

# Resonate RFID Reader Management

Version 2.0



**ZEBRA**

## User Guide

2025/09/05

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. ©2025 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: [zebra.com/informationpolicy](https://zebra.com/informationpolicy).

COPYRIGHTS: [zebra.com/copyright](https://zebra.com/copyright).

PATENTS: [ip.zebra.com](https://ip.zebra.com).

WARRANTY: [zebra.com/warranty](https://zebra.com/warranty).

END USER LICENSE AGREEMENT: [zebra.com/eula](https://zebra.com/eula).

## 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

<b>About This Guide.....</b>	<b>6</b>
Icon Conventions.....	6
Notational Conventions.....	6
Workflow.....	8
<b>Introduction.....</b>	<b>9</b>
Resonate RFID Reader Management Overview.....	9
RFID Reader Requirements and Supported Modes.....	10
<b>Launching the Application.....</b>	<b>11</b>
Launching the Web Interface.....	11
<b>Creating Users and Assigning Roles.....</b>	<b>14</b>
Users and Roles.....	14
Creating a User.....	14
Supported Roles.....	18
<b>Sites and Maps.....</b>	<b>20</b>
Site Configuration.....	20
Adding a Site and Creating a Site Group.....	21
Adding a Map.....	22
Calibrating a Map Using Two Known Points.....	26
Calibrating a Map Using Its Width or Height.....	30
Determining the Site ID.....	32

<b>Enabling Communication with the RFID Readers.....</b>	<b>34</b>
RFID Reader Initialization.....	34
Resonate Device Initializer Basics.....	34
Using Resonate Device Initializer in Device-Discovery Mode.....	35
Selecting from Discovered Devices.....	38
<b>Deploying and Managing RFID Readers.....</b>	<b>40</b>
Managed RFID Readers.....	40
Device Grid.....	41
Device Configuration Overview.....	43
Identity Tab.....	44
Location Tab.....	45
Network Tab.....	46
Security Tab.....	47
Antennas Tab.....	48
Modes Tab for FX9600.....	50
Modes Tab for ATR7000.....	60
Configuring Dual-Portal Directionality.....	71
Monitoring Device Health and Status.....	73
RFID Reader Commands and Actions.....	75
Replacing an RFID Reader.....	76
<b>Templates.....</b>	<b>77</b>
Templates Overview.....	77
Creating a Template.....	77
Using a Template to Configure a Single RFID Reader.....	78
Using a Template to Configure Multiple Selected RFID Readers.....	79
<b>Connecting to RFID Readers to Get Tag Read Data.....</b>	<b>81</b>
Reader Connection for Tag Read Data.....	81
<b>Digital Certificates.....</b>	<b>83</b>
Certificates Overview.....	83

Installing a CA Certificate.....	85
<b>Alerting Targets.....</b>	<b>87</b>
Alerting Targets Overview.....	87
How Alerting Works.....	87
Steps to Send Alerts to Targets.....	88
Available Alerts.....	88
add-alerting-target.sh.....	89
add-alerting-target.sh Usage Examples.....	93
add-alerting-target.sh Advanced Usage Information and Examples.....	95
Sending Alerts to Zebra's OpsRamp instance.....	97
Validating the Alert Configuration.....	98
<b>Troubleshooting Application and RFID Reader Issues.....</b>	<b>99</b>
Resolving Application Issues.....	99
Determining the Root Cause of RFID Reader Issues.....	100
Troubleshooting the AlertManager Configuration.....	103
AlertManager Diagnostic Commands.....	104
<b>Disaster Recovery.....</b>	<b>105</b>
Recovery Overview.....	105
Recovery Setup.....	105
Setting Up Database Backups.....	106
Snapshot Backups.....	108
Recovery in the Event of a Disaster.....	109
<b>High Availability Operation.....</b>	<b>111</b>
Fault Tolerance and High Availability.....	111

# About This Guide

This guide provides information about using Resonate RFID Reader Management.

## Icon Conventions

The documentation set is designed to give the reader more visual clues. The following visual indicators are used throughout the documentation set.



**NOTE:** The text here indicates information that is supplemental for the user to know and that is not required to complete a task.



**IMPORTANT:** The text here indicates information that is important for the user to know.



**CAUTION:** If the precaution is not heeded, the user could receive a minor or moderate injury.



**WARNING:** If danger is not avoided, the user CAN be seriously injured or killed.



**DANGER:** If danger is not avoided, the user WILL be seriously injured or killed.

## Notational Conventions

The following notational conventions make the content of this document easy to navigate.

- **Bold** text is used to highlight the following:
  - Dialog box, window, and screen names
  - Dropdown list and list box names
  - Checkbox and radio button names
  - Icons on a screen
  - Key names on a keypad
  - Button names on a screen

- Bullets (•) indicate:
  - Action items
  - List of alternatives
  - Lists of required steps that are not necessarily sequential
- Sequential lists (for example, those that describe step-by-step procedures) appear as numbered lists.

### Workflow

This section provides an overview of the Resonate RFID Reader Management workflow.

1. Install Resonate RFID Reader Management; refer to the software installation guide.
2. Launch the Resonate RFID Reader Management web interface from your web browser and log in, as described in [Launching the Web Interface](#) on page 11.
3. Set up access for the different users of your Resonate RFID Reader Management instance, as described in [Creating a User](#) on page 14.
4. Add one or more sites where your RFID readers are located, and then upload site maps to each site, as described in [Sites and Maps](#) on page 20.
5. Enable communication between Resonate RFID Reader Management and your RFID readers, as described in [Enabling Communication with the RFID Readers](#) on page 34 .
6. Configure your RFID readers, as described in [Device Configuration Overview](#) on page 43.

When configuring several RFID readers with the same configuration, you can create and use a template for initial configuration, as described in [Templates](#) on page 77.

7. Activate your RFID readers, and then connect to them to receive to their tag read data as described in [Connecting to RFID Readers to Get Tag Read Data](#) on page 81.
8. Monitor and manage your RFID readers, as described in [Monitoring Device Health and Status](#) on page 73 and [RFID Reader Commands and Actions](#) on page 75.



# Introduction

This section provides an overview of Resonate RFID Reader Management and its interface.

## Resonate RFID Reader Management Overview

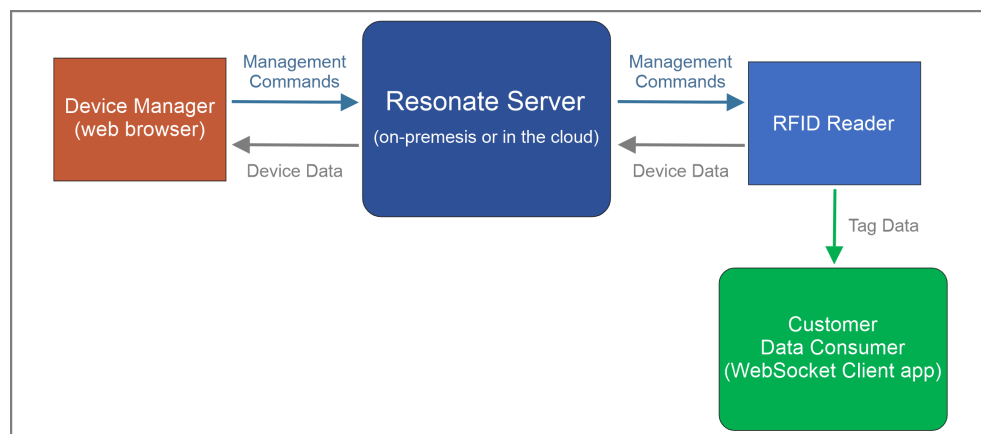
Resonate RFID Reader Management is a powerful, scalable, server-based platform for deploying, monitoring, managing, and configuring Zebra RFID readers in your asset tracking solution. It supports readers located on-site or around the world. It allows you to set up and define new sites and groups of manageable readers, update reader firmware and certificates, and update reader operating configurations. Additionally, it monitors deployed RFID readers, reporting any alerts and errors.

Main access to Resonate RFID Reader Management's functionality is through its web interface, although a REST API interface is also available. The web interface provides a clean and intuitive interface for managing the RFID readers. To access the web interface, use your web browser to navigate to the Resonate server address specified during Resonate RFID Reader Management installation. For installation instructions, architecture, and deployment options, refer to the Resonate RFID Reader Management Software Installation Guide.

Using the web interface, users and administrators of Resonate RFID Reader Management can access their specific functionalities. A management console allows for user administration, role assignment, and access control, ensuring users can only access features permitted by their roles.

Resonate RFID Reader Management can run locally with the RFID readers or connect to them from a cloud-hosted environment. Readers connect over standard secure internet connections using HTTPS and secure web sockets.

**Figure 1** Resonate Data Flow



You must initialize the RFID readers to work with Resonate RFID Reader Management using Resonate Device Initializer, a Windows utility that can discover the readers on the same subnet and report them to Resonate RFID Reader Management. You then choose which readers Resonate should manage. Resonate initializes these readers and installs the Resonate Agent on the readers. Resonate Agent enables the readers' cloud-ready protocols, forces improved connection security, and securely connects them to the Resonate RFID Reader Management instance responsible for managing them. After the RFID readers are initialized and running Resonate Agent, Resonate RFID Reader Management can take over and manage those readers through their useful operating life.

For the list of supported readers and reader modes, see [RFID Reader Requirements and Supported Modes](#) on page 10.

Resonate RFID Reader Management supports fault tolerance and high availability. Fault tolerance ensures Resonate software can recover automatically without human intervention in the event of a software failure, without the expectation of continuous uptime. High availability adds the ability to increase overall uptime by distributing the software operation across multiple machines (nodes). If a machine has a catastrophic hardware failure, the overall system can continue to operate. For information, refer to [Fault Tolerance and High Availability](#) on page 111.

## RFID Reader Requirements and Supported Modes

Resonate RFID Reader Management currently only supports the following Zebra RFID readers:

- FX9600
- ATR7000

In addition, for ATR7000 readers, Resonate RFID Reader Management only supports Portal Directionality mode. Consult your Zebra sales representative for future support of other Zebra fixed RFID readers and modes.

The RFID readers must run a firmware version compatible with Resonate RFID Reader Management. If they are currently running an earlier version, Resonate Device Initializer automatically elevates them to a firmware version high enough to support Resonate.

Resonate RFID Reader Management displays the firmware version and allows you to upgrade or downgrade the firmware of one or multiple readers simultaneously.

Currently, Resonate RFID Reader Management only supports a single type of data endpoint: WebSocket. Consult your Zebra sales representative for the roadmap of other endpoint types (for example, webhooks and MQTT).

# Launching the Application

This section describes launching Resonate RFID Reader Management.

## Launching the Web Interface

After installing Resonate RFID Reader Management, the system administrator receives an email notification and must use the link provided in the email to navigate to the new Resonate RFID Reader Management site to configure their password and verify their email. The system administrator should follow the instructions outlined below.

When following these instructions, note that Resonate RFID Reader Management only supports the Google Chrome web browser version 120 and above; Microsoft Edge and other Chromium-based derivatives might also work. Depending on the browser version, there might be some differences between the windows depicted in this document and those in your version.

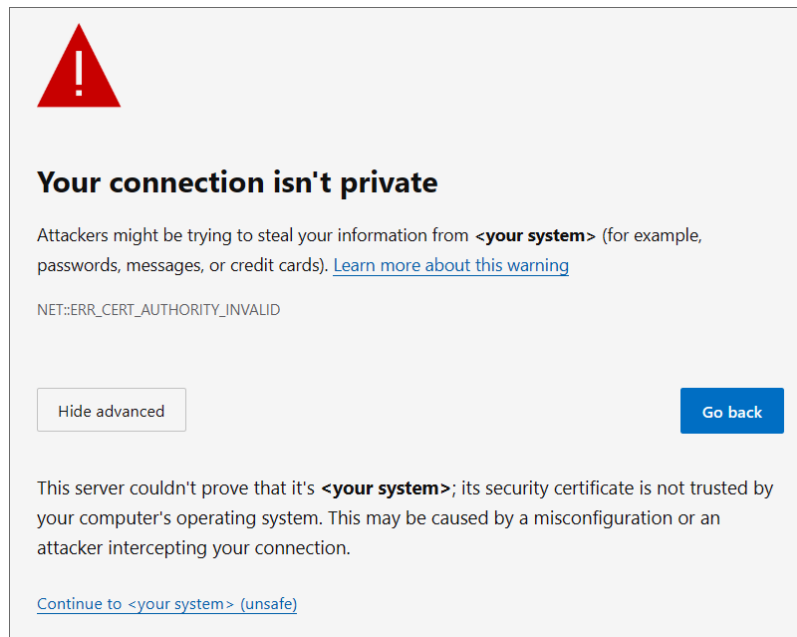
1. Click the link in the email.
2. If the browser displays a `not secure error` or a `certificate error` (or similar warning), click **Advanced** to expand the message.



**NOTE:** This error/warning occurs when using HTTPS because, by default, the Resonate installation script installs a self-signed Resonate certificate on the server. To avoid this error when accessing the web interface, add your own trusted enterprise certificate to the new Resonate server. Typically, do this at Resonate installation time or before adding readers;

otherwise, you will need to re-initialize the readers. For instructions, refer to [Resonate's Web Interface](#).

The message expands to the following (or similar):



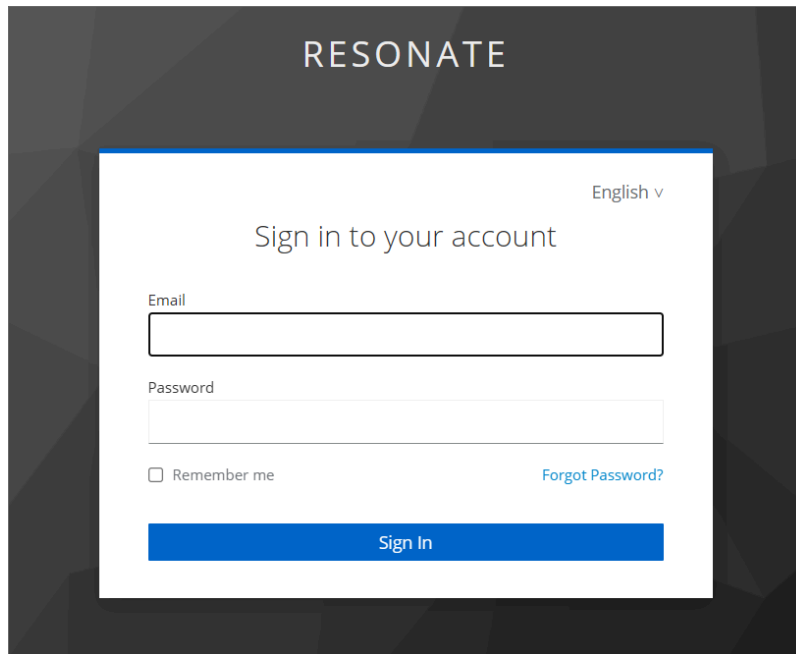
3. Click **Continue to <your system> (unsafe)** to access the Resonate RFID Reader Management site.
4. Follow onscreen instructions to configure the System Administrator password and confirm the email address.

Ensure that **Sign out from other devices** is enabled when setting the password.

A message displays `Your account has been updated` when successful.

5. Click **Back to Application** to return to the login page of the Resonate RFID Reader Management instance.

**6. Log in.**



The landing page includes a menu bar at the top with the following menus: **Infrastructure**, **Users**, and **<user>** (the name of the account currently logged in). The visibility of menu items depends on a user's assigned role and access permissions.

- 7.** Click **<user>** > **Settings** and set up your account settings.
- 8.** Set up other user accounts. To do so, refer to [Creating Users and Assigning Roles](#) on page 14.
- 9.** To sign out, click **<user>** > **Sign Out**.

To launch the Resonate RFID Reader Management web interface without the email, use your browser to navigate to:

```
https://<Fully Qualified Domain Name of Resonate Server>/
```

Replace <Fully Qualified Domain Name of Resonate Server> with the FQDN of the Resonate server, specified during installation.

# Creating Users and Assigning Roles

This section describes creating users and assigning them roles.

## Users and Roles

Resonate RFID Reader Management grants access to defined users based on their roles. Users with an administrator role can create users and assign roles from the **Users > Keycloak** menu, which opens the Keycloak main page. Resonate RFID Reader Management uses Keycloak to manage user authentication and role-based access control (RBAC).

When installing Resonate RFID Reader Management, you specify the first administrator. Refer to the Software Installation Guide.



**NOTE:** Groups are not currently supported.

You can configure the Keycloak trifecta-realm to use various authentication rules, including password policies for expiration and complexity, as well as support for Single Sign-On (SSO). If a user's password expires, they are asked for a new password when they next log in. For SSO, refer to the third-party open source Keycloak documentation at <https://www.keycloak.org/>.

## Creating a User

The following describes how to create a user account. You must have an administrator role.



**NOTE:** For SSO, refer to the third-party open source Keycloak documentation at <https://www.keycloak.org/>.

1. Navigate to **Users > Keycloak**.

The Keycloak main page is displayed.

## Creating Users and Assigning Roles

2. Select the **Users** tab on the left.

**ZEBRA** Infrastructure Users admin@customer.com

Users / Keycloak

trifecta-realm

**Users**  
Users are the users in the current realm. [Learn more](#)

User list

Search user → [Add user](#) Delete user 1 < >

<input type="checkbox"/>	Username	Email	Last name	First name	Status	
<input type="checkbox"/>	admin@customer.com	admin@customer.com	Nidea	Ida	—	⋮
<input type="checkbox"/>	user@customer.com	user@customer.com	Knapp	Anita	—	⋮

The **Users** page displays on the right.

3. Click **Add user**.

The **Create user** page is displayed.

The screenshot shows the ZEBRA Users / Keycloak interface. The top navigation bar includes the ZEBRA logo, 'Infrastructure', 'Users', and a user profile 'admin@customer.com'. The breadcrumb trail is 'Users > Create user'. The left sidebar lists various management options, with 'Users' currently selected. The main content area is titled 'Create user' and contains the following form elements:

- Required user actions:** A dropdown menu with 'Select action' as the current selection.
- Email:** A text input field.
- Email verified:** A toggle switch currently set to 'No'.
- First name:** A text input field.
- Last name:** A text input field.
- Groups:** A text input field.

At the bottom of the form are two buttons: 'Create' and 'Cancel'.

4. From the **Required user actions** dropdown list, select the actions that the user needs to take upon first logging into Resonate RFID Reader Management.

You can select multiple items.



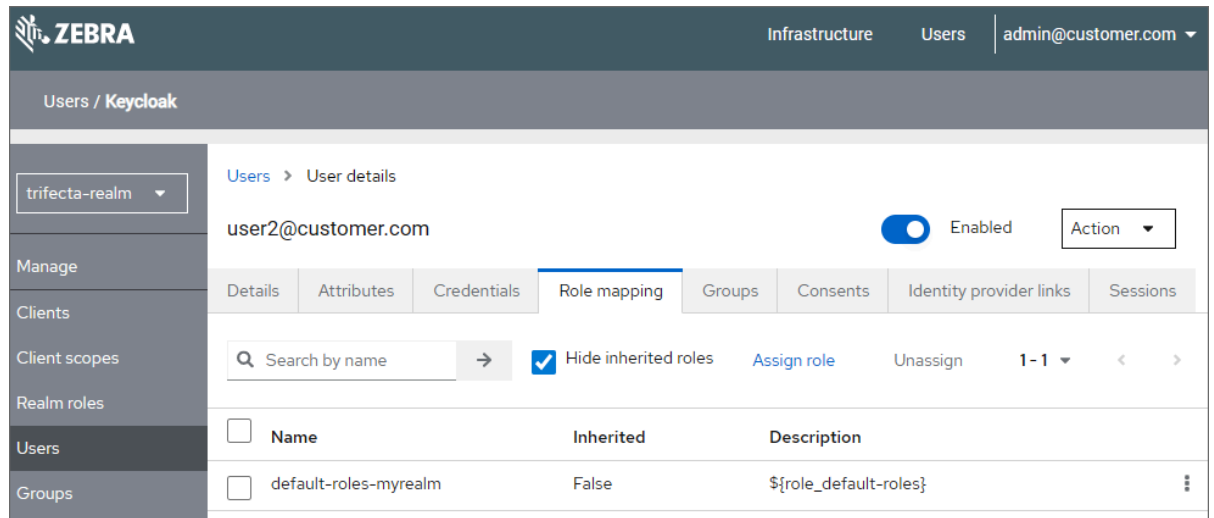
**NOTE:** If you select **Verify Email** as one of the actions, the user immediately receives an email with a link to create a password when you click **Create**; however, they will not have any other permissions since their role has not yet been set. To set the role and/or an initial password before they receive an email, ensure this option is not selected before clicking **Create**.

5. Enter the user's email address, first name, and last name in their respective fields.
6. Specify whether you have verified the user's email address.
7. Leave **Groups** as is. Groups are not currently supported.
8. Click **Create**.

The user is created, and the **User details** page is displayed.



- On the **Role mapping** tab, click **Assign role**.



The **Assign roles** page is displayed.


- Select the user's roles to establish their permissions, and click **Assign role**.

For information on the supported roles, refer to [Supported Roles](#) on page 18.

- On the **Credentials** tab, click either:

- Credential Reset:** Sends the user an email with a link to perform specific actions, such as setting their password, within a defined time period. A dialog allows you to select the actions (such as, **Update Password**) and expiration time before the email is sent.
- Set password:** Allows you to set the user's password. If the **Temporary** option is enabled, the user must change their password after logging in.

You can cancel out of either action.

Edit a user's account by clicking on their user name on the Keycloak main page and changing the required fields on the different tabs. To delete an existing user's account, select  **User Settings > Delete**.

## Supported Roles

Assign users' roles to define their permissions within the Resonate RFID Reader Management web interface. You must have an administrator role.

Manage a user's roles from the **Role mapping** tab of their Keycloak **User details** page. The page lists their current roles.

Click **Assign role** to assign additional roles. This displays the **Assign roles** page.

**Figure 2** Assign roles page

Assign roles to user2@customer.com

Filter by realm roles Search by role name 1 - 33

<input type="checkbox"/> Name	Description
<input type="checkbox"/> alerts_settings_add	
<input type="checkbox"/> alerts_settings_edit	
<input type="checkbox"/> alerts_settings_view	
<input type="checkbox"/> decoder_settings_edit	
<input type="checkbox"/> decoder_settings_view	
<input type="checkbox"/> device_create	
<input type="checkbox"/> device_edit	

Assign Cancel

The page lists all roles that are currently not assigned to the user. Set the dropdown to **1-50** to see all roles. The relevant roles that affect user capability are the following, and are the only roles currently supported.



**NOTE:** The rest of the roles are for internal use only and do not affect the user's capabilities.

**Table 1** Supported Roles

Role	Description
<b>device_create</b>	Allows a user to add RFID readers for management.
<b>device_edit</b>	Allows a user to configure or delete managed RFID readers.
<b>device_view</b>	Allows a user to view all managed RFID readers.

**Table 1** Supported Roles (Continued)

Role	Description
<b>file_create</b>	Allows a user to upload files to Resonate RFID Reader Management (for example, certificates).
<b>file_edit</b>	Allows a user to delete files. Note that editing of files is not supported.
<b>file_view</b>	Allows a user to view file information and to download files.
<b>map_edit</b>	Allows creation, modification, and deletion of levels, sites, site groups, regions, obstructions, datums, and uploading maps.
<b>map_view</b>	Allows viewing of levels, sites, site groups, regions, obstructions, datums, and uploading maps.
<b>user_keycloak_edit</b>	Allows user administration, including roles and groups.
<b>user_keycloak_view</b>	Allows viewing of users, including roles and groups.

To assign a user an administrator role, enable the checkbox (near **Name**) in the header; this selects all roles.

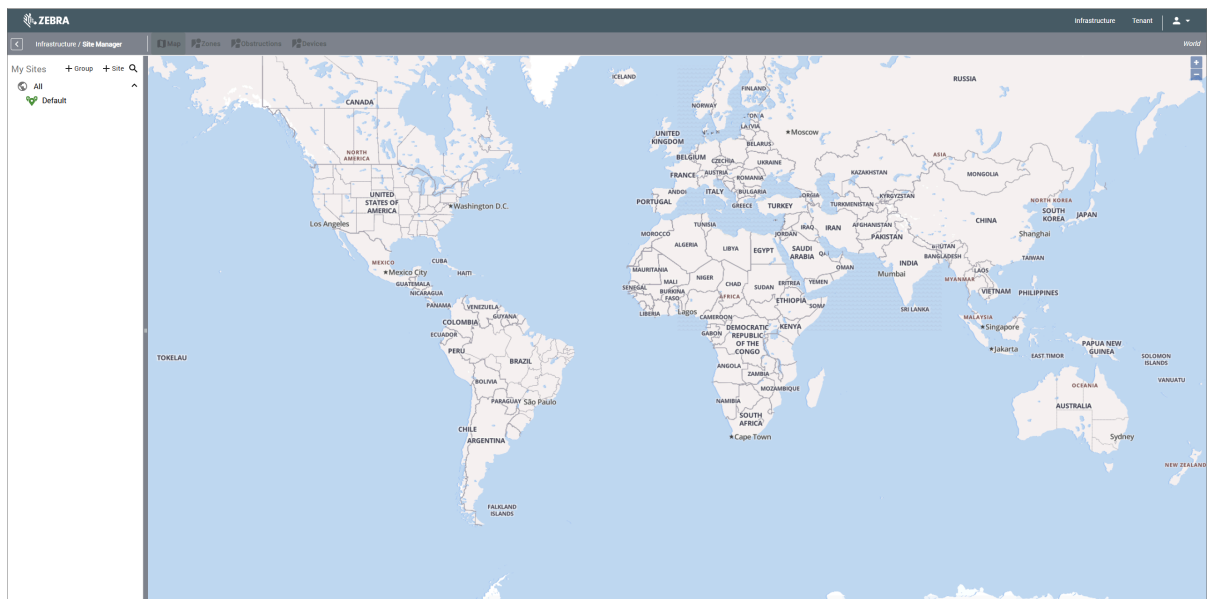
# Sites and Maps

This section describes adding sites and maps to the Resonate RFID Reader Management Site Manager.

## Site Configuration

Before adding a reader to Resonate RFID Reader Management, you must add a site and load a site map. This is done on the **Site Manager** page in the web interface, accessible using **Infrastructure > Site Manager**. You can have multiple sites and multiple maps under each site.

**Figure 3** Site Manager



The left panel displays the sites. The main window displays the location of each site and the readers in each site map, depending on what you select in the left panel.

## Adding a Site and Creating a Site Group

The following steps describe how to add a site to Site Manager and list it as part of a site group.

1. Navigate to **Infrastructure > Site Manager**.
2. If you want to list the new site with other sites under a single group name (site group), click **+Group** in the left panel, and define the group name (for example, New York), unless it already exists.
3. Click **+ Site** in the left panel to start defining the site.

The **Add Site** window is displayed.

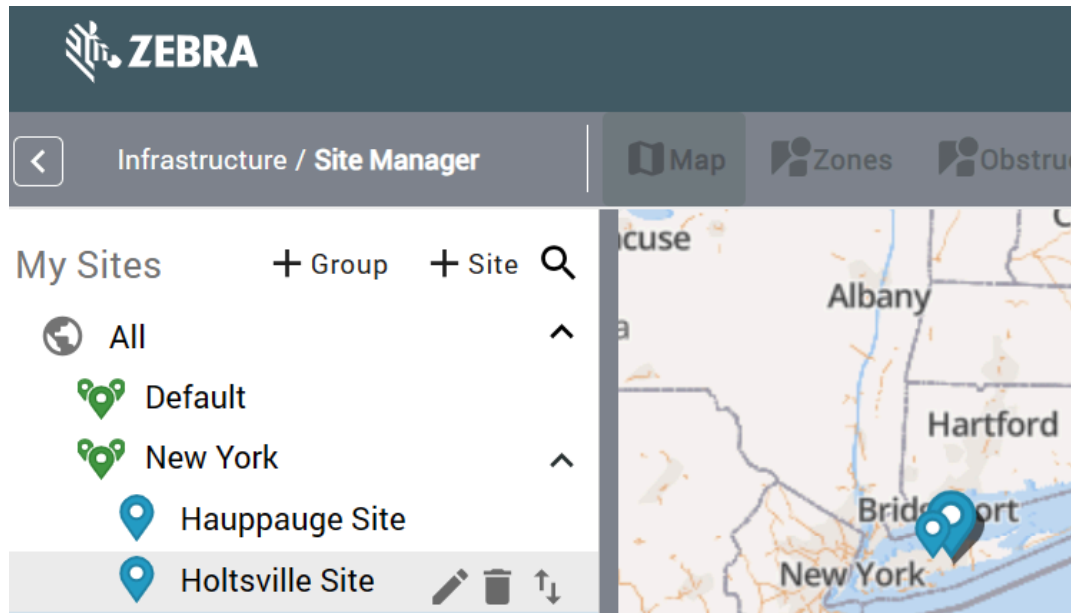
4. In the **Site Name** field, enter a name for the site (for example, Holtsville Site).
5. In the **Location** field, enter an address.  
A blue pin is placed on the map at that location. You can zoom and pan the map, and drag the blue pin to a more accurate location on the map.
6. If you are adding the new site to a site group, select the site group from the **Site Group** drop-down list.  
It only lists defined site groups. To skip using a site group, select **Default**.
7. From the **Time Zone** drop-down list, select the time zone.
8. In the **Device Domain** field, enter the domain to use for the site (for example, customer.com).  
All subnets must be on the same domain. To discover all supported RFID readers on a subnet, each subnet requires its own Resonate Device Initializer utility.
9. In the **Metadata** field, enter the text to display with events reported for devices at this site.  
For example, if set to `store #54`, any event for a device at this site includes the text `store #54`.
10. Click **Save**.




The main map shows a pin at the new site location, and the left panel lists the new site under the selected site group (for example, New York), if one was selected, or under **Default**.



**NOTE:** The **Publish** button is not functional.

11. Add additional sites as needed.




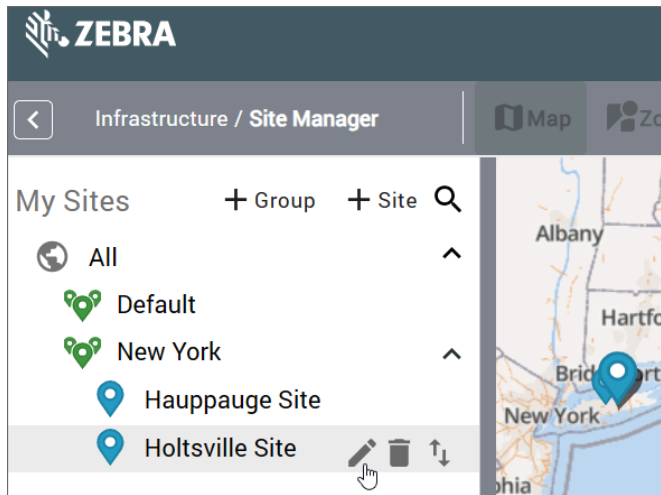
To edit a site's definition or delete the site, hover over its name; then, click the  **Edit** or  **Delete** button, respectively. To move the site to a different site group, click and drag the  **Move** button instead. After adding a site to Site Manager, add your site map(s) to the site. Refer to [Adding a Map](#).

## Adding a Map

You can add one or more maps to each site listed in Site Manager. Resonate RFID Reader Management uses the maps to show the location of managed RFID readers. For a multistory building site, add a map for each floor that has RFID readers to manage. For a campus site with several buildings and parking lots, add a map for each area that has RFID readers to manage.

1. Navigate to **Infrastructure > Site Manager**.

2. Hover over the site name or next to it and click the  **Edit** button.



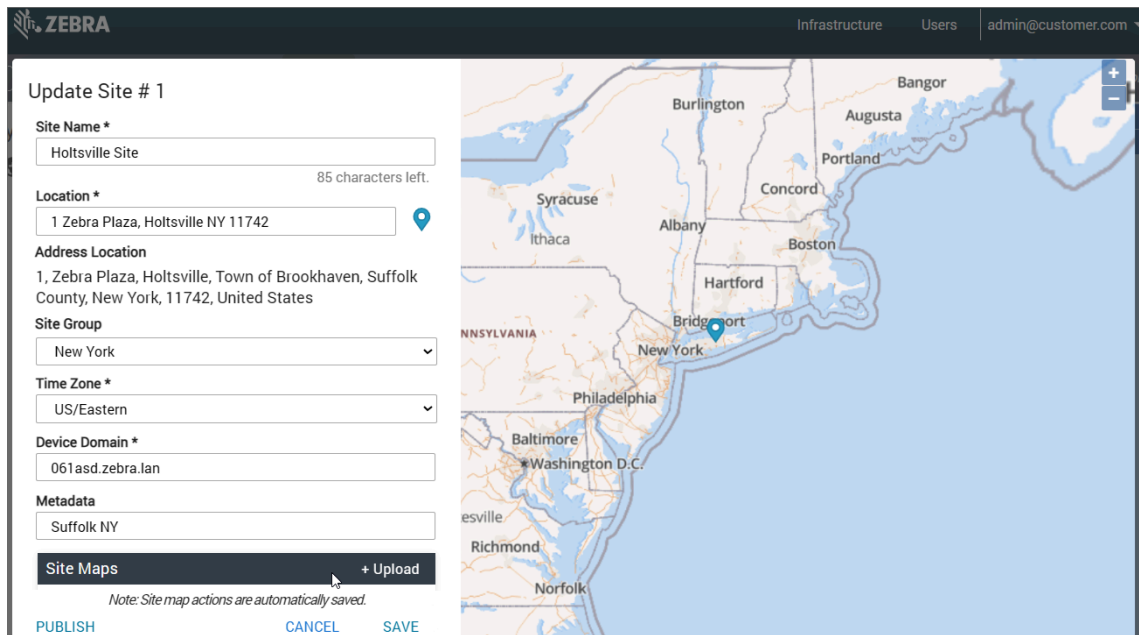
The **Update Site** window is displayed.

3. Note the site number (site ID) at the top of the Update Site window.

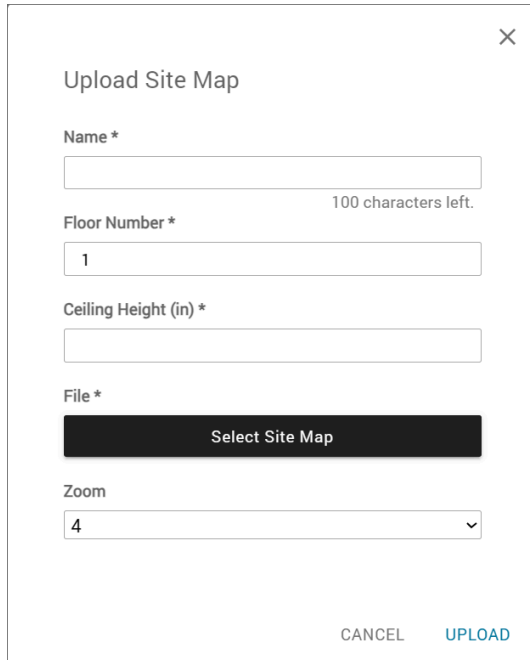


**NOTE:** During device initialization, you will need to specify this number.

4. Click **+ Upload**.



5. In the **Name** field, enter a name for the site map (for example, Floor1).



Upload Site Map

Name \*

100 characters left.

Floor Number \*

1

Ceiling Height (in) \*

File \*

Select Site Map

Zoom

4

CANCEL UPLOAD

6. In the **Floor Number** field, enter the floor number for this map, starting at 0 for the first floor.
7. In the **Ceiling Height** field, enter the floor-to-ceiling height for this map, in inches.
8. Click **Select Site Map** and navigate to the location of the site map file.
- Resonate RFID Reader Management supports Windows metafiles (.wmf), Joint Photographic Experts Group (.jpg), Portable Network Graphics (.png), Wireless Bitmap (.wbmp), Bitmap (.bmp), and Graphical Interchange Format (.gif).
  - A maximum file size of 8 MB is recommended.
9. In the **Zoom** field, set the maximum level to which users can zoom in when viewing the site map in the web interface.
- The default value is 4, and the maximum available value is 8. The higher the value, the longer the load time.
10. Click **Upload**.

The upload process can take a few seconds to many minutes, depending on the map size and the **Zoom** setting. 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 return to the site properties window,



but the tiling process continues in the background. The name of the uploaded site map is listed under **Site Maps**, and the map image is displayed in the lower section of the window.

**ZEBRA** Infrastructure Users admin@customer.com

### Update Site # 1

**Site Name \***  
Holtsville Site 85 characters left.

**Location \***  
1 Zebra Plaza, Holtsville NY 11742

**Address Location**  
1, Zebra Plaza, Holtsville, Town of Brookhaven, Suffolk County, New York, 11742, United States

**Site Group**  
New York

**Time Zone \***  
US/Eastern

**Device Domain \***  
061asd.zebra.lan

**Metadata**  
Suffolk NY

**Site Maps** + Upload

- floor1

Note: Site map actions are automatically saved.

PUBLISH CANCEL SAVE

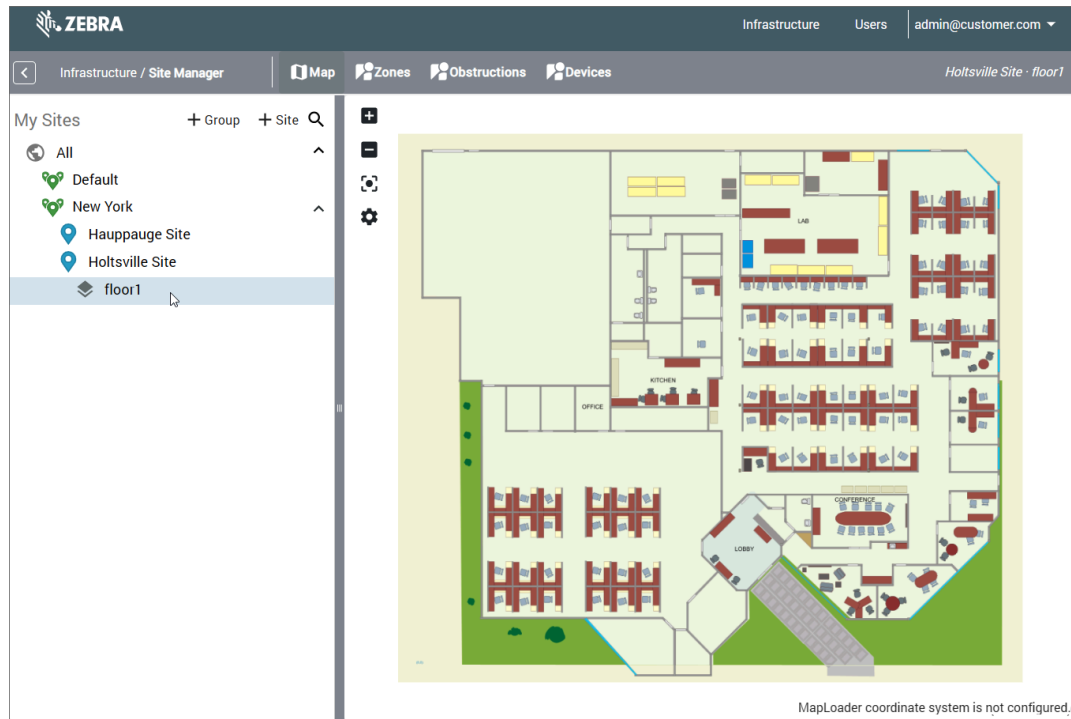
11. Click **Save**.

The site map is listed under the site name.



**NOTE:** The **Publish** button is not functional.

12. Click the map name to view the map.



13. Add additional maps as needed.

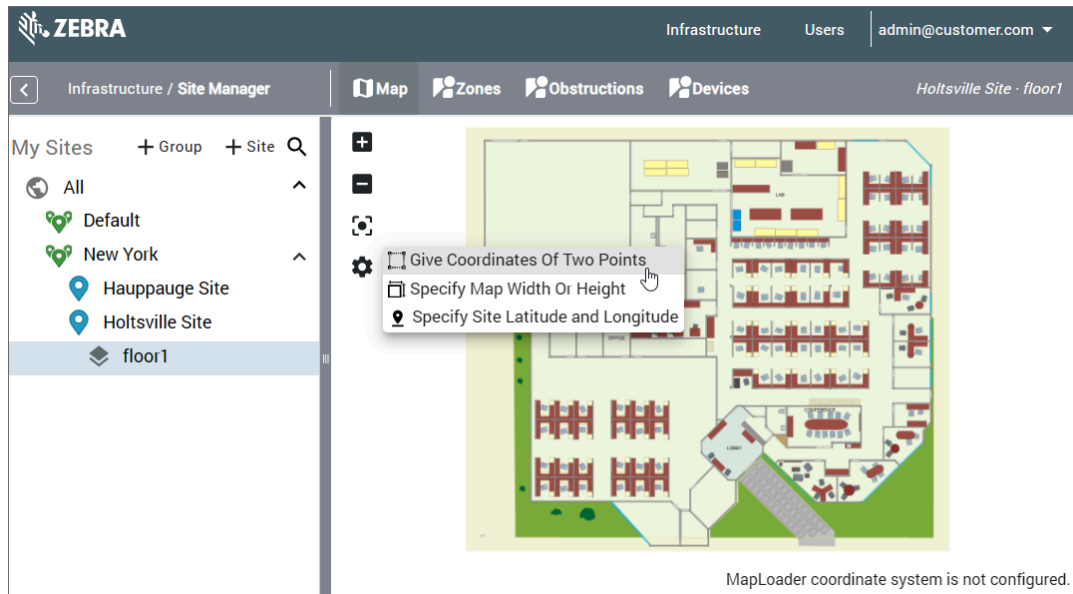
## Calibrating a Map Using Two Known Points

Before using a site map, you must calibrate it. To calibrate it using two known points, follow the steps below.

To calibrate it with its width or height, refer to [Calibrating a Map Using Its Width or Height](#) on page 30.

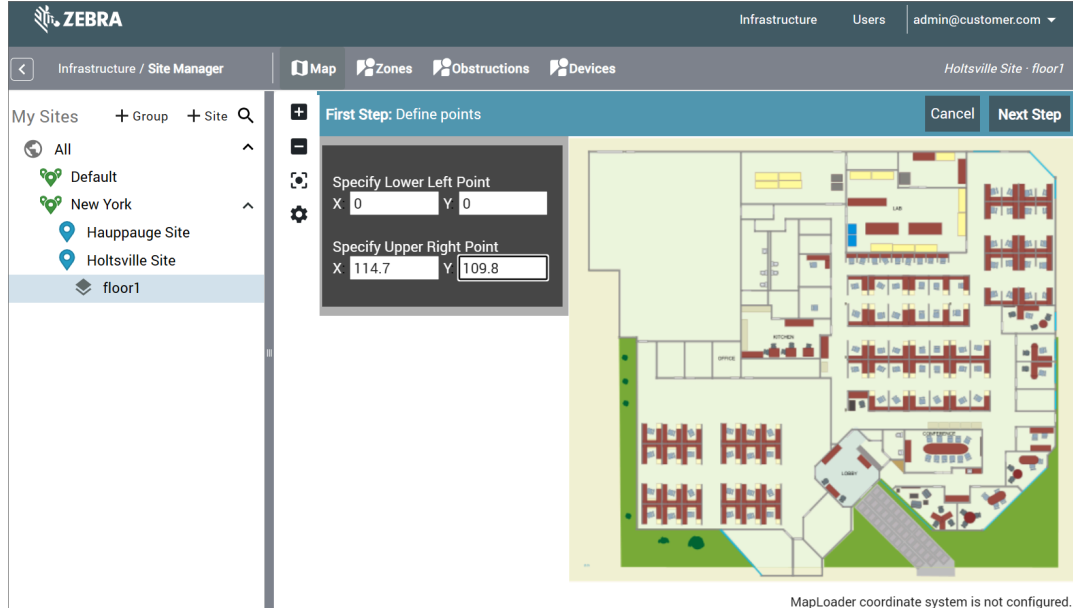
1. Navigate to **Infrastructure > Site Manager**.
2. Click the map name.

3. Select **Configure Map > Give Coordinates of Two Points** in the map window toolbar.



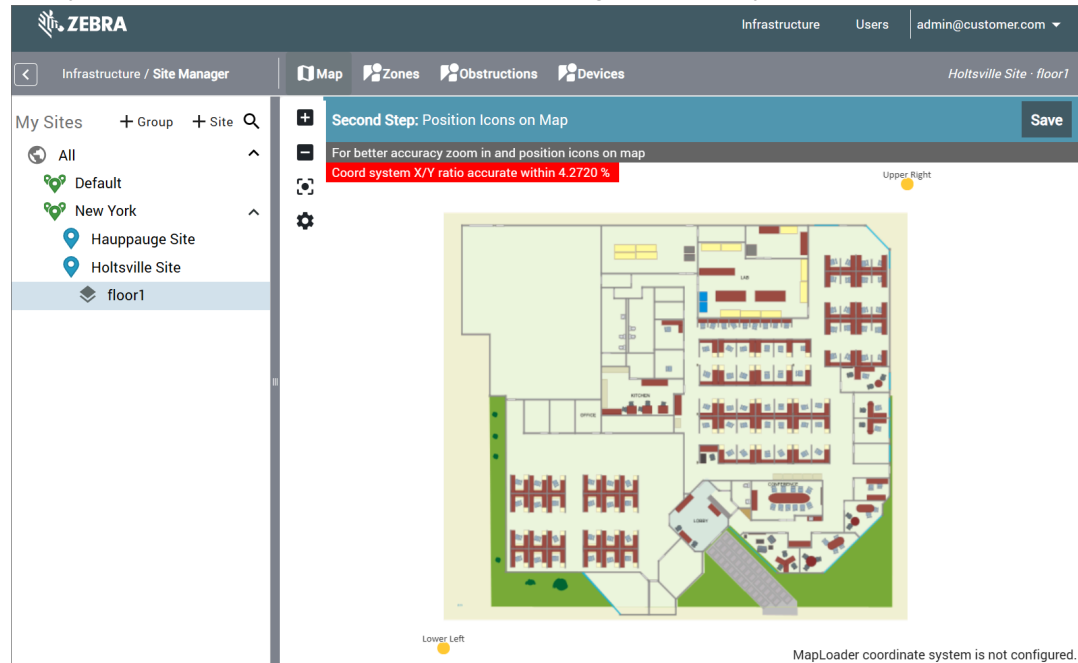
Notice the label at the bottom-right, which reads MapLoader coordinate system is not configured. Although the site map image is uploaded, the XY coordinate system has not been defined for the map. You accomplish this by calibrating the site map.

4. Enter the known X- and Y-coordinates for two known points on opposite corners of the map; units are in inches.



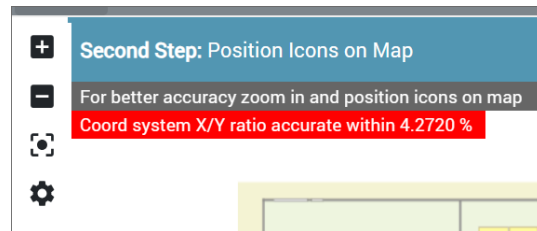
5. Click **Next Step**.

Two yellow dots labeled **Lower Left** and **Upper Right** are displayed.



6. 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.

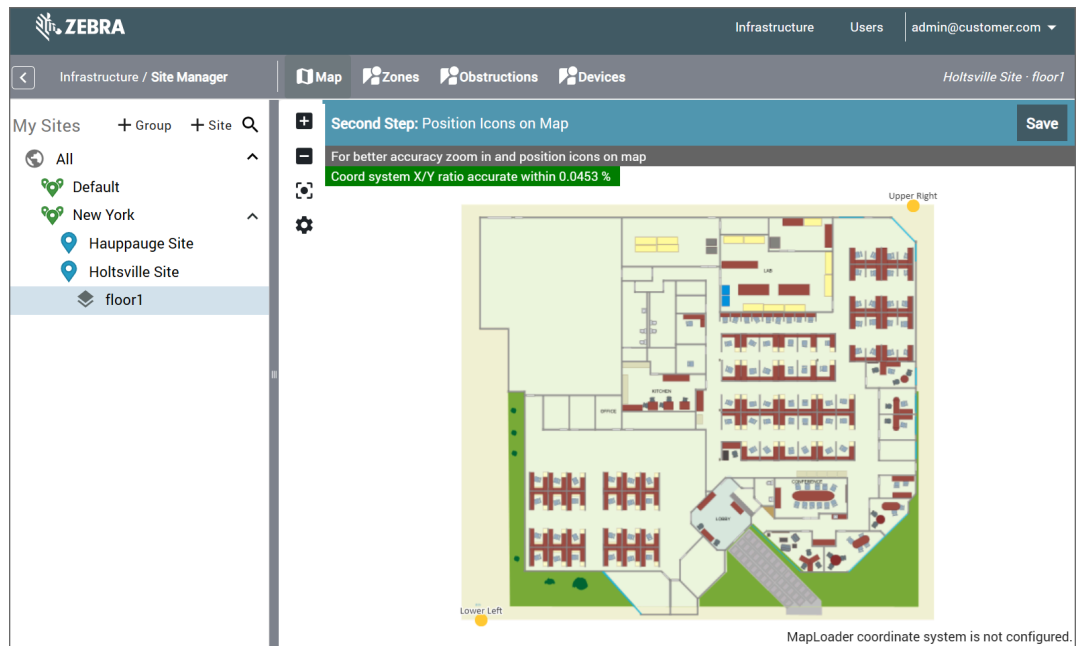
Notice the red bar at the top-right of the map window.



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

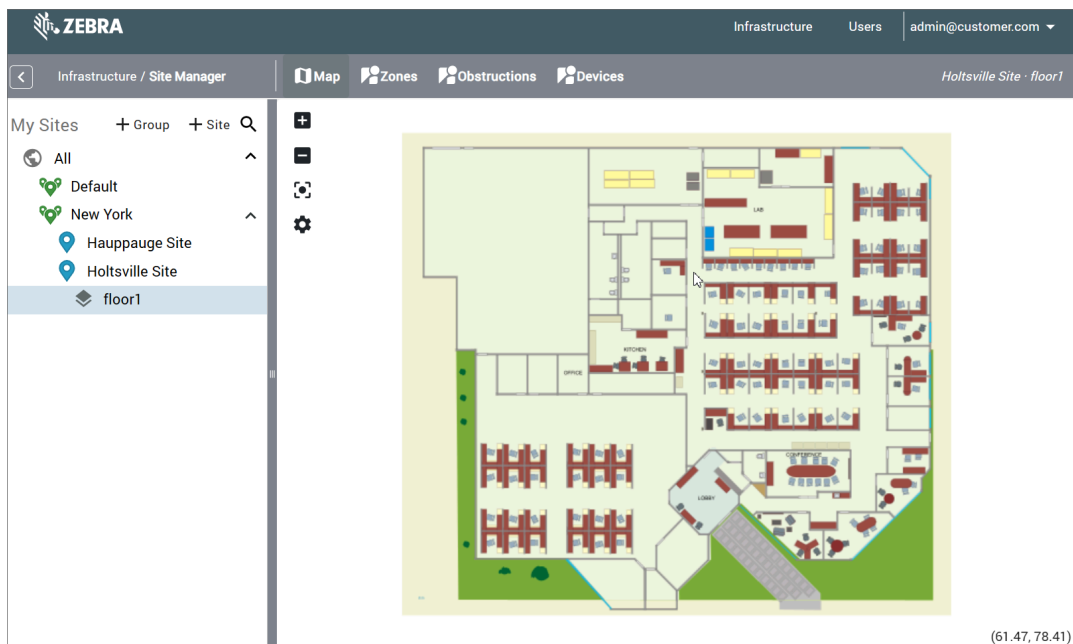
## Sites and Maps

you move the yellow calibration dots on the map, and the agreement of the aspect ratios is greater than 1%.



### 7. Click **Save**.

The map is now calibrated. Move the mouse over the map. The X- and Y-coordinates display in the bottom-right of the map window.

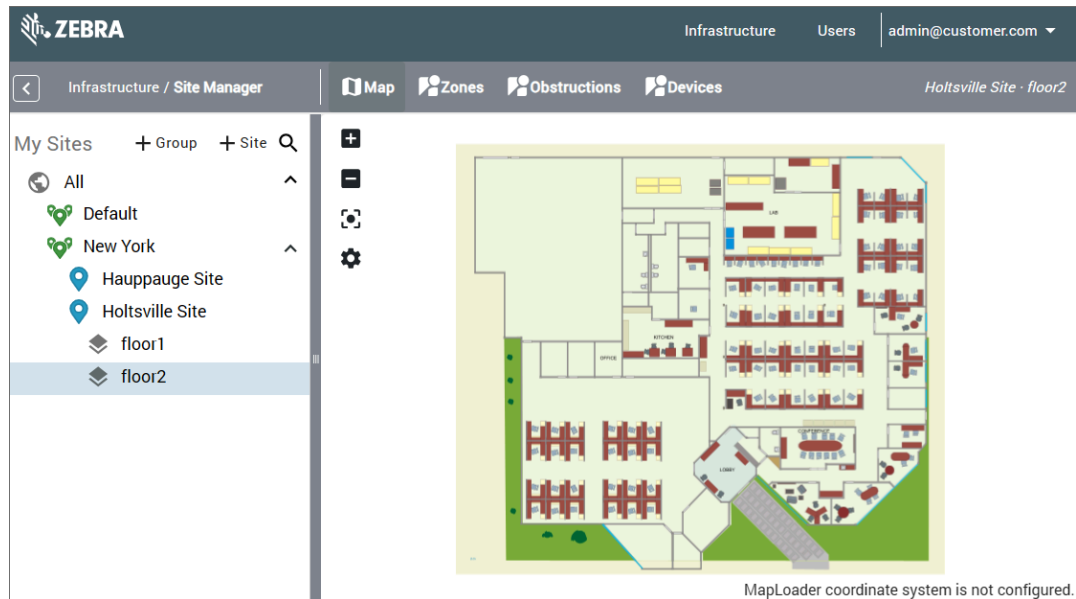


## Calibrating a Map Using Its Width or Height

Before using a site map, you must calibrate it. Follow the steps below to calibrate it using its width or height. The other dimension is automatically established.

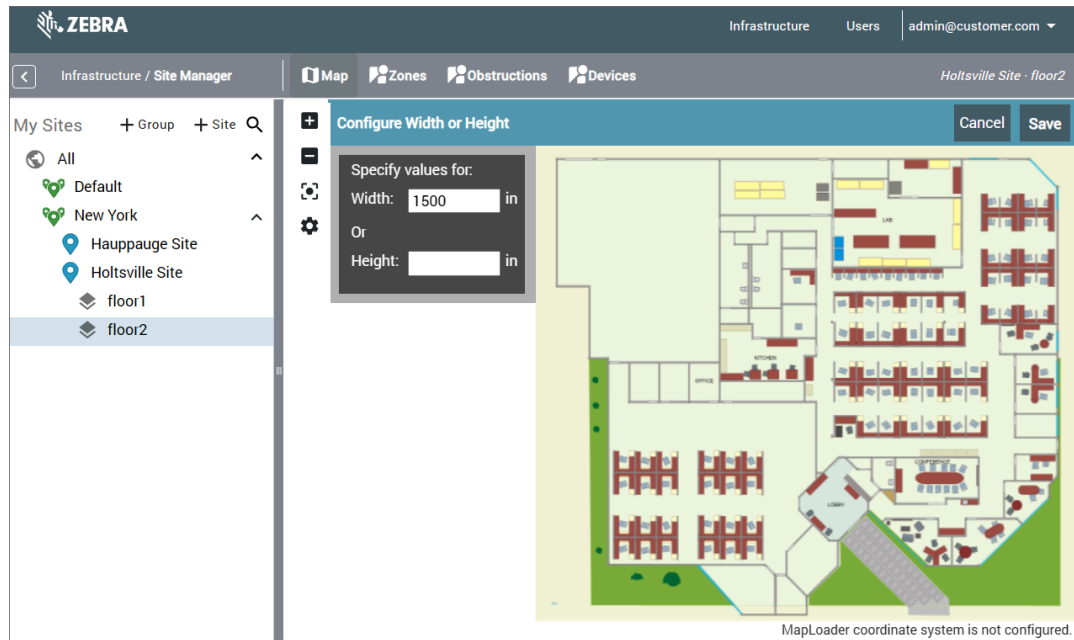
To calibrate it using two known points, refer to [Calibrating a Map Using Two Known Points](#) on page 26.

1. Navigate to **Infrastructure > Site Manager**.
2. Click the map name.
3. Click **⚙️ Configure Map > Specify Map Width Or Height** in the map window toolbar.



Notice the label at the bottom-right, which reads MapLoader coordinate system is not configured. Although the site map image is uploaded, the XY coordinate system has not been defined for the map. You accomplish this by calibrating the site map.

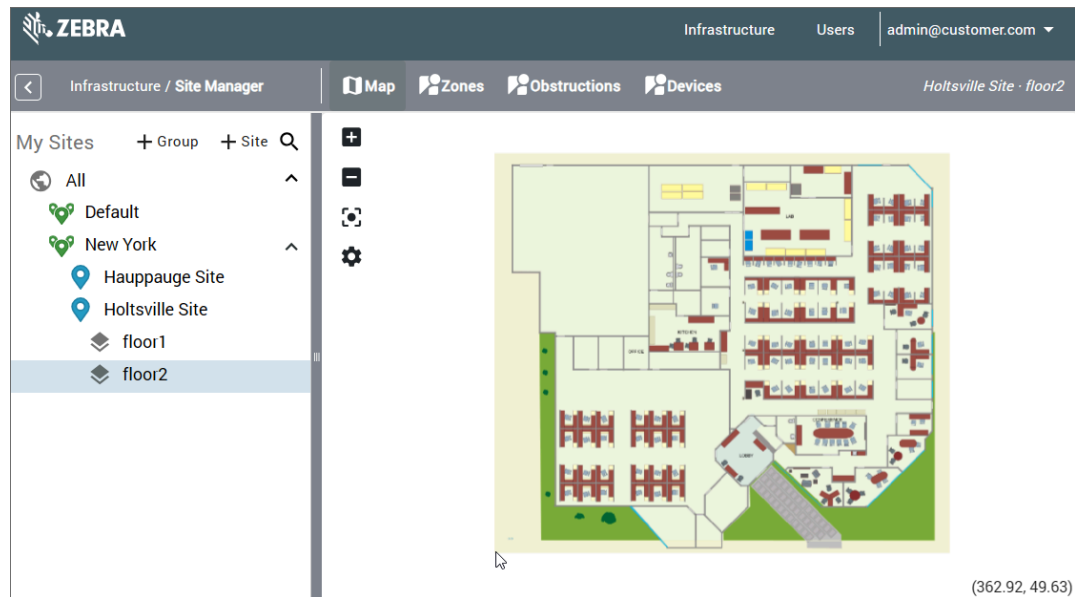
4. Enter the known width or height of the site map, in inches.



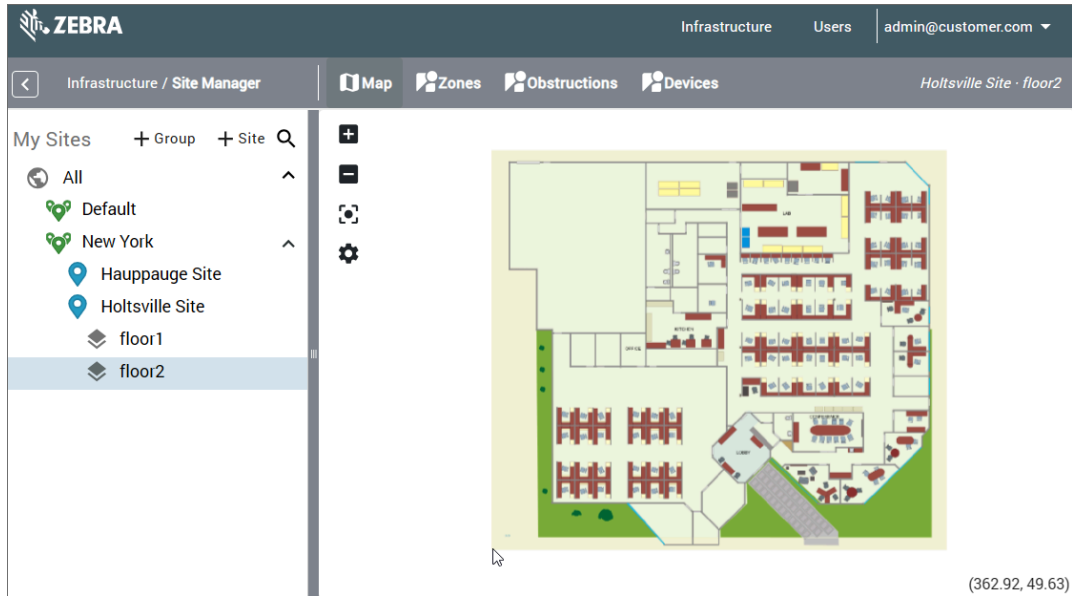
The other dimension is automatically established.

5. Click **Save**.

The map is now calibrated. Move the mouse over the map. The X- and Y-coordinates display in the bottom right corner of the map window.



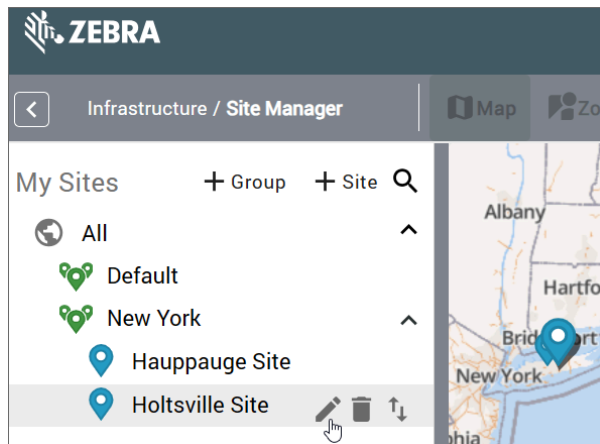
**NOTE:** If the source image was a PNG, the origin is placed at the bottom-left of the current map window (excluding the width of the window occupied by its toolbar). If you change the zoom or reposition the site map in the window, the origin remains at the location established during calibration. When you drag RFID readers on the site map or explicitly specify their location, it is relative to this origin.



## Determining the Site ID

When initializing your RFID readers, you need to know the ID of the site in Resonate with which to register the device (this should correspond to the site at which the reader is installed). To determine the site ID, follow the steps below.

1. Navigate to **Infrastructure > Site Manager**.
2. Hover over the site name or next to it and click **Edit**.



The **Update Site** window opens.



3. Take note of the site ID (site number) at the top of the window.

**Update Site # 1**

**Site Name \***  
Holtsville Site

85 characters left.

**Location \***  
1 Zebra Plaza, Holtsville NY 11742

**Address Location**  
1, Zebra Plaza, Holtsville, Town of Brookhaven, Suffolk County, New York, 11742, United States

**Site Group**  
New York

**Time Zone \***  
US/Eastern

**Device Domain \***  
xyz.zebra.lan

**Metadata**  
Suffolk NY

**Site Maps** + Upload

floor1

PUBLISH CANCEL SAVE

In this example, the site ID is 1.

4. Click **Cancel** to exit the window without making changes.

# Enabling Communication with the RFID Readers

This section describes how to initialize your RFID readers so that Resonate RFID Reader Management can communicate with them.

## RFID Reader Initialization

Resonate RFID Reader Management communicates with the RFID readers using a pull-based architecture, where the readers fetch instructions from the Resonate server. To add readers to a Resonate RFID Reader Management instance to be managed, they must be initialized. This term refers to the steps taken to find the readers, connect to them, install the Resonate Agent utility onto the readers, and connect the readers securely to the Resonate RFID Reader Management instance.

For this purpose, Resonate RFID Reader Management comes with a separate Windows utility for device initialization, Resonate Device Initializer. Run the Resonate Device Initializer utility to prepare the readers for this architecture. The utility can discover all supported RFID readers on the subnet, and you use the Resonate RFID Reader Management web interface to choose which to manage and control.

The Resonate Device Initializer utility is separate to allow the option of running locally on the same network segment as the readers.

## Resonate Device Initializer Basics

The Resonate Device Initializer utility initializes the RFID readers that Resonate RFID Reader Management needs to manage; the initialization also installs the Resonate Agent on the readers. Run the utility on a Windows 10 or 11 machine, according to the required onboarding mode.

The Resonate Device Initializer utility is a self-contained executable (`rm-device-initializer-<VERSION>.exe`) without an installer. It is distributed in the `resonate-<VERSION>.tar.gz` file that you received from Zebra to install Resonate RFID Reader Management.

Resonate Device Initializer supports two device onboarding modes:

- **Discovery-based mode:** Resonate Device Initializer automatically discovers all supported RFID readers on the same subnet. As it discovers devices, it presents them in the list of discovered devices to the Resonate server for display in the web interface. You then review the list of discovered devices and choose which ones Resonate should manage.

In this mode, you must run the utility onsite and on the same subnet as your RFID readers. Each subnet that has readers to manage must use the same DNS domain and requires its own instance of Resonate Device Initializer. This is the easiest and most common way to run the utility.

- File-based mode<sup>1</sup>: Resonate Device Initializer requires that you provide a file with an explicit list of supported RFID readers that you need Resonate RFID Reader Management to manage. You can run the utility from any Windows machine, provided there is network access to the RFID readers.

The utility elevates the device's firmware to a Resonate compatible version as needed.



**NOTE:** All RFID readers must be factory-reset before running the Resonate Device Initializer utility.

To run the Resonate Device Initializer utility, you must specify the URL of the Resonate server to use, as well as the ID of a site that you have set up in the **Site Manager** page of the web interface. For information on the site ID, refer to [Determining the Site ID](#) on page 32.

## Using Resonate Device Initializer in Device-Discovery Mode

Steps on how to run Resonate Device Initializer in device-discovery mode are outlined below.



**NOTE:** To initialize devices, you must have **device\_create** and **device\_edit** roles.

1. Ensure that your RFID readers are powered on and in the . If necessary, perform a factory reset; for instructions, refer to their documentation.
2. Extract `rm-device-initializer-<VERSION>.exe` from the `resonate-<VERSION>.tar.gz` file, into a Windows directory located onsite and on the same subnet as your RFID readers.

Each subnet that has readers to manage must use the same DNS domain and requires its own instance of Resonate Device Initializer.

3. Open a Command Prompt or PowerShell window, navigate to the directory, and run the following:

```
.\rm-device-initializer-.exe --url <RESONATE SERVER FQDN> --id <SITE ID>
```

Replace `<RESONATE SERVER FQDN>` with the fully qualified domain name (URL) of the Resonate server, and `<SITE ID>` with the ID of a site that you have set up in the **Site Manager** page of the web interface. For example, if the URL of your Resonate server is `https://customerresonate.com` and the site ID is 1, run:

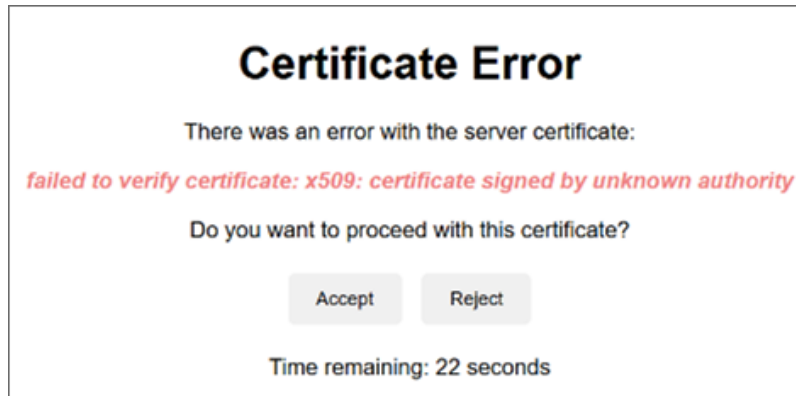
```
.\rm-device-initializer-.exe --url https://customerresonate.com --id 1
```

Resonate Device Initializer performs a validation check to ensure the Resonate RFID Reader Management certificate is both valid and signed by a user-trusted certificate authority (CA). If the

---

<sup>1</sup> File-based mode will be supported in an upcoming release.

certificate is trusted, Resonate Device Initializer proceeds without interruption. If not trusted, it opens a web page, prompting you to grant permission to use the certificate with the RFID readers.



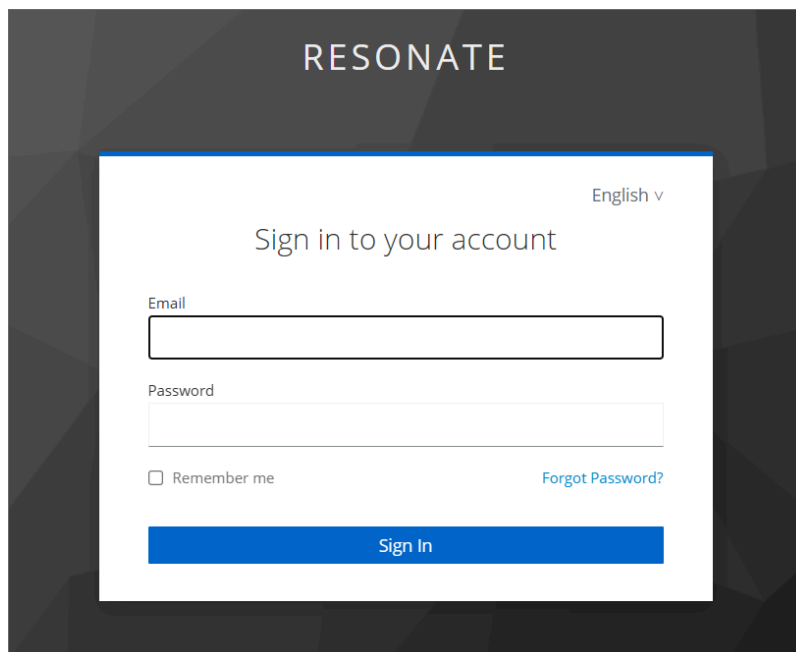
4. If you obtain this certificate error, perform one of the following:

- Click **Reject**. This rejects the certificate and stops Resonate Device Initializer. Replace your Resonate RFID Reader Management certificate with the one provided by your certificate authority (CA); then, restart the steps in this topic.
- Click **Accept**. This accepts the certificate and Resonate Device Initializer continues its process.

You have 30 seconds to click an option, after which Resonate Device Initializer stops and displays a timed-out message.

After the certificate is accepted, Resonate Device Initializer prompts you to grant it access to communicate with Resonate RFID Reader Management. It opens the default browser and takes you to the Resonate login page.

5. Log in.



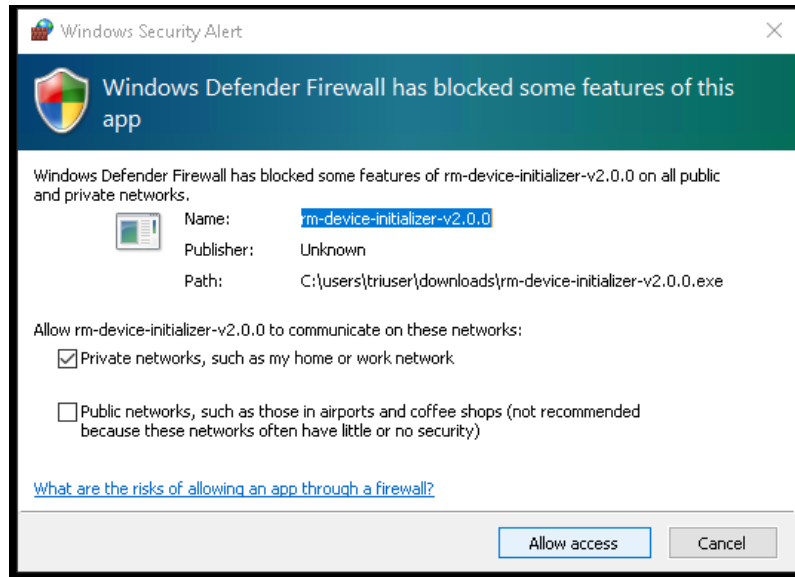
After you successfully log in, the utility prompts you to grant it access permission.

**6. Click Yes.**

Resonate Device Initializer receives authorization to proceed with RFID reader discovery and initialization.

For the utility to proceed, you must allow certain firewall rules; Windows Defender Firewall displays a message, prompting you to grant it access to open the necessary firewall ports.

**7. Click Allow Access.**



This grants the application listed in the warning access to all ports for the specific networks selected.



**NOTE:** If this alert is not prompted for some reason, and the firewall is turned on, a firewall rule is required to allow UDP ports 3702 and 12345 inbound to this application for the Resonate Device Initializer to work.

Upon successful authentication and port access, Resonate Device Initializer starts to scan the current subnet for supported RFID readers. If a discovered RFID reader's make, model, and part number are compatible with Resonate, the utility initializes the reader and installs the Resonate Agent on it. The reader is then visible in the web interface. The utility ignores other RFID readers, listing them with an unsupported message in the console.

**8. Open the web interface, and navigate to Infrastructure > Discovered Devices.**

**9. In the Command Prompt or PowerShell window, press CTRL+C when all readers are listed in the web interface.**

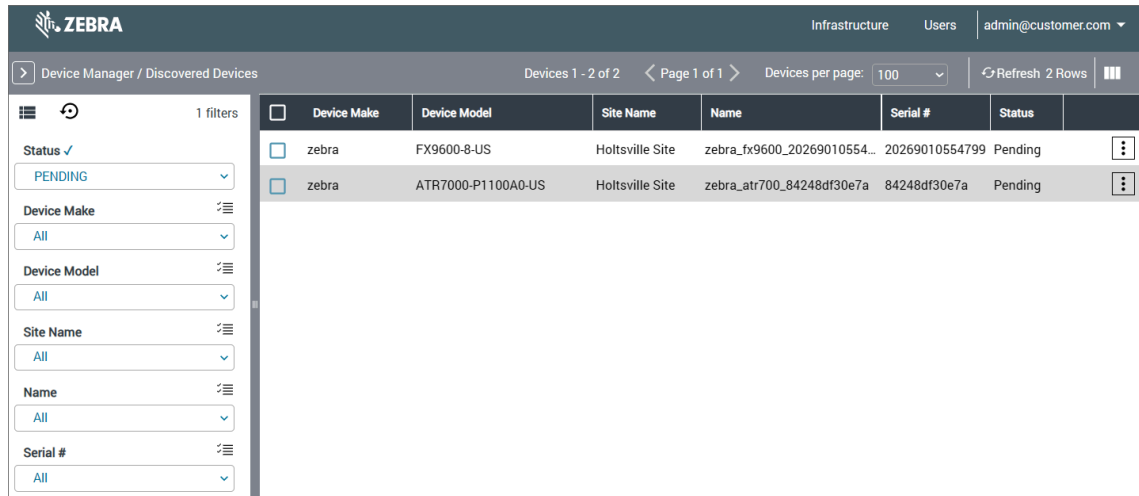
Although discovered, you must now select the readers that Resonate RFID Reader Management should manage. Refer to [Selecting from Discovered Devices](#) on page 38.

## Selecting from Discovered Devices

When you run the Resonate Device Initializer utility in device-discovery mode, the **Infrastructure > Discovered Devices** page in the web interface displays the list of compatible RFID readers discovered on the same subnet as the utility, which are not yet managed by Resonate RFID Reader Management. From this list, you must select the readers that Resonate RFID Reader Management should manage, allowing it to communicate with the readers.

### 1. Navigate to **Infrastructure > Discovered Devices**.

Discovered RFID readers appear on the discovered-devices grid as Resonate Device Initializer discovers them. To force a refresh, click **Refresh** in the secondary top bar. Discovery stops when you stop the Resonate Device Initializer utility.




Device Make	Device Model	Site Name	Name	Serial #	Status
zebra	FX9600-8-US	Holtsville Site	zebra_fx9600_20269010554...	20269010554799	Pending
zebra	ATR7000-P1100A0-US	Holtsville Site	zebra_atr700_84248df30e7a	84248df30e7a	Pending

### 2. If necessary, filter the list of discovered RFID readers using the filter options on the left.

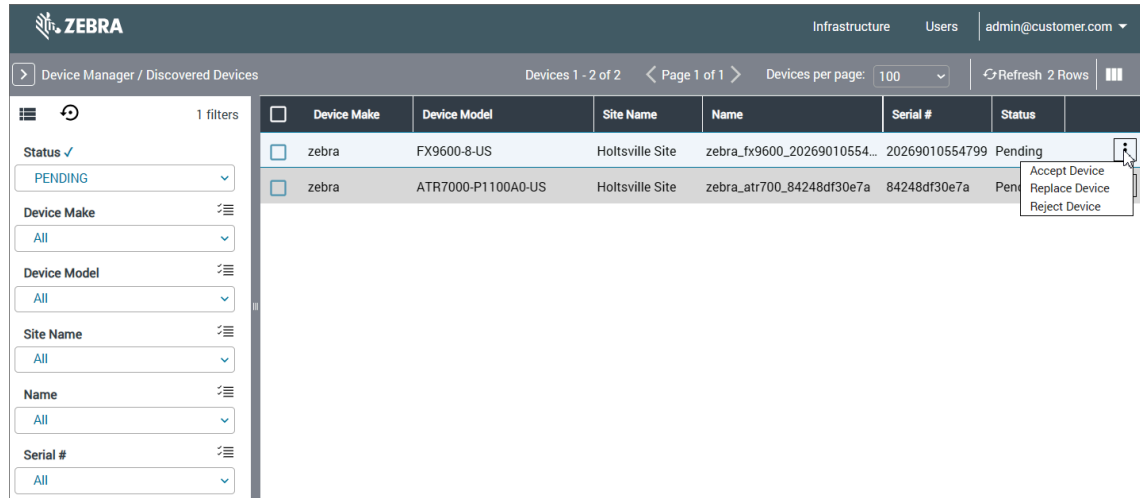
You can filter the list by status, device model, site name, name, and serial number.

## Enabling Communication with the RFID Readers


3. Select  **Device Settings** > **Accept Device** at the far right of an RFID reader's row to have Resonate RFID Reader Management manage it.




**NOTE:** When you click **Accept Device**, Resonate RFID Reader Management upgrades the reader's firmware, if necessary, and configures the device. Therefore, it is critical that you select the correct device.



Device Make	Device Model	Site Name	Name	Serial #	Status
zebra	FX9600-8-US	Holtsville Site	zebra_fx9600_20269010554...	20269010554799	Pending
zebra	ATR7000-P1100A0-US	Holtsville Site	zebra_atr700_84248df30e7a	84248df30e7a	Pen...

If an RFID reader fails and you want to replace it with a discovered reader, select  **Device Settings** > **Replace Device** instead. This allows you to maintain the original reader's configuration and use it for the new reader, without having to manually configure the new reader.

If an RFID reader should not have been discovered (for example, a truly unknown device that someone has on the network), select  **Device Settings** > **Reject Device**. The reader is removed from the list, will not be managed by Resonate RFID Reader Management, and will not be discovered on subsequent runs of Resonate Device Initializer.

When Resonate RFID Reader Management can communicate with an RFID reader to manage it, Resonate removes the reader from the **Infrastructure** > **Discovered Devices** page, moves it to the **Infrastructure** > **Devices** page, upgrades its firmware (if necessary), and configures it.

# Deploying and Managing RFID Readers

This section describes how to deploy and manage initialized readers.

## Managed RFID Readers

After enabling communication between Resonate RFID Reader Management and the required RFID readers using Resonate Device Initializer, you can configure, deploy, monitor, and manage the readers from the **Infrastructure > Devices** page. This page lists all the RFID readers that Resonate manages and controls.

Shortly after establishing communication with a reader, Resonate automatically checks and, if necessary, upgrades the reader's firmware to a Resonate compatible firmware version, installs and integrates required components on the reader, and then boots the reader. When complete, the reader's status shows as **ONLINE** in the **Status** column, which indicates the reader is communicating with Resonate and waiting for a command.

The status might show as **ELEVATING** before it shows as **ONLINE**, which indicates the reader's firmware was not compatible and is being automatically elevated to a compatible version.



**NOTE:** Avoid directly logging in to a reader (for example, using its web interface) if it is being managed by Resonate RFID Reader Management because this might interfere with the reader's operation. One exception is to install a reader endpoint certificate.



## Device Grid

The **Device** grid on the **Infrastructure > Devices** page displays all the RFID readers that Resonate manages and controls. You can filter the listed RFID readers, select and reorder the displayed columns, and sort the rows by a selected column in ascending or descending order.

**Figure 4** Device Grid

The screenshot shows the Zebra Infrastructure > Devices page. On the left is a filter panel with dropdowns for Device Make, Device Model, Serial #, Hostname, Site Name, Map Name, Name, and Firmware Version, each with an 'All' option. The main table displays three devices, all of which are Zebra FX9600-82320A58-US readers in an ONLINE status. The columns shown are Alerts, Device Make, Device Model, Status, Linked, Serial #, Hostname, Site Name, Map Name, Name, and Firmware Version.

Alerts	Device Make	Device Model	Status	Linked	Serial #	Hostname	Site Name	Map Name	Name	Firmware Version
<input type="checkbox"/>	zebra	FX9600-82320A58-US	ONLINE		17509705216...	fx9600d1b3...	Holtsville Site	floor1	zebra_fx9600_17509705216...	3.28.18
<input type="checkbox"/>	zebra	FX9600-82320A58-US	ONLINE		17509705235...	fx96001587...	Holtsville Site	floor2	zebra_fx9600_17509705235...	3.28.18
<input type="checkbox"/>	zebra	FX9600-82320A58-US	ONLINE		17509705225...	fx9600ceba52	Holtsville Site	floor1	zebra_fx9600_17509705225...	3.28.18

### Filters



Use the left panel to limit the readers listed in the grid. You can filter based on the values of any column. The left panel contains a dropdown list for each column, where you can select multiple values. Only readers matching those values are displayed. You can filter based on the values of multiple columns.

### Columns

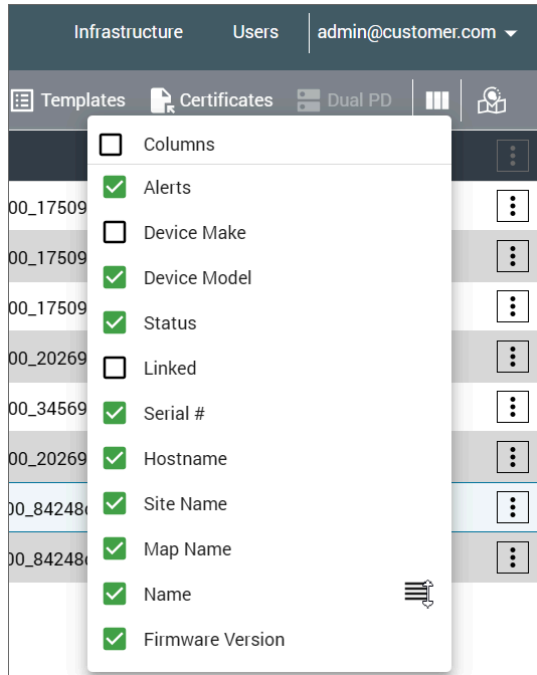
By default, the **Device** grid shows the following columns for each reader:

- **Alerts:** Indicates whether an alert is firing for the reader. For information, refer to [Monitoring Device Health and Status](#) on page 73.
- **Device Make:** Indicates the reader's manufacturer.
- **Device Model:** Indicates the reader's model number (which includes its type).
- **Status:** Indicates the reader's status. For information, refer to [Monitoring Device Health and Status](#) on page 73.
- **Linked:** Indicates whether the reader is paired with another to accomplish dual-portal directionality mode.
- **Serial #:** Indicates the reader's serial number.
- **Hostname:** Indicates the reader's hostname. Although each reader has its own hostname, avoid directly logging in to a reader (for example, using its web interface) if it is being managed by Resonate RFID Reader Management because this might interfere with the reader's operation.
- **Site Name:** Indicates the site where the reader is physically installed.
- **Map Name:** Indicates the site map containing the reader.
- **Name:** Indicates the reader's friendly name. By default, it displays the reader's device ID: Make\_Model\_SerialNumber (for example, zebra\_fx9600\_123456), but you can configure this name.

- **Firmware Version:** Indicates the reader's firmware version.

To change the set of columns displayed, click  **Column Selector** in the secondary bar at the top; then, enable or disable the listed columns. To change the position of a column, hover over the column name in the list and drag the  **Column Position** icon up or down.

**Figure 5** Column Selector



### Sorting Rows

To sort the rows in the grid by a specific column, click the column header. Clicking again toggles the sort order between ascending and descending.


## Device Configuration Overview

Before activating your RFID readers, you must configure them on the **Edit Devices** page. Regardless of the mode or tab, you should be aware of some general information related to Resonate reader configuration settings, how to access them, and distance units and time formats.



**NOTE:** Resonate uses the on-reader Resonate Agent app to control all reader configuration settings; it does not use ZloTC for this purpose. The on-reader web interface shows user ZloTC settings and not Resonate settings. Also, Resonate reader configuration settings often have the same name as those in the readers' web interface and the ZloTC APIs; however, these settings are not necessarily exactly the same. This is partly why you are instructed to use Resonate, and not to attempt to use both Resonate and the readers' web interface; the results will be inconsistent if you mix and match.

### Editing

Edit a device's configuration on the **Edit Devices** page. Typically, you access this page by clicking  **Device Settings** > **Edit** at the far right of the readers' row on the **Infrastructure** > **Devices** page.

The **Edit Device** page has the following tabs, depending on the RFID reader. Configure the appropriate fields. If required fields are not filled in, a warning icon appears next to the tab name, and the fields are highlighted to indicate the error.


- [Identity Tab](#) on page 44
- [Location Tab](#) on page 45
- [Network Tab](#) on page 46
- [Security Tab](#) on page 47 (for FX9600 only)
- [Antennas Tab](#) on page 48 (for FX9600 only)
- [Modes Tab for FX9600](#) on page 50 or [Modes Tab for ATR7000](#) on page 60

Only after you click **Save** does Resonate RFID Reader Management notify the RFID reader that a configuration change is on the server for the reader to pull.



**NOTE:** You must fill in required fields before you can save the configuration settings.

When configuring two ATR7000 RFID readers in dual-portal directionality, the procedure is initially different; refer to [Configuring Dual-Portal Directionality](#) on page 71 for details. After a reader is part of a

pair configured for dual-portal directionality, selecting  **Device Settings** > **Edit**, at the far right of either reader, accesses the **Edit Devices** page for dual-portal directionality.

### Distance Units and Time Formats

The following applies to all device configuration fields:

- **Distance units:** Distances are in inches.
- **Time duration format:** Time duration fields are text-based fields that accept the following units of time from left to right in the following order: days (d), hours (h), minutes (m), seconds (s), and milliseconds (ms). All time segments are optional; however, you must provide at least one. For example, to express 1 day, 2 hours, 3 minutes, 4 seconds, and 5 milliseconds, specify 1d2h3m4s5ms. To enter only one unit of time, enter just that one unit. For example, for 1 day, specify 1d; for 4 seconds, specify 4s.

## Identity Tab

The **Identity** tab allows you to view and/or configure the reader identity information, apply a template, and view pending actions on the reader.

**Figure 6** Identity Tab

**Table 2** Identity Tab Fields

Field	Description
<b>Part Number</b>	Displays the reader's make and model.
<b>Name</b>	Sets the user-friendly name of the reader. By default, the name is set to the reader's device ID, a 3-part identifier: Make_Model_SerialNumber (for example, zebra_fx9600_123456). Resonate uses this information to generate the zone names contained in the events.
<b>Template</b>	Allows you to select a template to configure the fields of the reader that correspond to the filled-in fields of the template. Templates are specific to the type and model of the reader; only applicable templates are listed. For information on templates and how to create one, refer to <a href="#">Templates</a> on page 77.  Click <b>Apply</b> to update the different tabs of the <b>Edit Device</b> page with the filled-in fields of the template. The template affects only those fields whose settings apply to multiple readers; fill in the remaining required fields. If required, you can modify fields set by the template. If you previously modified other fields on the different tabs and clicked <b>Save</b> , those fields are not modified. If you did not save your changes, the template might reset them.
<b>Current Device Operations</b>	Lists pending actions.

## Location Tab

The **Location** tab allows you to view and configure the reader's site and its location within the site.

**Figure 7** Location Tab

The screenshot shows the Zebra Infrastructure web interface. At the top, there's a header with the Zebra logo, 'Infrastructure' and 'Users' tabs, and a user dropdown for 'admin@customer.com'. Below the header is a 'Edit Device' section. The device information bar shows 'Sync' in progress, 'Name: zebra\_atr7000\_84248df30e7a', 'Serial: 84248df30...', 'MAC Address:', 'Make: zebra', and 'Type: ATR7000'. The 'Location' tab is selected in the sidebar. The main configuration area includes:
 

- Identity**: Site dropdown set to 'Holtsville Site'.
- Location**: Level dropdown set to 'floor1'.
- Position**: Fields for X (24), Y (36), and Z (120) coordinates.
- Orientation**: Yaw field set to 0.
- Adjustments**: Orientation Yaw field set to 0.

 At the bottom, there are 'Back' and 'Save' buttons.

**Table 3** Location Tab Fields

Field	Description
<b>Site</b>	Specifies the site where the reader is installed. By default, the site is the one specified when running Resonate Device Initializer to discover/add the reader to Resonate RFID Reader Management.
<b>Level</b>	Select the site map to use to specify the reader's location within the site.
<b>Position</b>	Specifies the reader's <b>X</b> , <b>Y</b> , and <b>Z</b> coordinates, relative to the calibrated origin of the reader's site map, in inches.
<b>Orientation</b>	Specifies the reader's physical yaw ( <b>Yaw</b> ), in degrees. Supported values are between 0 and 360, inclusive.
<b>Adjustments</b>	Specifies the reader's virtual yaw ( <b>Orientation Yaw</b> ), in degrees. This allows you to adjust the yaw through software without physically remounting the reader. Supported values are between 0 and 360, inclusive.

## Network Tab

The **Network** tab allows you to view and configure the reader's network settings.

**Figure 8** Network Tab

The screenshot shows the Zebra Infrastructure management interface. At the top, there's a header with the Zebra logo, 'Infrastructure' tab, 'Users' link, and a user dropdown 'admin@customer.com'. Below the header is a breadcrumb 'Edit Device'. A status bar shows 'Sync' with a 'In progress' indicator, and device details: 'Name: zebra\_atr7000\_84248df30e7a', 'Serial: 84248df30...', 'MAC Address:', 'Make: zebra', and 'Type: ATR7000'. The 'Network' tab is selected in the sidebar. The configuration fields include: 'Hostname' (set to ATR7000F30e7a), 'NTP Address' (placeholder), 'DNS Address' (placeholder), 'MAC Address' (placeholder), a radio button selection for 'DHCP' (selected) and 'Static', 'IP Address' (placeholder with an info icon), and 'Gateway' (placeholder). At the bottom, there are 'Back' and 'Save' buttons.

**Table 4** Network Tab Fields

Field	Description
<b>Hostname</b>	Specifies the reader's hostname. Each reader has a default, unique hostname, but you can change it. All readers must have different hostnames. Avoid directly logging in to a reader (for example, using its web interface) if it is being managed by Resonate RFID Reader Management because this might interfere with the reader's operation.
<b>NTP Address</b>	Specifies the address of the Network Time Protocol (NTP) server that the reader must use to synchronize its clock. Use the same NTP server as the one that the Resonate server uses. This is necessary to maintain consistent system time across the Resonate server and the readers.
<b>DNS Address</b>	Specifies the address of the reader's DNS server.
<b>MAC Address</b>	Displays the reader's MAC address.
<b>DHCP/Static</b>	Specifies whether the reader's network uses DHCP or Static IP.
<b>IP Address</b>	Specifies the reader's IP address. In DHCP network mode, this field is read-only.
<b>Gateway</b>	Specifies the reader's gateway. In DHCP network mode, this field is read-only.

Security Tab

For Zebra FX9600 readers, the **Security** tab is available to change the debug level for logging.

Figure 9 Security Tab

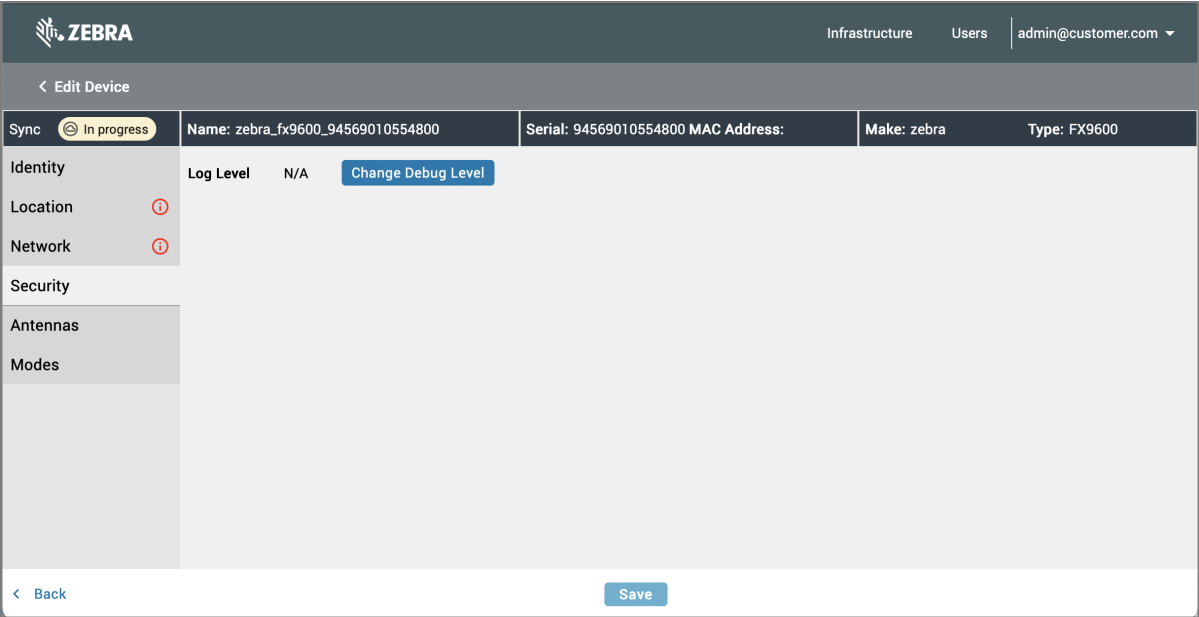


Table 5 Security Tab Field

Field	Description
Change Debug Level	<p>Specifies the level of detail to log. Click <b>Change Debug Level</b> to select a level from the following possible levels. Each log level includes information from the previous level in the following order.</p> <ul style="list-style-type: none"><li>• <b>ERROR</b>: Logs errors.</li><li>• <b>WARN</b>: Logs potential issues that might require attention but do not immediately disrupt functionality.</li><li>• <b>INFO</b>: Logs general information that highlight progress.</li><li>• <b>DEBUG</b>: Logs detailed, low-level information intended to troubleshoot issues.</li></ul>

## Antennas Tab

If the selected RFID reader uses external antennas (for example, Zebra FX9600), the **Antennas** tab is available to configure which antennas are connected to the reader, where they are on the site map, and whether they are enabled (turned on / connected). On the right of some fields, there is a symbol indicating whether the field is still in its device-configured state.

After configuring information about the antenna connected to a specific port, click **Add**.

After configuring the **Antennas** tab, use the **Antenna Defaults** and **Antenna Overrides** tabs, accessible from the **Modes** tab, to control the antennas' power, session, select, and target the RFID reads. These specify how to use the physical antennas (defined on this tab) to do RFID scanning.


**Figure 10** Antennas Tab

**Table 6** Antennas Tab Fields

Field	Description
Enabled	Allows you to enable the antenna port.
Location	Specifies the antenna's X, Y, and Z coordinates, relative to the calibrated origin of its reader's site map, in inches.



**Table 6** Antennas Tab Fields (Continued)

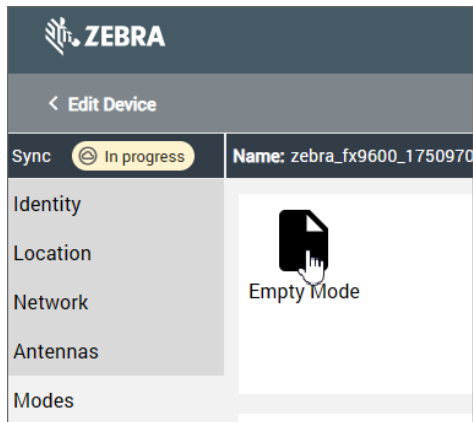
Field	Description
Cable	<p>Specifies the cable length (in) and loss (dB). The RFID reader uses this information to adjust its power output to compensate for cable attenuation and ensure it can accurately detect tags within the required range.</p> <p> <b>NOTE:</b> Specify the length in inches, unlike the units used for specifying it with MotionWorks RFID Reader Manager.</p>
Add	<p>Configures the reader with the antenna information. After you click <b>Add</b>, you must specify one or more labels (user-defined key and value pairs) to associate with the antenna to identify it. Click <b>Add</b> again to specify an additional label. For example, you could specify the following labels (key-value pairs) if the antenna was reading labels at door 1 and there was low interference.</p> <div><div>Labels</div><div><div>Add</div><div><div>Interference Low</div><div></div></div><div><div>Door 1</div><div></div></div></div></div>

## Modes Tab for FX9600

The **Modes** tab allows you to configure how a reader collects and processes data from passive RFID tags, as such the **Modes** tab is reader-type specific. This topic covers the **Modes** tab for FX9600 RFID readers. Currently, Resonate RFID Reader Management supports custom modes.

Initially, the **Modes** tab only has an **Empty Mode** button.

**Figure 11** Empty Mode Button



Double-click **Empty Mode** to access the **Empty Mode** page. Within this page, there are three subcategories of configuration settings, grouped by vertical tabs: **Mode**, **Antenna Defaults**, and **Antenna Overrides** tabs.

### Mode Tab

The **Mode** tab allows you to configure the mode of operation.

Figure 12 Mode Tab

Empty Mode

Mode

Antenna Defaults

Antenna Overrides

Environment

Environment

Filtering

Filter Type

Radio Start Conditions

Type

Automatic

Radio Stop Conditions

Duration ⓘ

0d0h0m0s0ms

Antenna Cycles

Type

GPI

☐ Port 1

Signal

Debounce Time ⓘ

0d0h0m0s0ms

GPI

☐ Port 2

Signal

Debounce Time ⓘ

0d0h0m0s0ms

Delays

After selects

Type

Duration

Reporting

Type

Duration ⓘ

0d0h0m0s0ms

☒ Default

Cancel

Save

Save


**Table 7** Mode Tab Fields

Field		Description
<b>Environment</b>		<p>Specifies the type of environmental conditions in which the reader operates. Along with the regulatory configuration of the reader, the environment field sets the default link profile parameters (such as, Miller mode, BLF, and Tari) and the receiver dynamic range (interference immunity).</p> <ul style="list-style-type: none"> <li>• <b>HIGH_INTERFERENCE:</b> Significant interference from external sources (for example, competing RF devices, industrial equipment generating electromagnetic noise, or physical obstructions like metal structures).</li> <li>• <b>LOW_INTERFERENCE:</b> Low interference from external sources (for example, minimal physical barriers or areas with limited RF activity).</li> <li>• <b>VERY_HIGH_INTERFERENCE:</b> Very high interference from external sources.</li> <li>• <b>AUTO_DETECT:</b> Automatically detected interference. The RFID reader continuously monitors the environment and dynamically adjusts its settings (for example, power levels, frequency hopping, or sensitivity) to optimize performance. This mode is useful when interference levels fluctuate or are difficult to predict during setup.</li> <li>• <b>DEMO:</b> Interference controlled for testing or demonstration purposes. This mode prioritizes simplicity and predictability over interference mitigation, making it suitable for trade shows, training, or troubleshooting in non-production environments.</li> </ul>
<b>Filtering</b>		Allows you to filter reads based on their RFID tag ID. If no filter is specified, all reads are considered.
	<b>Filter Type</b>	<p>Specifies whether and how to filter the tags that the reader reads and reports.</p> <ul style="list-style-type: none"> <li>• <b>blank:</b> Read all tags from all antennas and report the unique tags.</li> <li>• <b>RSSI:</b> Filter out tags with a weak RFID signal strength (within a certain radius of the reader). Specify the minimum strength in the <b>RSSI Threshold</b> field, in dBm. RSSI is specified as a negative value, typically in the range -40 to -80.</li> <li>• <b>TAG:</b> Filter out tags based on their RFID tag ID. Report only those that meet the condition specified using <b>Match</b>, <b>Value</b>, and <b>Operation</b>.</li> </ul>

**Table 7** Mode Tab Fields (Continued)

Field		Description
	<b>Match</b>	Specifies the segment of the tag ID to match or the method to use to match. Select between the following options: <b>PREFIX</b> , <b>SUFFIX</b> , and <b>REGEX</b> .
	<b>Value</b>	Specifies the value to match. For prefix and suffix filters, enter only hexadecimal digits, and the number of digits must be even. When a prefix filter is used, selects cannot be used. For a regex filter, use C++ STL regex values.
	<b>Operation</b>	Specifies the filter operation. Select between <b>INCLUDE</b> and <b>EXCLUDE</b> .
<b>Radio Start Conditions</b>		Specifies when, after you issue a <b>Start</b> command, the radio starts trying to inventory tags.
	<b>Type</b>	Specifies the type of start after you issue a <b>Start</b> command. <ul style="list-style-type: none"> <li>• <b>Automatic</b>: The radio starts trying to inventory tags immediately.</li> <li>• <b>GPI</b>: The radio waits for a general-purpose input (GPI) before trying to inventory tags.</li> <li>• <b>GPI with restart</b>: The radio waits for a general-purpose input (GPI) before trying to inventory tags. When the signal is received, it restarts the reader.</li> </ul>
	<b>Port</b>	Specifies whether to receive the GPI on port <b>1</b> or <b>2</b> .
	<b>Signal</b>	Specifies whether to start on a <b>HIGH</b> or <b>LOW</b> signal level.
	<b>Debounce Time</b>	Specifies the duration that the GPI must remain at the specified signal level to trigger the event (that is, the start).
<b>Radio Stop Conditions</b>		Specifies when an ongoing operation should complete. If not specified, the radio continues trying to inventory tags until you issue a <b>Stop</b> command.
	<b>Duration</b>	Specifies the duration to run until the radio stops.
	<b>Antenna Cycles</b>	Specifies the number of cycles through all enabled antennas before the radio stops.
	<b>Type</b>	Specifies to stop based on the tags read. <ul style="list-style-type: none"> <li>• <b>blank</b>: Specifies not to stop based on the tags read.</li> <li>• <b>Tag Count</b>: Specifies the number of tags to inventory until the radio stops.</li> <li>• <b>Duration After No More Unique Tags</b>: Specifies the duration after not inventorying any more unique tags to stop the radio.</li> </ul>
<b>GPI</b>	<b>Port1/Port2</b>	Specifies whether to wait for a general-purpose input (GPI) to stop the radio. It also specifies the port on which to receive the GPI, either port <b>1</b> or <b>2</b> . If the field is blank, a GPI is not used.
	<b>Signal</b>	Specifies whether to stop on a <b>HIGH</b> or <b>LOW</b> signal level.

**Table 7** Mode Tab Fields (Continued)

Field		Description
	<b>Debounce Time</b>	Specifies the duration that the GPI must remain at the specified signal level to trigger the event (that is, stop).
<b>Delays</b>	<b>After selects</b>	Specifies the duration, in milliseconds, to wait after issuing the final select before issuing a query. If absent, the minimum time is used. Possible values are from 0ms to 65ms (integer).
	<b>Type</b>	<p>Specifies to introduce a delay between antenna cycles if no tags are read or if no unique tags are read. This allows the reader to share the spectrum if there are no tags to be read. Possible values are the following. The default is <b>NO_UNIQUE_TAGS</b>.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>: Does not introduce a delay.</li> <li>• <b>NO_TAGS</b>: Introduces a delay if no tags are read.</li> <li>• <b>NO_UNIQUE_TAGS</b>: Introduces a delay if there are no unique tags read.</li> </ul>
	<b>Duration</b>	<p>Specifies the delay duration between antenna cycles if <b>Delay Between Antenna Cycles</b> is set to <b>NO_TAGS</b> or <b>NO_UNIQUE_TAGS</b>.</p> <p> <b>NOTE:</b> For <b>DISABLED</b>, <b>Delay Duration</b> must be 0 seconds; otherwise, it must be a non-zero value.</p> <p>Since the default is <b>NO_UNIQUE_TAGS</b>, the default delay duration is 75 milliseconds.</p>
<b>Reporting</b>		Controls when and how often a tag is reported.
	<b>Type</b>	<p>Configures the timeout by antenna or for the entire radio.</p> <ul style="list-style-type: none"> <li>• <b>RADIO_WIDE</b></li> <li>• <b>PER_ANTENNA</b></li> </ul>
	<b>Duration</b>	Specifies the duration to wait to report a tag again after it has already been reported. As long as the reader is reading the tag, it will not report unless the time since the previous report of this tag on this antenna meets the type and duration.

**Antenna Defaults Tab**

The **Antenna Defaults** tab allows you to configure the default scanning parameters that the antennas will use to perform RFID scanning. If required, use the **Antenna Overrides** tab to override settings for specific antennas. For example, you can configure the power, session, select, and target of the RFID reads.

**Figure 13** Antenna Defaults Tab

Empty Mode

Mode

Antenna Defaults

Antenna Overrides

Transmit Power

TX Power

0 5 10 15 20 25 30 35 40

Query

Population Sel Session

Target

Stop Condition

Type

Selects

Action Membank Target

Pointer Length Mask

Truncate

Accesses


Type

☒ Default

Cancel Save

Save

**Table 8** Antenna Defaults Tab Fields

Field		Description
<b>Transmit Power</b>	<b>TX Power</b>	Specifies the transmit power, in dBm. Drag the bar to the required transmit value (a value between 0 - 40).  <b>NOTE:</b> Account for the combined reader power and antenna gain, ensuring optimal performance and .
<b>Query</b>		Controls which tags are scanned, how collisions are handled, and how tag states are managed.
	<b>Population</b>	Specifies the approximate number of RFID tags expected in the antenna's read zone.

**Table 8** Antenna Defaults Tab Fields (Continued)

Field	Description
	<p><b>Sel</b></p> <p>Specifies the subset of tags to query based on the specified criteria. This helps the reader differentiate between tags in different sessions to avoid redundant reads or collisions.</p> <ul style="list-style-type: none"> <li>• <b>All:</b> Targets all tags in the antenna's read zone.</li> <li>• <b>SL:</b> Targets tags that have been preselected.</li> <li>• <b>Not SL:</b> Targets tags that have not been preselected.</li> </ul>
	<p><b>Session</b></p> <p>Specifies the session used to manage a tag's state during inventory operations. Tags can maintain their state across four different sessions (<b>S0</b>, <b>S1</b>, <b>S2</b>, <b>S3</b>), allowing multiple readers or antennas to work in the same environment without interfering with each other. Set <b>Session</b> to match how long tags need to maintain their state. For example, in a single reader/antenna environment with quick repeated scans, set <b>Session</b> to <b>S0</b> to reset the tags' state more frequently. In environments with multiple readers/antennas operating in the same area, use <b>S1</b>, <b>S2</b>, <b>S3</b>.</p>
	<p><b>Target</b></p> <p>Specifies the tag state (A or B) that the reader should query during scanning. Tags alternate between <b>A</b> and <b>B</b> states to help readers keep track which tags have already been read.</p> <ul style="list-style-type: none"> <li>• <b>A:</b> Queries tags in state A only.</li> <li>• <b>B:</b> Queries tags in state B only.</li> <li>• <b>AB:</b> Queries tags in states A or B during the same inventory round, ensuring all tags are read without redundancy by excluding recently flipped tags.</li> </ul>
<b>Stop Condition</b>	<p><b>Type</b></p> <p>Specifies the stop condition.</p> <ul style="list-style-type: none"> <li>• <b>blank:</b> No stop condition is applied.</li> <li>• <b>GPI:</b> Stops scanning when a signal is received on the specified general-purpose input (GPI) port.</li> <li>• <b>Duration:</b> Stops scanning after the specified duration.</li> <li>• <b>Inventory Count:</b> Stops scanning after reading the specified number of tags.</li> <li>• <b>Single Inventory Limited Duration:</b> Performs one inventory round and stops after completing the round or reaching the specified time limit.</li> </ul>



**Table 8** Antenna Defaults Tab Fields (Continued)

Field		Description
<b>Selects</b>	<b>Action</b>	<p>Determines how the reader sets or modifies the SL flag and A/B state of tags during preselection. This allows the reader to identify which tags should be included in inventory operations when <b>Sel</b> is set to <b>SL</b> or <b>Not SL</b>. The action is only applied to the subset of tags that meet the <b>Selects</b> criteria (<b>Membank</b>, <b>Target</b>, and the other filters).</p> <ul style="list-style-type: none"> <li>• <b>ASSERTSL_DEASSERTSL</b>: Sets the SL flag to selected and then immediately deselects it.</li> <li>• <b>ASSERTSL_NOTHING</b>: Sets the SL flag to selected and leaves it selected.</li> <li>• <b>NOTHING_DEASSERTSL</b>: Leaves the SL flag unchanged initially and then deselects it.</li> <li>• <b>NEGATES_NOTHING</b>: Toggles the SL flag, changing selected tags to deselected and deselected tags to selected.</li> <li>• <b>DEASSERTSL_ASSERTSL</b>: Sets the SL flag to deselected and then immediately selects it.</li> <li>• <b>DEASSERTSL_NOTHING</b>: Sets the SL flag to deselected and leaves it deselected.</li> <li>• <b>NOTHING_ASSERTSL</b>: Leaves the SL flag unchanged initially and then sets it to selected.</li> <li>• <b>NOTHING_NEGATESL</b>: Leaves the SL flag unchanged initially and then toggles its state.</li> <li>• <b>INVA_INVB</b>: Switches all tags from state A to state B.</li> <li>• <b>INVA_NOTHING</b>: Switches tags from state A but performs no additional action.</li> <li>• <b>NOTHING_INVB</b>: Leaves tags in state A but switches them to state B after processing.</li> <li>• <b>FLIPAB_NOTHING</b>: Flips tags between state A and state B without further action.</li> <li>• <b>INVB_INVA</b>: Switches tags from state B to state A.</li> <li>• <b>INVB_NOTHING</b>: Switches tags from state B but performs no additional action.</li> <li>• <b>NOTHING_INVA</b>: Leaves tags in state B but switches them to state A after processing.</li> <li>• <b>NOTHING_FLIPAB</b>: Leaves tags in their current state but flips them between A and B at the end.</li> </ul>

**Table 8** Antenna Defaults Tab Fields (Continued)

Field	Description
<b>Membank</b>	<p>Specifies which memory bank of the RFID tag the reader interacts with during operations. RFID tags have multiple memory banks, each storing specific types of data. This setting determines where the reader reads from or writes to on the tag.</p> <ul style="list-style-type: none"> <li>• <b>EPC</b>: Memory bank that contains the Electronic Product Code (EPC), a unique identifier for the tag.</li> <li>• <b>TID</b>: Memory bank that stores the tag's unique, factory-assigned Tag Identifier.</li> <li>• <b>USER</b>: Memory bank available for custom user-defined data.</li> <li>• <b>RES</b>: Memory bank that stores password data for accessing or locking the tag (for example, <b>Kill</b> and <b>Access</b> (password)).</li> </ul>
<b>Target</b>	<p>Specifies the tag session that the reader will target during preselection.</p> <ul style="list-style-type: none"> <li>• <b>SL</b>: Allows the reader to target tags based on their SL flag state rather than their session.</li> <li>• <b>S0 - S3</b>: Specifies the tag session.</li> </ul>
<b>Pointer</b>	<p>Specifies the starting bit address (or offset) in the tag's memory bank where the reader should begin applying the selection operation. The reader starts matching from this bit address and applies the <b>Mask</b> and <b>Length</b> to determine if the tag meets the selection criteria. For example, it allows you to filter tags based on a specific portion of your EPC.</p>
<b>Length</b>	<p>Specifies the number of bits in the tag's memory (starting from the <b>Pointer</b>) that the reader will evaluate for the Select command.</p>
<b>Mask</b>	<p>Specifies the exact bit pattern that the reader will compare against the tag's memory content (within the range defined by the <b>Pointer</b> and <b>Length</b>). Specify a binary or hexadecimal value that represents the pattern the reader must look for in the tag's memory.</p>
<b>Truncate</b>	<p>Specifies whether the reader should truncate the tag's memory response after the matched portion (defined by the <b>Pointer</b>, <b>Length</b>, and <b>Mask</b>).</p>

**Table 8** Antenna Defaults Tab Fields (Continued)

Field		Description
<b>Accesses</b>	<b>Type</b>	<p>Specifies the type of operation the reader will execute on the tag's memory or security features during the <u>access command</u>.</p> <ul style="list-style-type: none"> <li>• <b>READ:</b> Reads data from a specified memory bank on the tag. Displays the following fields that you must configure: <b>Membank</b>, <b>Word Pointer</b>, and <b>Word Count</b>.</li> <li>• <b>WRITE:</b> Writes data to a specified memory bank on the tag. Displays the following fields that you must configure: <b>Membank</b>, <b>Word Pointer</b>, <b>Word Count</b> and <b>Block Size</b>.</li> <li>• <b>LOCK:</b> Locks or unlocks specific portions of the tag's memory (for example, EPC, TID, User, Reserved) to control read/write access. Displays the following field that you must configure: <b>Lock Actions</b>.</li> <li>• <b>ACCESS:</b> Provides temporary access to protected memory on the tag using an <b>Access Password</b>.</li> <li>• <b>Kill:</b> Permanently disables the tag using a <b>Kill Password</b>, rendering it inoperable.</li> </ul>

**Antenna Overrides Tab**

The **Antenna Overrides** tab allows you to override the default antenna settings for specific antennas, and to do so in the specified order. Use antenna overrides to create a customized series of RFID scans that run in sequence to ensure all tags are read or operated on as needed for your use case. For example, you can configure a sequence to inventory several thousand tags in a defined area. Another example is configuring a sequence to kill certain tags, while writing to others. Additionally, you can ensure antennas take turns for best results. If required, adjust the series later by re-ordering the scan sequence.

To override the settings of an antenna, click and select the port of the antenna from the **Port** field; then, click in the **Power**, **Query**, **Stop**, **Condition**, **Selects**, or **Accesses** field to override and configure it as required. For information on the different fields, refer to [Antenna Defaults Tab](#). Click + to override the settings of another antenna. You can also override the settings of the same antenna, so that after it has finished scanning using one configuration, it starts scanning with another.

**Figure 14** Antenna Overrides Tab

Empty Mode

Mode

- Antenna Defaults
- Antenna Overrides

Antenna Overrides

Seq#	Port	Power	Query	Stop Condition	Selects	Accesses	Actions
-	-	-	-	-	-	-	+

☒ Default

Cancel Save

## Modes Tab for ATR7000

The **Modes** tab allows you to configure how a reader collects and processes data from passive RFID tags, as such the **Modes** tab is reader-type specific. This topic covers the **Modes** tab for ATR7000 RFID readers. Currently, Resonate RFID Reader Management only supports portal directionality mode for Zebra ATR7000 readers.

Portal directionality mode determines the direction of movement of RFID-tagged items as they pass through an RFID portal, identifying whether each tag is moving into or out of the monitored area. To learn about this mode, refer to reader's [documentation on portal directionality](#); however, use Resonate to configure the mode and follow the descriptions in the current document on how to set them. Resonate does not update the reader's web interface nor vice versa.

To configure two ATR7000 RFID readers in dual-portal directionality, pair the readers first, as described in [Configuring Dual-Portal Directionality](#) on page 71. Then, the **Modes** tab allows you to configure them simultaneously.

In the **Mode Name** field, assign the configuration a name.

Within the **Modes** tab, there are five subcategories of configuration settings, grouped by horizontal tabs: **Lanes**, **Events**, **Filter**, **Beams**, and **Advanced** tabs.

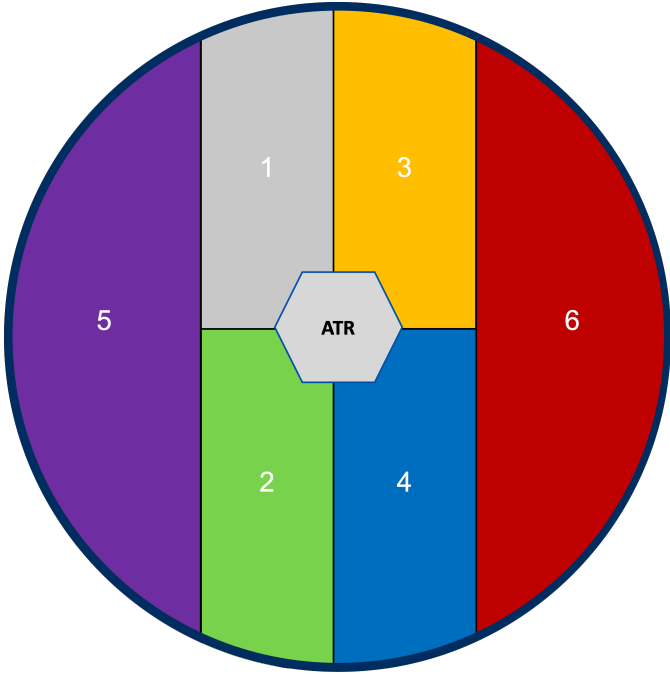
### Lanes Tab

The **Modes > Lanes** tab allows you to view and/or configure the lanes and zones.

**Figure 15** Lanes Tab

The screenshot displays the Zebra Resonate web interface for configuring an ATR7000 reader. The top navigation bar includes the Zebra logo, 'Infrastructure', 'Users', and a user profile dropdown for 'admin@customer.com'. Below this is a breadcrumb trail '< Edit Device'. The main content area is divided into a left sidebar with tabs: 'Sync' (with a status 'In progress'), 'Identity', 'Location', 'Network', and 'Modes'. The 'Modes' tab is selected, showing a configuration form for 'Mode1'. The form includes fields for 'Name' (zebra\_atr7000\_84248df30e7a), 'Serial' (84248df30...), 'MAC Address', 'Make' (zebra), and 'Type' (ATR7000). Below these is a horizontal tab bar with 'Lanes', 'Events', 'Filter', 'Beams', and 'Advanced'. The 'Lanes' tab is active, showing 'Lane Plan' with radio buttons for 'Single Lane' (selected) and 'Dual Lane'. Below this are input fields for 'Lane Width' (120), 'Lane Extension' (0), and 'Tag Height' (36), each with a user icon to its right. At the bottom left is a '< Back' link, and at the bottom right is a 'Save' button.

**Table 9** Lanes Tab Fields

Field	Description
<b>Lane Plan</b>	Specifies whether to configure 4 or 6 zones around the reader(s) for portal directionality. <b>Single Lane</b> corresponds to 4 zones, while <b>Dual Lane</b> corresponds to 6 zones.
<b>Lane Width</b>	<p>Specifies the width of the inner zones, in inches. This field specifies the distance of the inner zones (zones 1 and 2 if using a 4-zone configuration; zones 1, 2, 3, and 4 if using a 6-zone configuration) from edge to edge.</p> 
<b>Lane Extension</b>	Specifies the distance by which the division of the inner zones is offset from the center point of the reader(s), in inches. For example, if a reader is mounted slightly off-center in a portal or doorway, specify an offset for the zones to reflect the reader's true location.
<b>Tag Height</b>	Specifies the expected height from the floor to the tags, in inches.

**Events Tab**

The **Modes > Events** tab of the **Modes** tab allows you to select the portal directionality events to report. If you select any of these events, the reader transmits these events instead of tag read data to the endpoint server.

**Figure 16** Events Tab

Infrastructure

Users

admin@customer.com

[< Edit Device](#)

Sync

Name: zebra\_atr700\_84248df30e7a

Serial: 84248df30... MAC Address:

Make: zebra

Type: ATR7000

Identity

Location

Network

Modes

Mode Name

59 characters left.

Lanes

Events

Filter

Beams

Advanced

Types

Timeout

Direction

Kinds

Look Back Duration

Confirm With Final Zone ☐

Durations

Minimum

Maximum

Default

Sigma Multiplier

Include Zone History ☐

Include Location History ☐

[< Back](#)

Save

**Table 10** Events Tab Fields

Field	Description
<b>Types</b>	<p>Specifies which events to report. Select at least one event type to receive events; otherwise, no events are reported.</p> <ul style="list-style-type: none"> <li>• <b>New:</b> Generates a tag report with a <code>New</code> status when a tag is first detected in the reader's field of view, or when a tag exits the reader's field of view and then re-enters it.</li> <li>• <b>Transition:</b> Generates a tag report with a <code>Transition</code> status when a previously visible tag moves from one zone to another. The transition metadata indicates the current zone and prior zone.</li> <li>• <b>Timeout:</b> Generates a tag report with a <code>Timeout</code> status when a tag that was previously detected goes unseen for a user-defined time period.</li> <li>• <b>Update:</b> Generates a tag report with an <code>Update</code> status for each individual tag at regular intervals, even if no transitions or changes in the tag's state occur. Set <b>Update Interval</b> to the required interval.</li> </ul>

If you select to report **Timeout** events, the tab displays the following additional fields to configure:

**Table 11** Events Tab - Additional Timeout Events Fields

Field presented if Timeout is selected		Description
<b>Direction</b>	<b>Kinds</b>	<p>Specifies the direction in which to report a timeout event. Select one or more of the following:</p> <ul style="list-style-type: none"> <li>• <b>In:</b> The tag moved from south to north.</li> <li>• <b>Out:</b> The tag moved from north to south.</li> <li>• <b>None:</b> The tag has not moved in the north or south direction.</li> <li>• <b>Error:</b> There was an error in determining the direction of travel.</li> <li>• <b>Unknown:</b> The data from the tag is insufficient to determine the direction of travel.</li> </ul>
	<b>Look Back Duration</b>	Specifies the duration to consider before the last tag read (prior to the timeout) for determining the tag's direction.
	<b>Confirm With Final Zone</b>	Specifies whether to indicate the direction as <code>unknown</code> if the final zone conflicts with the direction determined in regression.
<b>Durations</b>	<b>Minimum</b>	Specifies the minimum duration until a tag is deemed gone.
	<b>Maximum</b>	Specifies the maximum duration until a tag is deemed gone.
	<b>Default</b>	Specifies the default duration until a tag is deemed gone.
	<b>Sigma Multiplier</b>	Specifies a multiple of the standard deviation of time between reads to determine an adaptive timeout.

**Table 11** Events Tab - Additional Timeout Events Fields (Continued)

Field presented if Timeout is selected	Description
<b>Include Zone History</b>	Specifies whether to include the zone history in the tag report for the <b>Timeout</b> event.
<b>Include Location History</b>	Specifies whether to include the location history in the tag report for the <b>Timeout</b> event.

**Filter Tab**

The **Modes > Filter** tab allows you to filter reads based on their RFID tag ID. If no filter is specified, all reads are considered.

**Figure 17** Filter Tab

The screenshot shows the Zebra Infrastructure Users interface. At the top, there's a header with the Zebra logo, 'Infrastructure', 'Users', and a user profile 'admin@customer.com'. Below this is a navigation bar with '< Edit Device'. The main content area is divided into a left sidebar and a right panel. The sidebar has sections: 'Sync' (with a status 'In progress'), 'Identity', 'Location' (with a red info icon), 'Network' (with a red info icon), and 'Modes'. The right panel shows device details: 'Name: zebra\_atr700\_84248df30e7a', 'Serial: 84248df30...', 'MAC Address:', 'Make: zebra', and 'Type: ATR7000'. Below this is a 'Mode Name' field with 'Mode1' and a character count '59 characters left'. There are five tabs: 'Lanes', 'Events', 'Filter' (selected), 'Beams', and 'Advanced'. The 'Filter' tab contains three fields: 'Match' (a dropdown menu), 'Value' (a text input), and 'Operation' (a dropdown menu). At the bottom, there are '< Back' and 'Save' buttons.

**Table 12** Filter Tab Fields

Field	Description
<b>Match</b>	Specifies the segment of the ID to match or the method to use to match. Select between the following options: PREFIX, SUFFIX, and REGEX.
<b>Value</b>	Specifies the value to match. For prefix and suffix filters, enter only hexadecimal digits, and the number of digits must be even. When a prefix filter is used, selects cannot be used. For a regex filter, C++ STL regex <u>values</u> should be used.
<b>Operation</b>	Specifies the filter operation. Select between <b>INCLUDE</b> and <b>EXCLUDE</b> .

**Beams Tab**

The **Modes > Beams** tab allows you to configure the beam of the integrated antenna of the ATR7000. The beam refers to the pattern and directionality of the radio frequency signals emitted by the antenna.



Figure 18 Beams Tab

InfrastructureUsersadmin@customer.com

< Edit Device

SyncIn progress

Name: zebra\_atr700\_84248df30e7a

Serial: 84248df30... MAC Address:

Make: zebra

Type: ATR7000

Identity

Location

Network

Modes

Mode Name

Mode1

59 characters left.

Lanes

Events

Filter

Beams

Advanced

Read Beams

Default

Polarization

LHCP

Custom

#

Azimuth

Elevation

Add New Beam

< Back

Save

Table 13 Beams Tab

Field	Description
Read Beams	<div>Specifies the beam configuration:</div> <ul style="list-style-type: none"><li><b>Default:</b> Uses the standard beam configuration optimized for general use cases, balancing performance and coverage.</li><li><b>Dense:</b> Configures beams with a higher density, providing more granular detection or coverage but potentially at the cost of performance or range.</li><li><b>Sparse:</b> Configures beams with lower density, focusing on broader coverage with reduced granularity. This is suitable for applications where fine detail is not necessary.</li><li><b>Custom:</b> Allows you to define a specific beam configuration tailored to your unique requirements, offering maximum flexibility.</li></ul>

**Table 13** Beams Tab (Continued)

Field	Description
<b>Polarization</b>	<p>Specifies the polarization of the beam:</p> <ul style="list-style-type: none"> <li>• <b>LHCP</b>: Left-hand circular polarization, where radio waves rotate in a circular motion to the left as they propagate, enhancing tag readability in varied orientations.</li> <li>• <b>RHCP</b>: Right-hand circular polarization, where radio waves rotate in a circular motion to the right as they propagate, enhancing tag readability in varied orientations.</li> <li>• <b>TOTAL</b>: Omni-directional coverage, where radio waves are emitted uniformly in all directions, creating a spherical or donut-shaped coverage area around the antenna. It ensures broad coverage without focusing on specific polarization.</li> <li>• <b>THETA</b>: Linear polarization with the radio waves oriented at a specific angle in the horizontal plane, optimizing signal propagation along this plane.</li> <li>• <b>PHI</b>: Linear polarization with the radio waves oriented at a specific angle in the vertical plane, optimizing signal propagation along this plane.</li> </ul>
<b>Custom</b>	<p>Specifies a custom array of beams to use when <b>Read Beams</b> is set to <b>Custom</b>. Each beam has the following settings:</p> <ul style="list-style-type: none"> <li>• <b>Azimuth</b>: Specifies the Azimuth angle of the beam, in degrees. The azimuth angle is the horizontal angle of the beam, measured from the forward facing direction of the reader. It indicates how far left or right the beam is oriented in the horizontal plane.</li> <li>• <b>Elevation</b>: Specifies the elevation angle of beam, in degrees. The elevation angle is the vertical angle of the beam, measured from the forward facing direction of the reader. It indicates how far up or down the beam is oriented in the vertical plane.</li> </ul> <p>Click <b>Add New Beam</b> to add a new one.</p>

**Advanced Tab**

The **Modes > Advanced** tab allows you to configure the following power and density (PD) settings.



**NOTE:** These settings should not normally be adjusted.

**Figure 19** Advanced Tab

Infrastructure
Users
admin@customer.com

< Edit Device

Sync
In progress

Name: zebra\_atr700\_74248df30e73
Serial: 74248df30...
MAC Address:
Make: zebra
Type: ATR7000

Identity
Location
Network
Modes

Mode Name
ATR700PD
56 characters left.

Lanes
Events
Filter
Beams
Advanced

Hysteresis Distance
0ft0in

Background Processing Interval
0d0h0m0s0ms

Moving Average Duration
0d0h0m0s0ms

Raw Location Confidence Threshold

Max Tag Count

Debug

Log Level

Include Raw
☐

Regression

Min N

Min Duration
0d0h0m0s0ms

Extrapolation Multiplier

Slope Threshold

Radio

Environment

Delay Between Antenna Cycles

Delay Duration
0d0h0m0s0ms

Radio Start Conditions

Type

Port

Signal

Debounce Time
0d0h0m0s0ms

Radio Stop Conditions

Duration
0d0h0m0s0ms

Antenna Cycles

Tag Count

Duration After No More Unique Tags
0d0h0m0s

Port

Signal


Debounce Time
0d0h0m0s0ms

Back
Save

**Table 14** Advanced Tab Fields

Field		Description
<b>Hysteresis Distance</b>		Specifies the distance a tag must go back into the zone it came from to be transitioned back into that zone. The default is 24 inches. This is not normally modified.
<b>Background Processing Interval</b>		Specifies the background processing interval at which reads are processed. The default is 500 milliseconds. This is not normally modified.
<b>Moving Average Duration</b>		Specifies the duration over which raw tag locations are averaged to smooth and stabilize their positions. The default is 3 seconds. This is not normally modified.
<b>Raw Location Confidence Threshold</b>		Specifies the minimum confidence level required for a raw location estimate to be used in determining the location, zone, or direction. The default is 50.
<b>Max Tag Count</b>		Specifies the maximum tag count.
<b>Debug</b>	<b>Log Level</b>	Specifies the level of information that the application should log. Possible values are <b>INFO</b> , <b>ERROR</b> , <b>DEBUG</b> , <b>WARNING</b> . The default is <b>INFO</b> .
	<b>Include Raw</b>	Specifies whether raw tag reads are included in the log.
<b>Regression</b>	<b>Min N</b>	Specifies the minimum number of data points required by regression to determine a direction other than <code>Unknown</code> . The default is 3.
	<b>Min Duration</b>	Specifies the amount of time over which data points must be collected or present within a specified time window (the lookback window) to ensure the regression algorithm has sufficient data to make a determination regarding direction. The default is 750 milliseconds.
	<b>Extrapolation Multiplier</b>	Specifies the <u>value</u> that regression uses to determine how far to extrapolate beyond the lookback duration for crossings. The default is 1.
	<b>Slope Threshold</b>	Specifies the value of the slope that regression uses to distinguish between the In and Out (and None) direction. The default is 0.

**Table 14** Advanced Tab Fields (Continued)

Field		Description
Radio	Environment	<p>Specifies the type of environmental conditions in which the reader operates. Along with the regulatory configuration of the reader, the environment field sets the default link profile parameters (such as, Miller mode, BLF, and Tari) and the receiver dynamic range (interference immunity). Possible values are the following. The default is <b>HIGH_INTERFERENCE</b>.</p> <ul style="list-style-type: none"> <li>• <b>HIGH_INTERFERENCE</b>: Significant interference from external sources (for example, competing RF devices, industrial equipment generating electromagnetic noise, or physical obstructions like metal structures).</li> <li>• <b>LOW_INTERFERENCE</b>: Low interference from external sources (for example, minimal physical barriers or areas with limited RF activity).</li> <li>• <b>VERY_HIGH_INTERFERENCE</b>: Very high interference from external sources.</li> <li>• <b>AUTO_DETECT</b>: Automatically detected interference. The RFID reader continuously monitors the environment and dynamically adjusts its settings (for example, power levels, frequency hopping, or sensitivity) to optimize performance. This mode is useful when interference levels fluctuate or are difficult to predict during setup.</li> <li>• <b>DEMO</b>: Interference controlled for testing or demonstration purposes. This mode prioritizes simplicity and predictability over interference mitigation, making it suitable for trade shows, training, or troubleshooting in non-production environments.</li> </ul>
	Delay Between Antenna Cycles	<p>Specifies to introduce a delay between antenna cycles if no tags are read or if no unique tags are read. This allows the reader to share the spectrum if there are no tags to be read. Possible values are the following. The default is <b>NO_UNIQUE_TAGS</b>.</p> <ul style="list-style-type: none"> <li>• <b>Disabled</b>: Does not introduce a delay.</li> <li>• <b>NO_TAGS</b>: Introduces a delay if no tags are read.</li> <li>• <b>NO_UNIQUE_TAGS</b>: Introduces a delay if there are no unique tags read.</li> </ul>
	Delay Duration	<p>Specifies the delay duration between antenna cycles if <b>Delay Between Antenna Cycles</b> is set to <b>NO_TAGS</b> or <b>NO_UNIQUE_TAGS</b>.</p> <p> <b>NOTE:</b> For <b>DISABLED</b>, <b>Delay Duration</b> must be 0 seconds; otherwise, it must be a non-zero value.</p> <p>Since the default is <b>NO_UNIQUE_TAGS</b>, the default delay duration is 75 milliseconds.</p>
Radio Start Conditions		<p>Specifies when, after you issue a <b>Start</b> command, the radio starts trying to inventory tags.</p>

**Table 14** Advanced Tab Fields (Continued)

Field		Description
	<b>Type</b>	Specifies the type of start after you issue a <b>Start</b> command. Possible values are: <ul style="list-style-type: none"> <li>• <b>blank</b>: The radio starts trying to inventory tags immediately.</li> <li>• <b>GPI</b>: The radio waits for a general-purpose input (GPI) before trying to inventory tags.</li> <li>• <b>GPI with restart</b>: The radio waits for a general-purpose input (GPI) before trying to inventory tags. When the signal is received, it restarts the reader.</li> </ul>
	<b>Port</b>	Specifies whether to receive the GPI on port <b>1</b> or <b>2</b> .
	<b>Signal</b>	Specifies whether to start on a <b>HIGH</b> or <b>LOW</b> signal level.
	<b>Debounce Time</b>	Specifies the duration that the GPI must remain at the specified signal level to trigger the event (that is, the start).
<b>Radio Stop Conditions</b>		Specifies when an ongoing operation should complete. If not specified, the radio continues trying to inventory tags until you issue a <b>Stop</b> command.
	<b>Duration</b>	Specifies the duration to run until the radio stops.
	<b>Antenna Cycles</b>	Specifies the number of cycles through all enabled antennas before the radio stops.
	<b>Tag Count</b>	Specifies the number of tags to inventory until the radio stops.
	<b>Unique Tag Count</b>	Specifies the duration after not inventorying any more unique tags to stop the radio.
	<b>Port</b>	Specifies whether to wait for a general-purpose input (GPI) to stop the radio. It also specifies the port on which to receive the GPI, either port <b>1</b> or <b>2</b> . If the field is blank, a GPI is not used.
	<b>Signal</b>	Specifies whether to stop on a <b>HIGH</b> or <b>LOW</b> signal level.
	<b>Debounce Time</b>	Specifies the duration that the GPI must remain at the specified signal level to trigger the event (that is, stop).

## Configuring Dual-Portal Directionality

The steps below describe how to pair and configure two ATR7000 readers to operate in dual-portal directionality mode.

1. Navigate to **Infrastructure > Devices**.
2. Select the two readers that should operate in dual-portal directionality mode.

anager / Devices

Devices 1 - 2 of 2

< Page 1 of 1 >

Devices per page: 100

Refresh

+ Add

Templates

<input checked="" type="checkbox"/>	Alerts	Device Make	Device Model	Status	Linked
<input checked="" type="checkbox"/>		zebra	ATR7000-P1100A0-US	ONLINE	
<input checked="" type="checkbox"/>		zebra	ATR7000-P1100A0-US	ONLINE	

Dual PD on the secondary bar becomes available.

Infrastructure	Users	admin@customer.com
Templates	Certificates	Dual PD
Map Name	Name	
floor1	zebra_atr700_84248df30e7a	
floor1	zebra_atr700_84248df30e7a	

3. Click **Dual PD**.

The **Edit Device** page for dual-portal directionality (dual-PD) configuration is displayed, allowing you to configure the two selected readers in this mode.

< Edit Device		
Sync Status 	Name: zebra_atr7000_173401655306280 Serial: 173401655306280 MAC Address:	Name: zebra_atr7000_173401655351281 Serial: 173401655351281 MAC Address:
Identity	Name: zebra_atr7000_173401655306280	Name: zebra_atr7000_173401655351281
Location	Template	
Network		
Modes		

## 4. On the **Identify** tab:

- a) In **Reader Name** field, specify a friendly location name that identifies the doorway location of the readers (for example, North, West, Backdoor).

Resonate uses this information to generate the zone names contained in the events.

- b) Optionally, select a template to configure the fields of both readers with the filled-in fields of the template, and click **Apply**.

Both readers must be of the same model; if not, the template field is grayed out. Templates are specific to the type and model of the reader; only applicable templates are listed. For information on templates and how to create one, refer to [Templates](#) on page 77.

Clicking **Apply** updates the different tabs of the **Edit Device** page with the filled-in fields of the template. The template affects only those fields whose settings can apply to multiple readers; fill in the remaining required fields. If required, you can modify fields set by the template. If you previously modified other fields on the different tabs and clicked **Save**, those fields are not modified. If you did not save, the template might reset them.

The values are not saved to the readers until you click **Save**. If the template field is grayed out or you choose not to use a template, you must configure both readers field-by-field.

## 5. On the **Location** tab, select the site and map (**Level**) of the readers, and set their coordinates and yaw.

For information on setting these fields, refer to [Location Tab](#) on page 45.

If the reader location was previously entered via **Device Edit** or the template, the location is automatically filled in on this page.

## 6. On the **Network** tab, configure the network settings for each reader.

For information on setting these fields, refer to [Network Tab](#) on page 46.

The screenshot shows the Zebra Infrastructure web interface. At the top, there's a header with the Zebra logo, 'Infrastructure' tab, 'Users' dropdown, and a user profile 'admin@customer.com'. Below the header is a breadcrumb 'Edit Device'. The main content area is divided into two columns, each representing a reader. The left reader has a 'Sync' status of 'In progress'. Both readers have the same Name, Serial, and MAC Address. The 'Identity' tab is selected on the left. The 'Location' tab has a red error icon. The 'Network' tab is active, showing fields for Hostname, NTP Address, DNS Address, MAC Address, IP Address (with a DHCP/Static toggle), and Gateway. The 'Modes' tab is also visible. At the bottom, there are 'Back' and 'Save' buttons.

	Reader 1	Reader 2
Sync	In progress	
Name	zebra_atr700_8...	zebra_atr700_8...
Serial	84248df30e73	84248df30e7a
MAC Address		
Hostname	ATR7000F3106F	ATR7000F310C1
NTP Address	pool.ntp.org	pool.ntp.org
DNS Address	10.61.226.5	10.61.226.5
MAC Address	MAC Address	MAC Address
IP Address	IP Address	IP Address
Gateway	Gateway	Gateway



- On the Modes tab, configure the dual-portal directionality mode.

For information on setting these fields, refer to [Modes Tab for ATR7000](#) on page 60.

The screenshot shows the 'Edit Device' page in the Zebra Infrastructure web interface. The 'Modes' tab is active, and the 'Lane Plan' is set to 'Dual Lane'. The 'Mode Name' is 'Mode1'. The 'Lane Width' is 120, 'Lane Extension' is 0, and 'Tag Height' is 36. The 'Sync' status is 'In progress'. The 'Name' and 'Serial' fields are visible at the top.

- Click **Save**.

You return to the **Infrastructure > Devices** page. Notice that the two readers that you just configured have active link icons, indicating they are paired with another for dual-portal directionality mode. Hover over an active link icon to see the paired reader.

<input type="checkbox"/>	Alerts	Device Make	Device Model	Status	Linked Device	Serial #	
<input checked="" type="checkbox"/>		zebra	ATR7000-P1100A0-US	ONLINE		zebra_atr7000_84248df30e73	
<input type="checkbox"/>		zebra	ATR7000-P1100A0-US	ONLINE		84248df30e7a	

<input type="checkbox"/>	Alerts	Device Make	Device Model	Status	Linked	Serial #	
<input checked="" type="checkbox"/>		zebra	ATR7000-P1100A0-US	ON		zebra_atr7000_84248df30e73	
<input type="checkbox"/>		zebra	ATR7000-P1100A0-US	ONLINE		84248df30e7a	

Selecting **Device Settings > Edit** for a linked reader now displays the **Edit Devices** page for dual-portal directionality (dual-PD) configuration again.

## Monitoring Device Health and Status




To monitor your RFID readers, use the **Infrastructure > Devices** page, which displays their statuses and notifications (alerts and errors).

Besides viewing reader alerts in the Resonate RFID Reader Management web interface, you can configure Resonate to send reader and/or server alerts to targets via email or webhooks. For information, refer to [Alerting Targets](#) on page 87.

## Notifications

The **Alerts** column of the **Device** grid displays the notifications. Hover over the icon to see details about the notifications. The following are the possible notifications and corresponding icons:

**Table 15** Possible Notifications Displayed in the Alerts Column

Device State	Icon	Description
Healthy		The RFID reader is reporting no issues.
Warning		The RFID reader is reading and transmitting tag read data, but the reader is experiencing an issue (for example, it is starting to disconnect or overheat).
Critical		The RFID reader is reading and transmitting tag read data, but the reader is experiencing an issue that is more serious than one that warrants just a warning (for example, it is overheating). You might also obtain this alert if the reader is not responding, so its status is unknown.
Error		The RFID reader is experiencing a real-time, immediate problem (for example, after you send it a command, something fails).

Refer to [Available Alerts](#) on page 88 for the possible alerts and to [Determining the Root Cause of RFID Reader Issues](#) on page 100 on how to establish the root cause.

## Status

The **Status** column of the **Device** grid displays the current status of each RFID reader. The status can be one of the following:


**Table 16** Possible statuses

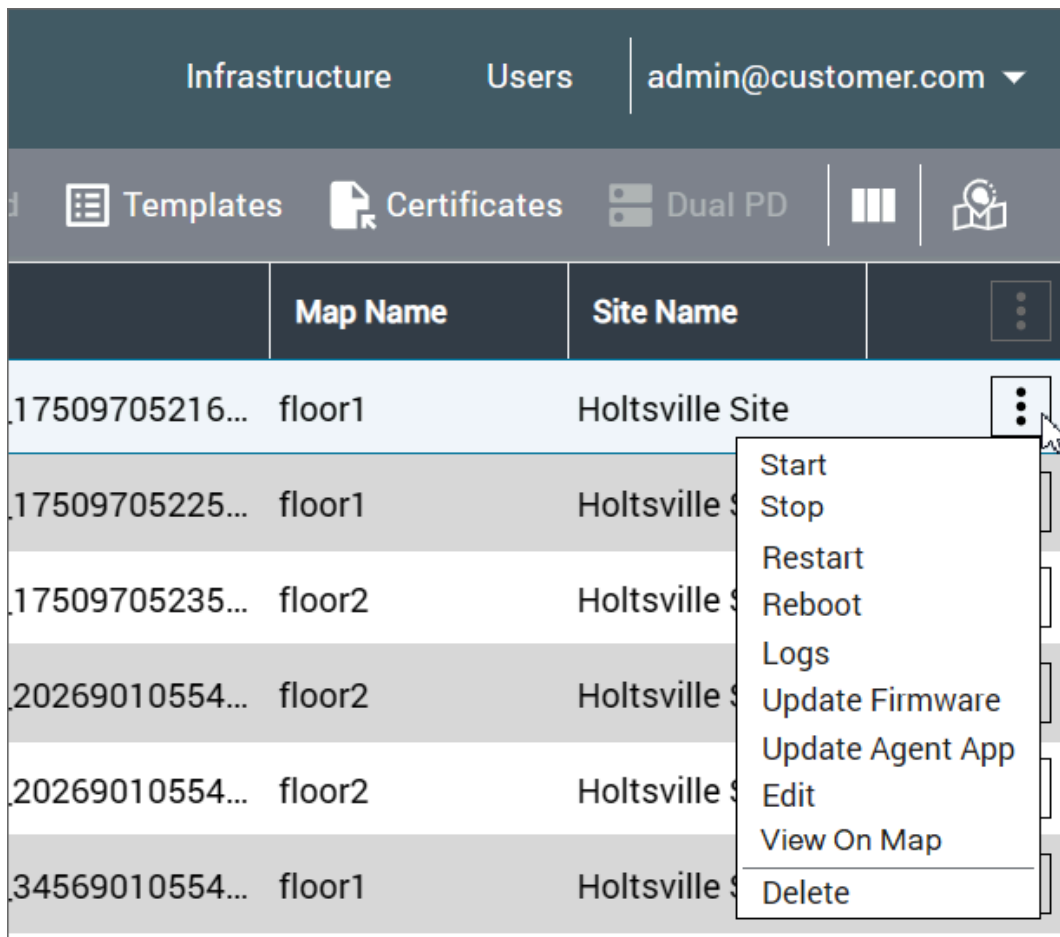
Status	Description
OFFLINE	The RFID reader is offline. It might be powered off or not connected to the network.
ONLINE	The RFID reader is online. It has established communication with Resonate and is waiting for a command.
ACTIVE [MODE]	The RFID reader is active and operating in the indicated mode. The reader is actively engaged in reading and reporting all unique tags in the radio's field of view (FOV).
REBOOTING	The RFID reader is rebooting (that is, powering down and starting up again).
ELEVATING	The RFID reader is running Resonate Agent for the first time, either during reader initialization or after a Resonate Agent update, and Resonate Agent is installing and integrating required components.
APPLYING [SETTING]	The RFID reader is applying changes to the indicated setting.
UPDATING [PROGRESS]	The RFID reader is updating its software (for example, Resonate Agent). The update progress is indicated.
RESTARTING	The RFID reader is restarting Resonate Agent (typically after it has been updated or you have issued a <code>Restart</code> command).

**Table 16** Possible statuses (Continued)

Status	Description
UPGRADING [PROGRESS]	The RFID reader is upgrading its firmware. The upgrade progress is indicated.

## RFID Reader Commands and Actions

Control and manage RFID readers using the commands and actions accessible from the  **Device Settings** menu at the far right of the readers' row on the **Infrastructure > Devices** page.

**Figure 20** Device Settings Menu

The commands and actions available are as follows:

- **Start:** Activates the reader so that it starts reading tags.
- **Stop:** Deactivates the reader so that it stops reading tags.
- **Restart:** Stops the Resonate Agent instance running on the reader (which communicates with Resonate RFID Reader Management), and then starts a new instance of that application.
- **Reboot:** Reboots the reader. To execute this command, you must select **Update Immediately**.


- **Logs:** Allows you to see the reader's logs (Application, System, Directionality, or Radio logs). This command might take several seconds to complete, depending on the size of the log being shown. Also, some logs are available for certain readers.
- **Update Firmware:** Updates the firmware version running on the reader. Select the version to install on the reader from the supported list. Note that only the listed firmwares are available; contact Zebra Product Support if you require a different version. To execute this command, you must select **Update Immediately**.
- **Update Agent App:** Updates the version of Resonate Agent that runs on the reader. Select the version to install on the reader from the supported list. To execute this command, you must select **Update Immediately**.
- **Edit:** Allows you to edit and view the settings of the reader.
- **Delete:** Removes the reader from Resonate RFID Reader Management. Resonate will no longer manage the reader.

## Replacing an RFID Reader

The following describes how to replace an installed RFID reader with a new one, while retaining the original configuration.



**NOTE:** The new RFID reader must be of the same type and model as the original.

1. Run the Resonate Device Initializer utility to discover the new reader. Refer to [Using Resonate Device Initializer in Device-Discovery Mode](#) on page 35
2. Navigate to **Infrastructure > Devices** and take note of the original reader's serial number.
3. Navigate to **Infrastructure > Discovered Devices**.
4. Select  **Device Settings > Replace** at the far right of the new RFID reader's row.

The **Replace Device** dialog opens.
5. Click **Replace** to the right of the reader to replace.

The original reader is replaced.

The **Infrastructure > Devices** page displays the new reader with the same configuration as the original reader, and it no longer displays the original reader.

# Templates

This section describes how to create a template to configure your RFID readers.

## Templates Overview

You might need to add several RFID readers in Device Manager with the same basic configuration. For example, you might want to add several FX9600 readers that have the same operation 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 configuring the new readers. You can also apply the template to multiple selected readers at a time. This automatically populates the corresponding fields in the newly added devices. You can then modify individual fields for specific readers, overriding the template values.

You can also update configured readers with a template; it applies only the filled-in template fields to the selected readers.

Templates are specific to a type and model of RFID reader. You need to create different templates for different types and models of RFID readers.

To create a template, you must have the role of Device Configurator (person(s) responsible for setting up the device configuration).

## Creating a Template

The following describes how to create a template. You must have the role of Device Configurator.



**NOTE:** Templates are specific to a type and model of RFID reader. You need to create different templates for different types and models of RFID readers.

1. Navigate to **Infrastructure > Devices**.

2. Click **Templates**.

The **Templates** page opens, displaying existing templates and allowing you to create new templates.

3. Click **+Add**.

The **Select a Device Type** dialog opens.

4. Select the type of RFID reader for which to create the template, and then click **Continue**.

The **Add Template** page opens.

This page includes the following tabs, depending on the RFID reader type: **Template**, **Location**, **Networking**, **Antennas**, and **Modes**. The template is created from the data contained on all the tabs.

5. On the **Template** tab:
  - a) Select the model number of the RFID reader for which to create the template.
  - b) Enter a name for the template.
6. On the remaining tabs, fill in the appropriate fields.



**NOTE:** If required fields are not filled in, a warning icon appears next to the tab name, and the fields are highlighted to indicate the error. You must fill in these fields before you can save the template.

The tabs only contain fields that apply to the selected RFID reader type and model, and that can apply to multiple devices. For information on the fields, refer to [Device Configuration Overview](#) on page 43.


7. Click **Save** to create and save the template.

The new template is displayed on the **Templates** page.

## Using a Template to Configure a Single RFID Reader

The following describes how to use a template to configure a single RFID reader.

To configure multiple selected RFID readers at once using a template, refer to [Using a Template to Configure Multiple Selected RFID Readers](#) on page 79.

1. Navigate to **Infrastructure > Devices**.
2. Select  **Device Settings > Edit** at the far right of an RFID reader's row.

The **Edit Device** window is displayed.

3. On the **Identity** tab, select the required template, and click **Apply**.

**Figure 21** Identity Tab

This updates the different tabs with the filled-in template fields. If you previously modified other fields on the different tabs and clicked **Save**, these other fields are not modified. If you did not save your changes, the template might reset them.

4. On the remaining tabs, fill in the appropriate fields.

If necessary, you can modify template-filled fields.

5. Click **Save**.

The RFID reader is configured with the settings of the different fields.

## Using a Template to Configure Multiple Selected RFID Readers

The following describes how to use a template to configure multiple selected RFID readers with the same basic configuration at the same time.

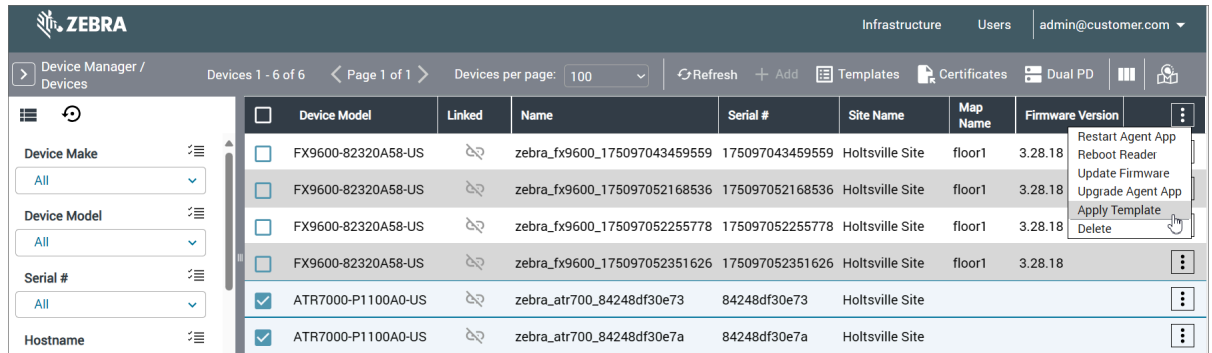
To configure a single RFID reader using a template, refer to [Using a Template to Configure a Single RFID Reader](#) on page 78.

1. Navigate to **Infrastructure > Devices**.
2. Select the RFID readers to configure.

The RFID readers must be of the same type and model. You can use the filters in the left panel to display only RFID readers of a specific type and model; then, click the checkbox in the selector column header to select all displayed RFID readers

## Templates

3. Select  **Device Settings > Apply Template** in the device settings column header.




Device Model	Linked	Name	Serial #	Site Name	Map Name	Firmware Version	
<input type="checkbox"/> FX9600-82320A58-US		zebra_fx9600_175097043459559	175097043459559	Holtsville Site	floor1	3.28.18	
<input type="checkbox"/> FX9600-82320A58-US		zebra_fx9600_175097052168536	175097052168536	Holtsville Site	floor1	3.28.18	
<input type="checkbox"/> FX9600-82320A58-US		zebra_fx9600_175097052255778	175097052255778	Holtsville Site	floor1	3.28.18	
<input type="checkbox"/> FX9600-82320A58-US		zebra_fx9600_175097052351626	175097052351626	Holtsville Site	floor1	3.28.18	
<input checked="" type="checkbox"/> ATR7000-P1100A0-US		zebra_atr700_84248df30e73	84248df30e73	Holtsville Site			
<input checked="" type="checkbox"/> ATR7000-P1100A0-US		zebra_atr700_84248df30e7a	84248df30e7a	Holtsville Site			

The **Select Template** window is displayed.

4. Select the required template and click **Apply**.

This updates the selected RFID readers with only the filled-in template fields. The **Devices** window is displayed again, and a message displays the operation status and the number of RFID readers updated.

After basic configuration using the template, access the settings of the individual RFID readers using  **Device Settings > Edit** at the far right of the reader's row, and configure the remaining fields appropriately.



# Connecting to RFID Readers to Get Tag Read Data

This section describes how to connect to RFID readers to get tag read data.

## Reader Connection for Tag Read Data

Resonate RFID Reader Management supports a user interface, commands, and APIs to manage populations of RFID Readers. It does not do data collection of RFID tag read data. Instead, you must configure RFID readers to send tag read data directly from the reader to your customers or partners solution software application.

Currently, Resonate only supports a single data output connection from the reader; this is a websocket server connection. The websocket is based off the `secure` setting of the reader; this determines if the websocket uses TLS. Consult your Zebra sales representative for the roadmap of other endpoint types (for example, webhooks and MQTT).

Resonate provides its own data contract definitions, separate from Zebra IoT Connector (ZIoTConnector). This allows Resonate to offer data output formats that emulate ZIoTConnector, as well as new data formats optimized for other solutions. For the current version of Resonate, the WebSocket connection provides an emulation of the standard ZIoTConnector Tag Data Events format. For details and documentation, refer to [https://zebradevs.github.io/rfid-ziotc-docs/schemas/tag\\_data\\_events/index.html](https://zebradevs.github.io/rfid-ziotc-docs/schemas/tag_data_events/index.html).

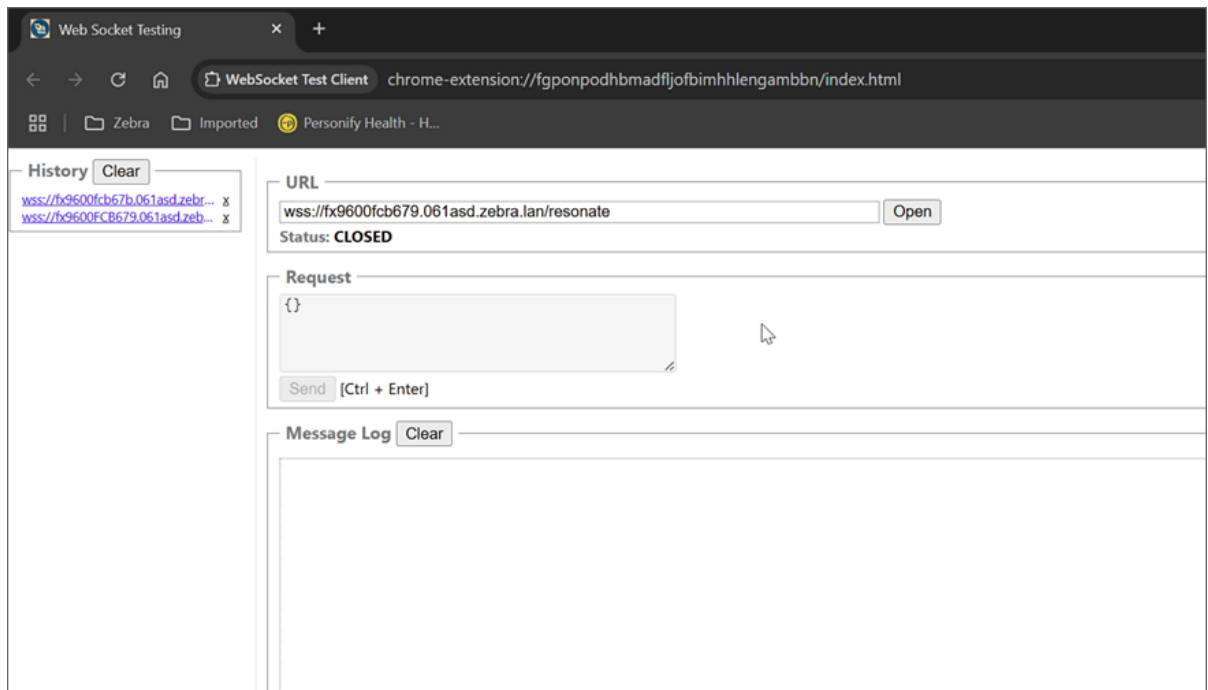
Since Resonate does not use ZIoTConnector and instead is controlled by an on-reader Agent app, connecting to the reader's tag read data output stream requires the use of a different WebSocket endpoint address from the address in the ZIoTConnector documentation. To connect to the reader to get its output, your application should connect to `ws://<reader_FQDN>/resonate` (if using a secure websocket, it should use `wss://`). Otherwise, the data that you receive will match the format and content defined in the ZIoTConnector [documentation](#).

To test, use any standard WebSocket client application to connect to the reader via WebSocket and receive tag read data. One example is a simple extension to the Google Chrome browser<sup>2</sup>: <https://chromewebstore.google.com/detail/websocket-test-client/fgponpodhbmadvfjofbimhhhengambbn>. If you prefer to write your own Websocket client test application, a code example in Python is available in the ZIoTConnector documentation ([https://zebradevs.github.io/rfid-ziotc-docs/other\\_cloud\\_support/Web%20Sockets/testing.html](https://zebradevs.github.io/rfid-ziotc-docs/other_cloud_support/Web%20Sockets/testing.html)). To test, setup a reader in Resonate, configure it with a mode from Resonate, and connect to the reader with `ws://<reader_FQDN>/resonate` (if using a secure websocket, use `wss://`).

---

<sup>2</sup> Note that Zebra technical support does not provide support for this extension.

**Figure 22** Google Chrome browser extension connected to a reader via a WebSocket



# Digital Certificates

This section describes using certificates with your RFID readers.

## Certificates Overview

Currently, Resonate supports CA certificates, but has limited support for endpoint certificates with readers.

X.509 digital certificates are files that contain information to secure connections between networked devices (for example, a server, reader, or web client (web interface)). Certificates work with public-private key pairs and with digital signatures to assert the identity of the networked device. These endpoint certificates can be self-signed at the time of generation or can be signed by a separate Certificate Authority (CA). Companies often have policies that prevent trusting self-signed certificates, so enterprises often require signed certificates. If both networked devices in the connection trust the CA (that is, both have a copy of the CA certificate), they can both trust the networked device (endpoint) certificate signed by that CA. Large enterprises often issue their own CA certificates so that devices restricted to their private enterprise network can trust their enterprise-signed endpoint certificates, without having to pay a third party to do so.

Resonate always sets readers to operate in their secure mode. This tells the readers to always require a secure connection when possible. For example, if you connect via browser to the reader's web interface, the reader will always require HTTPS. HTTPS requires TLS security, which uses X.509 digital certificates. The reader can support HTTPS using its default self-signed certificate, but this might cause a pop-up browser message, indicating that self-signed certificates are not trusted. To avoid this message, you can add a CA-signed certificate.

Currently, Resonate has limited support for endpoint certificates with readers, so in some cases, you must add those signed certificates using the reader's web interface instead of through Resonate.

In general, readers have three types of network connections that can be secured with the help of X.509 digital certificates:

- Reader-to-Resonate for management
- Reader data endpoints to share RFID read data
- Browser-to-readers direct web interface

In addition, the browser connection between users and the Resonate RFID Reader Management web interface can also be secured with X.509 digital certificates.

### Reader-to-Resonate

During device initialization, the Resonate on-reader management agent (Resonate Agent) is given a copy of the CA certificate used by Resonate. The reader initialization process uses that certificate to trust the

Resonate instance, so they can work together to securely generate reader keys and login tokens (Keycloak client credentials) for securing the reader's Resonate Agent management connection.

Resonate comes with a self-signed certificate, but you can choose to use an enterprise-signed or publicly signed certificate for Resonate. If so, copy the certificate to the Resonate server's file system; then, use the Resonate installer (`install.sh`) with the `--tls-certificate` and `--tls-key` options to assign the certificate to the server. This tells the Resonate `install.sh` script to include the new certificate instead of the self-signed one included by default. If required, this should typically be done at Resonate installation time or before adding readers; otherwise, you will have to re-initialize the readers.

### Read Data

Currently, Resonate managed readers support a single WebSocket server data export endpoint. This connection is secured with the reader's server certificate. In this case, the reader is serving the data, so the reader is the server side of the connection, not the client side. The customer's WebSocket client application can connect to the reader's WebSocket server endpoint at `wss://<reader FQDN>/resonate`.

Zebra readers come with a self-signed certificate, but you can choose to use an enterprise-signed or publicly signed certificate for reader communications. If so, you must load the new certificate onto the reader via the ZloTC APIs or the reader's built-in web interface.

### Reader's Web Interface

The third possible connection to a reader is through its built-in web interface, accessed from a browser. It allows you to access ZloTC settings on the reader, but not the Resonate settings. It is not recommended that users access the reader's web interface when using Resonate because this can cause confusion and potentially interfere with Resonate management of the reader. If you require web interface access, connect to the reader's web interface server endpoint at `https://<reader FQDN>/`.

Zebra readers come with a self-signed certificate, but you can choose to use an enterprise-signed or publicly signed certificate for reader communications. If so, you should load a new certificate onto the reader via the ZloTC APIs or via the reader's built-in web interface. The same reader server endpoint certificate is used to secure both the WebSocket server data endpoint and the web interface server endpoint.

### Resonate's Web Interface

Although not reader-related, Resonate can use an enterprise certificate to authenticate the Resonate server to its web client (Resonate's web interface loaded in the browser). This avoids receiving the self-signed certificate error when browsing to the Resonate web interface. If you added an enterprise-signed certificate during Resonate installation (as described above), this is already handled. If not, follow the same instructions to add the certificate (that is, copy the certificate to the Resonate server's file system; then, use the Resonate installer with the `--tls-certificate` and `--tls-key` options). If required, this should typically be done at Resonate installation time or before adding readers; otherwise, you will have to re-initialize the readers. For more information, refer to the `install.sh` topic in the Software Installation Guide.

### CA certificates

Although Resonate currently does not support endpoint certificate maintenance, Resonate can download a Certificate Authority (CA) certificate to the reader to authenticate the signature of a CA-signed endpoint certificate installed manually.

### Certificate Installation

When you enable communication between the Resonate server and an RFID reader, Resonate Device Initializer automatically secures the onboarding process using the Resonate server's digital certificate. After

the onboarding process, the new reader uploads all its known CA certificates to Resonate, and Resonate installs all CA certificates not already installed on the reader to it.

To install other CA certificates on the RFID readers, upload them to Resonate; Resonate automatically installs the certificates on all the RFID readers after you upload them. Refer to [Installing a CA Certificate](#) on page 85.

Zebra RFID readers come from the factory with CA certificates from many trusted Certificate Authorities. Zebra RFID readers also come from the factory preloaded with a self-signed reader certificate identifying and securing that reader. Zebra readers do not come with enterprise-signed certificates, allowing trusted operation on the customer's network. You must add those to the reader.

At this time, Resonate supports adding new CA certificates to readers and automatically handles the certificates securing the reader-to-Resonate management connection. However, it does not yet support managing other reader endpoint (client or server) certificates. For now, you must install them manually, using the reader's built-in web interface or ZIoT APIs. See the instructions for your specific reader.

## Installing a CA Certificate

After onboarding, new readers upload information about all of their existing CA certificates to Resonate RFID Reader Management, so they can be shown on the **Infrastructure > Devices > Certificates** page. The **Certificates** page also allows you to upload new CA certificates to send to readers. This is most often used to upgrade trust from self-signed to enterprise-signed certificates.



**NOTE:** Only PEM-formatted certificate files are supported.

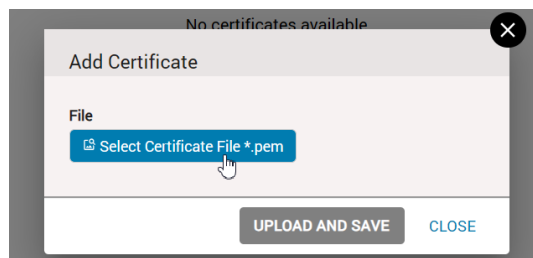
1. Navigate to the **Infrastructure > Devices** page.
2. Click **Certificates**.

The **Certificates** page opens, displaying existing CA certificates and allowing you to add new CA certificates.

3. Click **+ Add**.




4. Click **Select Certificate File**.



5. Navigate to your CA certificate file and click **Open**.  
A .pem file is required.
6. Click **UPLOAD AND SAVE** to upload the CA certificate.

## Digital Certificates

Resonate RFID Reader Management saves the CA certificate on its server, installs it on all the managed RFID readers, and lists it on the **Certificates** page.

<div>  <div>Infrastructure Users admin@customer.com</div> </div>				
<div> <div>Infrastructure / Devices / Certificates</div> <div>Refresh 135 Rows + Add</div> </div>				
Serial Number	Subject	Valid From	Valid To	Status
2a:38:a4:1c:96:0a:04:de:42:b2:28:a5:0b:e8:34:98:02	cn=GlobalSign,o=GlobalSign,ou=GlobalSign ECC Root CA - R4	11/12/12, 4:00:00 PM	1/18/38, 7:14:07 PM	ACTIVE
74:97:25:8a:c7:3f:7a:54	cn=AffirmTrust Premium ECC,o=AffirmTrust,c=US	1/29/10, 6:20:24 AM	12/31/40, 6:20:24 AM	ACTIVE
68:4a:58:70:80:6b:f0:8f:02:fa:f6:de:e8:b0:90:90	cn=CA WoSign ECC Root,o=WoSign CA Limited,c=CN	11/7/14, 4:58:58 PM	11/7/44, 4:58:58 PM	ACTIVE
6e:47:a9:c8:8b:94:b6:e8:bb:3b:2a:d8:a2:b2:c1:99	cn=GTS Root R4,o=Google Trust Services LLC,c=US	6/21/16, 5:00:00 PM	6/21/36, 5:00:00 PM	ACTIVE
6e:47:a9:c7:6c:a9:73:24:40:89:0f:03:55:dd:8d:1d	cn=GTS Root R3,o=Google Trust Services LLC,c=US	6/21/16, 5:00:00 PM	6/21/36, 5:00:00 PM	ACTIVE
60:59:49:e0:26:2e:bb:55:f9:0a:77:8a:71:f9:4a:d8:6c	cn=GlobalSign,o=GlobalSign,ou=GlobalSign ECC Root CA - R5	11/12/12, 4:00:00 PM	1/18/38, 7:14:07 PM	ACTIVE
3c:91:31:cb:1f:f6:d0:1b:0e:9a:b8:d0:44:bf:12:be	o=VeriSign, Inc.,ou=Class 3 Public Primary Certification Authority,c=US	1/28/96, 4:00:00 PM	8/2/28, 4:59:59 PM	ACTIVE
3f:69:1e:81:9c:f0:9a:4a:f3:73:ff:b9:48:a2:e4:dd	o=VeriSign, Inc.,ou=Class 1 Public Primary Certification Authority,c=US	1/28/96, 4:00:00 PM	8/2/28, 4:59:59 PM	ACTIVE
70:ba:e4:1d:10:d9:29:34:b6:38:ca:7b:03:cc:ba:bf	o=VeriSign, Inc.,ou=Class 3 Public Primary Certification Authority,c=US	1/28/96, 4:00:00 PM	8/1/28, 4:59:59 PM	ACTIVE
05:55:56:bc:f2:5e:a4:35:35:c3:a4:0f:d5:ab:45:72	cn=DigiCert Global Root G3,o=DigiCert Inc,ou=www.digicert.com,c=US	8/1/13, 5:00:00 AM	1/15/38, 4:00:00 AM	ACTIVE
0b:a1:5a:fa:1d:df:a0:b5:49:44:af:cd:24:a0:6c:ec	cn=DigiCert Assured ID Root G3,o=DigiCert Inc,ou=www.digicert.com,c=US	8/1/13, 5:00:00 AM	1/15/38, 4:00:00 AM	ACTIVE
35:fc:26:5c:d9:84:4f:c9:3d:26:3d:57:9b:ae:d7:56	cn=thawte Primary Root CA - G2,o=thawte, Inc.,ou=(c) 2007 thawte, Inc. - For authorized use only,c=US	11/4/07, 4:00:00 PM	1/18/38, 3:59:59 PM	ACTIVE
1f:47:af:aa:62:00:70:50:54:4c:01:9e:9b:63:99:2a	cn=COMODO ECC Certification Authority,o=COMODO CA Limited,c=GBJ=Salford,st=Greater Manchester	3/5/08, 4:00:00 PM	1/18/38, 3:59:59 PM	ACTIVE
5c:8b:99:c5:5a:94:c5:d2:71:56:de:cd:89:80:cc:26	cn=USERTrust ECC Certification Authority,o=The USERTRUST Network,c=USJ=Jersey City,st=New Jersey	1/31/10, 4:00:00 PM	1/18/38, 3:59:59 PM	ACTIVE
3c:b2:f4:48:0a:00:e2:fe:eb:24:3b:5e:60:3e:c3:6b	cn=GeoTrust Primary Certification Authority - G2,o=GeoTrust Inc.,ou=(c) 2007 GeoTrust Inc. - For	11/4/07, 4:00:00 PM	1/18/38, 3:59:59 PM	ACTIVE
00:a6:8b:79:29:00:00:00:00:50:d0:91:f9	cn=Entrust Root Certification Authority - EC1,o=Entrust, Inc.,ou=See www.entrust.net/legal-terms,c=US	12/18/12, 7:25:36 AM	12/18/37, 7:55:36 AM	ACTIVE
4c:c7:ea:aa:98:3e:71:d3:93:10:f8:3d:3a:89:91:92	o=VeriSign, Inc.,ou=Class 1 Public Primary Certification Authority - G2,c=US	5/17/98, 5:00:00 PM	8/1/28, 4:59:59 PM	ACTIVE
7d:d9:fe:07:cf:a8:1e:b7:10:79:67:fb:a7:89:34:c6	o=VeriSign, Inc.,ou=Class 3 Public Primary Certification Authority - G2,c=US	5/17/98, 5:00:00 PM	8/1/28, 4:59:59 PM	ACTIVE

# Alerting Targets

This section describes how to send Resonate alerts to targets via email or to OpsRamp.

## Alerting Targets Overview

Besides viewing reader alerts in the Resonate RFID Reader Management web interface, you can configure Resonate to send reader and/or server alerts to targets via email or webhooks. Typical targets include your system administrator and/or your case monitoring application (for example, OpsRamp or ServiceNow). If you are using Zebra's monitoring service, configure Resonate to send alerts to Zebra's OpsRamp instance, providing real-time visibility and insights into performance and operational status.

Resonate RFID Reader Management includes a comprehensive alerting system that you can configure to send notifications to various targets. The `add-alerting-target.sh` script provided in the installation directory allows you to easily configure multiple alerting targets.

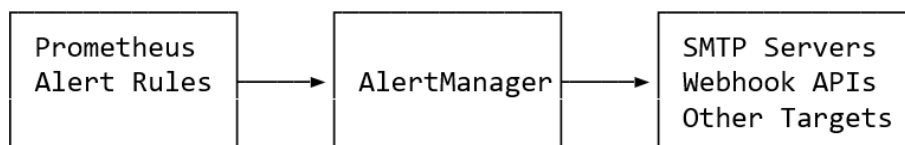
The alerting system in Resonate is built on Prometheus AlertManager, which enables sophisticated routing, grouping, and notification management. AlertManager can send notifications to targets via email (SMTP) or webhook endpoints.

## How Alerting Works

The alerting system in Resonate is built on Prometheus AlertManager, which enables sophisticated routing, grouping, and notification management. You can configure the AlertManager to send notifications to targets via email (SMTP) or webhook endpoints.

It performs the following steps:

1. Alert generation. Prometheus evaluates alert rules against metrics and generates alerts.
2. Alert processing. AlertManager receives alerts from Prometheus.
3. Alert grouping. Similar alerts are grouped based on configurable labels.
4. Alert notification. Notifications are sent to configured targets (for example, SMTP and webhooks).



## Steps to Send Alerts to Targets

Steps to send alerts to targets are outlined below.

To perform these steps, access the [primary machine](#) of the Resonate server (running Linux).

1. Run the following command to switch to the user `trif-user` account:

```
sudo su - trif-user
```

The home directory of the user `trif-user` should contain the `add-alerting-target.sh` and `trifecta.prometheusrules.yaml` scripts<sup>3</sup>.

2. Run a command similar to the following to start sending alerts to the target:

```
./add-alerting-target.sh --type webhook --webhook-url <URL> --name <LABEL FOR ALERTING TARGET>
```

For examples that show how to run the `add-alerting-target.sh` script in different scenarios, see [add-alerting-target.sh Usage Examples](#) on page 93 and [add-alerting-target.sh Advanced Usage Information and Examples](#) on page 95.

3. Verify that `add-alerting-target.sh` configured AlertManager correctly.

For information, refer to [Validating the Alert Configuration](#) on page 98.

When alerts happen, they are now also sent to the target, provided that they meet the specified requirements.

## Available Alerts

Resonate can report both Resonate server alerts and reader alerts.

### Resonate Server Alerts

Resonate can report the following server alert to a target via email or webhooks, if you configure Resonate appropriately; for information, refer to [Alerting Targets](#) on page 87. This type of alert is not reported in the Resonate RFID Reader Management web interface

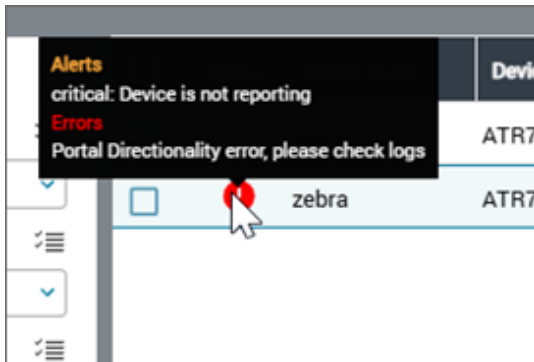
Alert Type	Message
Container Down	Resonate application failure. <i>Container_name</i> is down.

### Reader Alerts

Resonate can report the following alerts in the **Alerts** column of the **Devices** grid (**Infrastructure** > **Devices**). Hover over the notification icon to see the message:

<sup>3</sup> In Resonate 2.0, this is located in `opsramp.zip`, which is distributed alongside the `resonate-<VERSION>.tar.gz` installation file. Unzip this file and copy it to the home directory of `trif-user`.



**Figure 23** Reader Alerts

You can also configure Resonate to send these alerts to a target via email or webhooks; for information, refer to [Alerting Targets](#) on page 87 .

**Table 17** Alert Types

Alert Type	Message
Device Down	Device <i>Dev_ID</i> is not reporting.
Device temperature	Device <i>Dev_ID</i> reporting a temperature of <i>value</i> .
Radio failure	Radio failure, device <i>Dev_ID</i> reporting a temperature of <i>value</i> .
Command errors	Device <i>Dev_ID</i> has <i>N</i> command error(s).
DNS errors	Device <i>Dev_ID</i> has <i>N</i> DNS error(s).
Failed power negotiation	Device <i>Dev_ID</i> reporting power status: Failed.
Ongoing power negotiation	Device <i>Dev_ID</i> reporting power status: Ongoing.
Detached antenna	Device <i>Dev_ID</i> reporting <i>N</i> detached antenna(s).

*Dev\_ID* is a 3-part identifier: Make\_Model\_SerialNumber (for example, zebra\_fx9600\_123456). *N* is the number of items.

## add-alerting-target.sh

The `add-alerting-target.sh` script allows you to configure Resonate to send alerts to one or more targets via emails (SMTP) or webhooks. It creates `AlertManagerConfig` custom resources (CRs) that configure how `AlertManager` routes and delivers notifications.

### Command Syntax

```
./add-alerting-target.sh [options]
```

### Common Options

The following options are common to all alerting target types:

## Alerting Targets

Option	Description
<code>--help</code>	Display help message.
<code>--type &lt;smtp webhook&gt;</code>	Type of alerting target. Required: Yes
<code>--name &lt;name&gt;</code>	Name for the alerting target. Essentially, this is a user-assigned label for the target. It must be unique. Required: Yes
<code>--alertgroup &lt;device service both&gt;</code>	Filter alerts by alert group. Default: both
<code>--group-by &lt;label1,label2,...&gt;</code>	Labels by which to group alerts. See below for the list of possible labels. For example:  <code>--group-by app,severity</code> Default: ... (all labels)
<code>--group-wait &lt;duration&gt;</code>	How long to wait before sending the initial notification. Default: 30s
<code>--group-interval &lt;duration&gt;</code>	How long to wait before sending an updated notification. Default: 5m
<code>--repeat-interval &lt;duration&gt;</code>	How long to wait before repeating the last notification. Default: 4h
<code>--matchers</code> '<matcher1,matcher2,matcherN>'	Alert label matchers in the format "name=value" or "name!=value". There can be multiple matchers delimited by commas.

### Alert Grouping Options

The `--alertgroup` parameter lets you filter alerts based on their group:

- `device`: Only receive reader-related alerts.
- `service`: Only receive service-related alerts.
- `both`: Receive both device and service alerts, but exclude alerts with a different or missing alertgroup (default).

### Matchers and Filtering

The `--matchers` parameter allows for sophisticated filtering of alerts based on their labels. You can specify multiple matchers, which are applied as AND conditions.

- **Matcher Syntax**

Enter matchers using the following syntax. Multiple matchers can be comma-separated (for example, `severity=critical,instance=~prod.*`).

Syntax	Example	Description
<code>labelname=value</code>	<code>app=Device</code>	Exact match.
<code>labelname!=value</code>	<code>app!=Device</code>	Negative match (not match).
<code>labelname=~value</code>	<code>app=~Dev</code> <code>'app=~Dev,metric=~Power'</code>	Regex match (golang implementation of regex). The first example, matches reader alerts. The second example matches reader power alerts.
<code>labelname!~value</code>	<code>app!~Dev</code> <code>'app!~Dev,metric!~Power'</code>	Regex not match (golang implementation of regex). The first example, matches anything except reader alerts. The second example matches anything except reader power alerts.

- **Common Label Names**

Alerts in Resonate include these labels that you can filter on:

Label	Description
<code>metric</code>	The name of the alert.
<code>app</code>	The type of entity that threw the alert. Possible values: <ul style="list-style-type: none"> <li>• <code>Device</code></li> <li>• <i>Container Name</i></li> </ul>
<code>alertgroup</code>	The category of alert. Possible values: <ul style="list-style-type: none"> <li>• <code>device</code></li> <li>• <code>service</code></li> </ul>
<code>description</code>	Brief description of the alert.
<code>resource</code>	Unique identifier that threw the alert. Possible values: <ul style="list-style-type: none"> <li>• <i>Deviceld</i></li> <li>• <i>Container Name</i></li> </ul>

## Alerting Targets

Label	Description
severity	Severity of the alert. Possible values: <ul style="list-style-type: none"><li>critical</li><li>warning</li></ul>

### Target-Specific Options

#### SMTP (Email) Options

Option	Description
<code>--smtp-from &lt;email&gt;</code>	Sender email address. Required: Yes
<code>--smtp-to &lt;email&gt;</code>	Recipient email address. You can only specify one address. To send to multiple addresses, repeat the <code>add-alerting-target</code> command using a different address and name. Required: Yes
<code>--smtp-smarthost &lt;host:port&gt;</code>	SMTP server host and port. Required: Yes
<code>--smtp-auth-username &lt;username&gt;</code>	SMTP authentication username.
<code>--smtp-auth-password &lt;password&gt;</code>	SMTP authentication password.
<code>--smtp-require-tls &lt;true false&gt;</code>	Whether to require TLS. Default: true
<code>--smtp-hello &lt;hostname&gt;</code>	The hostname to identify to the SMTP server.

#### Webhook Options

Option	Description
<code>--webhook-url &lt;url&gt;</code>	The URL to which to send HTTP POST requests. Required: Yes
<code>--webhook-max-alerts &lt;number&gt;</code>	Maximum number of alerts to be sent per webhook message. Default: 0 (all alerts)
<code>--webhook-authorization-type &lt;basic bearer none&gt;</code>	Type of authorization to use for webhook requests. none performs no authorization. Default: none

Option	Description
<code>--webhook-basic-auth-username &lt;username&gt;</code>	Username for basic auth authentication. Required: With basic auth type.
<code>--webhook-basic-auth-password &lt;password&gt;</code>	Password for basic auth authentication type. Required: With basic auth type.
<code>--webhook-bearer-token &lt;token&gt;</code>	Bearer token for authorization. Required: With bearer auth type

## add-alerting-target.sh Usage Examples

The following examples show how to run the `add-alerting-target.sh` script in different scenarios.

### Basic Email Configuration

```
./add-alerting-target.sh \
  --type smtp \
  --name email-alerts \
  --smtp-from alerts@company.com \
  --smtp-to admin@company.com \
  --smtp-smarthost smtp.company.com:25
```

### Secure Email with Authentication

```
./add-alerting-target.sh \
  --type smtp \
  --name secure-email-alerts \
  --smtp-from alerts@company.com \
  --smtp-to admin@company.com \
  --smtp-smarthost smtp.company.com:587 \
  --smtp-auth-username your_username \
  --smtp-auth-password your_password \
  --smtp-require-tls true
```

### Webhook for a Team Chat Application

```
./add-alerting-target.sh \
  --type webhook \
  --name teams-alerts \
  --webhook-url https://teams-webhook-url.example.com
```

### Device-Only Alerts to Email

```
./add-alerting-target.sh \
  --type smtp \
```

```
--name device-email-alerts \  
--alertgroup device \  
--smtp-from alerts@company.com \  
--smtp-to device-team@company.com \  
--smtp-smarthost smtp.company.com:25
```

### Service-Only Alerts to Webhook

```
./add-alerting-target.sh \  
--type webhook \  
--name service-webhook-alerts \  
--alertgroup service \  
--webhook-url https://service-alerts-webhook.example.com
```

### Critical Alerts Only

```
./add-alerting-target.sh \  
--type webhook \  
--name critical-alerts \  
--matchers "severity=critical" \  
--webhook-url https://critical-alerts-webhook.example.com
```

### Webhook with Basic Authentication

```
./add-alerting-target.sh \  
--type webhook \  
--name secure-webhook-alerts \  
--webhook-url https://webhook.example.com/alerts \  
--webhook-authorization-type basic \  
--webhook-basic-auth-username api_user \  
--webhook-basic-auth-password s3cr3t_p@ssw0rd
```

### Webhook with Bearer Token Authentication

```
./add-alerting-target.sh \  
--type webhook \  
--name token-webhook-alerts \  
--webhook-url https://api.alertservice.com/webhook \  
--webhook-authorization-type bearer \  
--webhook-bearer-token  
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIn0
```

### Secure Webhook with Custom Alert Grouping

```
./add-alerting-target.sh \  
--type webhook \  
--name secure-custom-webhook \  
--webhook-url https://alerts-api.example.org/v1/webhooks \  
--webhook-authorization-type bearer \  

```

```
--webhook-bearer-token your_api_token_here \  
--group-by severity,instance,alertname \  
--group-wait 15s \  
--group-interval 2m
```

### Multiple Alert Groups

You can configure multiple alert targets with different filters:

```
# Device alerts to the device team  
./add-alerting-target.sh \  
--type webhook \  
--name device-team-alerts \  
--alertgroup device \  
--webhook-url https://device-team-webhook.example.com
```

```
# Service alerts to the service team  
./add-alerting-target.sh \  
--type webhook \  
--name service-team-alerts \  
--alertgroup service \  
--webhook-url https://service-team-webhook.example.com
```

```
# Critical alerts to everyone  
./add-alerting-target.sh \  
--type smtp \  
--name critical-email-alerts \  
--matchers "severity=critical" \  
--smtp-from alerts@company.com \  
--smtp-to all-teams@company.com \  
--smtp-smarthost smtp.company.com:25
```

## add-alerting-target.sh Advanced Usage Information and Examples

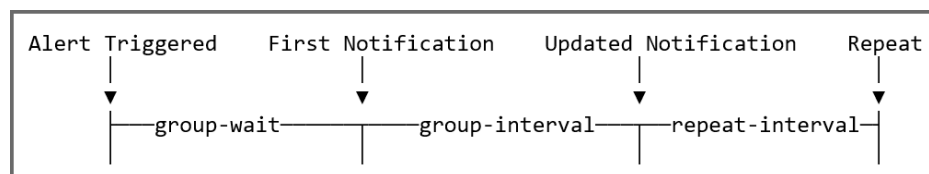
The following explains some advanced `add-alerting-target.sh` usage information and some examples that show how to run the script in different advanced scenarios.

For more information, refer to the [Prometheus AlertManager documentation](#).

### Alert Timing Explained

AlertManager uses several timing parameters to control when and how often notifications are sent:

**Figure 24** Timing diagram



## Alerting Targets

Parameter	Description	When to Adjust
<code>--group-wait</code>	Initial delay before sending first notification.	Decrease for more urgent alerts. Increase to collect more alerts in a group.
<code>--group-interval</code>	Delay before sending updated notifications for the same group.	Decrease for frequently changing alerts. Increase to reduce notification frequency.
<code>--repeat-interval</code>	Delay before resending an unresolved alert.	Decrease for critical alerts that need attention. Increase to reduce alert fatigue.

### Custom Grouping

Group alerts by specific labels to combine related alerts into a single notification:

```
./add-alerting-target.sh \  
  --type webhook \  
  --name grouped-alerts \  
  --group-by severity,instance \  
  --webhook-url https://webhook.example.com
```

### Multiple Matchers

You can specify multiple matchers to filter alerts:

```
./add-alerting-target.sh \  
  --type webhook \  
  --name specific-alerts \  
  --matchers "severity=critical,instance=~prod.*,alertname!=TestAlert" \  
  --webhook-url https://webhook.example.com
```

### Customizing Alert Timing

Adjust how alerts are grouped and repeated:

```
./add-alerting-target.sh \  
  --type webhook \  
  --name custom-timing-alerts \  
  --group-wait 10s \  
  --group-interval 1m \  
  --repeat-interval 30m \  
  --webhook-url https://webhook.example.com
```



## Sending Alerts to Zebra's OpsRamp instance

If you are using Zebra's monitoring service, use the steps below to configure Resonate to send alerts to Zebra's OpsRamp instance.

Before configuring, you must:

- Locate the file `trifecta.prometheusrules.yaml` packaged with the `add-alerting-target.sh` shell script<sup>4</sup>.
- Switch to `trif-user` with the command:

```
sudo su - trif-user
```

1. Copy the `add-alerting-target.sh`, and `trifecta.prometheusrules.yaml` files over to the Resonate server.

With `scp`, that would be:

```
scp ./add-alerting-target.sh ./trifecta.prometheusrules.yaml
```

2. Edit the file `trifecta.prometheusrules.yaml` so that the customer label (defined on each alert in the file) is the correct value:

- You could do this with a `sed`:

```
sed -i 's@customer: .*$@customer: "Your Customer ID"@'
```

- Alternatively, you can do this manually with a text editor of your choice.

3. Install the change with the command:

```
kubectl apply -f <path/to/your/trifecta.prometheusrules.yaml>
```

4. Add OpsRamp as an alerting target with the command:

```
./add-alerting-target.sh --type webhook --webhook-url <URL> --name opsrampp
```



**NOTE:** Your Zebra representative should provide you with the webhook URL to pass to this command. When setting up multiple alerts to OpsRamp, pass different names to `--name` for each different alert configuration.

Resonate is now configured to send alerts to OpsRamp.

<sup>4</sup> In Resonate 2.0, this is located in `opsramp.zip`, which is distributed alongside the `resonate-<VERSION>.tar.gz` installation file. Unzip this file and copy it to the home directory of `trif-user`.

## Validating the Alert Configuration

After running the `add-alerting-target.sh` script, validate that it configured AlertManager correctly.

1. Check the AlertManagerConfig resources:

```
kubectl get alertmanagerconfig -n monitoring
```

2. Viewing the details of a specific configuration:

```
kubectl describe alertmanagerconfig -n monitoring
```

For troubleshooting information, refer to [Troubleshooting the AlertManager Configuration](#) on page 103 and [AlertManager Diagnostic Commands](#) on page 104.

# Troubleshooting Application and RFID Reader Issues

This section describes solutions to possible application issues and how to establish the root cause for RFID reader issues.

## Resolving Application Issues

This section provides troubleshooting solutions for potential application problems.

**Table 18** Troubleshooting potential application problems

Problem	Potential Cause	Solution
When launching the web interface (that is, when attempting to connect to <code>http(s)://&lt;server_IP_or_Name&gt;</code> ), the following message is displayed: Cannot reach/connect to web page (or a similar message).	<ul style="list-style-type: none"><li>No network connectivity between the client machine and the Resonate server.</li><li>Firewall or router blocking port 443 between the client machine and Resonate RFID Reader Management server.</li></ul>	Verify that there is network connectivity between the client machine and the Resonate server.
When entering login credentials in the login page of the web interface, the following message is displayed: Incorrect username or password.	Incorrect username or password entered.	<p>Verify the user has the correct username and password.</p> <p>Have the admin user reset the user password. This is done in the <b>Users</b> menu of the web interface.</p> <p>Have the admin user delete the user and add it back. This is done in the <b>Users</b> menu of the web interface. Then, the user can log in and change the password in the login account menu (rightmost link in the menu bar).</p>

**Table 18** Troubleshooting potential application problems (Continued)

Problem	Potential Cause	Solution
When trying to load a map image (.wmf file) in <b>Site Manager</b> , the following message is displayed 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 a WMF file generated using AutoCAD. When opening the project file in AutoCAD, if prompted, select the <b>Do not show proxy graphics</b> option. Then, select to export as a WMF file.

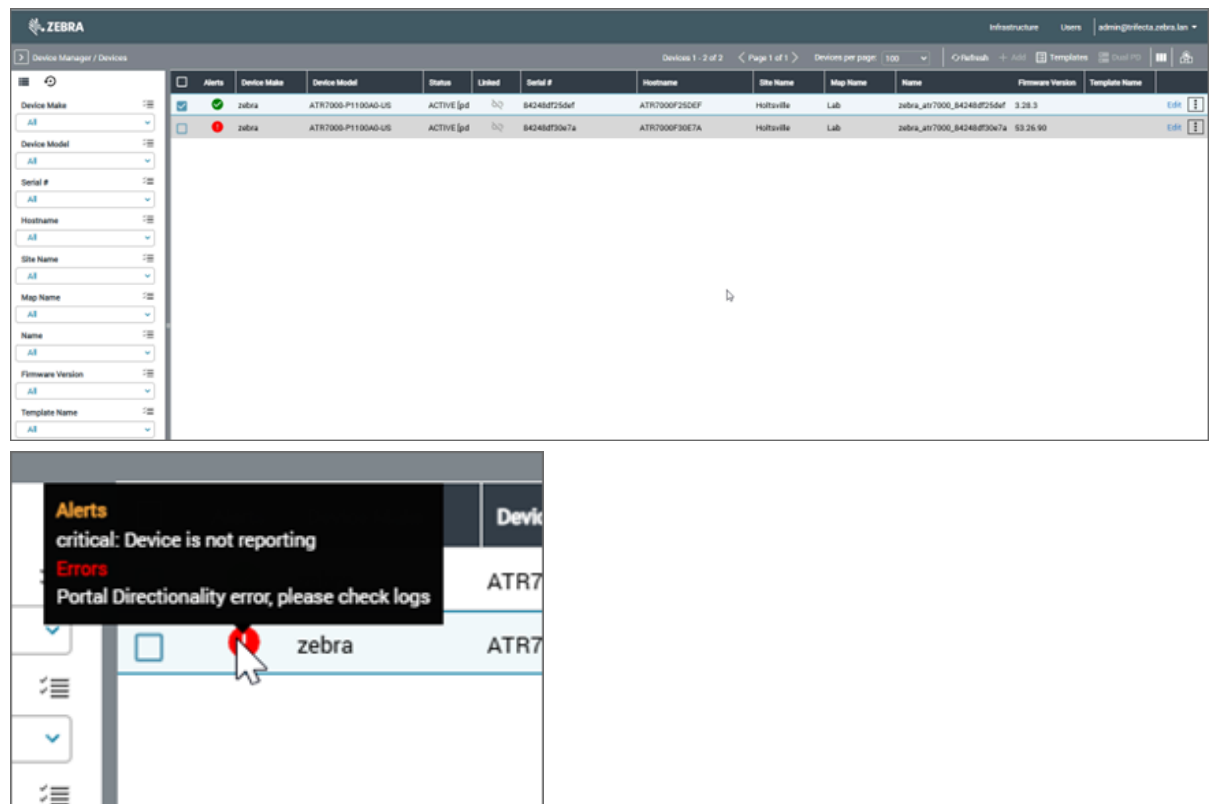
## Determining the Root Cause of RFID Reader Issues

The Resonate RFID Reader Management web interface displays notifications on the **Infrastructure > Devices** page to provide information on RFID reader health. You can also access the RFID readers' logs from this page. Use this information to know the health of your readers, and if there is an issue, to help you determine the root cause of the issue, possibly remediating the issue before escalating it to Zebra support.





### Troubleshooting RFID Reader Issues

If an RFID reader is experiencing an issue, the device grid displays warning and/or error alerts in the **Alerts** column, as shown below.


**Figure 25** Devices Page with an Alert



The following are the possible notification icons:

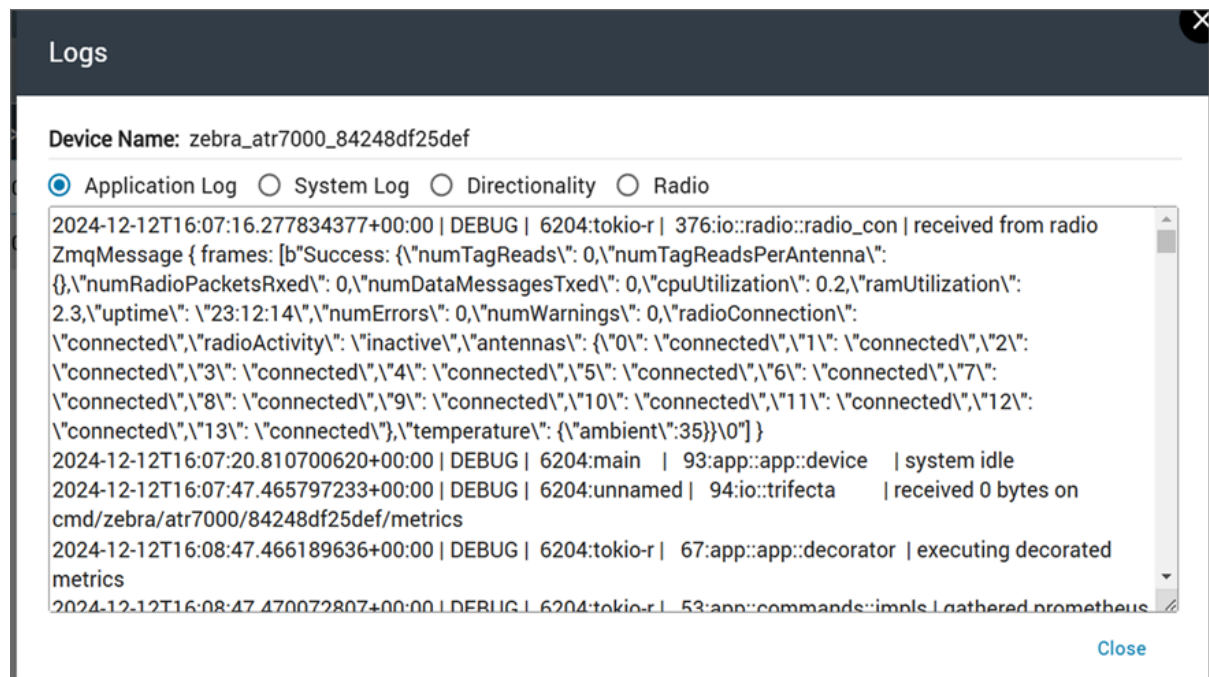
Device State	Icon	Description
Healthy		The RFID reader is reporting no issues.
Warning		The RFID reader is reading and transmitting tag read data, but the reader is experiencing an issue (for example, it is starting to disconnect or overheat).
Critical		The RFID reader is reading and transmitting tag read data, but the reader is experiencing an issue that is more serious than one that warrants just a warning (for example, it is overheating). You might also obtain this alert if the reader is not responding, so its status is unknown.
Error		The RFID reader is experiencing a real-time, immediate problem (for example, after you send it a command, something fails).

Hover over the icon to see more details about the alert or error; refer to [Available Alerts](#) on page 88 on how to resolve the issue.

For more information on an error, view the RFID reader's logs; to access the logs, select  **Device Settings > Logs** at the far right of the reader's row. The **Logs** dialog opens. After a few seconds, the reader's different logs load. You should typically start with the Application log for a general indication of what is happening with the Resonate Agent; then, click on one of the other logs based on your specific error.

- **Application Log:** Records general events and errors related to Resonate Agent.
- **System Log:** Records events and errors related to transport or management.
- **Directionality Log** (if applicable): Records events and errors related to the portal or directionality.
- **Radio Log:** Records events related to the radio.

**Figure 26** Example Application Log



After viewing the logs accessible from the **Devices** page, you should then look at the reader adapter logs on the Resonate server. To do this, log in to a cluster node as `trif-user`, and retrieve the name of the device manager pods using the command:

```
kubectl get pods -n zebra-reader-management | grep iotc-adapter-fixreader
```

This displays information about the reader adapter pod. Ensure the pod is in a `Running` state.

Retrieve the detailed status of the pod by running:

```
kubectl describe pods -n zebra-reader-management <pod name from above>
```

Retrieve the logs of the pod by running:

```
kubectl logs -n zebra-reader-management <pod name from above>
```

The Resonate RFID Reader Management Software Installation Guide provides additional commands to further troubleshoot issues. If you need to escalate the issue to another team, the best practice is to include the application logs and other device logs (if applicable), along with the reader adapter log.

## Troubleshooting Issues between Resonate and RFID Readers

Follow similar steps as for device errors.

Check for specific errors in the application logs of the device.

Attempt to correlate these errors with the reader adapter log.

If no issues are found in the reader adapter log, retrieve the name of the `mqtt` pod using the command:

```
kubectl get pods -n zebra-reader-management | grep mqtt
```

Retrieve the logs of the mqtt pod by running:

```
kubectl logs -n zebra-reader-management <pod name from above>
```

## Troubleshooting the AlertManager Configuration

This section describes troubleshooting the AlertManager configuration after using `add-alerting-target.sh`.

**Table 19** Troubleshooting Configured Alerts

Problem	Cause	Solution
No alerts being received	AlertManager is not running	Check:  <pre>kubectl get pods -n monitoring   grep alertmanager</pre>
	Incorrect SMTP server	Verify the SMTP server address and port.
	Network connectivity	Ensure the cluster can reach the SMTP server or webhook endpoint.
	Authorization failure	Check credentials and ensure secrets were created properly.
Duplicate alerts	Multiple similar configurations	Check existing configurations with:  <pre>kubectl get alertmanagerconfig -n monitoring</pre>
Alerts missing	Incorrect matchers	Review matchers to ensure they match expected alerts.
	--alertgroup filter too restrictive	Try <code>--alertgroup both</code> to see all alerts.

## AlertManager Diagnostic Commands

Use the following diagnostic commands when troubleshooting the AlertManager configuration after using `add-alerting-target.sh`.

**Table 20** Check AlertManager Status

Command	Description
<code>kubectl get pods -n monitoring   grep alertmanager</code>	Checks if AlertManager is running.
<code>kubectl logs -n monitoring -l app=alertmanager</code>	Checks AlertManager logs.

**Table 21** Examine Configuration

Command	Description
<code>kubectl get alertmanagerconfig -n monitoring</code>	Lists all alert configs.
<code>kubectl describe alertmanagerconfig -n monitoring</code>	Checks details of a specific configuration.
<code>kubectl get secrets -n monitoring   grep alertmanager</code>	Checks if secrets were created properly.



# Disaster Recovery

This section provides information about backups and disaster recovery for Resonate RFID Reader Management.

## Recovery Overview

Resonate RFID Reader Management supports fault tolerance to ensure Resonate can recover automatically without human intervention in the event of a software failure, without the expectation of continuous uptime. It also supports being distributed across multiple machines (nodes) to recover in case a machine goes down. However, in the case of a single-node configuration, you are responsible for backup and restore.

Resonate uses several internal databases for persistent settings data and configuration of Resonate. These are typically databases internal to a containerized service and not some large, centralized database holding everything. Transient data, or data that is expected to change soon anyway, is generally held in one or more of the various message queues to support quick resumption of operation in the event of containers going offline and coming online due to restart, scale up, or other reasons.

Most of the extra reliability built into Resonate RFID Reader Management focuses on making the containers automatically recover instantly and on using Kubernetes for software, data, and state replication across multiple high availability (HA) nodes. In general, however, Resonate RFID Reader Management is not set up to take periodic snapshots of the state and save extra copies outside Kubernetes and the high-availability nodes. Therefore, when installed in a single-node configuration, it is highly recommended that administrators use external tools to set up regular copy backups of either full disk or individual volumes, and that those backups be written to external devices off the main server node.

Keep in mind that Resonate does not do data collection of RFID tag read data, so Resonate does not have any tag data to backup/recover.

## Recovery Setup

The Resonate RFID Reader Management should be installed to ensure that recovery is simple.

### DNS Alias for Recovery

Zebra recommends deploying using a DNS alias, since this allows a single point of access to the [system](#). If one node fails, the DNS alias can be updated to point to another node, ensuring minimal downtime. Some DNS providers allow for automatic failover, which can further enhance reliability.

In the event of a catastrophic failure of the cluster (or single node), the DNS alias can be updated to point to a new cluster or node, allowing for quick recovery. This setup ensures that the system remains accessible even in the face of significant issues.

**Additional Disks**

If you choose to use one of the in-cluster backup solutions, you should have another disk present on each node, so that backups can be stored on their own logical device, helping to prevent the risk of both the primary data and the backups being lost in the event of a disk failure.

**Setting Up Database Backups**

Currently, database backups are handled in multi-node deployments through the presence of database replicas running simultaneously on each node. This ensures that if one node fails, the data is still available on another node. In the event that you need database backups for a single-node deployment, or if you want to have additional backups for your multi-node deployment, you can set up periodic database dumps using the postgres system that Resonate RFID Reader Management uses.

**CNPG Backups using Barman**

Resonate RFID Reader Management uses Cloudnative Postgres (CNPG), which has [its own documentation on setting up database backups](#).

CNPG allows you to configure your cluster to automatically upload backups to one of various cloud storage providers, including AWS S3, Google Cloud Storage, and Azure Blob Storage. This can be set up to run at regular intervals, ensuring that you always have a recent backup available.

Configure this according to [CNPG's documentation](#), by adding backup rules to the following files:

- manifests/base/postgres.yml (For application data, configuration of readers, etc.)
- manifests/base/keycloak.yml (For user and authentication data)

Add a backup section under the `spec` of the kind: Cluster objects in both files.

Also, create a secret with the relevant credentials for your chosen cloud provider, and reference this secret in the `barmanObjectStore` section of the backup configuration.

Set up a schedule for the backups by creating a `ScheduledBackup` object in those files, similar to the following:

```
--- # For backing up the application database
apiVersion: postgresql.cnpg.io/v1
kind: ScheduledBackup
metadata:
  name: trifecta-backup
  namespace: zebra-reader-management
spec:
  cluster: trifecta-postgres
  schedule: "0 0 2 * * *" # Daily at 2 AM

--- # For backing up the Keycloak database
apiVersion: postgresql.cnpg.io/v1
kind: ScheduledBackup
metadata:
  name: keycloak-backup
  namespace: zebra-reader-management
spec:
  cluster: keycloak-db
  schedule: "0 0 3 * * *" # Daily at 3 AM
```

After you have configured it according to your needs, apply the changes by running the install script again, or by applying the manifests directly using:

```
kubectl apply -k deploy
```

### Single-Node Database Backups

For single-node deployments, use the `pg_dumpall` command to create a backup of your database. Schedule this command using `corn jobs` or similar scheduling tools to ensure regular backups:

```
kubectl exec -i trifecta-postgres-1 -n zebra-reader-management -- pg_dumpall  
| gzip > /path/to/backup/trifecta-$(date +%Y%m%d%H%M%S).sql.gz  
  
kubectl exec -i keycloak-db-1 -n zebra-reader-management -- pg_dumpall | gzip  
> /path/to/backup/keycloak-$(date +%Y%m%d%H%M%S).sql.gz
```

### Multi-Node Database Backups

The single-node backup procedure also works for a multi-node deployment, although you might need to identify the correct pod names for the PostgreSQL instances. You can find the pod names using:

```
kubectl get pods -n zebra-reader-management
```

This lists all pods in the `zebra-reader-management` namespace, allowing you to identify the PostgreSQL pods for both the application and Keycloak databases. They should have names such as `trifecta-postgres-<N>` and `keycloak-db-<N>`.

After you have identified the correct pod names, run the `pg_dumpall` commands as follows to create backups of both databases:

```
kubectl exec -i trifecta-postgres-1 -n zebra-reader-management -- pg_dumpall  
| gzip > /path/to/backup/trifecta-$(date +%Y%m%d%H%M%S).sql.gz  
  
kubectl exec -i keycloak-db-1 -n zebra-reader-management -- pg_dumpall | gzip  
> /path/to/backup/keycloak-$(date +%Y%m%d%H%M%S).sql.gz
```

### Recovering from Database Backups

For recovery, restore the database from the backup using the `psql` command:

```
zcat /path/to/backup/trifecta-YYYYMMDDHHMMSS.sql.gz | kubectl exec -i  
trifecta-postgres-1 -n zebra-reader-management -- psql  
  
zcat /path/to/backup/keycloak-YYYYMMDDHHMMSS.sql.gz | kubectl exec -i  
keycloak-db-1 -n zebra-reader-management -- psql
```

## Snapshot Backups

Snapshot backups are a crucial part of maintaining the integrity and availability of your data. They allow you to capture the state of your application and its data at a specific point in time, which can be invaluable for disaster recovery, testing, and development purposes.

### Snapshot Backups Overview

Snapshot backups involve creating a complete copy of your application's data and configuration at a specific moment. There are various tools and methods, depending on your deployment environment and the technologies you are using.

### Native Disk Backups

In a single-node installation, all application data is stored in the `/data` directory of your server. It should be located on its own disk partition to ensure that it is not affected by the operating system or application updates.

There are several ways to create backups of this data, depending on the tools at your disposal:

- Take a cloud snapshot of the disk that backs the `/data` directory.
- Use a tool such as `rsync` to copy the contents of the `/data` directory to another location, such as a remote server or a cloud storage service.
- Copy the raw disk, using a tool such as `dd` or `partclone`, to create a complete image of the disk.
- Use a backup tool that supports disk snapshots, such as `BorgBackup` or `Restic`, to create incremental backups of the `/data` directory.

### Remote Backups

In a multi-node installation, Rook is used for application data and ensures that data is replicated across nodes. However, it is still important to create backups of your data to protect against data loss.

There are a number of tools that you can use to back up or migrate application data, such as:

- [Velero](#): A tool for managing Kubernetes backups, which can be used to backup Rook volumes.
- [Rook's built-in snapshot capabilities](#): Rook supports taking snapshots of Ceph volumes, which can be used to create backups of your application data.

You can also use cloud or hypervisor tools to create snapshots of the underlying storage volumes used by Rook. This can be done using the cloud provider's snapshot capabilities or hypervisor tools like VMware's `vSphere` or OpenStack's `Cinder`.

### Snapshot Backups Overview

Snapshot backups involve creating a complete copy of your application's data and configuration at a specific moment. This can be done using various tools and methods, depending on your deployment environment and the technologies you are using.

### Native Disk Backups

In a single-node installation, all application data is stored in the `/data` directory of your server. It should be located on its own disk partition to ensure that it is not affected by the operating system or application updates.

There are several ways to create backups of this data, depending on the tools at your disposal:

- Take a cloud snapshot of the disk that backs the `/data` directory.

- Use a tool such as `rsync` to copy the contents of the `/data` directory to another location, such as a remote server or a cloud storage service.
- Copy the raw disk using a tool such as `dd` or `partclone`, to create a complete image of the disk.
- Use a backup tool that supports disk snapshots, such as BorgBackup or Restic, to create incremental backups of the `/data` directory.

### Remote Backups

In a multi-node installation, Rook is used for application data and will ensure that data is replicated across nodes. However, it is still important to create backups of your data to protect against data loss.

There are a number of tools that you can use to back up or migrate application data, such as:

- [Velero](#): A tool for managing Kubernetes backups, which can be used to backup Rook volumes.
- [Rook's built-in snapshot capabilities](#): Rook supports taking snapshots of Ceph volumes, which can be used to create backups of your application data.

You can also use cloud or hypervisor tools to create snapshots of the underlying storage volumes used by Rook. Use the cloud provider's snapshot capabilities or hypervisor tools, such as VMware's vSphere or OpenStack's Cinder.

## Recovery in the Event of a Disaster

Disaster recovery for Resonate RFID Reader Management will have differences and similarities depending on whether it is installed in a single-node or multi-node configuration. In the event of a disaster, such as a crashed drive or server node, the first step is to get a new node up and running; the second step is to ensure the readers are re-attached to the system at the new node.

### Replacing a Failed Resonate Node in a Multi-Node Configuration

When preparing to install the Resonate server on multiple nodes, one common way of deciding how many nodes are needed is to double the number of nodes required at a minimum to run the system, and then add one as a spare for a higher level of redundancy and fault tolerance. This configuration,  $2n+1$ , is considered a good level of redundancy in much of the commercial IT industry. It can withstand multiple component failures with near-zero downtime. In general, Resonate RFID Reader Management can manage up to 2,000 readers using the requirements described in the Resonate RFID Reader Management Software Installation Guide; this is the maximum that the standard Resonate license SKUs currently support. Therefore, a very reliable system can be run with  $2n+1$  nodes, where  $n$  is the number of nodes that can be down simultaneously. For example, to allow 1 node to be down at a given time, use 3 nodes. Increase  $n$  for additional redundancy with the current Resonate SKUs. In the future,  $n$  will also increase as additional nodes are added to support higher reader counts with future high-scalability Resonate license SKUs.

In the case of Resonate multi-node operations, if a disaster removes one node completely, the existing high-availability support will simply continue running with no loss of performance or data, but with no advanced redundancy or increased reliability. After a new node is in place and assigned to the Kubernetes High-Availability cluster, the node will automatically be recovered and become a part of the cluster, and data will be replicated to it. At this point, the redundancy and increased reliability are back in place.


### Replacing a Failed Resonate Node in a Single-Node Configuration


When configured to run as a single-node Resonate system, there is no additional redundancy or reliability over that of the base software and the computer it's running on. In this case, a catastrophic failure of the node can also be recovered by restoring the full backup onto a new node computer and restarting it. This naturally allows for a longer downtime than the HA multi-node configuration, but it is a very straightforward

task. In this case, one key issue will be to ensure that when readers re-attach, they can access the correct Resonate control and management data queues and service endpoint addresses. To facilitate this, it is recommended to use the same hostname and fully qualified domain name (FQDN) on the new node as was used on the node that experienced the disaster. This can be handled via DNS Alias, via common IT tools, or via manual reassignment. When complete, there will be a new node, just like the old node, ready to go.

### Ensuring Readers are Re-attached to the New Resonate Node

After ensuring your new node is up and running as described above, you must send a **Restart** command from Resonate RFID Reader Management to all the readers. The restart causes the on-reader Resonate Agent app to restart, which causes it to resend all the required information about the state and configuration of the reader to Resonate. This, in turn, repopulates any live queues lost during the previous disaster, the last of the Resonate data that needs to be recovered. The Restart command is a menu item

in the  **Device Settings** menu at the far right of the readers' row on the **Infrastructure > Devices** page.

It is also available as a multi-select action from the column header  **Device Settings** button, letting you restart Resonate Agent on up to 100 readers at a time.

# High Availability Operation

This section describes Resonate RFID Reader Management's support for fault tolerance and high availability.

## Fault Tolerance and High Availability

Resonate RFID Reader Management supports fault tolerance and high availability.

Fault tolerance ensures Resonate can recover automatically without human intervention in the event of a software failure, without the expectation of continuous uptime. This is built directly into the software, within each individual component or container. Fault tolerance is supported by running the Resonate containers with Kubernetes. If a component fails, it automatically restarts and picks up where it left off. Data queues are buffered to allow the recovering processes to continue without losing critical data. Fault tolerance is supported in both single-node and multi-node configurations.

High availability adds the ability to increase overall uptime by distributing the software operation across multiple hardware nodes. If a node has a catastrophic hardware failure, the overall system can continue to operate. Resonate must be installed in a multi-node configuration to support high availability.

When operating in high availability mode, the system ensures that the software and the data being processed are replicated across the multiple nodes. High availability coordination and replication require their own processing and networking, so some of the increased processing power from the additional nodes is used for that purpose. All the nodes share the data being processed, and replicate copies of the software and the databases. Nodes mostly run the same code, but some of the databases use a primary and secondary architecture. The software automatically ensures that one of the nodes is primary and the others are secondary.

In the event of a failure of a secondary node, the system continues to operate at reduced net reliability. In the event of a failure of the primary node, the system automatically negotiates which secondary node becomes the new primary, reconfigures it as necessary, and resumes operation. Operations other than database reads and writes, such as RFID reading, network data queueing, and algorithm processing, mostly continue while the database operation recovers. Depending on the specific failure (for example, power off, hard disk removal, or network disconnection), the recovery can take from no time up to a few minutes.

High availability mode requires multiple nodes and further requires an odd number of nodes. The Resonate RFID Reader Management Software Installation Guide describes how to set up a three (3) node system. It is possible to install a system using more nodes (for example, 5 or 7 or more) to get higher reliability and availability (but not higher capacity). If this is required, contact your Zebra salesperson, who can help you work up a special project and statement of work with Resonate product management and Professional Services.

Resonate is currently offered only for on-premises or customer cloud deployment. Resonate is only part of a system solution consisting of the customer's computers, network, and other solution software. Due to these factors, Zebra cannot offer a specific service level agreement (SLA) or predefined system uptime percentage. Zebra performs long-term testing and will provide updates on our observed reliability as and when possible.



