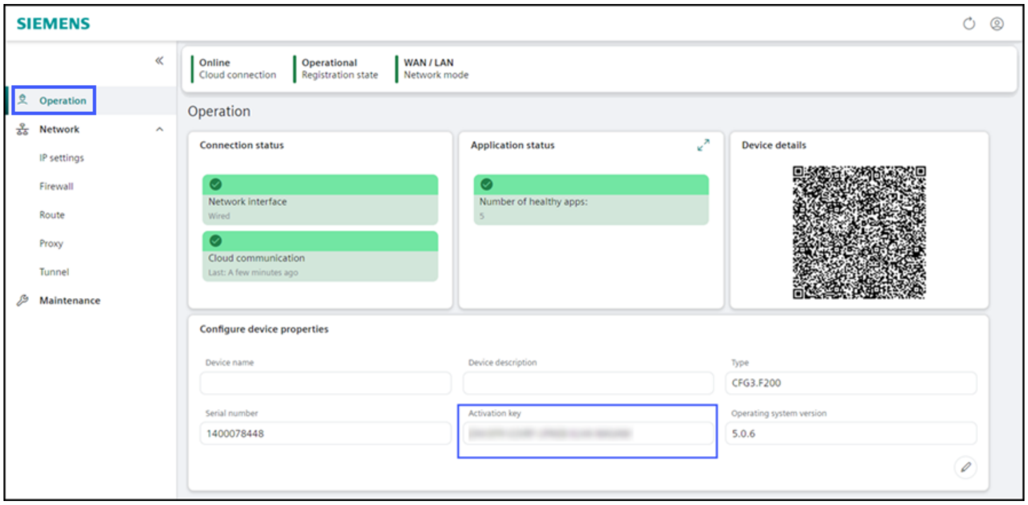
Online Cloud connection | Operational Registration state | WAN / LAN Network mode

Proxy

Enable proxy: on

Server address: 192.168.251.2 Server port: 3128

5. In the **Operation** tab, copy the activation key. Proceed to the **Devices** application to complete activating your gateway.



Online
Cloud connection

Operational
Registration state

WAN / LAN
Network mode

Connection status

Network interface
Wired

Cloud communication
Last: A few minutes ago

Application status

Number of healthy apps:
5

Configure device properties

Device name	Device description	Type
		CFG3.F200
Serial number	Activation key	Operating system version
1400078448	[redacted]	5.0.6

Device cloud connection may appear as offline.

Troubleshooting

If your F200 device does not properly register or the Cloud connection state shows disconnected, follow these steps:

1. Power off the gateway device.
2. Power on the gateway device.
3. Press the SVC button.
4. Directly connect your PC to the LAN port via 169.254.169.254.

➪ The F200 device is now properly registered and the Cloud connection state shows connected.

4 Adding devices

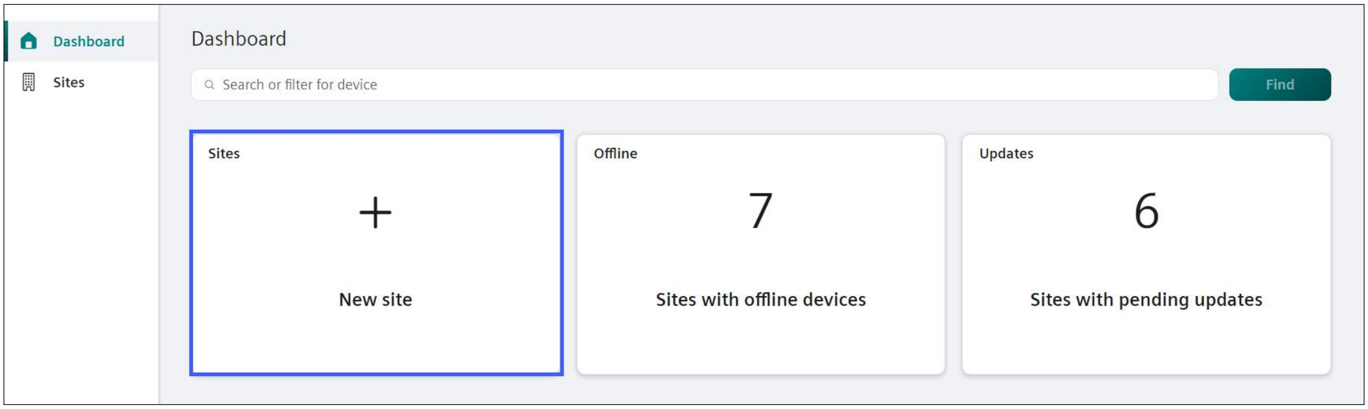
Before using FIN Stack, you need to create a site, add and activate your device, and update your device in Horizon.

1. Use the following link to access Horizon: https://assets.bpcloudapps.siemens.com/#/login
2. Log in using your credentials.

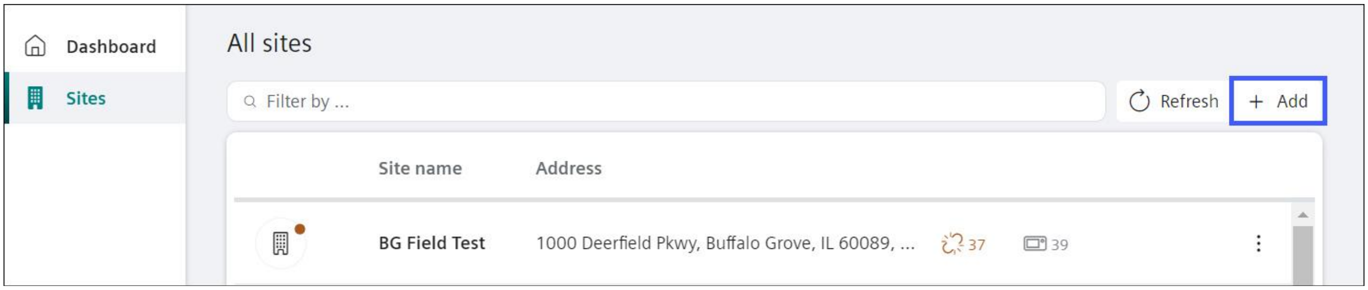
Creating a site

▷ In **Devices**:

1. Create a new site via one of the options below:
   – Go to **Dashboard** > **New site**.

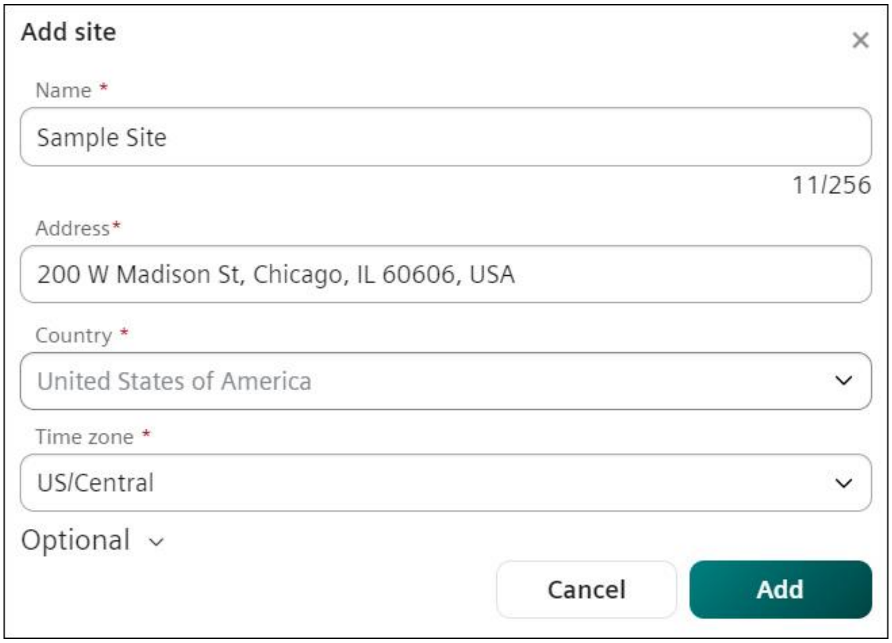

Dashboard
Sites
Dashboard
Search or filter for device
Find
Sites
+
New site
Offline
7
Sites with offline devices
Updates
6
Sites with pending updates

   – Go to **Sites** > **Add**.



Site name	Address		
BG Field Test	1000 Deerfield Pkwy, Buffalo Grove, IL 60089, ...	37	39

2. Fill in the fields on the **Add site** form.



Add site

Name *

Sample Site

11/256

Address*

200 W Madison St, Chicago, IL 60606, USA

Country *

United States of America

Time zone *

US/Central

Optional

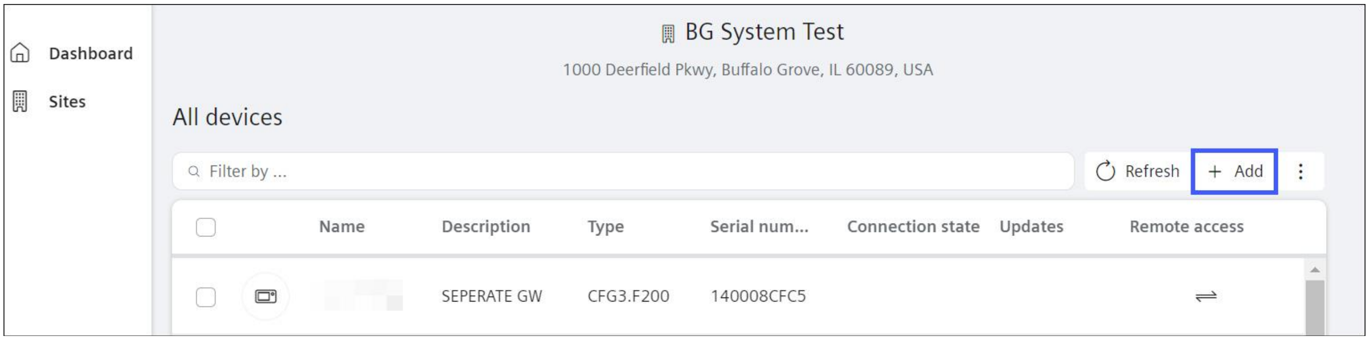
3. Click **Add**.

The **Address** field will automatically suggest addresses. Selecting a suggested address will automatically populate the **Time Zone** field. If Google API is unavailable, you will need to enter in an address and time zone manually.

Adding and activating device

▷ After adding a site, in **Devices**:

1. Go to **Sites**.
2. Select the site where you want to add your device.
3. Click **Add**.



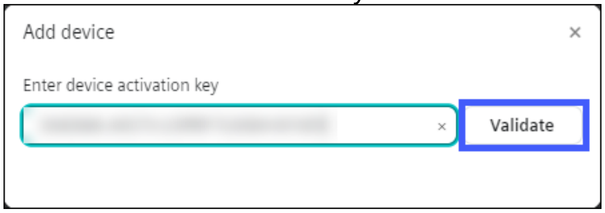
BG System Test

1000 Deerfield Pkwy, Buffalo Grove, IL 60089, USA

All devices

□		Name	Description	Type	Serial num...	Connection state	Updates	Remote access
□		[redacted]	SEPERATE GW	CFG3.F200	140008CFC5			⇌

4. Enter the device activation key and select **Validate**.



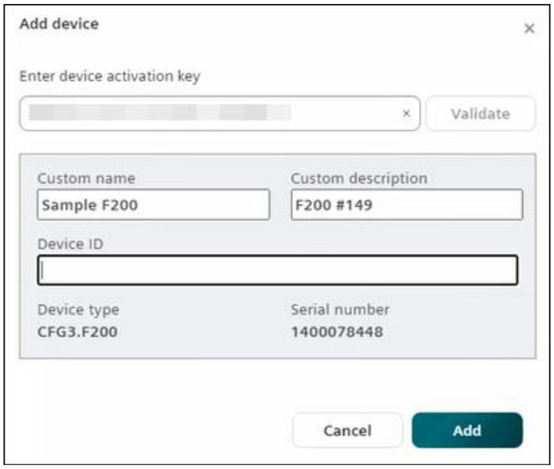
Add device

Enter device activation key

[redacted]

For F200 devices, the activation key is available in the **Operation** tab of the Config UI.

5. Confirm the details of your device.
6. Click **Add.**



Add device

Enter device activation key

[redacted]

Custom name: Sample F200

Custom description: F200 #149

Device ID:

Device type: CFG3.F200

Serial number: 1400078448

When defining or changing the custom name of the device, it will only affect the display name in the cloud. The Custom name and Custom description fields can be left blank.

Assigning distributions

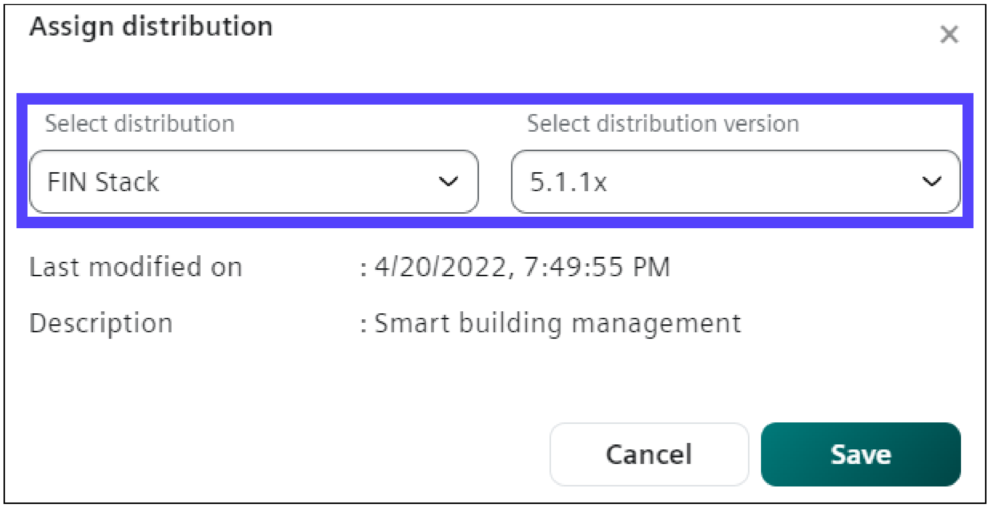
After adding and activating the device, you will need to assign the distribution to enable FIN Stack Discovery. To assign a distribution to the device, follow the steps below.

Assigning a distribution set will only need to be done once. The assign distribution pop-up will only appear after adding a device in a site. If you do not assign a distribution, this pop-up will appear until the device is assigned a distribution.

▷ In **Devices**:

1. Go to **Sites**.
2. Select the site with the F200 device.
3. Select the device.

4. Go to **Applications**.
5. In the pop-up, use the drop-down menus to **Select distribution** and **Select distribution version**.
   NOTE: Verify that the latest **distribution version** is selected.
6. Click **Save**.



Assign distribution

Select distribution: FIN Stack

Select distribution version: 5.1.1x

Last modified on : 4/20/2022, 7:49:55 PM

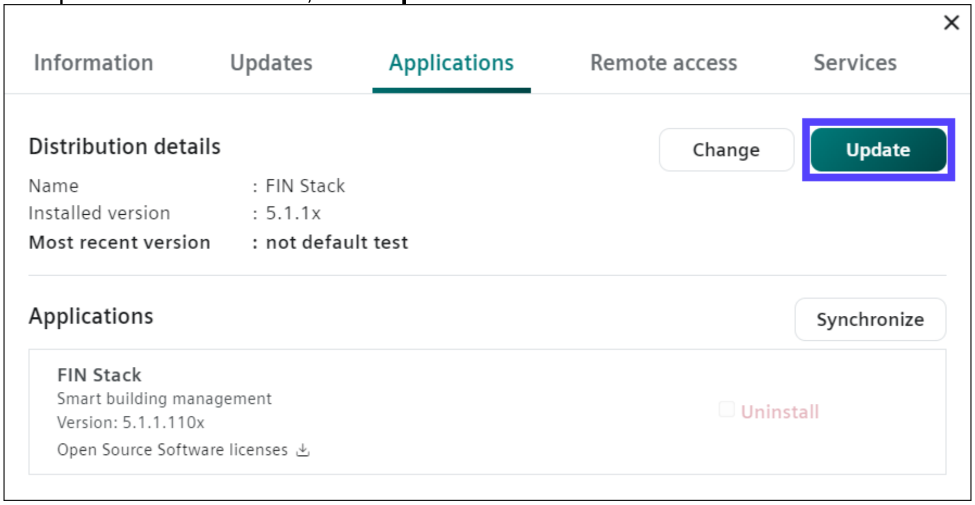
Description : Smart building management

Updating distributions

To update a distribution on a device, follow the steps below.

▷ In **Devices**:

1. In the **Sites** tab, select the site with the F200 device.
2. Select the device.
3. Go to **Applications**.
4. To update the distribution, click **Update**.



Distribution details

Name : FIN Stack

Installed version : 5.1.1x

Most recent version : not default test

Applications

FIN Stack

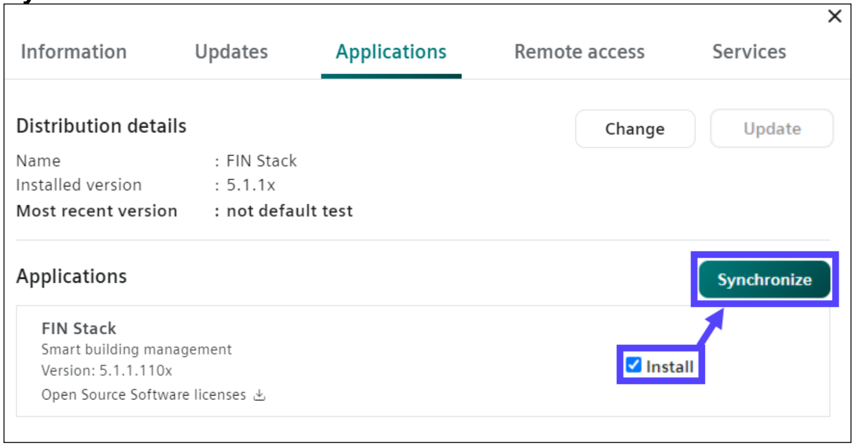
Smart building management

Version: 5.1.1.110x

Open Source Software licenses

5. Confirm with **Update**.

6. FIN Stack is not installed by default. To install FIN Stack, click **Install** > **Synchronize**.



Information | Updates | Applications | Remote access | Services

Distribution details

Change | Update

Name : FIN Stack
Installed version : 5.1.1x
Most recent version : not default test

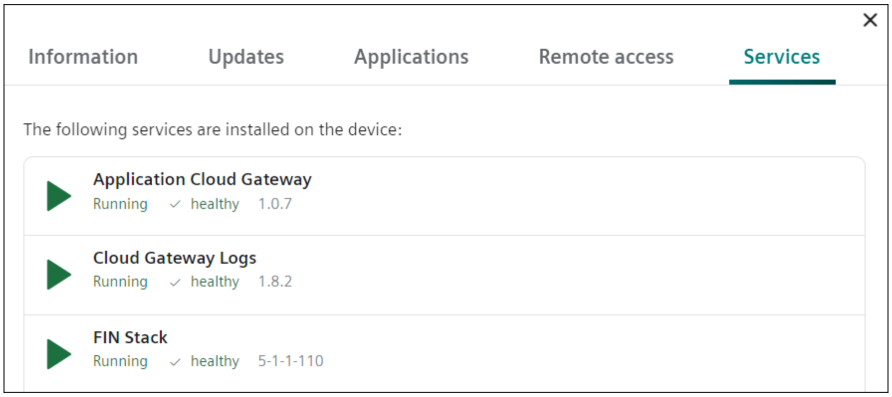
Applications

Synchronize

FIN Stack
Smart building management
Version: 5.1.1.110x
Open Source Software licenses

☑ Install

7. Navigate to the **Services** tab and find the status of your application. The controller is ready to be used when the application displays as **Running** and **healthy** in the **Services** tab.



Information | Updates | Applications | Remote access | Services

The following services are installed on the device:

Application Cloud Gateway
Running ✓ healthy 1.0.7

Cloud Gateway Logs
Running ✓ healthy 1.8.2

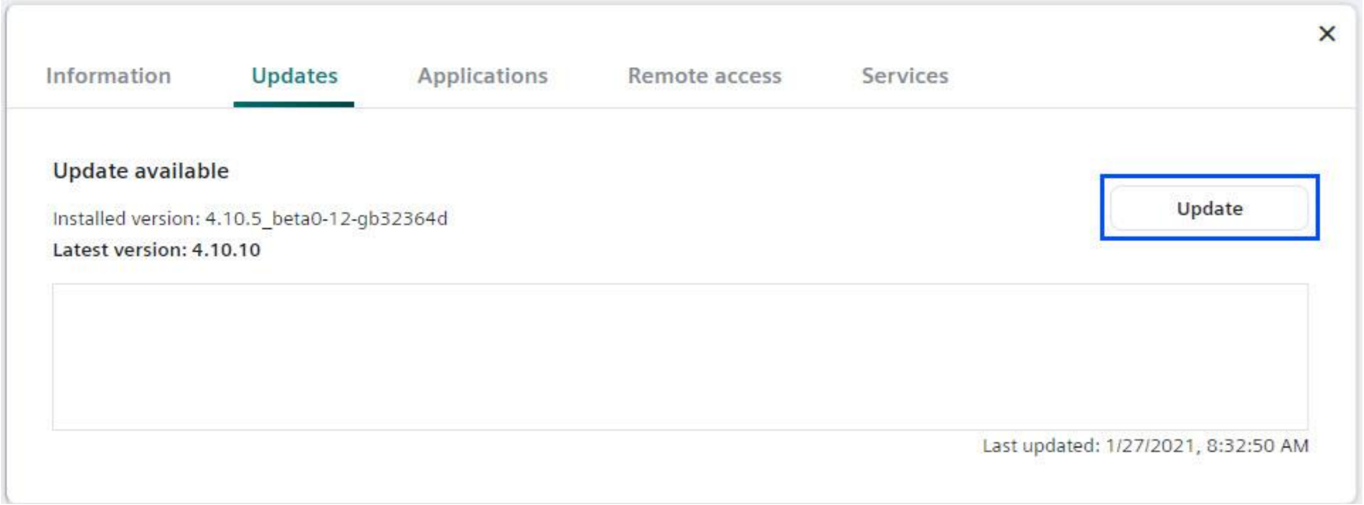
FIN Stack
Running ✓ healthy 5-1-1-110

Update Operating System

To update the operating system of the Connect device, follow the steps below.

▷ In **Devices**:

1. Go to **Sites**.
2. Select the site with the F200 device.
3. Select the device > **Updates**.
4. Click **Update**



Update available

Installed version: 4.10.5_beta0-12-gb32364d

Latest version: 4.10.10

Last updated: 1/27/2021, 8:32:50 AM

5. Confirm with **Update**.

ℹ The operating system update could take approximately 20 minutes depending on your network bandwidth. Ensure that the download rate of your network bandwidth is at least 8Mbit/second, or else the update will likely time out. Wait before proceeding to the next step.

If you update the operating system, you’ll be logged out of the F200 Device Interface.

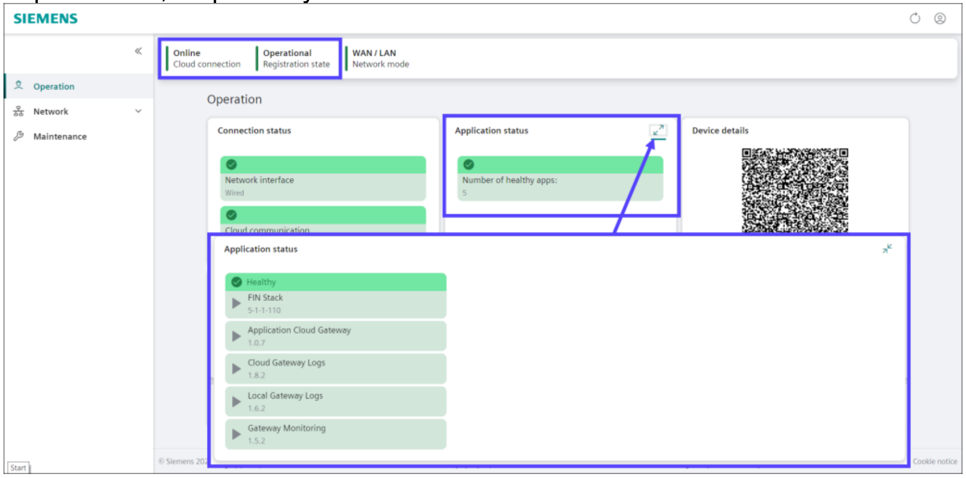
▷ (Optional) In F200 device:

◈ Go to the **Maintenance** tab in FIN Stack to follow the software update in real-time.

5 Verifying the Registration State and Software Updates

▷ (Optional) In FIN Stack:

1. To check the status of all applications on the F200 device, select the **Operation** tab in the side navigation bar.
2. Click ⤢ to expand the **Applications** menu. Ensure all applications are healthy. You will also note that **Cloud connection** is “Online” and **Registration state** is “Operational”, respectively.



Online
Cloud connection

Operational
Registration state

WAN / LAN
Network mode

Network interface
Wired

Cloud communication

Number of healthy apps:
5

Application status

Healthy

FIN Stack
5-1-1-110

Application Cloud Gateway
1.0.7

Cloud Gateway Logs
1.8.2

Local Gateway Logs
1.6.2

Gateway Monitoring
1.5.2

If you update FIN Stack operating system, you will be logged out of the F200 interface.

6 Configuring the F200 Firewall

Once you have ensured cloud connectivity and updated the latest gateway application software to the F200 device, you must next configure the firewall rules. By default, inbound traffic is not allowed on the device. You must open the ports so the F200 device can communicate with the building automation network.

The FIN Stack operating system **must** finish updating before you configure the firewall rules in the device (as outlined in the section above).
To manually configure the F200:

1. Select the **Network** tab. Then, select the **Firewall** header.
2. Create the following **inbound** rules for:

Separate Network Mode

Description	Protocol	Source Port
BACnet IP devices	udp	47808
FIN Stack Web-client	tcp	8090 (HTTPS) 8085 (HTTP)
Default	All rejected	

Single Network Mode

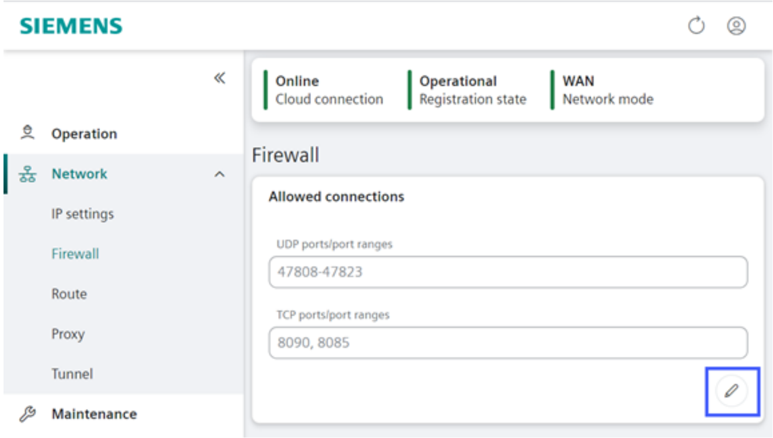
Description	Protocol	Source Port
BACnet IP devices	udp	47808
FIN Stack Web-client	tcp	8090 (HTTPS) 8085 (HTTP)
Default	All rejected	

Requirements for Horizon (Devices)

Description	Protocol	Source Port
HTTPS	tcp	443
MQTTS	tcp	443
NTP	udp	123

Depending on building automation network configuration on site, the source ports may differ.

◈ Click **Edit** ✎ to change the port.



Firewall

Allowed connections

UDP ports/port ranges: 47808-47823

TCP ports/port ranges: 8090, 8085

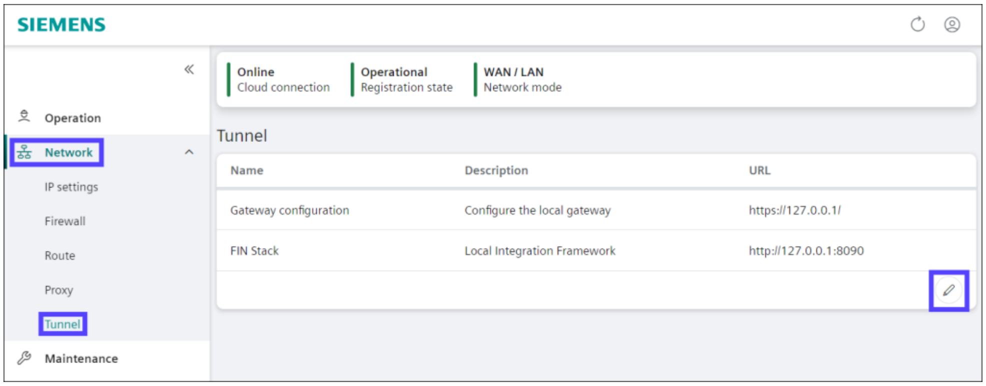
7 Enabling remote web access in the F200 UI

To use remote web access, you must configure your endpoints in the F200. To configure your endpoints, follow the steps below.

NOTE: If you are configuring a static IP, you must enter a gateway address for the interface connected to the internet.

▷ In the Configuration UI:

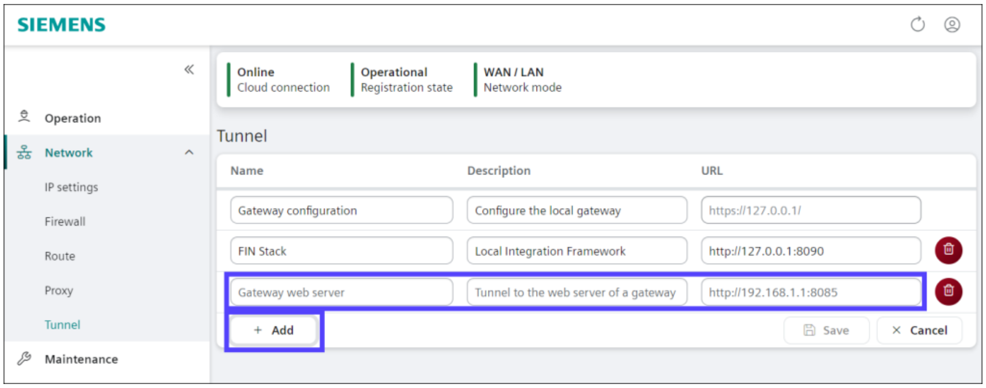
1. Select **Network** > **Tunnel** > **Edit** ✎



Tunnel

Name	Description	URL
Gateway configuration	Configure the local gateway	https://127.0.0.1/
FIN Stack	Local Integration Framework	http://127.0.0.1:8090

2. Click **Add**.

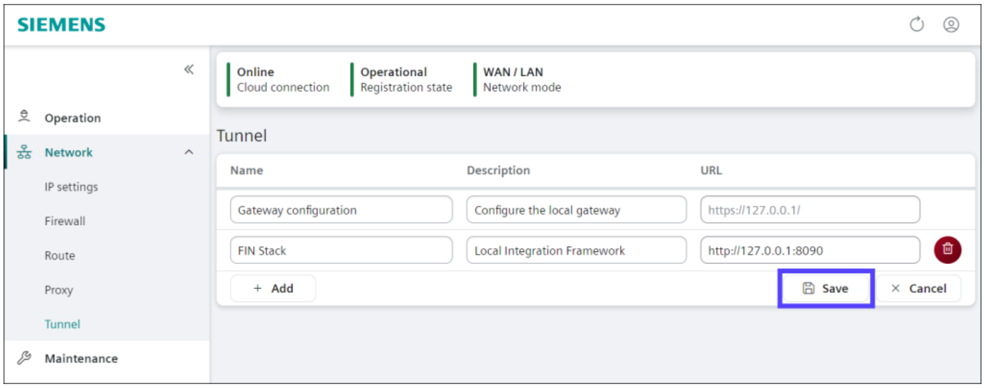


Tunnel

Name	Description	URL
Gateway configuration	Configure the local gateway	https://127.0.0.1/
FIN Stack	Local Integration Framework	http://127.0.0.1:8090
Gateway web server	Tunnel to the web server of a gateway	http://192.168.1.1:8085

3. Enter the Name, Description, and URL.

4. Click **Save**.



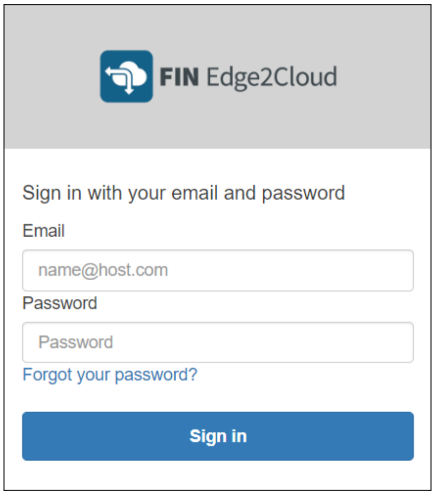
Tunnel

Name	Description	URL
Gateway configuration	Configure the local gateway	https://127.0.0.1/
FIN Stack	Local Integration Framework	http://127.0.0.1:8090

8 Licensing the F200

Complete this procedure add a license to your F200 through Edge2Cloud.

1. Use the following link to access Edge2Cloud: https://portal.e2cloud.io/
2. Enter your credentials to sign in.



Sign in with your email and password

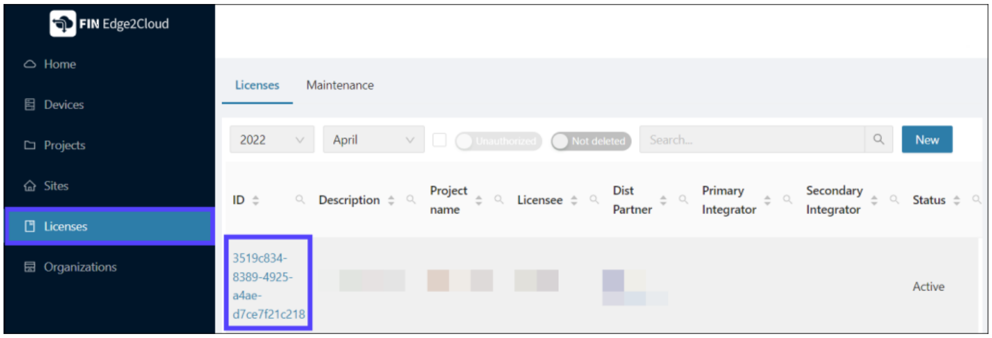
Email

name@host.com

Password

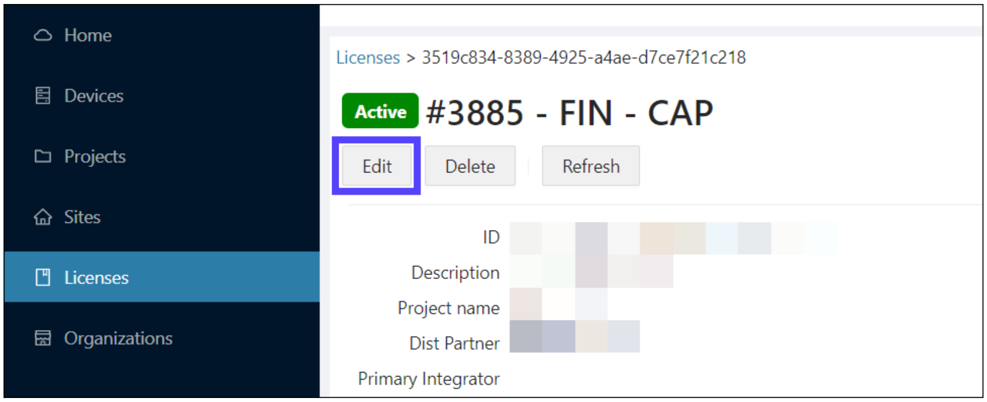
Password

3. Click **Licenses**.
4. In the list, locate your license > Click on the **ID**.



ID	Description	Project name	Licensee	Dist Partner	Primary Integrator	Secondary Integrator	Status
3519c834-8389-4925-a4ae-d7ce7f21c218	[redacted]	[redacted]	[redacted]	[redacted]			Active

5. A page with your license information will open. Click **Edit.**



Licenses > 3519c834-8389-4925-a4ae-d7ce7f21c218

Active #3885 - FIN - CAP

ID [redacted]

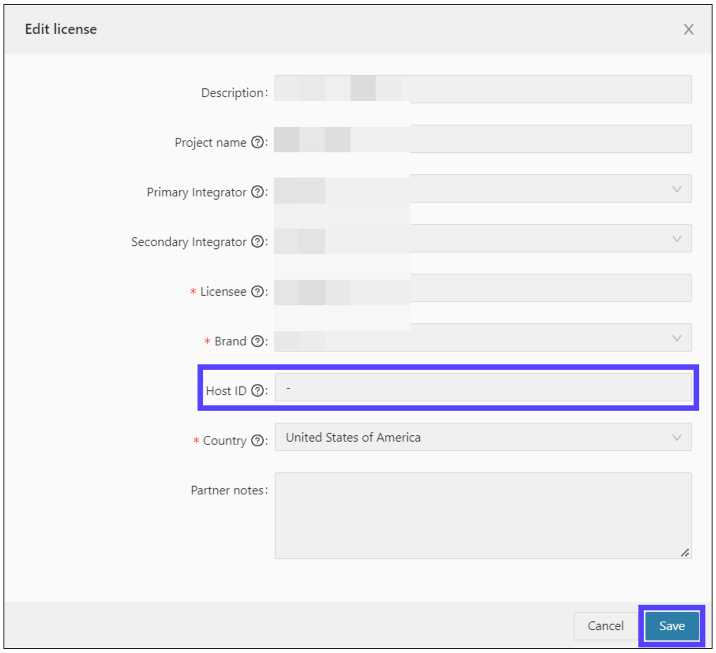
Description [redacted]

Project name [redacted]

Dist Partner [redacted]

Primary Integrator

6. The **Edit license** window will open. Enter your device’s serial number into the **Host ID** field. You can find the serial number on the back of the device or in Horizon.



Edit license

Description:

Project name ⓘ:

Primary Integrator ⓘ:

Secondary Integrator ⓘ:

* Licensee ⓘ:

* Brand ⓘ:

Host ID ⓘ: -

* Country ⓘ: United States of America

Partner notes:

7. Click **Save**.

   ⇨ Your license is now available for download.

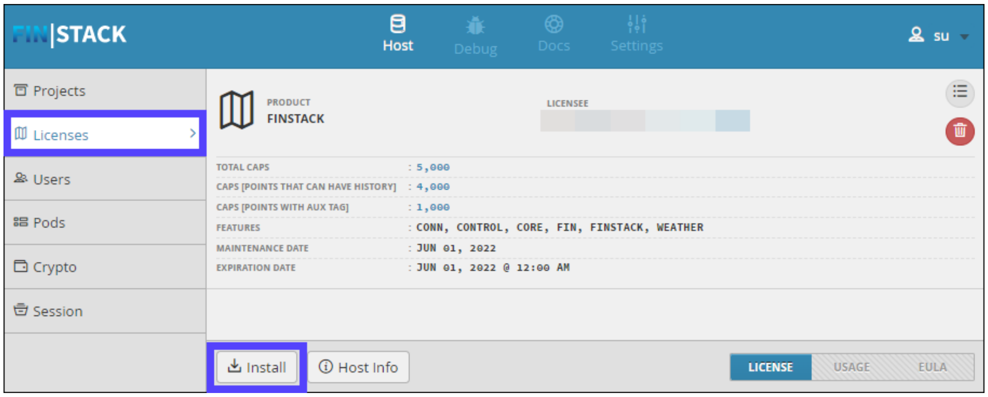
8. On the license information page, click **Download** > **Yes**.

   – Your license will download as a .prop file.
   ⇨ You can now upload your license to FIN Stack.

9. Login to FIN Stack as a Super User (su).

   – The default password is su.
   – You will be required to change the default password.
   – You will be locked out after three failed login attempts.
   – If you forget your password, reset your device configuration. You will lose FIN data.
   – Create another Super User account as a backup in case you lock yourself out of FIN Stack.

10. Click **Licenses** > **Install**.



PRODUCT
FINSTACK

LICENSEE
[redacted]

TOTAL CAPS	: 5,000
CAPS [POINTS THAT CAN HAVE HISTORY]	: 4,000
CAPS [POINTS WITH AUX TAG]	: 1,000
FEATURES	: CONN, CONTROL, CORE, FIN, FINSTACK, WEATHER
MAINTENANCE DATE	: JUN 01, 2022
EXPIRATION DATE	: JUN 01, 2022 @ 12:00 AM

11. Browse through your files for the license and click **Open**.

12. Reboot the controller.

➪ The controller is now licensed.

9 Appendix A - Configuring the subnet mask

Use the following table as a guide to define the number of bits in a **Subnet mask**.

Subnet mask	Number of bits
255.255.255.252	30
255.255.255.248	29
255.255.255.240	28
255.255.255.224	27
255.255.255.192	26
255.255.255.128	25
255.255.255.0	24
255.255.254.0	23
255.255.252.0	22
255.255.248.0	21
255.255.240.0	20
255.255.224.0	19
255.255.192.0	18
255.255.128.0	17
255.255.0.0	16

Issued by
Siemens Industry, Inc.
Smart Infrastructure
1000 Deerfield Pkwy
Buffalo Grove IL 60089
+1 847-215-1000