MotionWorks Enterprise RFID

Reader Management

User Guide

ZEBRA

P1129974-03EN Rev A

Copyright

2024/02/12

Terms of Use

Proprietary Statement

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

Product Improvements

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

Liability Disclaimer

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

Limitation of Liability

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Contents

Contents

About this Guide

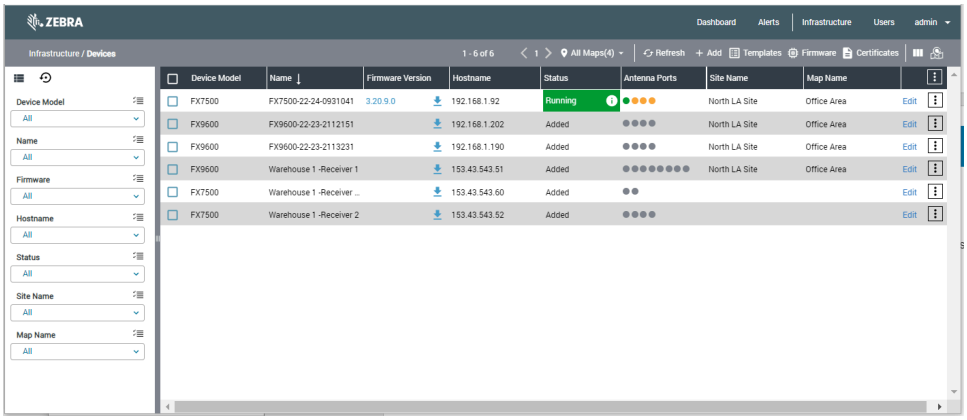
MotionWorks Enterprise RFID Reader Management is Zebra's next-generation RFID software. A state-of-the-art and powerful platform for RFID device management, data capture, identification, and location of EPC Gen2 tagged passive RFID assets.

This guide focuses on the Reader Management web client—the main venue for accessing reader functionality—and Device Manager, a management console available within the Reader Management web client.

Device Manager is a simple yet powerful tool to deploy, monitor, and manage Zebra RFID readers on-site or anywhere in the world. Device Manager is accessed via the menu in the Reader Management web client. Device Manager communicates with a server on-premises or in the cloud, which forwards configuration and management commands to RFID devices and receives health, status, and current configuration information from the devices.

Device Manager offers a clean and intuitive interface to monitor and manage RFID readers.

Figure 1 Device Manager



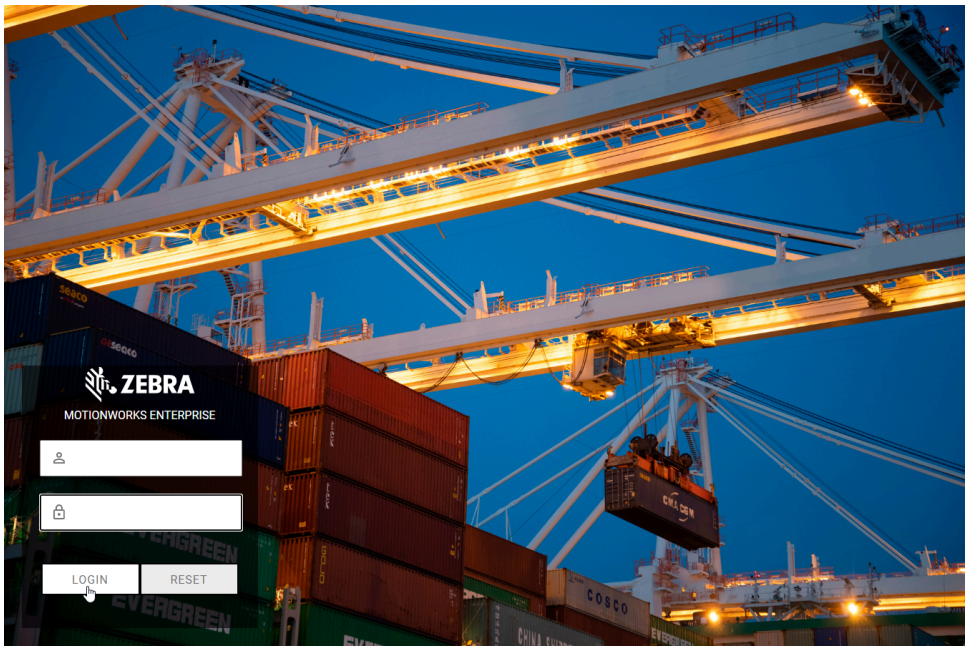
Launching Reader Management

This section describes launching Reader Management.

Launching the Reader Management Web Client

This section describes how to access the Reader Management web client from a browser.

- Open a browser window and go to https://[RM Server Name or IP address]. The login page is displayed.



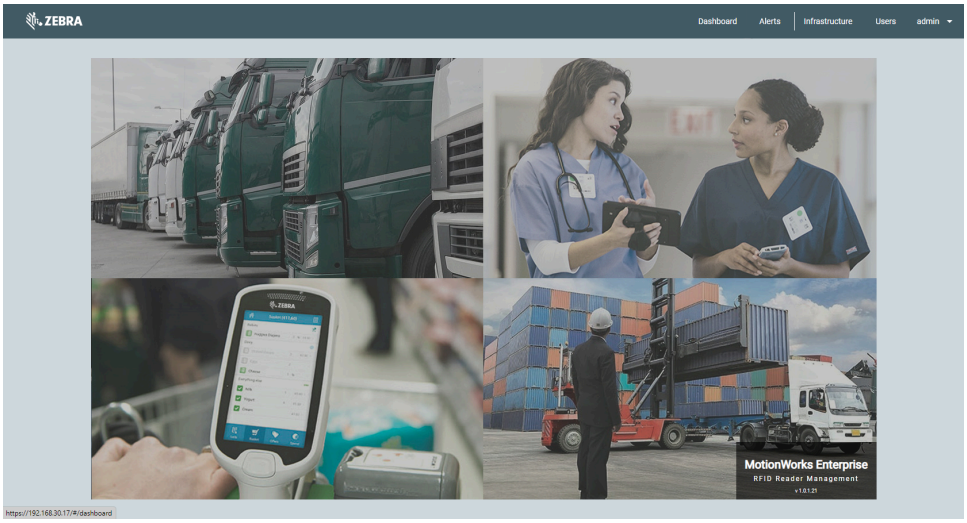
NOTE:

- Only the Google Chrome web browser is supported in Reader Management release 1.0.0; Microsoft Edge and Mozilla Firefox may also work.
- Depending on your version, you may see some differences between the screens depicted in this document and those in your version.

For the initial login, the Reader Management installation script creates an administrator account with the username: admin and password: TriAdmin123, which has administrator access level and access to all menu items in the Reader Management web client. The login account can be a local account created and stored in the local Reader Management database or a domain account authenticated by an OpenLDAP, Active Directory, OIDC, or ADFS server. Refer to the MWE RFID Reader Management Installation Guide for

instructions on configuring authentication modes. The browser may display a not secure or certificate error or a similar warning in the URL bar when using https. The installation script installs a default self-signed certificate on the Reader Management server. After logging in, you should see the landing page with a menu bar at the top. The menu items visible on the menu bar depend on the access level granted to your login account. If you have full access, you should see **Dashboard**, **Alerts**, **Infrastructure**, **Users**, and **admin** in the menu bar.

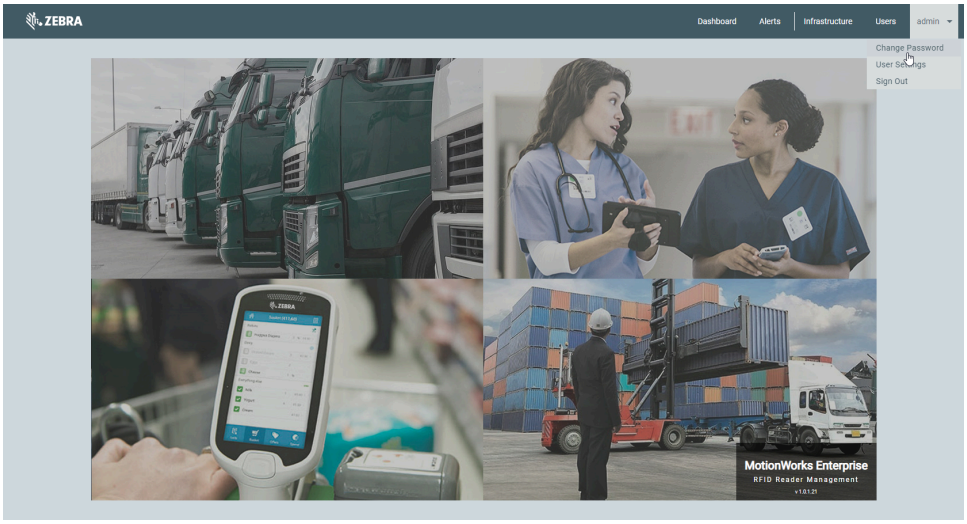
Figure 2 Reader Management Web Client



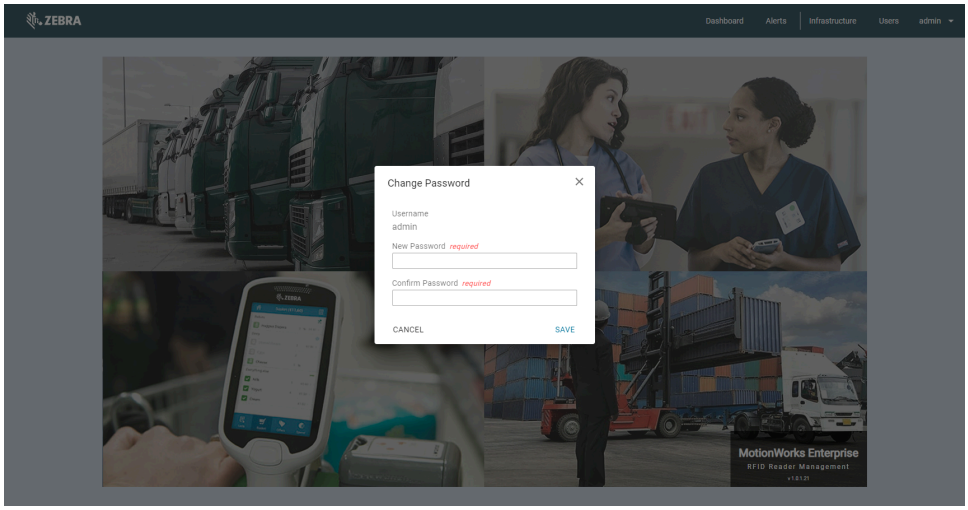
Changing a Password

You can change the account password if you have logged into the Reader Management web client using a local account.

1. Click the **admin** (user name) drop-down menu and select **Change Password**.



2. Enter the new password, and then re-enter the new password to confirm.

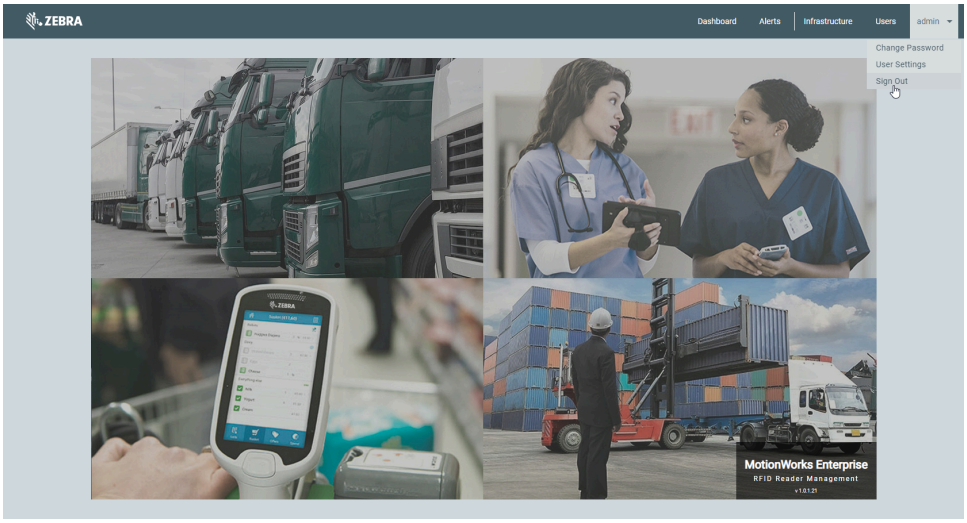


3. Click **Save**.

Signing Out

You can sign out of the Reader Management web client.

From the **admin** (user name) menu, click **Sign Out**.

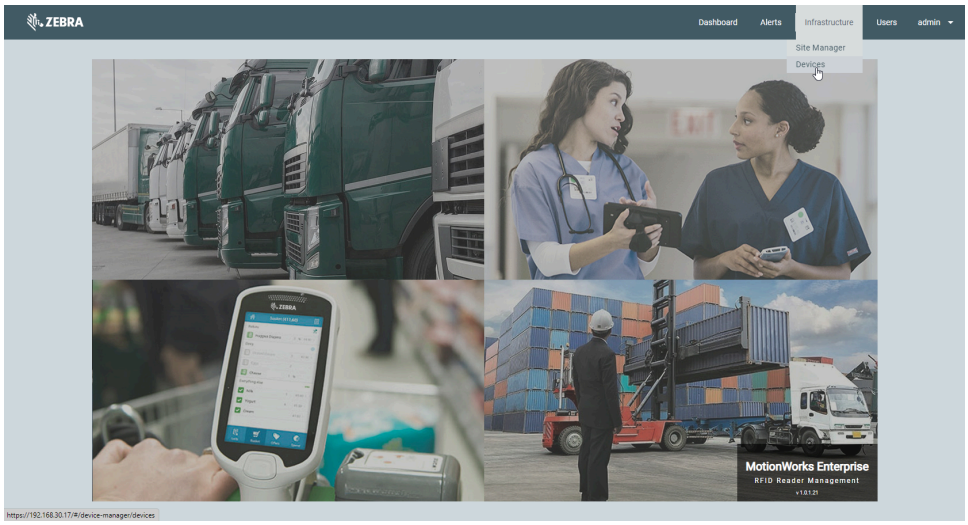


You are returned to the login page.

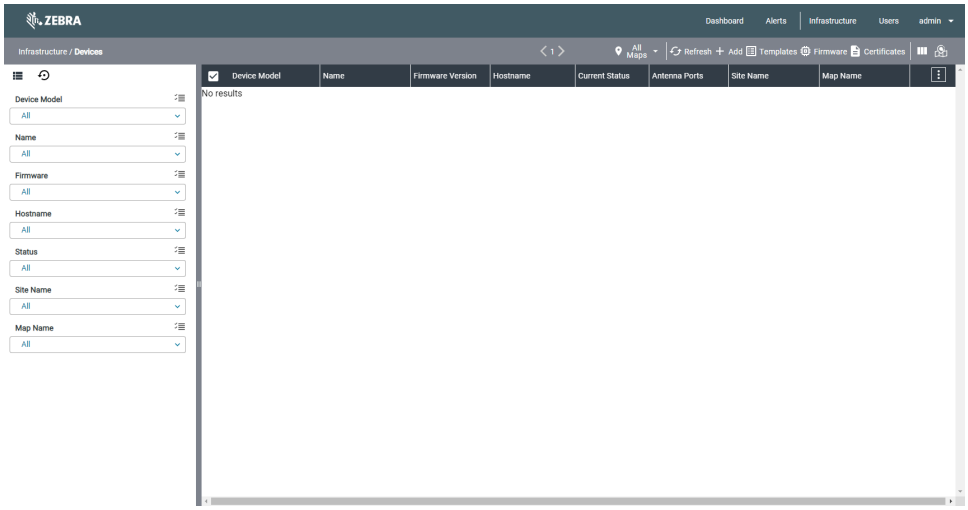
Launching Device Manager

You can launch the Device Manager from the Reader Management web client.

- From the **Infrastructure** menu, click **Devices**.



The first time you open Device Manager, it displays a default set of columns with no devices.



Deploying a Reader

This section explains how to deploy a reader using Device Manager.

Before deploying a reader, go to the reader support page to download the latest firmware for your reader:

- FX7500 go to www.zebra.com/fx7500-info
- FX9600 go to www.zebra.com/fx9600-info
- ATR7000 go to www.zebra.com/atr7000-info

After you log in and connect to the Reader Management web client, you can deploy a reader using the steps outlined:

1. Use Site Manager to add a site and upload a map.
2. Use Device Manager to add a reader.
   a. Assign the reader to a site and map.
   b. Provide an IP address or FQDN.
   c. Specify the number of antennas the reader uses.
   d. Enter the coordinates for the reader and its antennas.
3. Initialize a Reader.
   a. Start the R2C application.
   b. Enable communication between the reader and the Reader Management server or cloud service.
   c. Download the reader certificate.
4. Edit a Reader.
   a. Specify the R2C operation mode.
   b. Specify the operation mode parameters.
5. Publish the configuration settings to a server and a reader.
6. Begin processing tag blink data.

Reader Requirements

MotionWorks Enterprise RFID Reader Management supports the following Zebra RFID readers:

- FX7500
- FX9600

- ATR7000

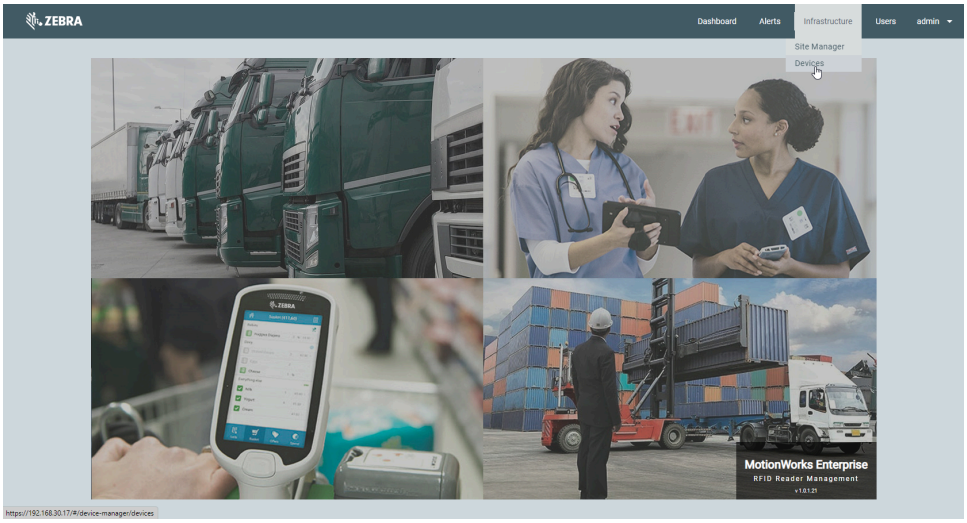
RFID readers must be running firmware version 3.21.23 or later, which includes the Reader to Cloud (R2C) connect application enabling the readers to communicate with the cloud and with a server. If your reader is running a firmware version before 3.21.23, manually update the reader firmware before adding it using Device Manager.

Device Manager displays the firmware version and enables you to upgrade or downgrade the firmware of one or multiple readers simultaneously.

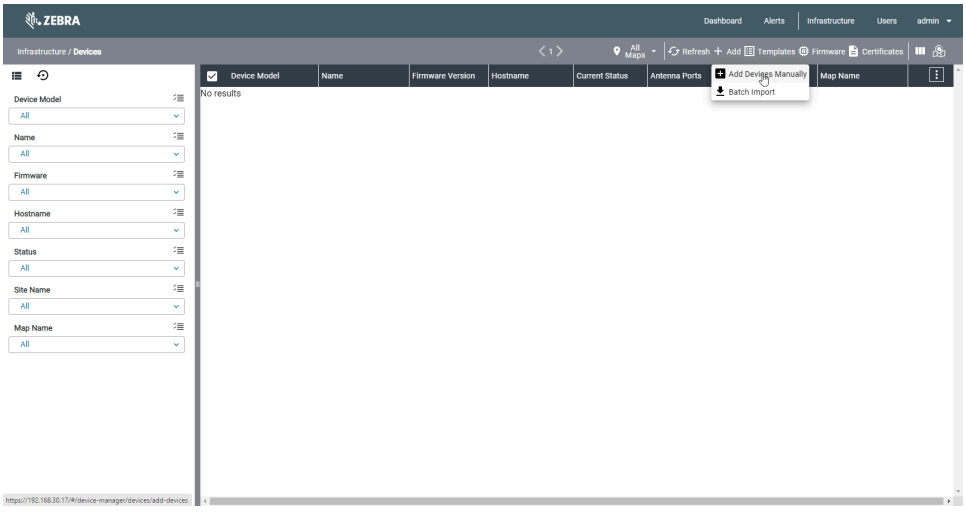
Adding a Reader

This topic describes how to add an RFID reader using the Device Manager.

1. From the **Infrastructure** menu, click **Devices**.

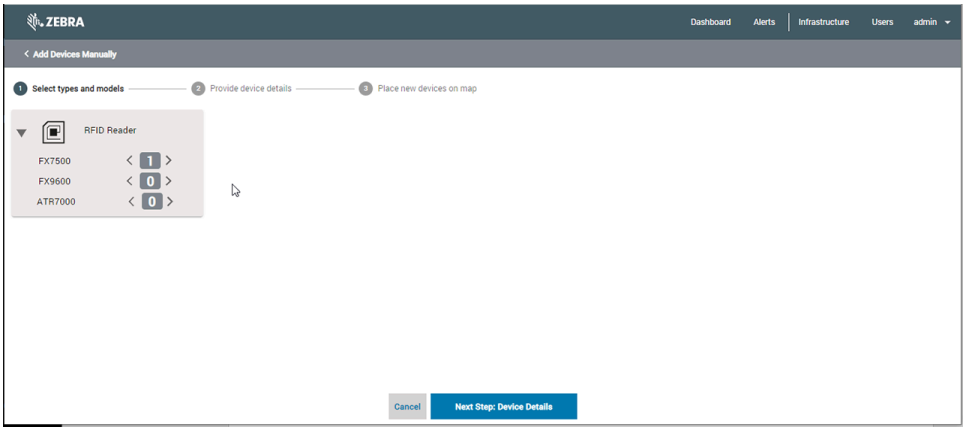


2. Click **+ Add** on the toolbar, and then click **Add Devices Manually**.

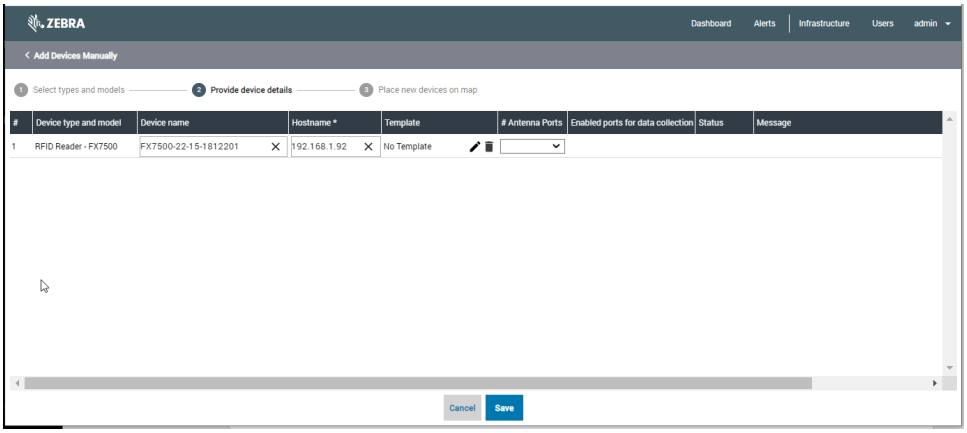


3. Click **RFID Reader** to display the supported reader models.
4. Click **<** and **>** to decrease or increase the quantity of the device type to add.

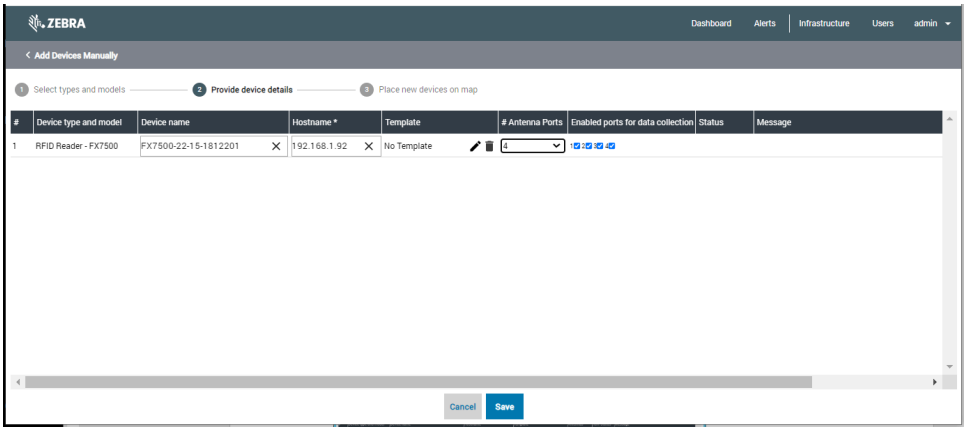
5. Click **Next Step: Device Details**.



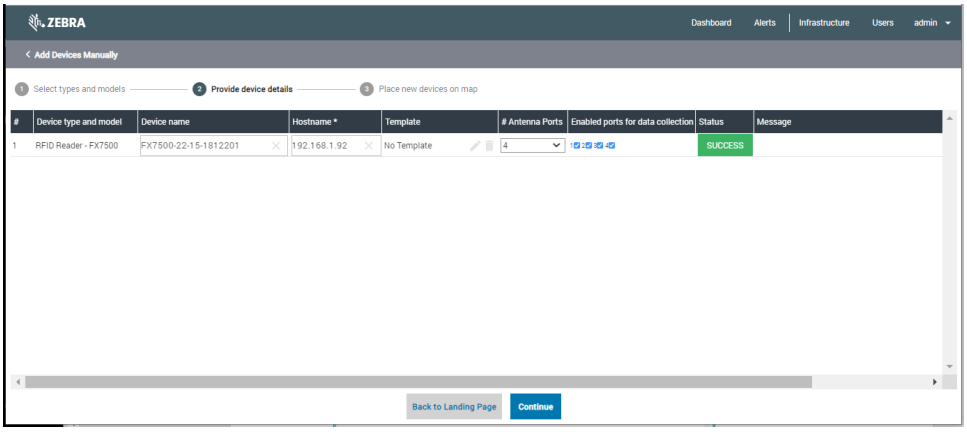
6. The next screen displays the device type, model, and an auto-generated device name that has the form [DeviceModel]_[UniqueNumber] (11-digit date and time stamp). You can change the device name from the device name field. In the **Hostname** field, type the IP address or a fully qualified domain (FQDN) for the device; this IP or FQDN must be reachable from the MWE RFID server, as this server hosts the service that communicates with the devices.



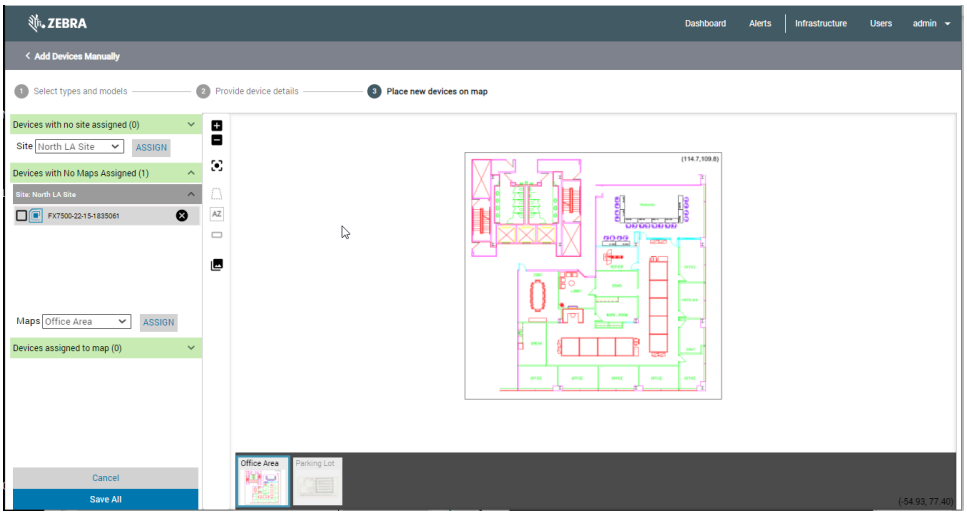
7. In the **# Antenna Ports** column, click the number of ports your reader has from the drop-down list.
8. Click **Save**.



9. A yellow banner showing the operation progress displays for a few seconds, then the **Status** column displays the result.
10. Click **Continue**.



11. Click the checkbox next to the reader.
12. From the **Site** drop-down list select a site.
13. Click **Assign**.

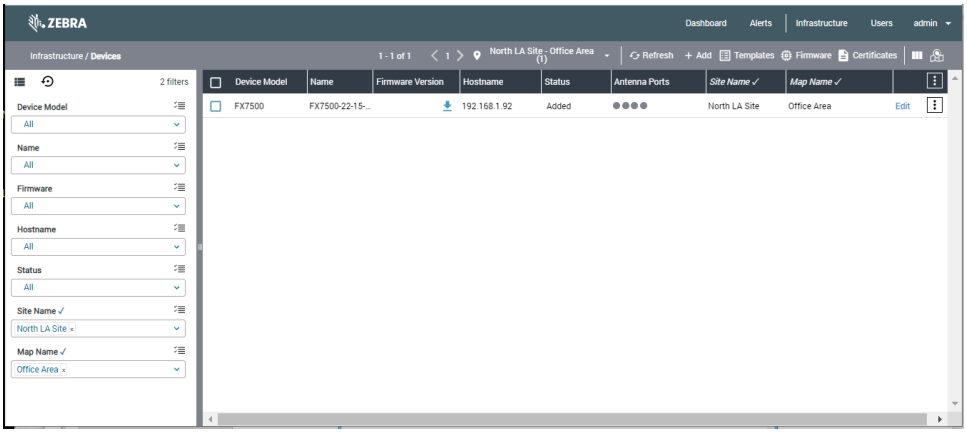


14. Click the checkbox next to the reader.
15. From the **Maps** drop-down list, click a map.
16. Click **Assign**.

    The reader is placed on the map. The coordinates of the reader and each antenna will be shown on the left. By default, the antenna coordinates are the same as the reader coordinates. If you drag the reader to a different location on the map, the coordinates will be updated simultaneously. Deselecting the checkbox labeled **All antennas use with reader position** will allow entering different coordinates for each antenna and will enable you to drag each antenna individually to a different position on the map.

17. Click **Save All** when the reader and its antennas are in position.

    You are returned to the main Devices page, which displays the previously configured devices.



Initializing a Reader

Initializing is a one-time process for readers added in Device Manager.

The initialization process performs the following tasks:

- Stops LLRP application (if running) and loads and starts the R2C application on the reader.
- Adds an MQTT endpoint on the reader pointing to the MWE RFID RM server.
- Pushes a reader certificate from the MWE RFID Reader Management server to the reader.

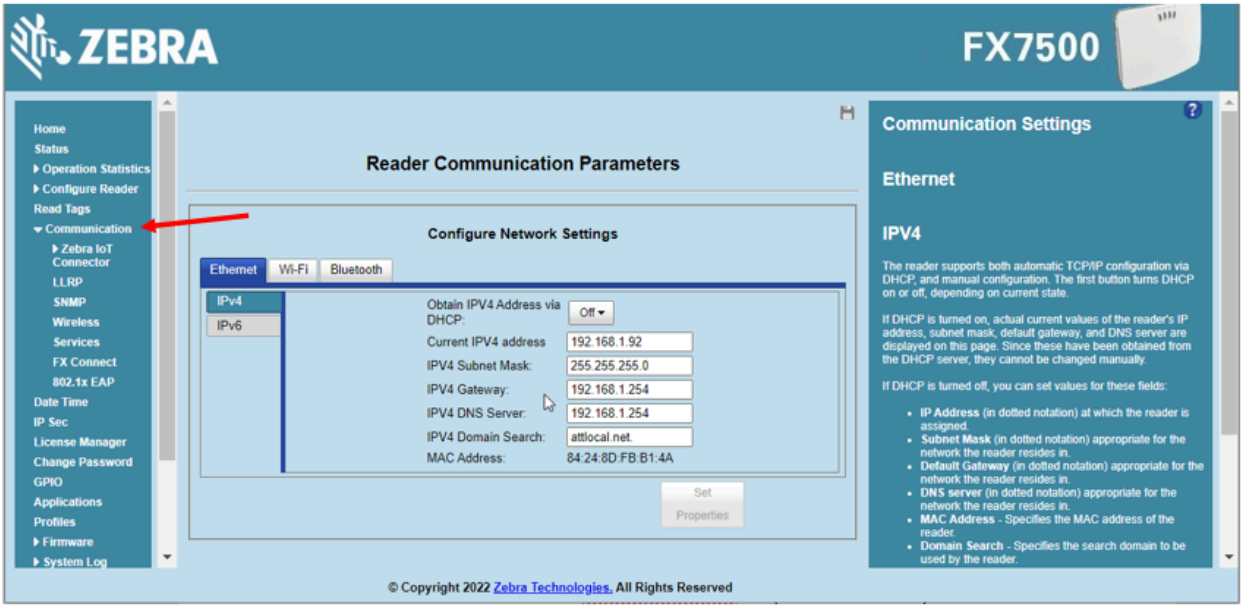
The R2C application enables a reader to communicate with an MWE RFID server or a cloud service. The reader-MWE RFID secure websocket connection is used for reader management commands, retrieving reader status, and pushing configuration changes to the reader. Device Manager allows configuring R2C to use HTTP(S) server or MQTT broker endpoints to post tag blink data to a third-party system or cloud service.

If the MWE RFID server can reach the http / https port on the reader, initialization can be done from Device Manager. If, however, the MWE RFID server is in the Cloud or otherwise cannot reach the http / https port on the reader, the initialization is done using the RFIDReaderInitializer tool, which can be run on any local Windows machine that can access the reader's http / https port.

Before you attempt to Initialize a reader, verify that the reader is powered on and on the network. The MWE RFID server or the RFIDReaderInitializer tool (server in cloud case) should be able to reach port TCP 80 or TCP 443 on the reader. You can view the reader network configuration from the **Communication** menu on the reader web page.

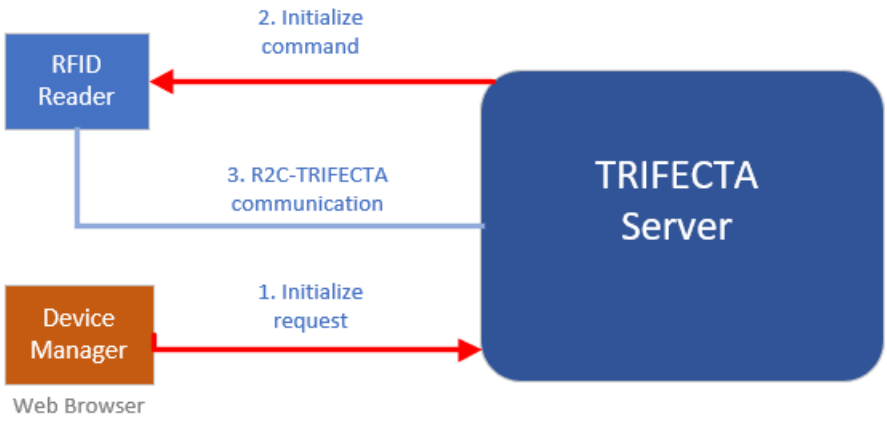
NOTE: You must use a version of the RFIDReaderInitializer tool that is compatible with the MWE RFID RM server version. For example, use RFIDReaderIntializer version 1.0.4.x with MWE RFID RM server version 1.0.4.

Figure 3 Reader Communication Menu

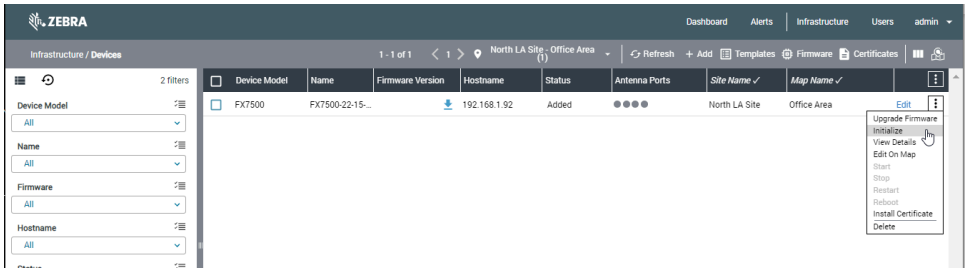


In this case, the MWE RFID server can access either http port 80 or https port 443. Tthe Initialize request is sent from Device Manager to the MWE RFID server, which forwards the Initialize command to the reader. The MWE RFID server tries to connect to port 80 and port 443 on the reader and use whichever port is open. When the reader initialization is done, the R2C application on the reader can communicate back with the MWE RFID server.

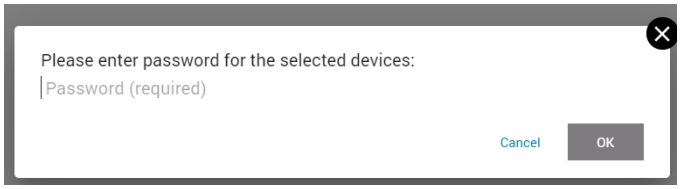
Figure 4 Reader / Server Connection on the Same Network



1. Click ⋮ (in the last column in Site Manager), and then click **Initialize**.

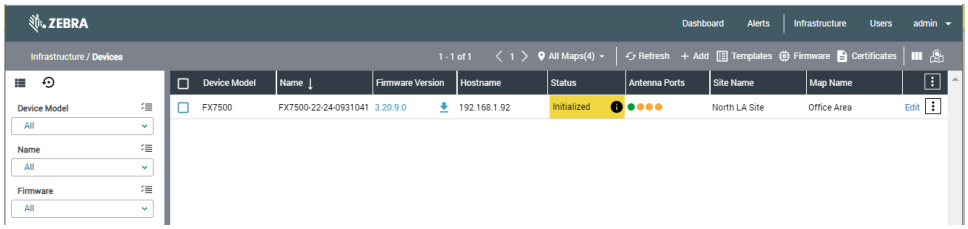


2. Enter the reader password.

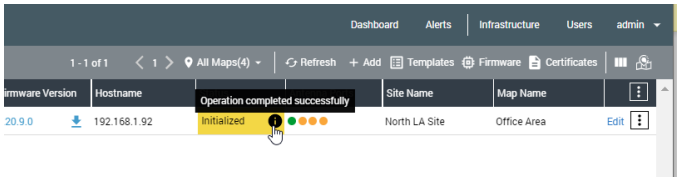


3. Click **OK**.

   The firmware version of the reader displays and Initialized appears in the **Status** column.



   Hovering the mouse over the information icon next to the Initialized status provides information on the results of the initialization process.

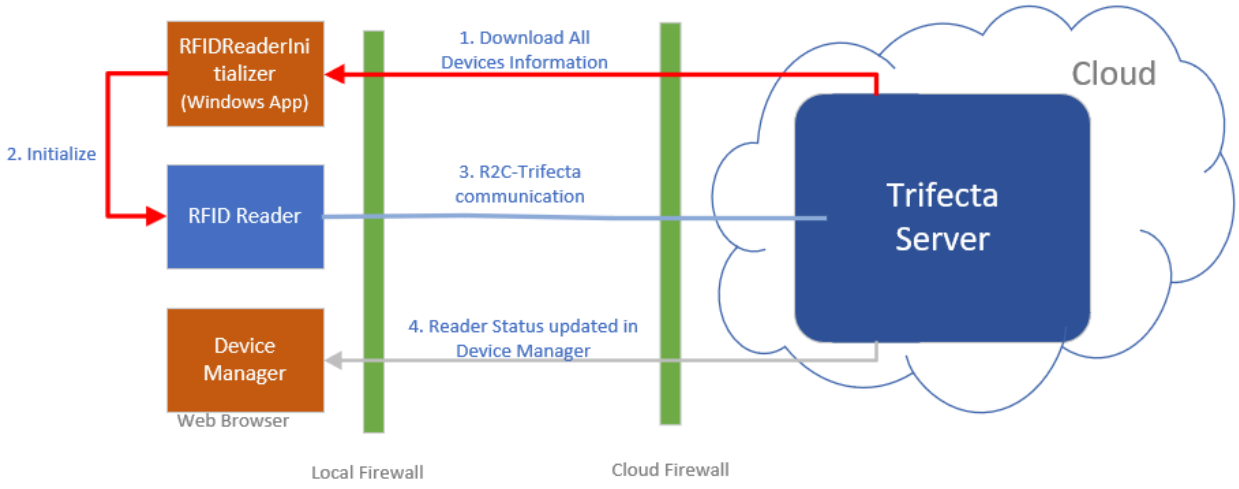


MWE RFID Server in the Cloud

In this scenario, the MWE RFID server cannot directly reach port 80 or port 443 on the readers. A typical example is when the MWE RFID server is in the cloud, and the readers are in a private network behind a firewall. In this case, the RFIDReaderInitializer tool running on a local Windows machine that can reach port 80 or port 443 is used to initialize the readers. This is a one-time step needed when first deploying a reader. The RFIDReaderInitializer application connects to the MWE RFID server, downloads information for all readers added in Device Manager and performs the initialization after contacting the readers on the local network.

After a local reader is initialized, communication between the local reader and the MWE RFID server in the cloud is done via a secure web socket connection, as mentioned in the previous section. The diagram below summarizes these steps.

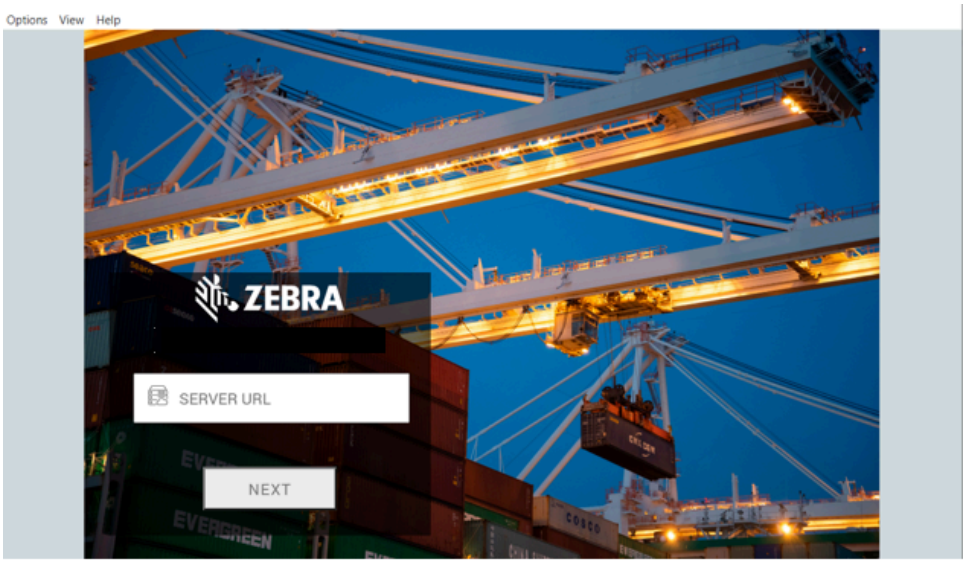
Figure 5 Reader / MWE RFID Server Connection



Communicating with the MWE RFID Server

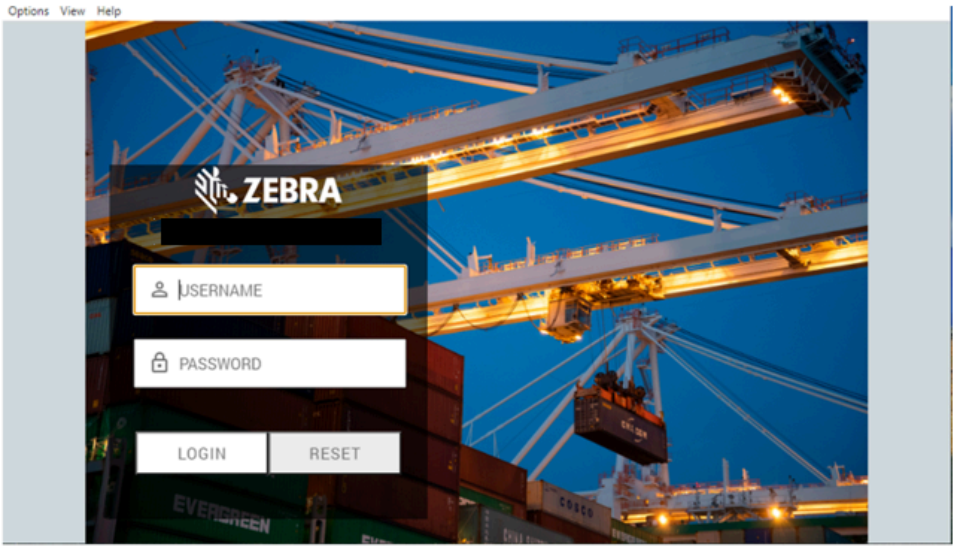
The RFIDReaderInitializer tool is installed via a separate Windows installer.

1. Enter the MWE RFID server URL, the same URL used when launching the Reader Management web client (for example, https://MWE RFID RM.company.com).



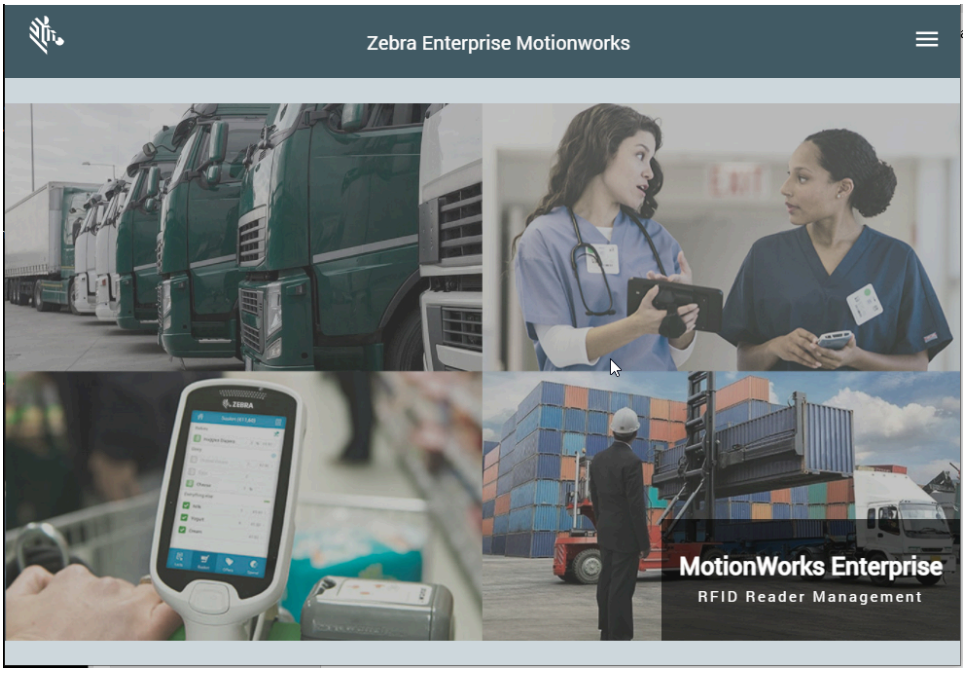
2. Click **Next**.

3. Enter your login credentials, the same credentials you use to login to the Reader Management web client.



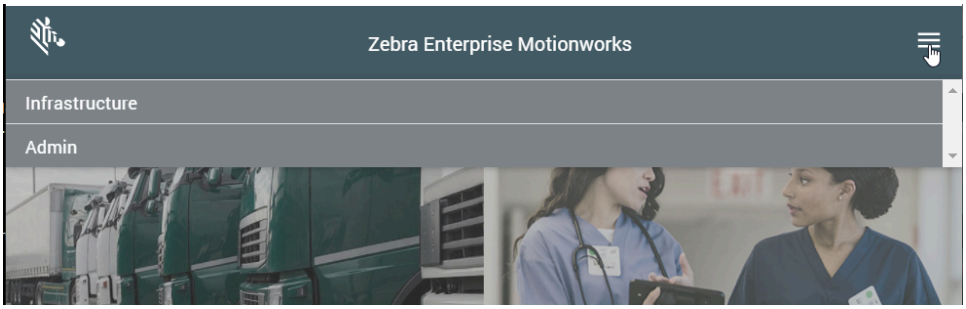
4. Click **Login**.

   The landing page is like the Reader Management web client but has different menu options.

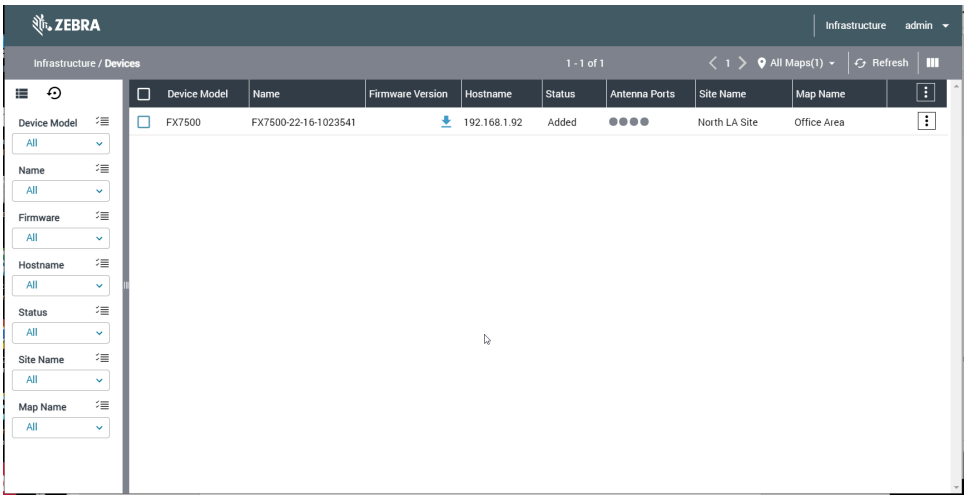


5. Click ☰ on the top right to view the menu options.

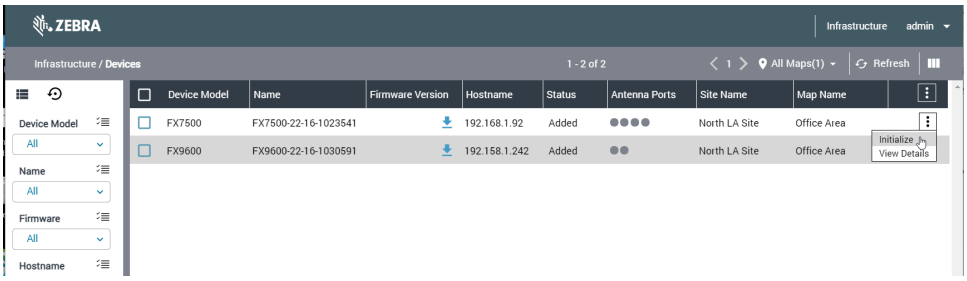
6. Click **Infrastructure** > **Devices** to open the Device Manager page.



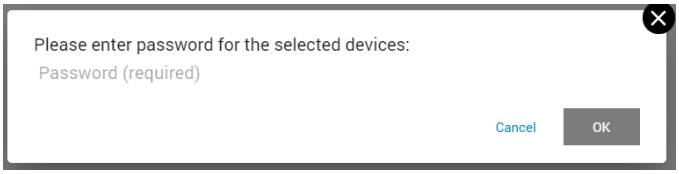
The Devices page is like the Reader Management web client with limited menu items and functionality.



7. Click ⋮ > **Initialize**.

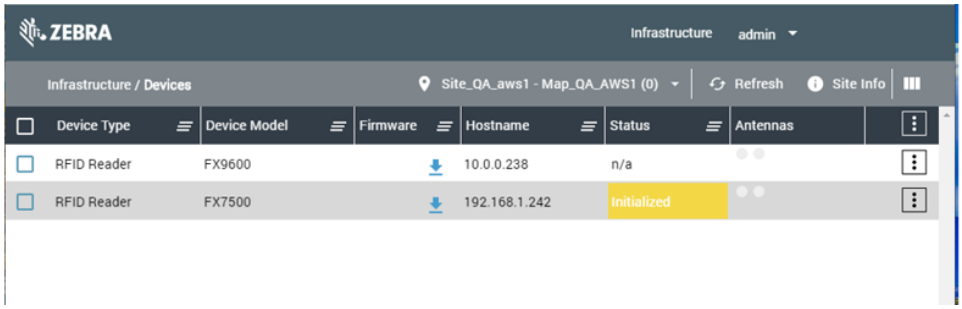


8. Enter the reader password.



9. Click **OK**.

10. After a few seconds, the **Status** column displays **Initialized**.

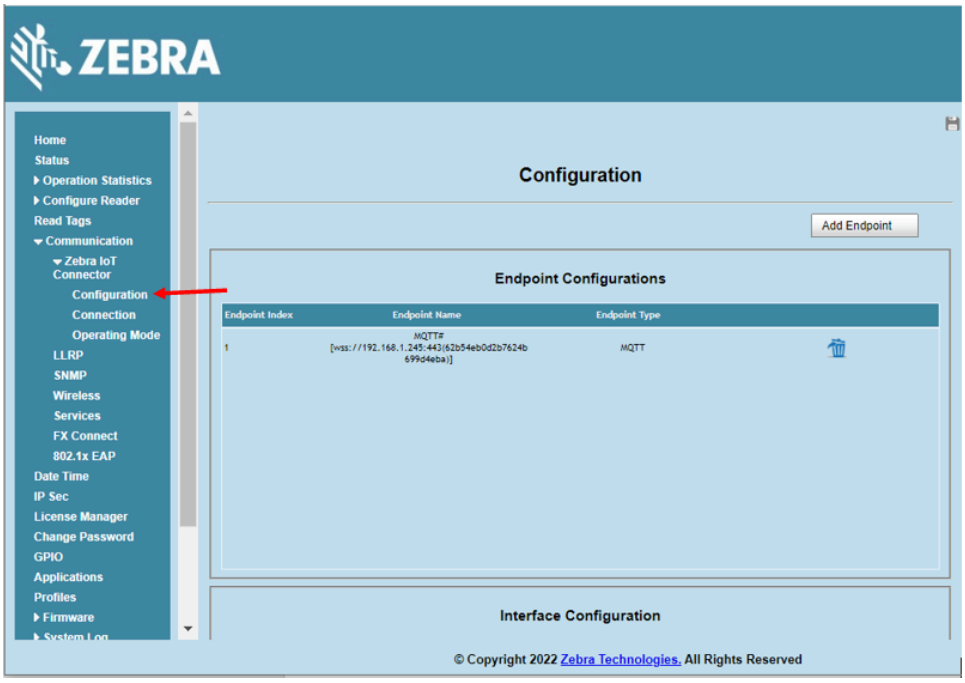


The **Status** column in Device Manger also displays Initialized.

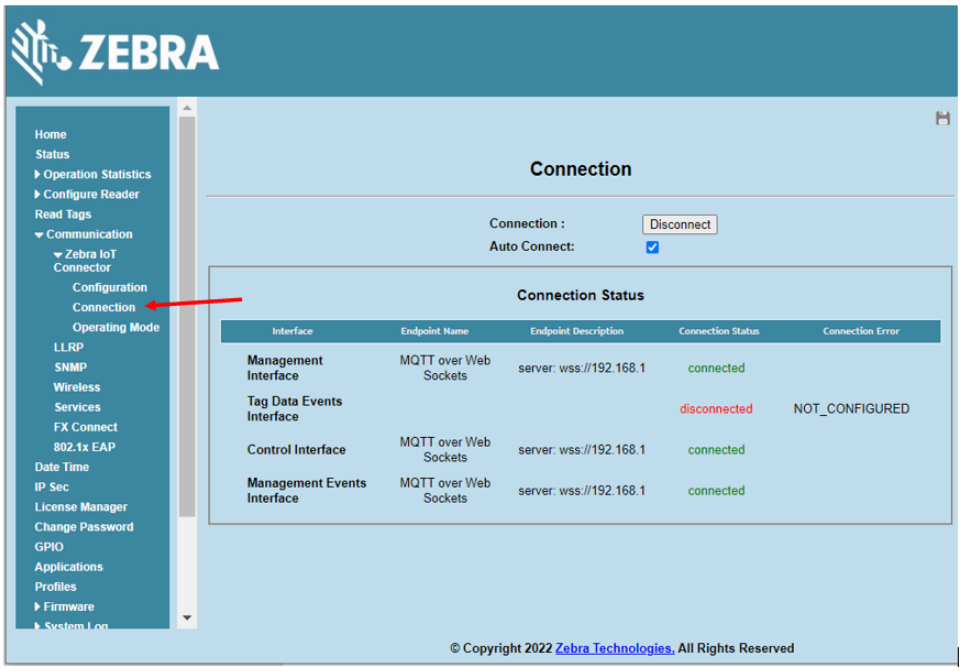
Verifying Connections

You can verify the connection endpoints on the reader.

1. From the **Communications** menu, click **Zebra IoT Connector** > **Configuration** .



2. To show the current reader connections, click **Connection**.



Manually Upgrading Firmware

Go to the reader support page to download the latest firmware for your reader:

- FX7500 go to www.zebra.com/fx7500-info
- FX9600 go to www.zebra.com/fx9600-info
- ATR7000 go to www.zebra.com/atr7000-info

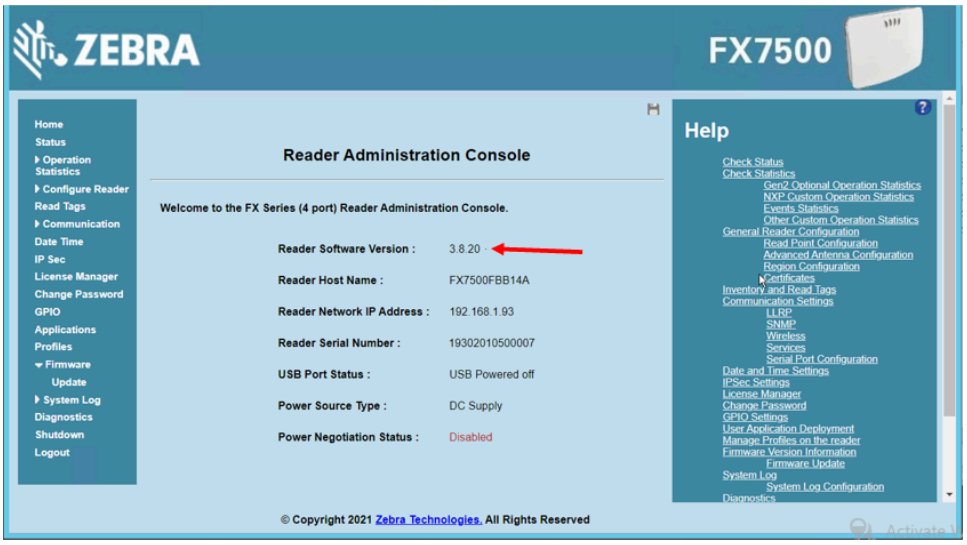
You must unzip the firmware file before updating the reader.

NOTE: If you cannot connect to the reader using https, try using http.

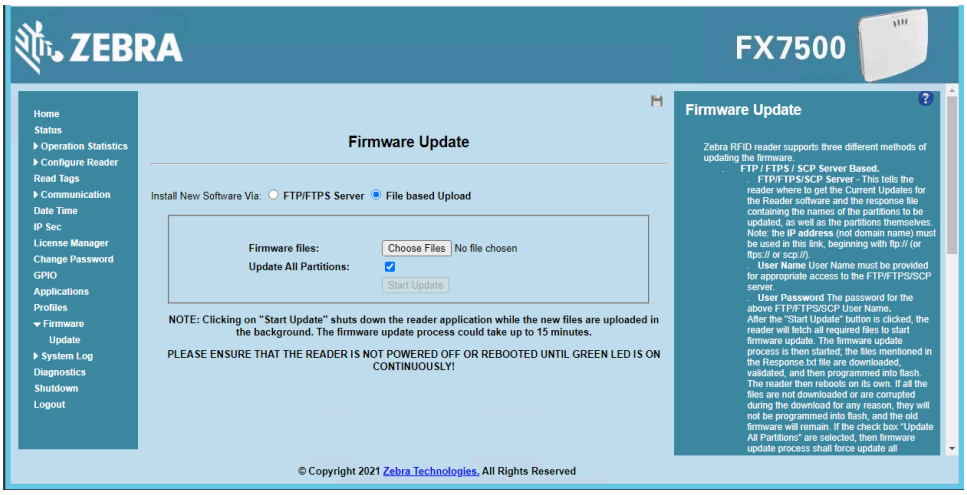
To verify the firmware version on your reader, login to the reader home page on a web browser. Using the IP address of the reader, go to https://[reader IP address]. The default login credentials are admin / change; depending on the firmware version, you may be prompted to change the password.

The home page displays the reader software version loaded on the reader.

Figure 6 Reader Administration Console



1. From the menu, click **Firmware** > **Upgrade**. Follow the instructions on the right-side panel.

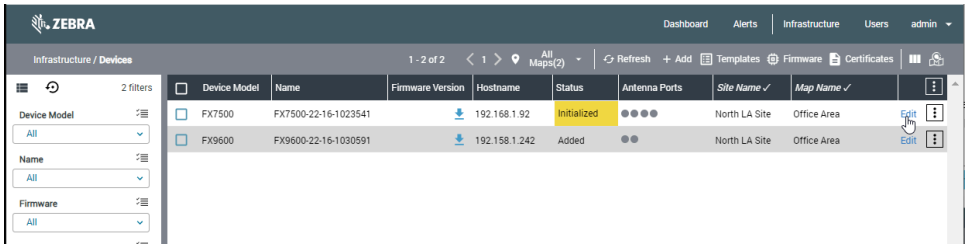


2. Click **Choose Files**.
3. From the **Open File** dialog box, browse to the location of the previously downloaded firmware files and select them. Then click **Open**.
4. Click the **Update All Partitions** checkbox.
5. Click **Start Update**.

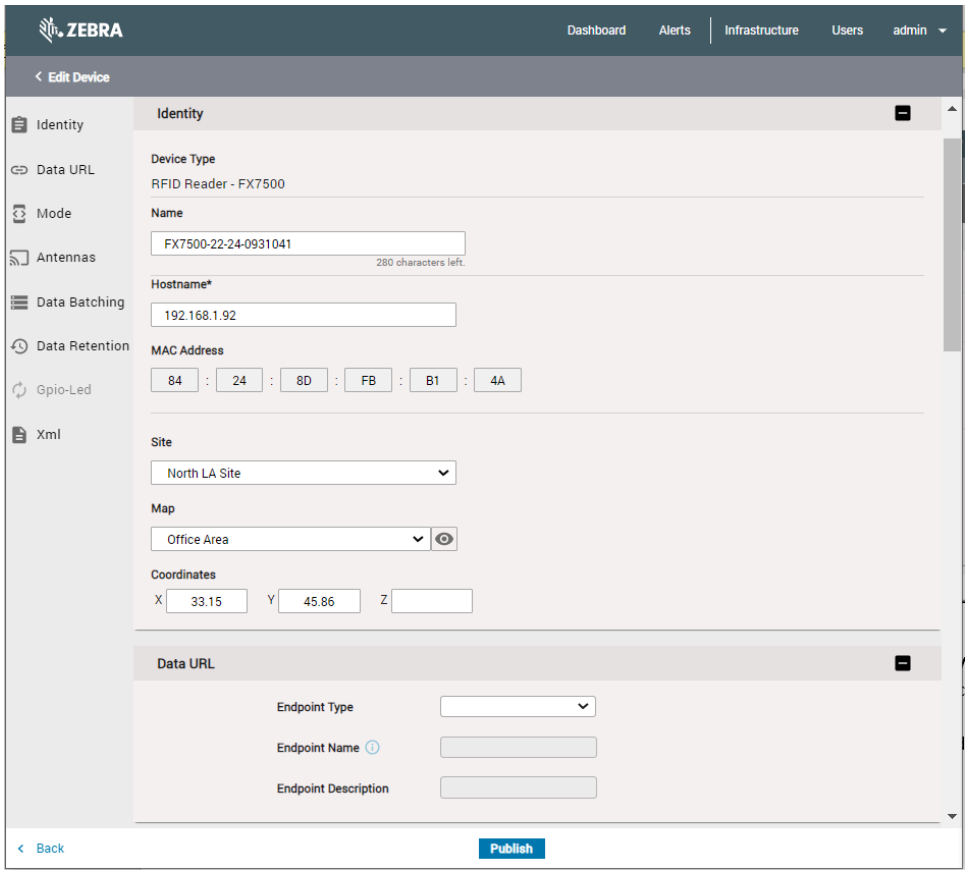
Editing a Reader

The Edit Device window is used to set the operation mode and other parameters for the reader to collect data.

1. Click **Edit**.



2. The **Edit Device** page opens.



The **Edit Device** page has the following sections:

- Identity
- Data URL
- Mode
- Antennas
- Data Batching

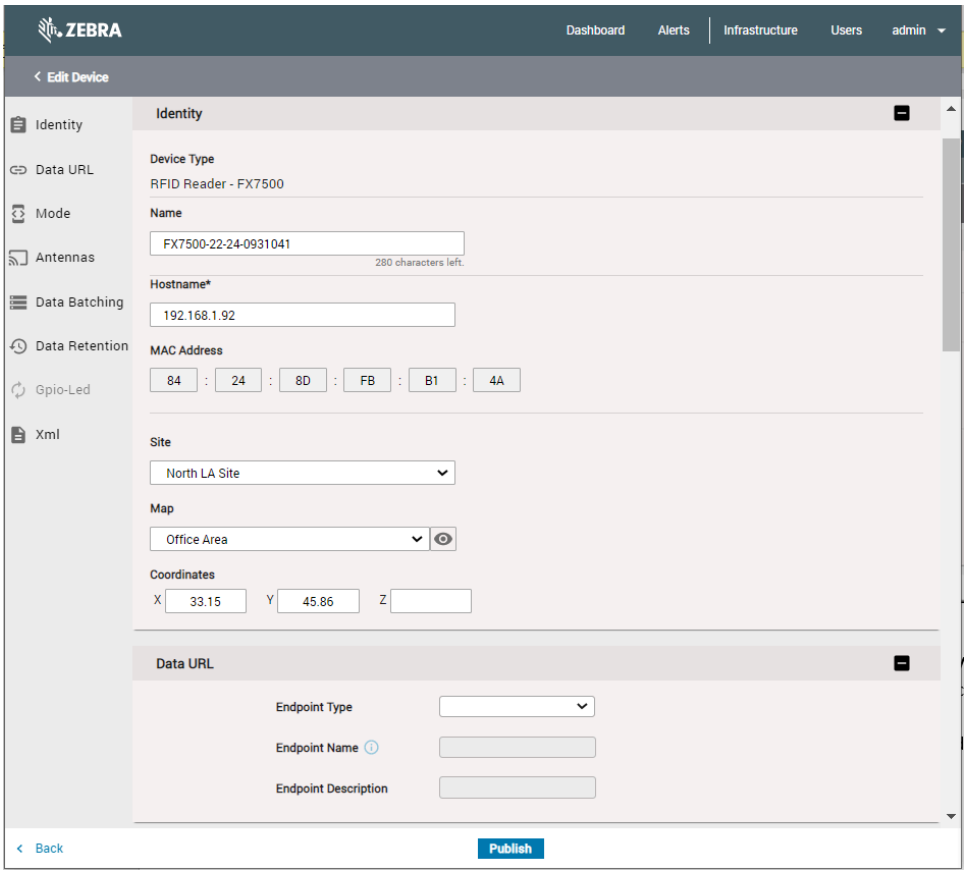
- Data Retention
- GPIO-LED
- XML

Identity

This section includes Device Type, Name, Hostname, MAC address, Site, Map, and the x,y,z coordinates of the reader.

NOTE: Some fields are editable.

Figure 7 Identity Section



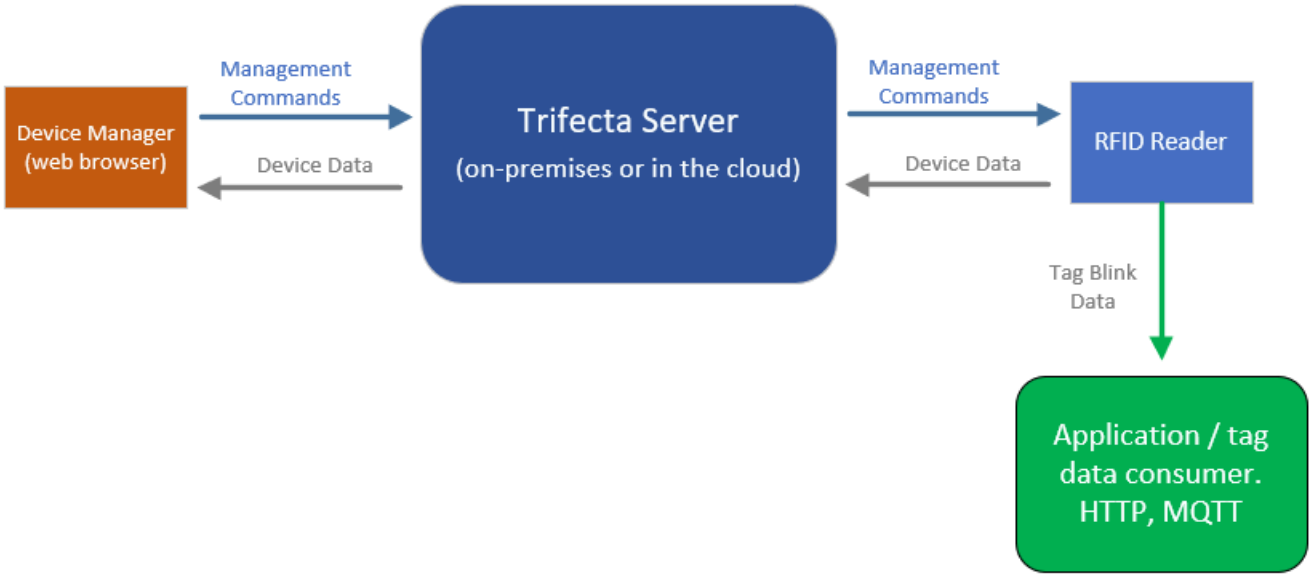
Data URL

In the Data URL area, specify where the RFID reader tag blink data is forwarded/posted.

The **Endpoint Type** drop-down list offers two options: HTTP and MQTT Post.

The following figure shows how blink data is forwarded.

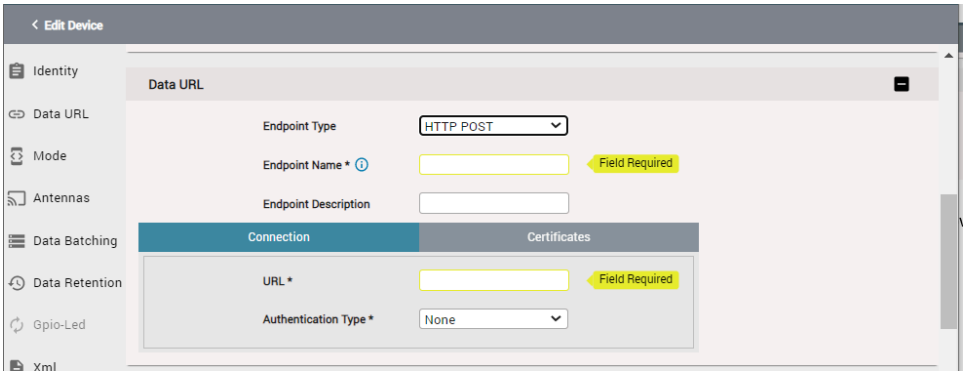
Figure 8 Blink Data Forwarding



HTTP Post Endpoint

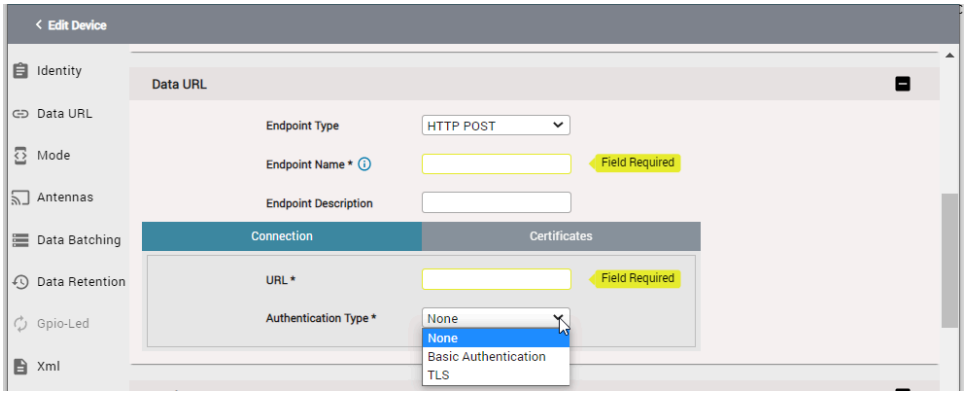
When you select the HTTP Post endpoint type, two additional tabs are displayed: **Connection** and **Certificates**.

Figure 9 HTTP Post Endpoint



An asterisk (*) next to a field name indicates that the field is mandatory. In the **Connection** tab, type an Endpoint Name and Endpoint Description of your choosing. In the **URL** field, specify the actual URL of the HTTP server. For **Authentication Type** there are two options: **Basic Authentication** and **TLS**.

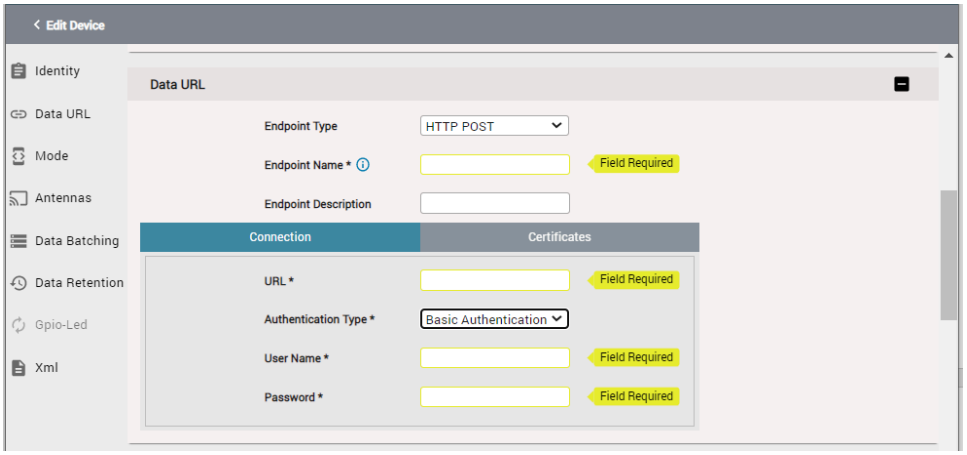
Figure 10 HTTP Post Endpoint Authentication Type



Basic Authentication

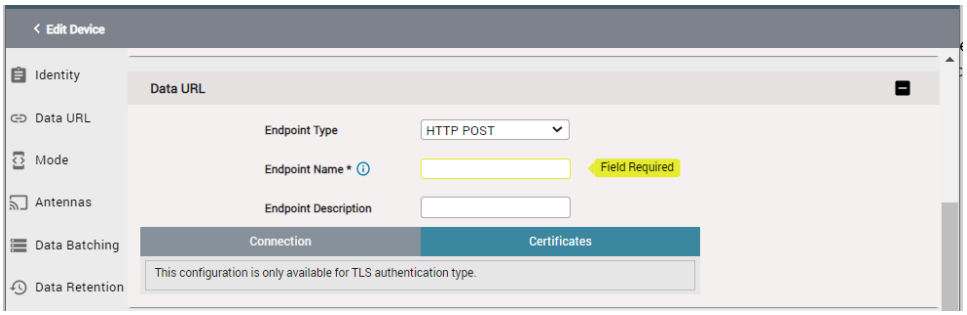
Selecting **Basic Authentication** displays additional fields. Enter a user name and password that the reader will use to login to the remote HTTP server.

Figure 11 HTTP Post Endpoint Basic Authentication



This authentication mode does not require a certificate. Clicking the Certificates tab will display the message: This configuration is only available for TLS authentication type.

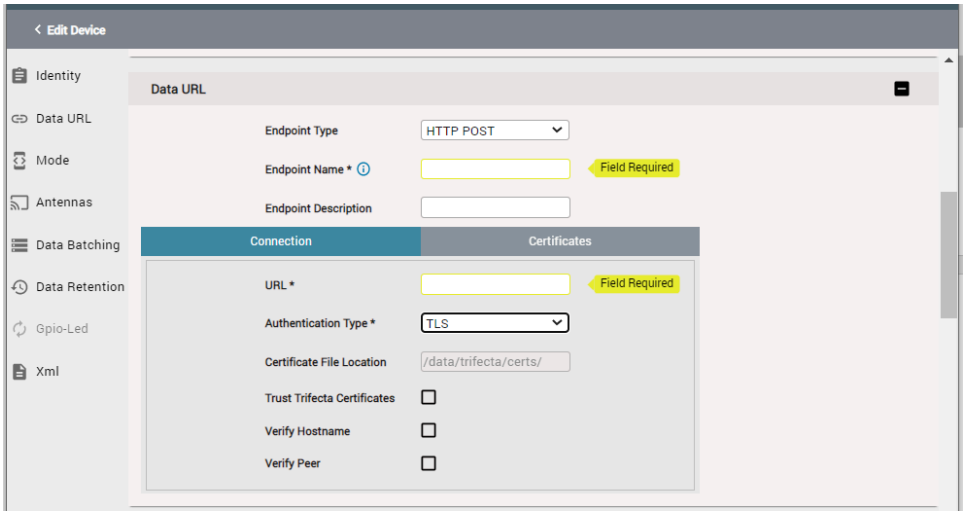
Figure 12 HTTP Post Certificates



TLS

Selecting **TLS** authentication type will display additional fields.

Figure 13 HTTP Post Endpoint TLS Connection



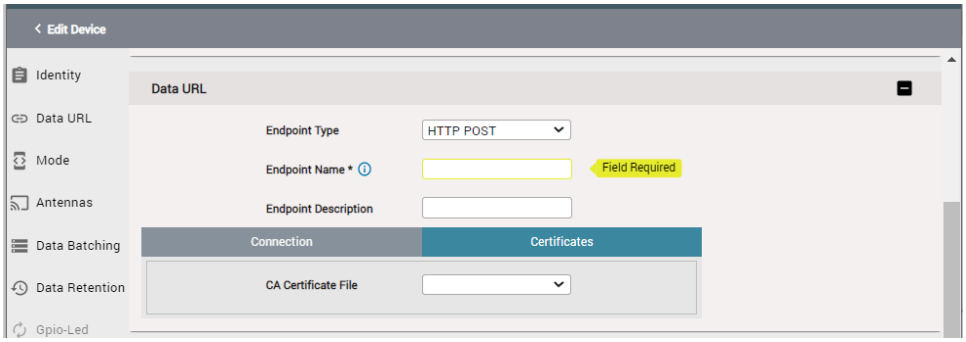
The **Certificate File** Location displays the location on the MWE RFID server for the certificates that you have uploaded. Uploading a certificate copies the certificate to the indicated path; it does not apply the certificate to a reader.

Checking the **Trust Trifecta Certificates** checkbox instructs the reader to use the same certificate it uses to connect to the MWE RFID server (for management purposes) when connecting to the HTTP server (for posting tag blink data). For this to work, you must install on the HTTP server the same certificate being used on the MWE RFID server.

The Verify Hostname and Verify Peer options are well-known options of the handshake TLS protocol.

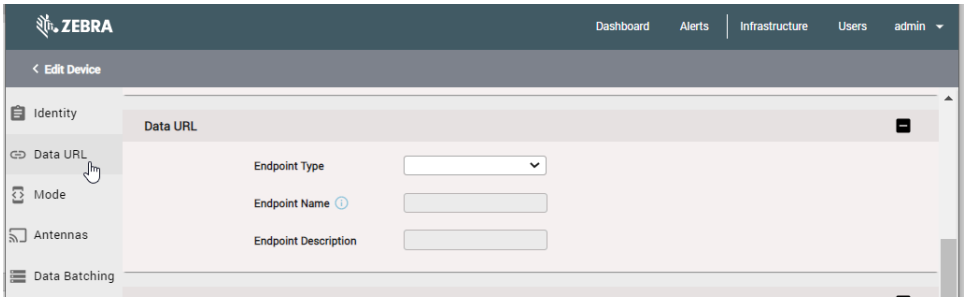
To choose a specific certificate for a reader, click the **Certificates** tab and select a certificate from the dropdown list. If no certificates have been uploaded to the MWE RFID server, the list will be empty. Refer to Uploading a Certificate for instructions on how to upload a certificate to the MWE RFID server.

Figure 14 TLS Connection Certificates



NOTE: If you use a self-signed certificate, you cannot select the **Verify Hostname** and **Verify Peer** checkboxes. Using a valid CA certificate, you can choose whether to click these checkboxes.

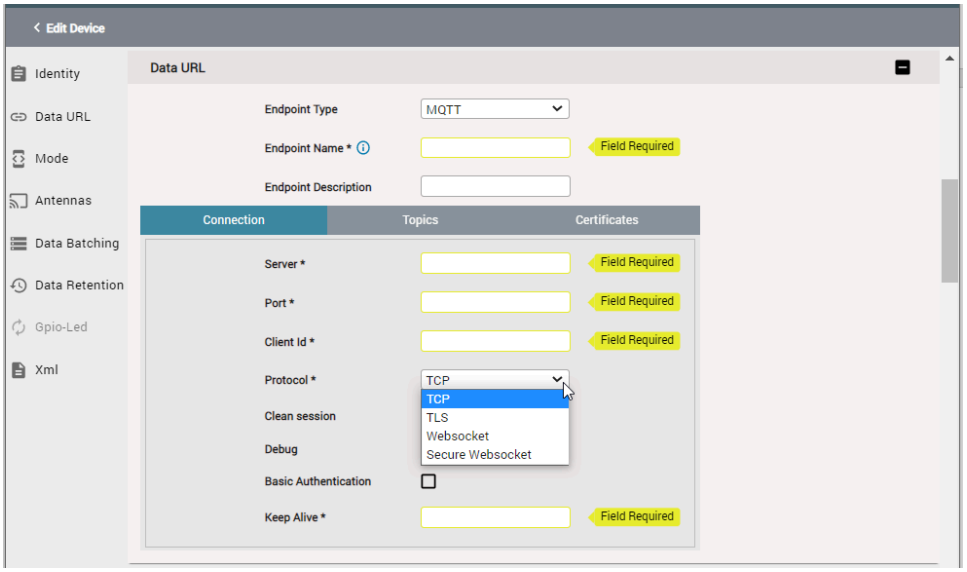
Figure 15 Data URL



MQTT Endpoint

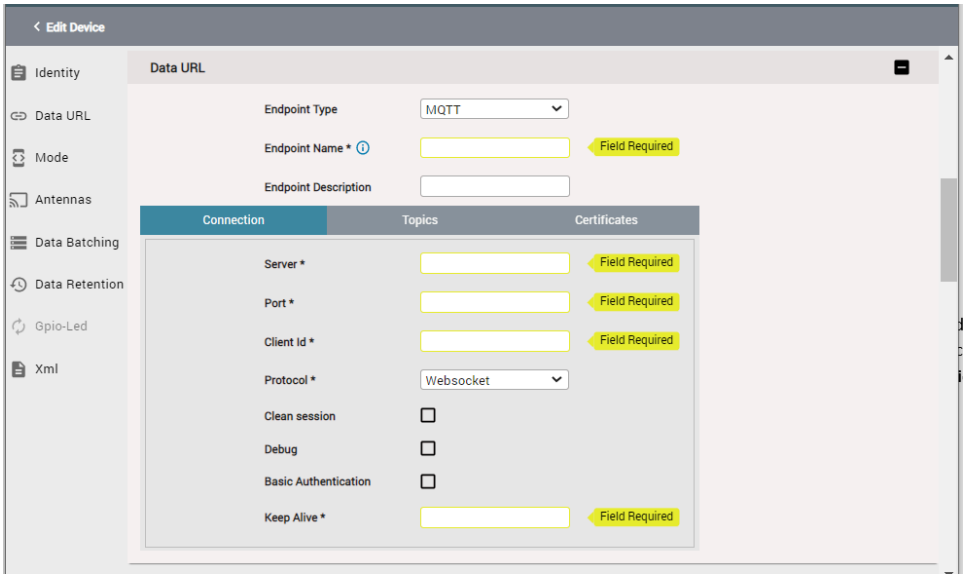
When you select the MQTT endpoint type, you will see additional fields in three tabs: Connection, Topics, and Certificates. The set of fields displayed in the Connection and Certificates tabs will depend on the protocol you select in the **Protocol** drop-down list. The protocol options are TCP, TLS, Websocket, and Secure Websocket.

Figure 16 MQTT Endpoint



For the TCP and Websocket protocols, the fields in the Connection tab are shown in the following figure.

Figure 17 MQTT Data Endpoint Connection



An asterisk (*) next to a field name indicates that the field is mandatory, and you must provide a value. Type an Endpoint Name and Endpoint Description of your choosing. Provide the server IP address or FQDN in the Server field. Specify the Port number and Client id in the provided fields. Other parameters in the Connection tab and Topics tab are known standard parameters for an MQTT server and will not be explained in this document. The following figures show the Topics and Certificates tabs.

Figure 18 MQTT Data Endpoint Topics

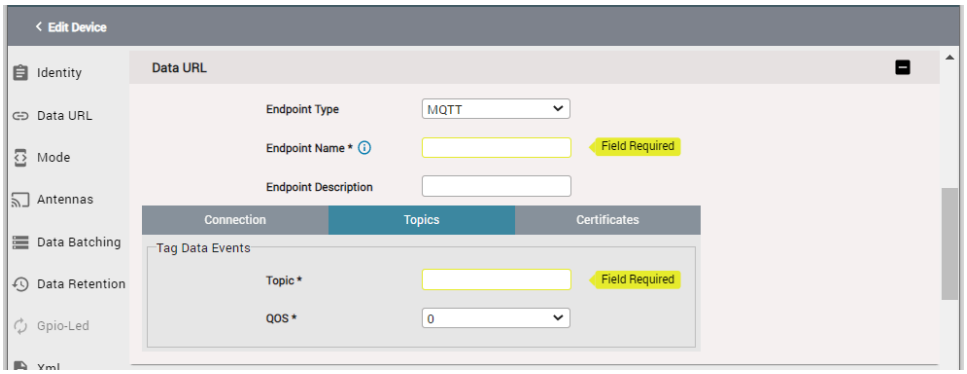
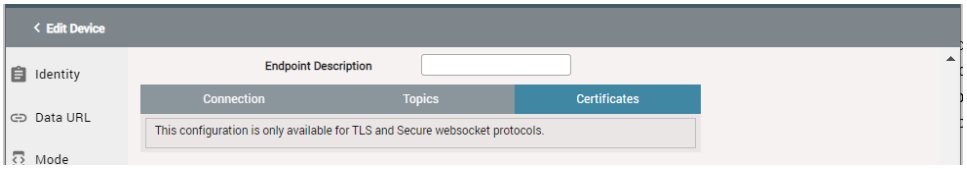


Figure 19 MQTT Data Endpoint Certificates



For the TLS and Secure Websocket protocols, the fields in each tab are shown in the following figures. All these fields have been previously mentioned in this section.

Figure 20 MQTT Data Endpoint

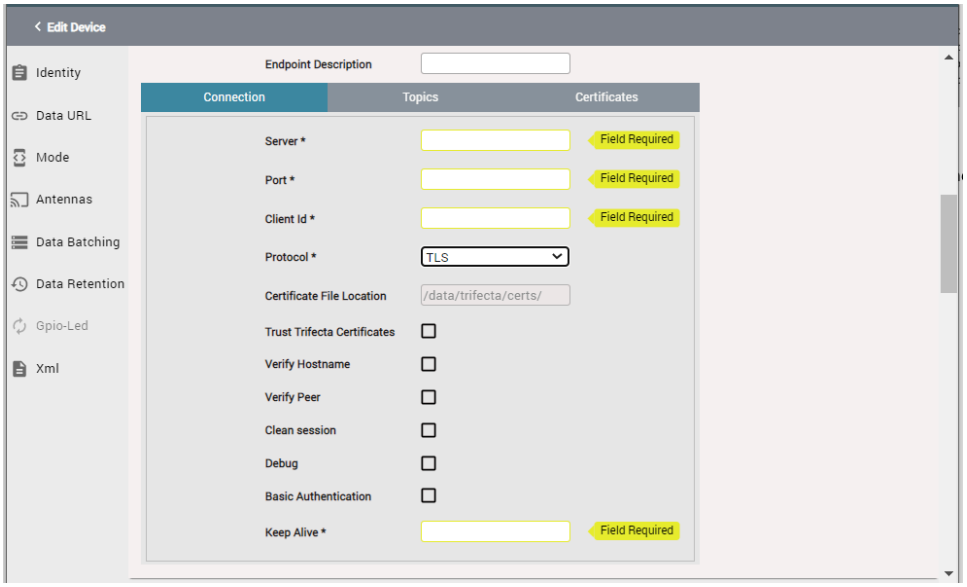


Figure 21 NQTT Data Endpoint

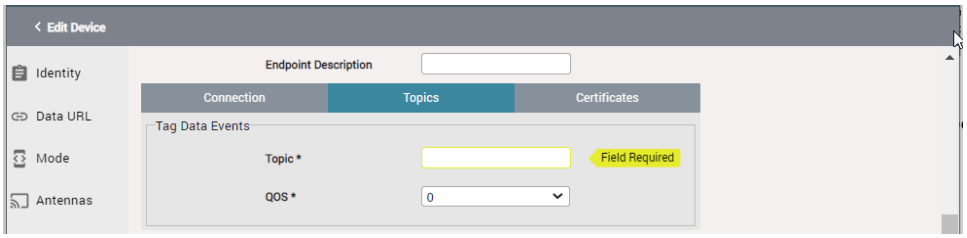
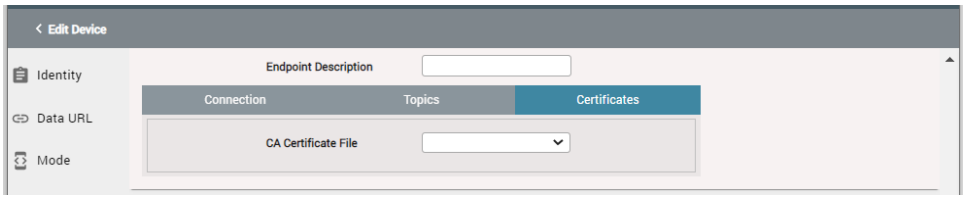


Figure 22 MQTT Data Endpoint

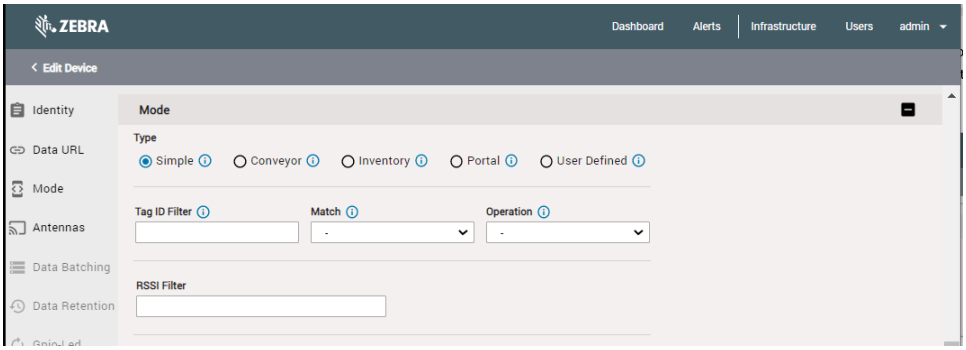


Mode

An operation mode is a set of configuration parameters that define how a reader collects and processes data from passive RFID tags.

There are four predefined operation modes corresponding to common scenarios or use cases: Simple, Conveyor, Inventory, and Portal. Additionally, there is the more flexible User Defined mode that allows uploading a custom configuration file (JSON format).

Figure 23 Mode



You can see a brief description of each mode by hovering the mouse pointer over the information icon.

When you select an operation mode in the **Edit Device** window (figure above), a set of corresponding filters or parameters is displayed, all blank by default.

Simple Mode

Simple mode configures the reader radio component to read and report all unique tags in the radio's field of view (FOV). Each tag ID is reported a single time. If a tag leaves the FOV and comes back, it will be reported a single time again. This mode does not report the ID of the antenna reading a tag ID.

By default, the radio attempts to read tags on all antennas and reports all unique tags. On the **Edit Device** page, you can enable/disable antennas, adjust antenna power, apply a tag ID filter, and more.

The Simple mode, as well as the other predefined modes, includes a Tag ID Filter consisting of three fields:

Figure 24 Simple Mode

- Tag ID Filter: string value to match in the tag ID
- Match: Selectable values are Prefix, Sufix, and Regex (regular expressions)
- Operation: Selectable values are Include, Exclude

All four predefined modes also include an RSSI Filter to filter out blinks with weak RFID signal strength.

Figure 25 RSSI Filter

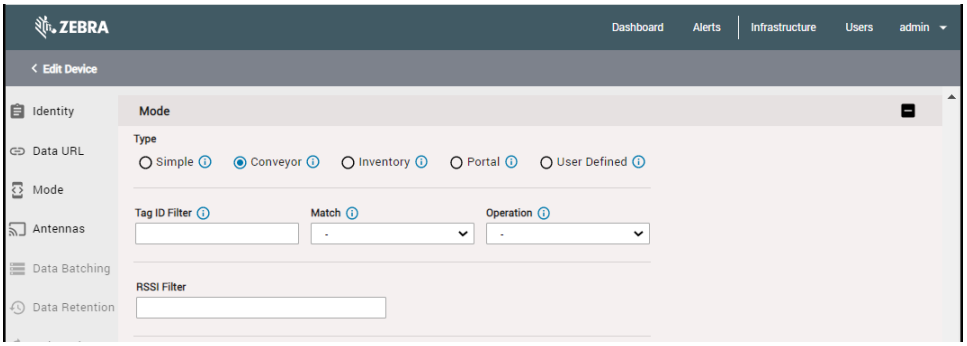
Use this filter to report only tags within a certain radius of the reader. RSSI is specified as a negative value typically in the range -40 to -80. If left blank, tag reads will be reported regardless of signal strength.

Conveyor Mode

Conveyor mode configures the radio to read and report all unique tags for each antenna. It is like Simple mode, but the reader also reports the antenna that read each tag. Each tag ID is reported a single time. If a tag leaves the FOV and comes back, it will be reported a single time again.

By default, the radio attempts to read tags on all antennas and reports all unique tags. In the Edit Device page, you can configure a Tag ID filter, an RSSI filter, enable/disable antennas, adjust antenna power, and more.

Figure 26 Conveyor Mode

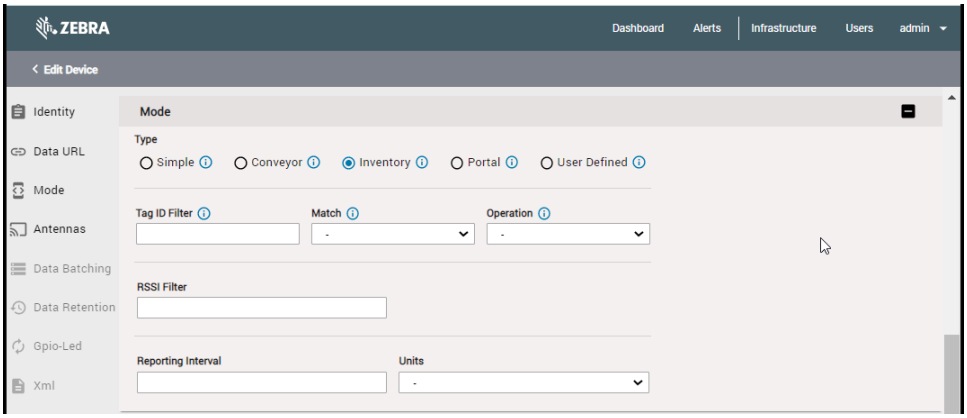


Inventory Mode

Inventory mode configures the radio to read tags and report all unique tags for each antenna on a periodic interval. Antenna ID and additional meta-data (that is, peak RSSI and number of reads for each antenna during the interval) are reported.

By default, the radio attempts to read tags on all antennas; it reports all unique tags (once in the interval) and reports tags every second. In the **Edit Device** page, you can adjust the reporting interval, configure a Tag ID filter, an RSSI filter, enable/disable antennas, adjust antenna power, and more.

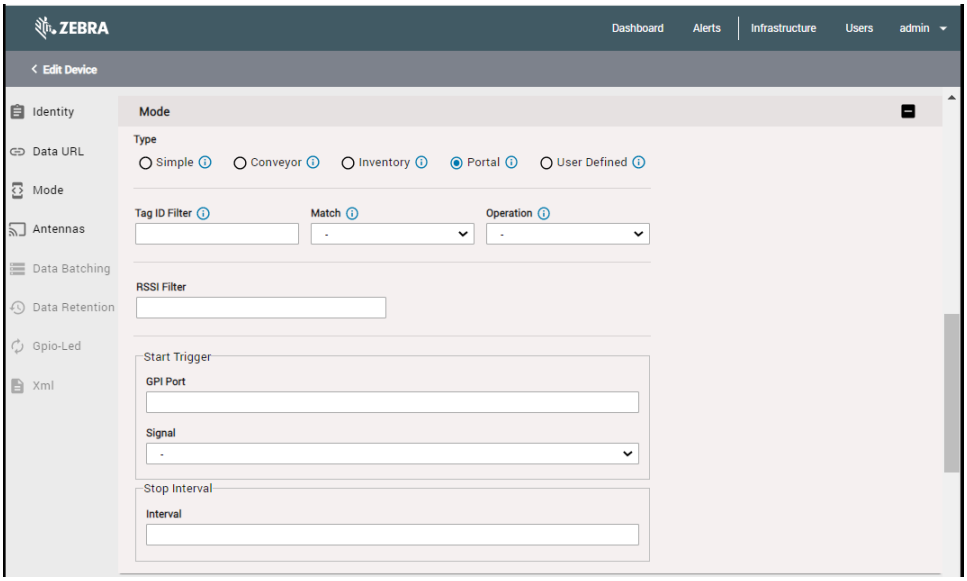
Figure 27 Inventory Mode



Portal Mode

Portal mode configures the radio to report all unique tags that pass by each antenna immediately following a general purpose input (GPI) event. The GPI event signals the beginning of the read period. As soon as the GPI event triggers the radio, the radio reads tags until no new unique tags are read for a configurable stop interval. When the radio stops reading tags, it waits for the next GPI event to start the process again.

Figure 28 Portal Mode



By default:

- The radio attempts to read tags on all antennas. This can be adjusted using the antenna settings in the Edit Device page.
- The radio reports all unique tags (once). This can be adjusted using the tag ID filter in the Edit Device page.
- The radio waits for a LOW signal on GPI 1. This can be changed using the Start Trigger (GPI Port and Signal parameters) in the Edit Device page.
- The radio continues to read until no new unique tags have been read for 3 seconds. This can be adjusted using the Stop Interval parameter in the Edit Device page.

User Defined Mode

This mode offers greater flexibility by allowing the modification of a larger number of parameters. There are two options available in this mode:

- JSON File: The custom configuration file is uploaded in JSON format. Click **Show Example** to see a sample file.
- Fill Form: Here, you can adjust the values of different parameters directly on a form.

The following figures show the user interface for each option.

Figure 29 User Defined Mode-Fill Form

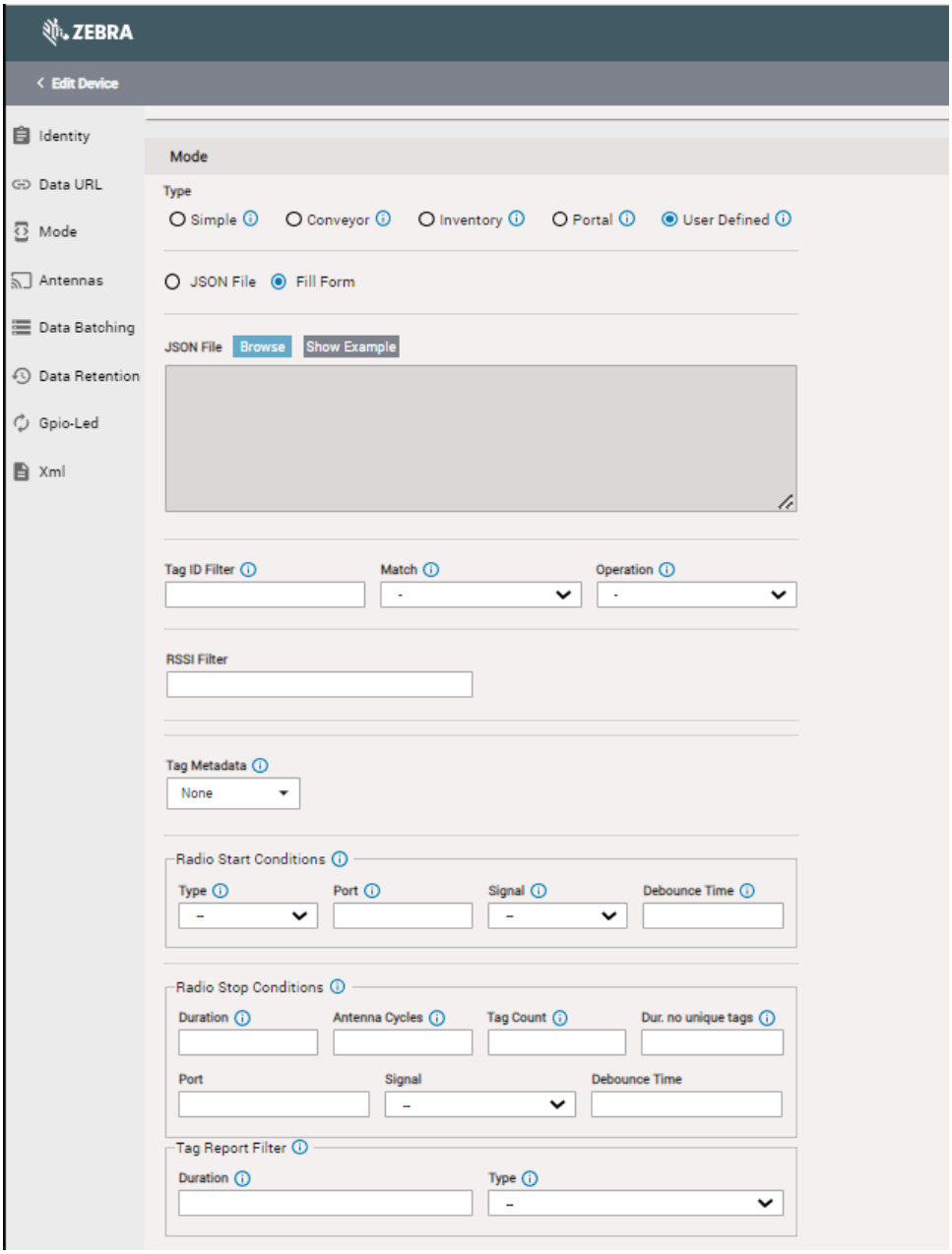
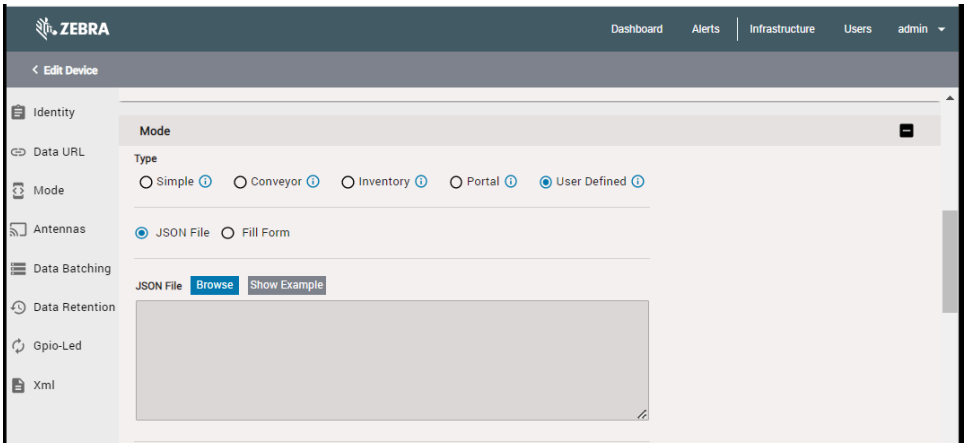


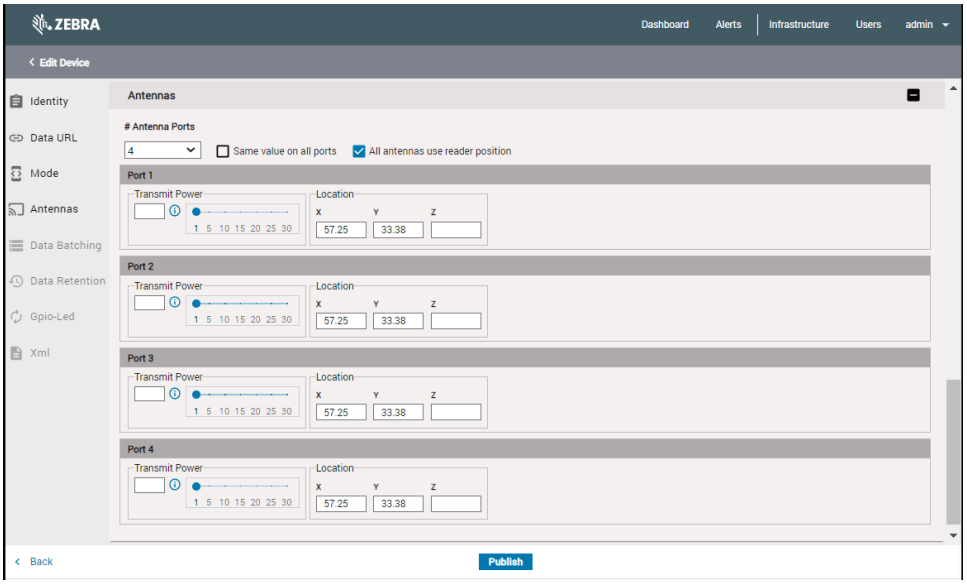
Figure 30 User Defined Mode JSON File



Antennas

In this section of the Edit Device page, you can specify the antenna power and, if desired, specify or update the number of antenna ports and the x,y coordinates for each antenna.

Figure 31 Antennas



Data Batching

Data batching combines multiple tag events into single event. Batching reduces network usage as well as reader CPU usage. The following parameters can be adjusted:

- Reporting Interval: Event Report interval in milliseconds
- Max Payload Size Per Report: Maximum payload size in bytes. Default is 256 kb.

Data Retention

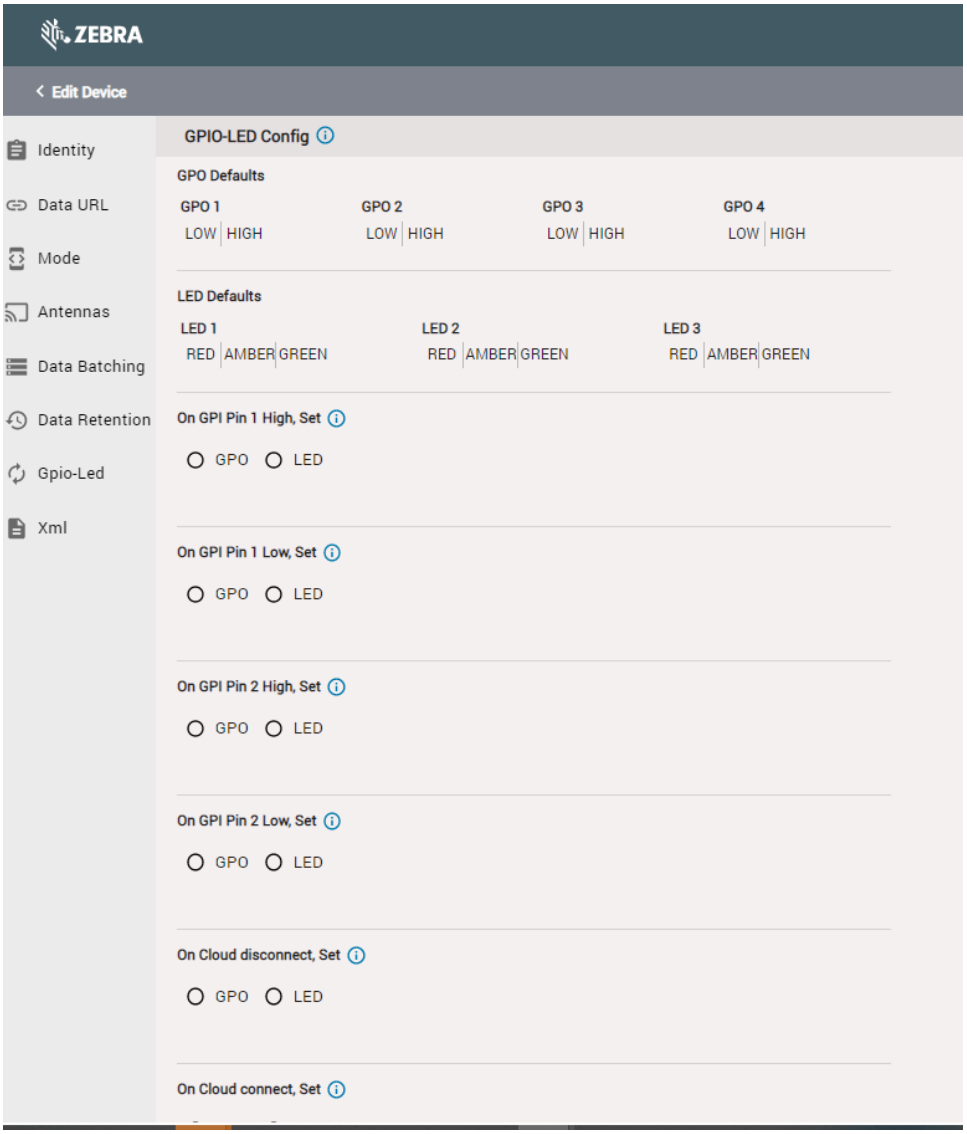
Data retention enables a reader to buffer the tag events and stream data back to a server in case of network issues or server failures. By default, retention will be enabled, and reader can retain the last 150,000 tag events and can stream data back to server at 500tps. The following parameters can be adjusted:

- Throttle: Rate (in events per second) to report data events when network is reconnected
- Maximum number of events to retain
- Maximum event retention time (in minutes): Value of 0 or -1 indicate that the events that first fill the buffer will be retained forever. A value of, for example, 10 indicates that events generated in last 10 minutes will be retained. Default value is 0.

GPIO-LED

If you have selected the Portal mode of operation, the GPIO-LED menu is enabled. Here you can configure GPIO and LED behavior based on pin high/low events.

Figure 32 GPIO-LED Configuration

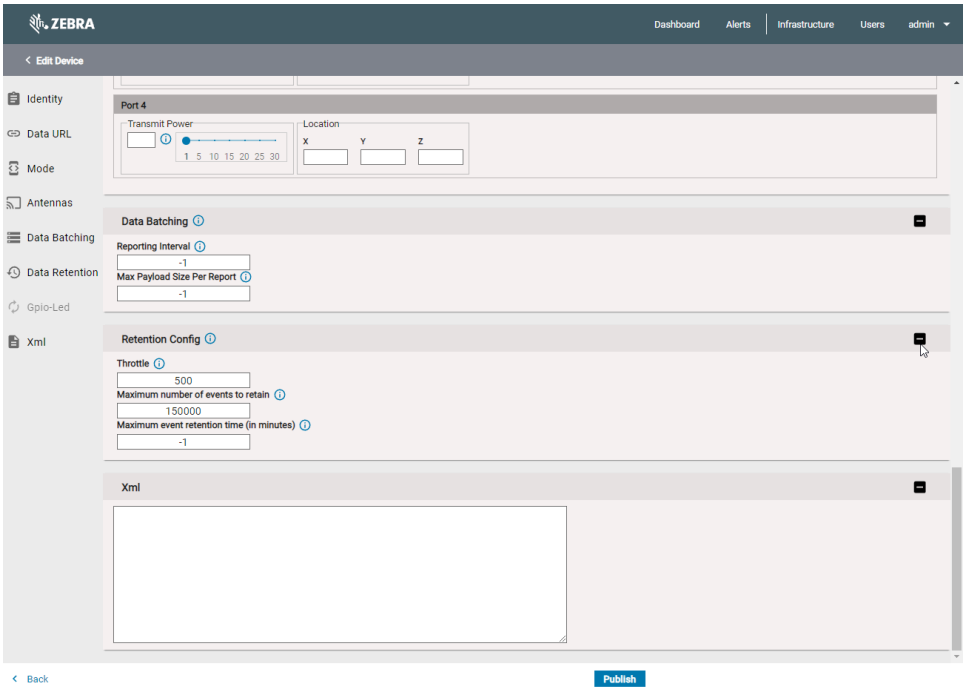


XML

Fixed RFID readers can accept XML input (profile) with the settings for all configurable options.

One reader can be set up as the main reader, and its profile can be exported as XML. The profile can then be published to other readers in Device Manager.

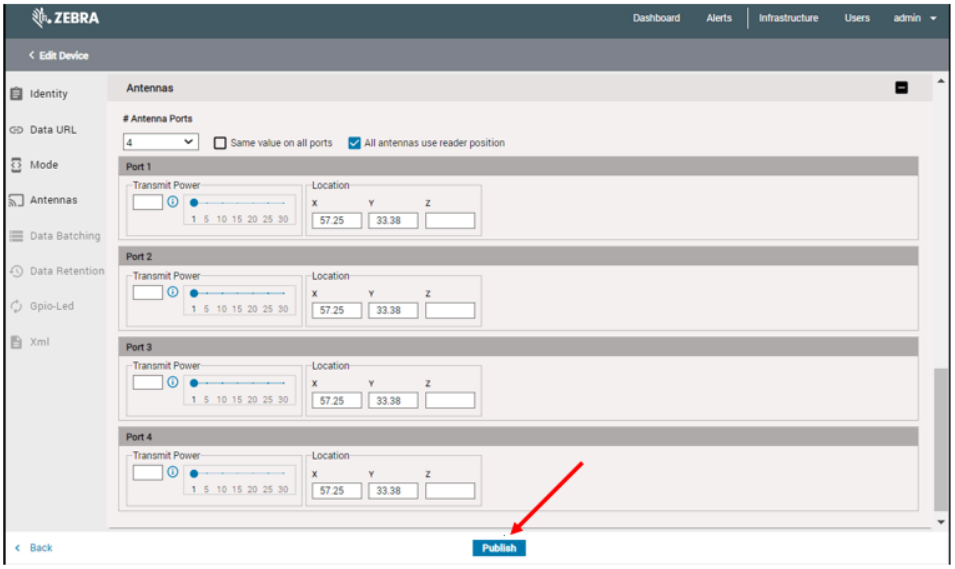
Figure 33 XML Profile Window

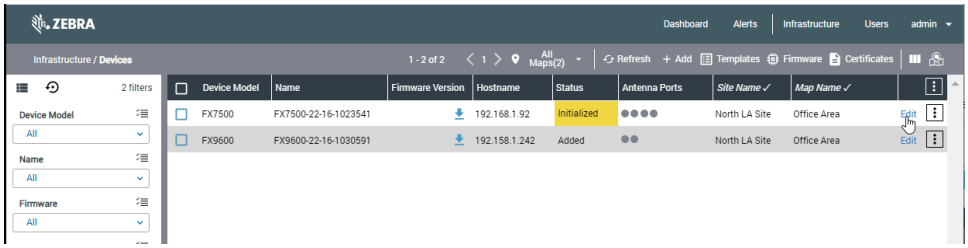


Publishing

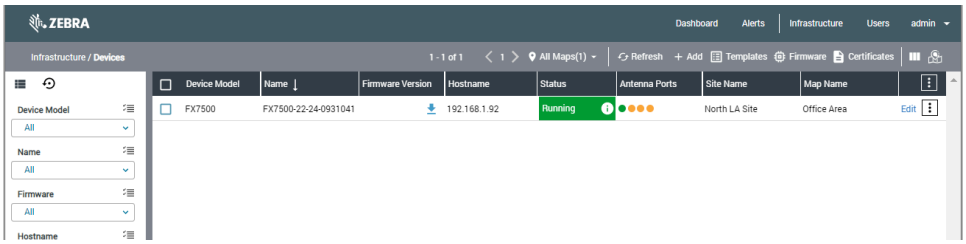
Publishing sends all the configuration information to the reader.

- At the bottom of the Edit Device page, click **Publish**. Remember, you can open the Edit Device window by clicking the **Edit** link in Device Manager.





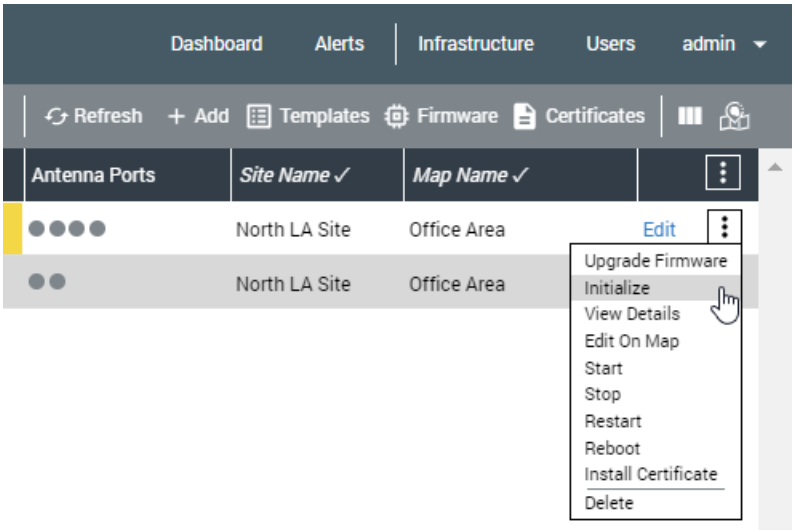
After a few seconds, the Status column in the Devices report displays **Running**, and the reader starts reading tags and posting tag blink data to the specified Data URL endpoint.



Reader Menu

The Reader menu is a **3-dot menu** located at the far right on the reader line (not the header line).

Figure 34 Reader Menu



The menu selections include:

- Upgrade Firmware: Displays window enabling you to upgrade the reader firmware.
- Initialize: Turns off LLRP protocol and loads and starts the R2C application, enabling the reader to communicate with cloud servers and the DMSVC service on a MWE RFID RM server.
- View Details: Displays a vertical column with reader information.
- Edit on Map: Allows placing a reader on a map and configuring the x and y coordinates of the reader and its antennas.
- Start: Command sent to the reader to start reading tags.
- Stop: Command sent to the reader to stop reading tags.
- Restart: Stop and Start commands sent to the reader.
- Reboot: Reboots the reader.
- Install Certificate: This menu item installs on the reader the certificate selected when configuring the Data URL section in the Edit reader page. The reader uses this certificate to post data to the data endpoint (HTTP or MQTT server).
- Delete: Removes a reader from Device Manager. Device Manager no longer manages the reader.

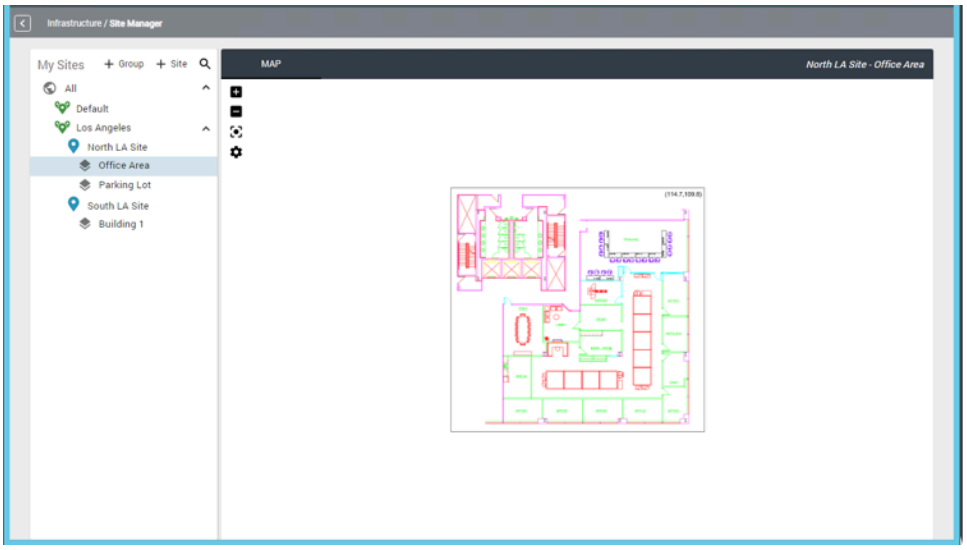
Sites and Maps

This section describes adding sites and maps to the Site Manager.

Site Manager

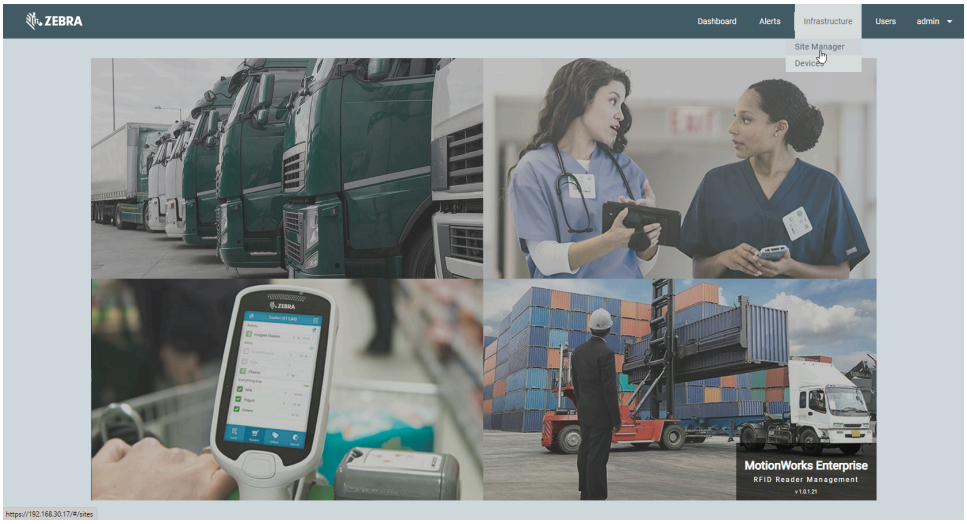
Before adding a reader in Device Manager, you must add/create a site and load a site map. This is done on the Site Manager page in the Reader Management web client. You can have multiple sites and multiple maps under each site.

Figure 35 Site Manager



Launch the Reader Management web client. Click **Infrastructure**, and then click **Site Manager**.

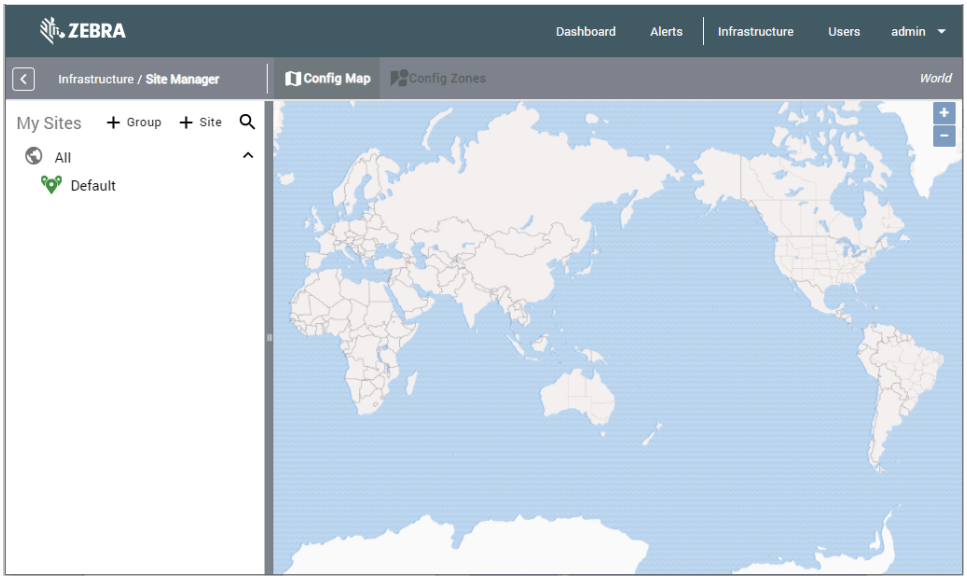
Figure 36 Infrastructure Menu



The Site Manager window is displayed.

The left-side panel displays the site groups and sites. The right-side panel is the Config Map which displays the location of each reader.

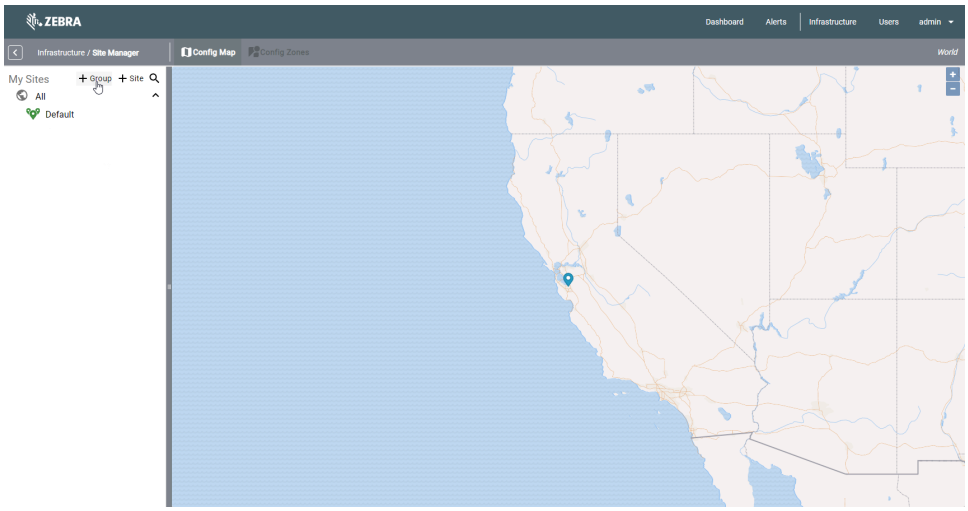
Figure 37 Config Map



Adding Site Groups

This section describes how to add Site Groups in the Site Manager.

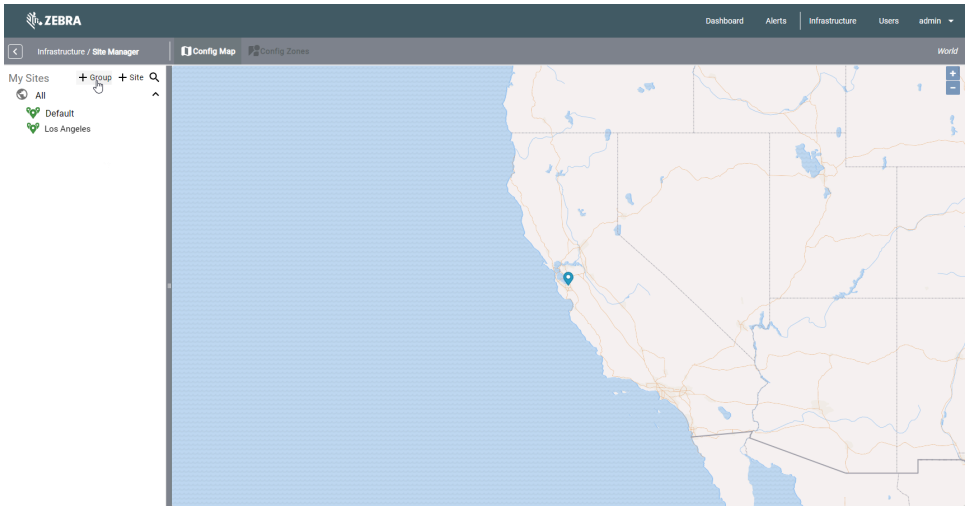
1. Click + **Group**.



2. In the **Site Group Name** field, enter a site name. For example, Los Angeles.

3. Click **Save**.

The Site Manager tree-view pane displays the newly added site group name.

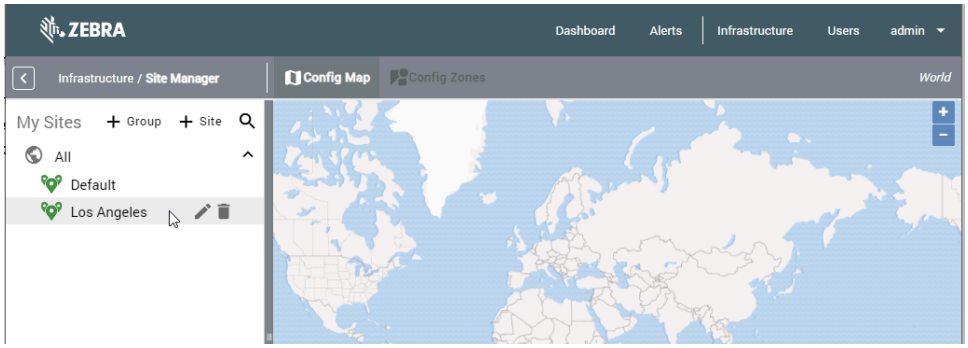


4. Create additional site groups as needed.

Editing a Site Group

This section describes how to edit a Site Group in Site Manager.

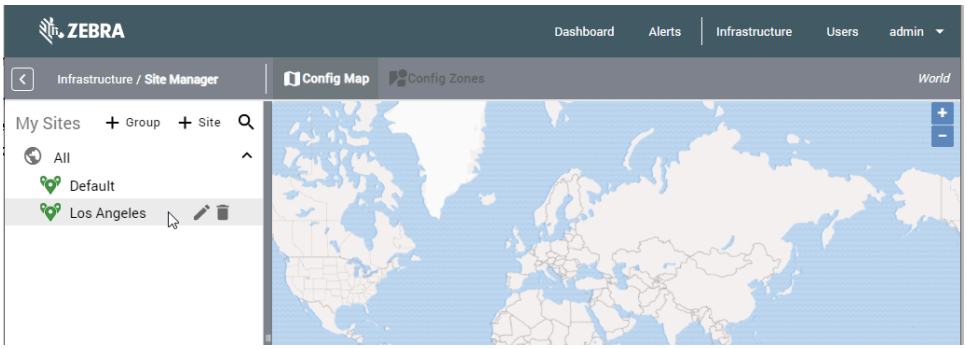
1. Hover the mouse over the site group name.
2. Click to edit the site group name.



Deleting a Site Group

This section describes how to delete a Site Group in Site Manager.

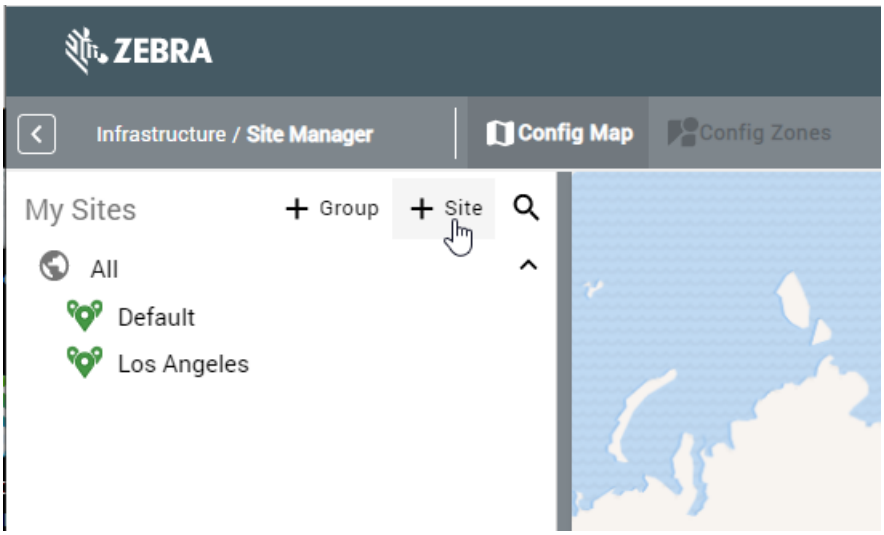
1. Hover the mouse over the site group name.
2. Click to delete the site group.



Adding a Site

This section describes creating and adding a site to a Site Group in Site Manager.

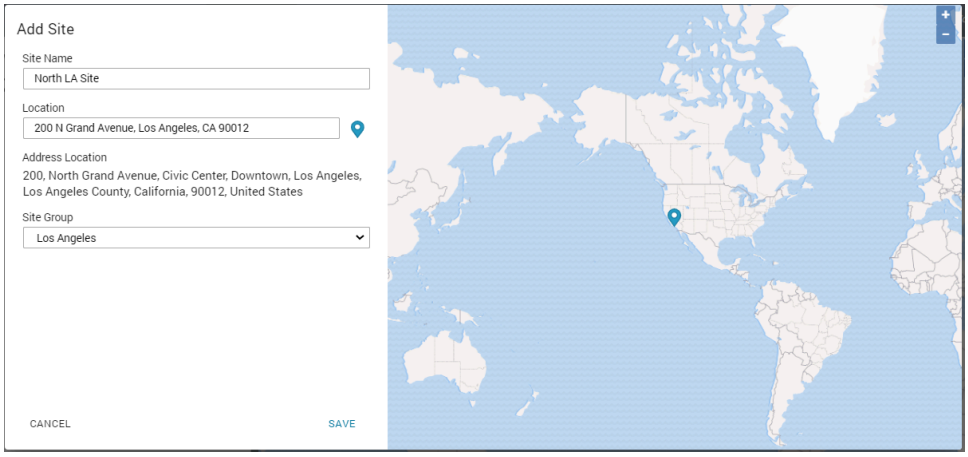
1. Click + **Site**.



2. In the **Site Name** field, enter a name for the site. For example, North LA Site.
3. In the **Location** field, enter an address.

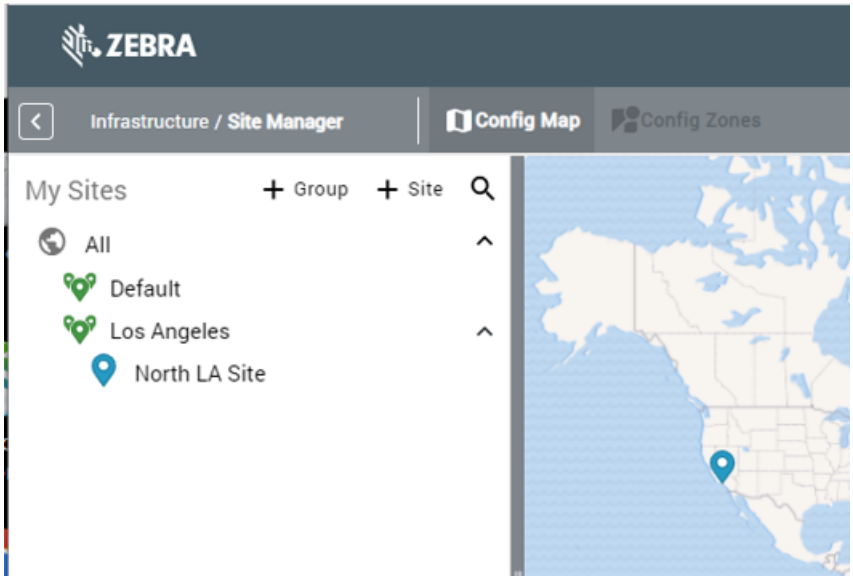
   A blue pin is placed on the map at that location. You can zoom and pan the map, and drag the blue pin to a more accurate location on the map.

4. From the **Site Group** drop-down list, select the Site Group. For example, Los Angeles.



5. Click **Save**.

   The North LA Site is displayed as part of the Los Angeles site group.

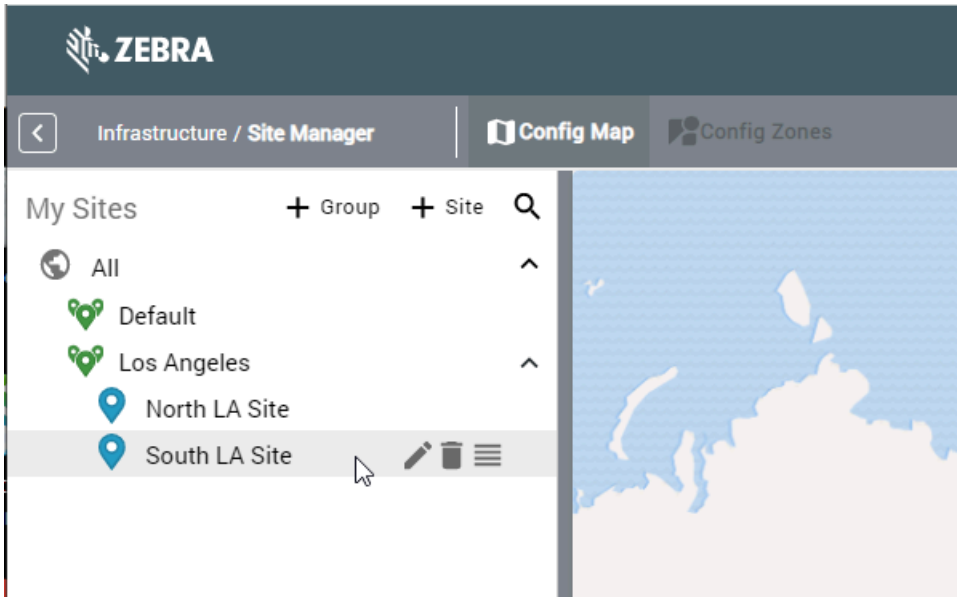


6. Create additional sites as needed.

Editing a Site

This section describes editing a Site in Site Manager.

1. Hover the mouse over the site name.

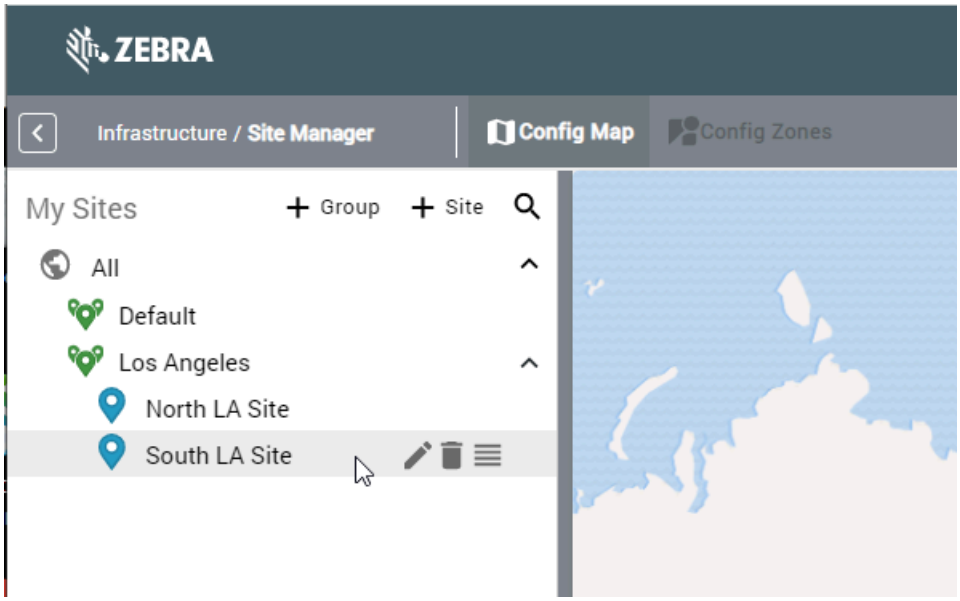


2. Click to edit the site name.

Deleting a Site

This section describes how to delete a Site in Site Manager.

1. Hover the mouse over the site name.

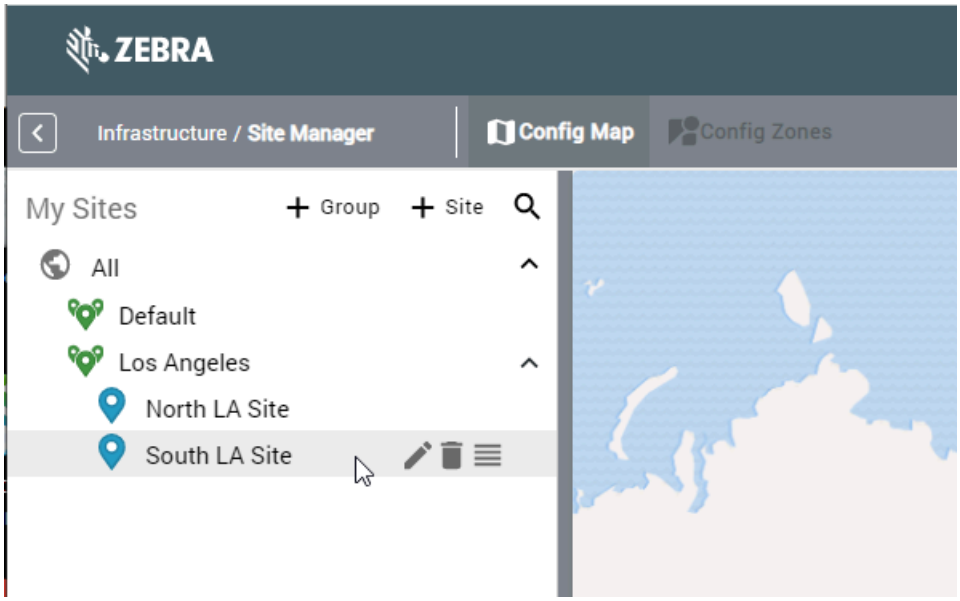


2. Click to delete the site.

Moving a Site

This section describes moving a site to another site group in Site Manager.

1. Hover the mouse over the site name.

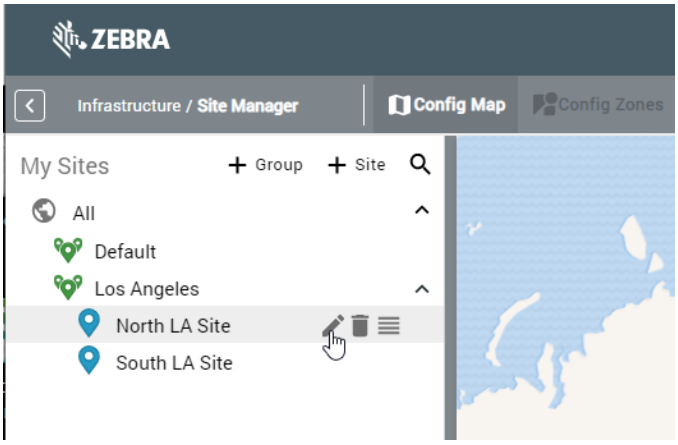


2. Click ☰ and drag to move the site to a different site group.

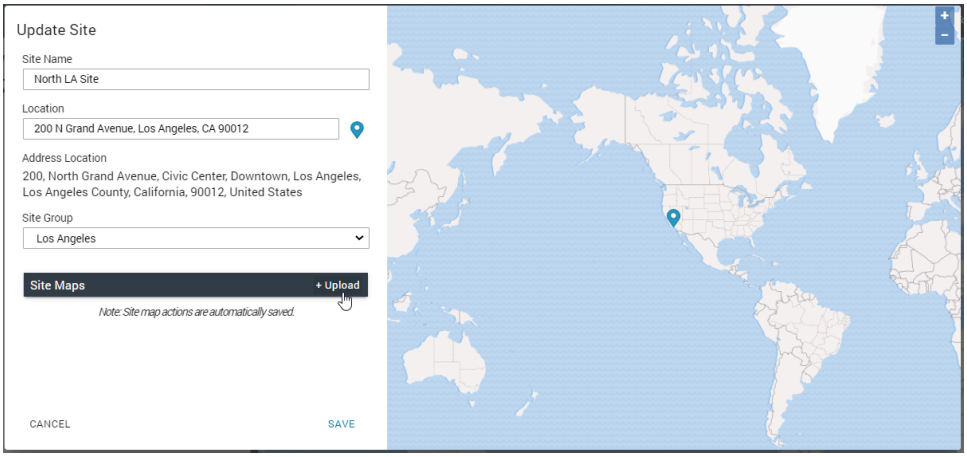
Adding a Map

You can add one or more maps under each site. Asset locations being tracked will be shown on these maps. If you have a multistory building at a site, you can add a map for each floor. Or multiple maps can be added for a campus with several buildings and parking lots.

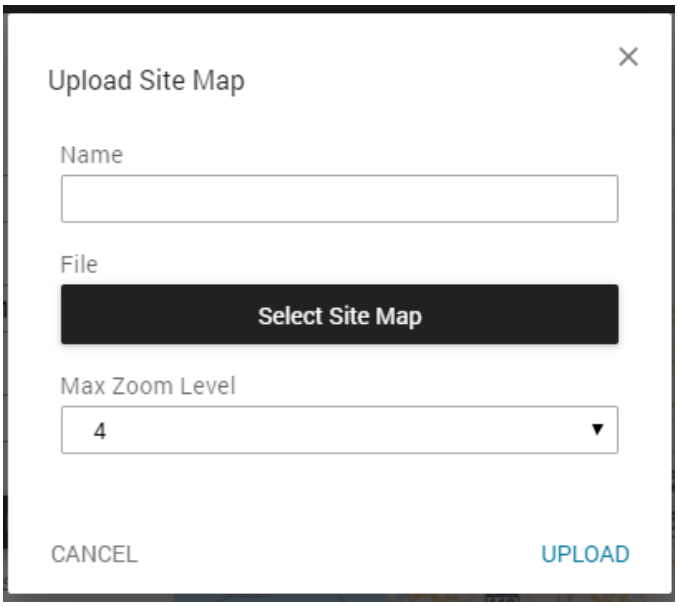
1. Hover the mouse over the site name or next to it and click ✎.



2. Click + **Upload**.



3. In the **Name** field, enter the Name of the map. For example, Office Area.

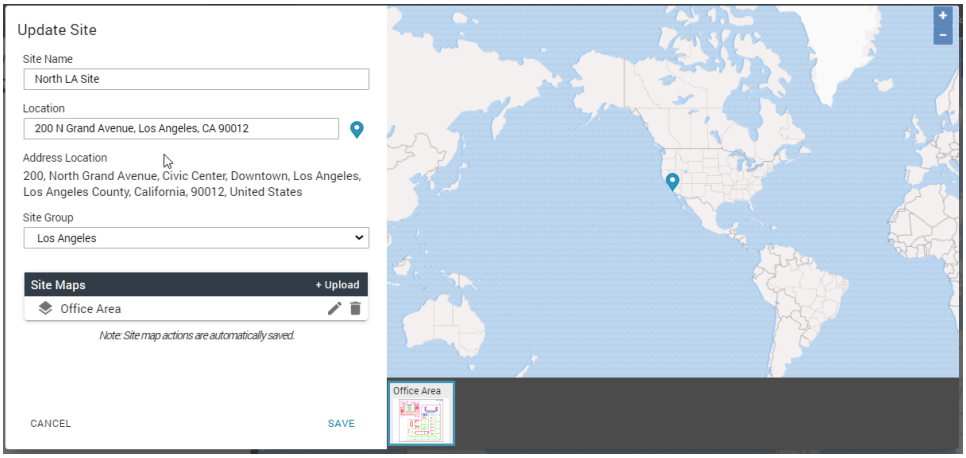


4. Click **Select Site Map** and navigate to the location of the map file.
   - If you are using Reader Management software version 1.0, only Windows metafiles (.wmf) are supported.
   - A maximum file size of 8 MB is recommended.
5. Set the Max Zoom Level.

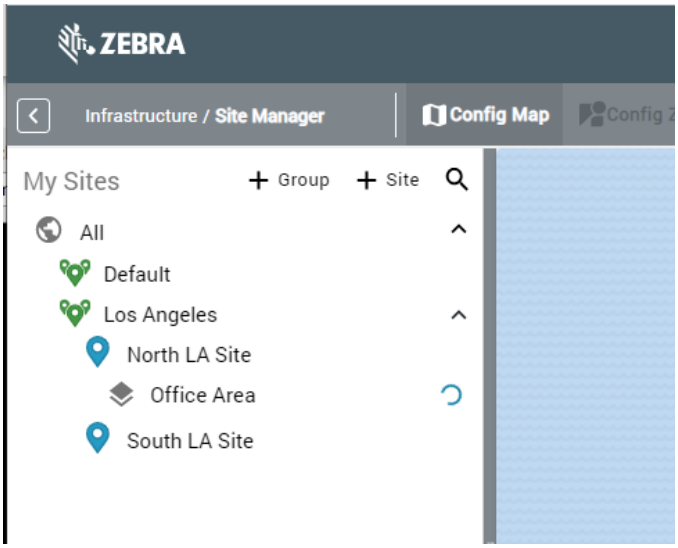
   This defines how much you can zoom in when displaying the map in the web client. The default value is 4, and the maximum available value is 8.
6. Click **Upload**.

   The upload process may take a few seconds to many minutes, depending on the map size and Max Zoom Level selected. The reason is that the map is uploaded and tiled for later use. Tiling is done only when uploading a map into the system. After a few seconds, you will be returned to the site properties window, but the tiling process will continue in the background. The name of the uploaded map is listed under Site Maps, and the map image is displayed in the lower section of the window.

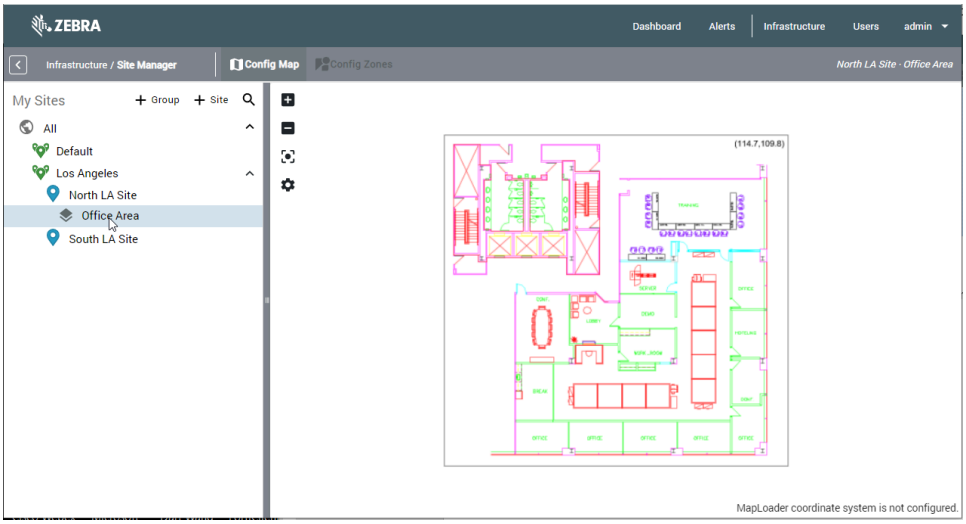
7. Click **Save**.



8. The map named Office Area is displayed under the North LA Site. A rotating circle may be displayed next to the map name, indicating the background tiling process.

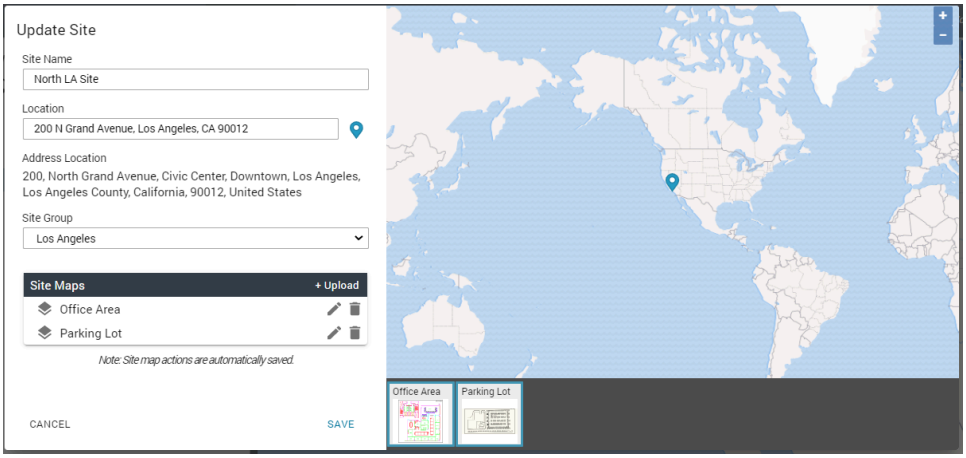


9. When the tiling process is complete, click the map name to view the map.

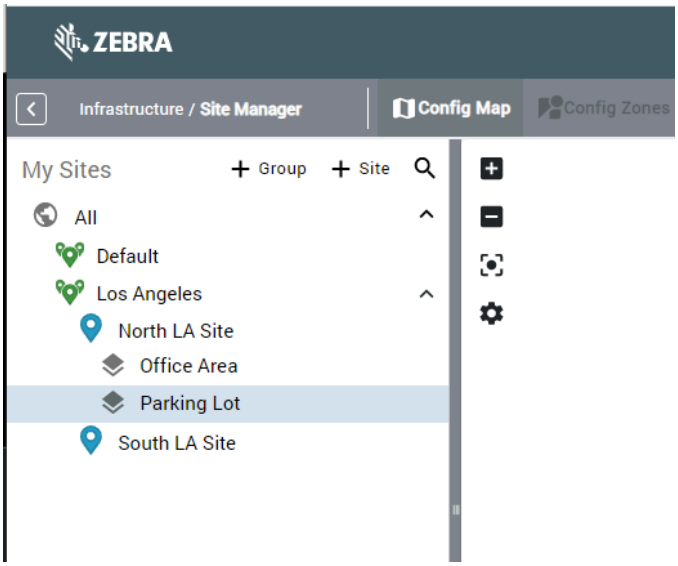


10. Add additional maps as needed. For example, Parking Lot.

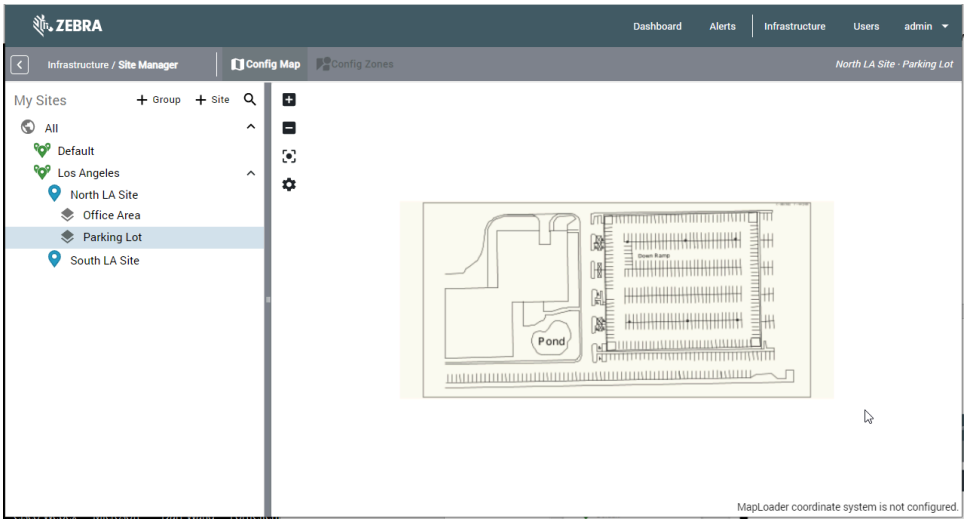
11. Click **Save**.



The tree-view pane will show the maps added under the North LA Site.



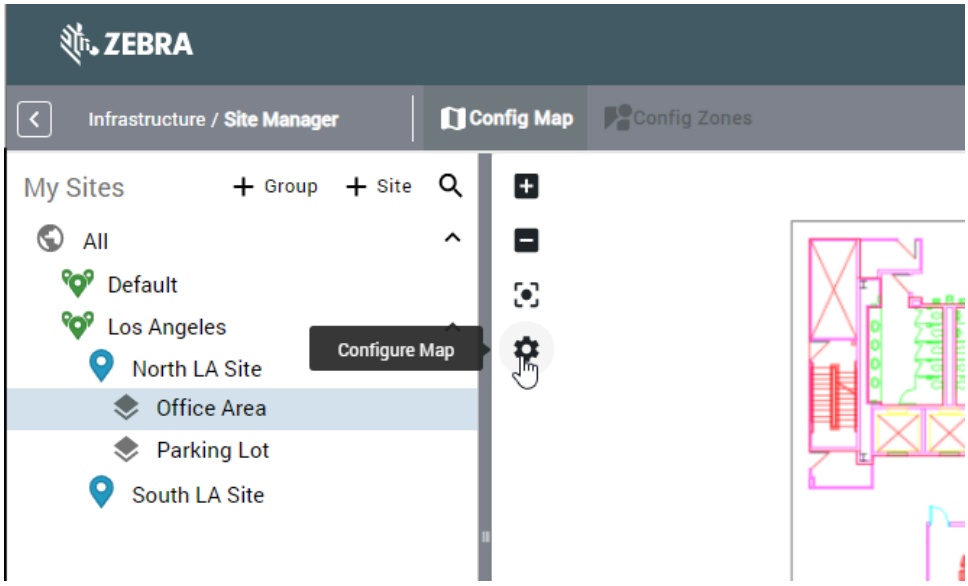
Clicking on a map entry will display the image in the map window.



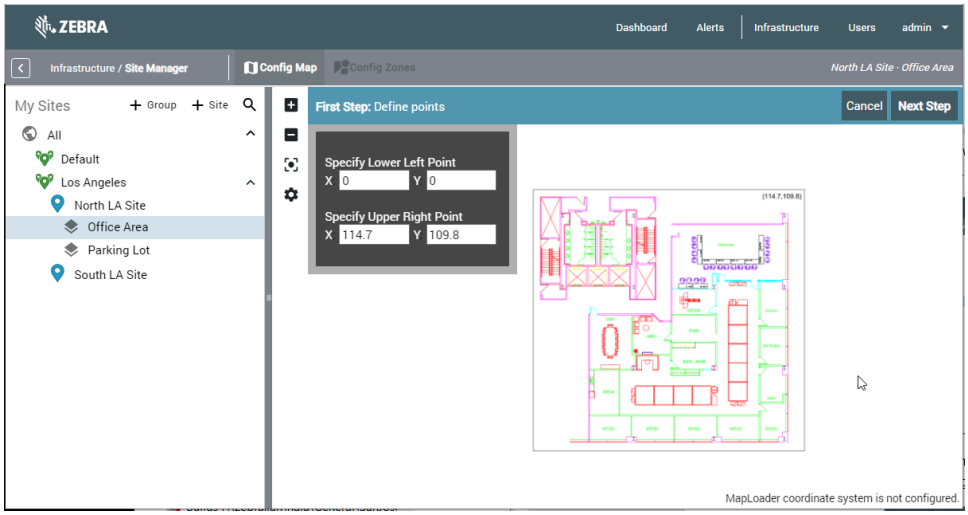
Calibrating a Map

This section describes how to calibrate a map in Site Manager.

1. Click ⚙ in the map window toolbar.

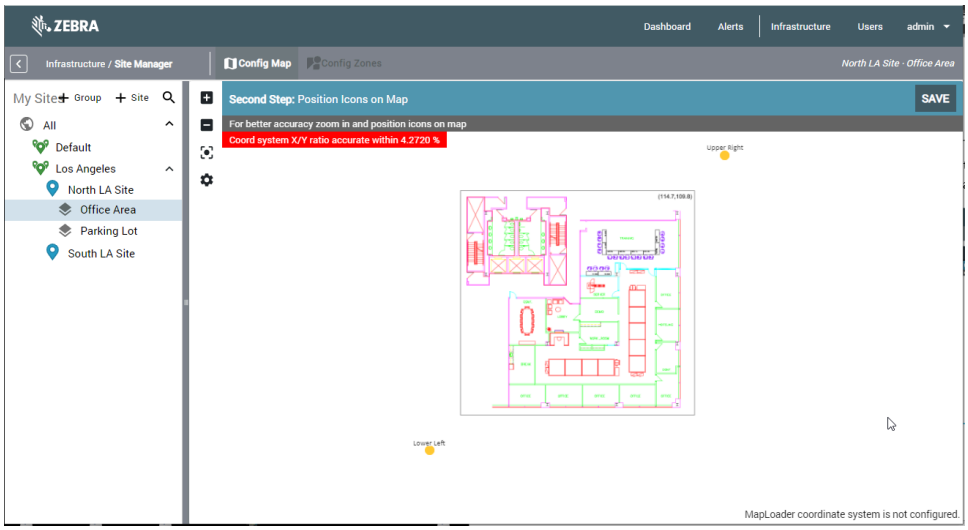


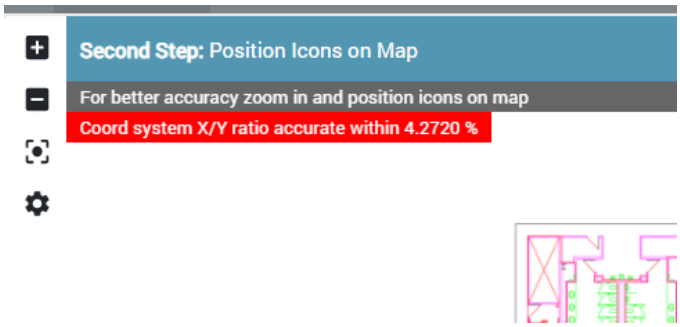
2. Enter the known x- and y-coordinates for two points on opposite corners of the map. In this example, the coordinates of the lower left and upper right corners of the square surrounding the map image are known.



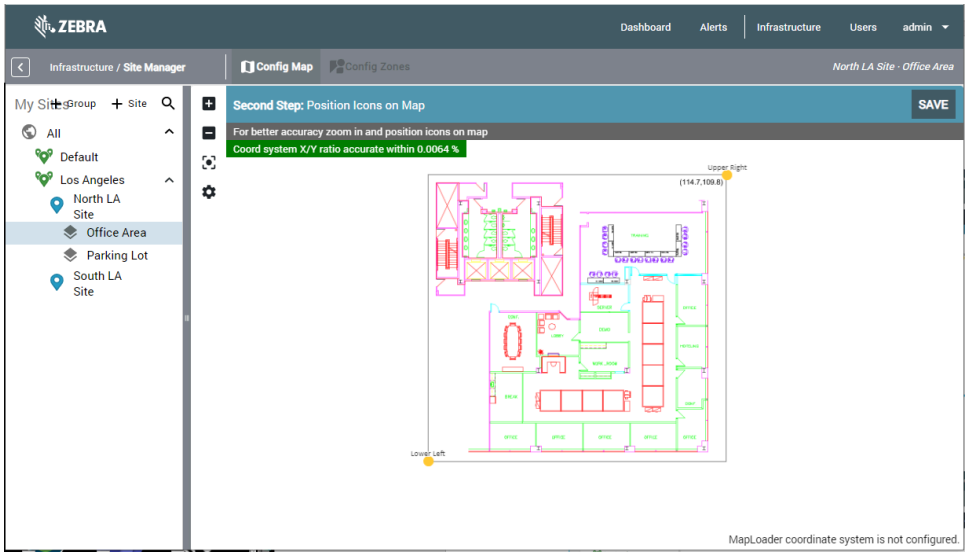
3. Click **Next Step**.

4. Two yellow dots labeled Lower Left and Upper Right are displayed. You can drag the dots to the correct position on the map. For increased accuracy, you can zoom in/out using your mouse wheel or the + and – buttons on the map toolbar.





5. The calibration algorithm compares the aspect ratio of the map image with the aspect ratio of the coordinate system you are defining by entering two reference points. The aspect ratios should match if the map image and the two reference points are correct. The bar's color switches from red to green as you move the yellow calibration dots on the map, and the agreement of the aspect ratios is greater than 1%. Click **SAVE**.



The map is now calibrated. Move the mouse over the map. The x- and y-coordinates are displayed in the lower right corner of the map window.

Editing a Map

This section describes how to edit a map in Site Manager.

1. To edit a map, hover the mouse over the map name.
2. Click to edit the map name.

Deleting a Map

This section describes how to delete a map in Site Manager.

1. To delete a map, hover the mouse over the map name.
2. Click to delete the map.

Certificates

Certificates are used to secure the connection between a reader and the MWE RFID server and between a reader and a data endpoint server.

Certificates are categorized as follows:

- Reader-MWE RFID Server Certificate
- Data Endpoint Certificates
- Reader Certificates

Reader-MWE RFID Server Certificate

The Initialize command pushes a certificate from the MWE RFID server to the reader that is used in a secure websocket connection between the reader and the MWE RFID server. This connection is used for managing and monitoring the readers. The certificate is included with MWE RFID and normally does not need to be replaced. If, for some reason, you do need to replace this certificate, contact Zebra Product Support for instructions.

Data Endpoint Certificates

Some protocols such as TLS and secure websocket require a certificate to be installed on the reader that will be used by the reader to validate the data endpoint server (HTTP or MQTT server). In other words, we need to install the same certificate on the reader that is being used by the data endpoint server.

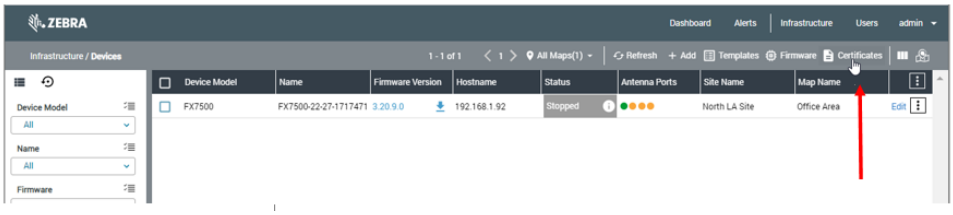
There are three steps:

1. Upload data endpoint certificates to MWE RFID server.
2. Assign a data endpoint certificate to a reader on the Edit Device page.
3. Install/push the certificate to the reader(s).

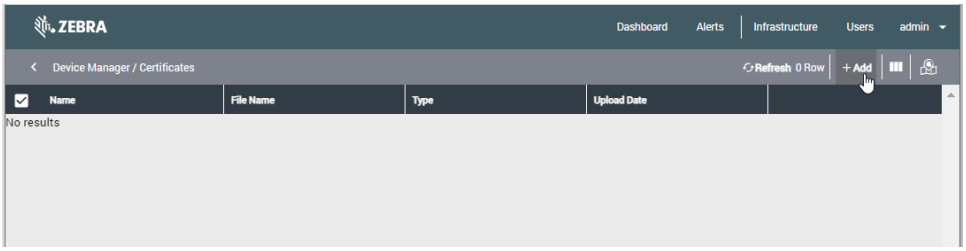
Uploading a Certificate

This section describes how to upload a certificate.

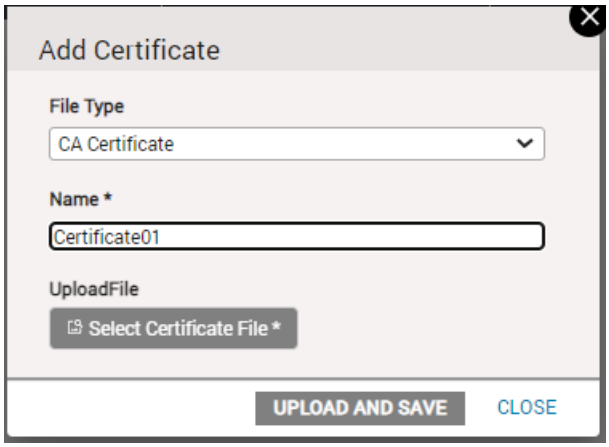
1. Click **Certificates**.



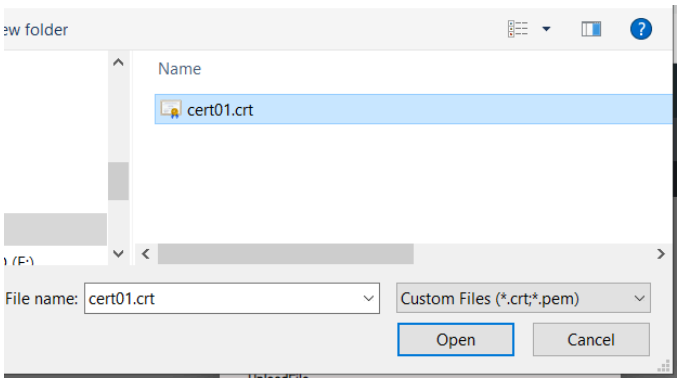
2. Click + **Add**.



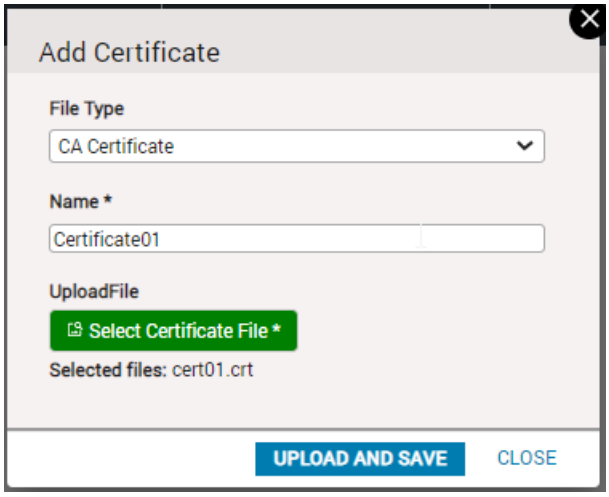
3. Type a Name for your certificate and click **Select Certificate File**.



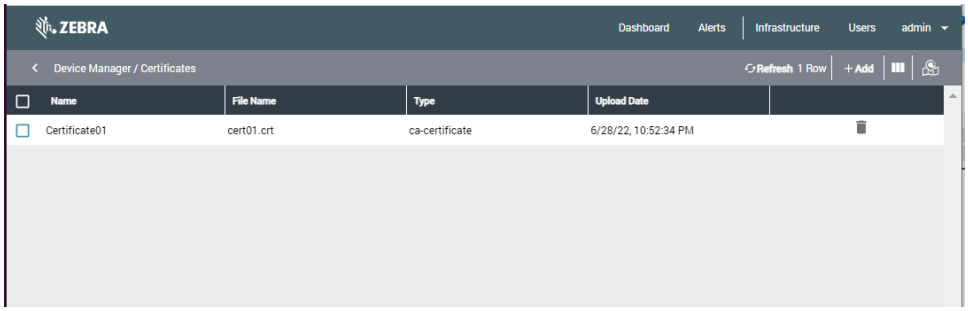
4. A .pem file or a .crt file is required. Navigate to your certificate file and click **Open**.



5. Click **UPLOAD AND SAVE**.

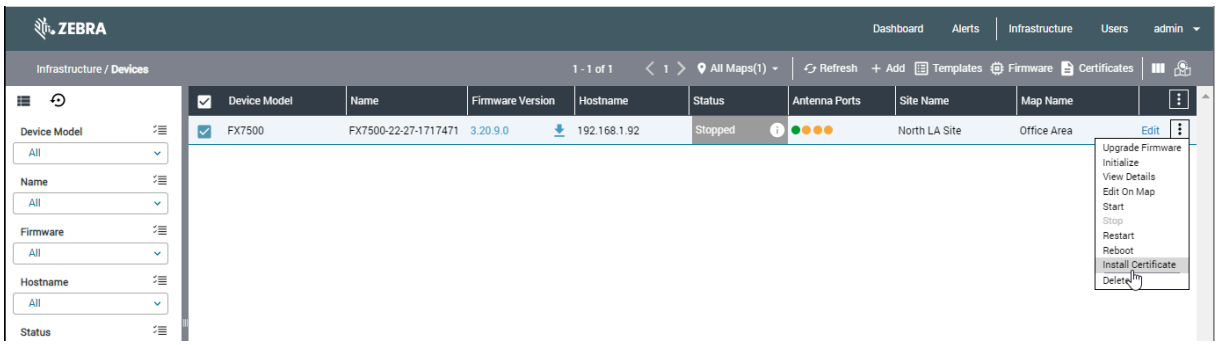


The certificate displays on the Certificates page.



Pushing a Certificate to a Reader

- In Device Manager, click ⋮ in the reader line (not the header line), and then click **Install Certificate**.

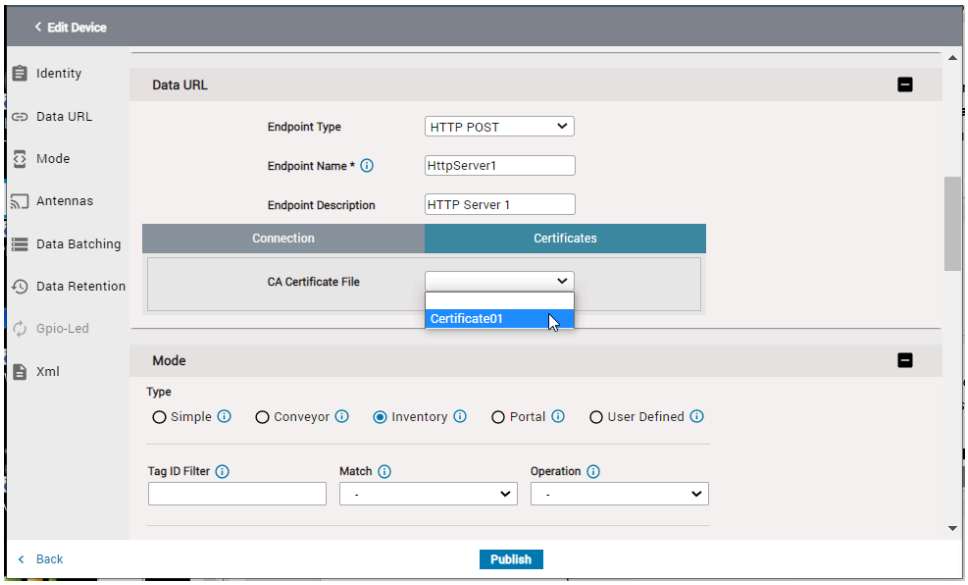


Assigning a Certificate to a Reader

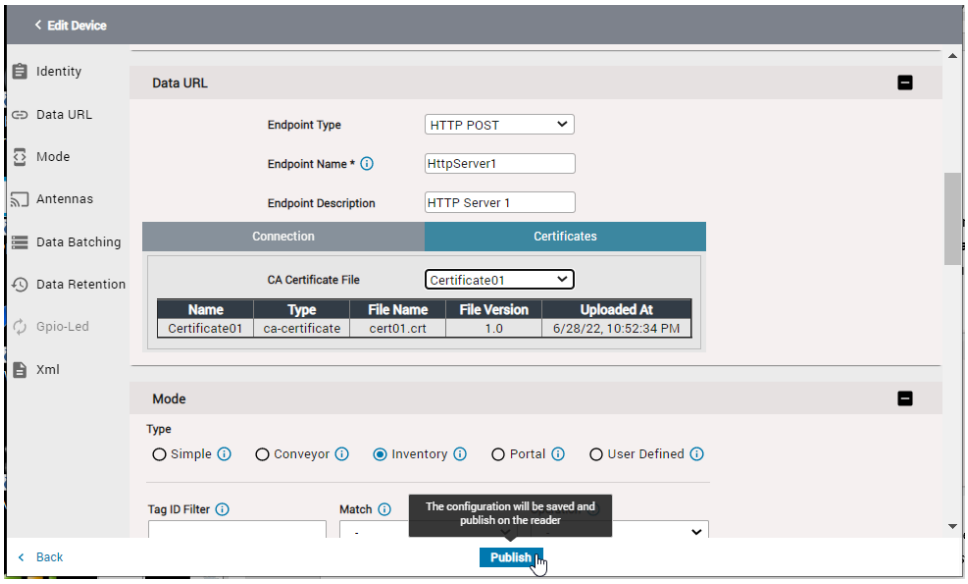
A data endpoint certificate is assigned to a reader in Device Manager.

1. From the **Edit Device** page, select the **Data URL** section and then click the **Certificates** tab.
2. Click the **CA Certificate File** drop-down list to see all the certificates you have previously uploaded and select one of them for this reader.

   The **CA Certificate File** drop-down list becomes enabled only when you select a protocol that requires a certificate, such as TLS or Secure Websocket. See Data Endpoint Certificatesfor more details.



3. Click **Publish** to save your changes.



Reader Certificates

When the reader connects to the data endpoint, it retrieves the certificate on the server and compares it to the data endpoint certificate installed on the reader. If they match, the reader will send tag blink data to the endpoint. In this case, the reader authenticates the server.

Some servers require authenticating the client (in this case, the reader) before accepting data. In this scenario, the reader presents a certificate (.pfx file) to the server, and the server compares it with a device certificate stored on the server. If they match, the server accepts data from the reader. In this case, the server authenticates the client.

Enabling Certificate Authentication

This section describes how to generate and install a reader certificate on the reader.

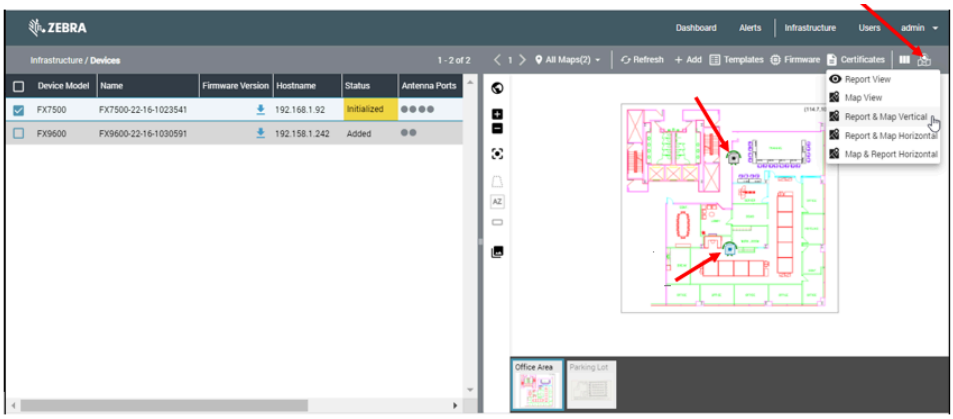
1. Generate a reader certificate. The customer might do this depending on what kind of certificate they want to use. Follow the naming convention endPointName_Hostname.pfx where endPointName and Hostname are the values shown in the Edit Device page for the reader in Device Manager.
2. Copy the .pfx certificate to the MWE RFID Reader Management folder in the directory /data/MWE RFID RM/certs.
3. In Device Manager, click **Install Certificate** from the reader actions menu (three vertical dots in the last column)
4. Copy the .pfx certificate to the appropriate directory on the data endpoint server.

Customization

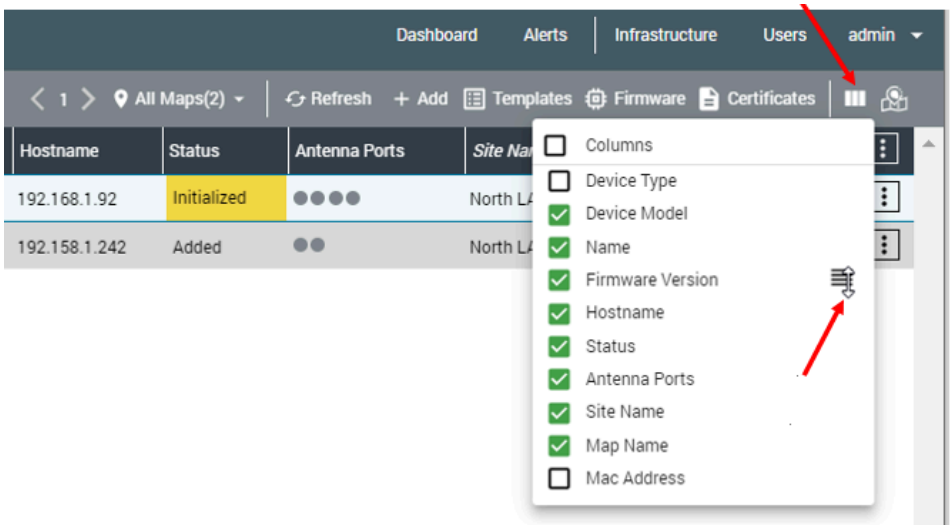
The Devices page offers several customization options, including what columns to show/hide, the order of the columns, report/map views, and details column, as illustrated in this section.

Customizing the Device Manager

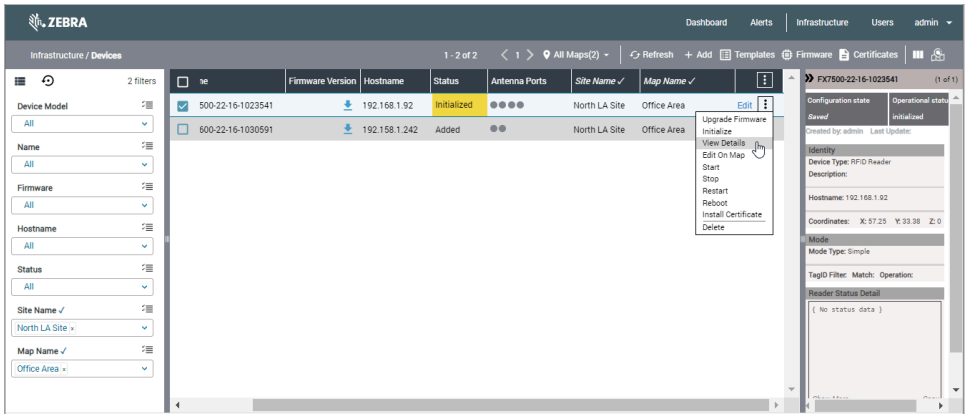
1. To select a report/map view, click  on the toolbar. The following figure shows the Report & Map Vertical option. The readers are listed in the report window on the left side and are displayed on a map on the right side.



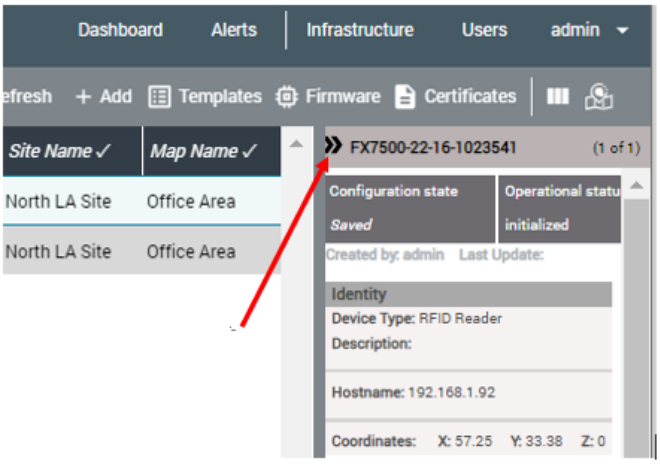
2. To change the set of columns displayed, click on the toolbar, and then check or uncheck the desired columns. To change the position of a column, hover the mouse pointer over a column name, and then click and drag up or down.



3. To show the vertical details panel, click on a reader row and click **View Details** from the drop-down menu. You can select multiple readers in the report and move from one reader to the next using the single arrow at the top of the vertical details panel.



4. To hide the Details column, click ».

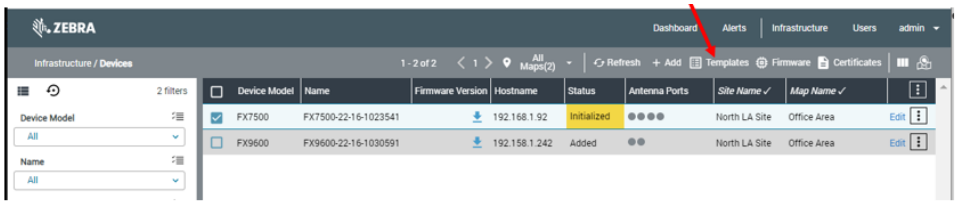


Templates

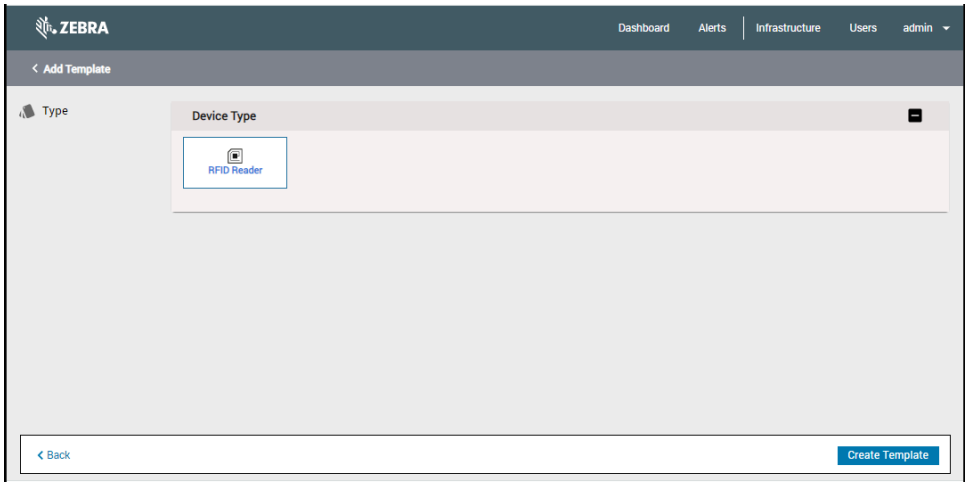
You may need to add several devices in Device Manager with the same basic configuration. For example, you may want to add several FX readers that have the same Operation Mode, for example, Conveyor Mode, and have the same number of antennas. To save time, instead of adding this information every time you add a new reader, you can define a template with this configuration and select the template with one click when adding the new readers. This automatically populates the corresponding fields in the newly added devices.

Creating a Device Template

1. To create a template, click **Templates** on the toolbar. If there are not any previously defined templates, a blank page is displayed.



2. Click + **Add** on the toolbar to add a new template. A page showing the device types available is displayed.

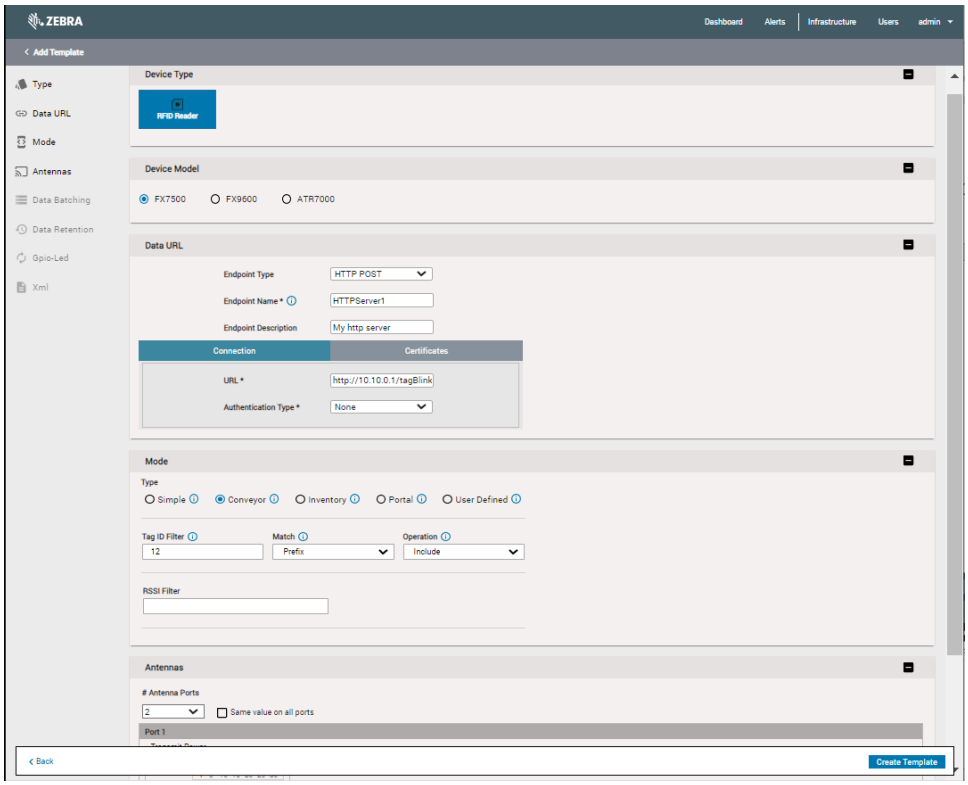


3. Click **RFID Reader**.

   A screen is displayed with basic configuration parameters that apply to the device type selected, such as the Data URL, the Operation mode and its parameters, and the number of antennas enabled.

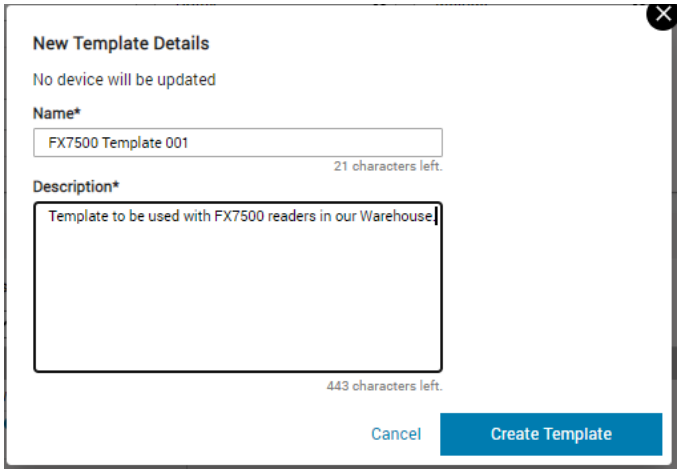
4. Fill in the values in the appropriate fields.

5. Click **Create Template**.

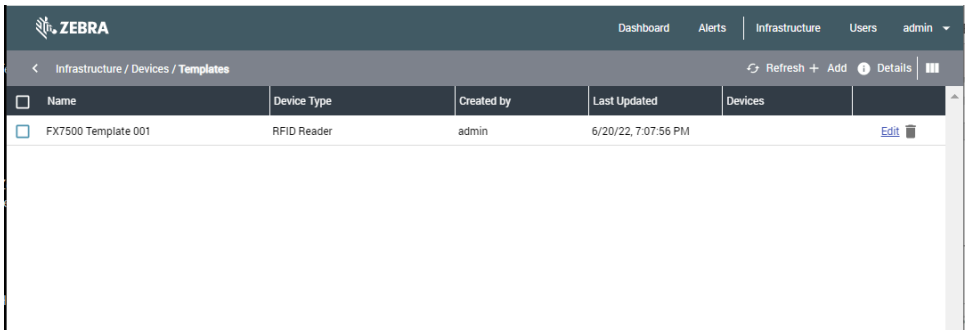


6. Enter a name for the template and a description

7. Click **Create Template**.



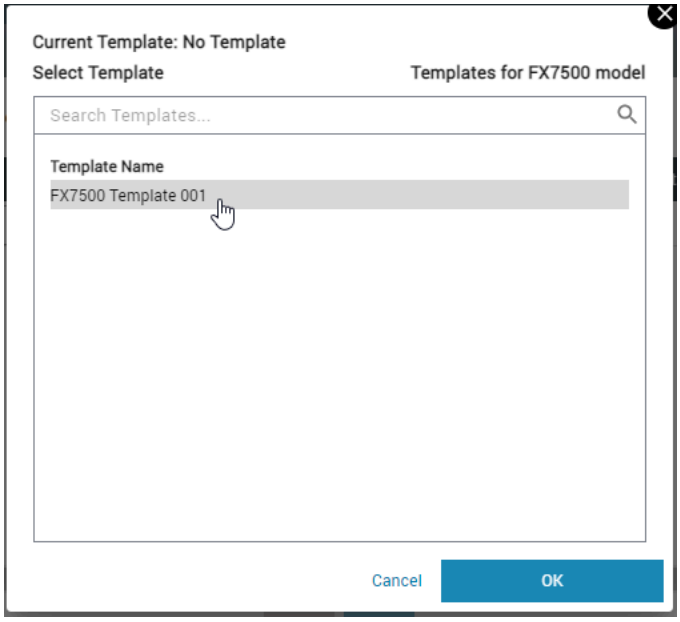
The new template is displayed on the Templates page.

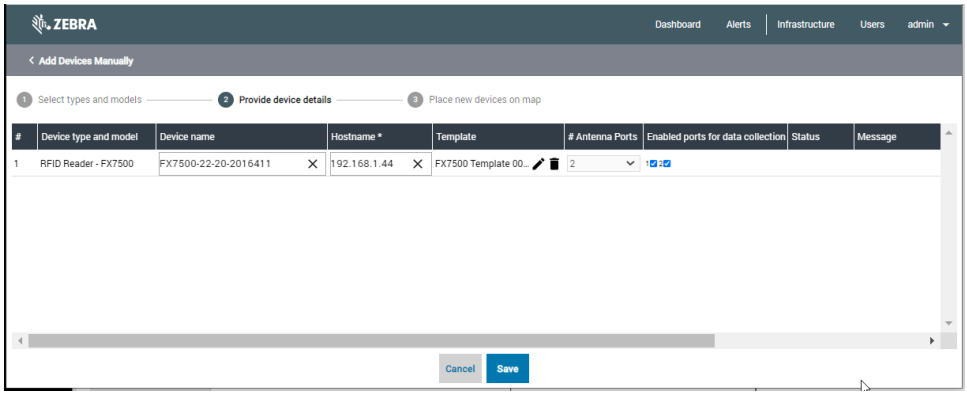


Using a Device Template

1. Select the desired template.

2. Click **OK**.





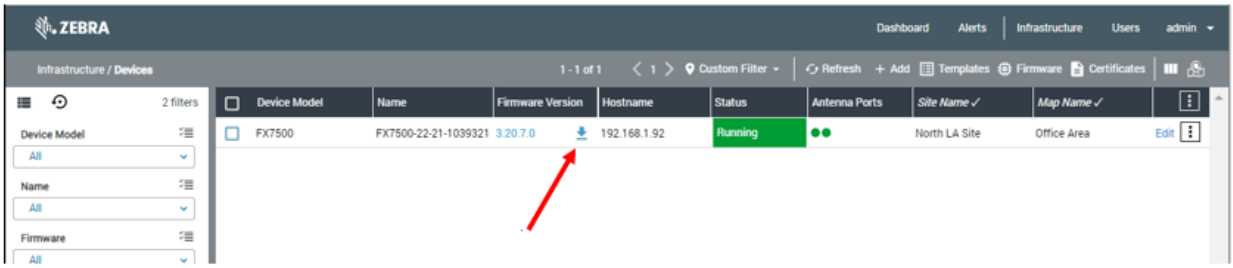
NOTE: The number of antennas (and other parameters not visible in this window) are automatically populated. After entering the Hostname, click **Save** and continue adding a reader.

Firmware

Device Manager allows you to easily upgrade the firmware of one or multiple readers at a time. After a reader is initialized, you will see the firmware version running.

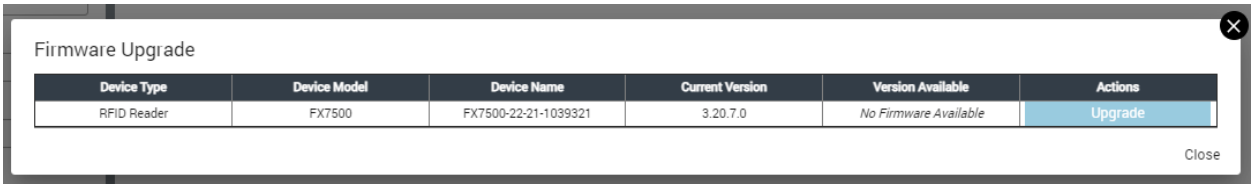
When it has been initialized, you can upgrade the reader firmware from Device Manager. Click in the Firmware column.

Figure 38 Firmware Upgrade Select



The Firmware Upgrade window is displayed.

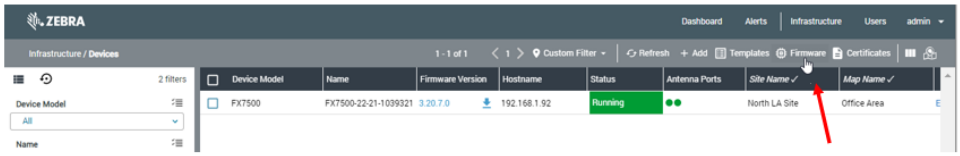
Figure 39 Firmware Upgrade Window



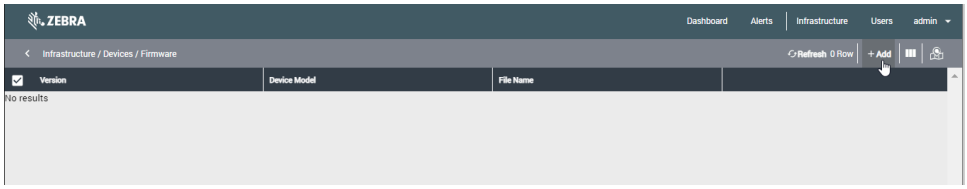
In the Version Available column, the message No Firmware Available is shown. This is because there is no firmware file on the MWE RFID server that can be pushed to the readers.

Uploading Firmware Files

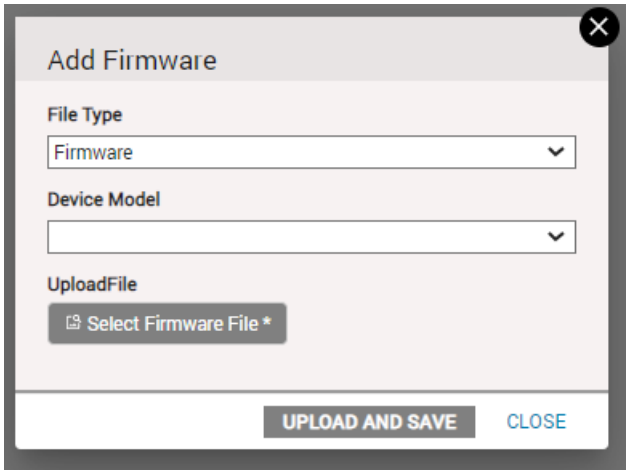
1. Click **Firmware** on the menu bar.



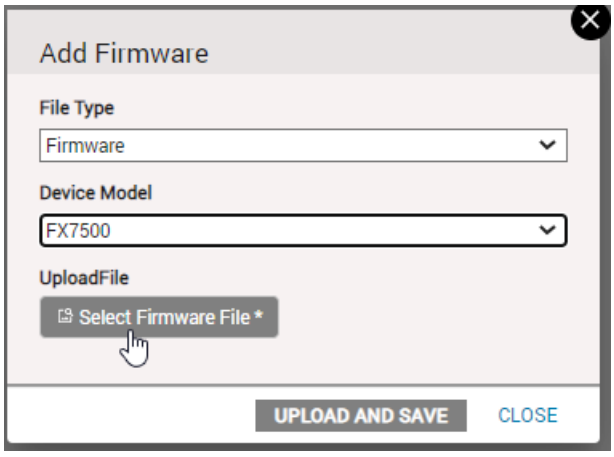
The Firmware window displays firmware files on the MWE RFID server.



2. Click **+Add**.

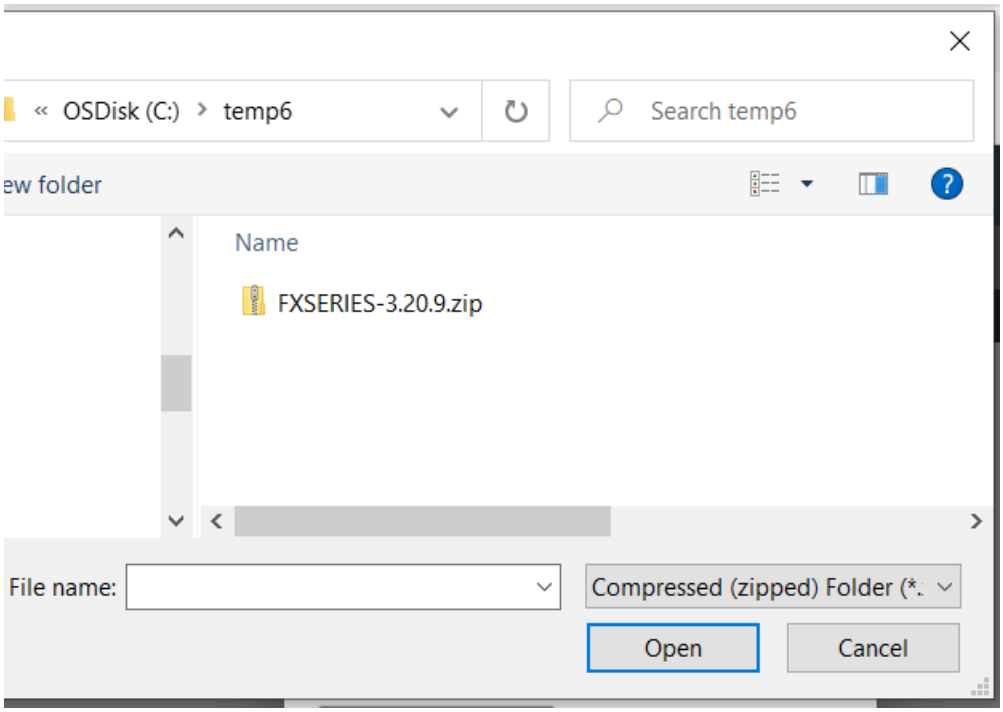


3. Select a Device Model and then click **Select Firmware File**.

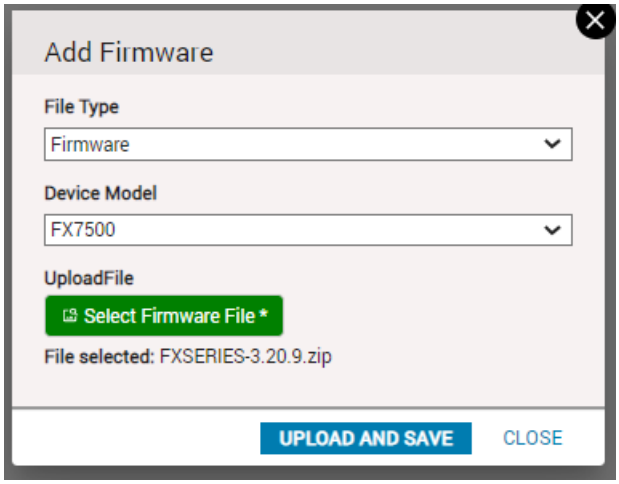


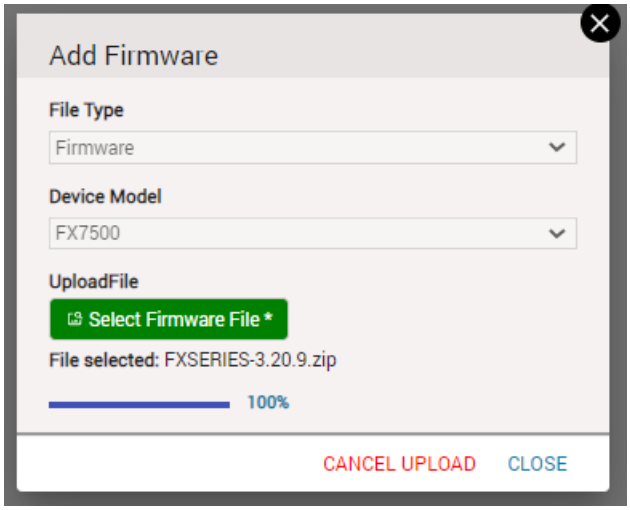
4. Navigate to the location of the firmware file.

5. Select the file, and then click **Open**.

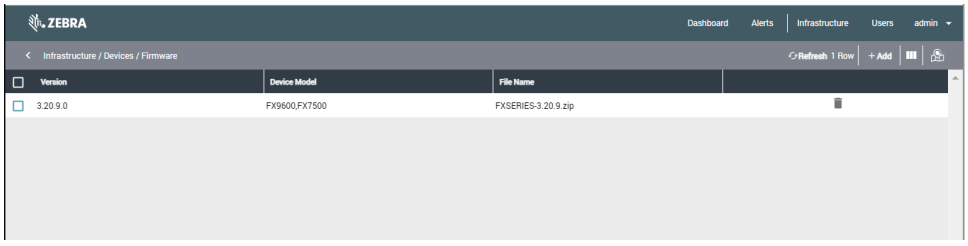


6. Click **Upload and Save**.





7. Once the upload is complete, click **CLOSE** and the Firmware page displays the uploaded firmware version.



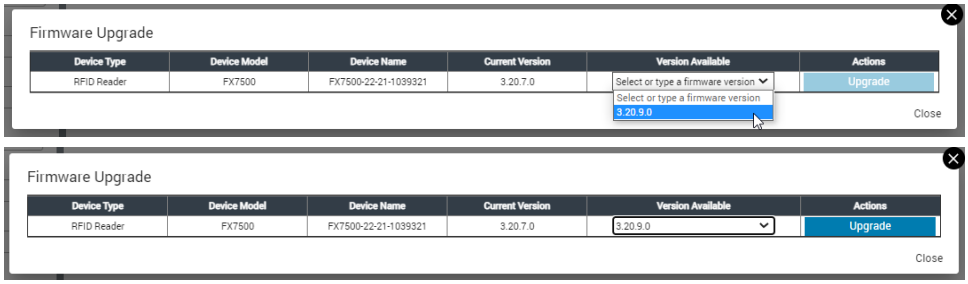
You can upload different firmware versions to upgrade or downgrade your readers.

Upgrading Firmware on a Reader

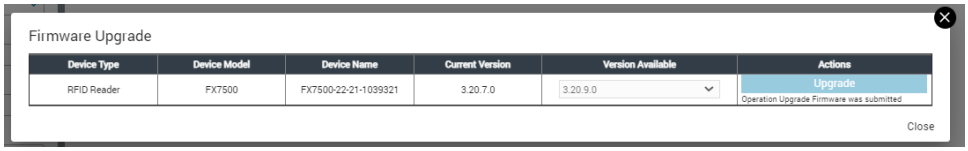
Once you have uploaded one or more firmware versions, you can select any version to push to one or more readers.

1. On the Device Manager page, click next to the reader firmware version, or click in the reader row (not the header row) then select **Upgrade Firmware**.

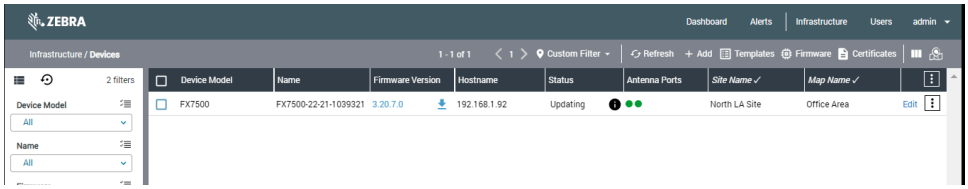
2. In the drop-down list under the **Version Available** column, select the desired version, and then click **Upgrade**.



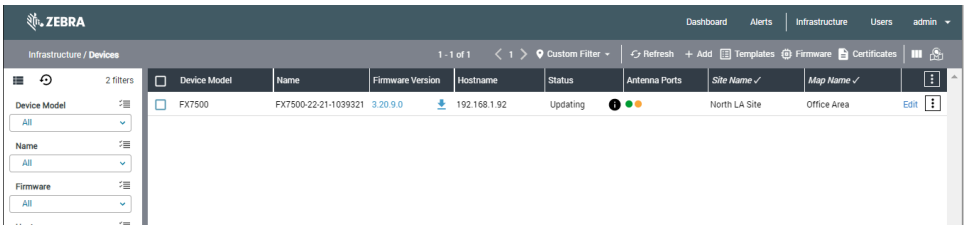
3. Close the Firmware Upgrade window.



Device Manager updates the status in the Status column of the reader row.



When completed (update may take several minutes), Device Manager displays the new version in the **Firmware Version** column of the reader row.

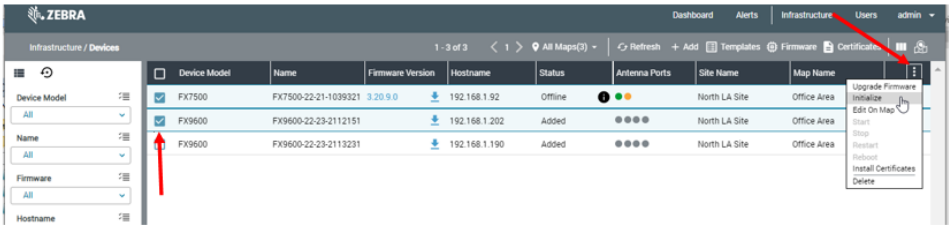


Bulk Operations

Some actions done on a single reader can be performed on multiple readers simultaneously.

Performing Actions on Readers

1. To perform an action on a reader or multiple readers, click the checkbox next to the reader.
2. Click  in the header row (not the reader row), and then click the desired action.



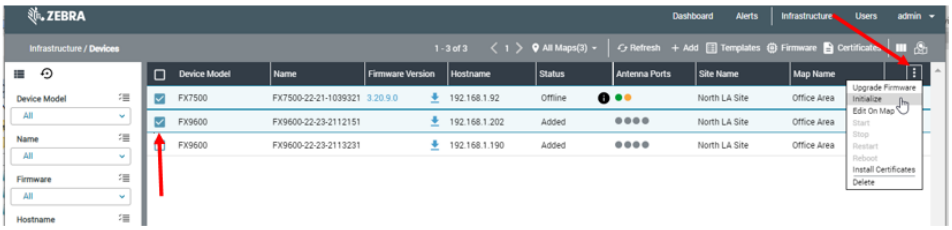
Actions for multiple readers are limited to:

- Upgrade Firmware
- Initialize
- Edit On Map
- Install Certificates

Performing a Batch Import

You can add multiple devices in Device Manager is using Batch Import.

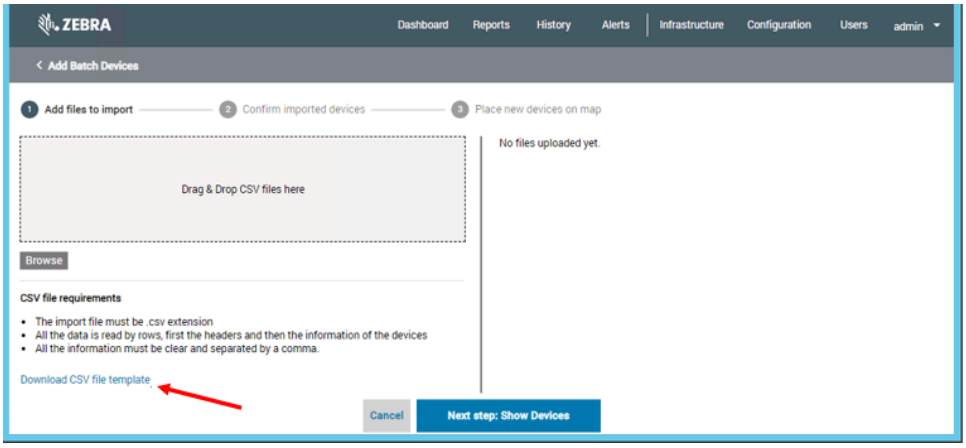
- Click + **Add**, and then click **Batch Import**.



The Batch Import window is displayed.

Creating an Import File

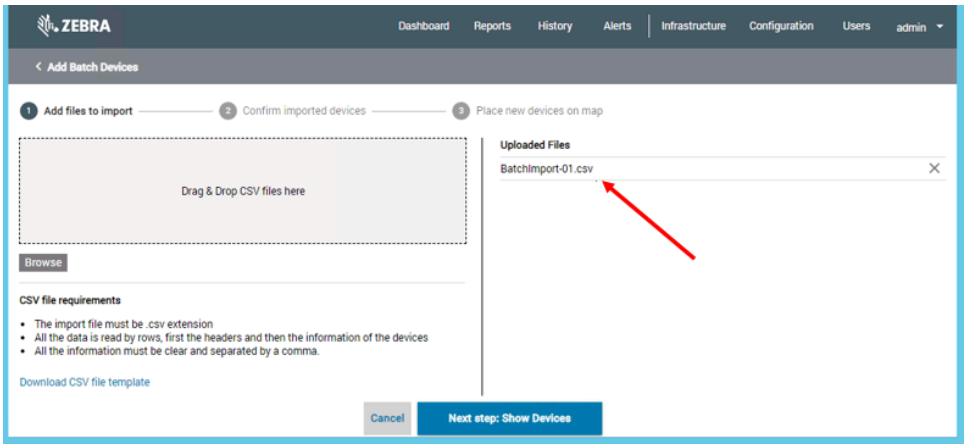
1. In the Add Batch Devices window, click **Download CSV file template** template.



2. Enter the requisite date into the template fields and save the file with an easily identifiable name.

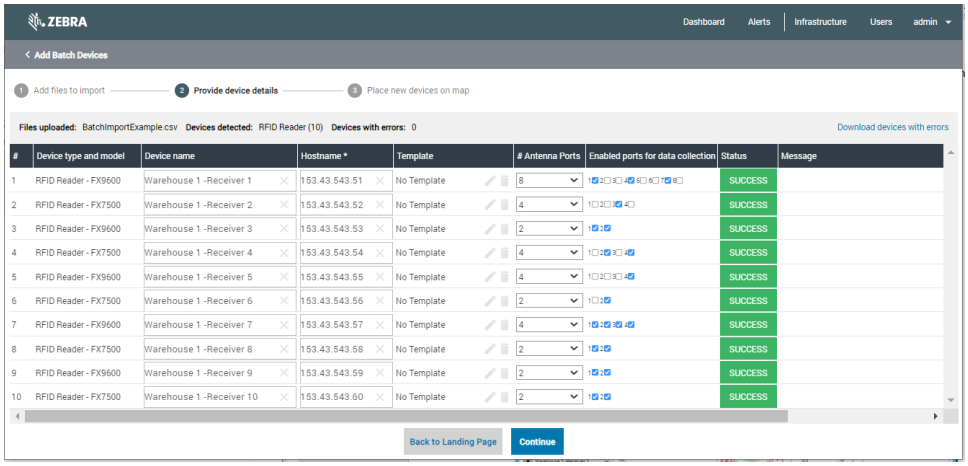
Uploading a Batch File

1. Drag the import file to the drop area. The file is shown under Uploaded Files.
2. Click **Next step: Show Devices**.

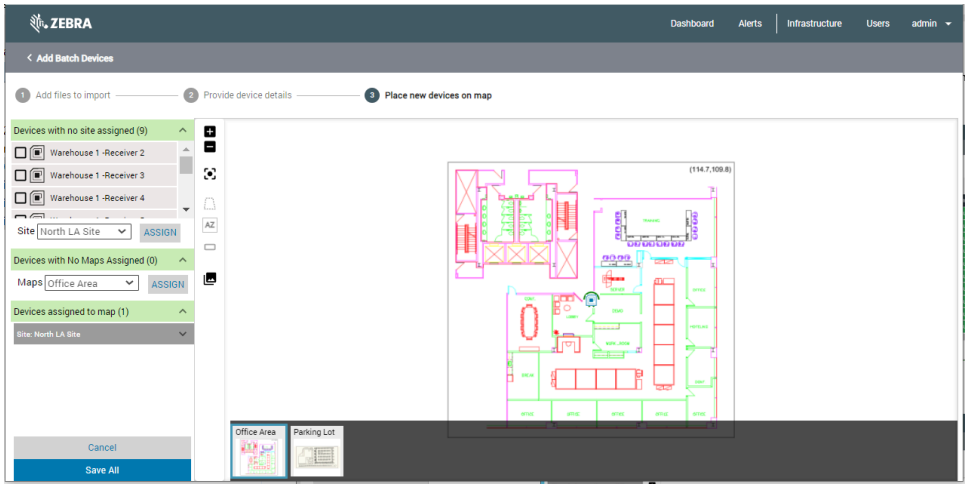


3. Click **Save** to add the readers to Device Manager. The Row Status column will show if the reader was added successfully.

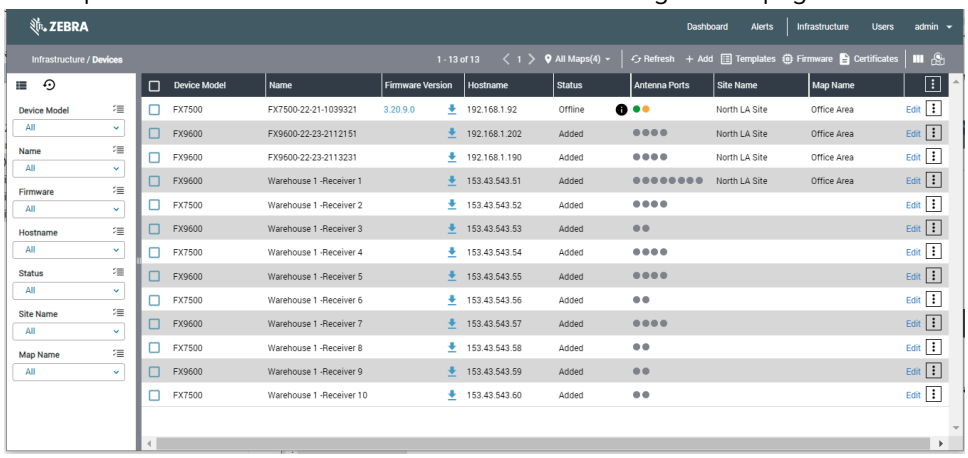
4. Click **Continue**.



5. Position the readers and antennas on the map.



The imported readers will be shown in the Device Manager main page.



6. Click **Save All**.

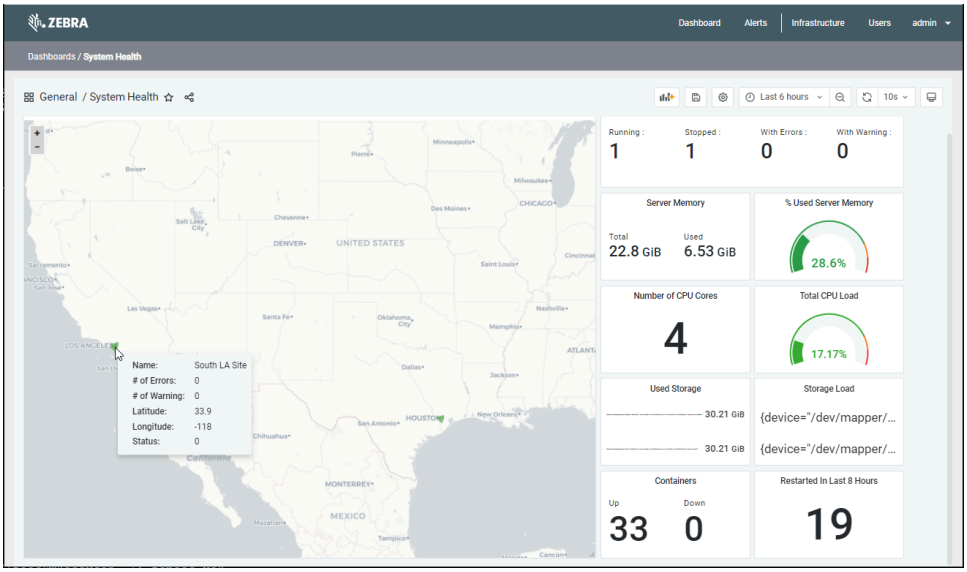
Dashboard

The Dashboard panel offers an overview of devices and MWE RFID server heath. To open the Dashboard page, click **Dashboard** on the menu bar in the Reader Management web client.

Figure 40 Dashboard Menu

The following figure shows an example of data displayed in the Dashboard panel.

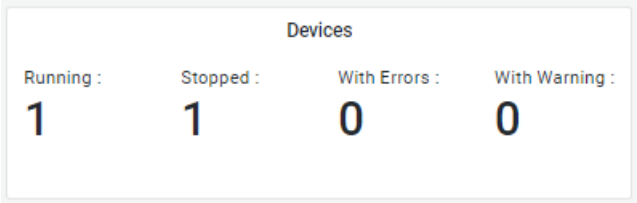
Figure 41 Dashboard



Device Status

This Device Status panel displays the number of devices Running, Stopped, With Errors, and With Warning.

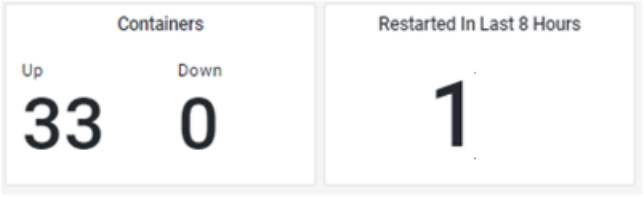
Figure 42 Device Status



Status of Services

MWE RFID Reader Management service runs as Docker containers. This panel displays how many services/containers are up or down. It also shows how many service restarts have happened in the last 8 hours.

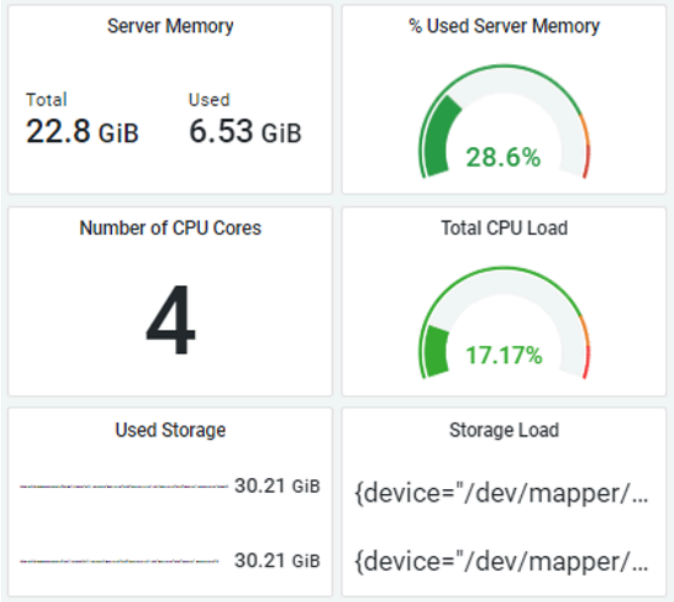
Figure 43 Status of Services



Server Resources

This Server Resources panel displays available and used memory, CPU, and disk space on the MWE RFID server (under / and /home partitions).

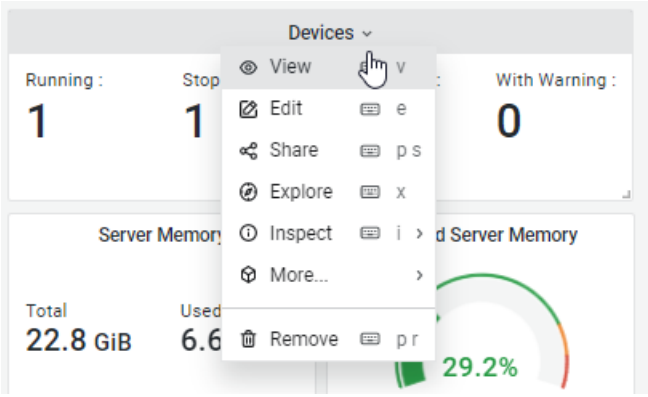
Figure 44 Server Resources



Panel Menu

Click the **Devices** drop-down. From this menu you can View or Hide the panel, Edit, Share, Explore, or Inspect the panel, and more.

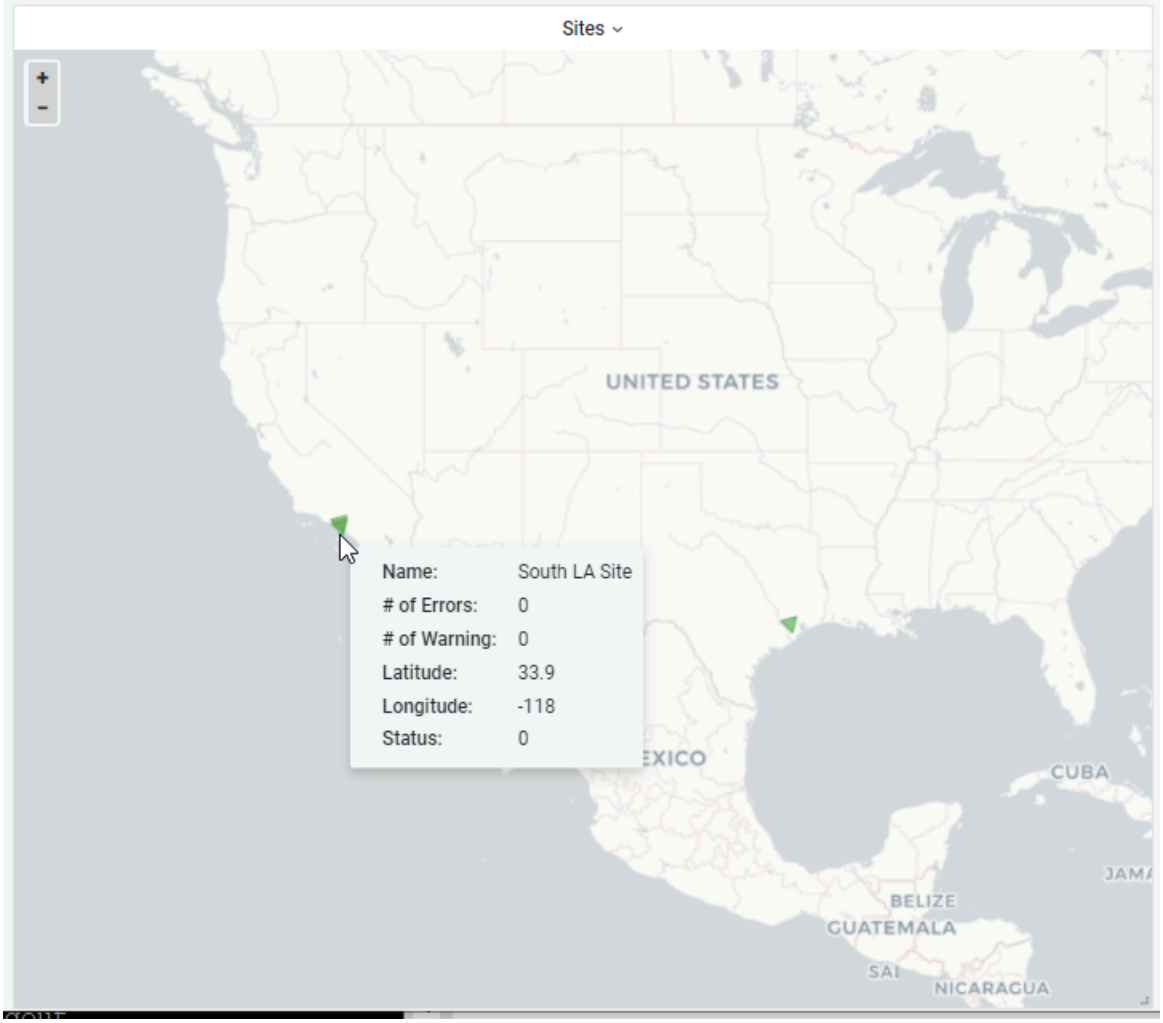
Figure 45 Panel Menu



Map

The Map panel displays each site as a triangle on the map. If no devices show errors in Device Manager, then the triangle is green. If devices at this site show errors in Device Manager, the triangle will be red. Hovering over a triangle displays a popup window with information, including the site name and the number of errors and warnings currently open for this site.

Figure 46 Map Panel



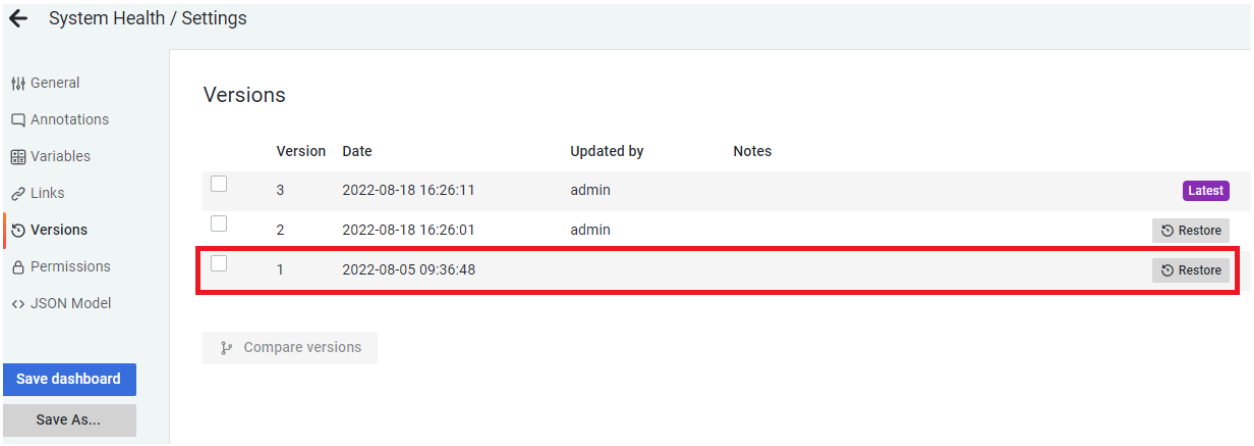
Dashboard Versions

If changes are made to the dashboard, and you want to revert the dashboard to its original state, use this url:

https://trifecta-server/trifecta/v1/app/grafana/d/teT6wS8nz/system-health?orgId=1&refresh=10s&editview=versions

The version history of the dashboard is shown, allowing you to revert the dashboard to its original form.

Figure 47 Dashboard Version History



Troubleshooting

This section provides troubleshooting solutions for potential problems.

Table 1 Troubleshooting

Problem	Potential Cause	Solution
When launching MWE RFID Reader Management web client, that is, when attempting to connect to http(s):// [server_IP_or_Name], the message is displayed: 'Cannot reach/connect to web page' or a similar message.	No network connectivity between the client machine and the MWE RFID Reader Management server. Firewall or router blocking port 80 or 443 between the client machine and MWE RFID Reader Management server.	Verify that there is network connectivity between the client machine and the MWE RFID Reader Management server. Verify that port 80 or 443 are open for traffic between the client machine and the MWE RFID Reader Management server at routers/firewalls. To verify that port 80 or 443 on the server can be reached from the Windows machine hosting the web browser, run this command in a CMD window: • For testing port 80: telnet http:// Server_IPaddress_or_Name Browser • For testing port 443: telnet https:// Server_IPaddress_or_Name Browser If you get a blank command window with no error message, that is good. If you get a 'failed to connect' or similar message, that is bad.
When entering login credentials in the login page in the MWE RFID Reader Management web client, the following message is displayed: 'Incorrect username or password.	Incorrect username or password entered.	Verify the user has the correct username and password. Have admin user reset the user password. This is done in the Users menu in the MWE RFID Reader Management web client. Have admin user delete the user and add it back. This is done in the Users menu in the MWE RFID Reader Management web client. Then the user can log in and change the password in the login account menu (rightmost link in the menu bar).

Table 1 Troubleshooting (Continued)

Problem	Potential Cause	Solution
When launching the MWE RFID Reader Management web client or when entering login credentials, the following message is displayed: 'Server error' (or some message other than 'incorrect username or password').	A required MWE RFID Reader Management service is not running.	**1.** Connect a Putty window to the MWE RFID Reader Management server. **2.** Login using the login credentials (username/password) trif-user / Zebra123. **3.** Perform the steps listed below running the commands indicated: **a.** Verify that all MWE RFID Reader Management services are up and running: # cd /data/trifecta # docker-compose ps. All services should show State = Up. If a service is down, start it manually: # docker-compose start (service name). **b.** If the issue persists, restart all services: # ./ trifecta --restart. **c.** If the issue persists, select the logs of any service that is down. Use this command to select the logs: # docker logs (service name). **d.** If the issue is unclear from the logs, send the logs to L3 Support or Engineering. **e.** Also, check messages in the browser Console: open your browser and press F12 on your keyboard to open the browser console. Attempt to log in and select error messages in the Console tab and in the Network tab in the browser console.
When trying to load a map image (.wmf file) in Site Manager, the following message is returned within a few seconds: 'Tiling process exited with code 1' or similar message.	The .wmf file is corrupted or is not a fully compliant .wmf file.	Use .wmf file generated by Autocad. When opening the project file in Autocad, if prompted, select the 'Do not show proxy graphics' option. Then export a .wmf file.
When opening or refreshing a report in the MWE RFID Reader Management web client, the following message is displayed for more than a minute: 'Retreiving data from server'.	The user has been logged out for exceeding idle time, and the browser failed to display the message 'login token expired' or similar message.	Refresh the browser page or relaunch the browser.

Table 1 Troubleshooting (Continued)

Problem	Potential Cause	Solution
When opening or refreshing a report in the MWE RFID Reader Management web client or when performing a data entry operation, one of the following messages is displayed: 'Server error' 'Could not complete action' ' 500 server error'.	A required MWE RFID Reader Management service is not running.	**1.** Connect a Putty window to the MWE RFID Reader Management (Linux) server. **2.** Login using the login credentials (username/ password) trif-user / Zebra123. **3.** Perform the steps listed below running the commands indicated: **a.** Verify that all MWE RFID Reader Management services are up and running: # cd /data/Trifecta # docker-compose ps All services should show State = Up. **b.** If a service is down, start it manually: # docker-compose start (service name). **c.** If the issue persists, restart all services: # ./ Trifecta --restart **d.** If a service still does not start, check the service logs using this command: # docker logs (service name) **e.** If the issue is unclear from the logs, please send the logs to L3 Support or Engineering. **f.** Also, check messages in the browser Console: open your browser and press F12 on your keyboard to open the browser console. Attempt to log in and check for error messages in the Console tab and in the Network tab in the browser console.