VERTIV.

Next Connect

User Guide

The information contained in this document is subject to change without notice and may not be suitable for all applications. While every precaution has been taken to ensure the accuracy and completeness of this document, Vertiv assumes no responsibility and disclaims all liability for damages result from use of this information or for any errors or omissions.

Refer to local regulations and building codes relating to the application, installation, and operation of this product. The consulting engineer, installer, and/or end user is responsible for compliance with all applicable laws and regulations relation to the application, installation, and operation of this product.

The products covered by this instruction manual are manufactured and/or sold by Vertiv. This document is the property of Vertiv and contains confidential and proprietary information owned by Vertiv. Any copying, use, or disclosure of it without the written permission of Vertiv is strictly prohibited.

Names of companies and products are trademarks or registered trademarks of the respective companies. Any questions regarding usage of trademark names should be directed to the original manufacturer.

Technical Support Site

If you encounter any installation or operational issues with your product, check the pertinent section of this manual to see if the issue can be resolved by following outlined procedures.

Visit https://www.vertiv.com/en-us/support/ for additional assistance.

TABLE OF CONTENTS

This page intentionally left blank

1 Introduction

1.1 About Vertiv™ Next Connect

Next Connect is a secure cloud-based software platform that helps manage and monitor assets. It can be used by both direct customers and channel MSP partners. The software platform allows devices to be monitored through a local agent that is installed on the customer's network. The local agent is designed based on Azure IoT Edge and communicates with hundreds of devices via Simple Network Management Protocol (SNMP).

Next Connect offers various fleet management capabilities such as bulk provisioning, device settings and firmware updates, as well as monitoring features like trending and alarming. Users can effortlessly manage the lifecycle of their devices through a unified cloud portal. This makes it easy to keep firmware and device settings current.

Since Next Connect is a cloud-based solution, customers will always have access to the latest version of the software. They will also get access to new features and supported devices as soon as they are released.

Next Connect is easily accessible from anywhere through its user-friendly, web-based, and device-agnostic interface, designed to work seamlessly on mobile and desktop environments.

1.2 Features

- Monitoring of Vertiv and 3rd party devices via SNMP
- Alarms and notifications (via email and SMS)
- Device discovery
- Remote firmware upgrade and configuration
- Device reports
- Customizable customer, site, and group dashboards
- Desktop, tablet, and mobile support
- User management
- Feedback and support directly within the product

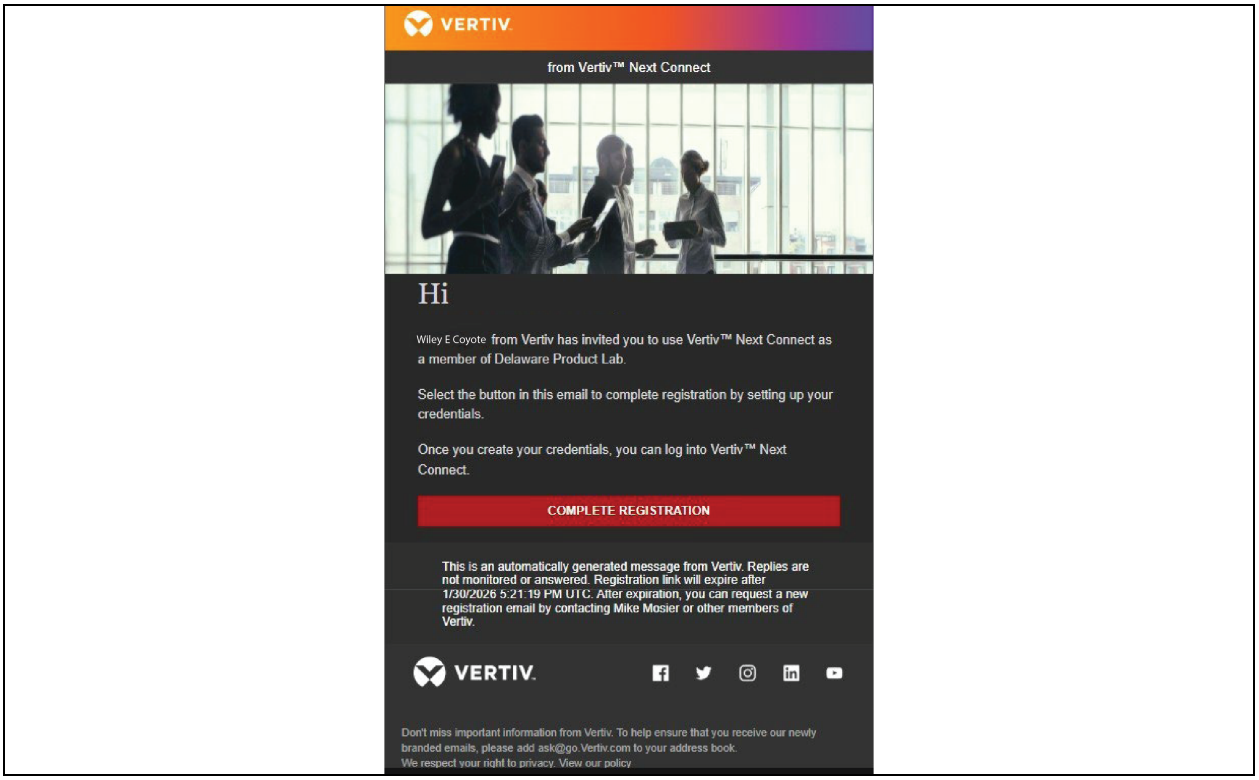
This page intentionally left blank

2 Initial Setup

2.1 Registering with the Connect Platform

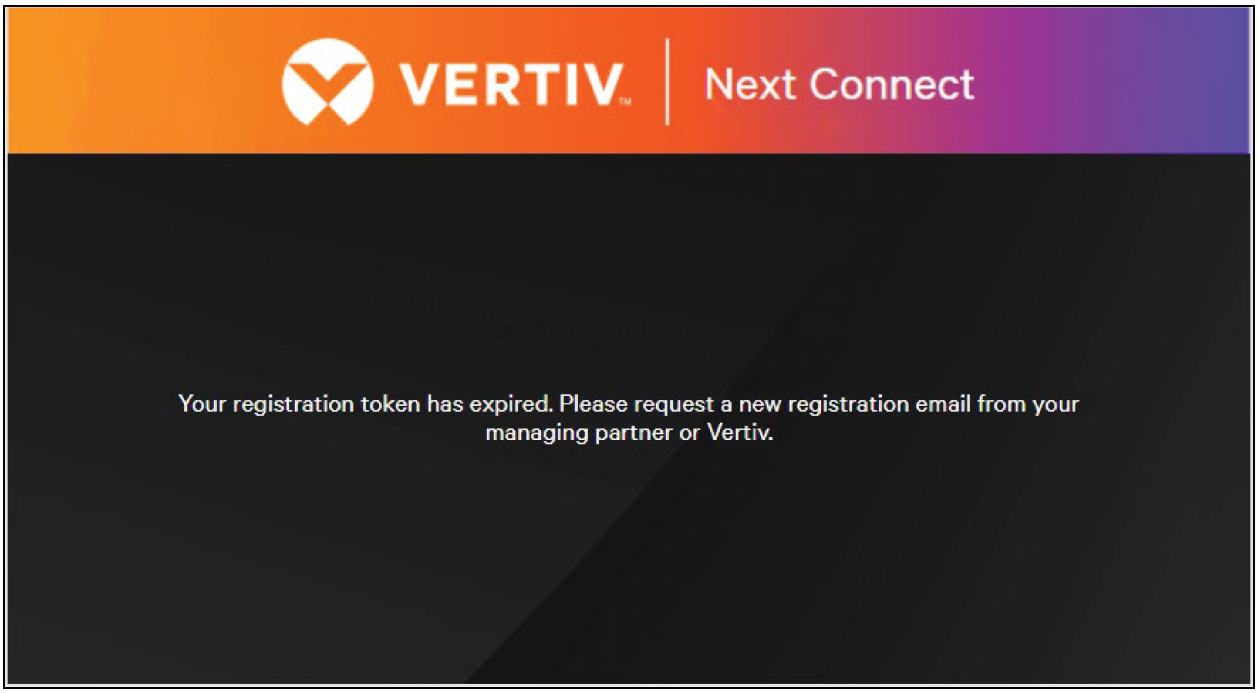
New users are invited to Next Connect via a registration email sent by Vertiv, their managing partner, or their fellow customer users. See Inviting New Users on page 36. This email may take a few minutes to be received after the user is first created in the system. If the new user has not received a registration email within the expected time interval, they should check their junk/spam folder for emails from next-connect@vertiv.com.

Figure 2.1 Registration Email



Registration emails are valid for 48 hours and expiration time is noted in the bottom of the message. If the registration email has expired, the user can request the email be resent by contacting the inviting user (noted at the bottom of the email) or other users of their organization (Customer, Partner, or Vertiv). When the registration email has expired, you will receive a message that the registration has expired.

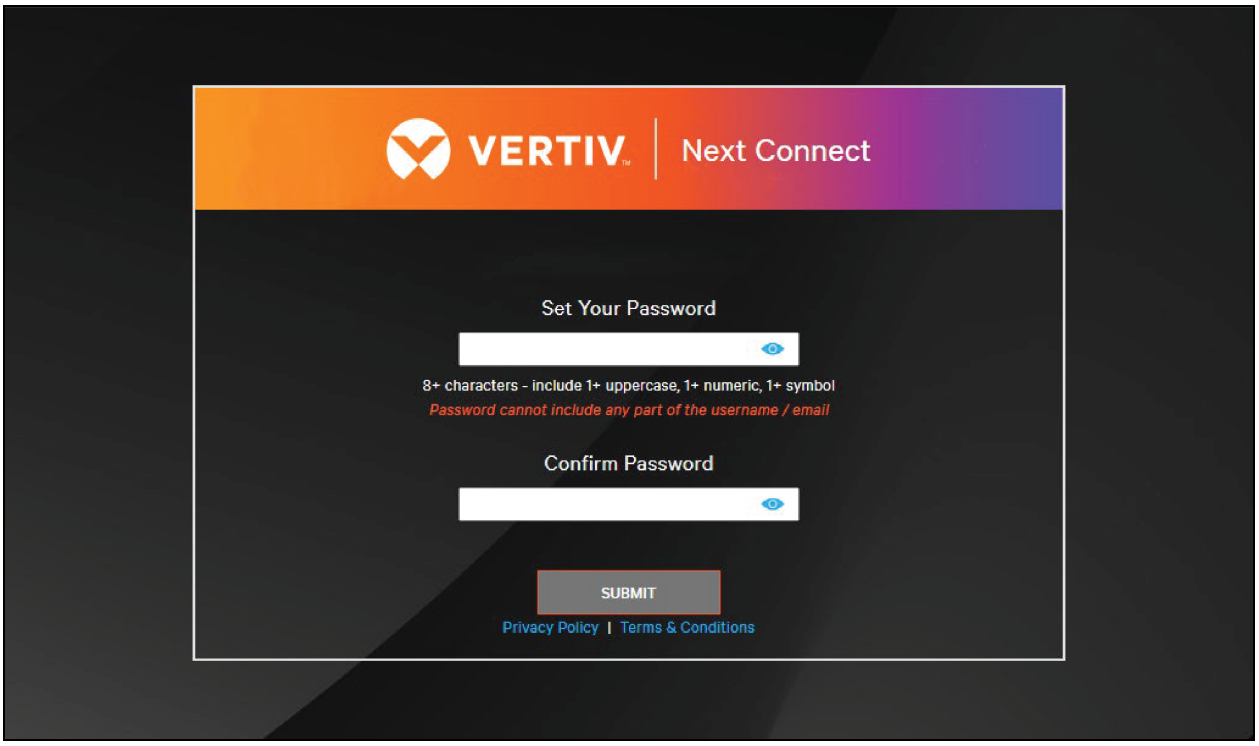
Figure 2.2 Registration Expired Notification



The registration email contains information about who invited the user to the Connect platform and to what organization (Vertiv, Partner, Customer) the new user has been added as a member. To begin the registration process, click the **Complete Registration** button in the email.

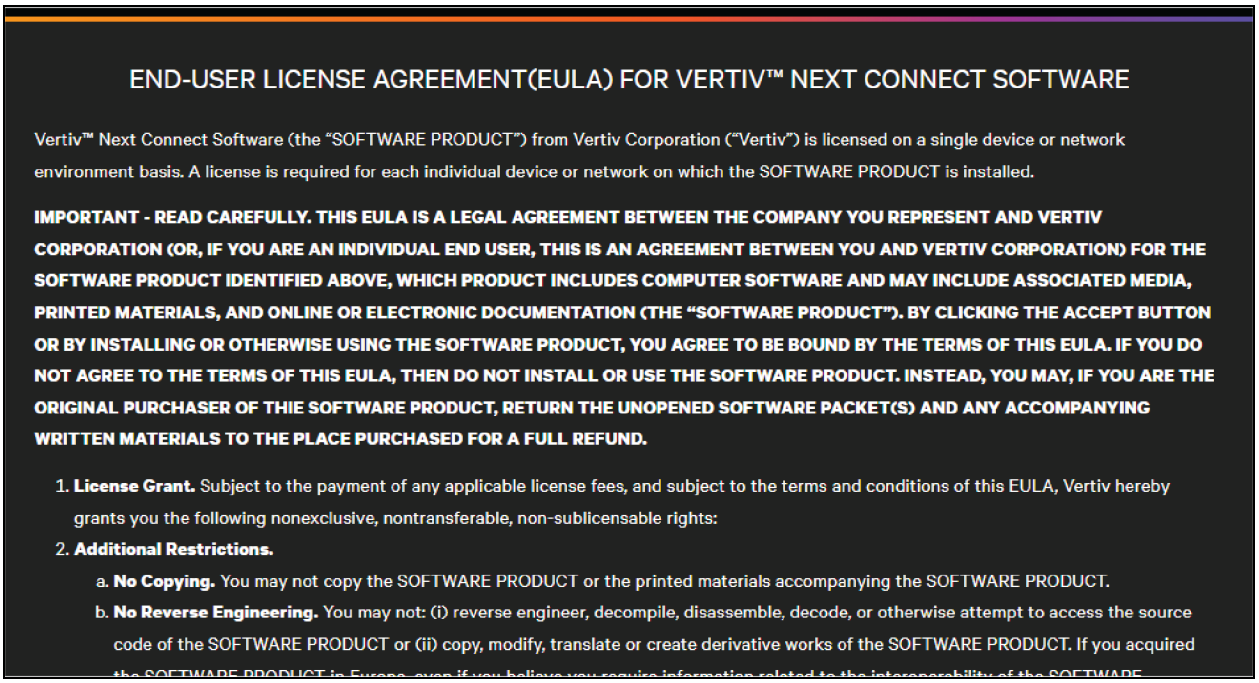
After clicking **Complete Registration**, the **Set User Password** dialog opens. You are then prompted to set their password. Password requirements are noted in beneath the **Set Your Password** field.

Figure 2.3 Set User Password



After a password has been specified, click **Submit** to confirm. An End User License Agreement (EULA) is displayed. Read the EULA and confirm by clicking **Agree**. You may need to scroll down the page to click. See Figure 2.4 below.

Figure 2.4 EULA Agreement Page



END-USER LICENSE AGREEMENT(EULA) FOR VERTIV™ NEXT CONNECT SOFTWARE

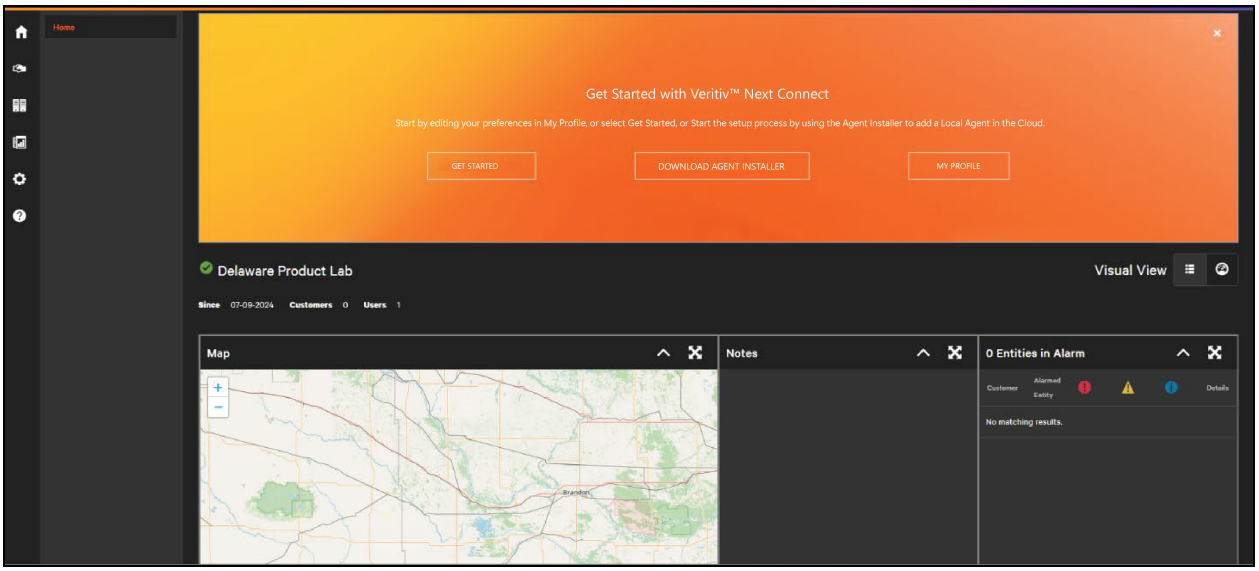
Vertiv™ Next Connect Software (the "SOFTWARE PRODUCT") from Vertiv Corporation ("Vertiv") is licensed on a single device or network environment basis. A license is required for each individual device or network on which the SOFTWARE PRODUCT is installed.

IMPORTANT - READ CAREFULLY. THIS EULA IS A LEGAL AGREEMENT BETWEEN THE COMPANY YOU REPRESENT AND VERTIV CORPORATION (OR, IF YOU ARE AN INDIVIDUAL END USER, THIS IS AN AGREEMENT BETWEEN YOU AND VERTIV CORPORATION) FOR THE SOFTWARE PRODUCT IDENTIFIED ABOVE, WHICH PRODUCT INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE ASSOCIATED MEDIA, PRINTED MATERIALS, AND ONLINE OR ELECTRONIC DOCUMENTATION (THE "SOFTWARE PRODUCT"). BY CLICKING THE ACCEPT BUTTON OR BY INSTALLING OR OTHERWISE USING THE SOFTWARE PRODUCT, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, THEN DO NOT INSTALL OR USE THE SOFTWARE PRODUCT. INSTEAD, YOU MAY, IF YOU ARE THE ORIGINAL PURCHASER OF THIE SOFTWARE PRODUCT, RETURN THE UNOPENED SOFTWARE PACKET(S) AND ANY ACCOMPANYING WRITTEN MATERIALS TO THE PLACE PURCHASED FOR A FULL REFUND.

1. **License Grant.** Subject to the payment of any applicable license fees, and subject to the terms and conditions of this EULA, Vertiv hereby grants you the following nonexclusive, nontransferable, non-sublicensable rights:
2. **Additional Restrictions.**
   a. **No Copying.** You may not copy the SOFTWARE PRODUCT or the printed materials accompanying the SOFTWARE PRODUCT.
   b. **No Reverse Engineering.** You may not: (i) reverse engineer, decompile, disassemble, decode, or otherwise attempt to access the source code of the SOFTWARE PRODUCT or (ii) copy, modify, translate or create derivative works of the SOFTWARE PRODUCT. If you acquired the SOFTWARE PRODUCT in Europe, even if you believe you require information related to the interoperability of the SOFTWARE

After agreeing to the EULA, you will see the Home screen. You are now fully registered and can begin using the Next Connect platform.

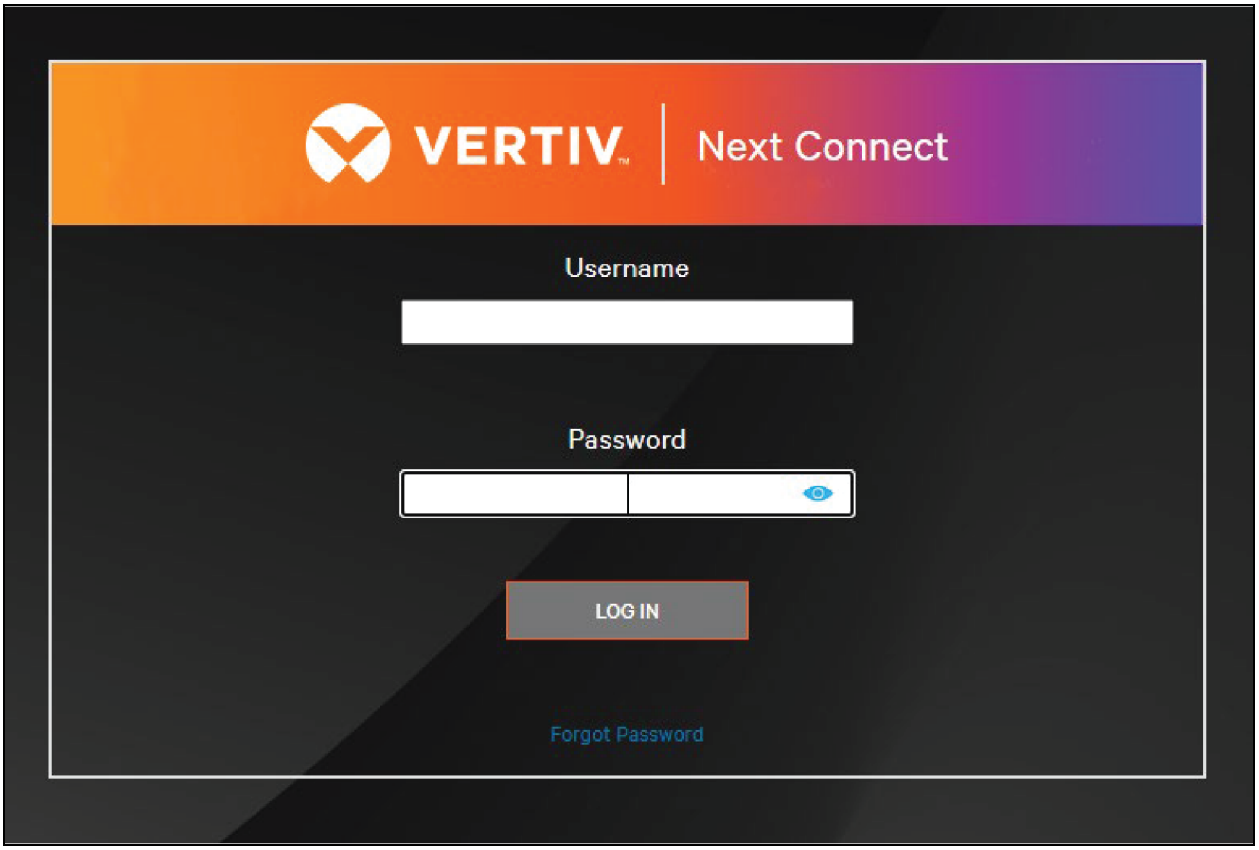
Figure 2.5 First Login



2.2 Login Screen

When logging back into Next Connect go to next-connect.vertiv.com/login.

Figure 2.6 Next Connect Login Screen



Enter your username (this is the email address where you received the registration email) and your password to login.

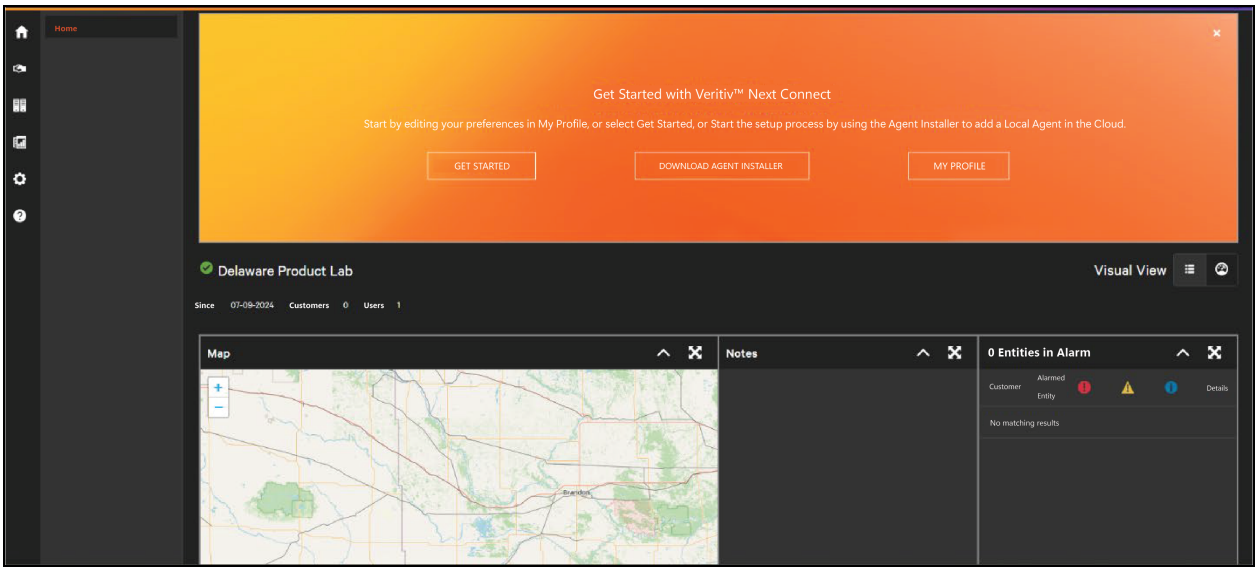
You can reset your password from this screen by clicking **Forgot Password.**

2.3 First Steps

When logging into Next Connect, a welcome banner is displayed that contains links to

1. Download a Quick Start Guide (Get Started)
2. Download local agent installers
3. Setup a user profile

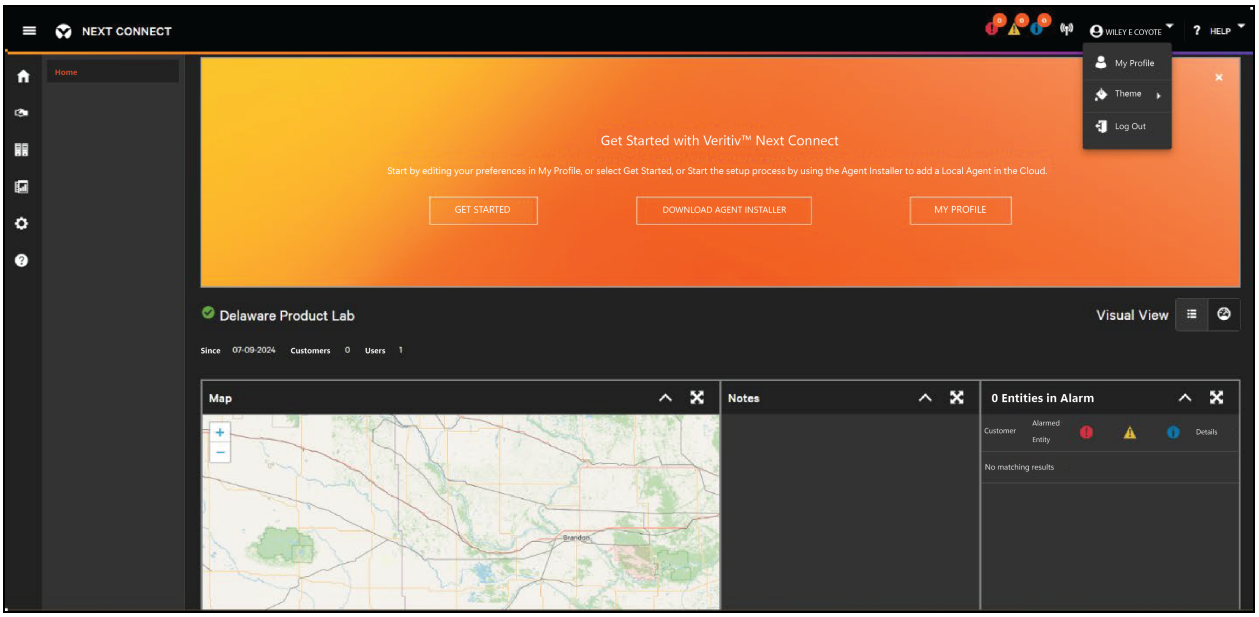
Figure 2.7 Welcome Banner



The Welcome Banner has a popup that provides links to download the Windows Agent and the Linux Agent. To permanently dismiss the Welcome Banner, click the X in the top right corner. You can also access these functions to Download the Windows Agent and Download the Linux Agent in the Agents menu under Equipment.

The first step for most users will be to finish setting up their user profile. You can do this by clicking the **My Profile** button on the Welcome Banner or by clicking the menu under your name in the top right corner.

Figure 2.8 Read-Only Profile View



Edit your profile by clicking the **Edit** button in the profile view. This is where you set contact preferences, alarm notifications, and other settings. See Managing Users on page 39 for further detail.

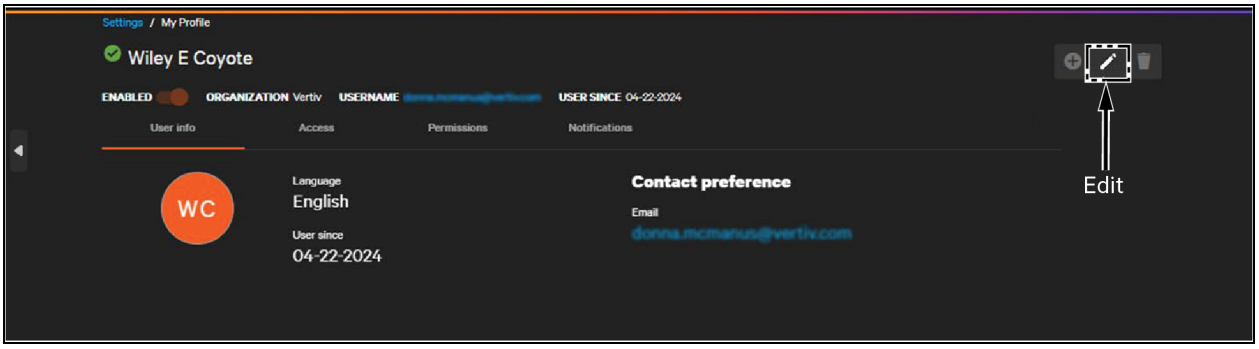
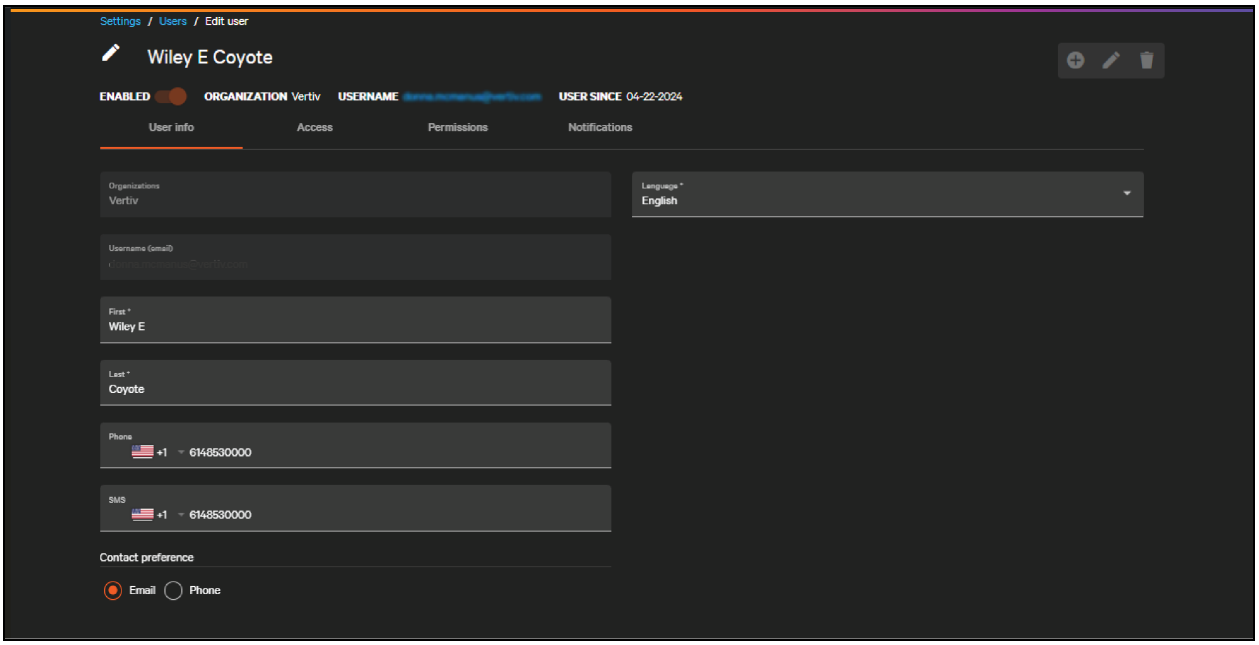


Figure 2.9 Edit Profile

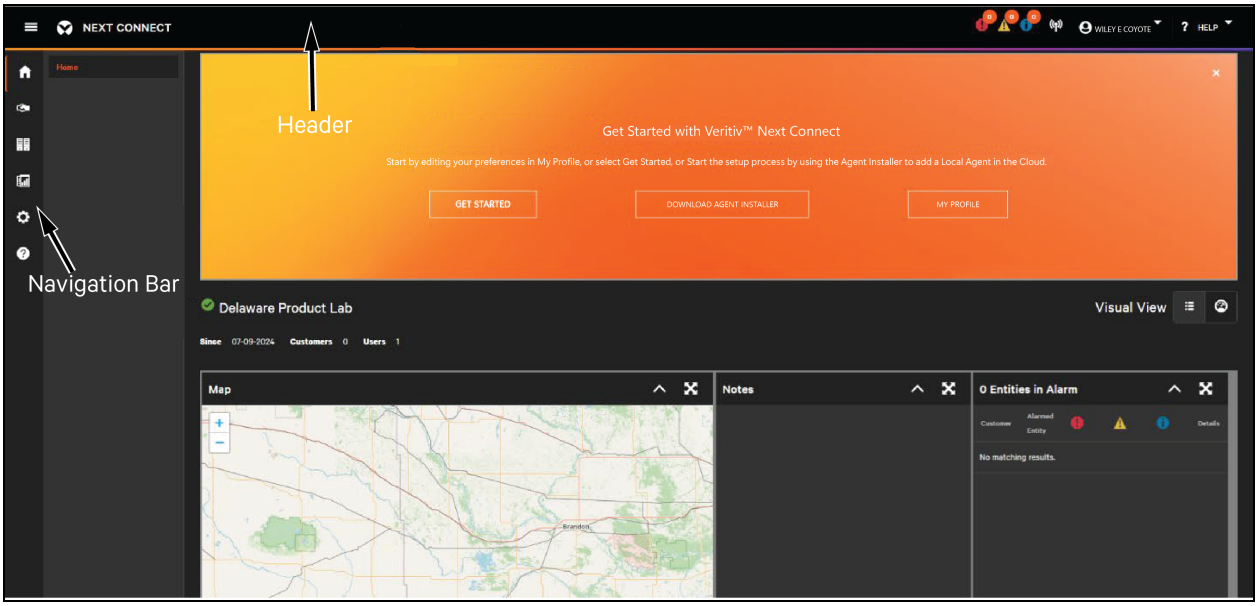


You can change your name, contact preferences, and preferred language. You cannot change your member organization or username. Click **Save** after completing your changes and you are ready to explore the Connect platform. (You may need to scroll down the page.)

3 Home Page Components and Connect Layout

Connect's layout is similar to other Vertiv monitoring products such as VCI and Environet Alert. The layout is organized into three main areas: the header bar, navigation menu, and content area.

Figure 3.1 Next Connect Layout



3.1 Header Bar

The left hand side of the header bar contains the product identification and a Collapse/Expand button. The Collapse/Expand button controls whether the Navigation menu is shown. Click the **Collapse/Expand** menu to show or hide the Navigation menu.

Figure 3.2 Header Bar (Left)

The right hand side of the header bar contains:

1. Alarm Counts
2. Discovery Results
3. User Menu

4. Help Menu

Figure 3.3 Header Bar Right

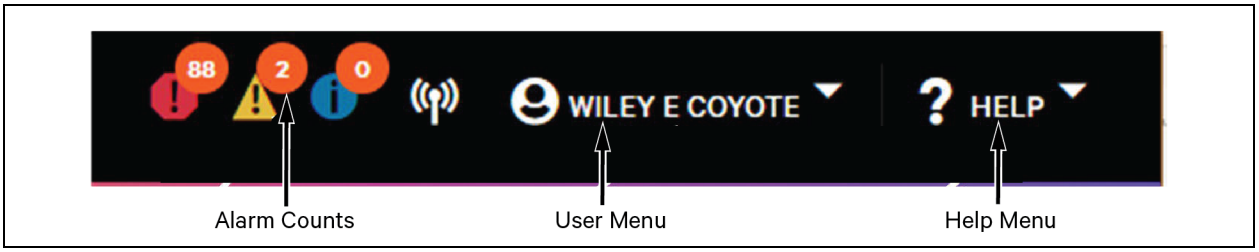


Table 3.1 Header Bar (Right) Icons

Icon	Name	Description
	Alarm Counts	Shows the number of currently active alarms for the scope of the logged in user, separated by alarm severity.
	Discovery Results	Shows the running status of a discovery scan or the results found when a scan is complete.
	User Menu	Provides access to profile details, can change from light to dark them, and log out.
	Help Menu	Quick link to the feedback form to submit questions or reporting bugs.

3.2 Navigation Menu

Table 3.2 Navigation Menu Icons

Icon	Name	Description
	Home Menu	Returns you to the dashboard (the view you see when first logged into Connect). The dashboard view can be customized to suit the needs of each organization. See Dashboard Management on page 121.
	Accounts	The Accounts menu contains options for Partner, Customer, and site—you can navigate to see a list of partners, customers, or sites to which you have access. You can also create new partners, customers, and sites depending upon your user type and role. Licensing New Partners and Customers on page 19 covers creating and licensing Partners and Customers. Sites are discussed as part of adding devices in Alarms on page 133.
	Equipment	The Equipment menu contains device management and configuration options. From here, you can see a list of monitored devices and a list of device groups. You can manage the local agents that monitor devices as well as see uploaded device or card configurations and see the latest firmware available for Vertiv devices. Device Management on page 91 covers installing the local agent, Dashboard Management on page 121 covers adding devices. Provisioning on page 143 covers configuration and firmware updates.

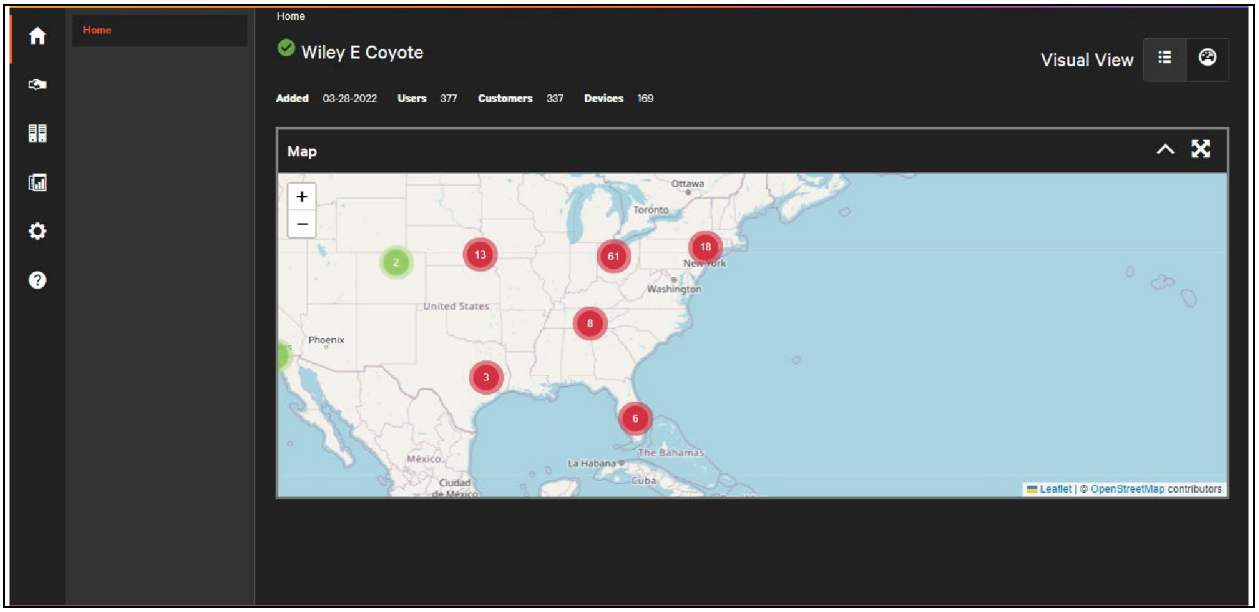
Table 3.2 Navigation Menu Icons (continued)

Icon	Name	Description
	Reports	From the Report menu, you can run reports on monitored devices as part of lifecycle management. The device report allows you to extract device metadata including networking, lifecycle, and location data for devices throughout the system. More reports will be added to the system with new versions. Reports are covered in Reports on page 175.
	Settings	The Settings menu provides information about users. All users can edit their own user information. For users with the User Management permission, they can also edit the credentials of other users in their organization. More settings may be added with future versions. User Management is covered in Managing Users on page 39.
	Support	The Support menu provides documentation and feedback options. You can also find the EULA here. Support on page 185 provides support options in detail.

3.3 Home Dashboard

The Home Dashboard is the landing page when you first log into the Connect platform. The dashboard provides summary information about monitored sites and customers and any active alarms.

Figure 3.4 Connect Home Page

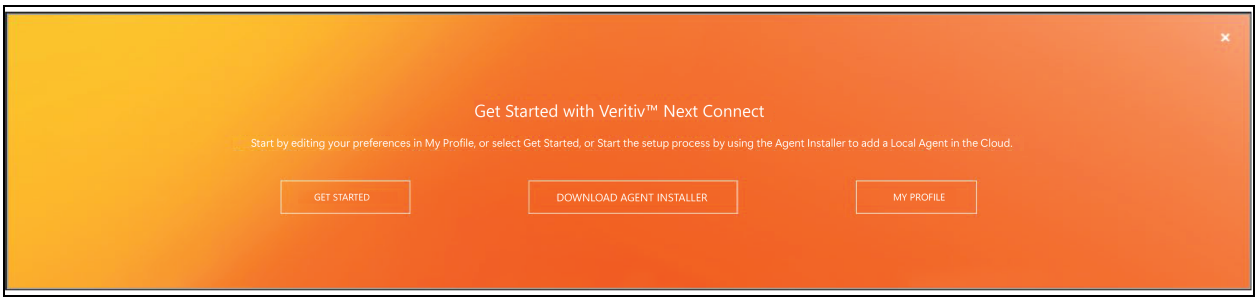


This view is created with some standard components when customers and partners are first added to the system but this view can be customized. See Licensing New Partners and Customers on page 19 and Dashboard Management on page 121.

3.3.1 Welcome Banner

When you first register with Connect, you will see a Welcome Banner on the home dashboard. You can permanently dismiss this banner on future logins. The Welcome Banner contains links to the Quick Start Guide, the local agent installer, and a link to setup your profile.

Figure 3.5 Welcome Banner



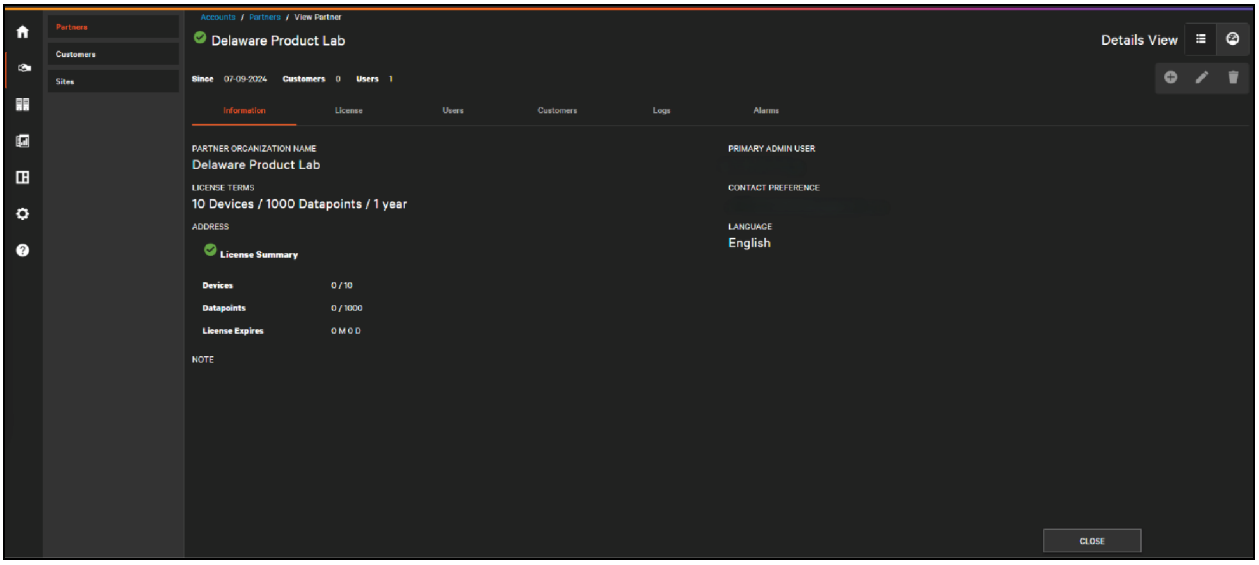
3.3.2 Visual Views and Detail Views

On single entity views, you will see a toggle between Visual View (Dashboard) and the Details view (Tabs/Forms).

Figure 3.6 Visual View/Details View Toggle

The toggle displays the currently active view in text to the left and with highlighting on the toggle. Broadly speaking, the Details view contains more of the configuration options for the entity (customer, device, group, etc.) and the Visual view is a presentation of current state and historical telemetry. On the Home Dashboard this will toggle between the organization dashboard and the organization details.

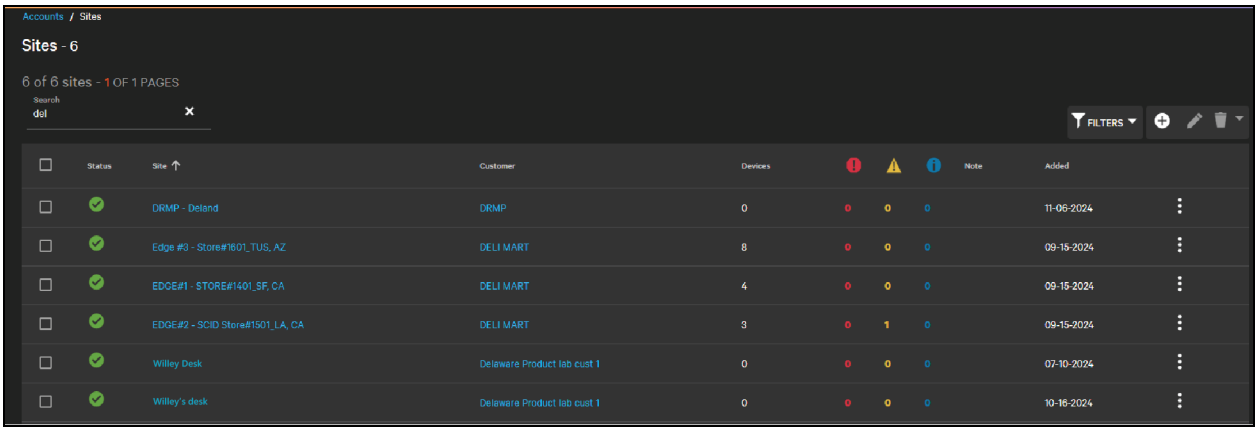
Figure 3.7 Example Details View



3.4 Lists

Groups of entities in Connect are shown in lists. Lists are the primary place to create partners, customers, sites, groups, devices, agents, users, etc. Each list is tailored to the specific entity or file but shares a few components in common.

Figure 3.8 Example List



Lists can be searched and filtered. Both searching and filtering narrow the entities shown in the list view. Each column can be sorted in ascending or descending order by clicking the column header.

Search icon

Filter icon

List operations are at the top right of the list, next to the filter. List operations are Add, Edit, and Delete.

Add icon

Add icon

Edit icon

Delete icon

Some functions can be performed on multiple rows. Select the rows you wish to edit or delete by selecting the checkbox to the left of each row.

Most objects have a status that indicates whether the object is enabled, online, offline, or if the device is disabled or not monitored.

Enabled icon

Online icon

Offline icon

Disabled icon

Additional columns provide context for related entities. For example, which customer contains the site on each row. Name and context columns are hyperlinked to allow for easy navigation throughout the product.

Lists contain rolled up alarm counts showing the number of active alarms separated by severity.

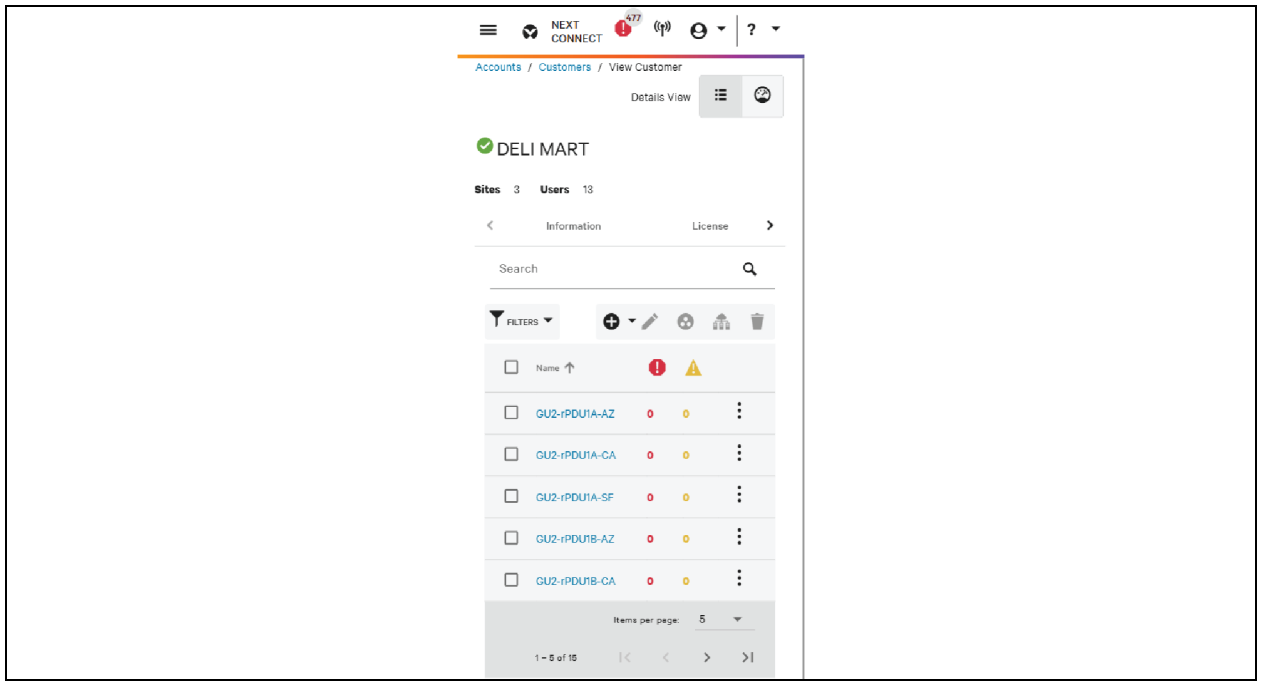
Pagination controls are in the bottom right of the list. These controls provide a way to change the number of entities shown on each page as well as to navigate to each page of objects.

Lists appear off the main menus (Account, Equipment, User, etc.) and can appear under tabs of their parent entity, such as customers managed by a partner.

Some lists, like the Configuration library, refer to files rather than entities. The functionality of lists is largely the same.

The mobile view for lists hides some columns to better fit the list into the mobile view. Entity detail can still be seen by clicking on the individual entity.

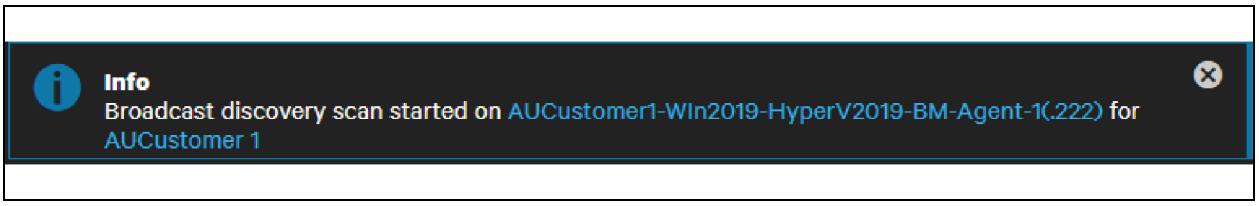
Figure 3.9 Mobile List



3.5 Notifications

Notifications in Connect are primarily presented as toast notifications at the bottom right of the screen. These show when operations begin and finish.

Figure 3.10 Example Toast Notification

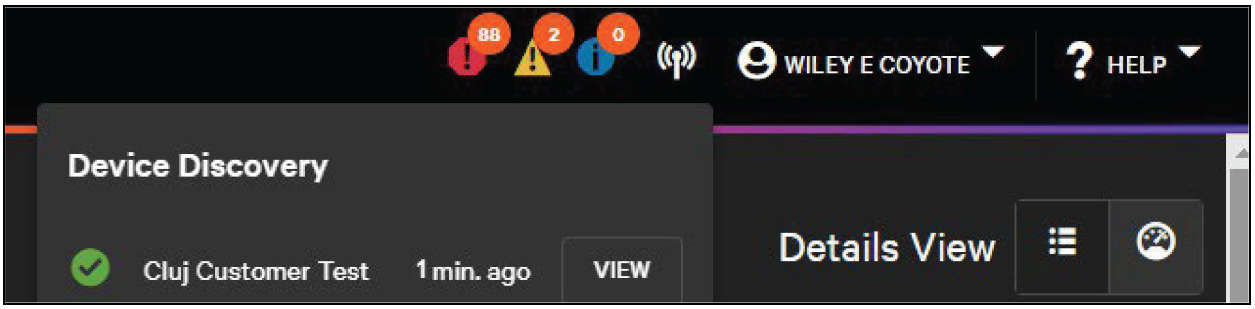


Alarm indicators are in the top right of the header bar and are visible throughout Connect.

Figure 3.11 Alarm Indicators

Some operations like Discovery show an indicator next to the icon when the operation is completed.

Figure 3.12 Discovery Results Indicator



License expiration warnings and expired messages are indicated by banner message.

Alarm notifications are external to Connect and can be received via email or SMS. See User Notification Preferences on page 50.

This page intentionally left blank

4 Licensing New Partners and Customers

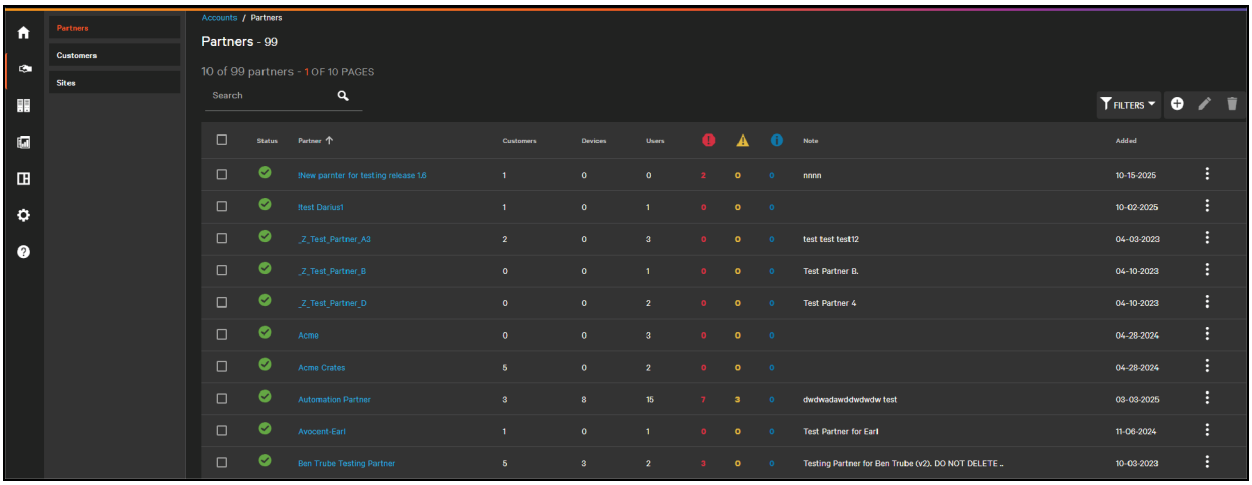
Next Connect is a multi-tenant platform that allows partners and customers to create users, establish local agents, add devices and configure groups and sites within their designated area of the platform. Users with account and licensing responsibilities can create the initial partner and customer entities required to add new companies to Connect.

4.1 Creating Partners

Partners manage the assets/devices of their customers independently of Vertiv. Only Vertiv users can create partners. Sometimes partners are referred to as channel partners or managed service provides (MSPs).

Partners can be created, edited, viewed, and deleted from the **Partners** list in the **Accounts** menu.

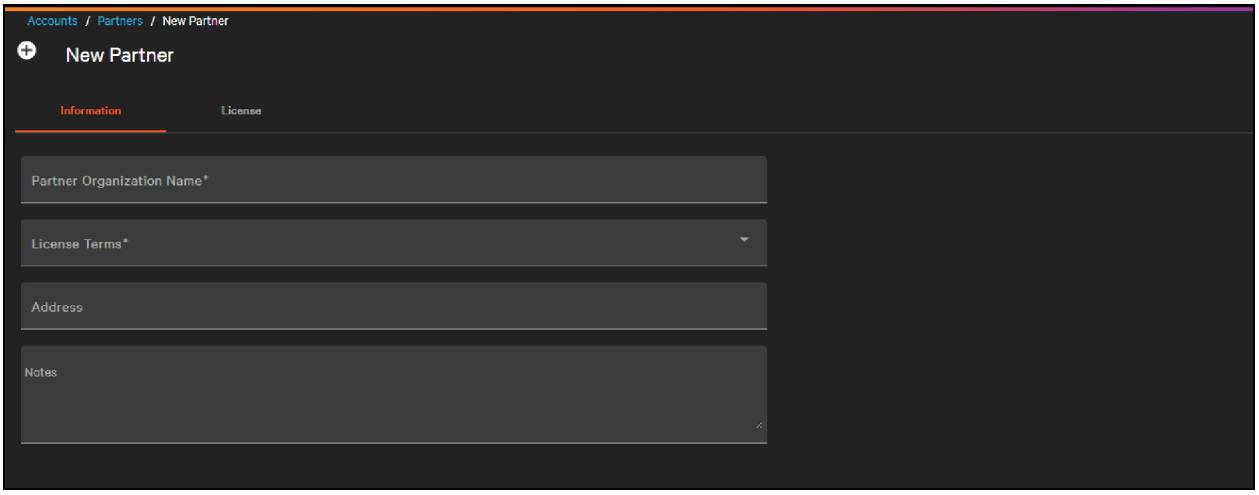
Figure 4.1 Partners List



To add a partner to this list, click the

Add icon.

Figure 4.2 New Partner Dialog (Info Tab)

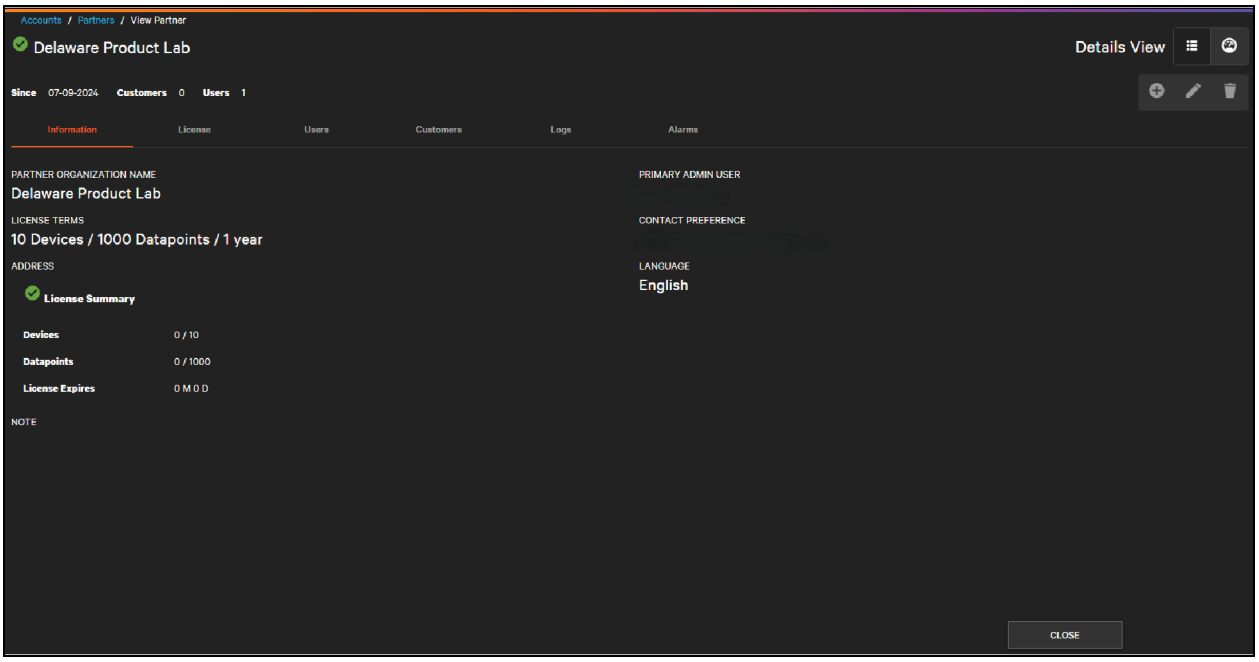


The minimum information required for a partner is a name and a license (which can be selected from the drop down), though it is suggested that you also provide an address for the partner, if available. This places the partner automatically on map widgets. After clicking **Save**, the new partner will appear in the partners list.

4.2 View, Update, Delete Partners

From the partners list, users can search for the partner they wish to view or modify. Clicking the name of the partner will take the user to that partner's read-only view.

Figure 4.3 Read Only Partner View (Info Tab)



New tabs become available after the partner is created:

- Users
- Customers
- Logs
- Alarms

Later sections explain each tab in more detail. Creating a partner also creates a default dashboard, which is used adjust to their needs. See Basic Dashboard Editing on page 121.

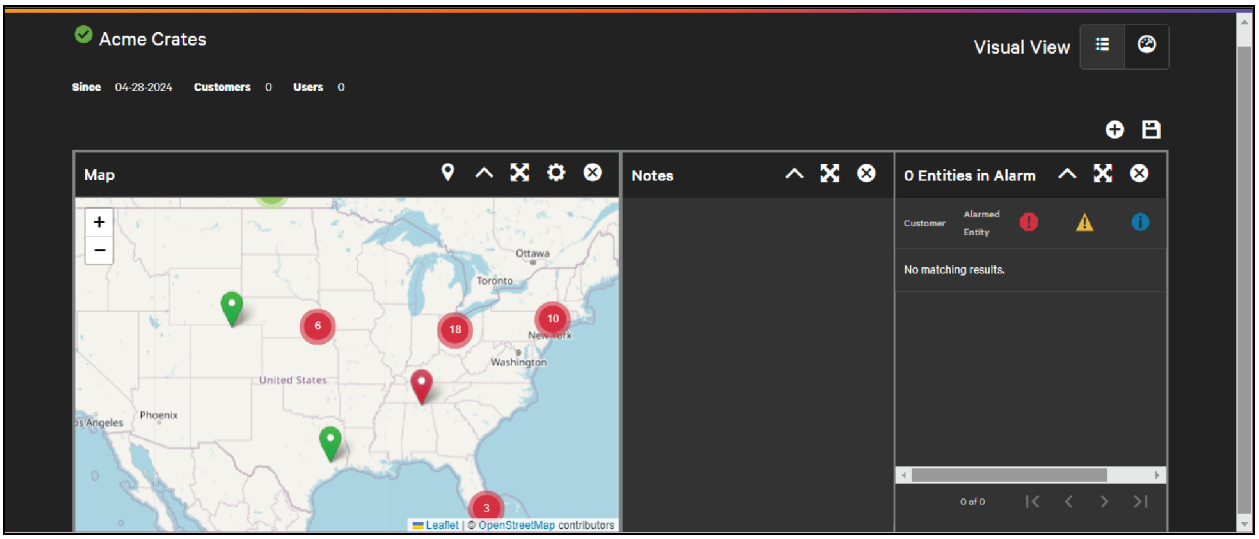
By default, the system takes you to the Details View for the partner. You can toggle to the partner's dashboard by clicking **Visual View**.

Visual View icon

You can toggle back to the Details View by clicking the **Details View**.

Details View icon

Figure 4.4 Default Dashboard for New Partner



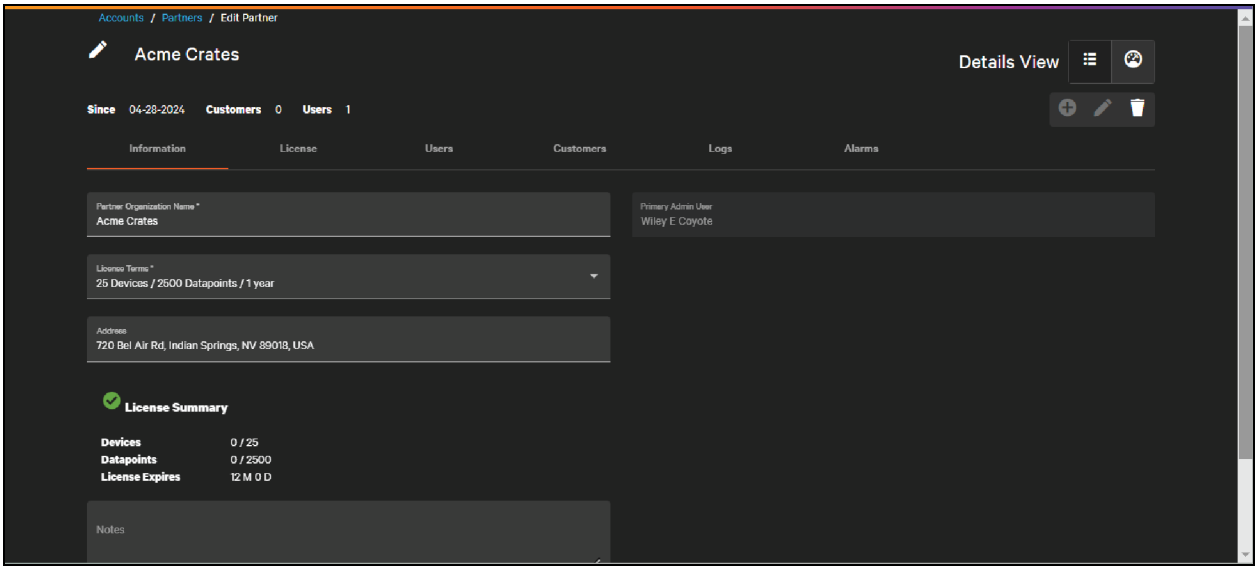
Edit Partner details by clicking the

Edit icon.

NOTE: Only Vertiv users can edit Partners, with the exception of the dashboard which the partner can customize.

You can edit all fields on the information tab, except Primary Users. Primary Users is set on the Users Tab. See Inviting New Users on page 36.

Figure 4.5 Edit Partner View (Info Tab)



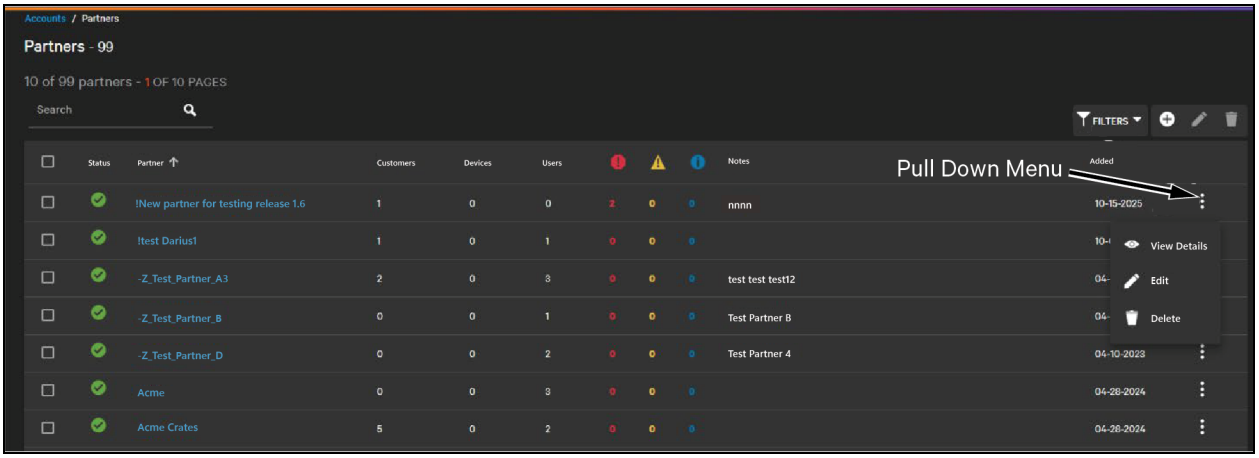
A Partner can be deleted by clicking the

Delete icon.

This deletes the partner as well as any users of that partner and customers that are managed by that partner and any devices, sites, groups, agents, or users of those customers.

To view, edit, or delete a partner, click the pull down menu next to the partner in the Partners list.

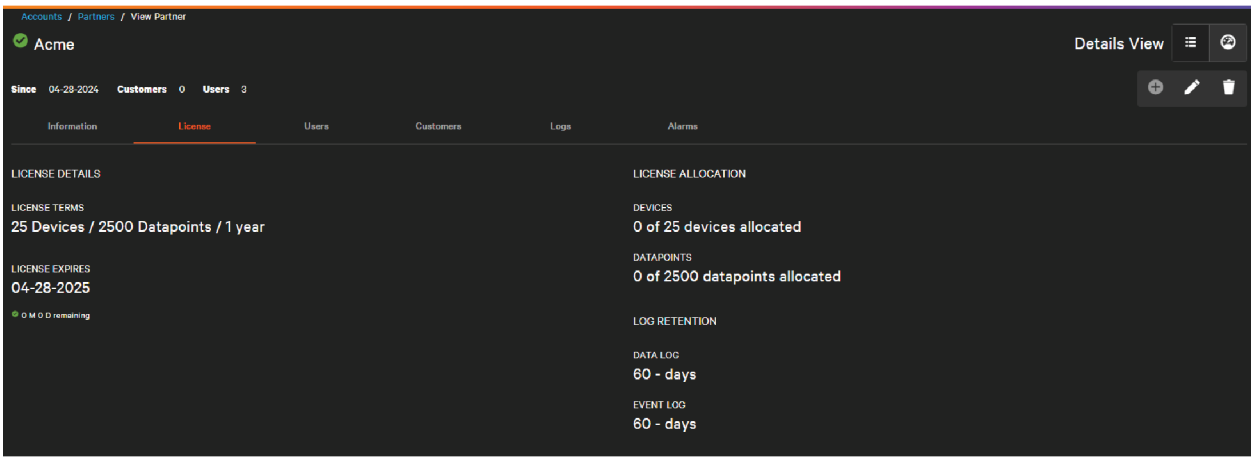
Figure 4.6 Pull Down Menu in Partners List



4.3 Choosing and Adjusting Licenses

When creating a partner, set the license by selecting an option from the License Terms drop down on the Information tab. These licenses should align to the latest license packs available for purchase. However, since multiple device packs can be purchased, you can manually adjust the entitlements of a license to match what was purchased for a specific partner or customer on the License tab.

Figure 4.7 License Tab



Licenses consist of several entitlements that define limits on the partner's or customer's use of the license. Each of these entitlements can be manually adjusted after the license has been selected:

- **License Expiration**—Connect is a subscription that can be renewed. The license expiration date indicates when that subscription is due to expire.
- **Device Limit**—The number of devices an individual partner can add for monitoring.
- **Datapoint Limit**—The number of individual data points that can be collected among monitored devices.
- **Data Log Retention**—The number of days Connect will retain data logs (numeric values, multi-state values, string values). Connect will always retain the most recent value.
- **Event Log Retention**—The number of days Connect will retain event logs (Boolean values, events from traps). Connect will always maintain the most recent value.

The system prevents actions that would exceed license entitlements such as adding devices beyond the device limit.

Users of a particular partner or customer whose license is about to expire will receive a notification eight weeks before the license is due to expire, and weekly notifications after that until the license expires.

After the license expires users are still able to log in but they will be unable to make changes to their system. They also do not receive live data or alarms until the license has been renewed.

4.4 Creating Customers

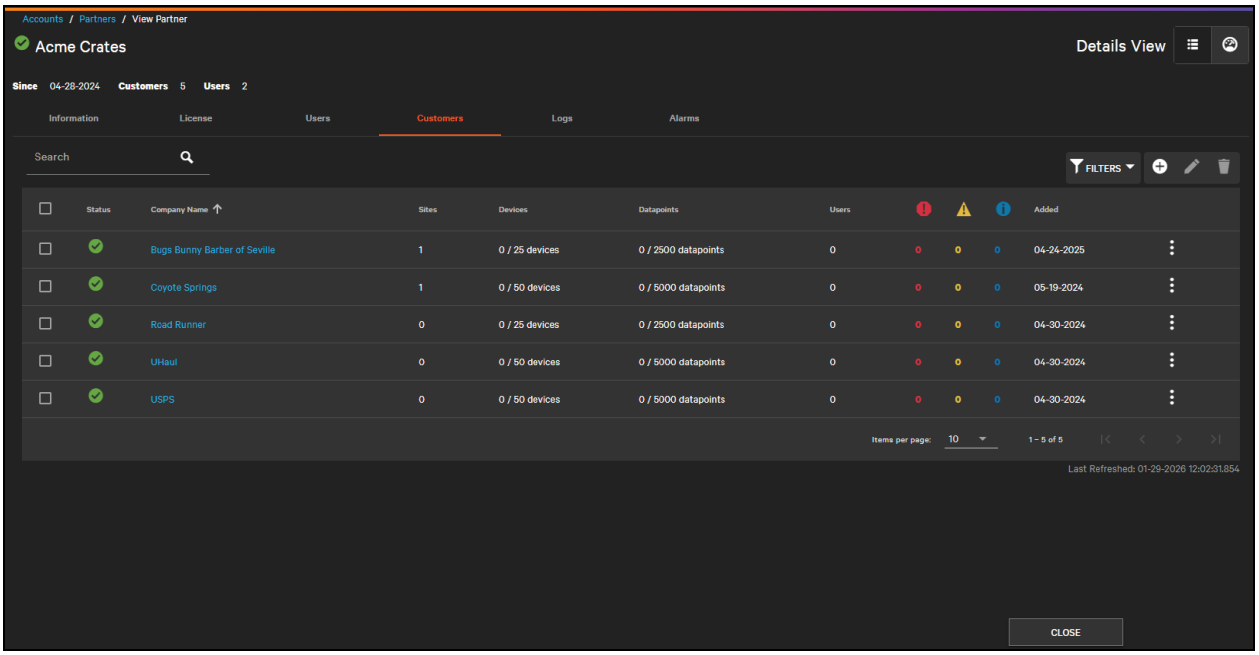
Two types of customers can be created within Connect: Partner Managed and Directly Licensed.

4.4.1 Partner Managed Customers

Partner Managed Customers are primarily created and managed by partners. They do not have their own license, but rather receive an allocation or a chunk of the partner's license.

Partner Managed Customers are managed from the Customers tab of the partner. This list shows partners how much of their license that they've allocated to each customer.

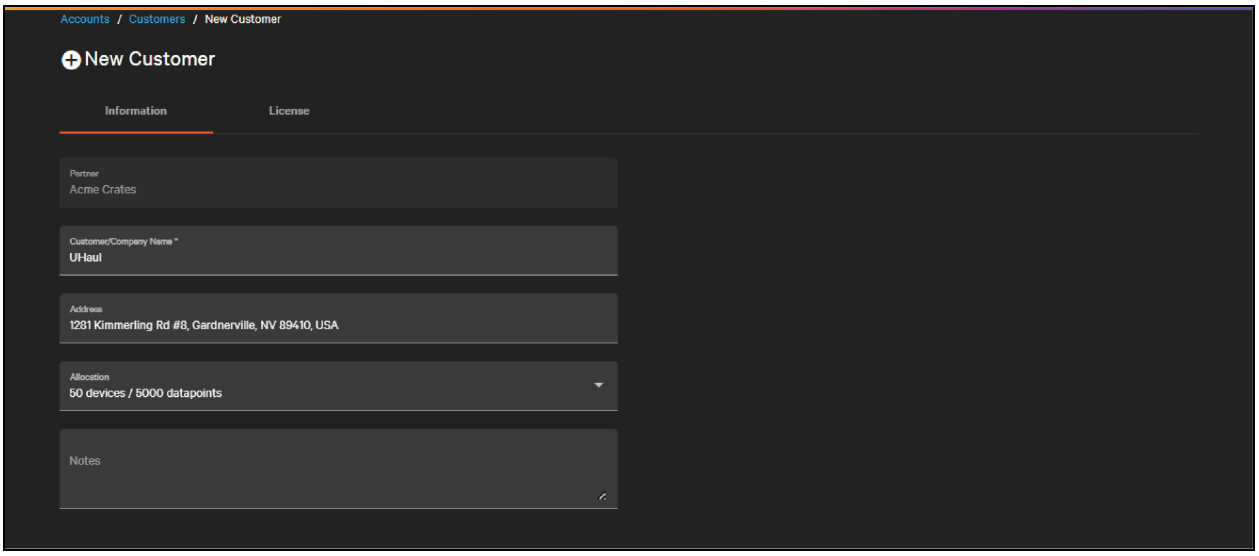
Figure 4.8 Customer Tab Under a Partner



To add a new customer, click the

Add icon.

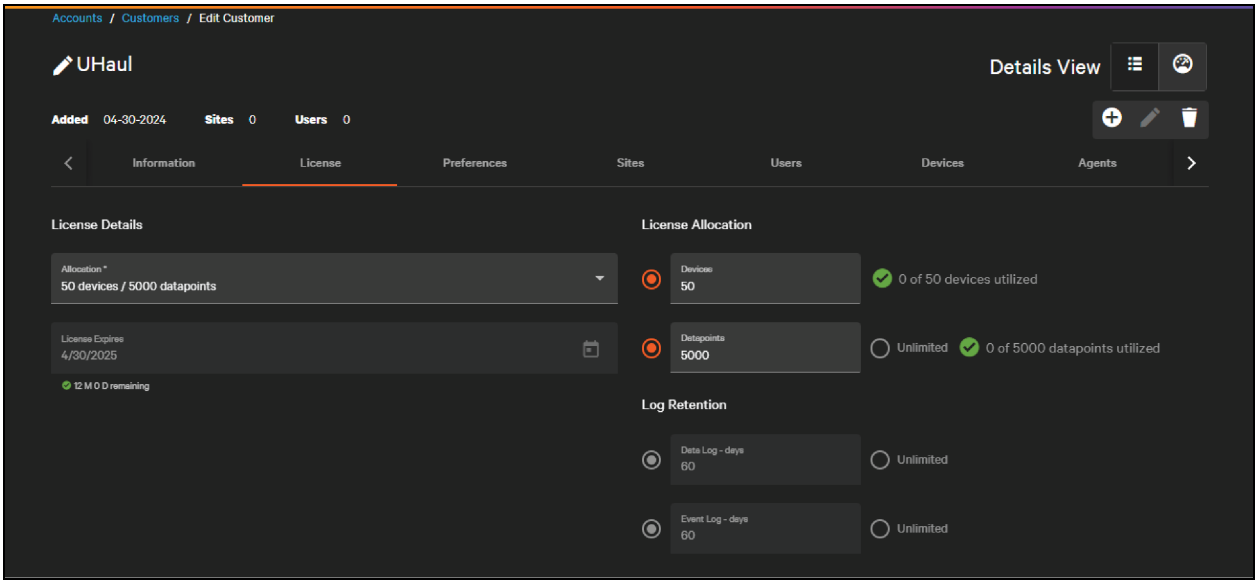
Figure 4.9 Customer License Allocation from Partner



Creating a customer this way will auto select the correct partner. The only required fields are the customer's name and allocation, although an address is recommended for placement on map widgets.

A partner can allocate some or all their license devices and data points to their individual customers. The allocation drop down provides suggested allocation sizes, although like licenses, these can be manually adjusted on the license tab.

Figure 4.10 Customer License Allocation from Partner



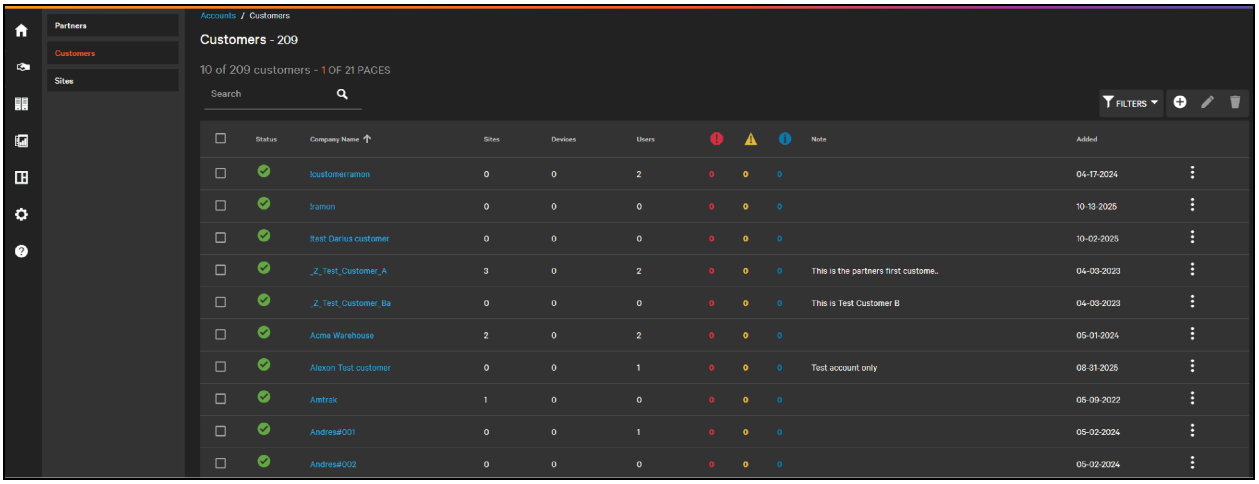
Because the customer inherits its license from the partner, it has the same expiration date and data retention limits. Its devices and data point limits cannot exceed the limits of the partner.

4.4.2 Directly Licensed Customers

Directly Licensed Customers do not have a partner intermediary between their company and Vertiv. In the Connect system, Vertiv acts as the Partner, but the customer has their own license. The customer does not have an allocation because they are not sharing a partner's license.

Vertiv users can create a directly licensed customer from the Customers List under the Accounts tab.

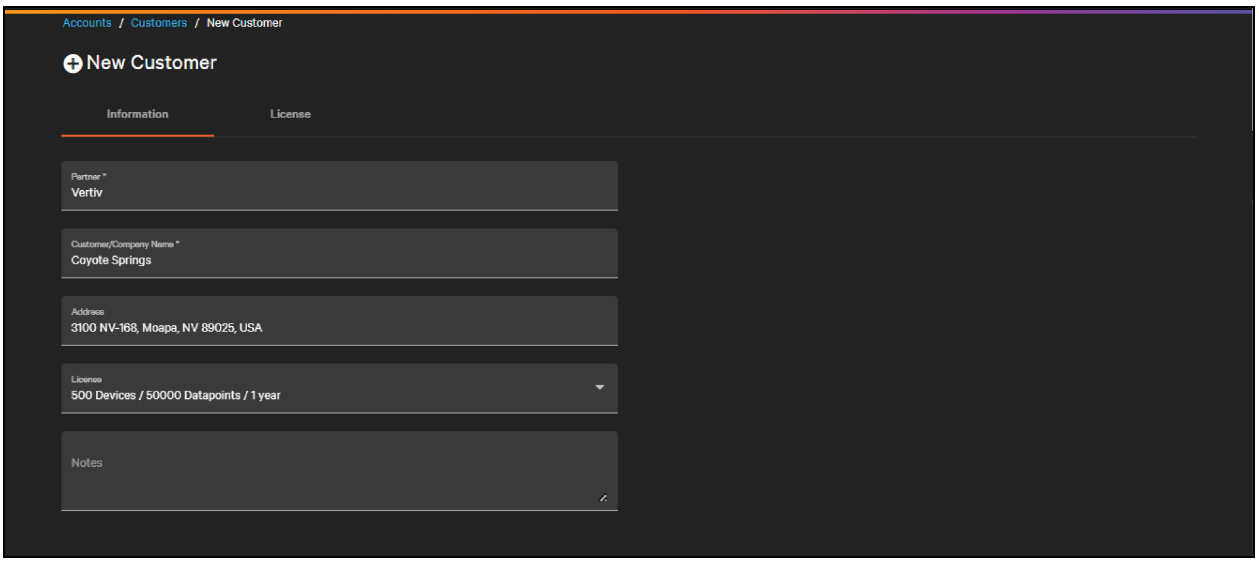
Figure 4.11 Directly Licensed Customers List



To add a new customer, click the

Add icon.

Figure 4.12 New Directly Licensed Customer Dialog (Info Tab)



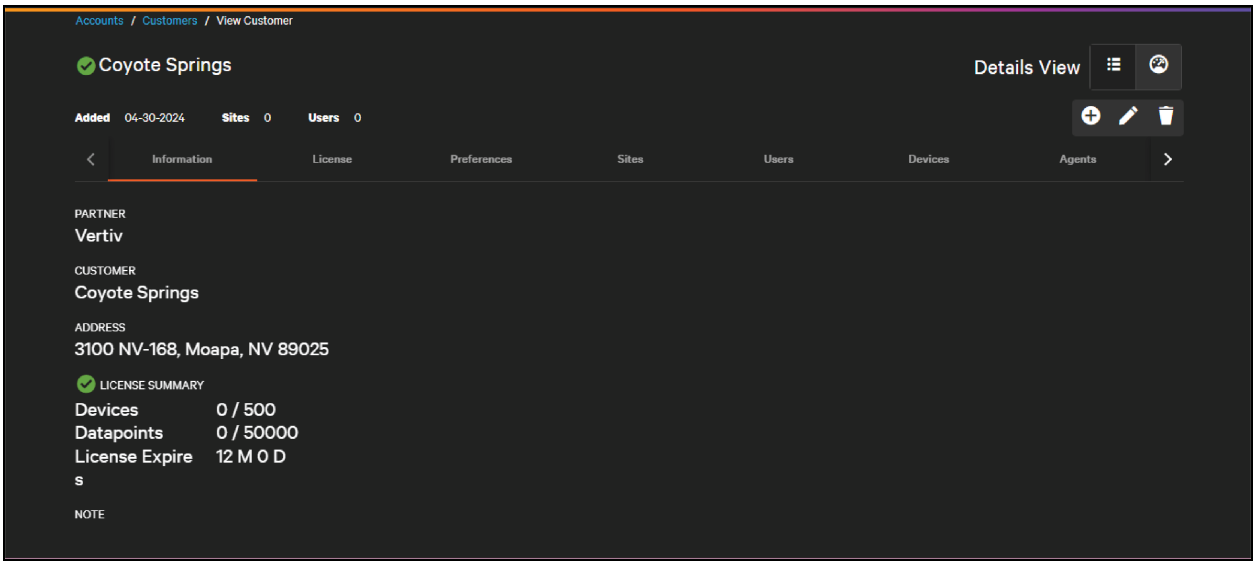
Select Vertiv as the Partner. This enables the license drop down. As with partner managed customers, only the name and license are required, though address is suggested.

The license selection and adjustment process for directly licensed customers is the same as the one for partners. See Choosing and Adjusting Licenses on page 24.

4.5 View, Update, Delete Customers

Search for the customer to view or modify from the list under the Accounts menu or the Customers tab under a partner. Clicking the name of a customer will take the user to that customer's read-only view.

Figure 4.13 Read-Only Customer View (Info Tab)



Creating a customer also creates a default dashboard, which can be adjusted later to suit your needs. See Basic Dashboard Editing on page 121.

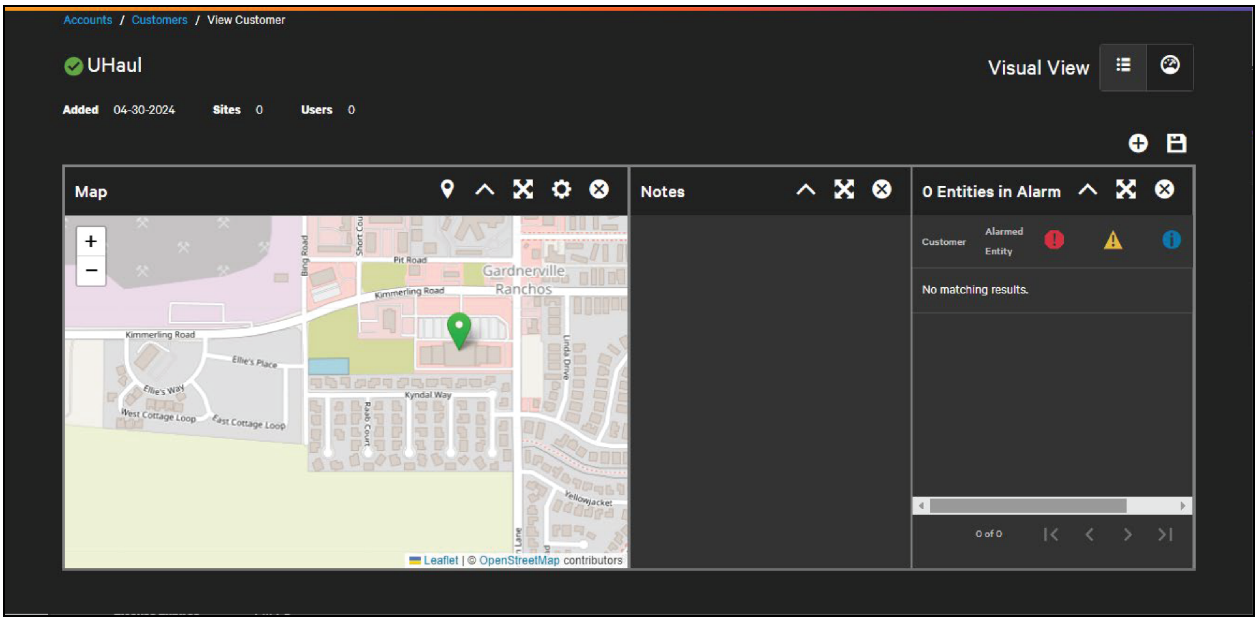
The system defaults to the Details View for customers. You can toggle to the customer's dashboard by clicking

Visual View icon.

Toggle back to Details View by clicking

Details View icon

Figure 4.14 Default Dashboard (Visual View) for New Customer



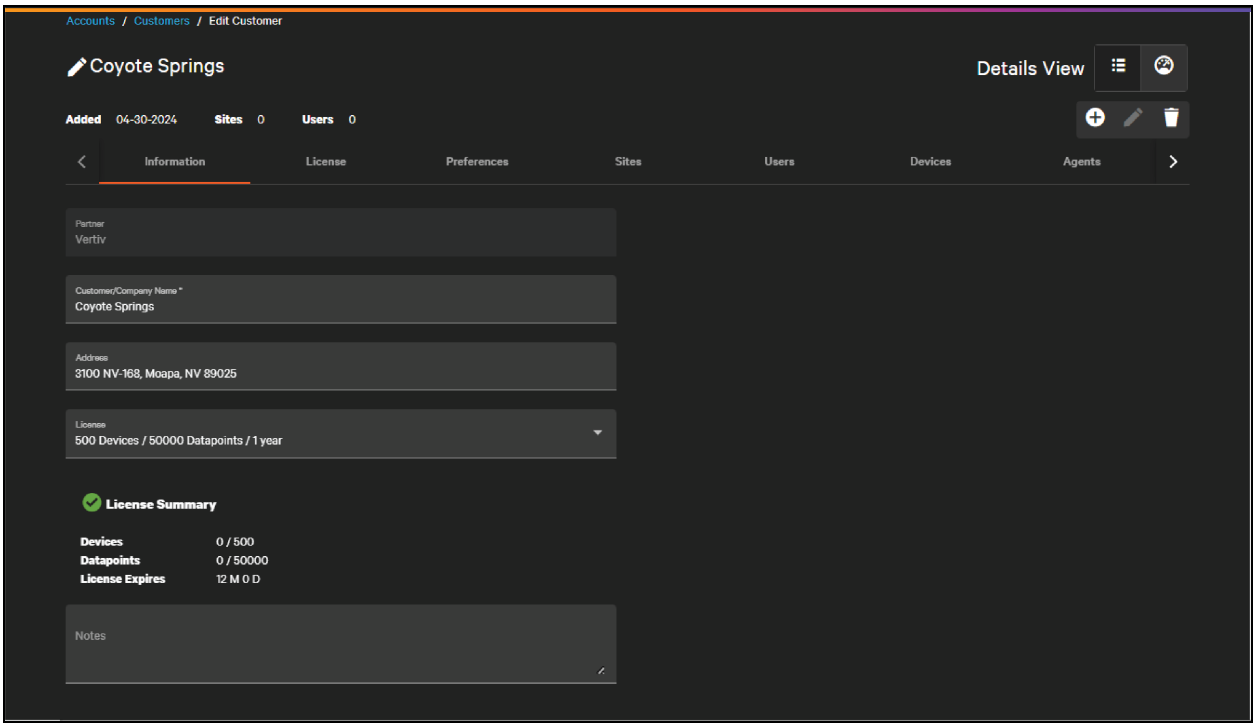
Edit customer details by clicking the

Edit icon

All fields can be edited on the information tab.

NOTE: Only the managing partner or Vertiv can edit customers with the exception of the dashboard which the customer can customize.

Figure 4.15 Edit Customer View (Info Tab)



After a customer is created, new tabs become available:

- Preferences
- Sites
- Users
- Assets
- Agents
- Logs
- Alarms

Later sections explain these in more detail. Creating a customer also creates a default dashboard, which can be adjusted to a customer's needs. See Dashboard Management on page 121.

The system defaults to the Details View for customers. You can toggle to the customer's dashboard by clicking

Visual View icon.

Toggle back to Details View by clicking

Details View icon

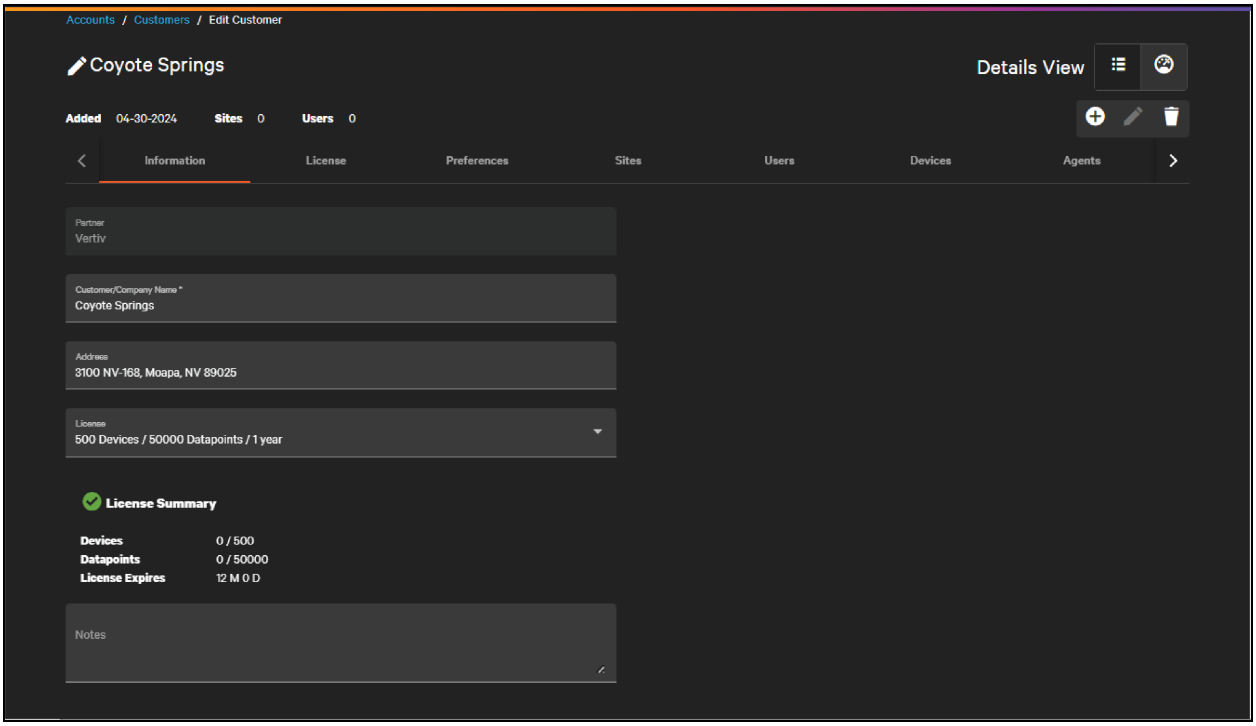
From the Details View, edit the customer details by clicking the

Edit icon.

NOTE: Only the managing partner or Vertiv can edit customers with the exception of the dashboard which the customer can customize.

All fields can be edited on the information tab.

Figure 4.16 Edit Customer View (Info Tab)



To delete a customer, use the

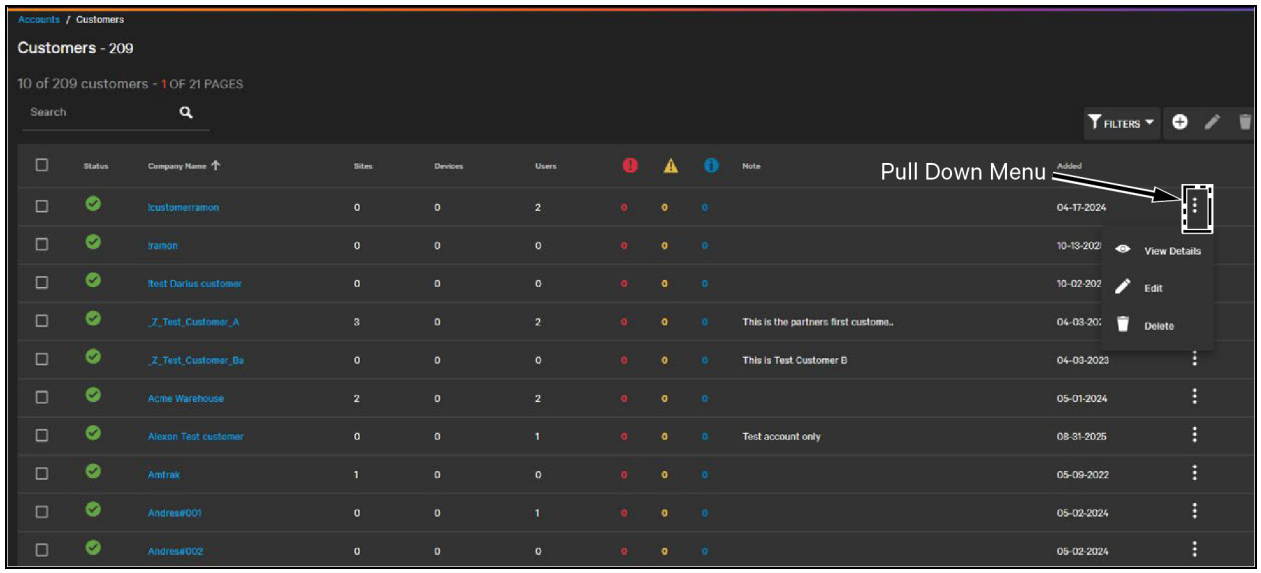
Delete icon.

When a customer is deleted, all users of that customer and any services, sites, groups, agents, users of that customer are also deleted.

View, edit, or delete a customer by clicking the pull down icon next to the customer in the Customers List.

Pull down icon

Figure 4.17 Pull Down Menu in Customers List

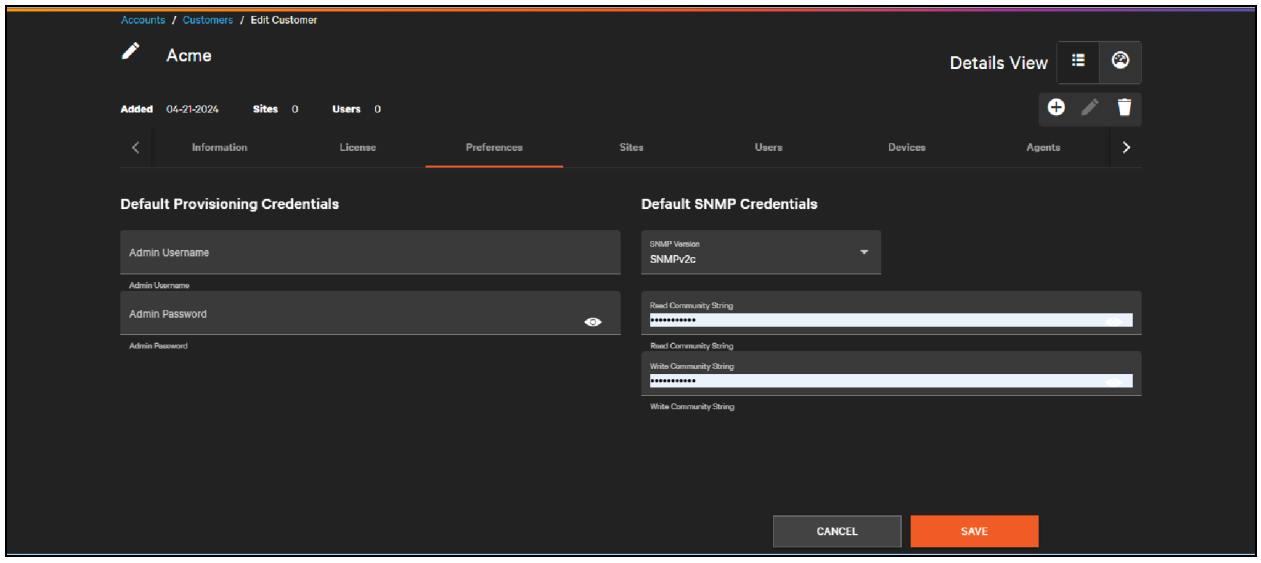


4.6 Customer Preferences

Specify the device credentials that are common across all or most of a customer's devices from the Preferences tab. These credentials are assumed as default for any discovery or monitoring but they can be changed manually at the individual device level.

Currently, two sets of default credentials can be specified: Provisioning Credentials and SNMP Credentials.

Figure 4.18 Customer Preferences Tab (Edit Mode)

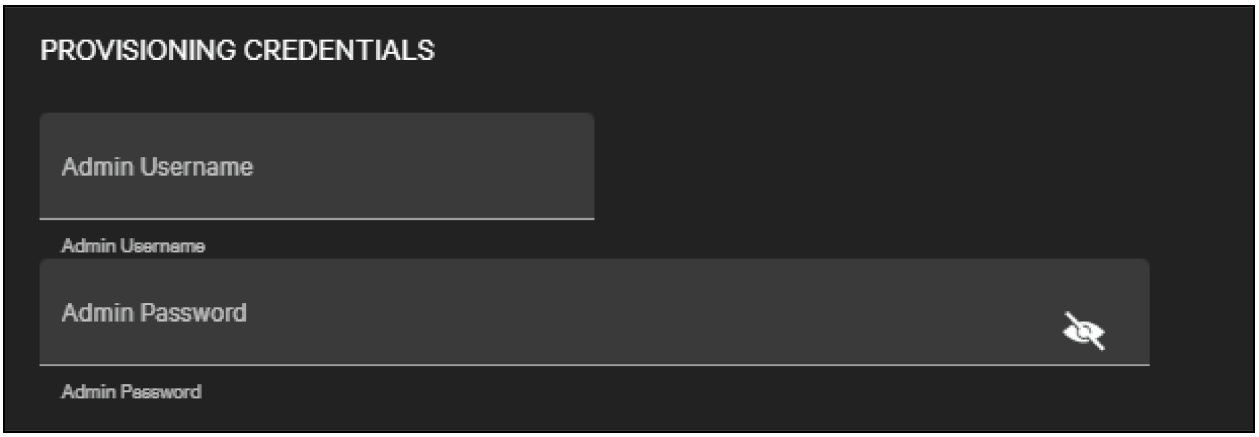


4.6.1 Provisioning Credentials

For a limited set of Vertiv devices only, we offer the ability to complete provisioning actions that require an administrator login on the edge card or device. Provisioning features are described in Provisioning on page 143.

This admin username and password is not used for access to Connect, but rather it gives Connect the ability to access the edge device. Users should not use their Connect login in these fields.

Figure 4.19 Default Provisioning Credentials



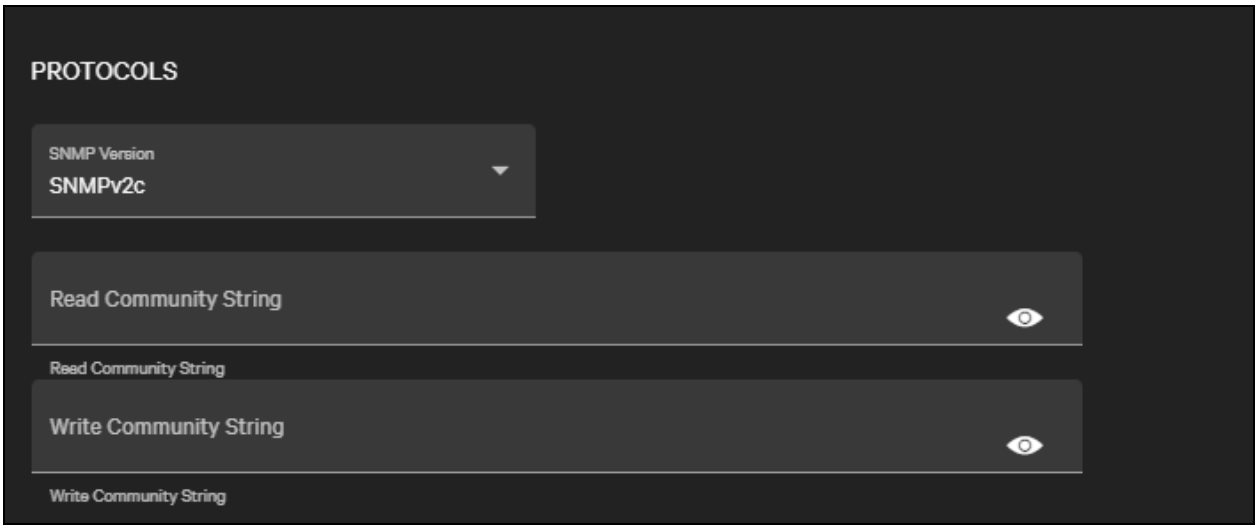
4.6.2 SNMP Credentials

The default SNMP credentials are used during device discovery to poll common device OIDs like manufacturer and model to attempt to identify the edge device. They are also used as the default SNMP credentials when polling the device for readings.

Connect supports SNMP v1, v2c, and v3.

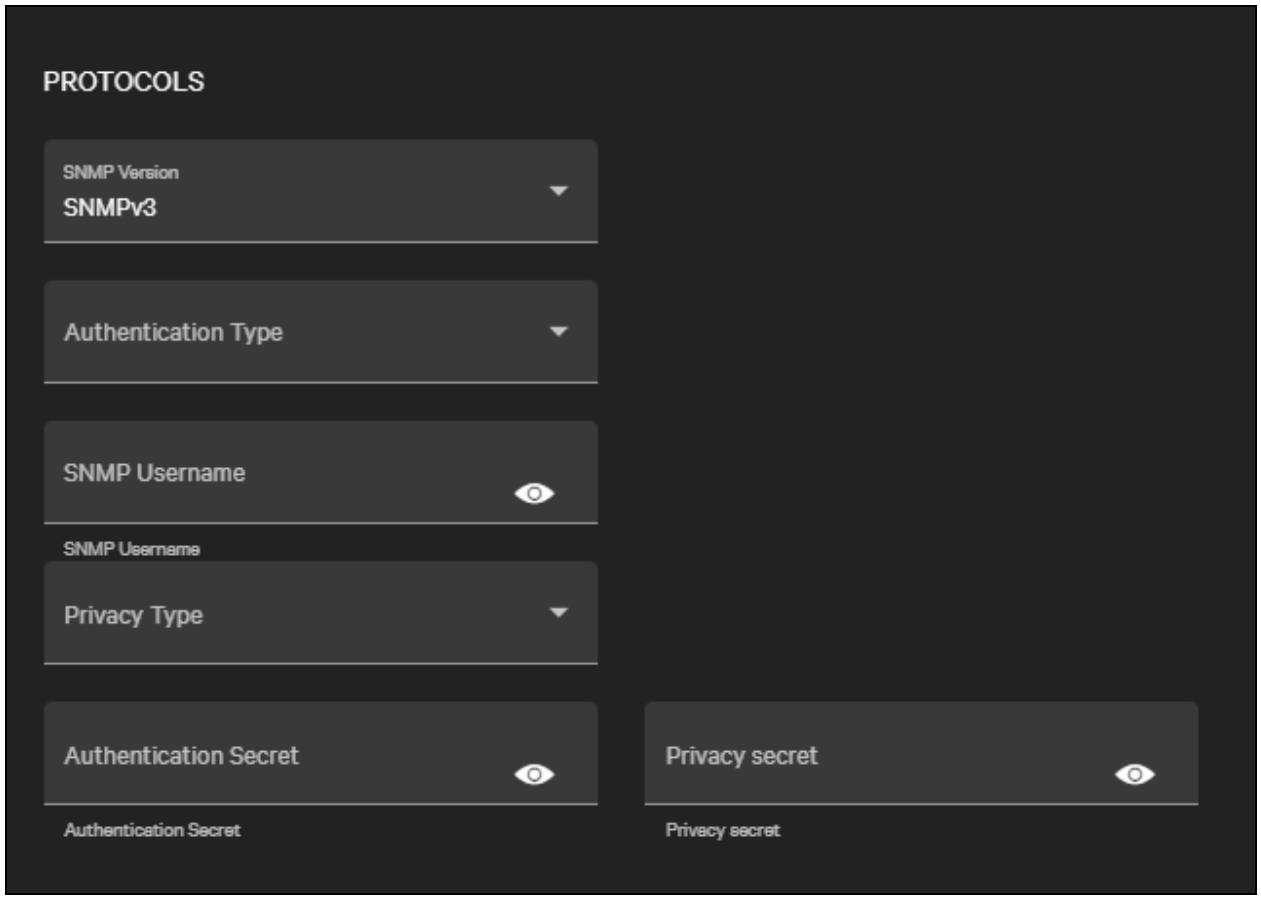
For v1 and v2c, the SNMP credentials are the read and write community strings used to poll or update OIDs on the edge device.

Figure 4.20 Default SNMP v2c Credentials



SNMP v3 offers more options with user-based authentication. Connect supports the authentication and privacy types supported on Vertiv cards and devices.

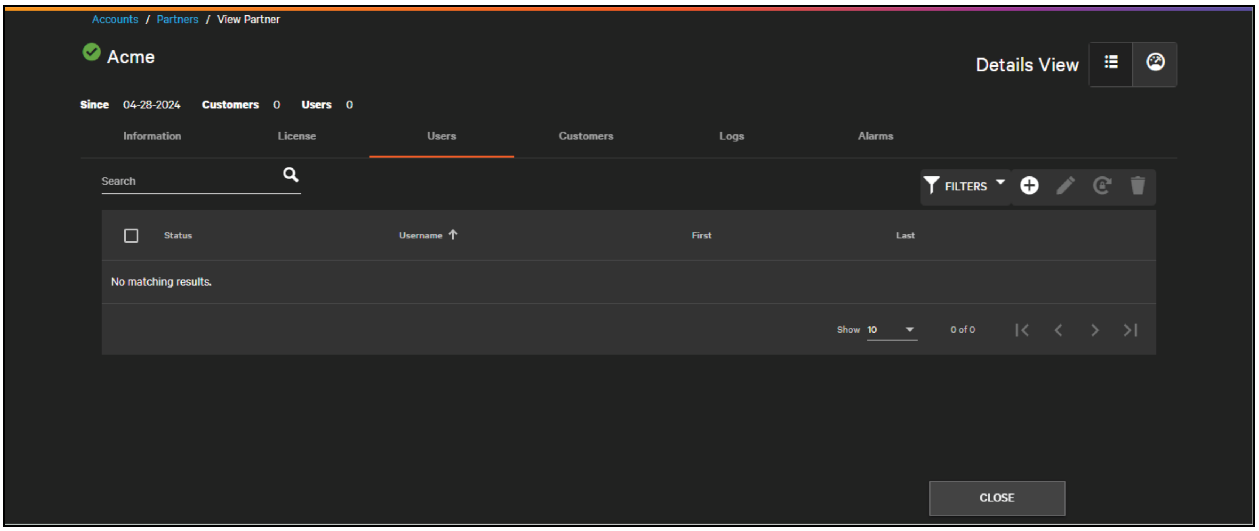
Figure 4.21 Default SNMP v3 Credentials



4.7 Inviting New Users

After the partner or customer has been created in the Connect platform, the last step is to create the first user. This is done from the Users tab on either the partner or the customer.

Figure 4.22 Users Tab Under a Partner

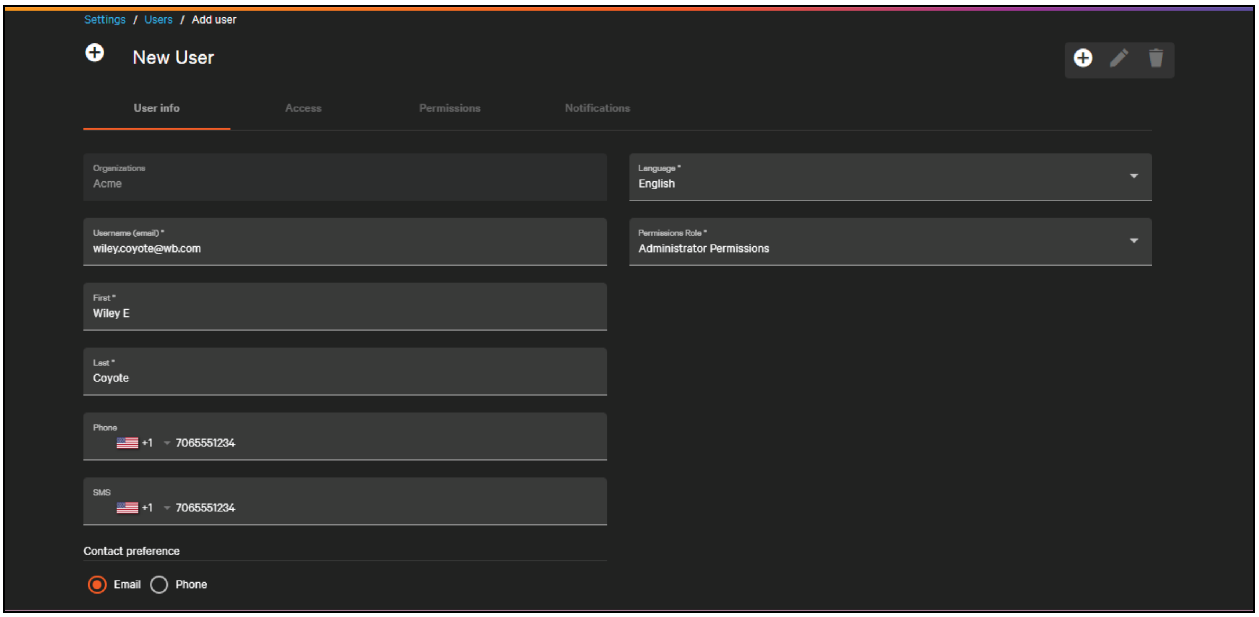


Create a new user by clicking the

Add icon

on the users list.

Figure 4.23 New Partner User Dialog



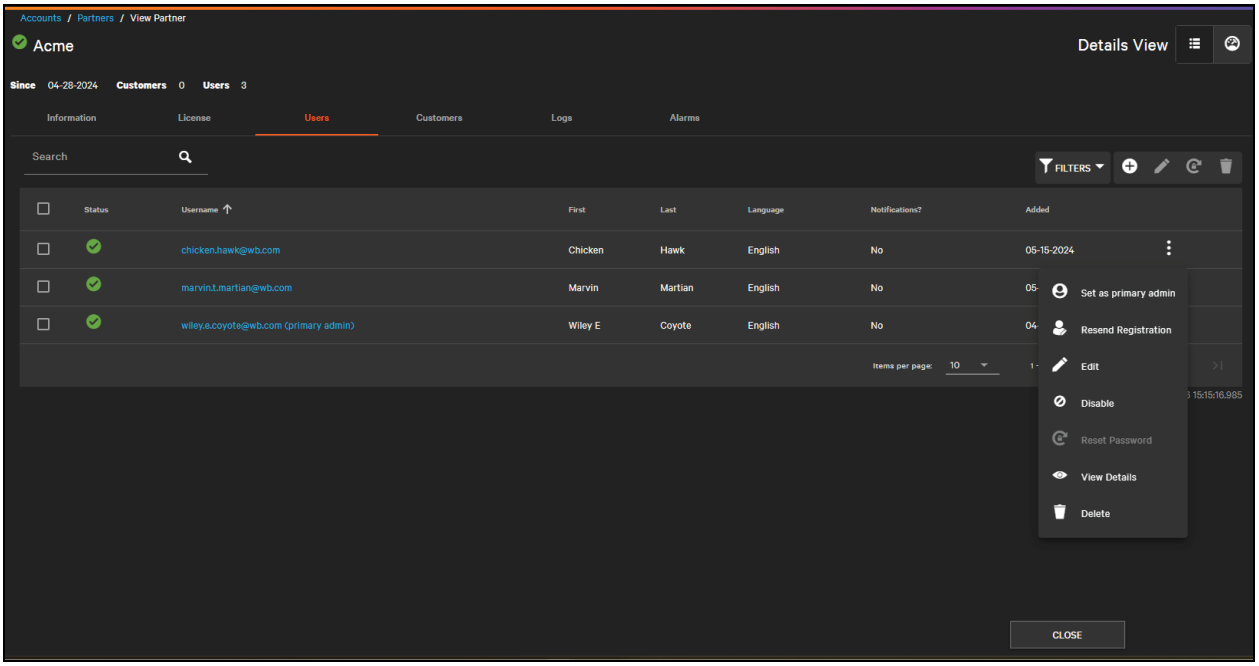
The minimum information required for the user:

- An email (which doubles as their username)
- First and last name
- Language (default is English)
- Their role

For the first user of a Partner or Customer, the role should be Administrator. The Partner or Customer organization should be auto selected if created from the Users tab under the respective Partner or Customer.

The first user created for the partner or customer is the Primary Admin. The Primary Admin serves as the primary contact for the partner or customer during support calls. The Primary Admin cannot be deleted in order to prevent the partner or customer from being locked out of Connect, but the role can be transferred to another user using the pull down menu.

Figure 4.24 Partner Users List Pull Down Menu to Change Primary User



Registration emails can take a few minutes to be received. If a user has not received their registration within a few minutes, they should double-check their junk or spam folder for the invite. If the invited user does not receive the registration email, or if the registration token expires, an admin user can resend the invitation from the pull down menu and clicking **Resend Registration**.

Once the partner and customer have access to the system, they can invite other users to their organization, and create users for the customers they manage.

User Creation is covered in detail in Managing Users on page 39.

This page intentionally left blank

5 Managing Users

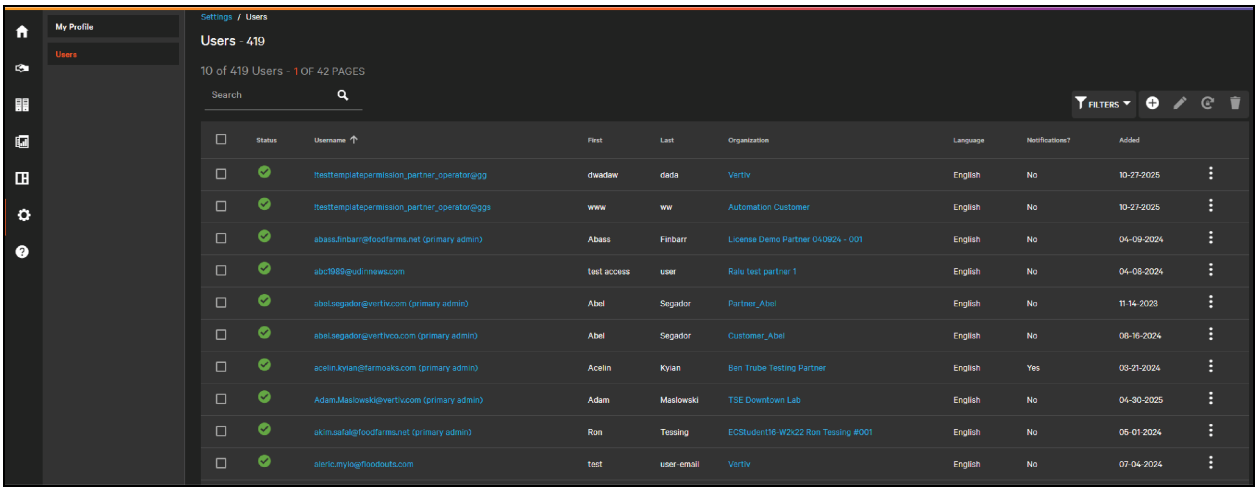
Account access to Next Connect is currently managed from within the Connect platform.

As discussed in Licensing New Partners and Customers on page 19, initial access to Connect is granted when new Partners or Customer are licensed in the product. This section covers managing users in more detail including creating, editing, deleting, defining a user's role and access, and dealing with temporary lockouts.

5.1 Creating Users

Users can be created from the Users tab of a specific partner or customer (see Inviting New Users on page 36) or from the Users List under the Settings menu. Vertiv, Partner, and Customer users can all create users within the Connect system, provided they have the User & Locale Management permission enabled.

Figure 5.1 Users List Under Settings Menu

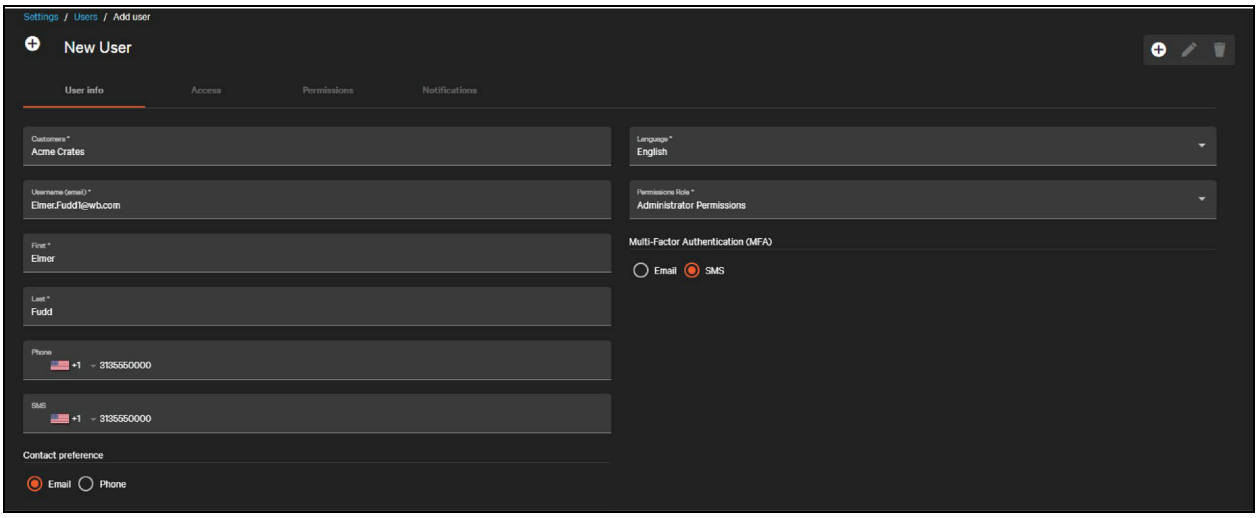


Click the

Add icon

to create a new user from the Users List. The New User dialog opens.

Figure 5.2 Create New User Dialog (Custom User)

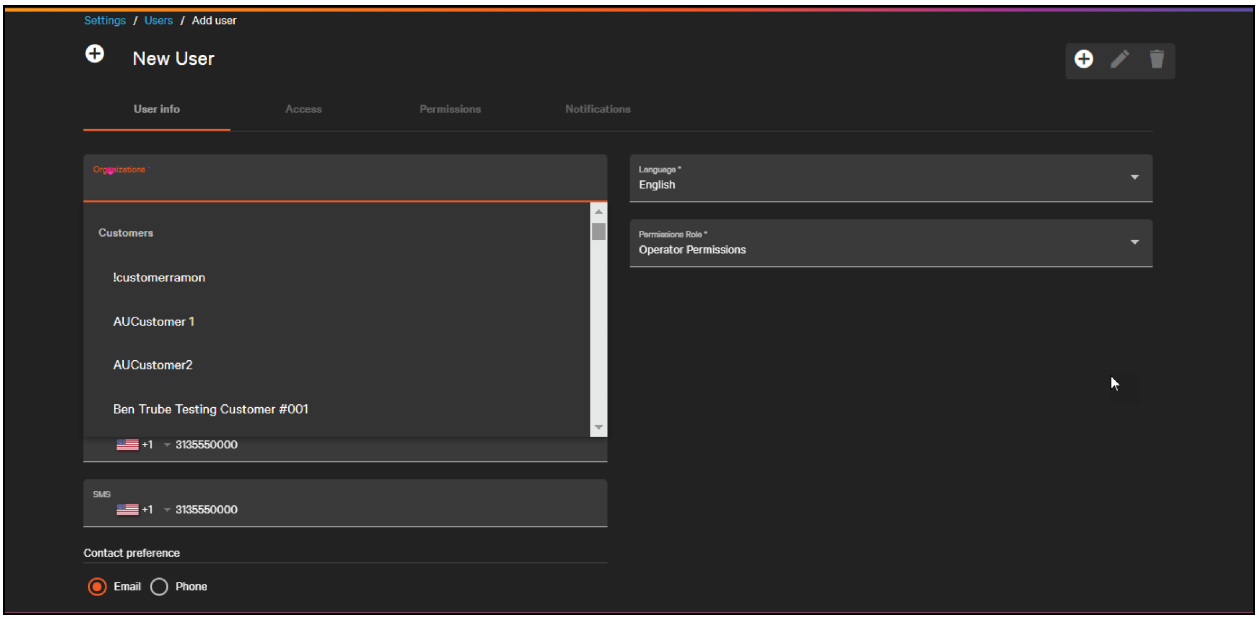


The **User Info** tab contains the minimum information required to create a user.

Table 5.1 Minimum Information Required to Create a User

Information	Description	Required?
Organization	The specific partner or customer in which the new user will be a member of. This can also be Vertiv.	Yes
Username (email)	The username used to access the system. Used to send registration email and other platform notifications, including license expiration and alarm notifications. This must be unique within the system.	Yes
First	The user's first name. Used to personalize emails and to display their name without revealing their username.	Yes
Last	The user's last name.	Yes
Phone	The user's phone number. Used for entering customer contact but is not directly used by the platform to send messages.	No
SMS	Phone number or SMS email for receiving text notifications from the platform. This field is optional and is used when a user wants to receive SMS notifications.	No
Language	Currently only English is supported. Additional language support is to be added in future versions.	Yes
Permissions Role	The user's overall role within their organization. This defines the scope of their responsibility broadly and can be fine tuned on the permissions tab after the user is created. See User Permissions (Capabilities) on page 51.	Yes
Multi-Factor Authentication (MFA)	Method by which the platform will send a multi-factor authentication code.	Yes

Figure 5.3 Organization Drop Down Showing Partners and Customers Grouped

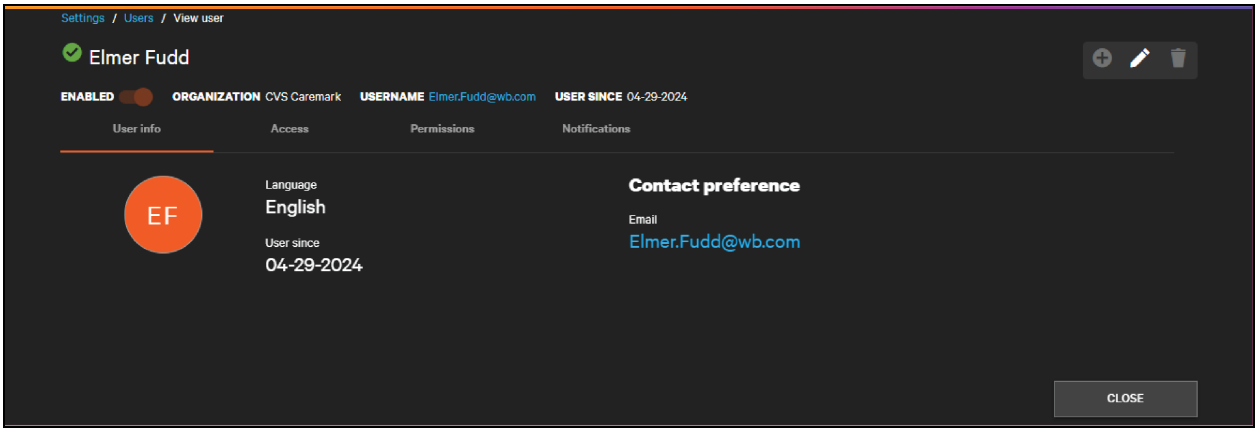


After all required fields are completed, the managing user clicks Save to create the new user. The new user will receive a registration email within a few minutes. See Inviting New Users on page 36.

5.2 View, Update, Delete Users

From any Users list (tab under partner/customer, menu item under Settings), users with the User & Locale Management permission enabled can search for other users within their organization and child organizations they manage. Click the name of a user to see that user's read-only view.

Figure 5.4 Users Read Only View (Info Tab)



The username and organization cannot be changed once the user has been created, but all other fields are editable.

A user can be deleted by clicking on the

Delete icon.

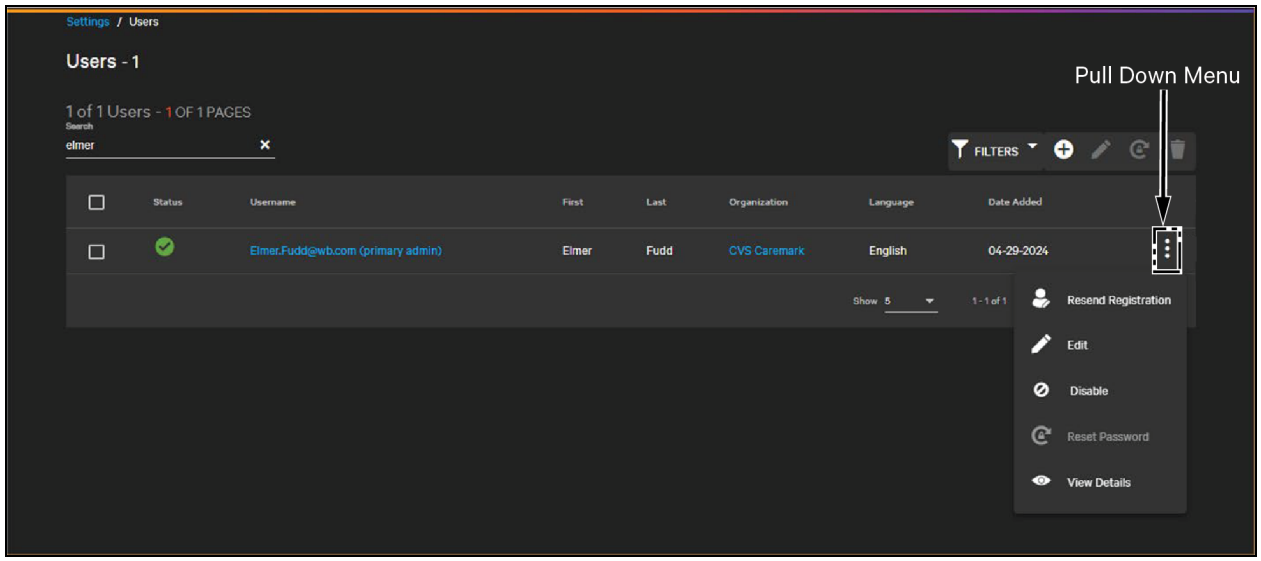
The deleted user will be logged out of any active sessions and will be unable to log back into the system. Any audit logs with entries for that user are maintained. Primary Admin users cannot be deleted to prevent partners and customers from being locked out of the system, but the role can be assigned to other users. See Inviting New Users on page 36.

Users cannot modify their own access or permissions and they cannot delete themselves, but they can modify their own preferences and identifying information. See First Steps on page 8.

The pull down menu shows all available actions that can be taken on a user, including some or all of the following:

- View Details
- Edit
- Disable
- Unlock (only if user is locked)
- Delete
- Resend Invite (available only when user has not completed registration)
- Set as Primary Admin (available only if the user is not already the primary admin, applies to that user's organization only)

Figure 5.5 Pull Down Menu with Available Actions



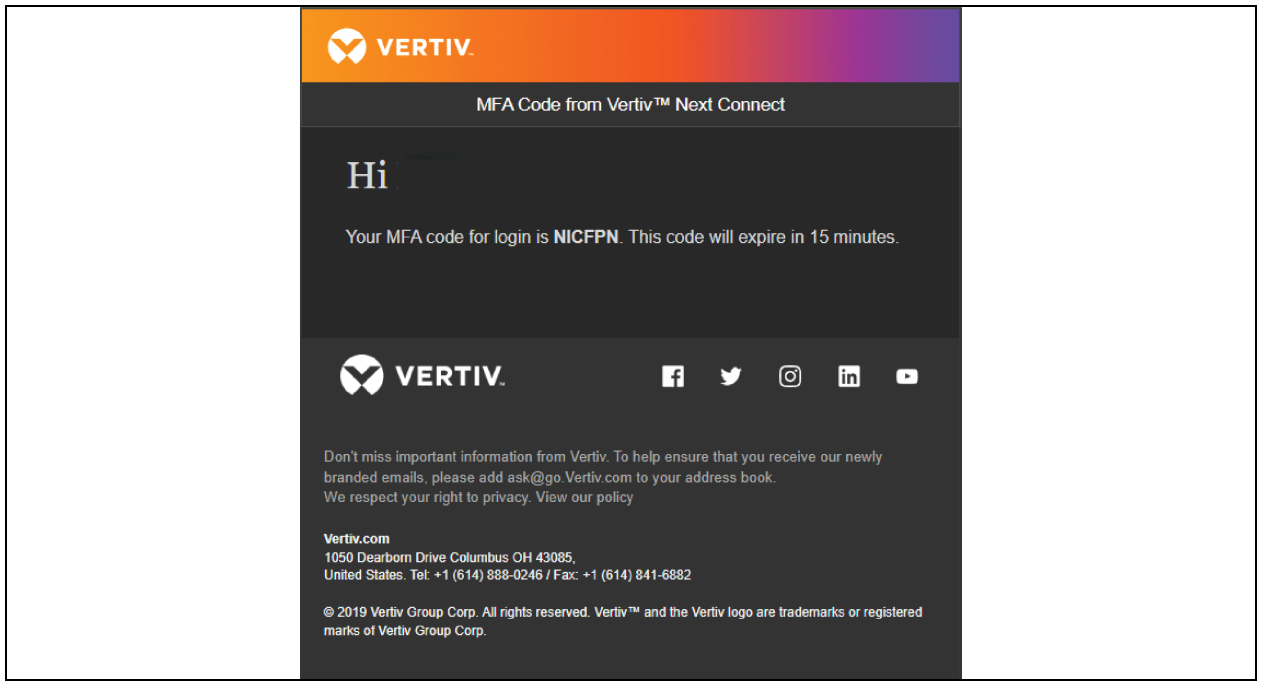
5.3 Multi-Factor Authentication

As of version 1.4, Connect requires two-factor authentication to log into the platform. This consists of a username and password plus a code sent to either email or SMS.

Users can set their MFA code preference by editing their profile. By default, the system will send MFA codes via the email used for the username but can also send a text message to the SMS phone number if preferred.

NOTE: Sending an MFA code via SMS requires an SMS phone number to be specified on the user profile. This is a separate field from the phone number, though it can be the same value.

Figure 5.6 Example of an MFA Code Email

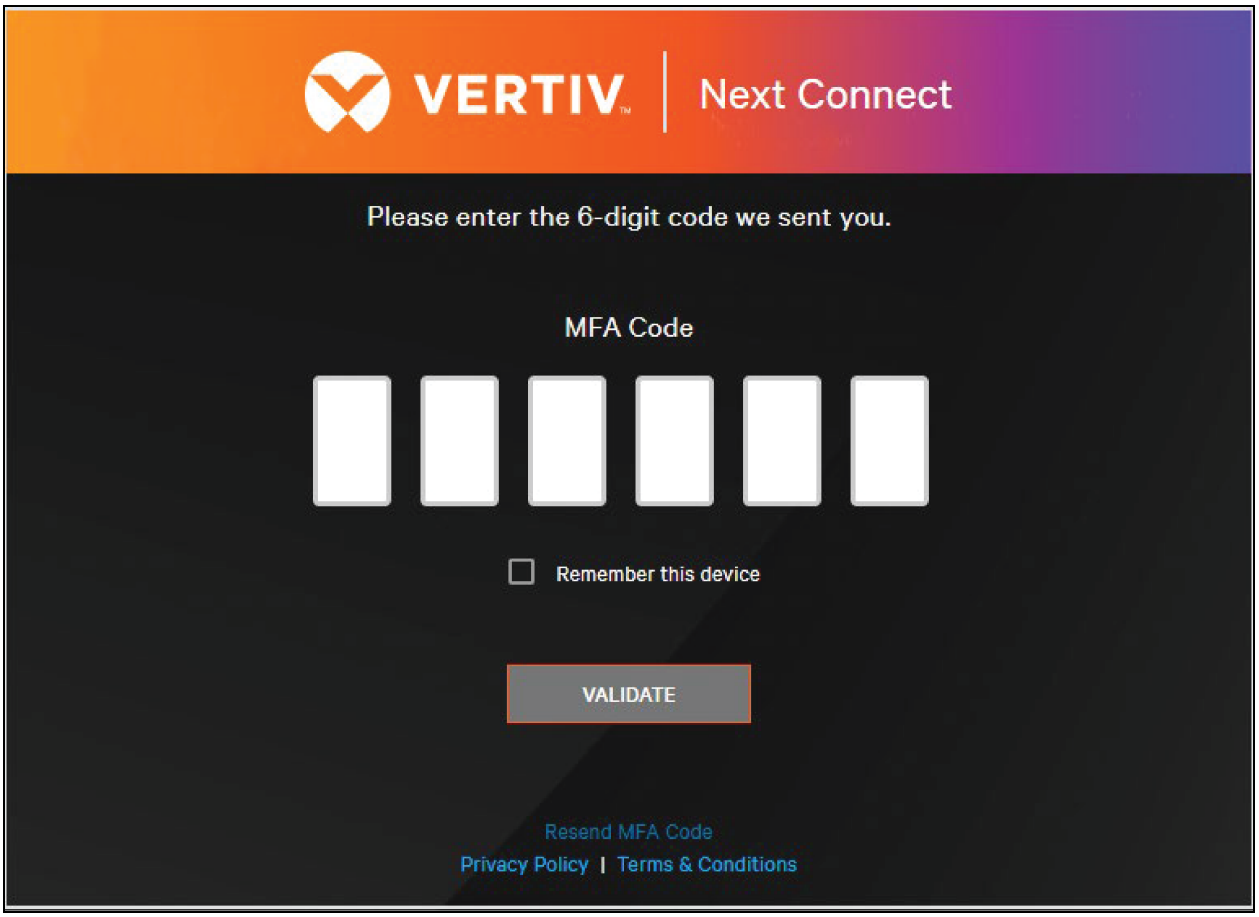


After the user enters their correct username and password, Connect will send a temporary code via the user's preferred MFA method. This code will expire within 15 minutes. The Figure 5.6 above shows an example of an MFA code email.

IMPORTANT! Check your spam folder if you are not receiving the MFA code email as expected.

To complete logging in, copy the code from the email or SMS into the MFA code form and click Validate (see Figure 5.7 on the next page). If the code has expired, or if the SMS or Email has not been received, you can click Resend MFA Code on this form to get a new code.

Figure 5.7 MFA Code Entry Form

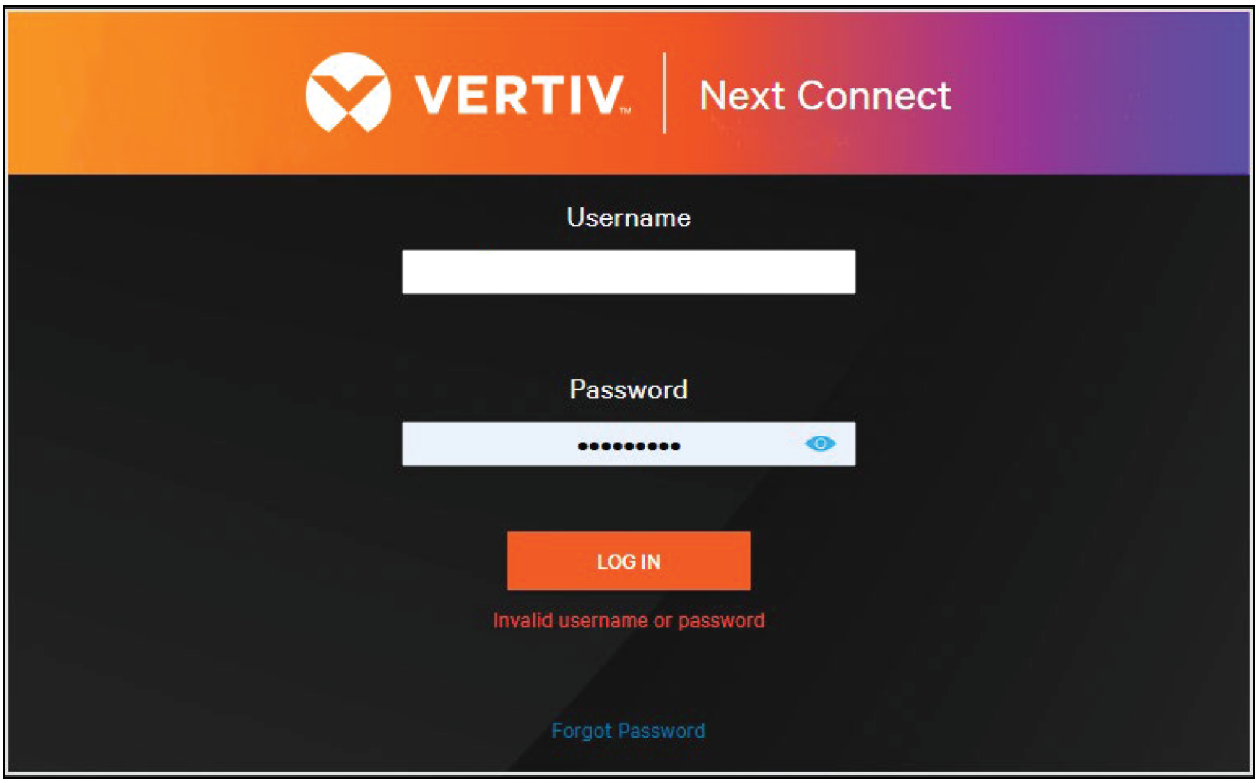


To reduce the number of MFA checks, you can tick the box next to “Remember this device”. This will allow the user to log in without MFA codes for a week.

5.4 User Lockout, Session Timeout

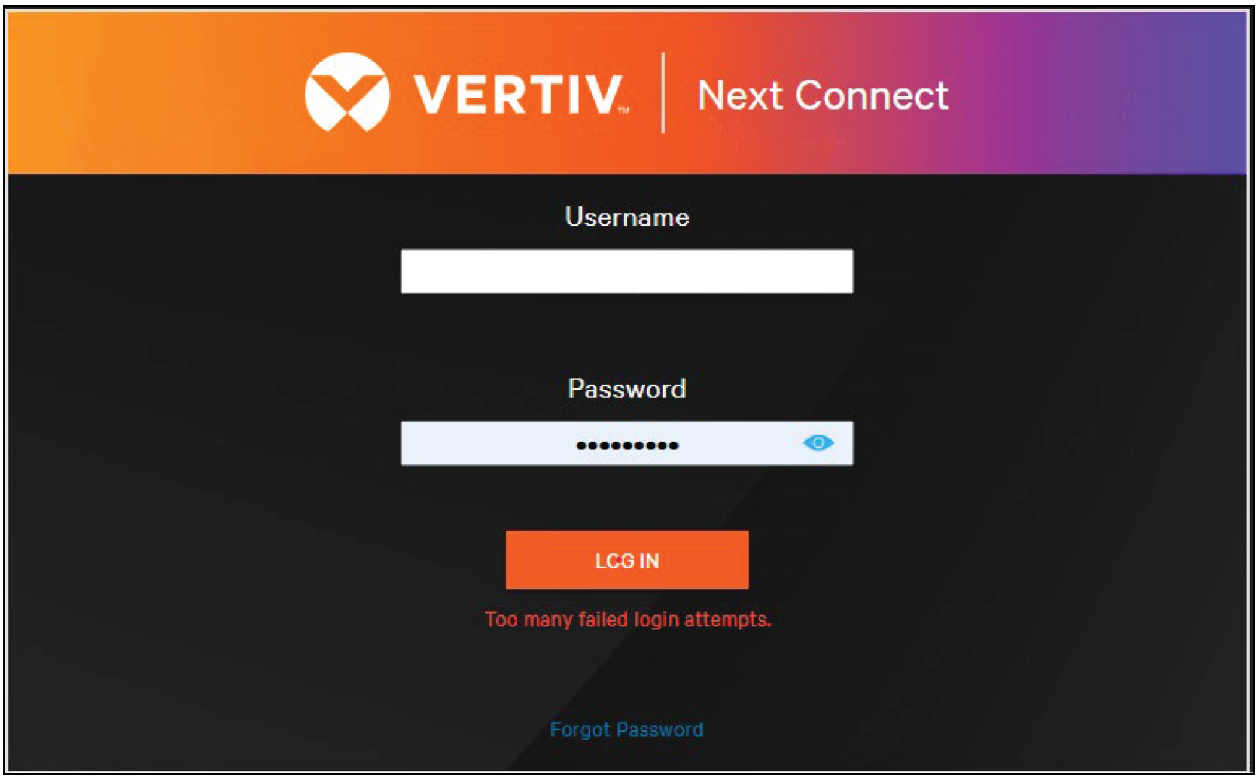
Users are locked out of the Connect platform after three failed password attempts. After the first missed username or password they receive a warning.

Figure 5.8 User Lockout Warning



The system has a lockout timer. After two additional failed attempts the user is locked out of the system for 30 minutes. After the 30 minute timer has elapsed, the user can log back into the system. If they attempt to log back in before the lockout timer has expired, the timer is reset to 30 minutes.

Figure 5.9 User Locked out with Lockout Timer

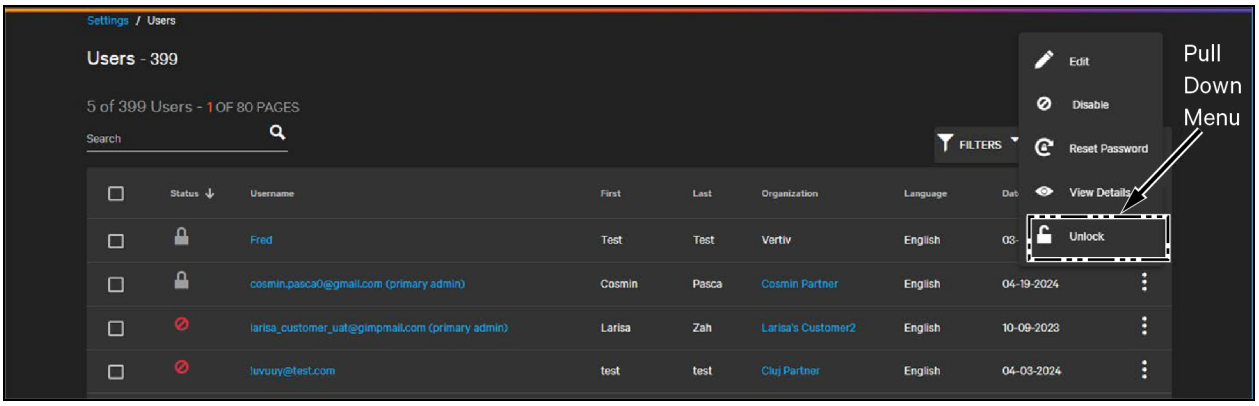


Users with the User & Locale Management permission enabled can unlock their fellow users before the lockout timer has expired.

The status of any user can be seen from the Users list. A user can be one of

- OK/Enabled
- Disabled
- Locked

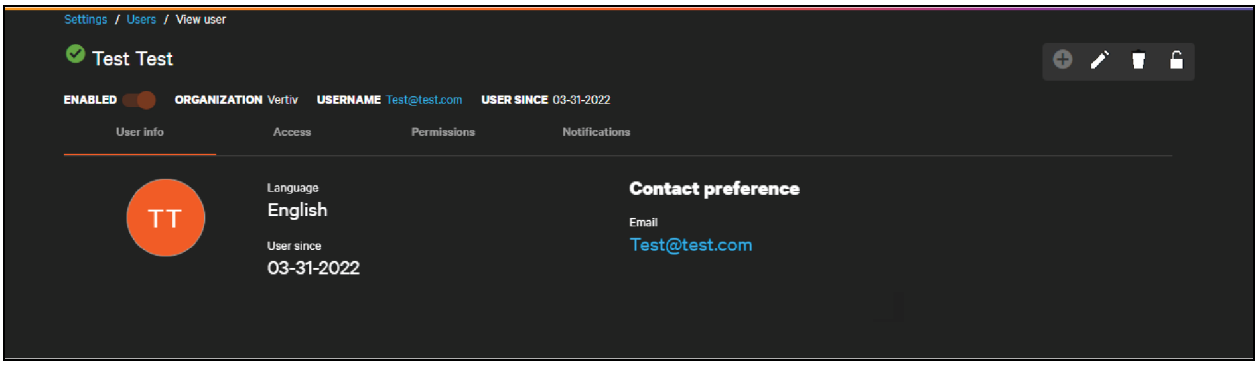
Figure 5.10 User List with Locked User



The Figure 5.3 on page 41 shows the bottom user has been locked out. To unlock this user, click the pull down menu next to that row and click **Unlock** or click the User's details and click the

Unlock icon.

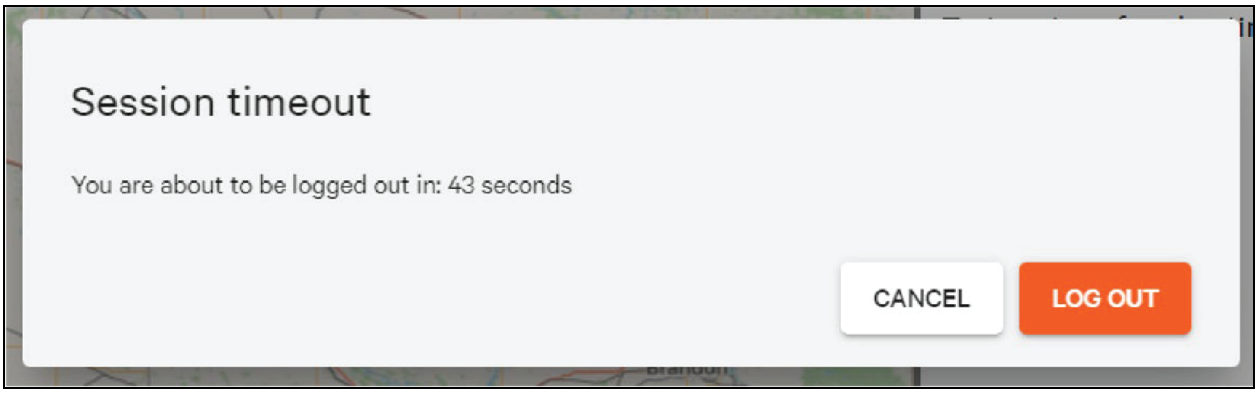
Figure 5.11 Locked User Details



After the user has been unlocked, either manually or automatically, that user can attempt to log back in again. The attempts counter and lockout timer are reset.

An idle user is automatically logged out of the system after a fixed period. A minute before being logged out, the user is given a warning their session is about to expire and can press **Cancel** to resume their session. Otherwise, they are logged out and redirected to the login screen.

Figure 5.12 Session Timeout

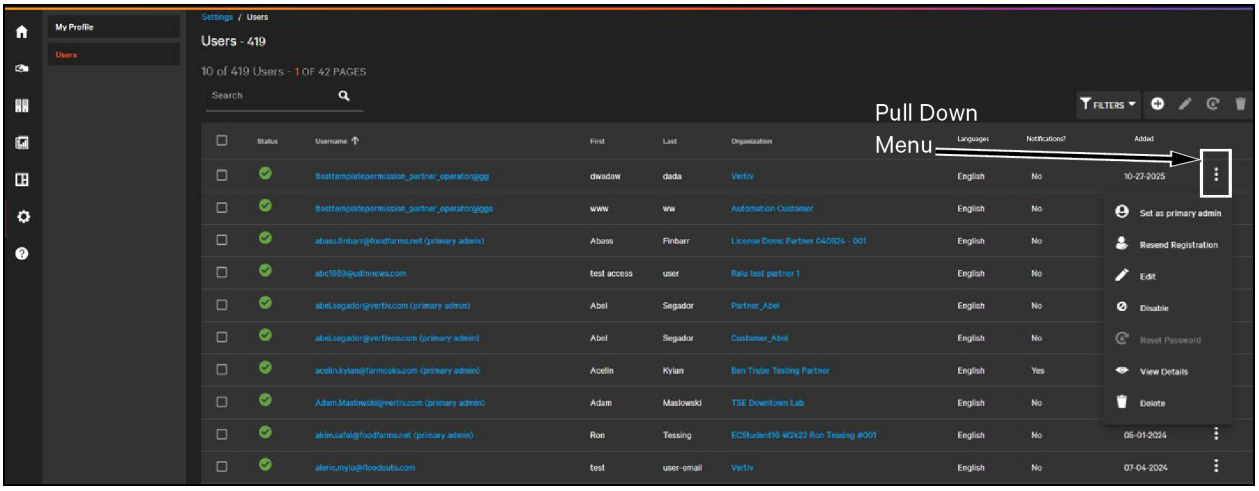


5.5 Disabling and Enabling Users

Disabling a user is a way to temporarily prevent a user from logging into the system without deleting them. It differs from user lockout (see User Lockout, Session Timeout on page 45) in that it is manually applied and removed. Disabled users are unable to log into the system until another user enables them as there is no lockout timer.

Managing users can disable other users by clicking the **Disable** option on the pull down menu.

Figure 5.13 Disabling User in Users List



The status for the disabled user is indicated with a

Disabled icon.

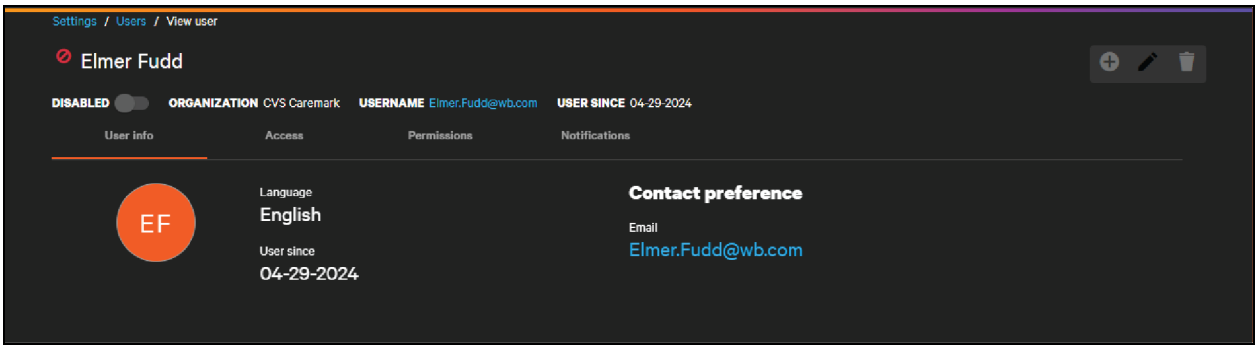
The disabled user can be re-enabled by clicking the

Enable icon

on the pull down menu.

The disable/enable status can also be viewed in the header for the user in two places: the overall status to the left of the user's name, and the disable/enable toggle on the second row.

Figure 5.14 Disabled User Statuses in Read-Only User View (Header)

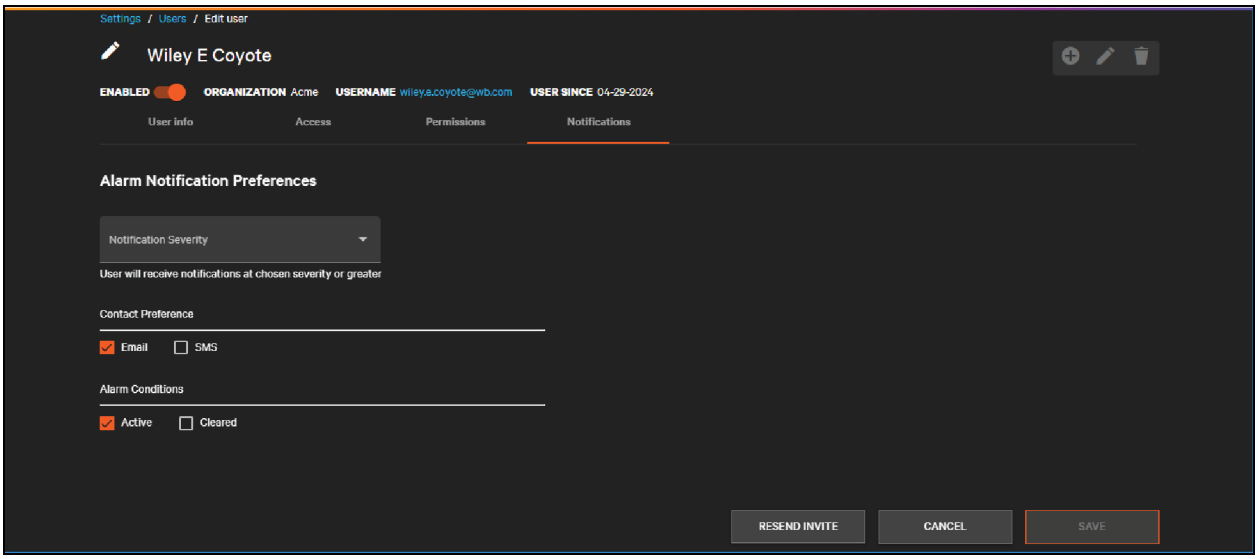


5.6 User Notification Preferences

On the **Notifications** tab, users can set their preferences for when and how they receive alarm notifications. To edit these preferences, click the

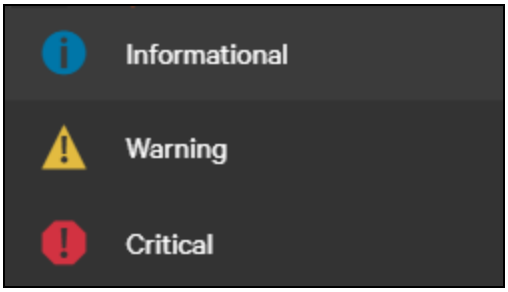
Edit icon.

Figure 5.15 User Notification Preferences



The Alarm Notification Preferences drop down provides choices on how severe an alarm must be before being sent to the user. By default, users are set to **Informational** which sends all alarms—informational severity and above. However, users can change this setting to receive only warnings or critical. **Warnings** will send the user only warnings and critical severity alarms. **Critical** will send the user only critical severity alarms.

Figure 5.16 Notification Severity Preferences



The Contact Preference specifies how alarm notifications are received. This differs from the contact preference on the User Info tab which is intended for service calls. Users can receive alarm notifications by email and/or SMS. If they disable both options, they will not receive any notifications except when logged into the product.

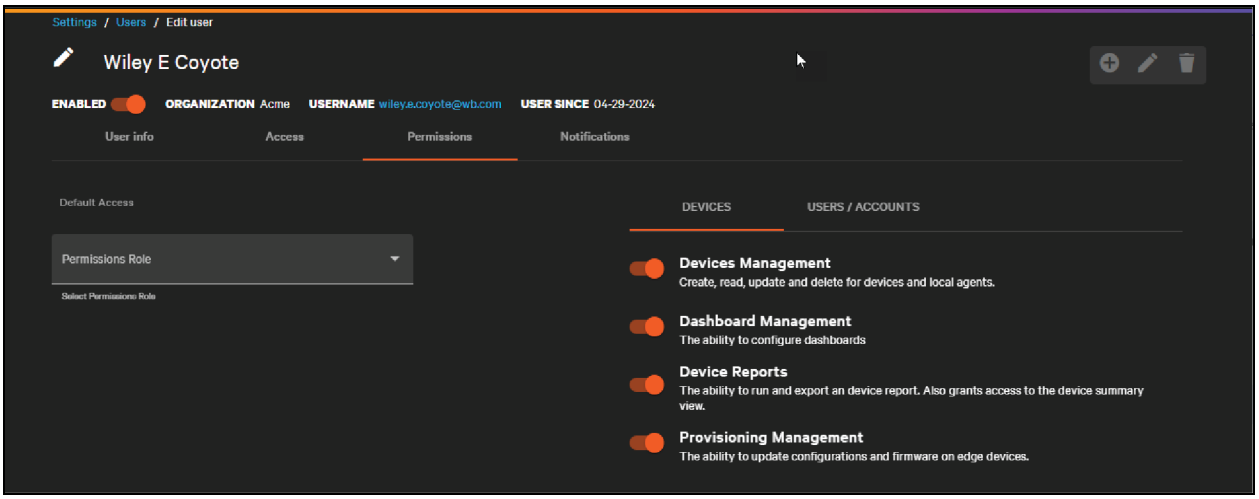
The Alarm Conditions options determine if users will see alarms when they become active, when they are cleared, or both. If they disable both options, they will not receive any notifications except when logged into the product.

Click **Save** to save user notification preferences.

5.7 User Permissions (Capabilities)

When editing or viewing a user, the Permissions tab contains a detailed view of what that user can do within the Connect platform. Some functionality is not available to all types of users (Vertiv, Partners, Customers) and new functionality will be added to the platform in future releases.

Figure 5.17 Permissions Tab (Edit Mode)



Use the toggles to the right to choose or manage what users can do. When first creating a user, choose a role to set the initial values for these permissions. When managing users, manually adjust each individual capability depending on the user's responsibilities.

Switching permissions off may hide functionality within the product. For example, turning off the User & Locale Management permission will hide the users list. Turning off other permissions will disable that permission to a only read-only view.

The current list of permissions is listed in Table 5.2 below.

Table 5.2 Permissions

Permission	Description
Device Management	Allows the user to create devices and local agents. Users without this permission can still view device data, but they cannot change device configurations.
Device Reports	Allows the user to run asset reports which can be exported for use in external tools. See Provisioning on page 143.
Dashboard Management	Allows users to modify partner, customer, site, and asset group dashboards (visual views). Users without this permission can still view dashboards but cannot modify them. **NOTE: This does not apply to the visual view on devices.**
Alarm Management	Allows the user to manually clear alarms. See Manually Clearing Alarms on page 141.
User & Locale Management	Allows the user to create new users within their organization or child organizations. Required for all functionality described in this section. Users without this permission can modify their own user preferences but cannot make other changes.
Account Management	Allows the user to create new partners and customers (Vertiv) or new customers only (Partners). This permission does not apply to customer users.

Table 5.2 Permissions (continued)

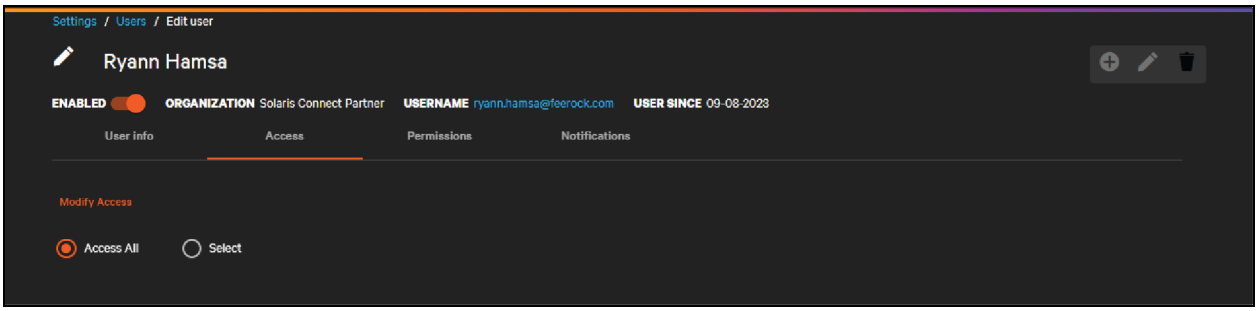
Permission	Description
License Management	Allows the user to directly license partners and customers (Vertiv) or allocate portions of the partner's license to customers (Vertiv, Partners). This permission does not apply to customer users.
Audit Log	Allows the user to view actions taken by other users within the platform. This can include create, delete, edit, disable, enable, log in, log out, and other actions that affect system operation.
Provisioning Management	Allows updates to configurations and firmware of a limited set of Vertiv devices.

5.8 User Access (Scope, Visibility)

When editing or viewing a user, the Access tab contains a detailed view of what that user can see within the Connect platform. This allows managing users to define the scope of other user's access, restricting them to only the partners, customers, sites, groups, and/or devices they manage.

This affects what the user can see throughout the product on maps and lists as well as what notifications they receive. Some actions can be restricted such as deleting entities—a user must be able to access everything affected by a deletion in order to complete the action.

Figure 5.18 User Default Access



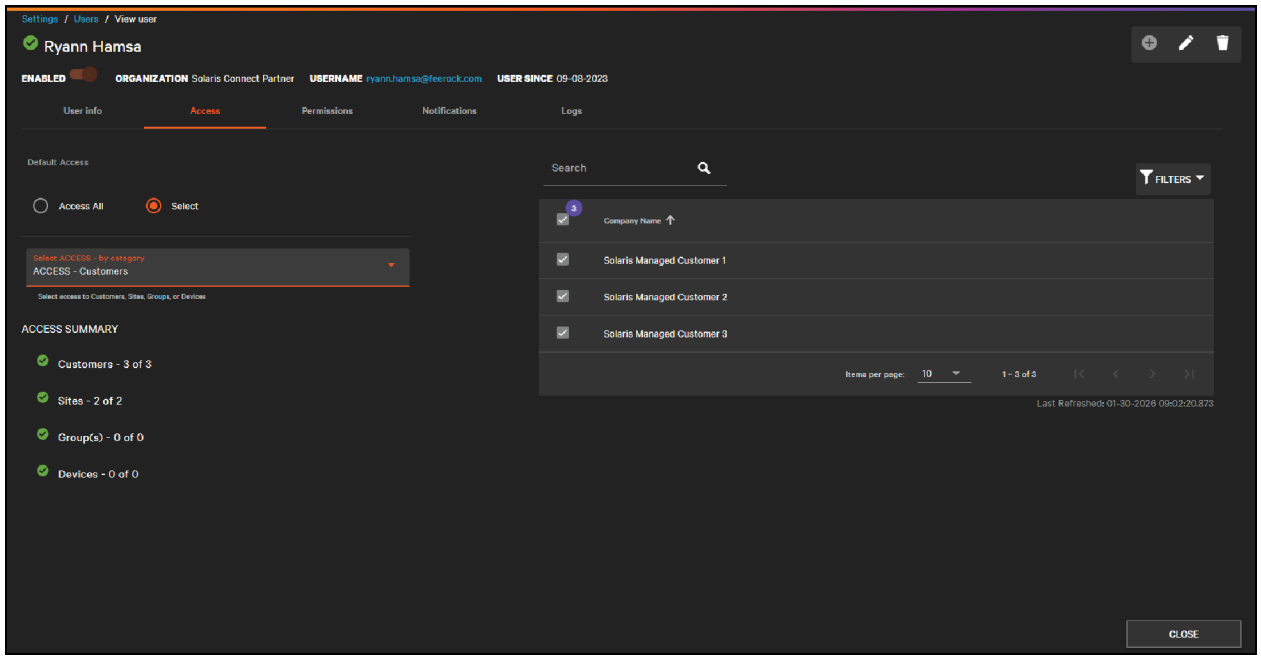
By default, new users can see all entities managed by their parent organization.

- A customer user can see all sites, groups, and devices within their customer
- A partner user can see all customers, sites, groups, devices managed by their partner
- A Vertiv user can see everything in the system.

If new partners, customers, sites, groups, devices are created, the user automatically gets access to them. Users can see but not edit their own access.

When editing a user, a managing user can toggle to the Select option. This gives the ability to select only the partners, customers, sites, groups, or devices that the user can access.

Figure 5.19 Selecting the Type of Entity for Editing Access



From the drop down the managing user can choose to edit partners (Vertiv only), customers (Vertiv and Partners only), sites, groups, or devices. This brings up a list of all entities accessible to the logged-in user.

Figure 5.20 Selecting Which Customers a User Can Access

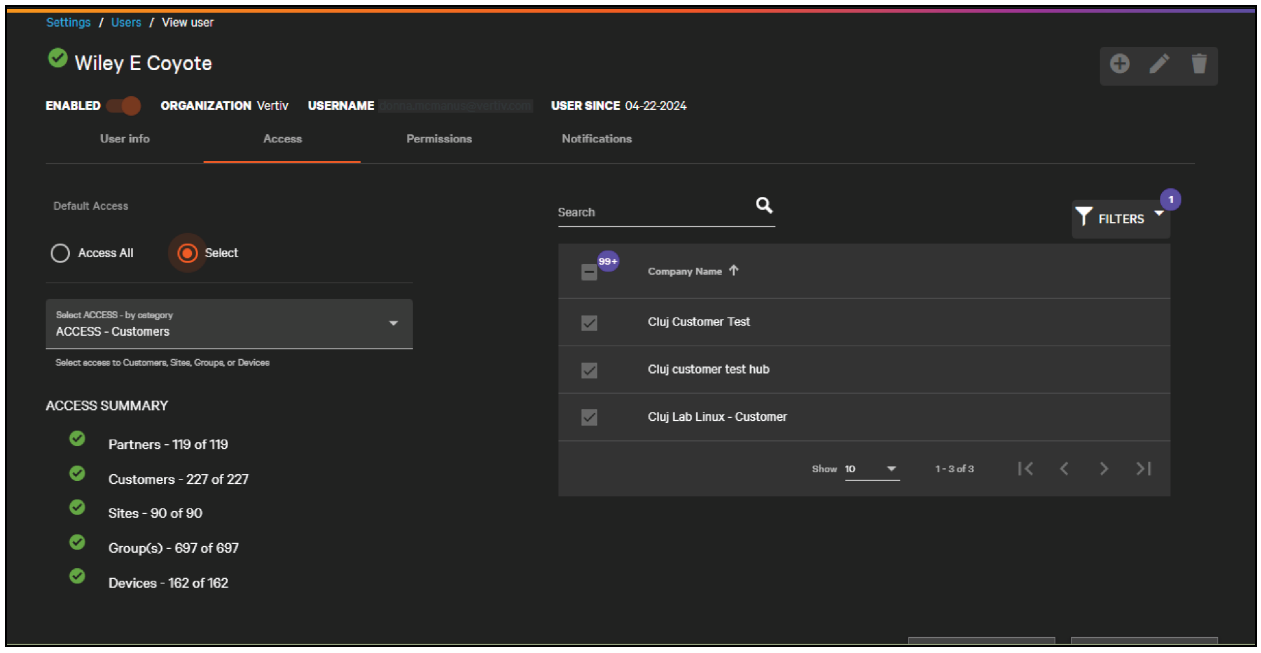
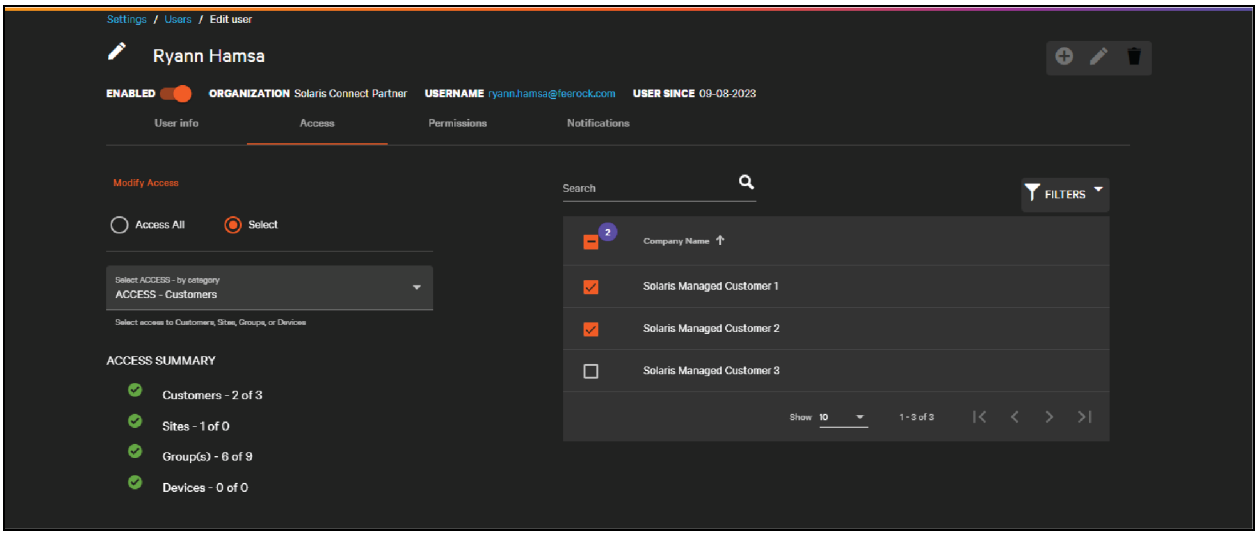


Figure 5.20 above shows that Customers are selected from the category drop down. If one of the customers is unselected, access is removed not only from that customer but also from any sites, groups, and devices contained within that customer. A summary of the user's full access is shown on the left hand side.

Figure 5.21 Access to Customer Removed



Managing users can edit access at any level, but if they grant access to a child entity, access to the parent will be granted as well.

For example, if the managing editor first edited customers and removed Customer 2, this would remove access to all the sites, groups, and devices in Customer 2. If they then edit sites and add visibility to a site that is part of Customer 2, then access to Customer 2 is also added, but not access to all other sites, groups, devices that are within Customer 2.

If a partner user is restricted to one or more customers, they will not get access to new customers added to the partner automatically. If no additional restrictions were placed on the sites, groups, devices under the customers they can access, then they will see any new sites, groups, devices that are added to those customers.

6 Installing the Local Agent

Next Connect communicates with devices through a software local agent installed in the customer network. The agent needs to be able to communicate both with the device network to poll data and provision devices and with the internet to send data to the Connect cloud.

The Windows and Linux agents are based on Microsoft's Azure IoT Edge. See https://learn.microsoft.com/en-us/azure/iot-edge/support.

Azure IoT Edge handles the authentication of each agent and sends data to the Connect cloud. Data is collected within the customer network via SNMP (v1, v2c, or v3). The agent supports polling of device data as well as receiving and processing traps/informs from devices.

A single agent can collect data for approximately 800 devices, assuming 100 datapoints per device. For larger customers, multiple agents need to be installed, each on their own dedicated virtual machine (VM) or “bare metal” hardware.

If connectivity is lost, a local agent will continue to poll devices and receive traps, caching that data for transmission to the cloud once connectivity is restored.

6.1 Network and Firewall Requirements

This section outlines required network and firewall configurations that are necessary for successful deployment and operation of the Next Connect Local Agent. Proper configuration ensures communications between the Local Agent, monitored devices and the associated Next Connect Cloud Service.

To maintain proper operations the following network ports must be open and the designated cloud service endpoints must be reachable through the organization’s firewall.

The following table defines inbound and outbound ports that are necessary for communication between the monitored devices and the Local Agent.

Table 6.1 Required Ports for Local Agent Communication

Port	Protocol	Transport	Description
0	ICMP	ICMP	Open to allow network connectivity verification over ICMP.
161	SNMP	UDP	Open to allow connectivity to SNMP based targets and clients.
162	SNMP	UDP	Open to send and receive SNMP traps.
22	SSH	TCP	Open to allow SSH sessions to appliance.
80	HTTP	TCP	• Open to allow internet access to Next Connect portal. • Open to allow monitoring device discovery. • Open to allow communication to monitoring device communication card. • Open to allow provisioning of monitoring device card firmware. • REST-HTTPS for Sending Commands.
443	HTTPS	TCP	• Open to allow web user interface. • REST-HTTPS for Sending Commands.
21001	HTTPS	TCP	Local Web Application.
5671	AMQP	TCP	• Open for Azure IoT Hub.

Table 6.1 Required Ports for Local Agent Communication (continued)

Port	Protocol	Transport	Description
			• Open for sending device data. • Open for Blob Storage Connection for Device Configuration.
8883	MQTT	TCP	• Device provisioning and communication with Azure IoT Hub. • Azure provision certificate. • Receiving Commands. • Sending results. • Heartbeats.
6687	Geist™ Discovery Protocol	UDP	Geist™ device discovery protocol.

The following table lists outbound endpoints that are required for the Local Agent to communicate securely with the Next Connect Cloud service. These endpoints will need to be configured for outbound communications on your organization's firewall.

Table 6.2 Outbound Firewall Endpoints for Cloud Connectivity

Service	Endpoint	Transport	Port Number	Description
IoT Hub MQTT / AMQP / HTTPS	*.azure-devices.net	TCP	8883,5671,443	Used for all IoT Hub communications
Device Provisioning Service (DPS)	*.azure-devices-provisioning.net	TCP	443	Used during initial registration / reprovisioning
Azure Edge Agent / Hub updates	mcr.microsoft.com and *.data.mcr.microsoft.com	TCP	443	Microsoft Container Registry (MCR) — IoT Edge runtime modules
Azure Container Registry	*.azurecr.io	TCP	443	Used for pulling custom container images
Application specific API's	https://stfdtnpublicprdeastus002.blob.core.windows.net https://stfoundationprdeastus002.blob.core.windows.net https://next-connect.vertiv.com/* https://next-connect-api.vertiv.com/*			

6.2 Downloading the Agent

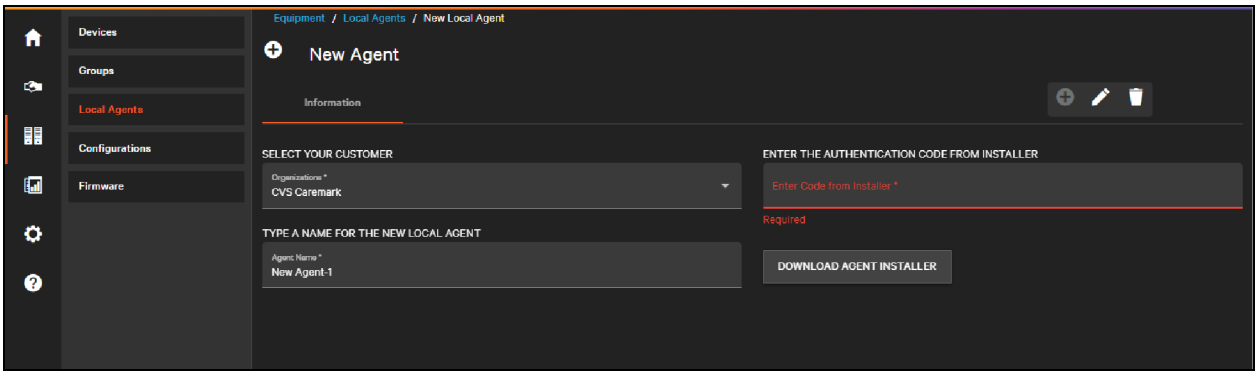
You can download the Windows and Linux Agents from the Download Agent Installer button in the Welcome banner. You can also download the installer by navigating to the Local Agent list (under the Equipment menu), then clicking the

Add icon

to add a new agent.

The New Agent dialog opens. From this dialog, click the **Download Agent Installer** button to download the agent.

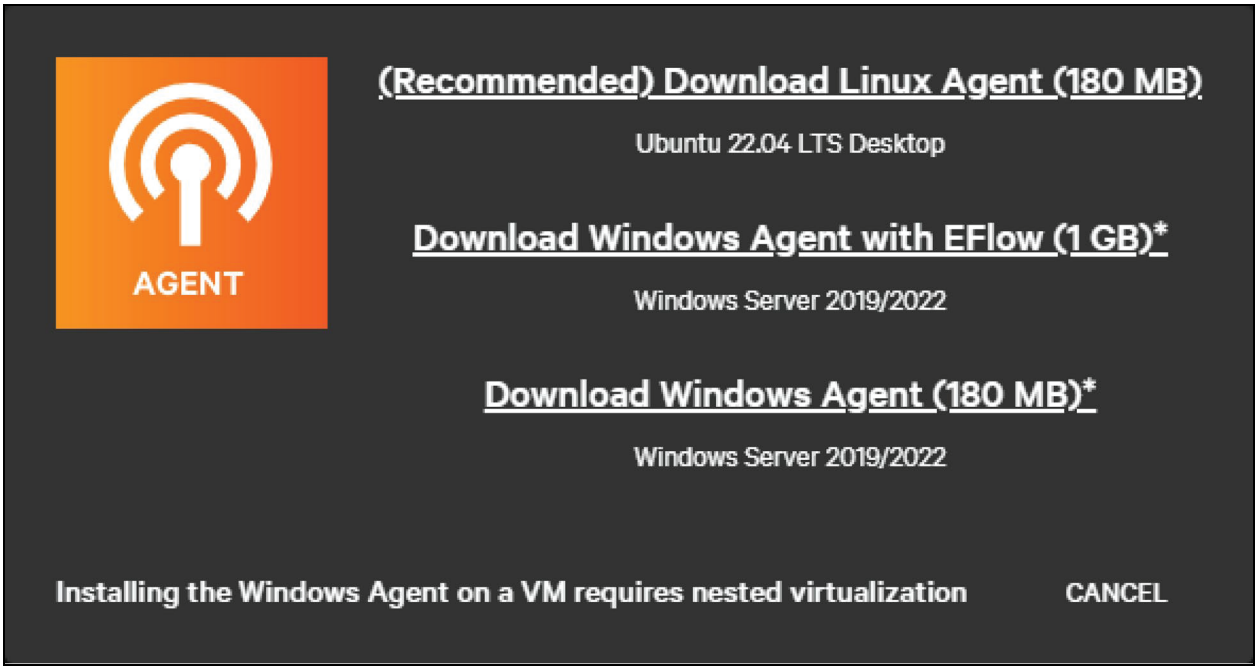
Figure 6.1 New Agent Dialog



Clicking the download button opens a dialog with links to the Windows and Linux versions of the installer. The Windows Agent requires a component called Edge for Linux on Windows (EFlow). Because of this, the download page offers two options for the Windows Agent. Both installers use EFlow and result in the same installation.

1. **Download Windows Agent.** This link downloads the latest EFlow during the installation process.
2. **Download Windows Agent with EFlow.** This link includes EFlow embedded in the installer.

Figure 6.2 Agent Download Links



Internet access is required to install the agent and receive updates, and for the agent to send data to the Next Connect platform.

IMPORTANT! Installing the Windows Agent on a virtual machine requires nested virtualization. Because of this, we recommend using the Linux agent if supported in your organization.

6.3 Windows Installation

6.3.1 System Requirements

The Windows Agent has the following minimum system requirements:

Table 6.3 Windows Agent Minimum Requirements

Requirement		Detail
Operating System	Windows 11 Enterprise or Server 2019/2022	All Windows operating systems must be minimum build 17763 with all current cumulative updates installed.
Hardware	Memory	• Minimum Free Memory: 2 GB, 4 GB recommended. Memory used exclusively by the agent process. • Total Minimum Memory: 4 GB, 8 GB recommended. Total memory required for the VM or bare metal machine (based on OS minimum + agent minimum).
	Disk Space	• Minimum Free Disk Space: 27 GB, 60 GB recommended. Disk space used exclusively by the agent. • Total Minimum Disk Space : 60 GB, 100 GB recommended. Size of virtual or physical hard drive used by the OS and installed agent.
	CPU Cores	2+ Intel Xeon CPU E5-2673 v3 at 2.40 GHz or equivalent

A dedicated VM or physical hardware (“bare metal”) is recommended for the agent installation.

The following host hypervisors are supported as of this writing:

- Microsoft Hyper-V
- VMWare ESXi

Other hypervisors may be supported in later releases.

NOTE: Broadcast discovery may not be available in all environments. As of this writing broadcast scans are unavailable on Azure hosted virtual machines.

Hyper-V Host Hypervisor Additional Setup

If you are using Hyper-V as the host hypervisor for Windows, you will need to enable nested virtualization by running the following PowerShell Command on the host machine:

```
Set-VMProcessor -VMName <VMName> -ExposeVirtualizationExtensions $true
```

To route network packets through two virtual switches, you must enable MAC address spoofing on the first (L1) level of the virtual switch. You can do this with the following PowerShell Command on the host machine:

```
Get-VMNetworkAdapter -VMName <VMName> | Set-VMNetworkAdapter -MacAddressSpoofing On
```

NOTE: The Windows Agent also uses Hyper-V for configuring EFlow, a dependency of IoT Edge in the Windows environment.

VMware ESXi Host Hypervisor Additional Setup

If you are using VMware ESXi as the host hypervisor for Windows, you'll need to enable hardware virtualization, enable CPU performance counters, and adjust your networking to allow for promiscuous mode.

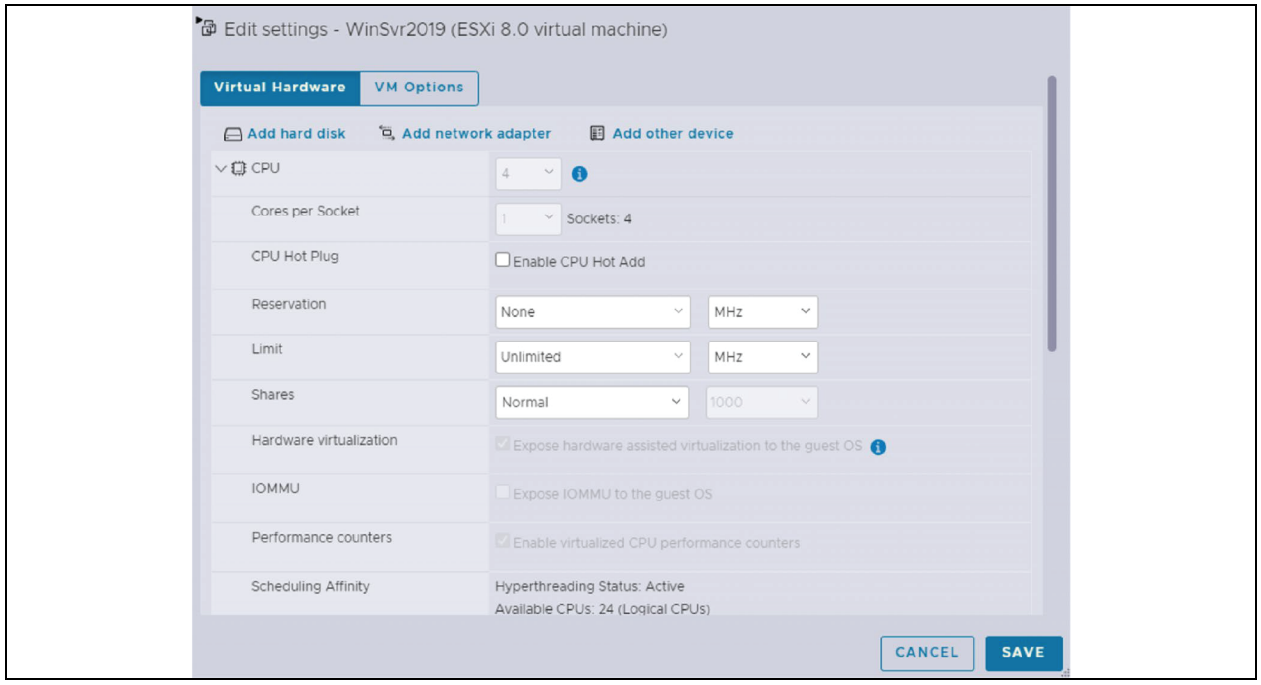
Step 1: Enable Hardware Virtualization and Performance Counts

1. From the ESXi dashboard, navigate to the virtual machine for your agent and power it off.
2. After the VM has shutdown, edit the virtual machine settings.
3. Expand the CPU menu and select **Hardware virtualization** and **Performance counters**.

NOTE: These settings cannot be changed while the VM is running.

4. Click **Save** to save changes.

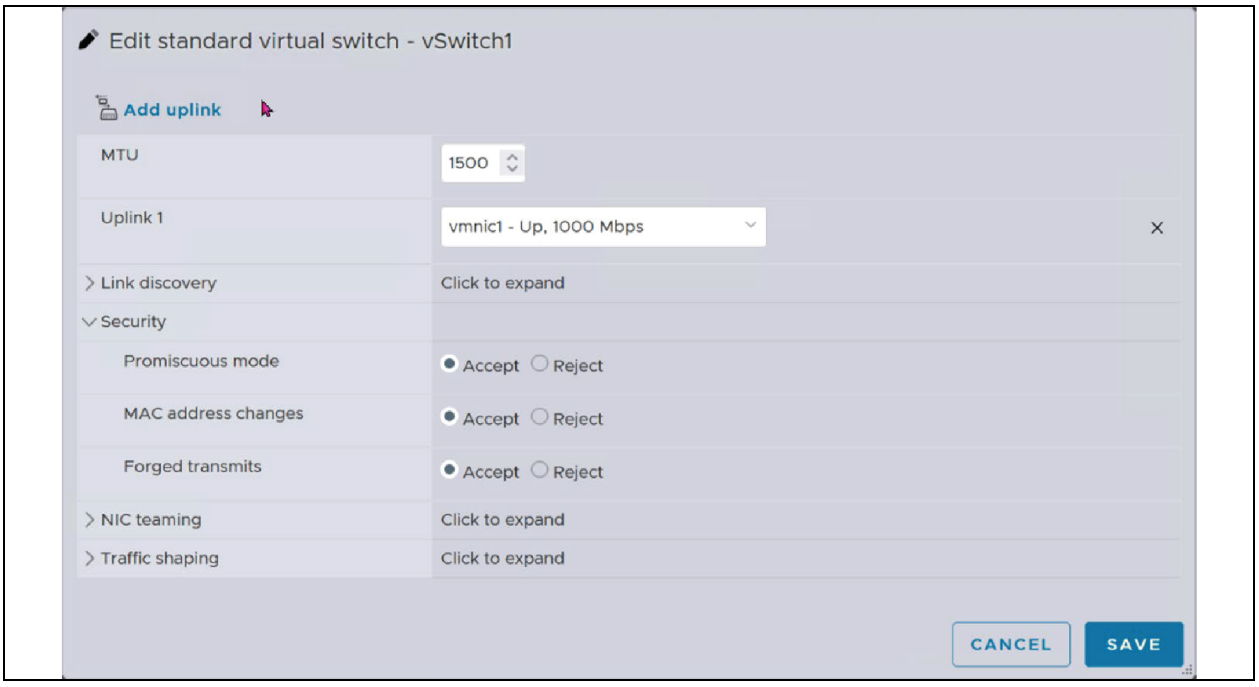
Figure 6.3 Edit VM Settings



Step 2: Enable Promiscuous Mode and Related Settings

1. Select the virtual switch(es) used for the agent.
2. Expand **Security** and select **Promiscuous mode**, **MAC address changes**, and **Forged transmits**.
3. Click **Save** to save the changes.

Figure 6.4 Edit vSwitch Settings



Step 3: Power on the Virtual Machine after all Changes Have Been Saved

6.3.2 Installation Steps

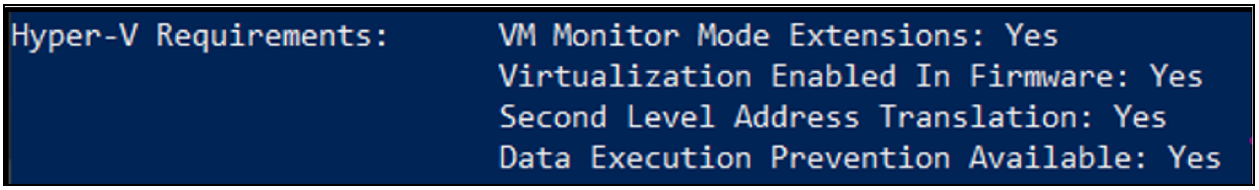
Installation Preparation

Validate that the OS is Hyper-V capable by opening a PowerShell and running the following command:

```
systeminfo
```

This produces a report on the system's capabilities. The Hyper-V section is near the bottom of the report and look like the following:

Figure 6.5 Hyper-V Section of System Info Report



If all requirements say Yes, then Hyper-V can be installed on the machine. If not, review the additional setup requirements for System Requirements on page 58.

Powershell Script Execution

The Windows Local Agent installer needs execution rights to run Powershell scripts. By default the execution policy is set to Restricted which prevents running any script on the system.

Use the following Powershell command to permit running only scripts that are digitally signed.

```
Set-ExecutionPolicy -ExecutionPolicy AllSigned
```

Prerequisite Check

After running the installer and clicking next, the Local Agent will run a check of your machine's prerequisites to confirm that the agent can be installed. Assuming that all checks pass you can proceed to the next step.

If any checks fail, refer to the troubleshooting guide for uninstalling a previous installation attempt or resize your agent's VM.

Network Configuration

The next step of the Windows installation process is network configuration. This involves the following:

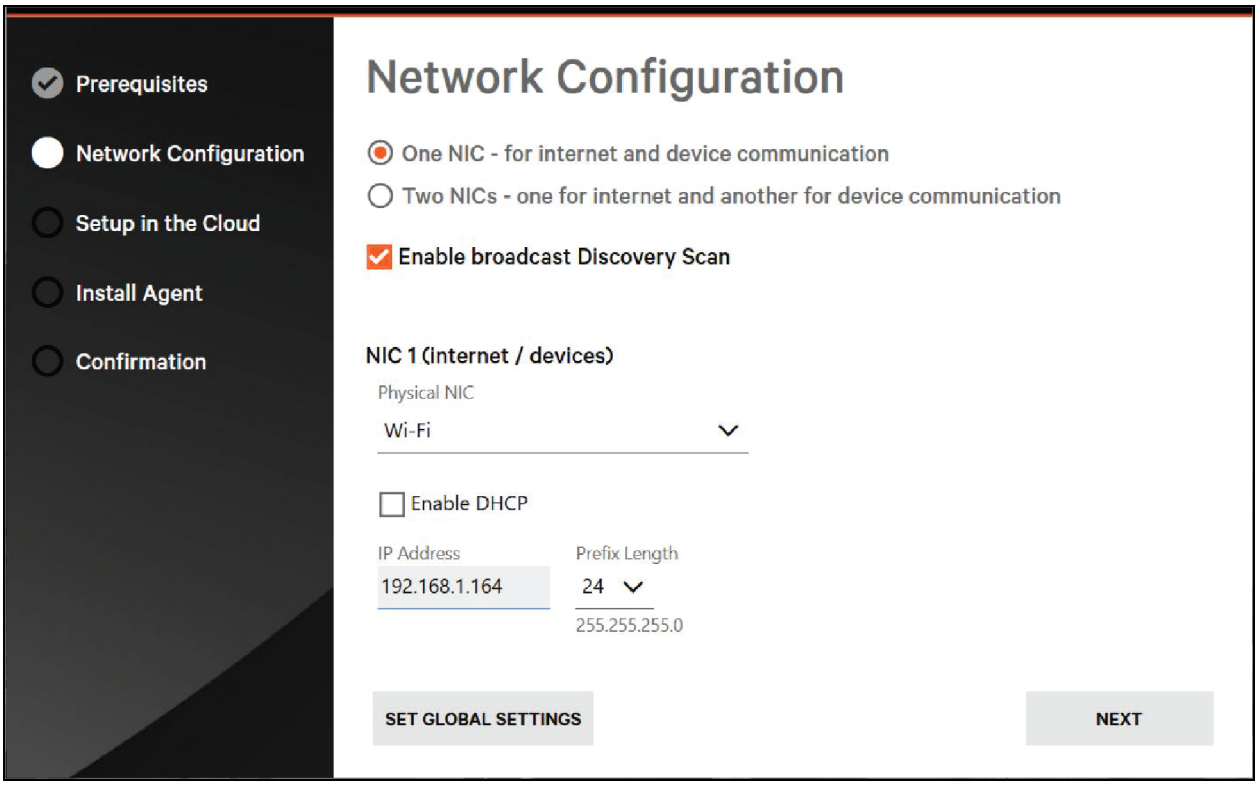
- Selecting your network configuration (One NIC or Two NIC).
- Enabling or disabling broadcast discovery scans.
- Specifying the physical NICs for the selected networking configuration.
- Creating IPs for the agent (static or DHCP).
- Confirming default gateway and DNS settings.

Step 1: Select a Network Configuration

Depending on the networking configuration of the machine being used for the agent, you may choose either a one or two network interface card (NIC) setup.

- In a one NIC setup, devices can be found on the same network that can also be used to access the internet.
- In a two NIC setup, devices can be on a different network from the one used to access the internet. In this case, the agent has two static IPs: one on the device network and on the internet accessible network.

Figure 6.6 One NIC Configuration



Step 2: Enable or Disable Broadcast Discovery Scans

By default, broadcast scans are enabled. This allows the agent to find devices that may have default or unconfigured IPv4 addresses. This also can be used to find configured devices without specifying an IP range. It is recommended that you enable Broadcast scans unless your network specifically does not support broadcast.

NOTE: If you do not enable broadcast scans, the agent is unable to receive traps from edge devices.

Step 3: Select Physical NICs for the Device and/or Internet Networks

Figure 6.7 Two NIC Configuration

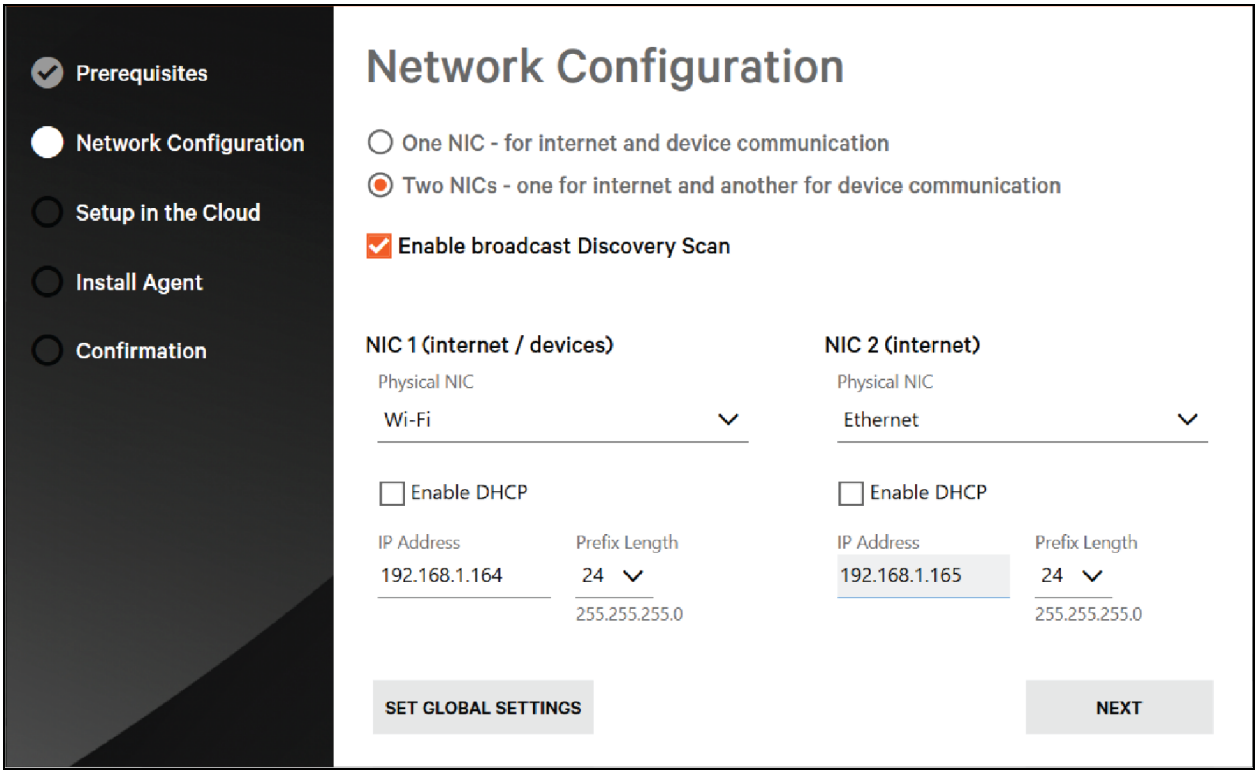


Figure 6.7 above shows the two NIC network configuration. The drop downs below Physical NIC include network interfaces that the installer has detected. In either the one or two NIC configuration, the first NIC should be the network that can communicate with devices.

With a one NIC setup, this also is the NIC that communicates with the internet. In a two NIC setup, the second NIC is reserved for communicating with the cloud and IPv4 address.

NOTE: WiFi adapters are not recommended for the Windows agent. This configuration may encounter an error when installing.

Step 4: Select IP Address(es) for the Agent

When broadcast is enabled, the agent requires an IPv4 address on the customer network for each NIC. If the network has a DHCP server, the agent can be auto-assigned an address by ticking the box next to “Enable DHCP.” Enabling DHCP will fail to assign an address to the agent if DHCP is not enabled on the selected network.

NOTE: The IPv4 address of the agent cannot be the same IPv4 address as the host machine.

Alternatively, you can specify static IPv4 address(es) and subnet(s), in prefix format, for the agent, one for each NIC.

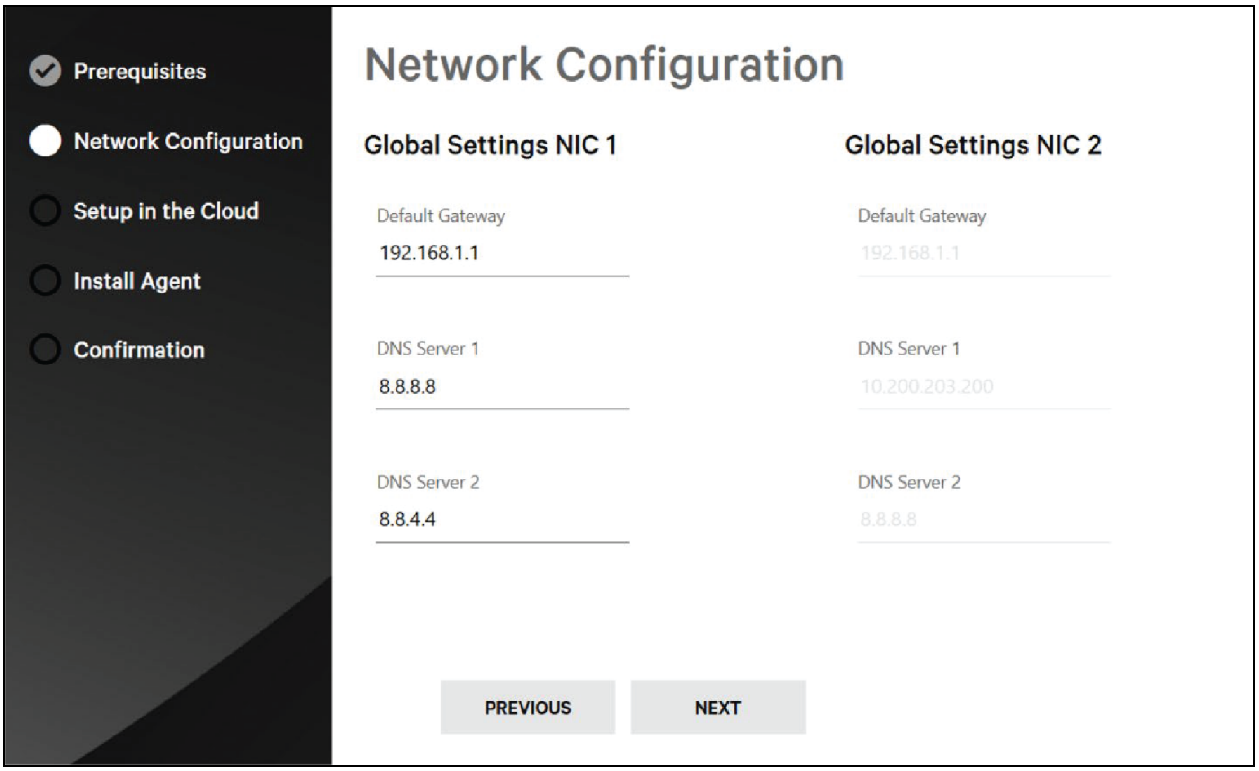
IMPORTANT! In a two NIC setup, each IPv4 address must be unique.

NOTE: For further information on the prefix format, refer to this article: https://www.routerfreak.com/understand-subnet-masks/.

Step 5: Confirm Default Gateway and DNS Settings

After completing Steps 1 through 4, click **Next** to go to the Global Settings dialog.

Figure 6.8 Global Settings

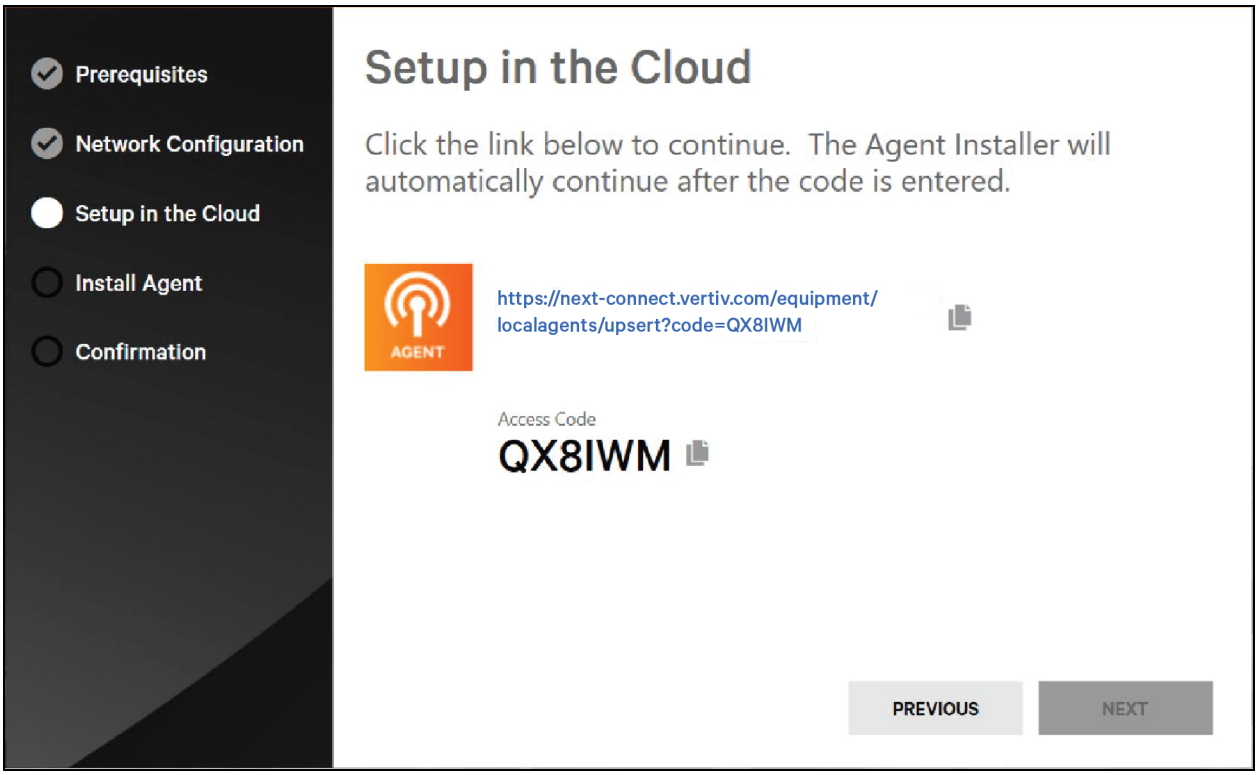


The Default Gateway and DNS servers are auto detected by the installer based on the physical NIC(s) selected in Step 3. These settings can be confirmed or modified on this page. You can also go back to the previous network configuration screen to make adjustments. Once all networking settings are as desired, click **Next** to continue with installation by registering the agent.

Registering the Agent

The next step is to register the agent with the Connect Cloud. This does require that you already have a login for Connect and a Customer in place to associate with the agent.

Figure 6.9 Code for Authorizing the Agent

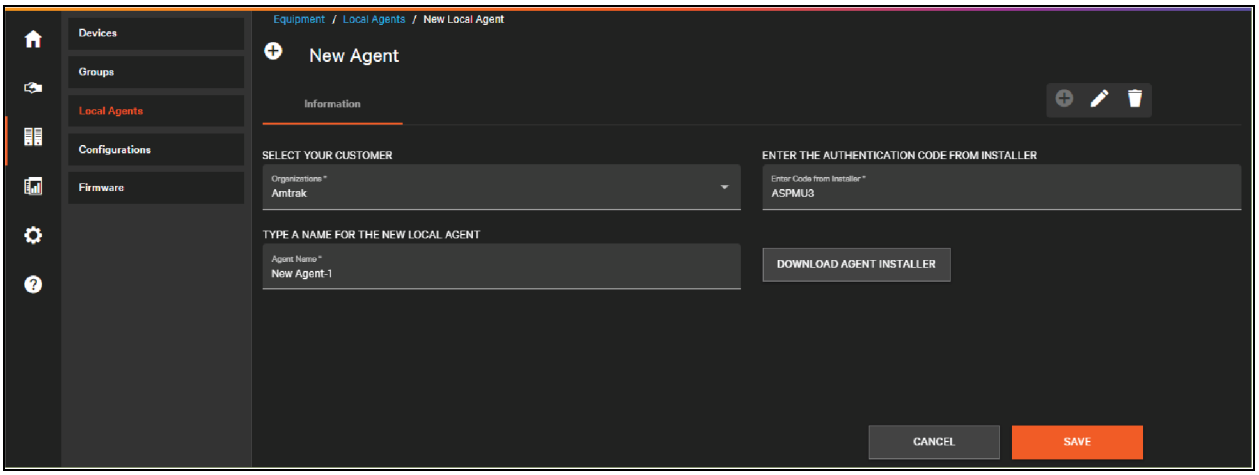


The installer will generate a temporary registration code.

IMPORTANT! This code is valid for 15 minutes. If it expires you will need to restart the installation process.

Click the link in the installer to be automatically directed to the Connect platform. Login and then you are directed to the New Agent dialog. The code is auto filled when the link is clicked but you can also copy and paste it from the installer.

Figure 6.10 New Agent Dialog with Code

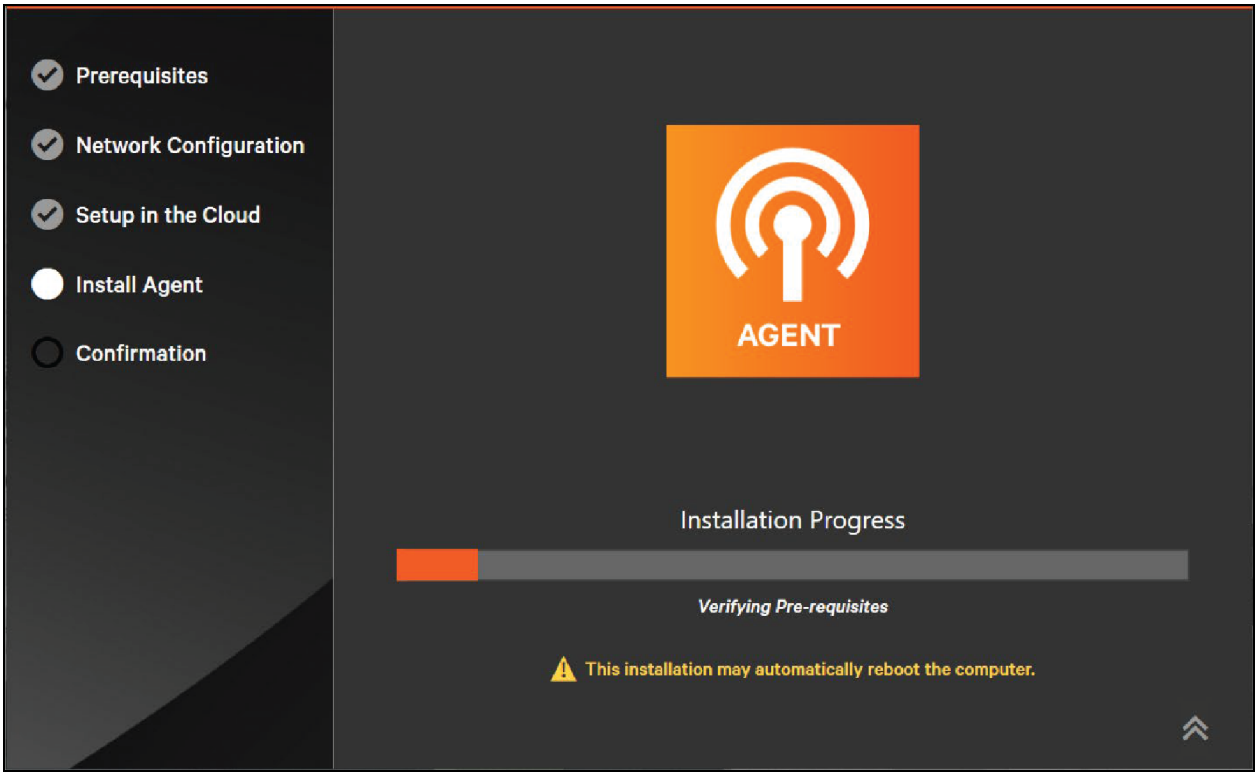


Select the customer from the drop down in the top-left of the new agent dialog (if not auto-filled). Choose a memorable name for the agent and confirm the code matches what you see in the installer. Once you click **Save**, the agent is created in the cloud, and the installation will automatically continue after a few moments.

Installing Pre-requisites, Configuring Switches

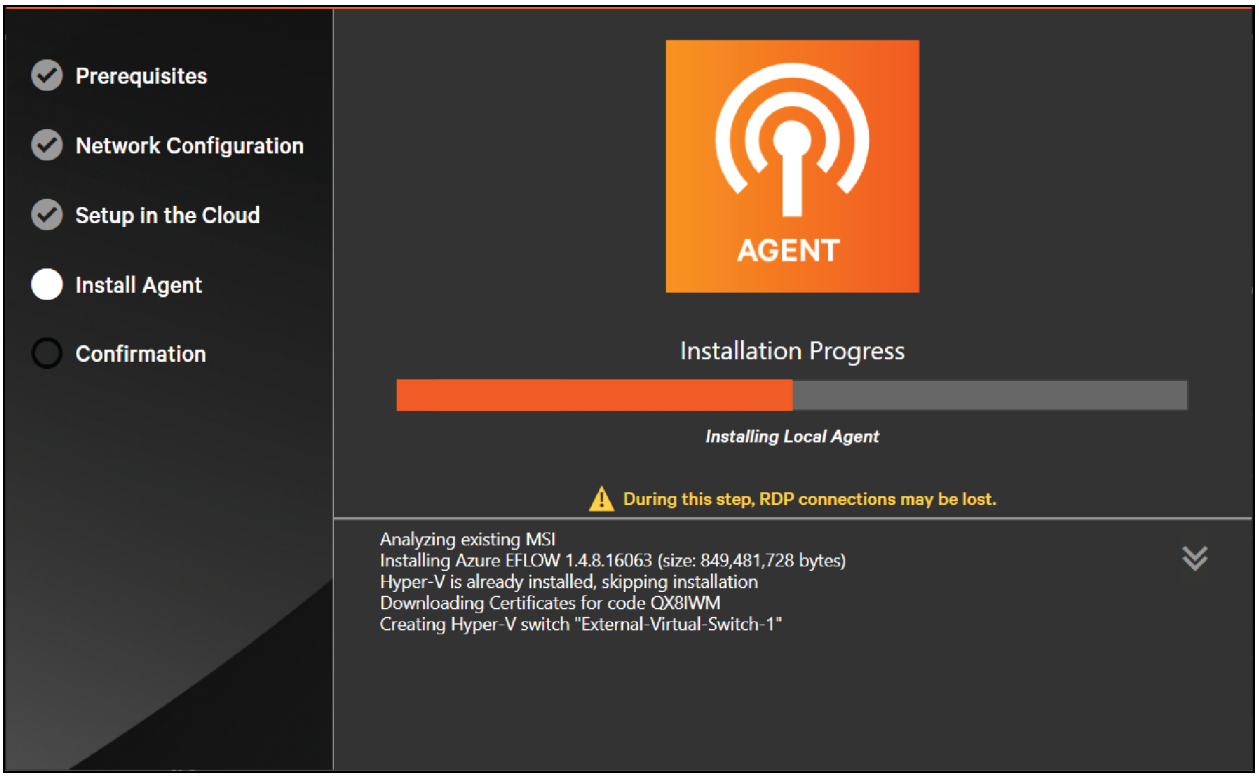
If Hyper-V is not enabled on the agent machine, the installer will install it and any dependencies. This may require a reboot to complete. When the reboot is finished, the installer will continue automatically. See Installation Steps on page 60.

Figure 6.11 Installing Hyper-V



During the virtual switch configuration phase, the agent may briefly lose network connectivity. If you are logged into the agent machine using RDP, you may briefly lose your connection.

Figure 6.12 Configuring Switches

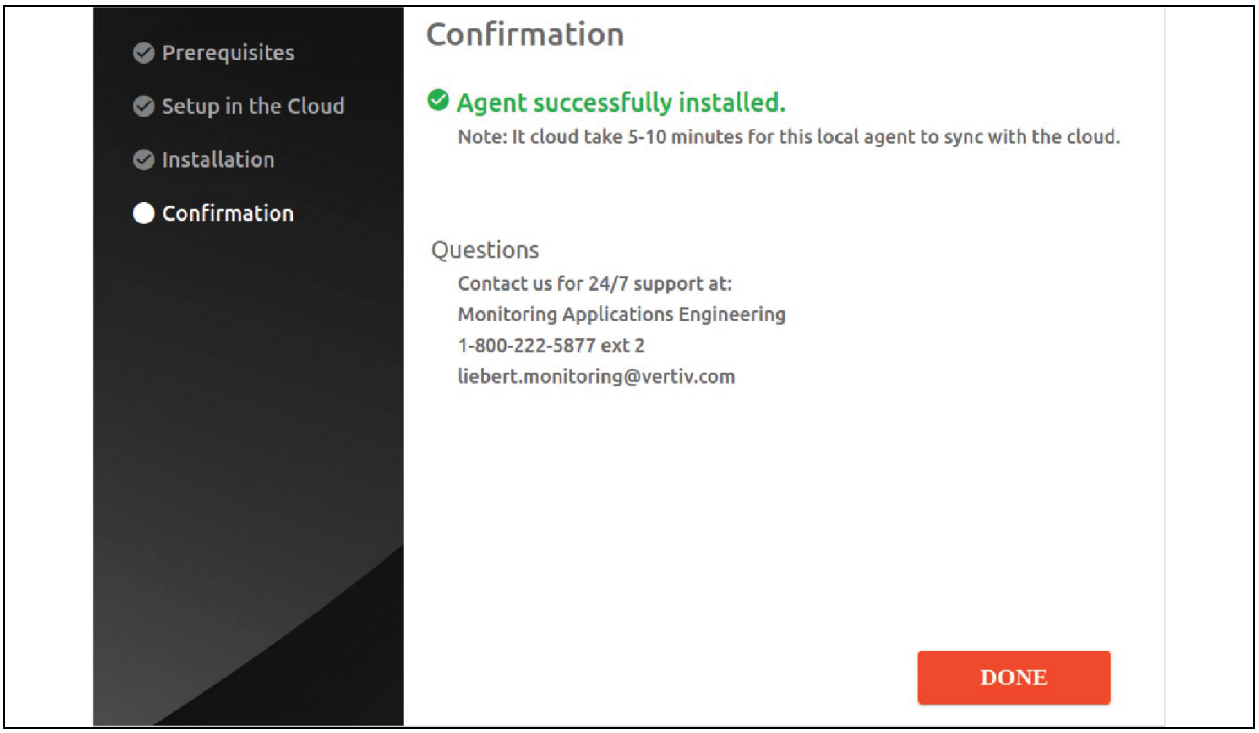


Detailed installation progress can be toggled by clicking the Up/Down Arrows on the right side of the installer.

Up/Down Arrows

When installation is complete, the agent downloads additional components and updates. This process can take 10 to 15 minutes, or longer depending upon network speed and latency. Afterward, the agent is fully online and ready to scan for and poll devices.

Figure 6.13 Installation Success

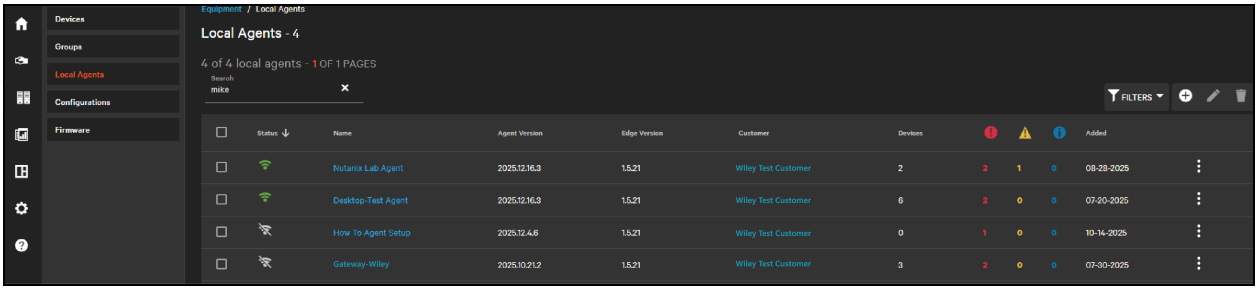


Post Installation

View a list of all agents in the **Equipment** menu and then select **Local Agents**.

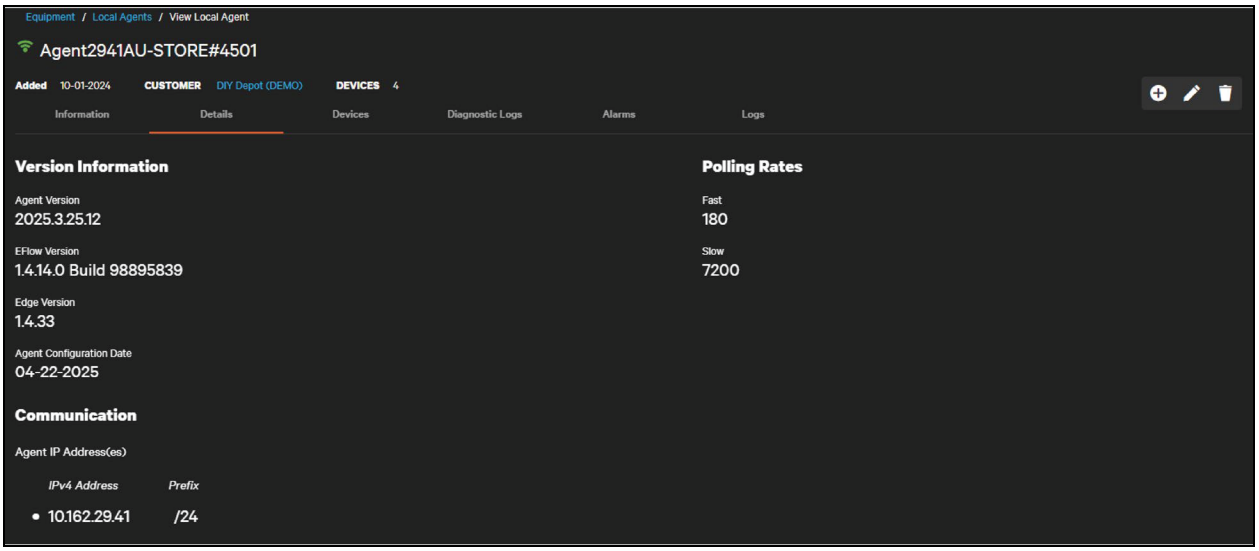
The status column shows if the agent is currently online. From this list, click on an individual agent to see its details.

Figure 6.14 Local Agents List



View the version information for the running agent using the Details tab.

Figure 6.15 Windows Agent Version Information



The Agent, EFlow, and Edge versions will auto update as we release new versions of the agent.

NOTE: EFlow applies only to the Windows Agent. Linux Agents will not have an EFlow version.

6.3.3 Troubleshooting

Retrieving Local Agent IP Address

If you failed to record the IP(s) set for the agent during the networking step, or if they were configured via DHCP, you can retrieve them either directly in the Connect platform or locally. Both procedures assume a successful installation.

To find the IP address(es) in the cloud navigate to local agent and click the details tab. The IP address(es) will show in a list under the configuration date and will update if the networking configuration of the agent changes (see Figure 6.15 above).

You can also retrieve the networking information directly on the local agent machine using the following procedure:

1. Open Windows PowerShell Administrator on the agent machine.
2. Run the following command to retrieve the networking settings for the agent.

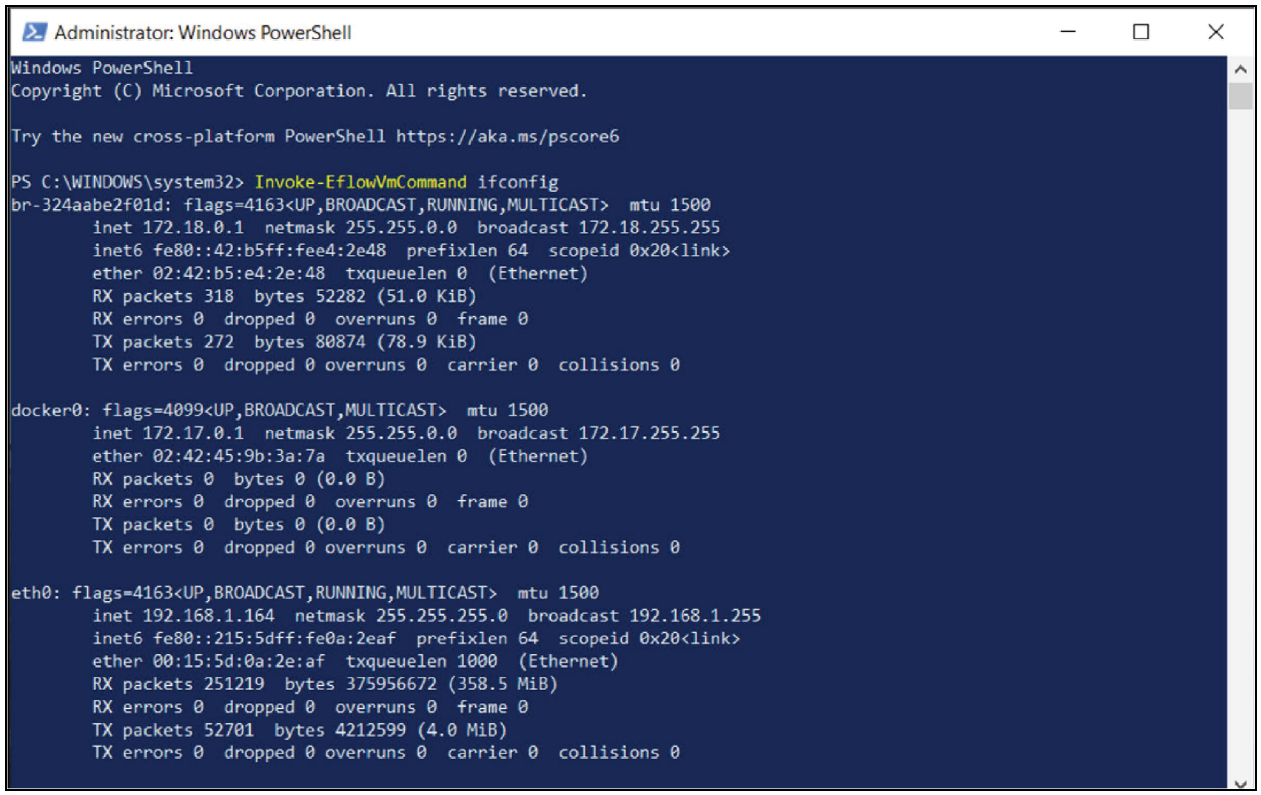
```
Invoke-EflowVmCommand ifconfig
```

NOTE: You can find additional EFlow PowerShell Commands using this link: https://learn.microsoft.com/en-us/azure/iot-edge/reference-iot-edge-for-linux-on-windows-functions?view=iotedge-1.4.

3. Look for the **eth0** adapter. The IP address for this adapter can be used as the trap/inform target of the agent. It should also be the IP address used to view the local agent logs.

NOTE: inet is the IPv4 address and inet6 is the IPv6 address.

Figure 6.16 Results of the Invoked ifconfig Command



Alternatively, you can replace Step 2 with the following:

1. Invoke the following command to connect to the EFlow VM. This will make an SSH connection to the EFlow VM:

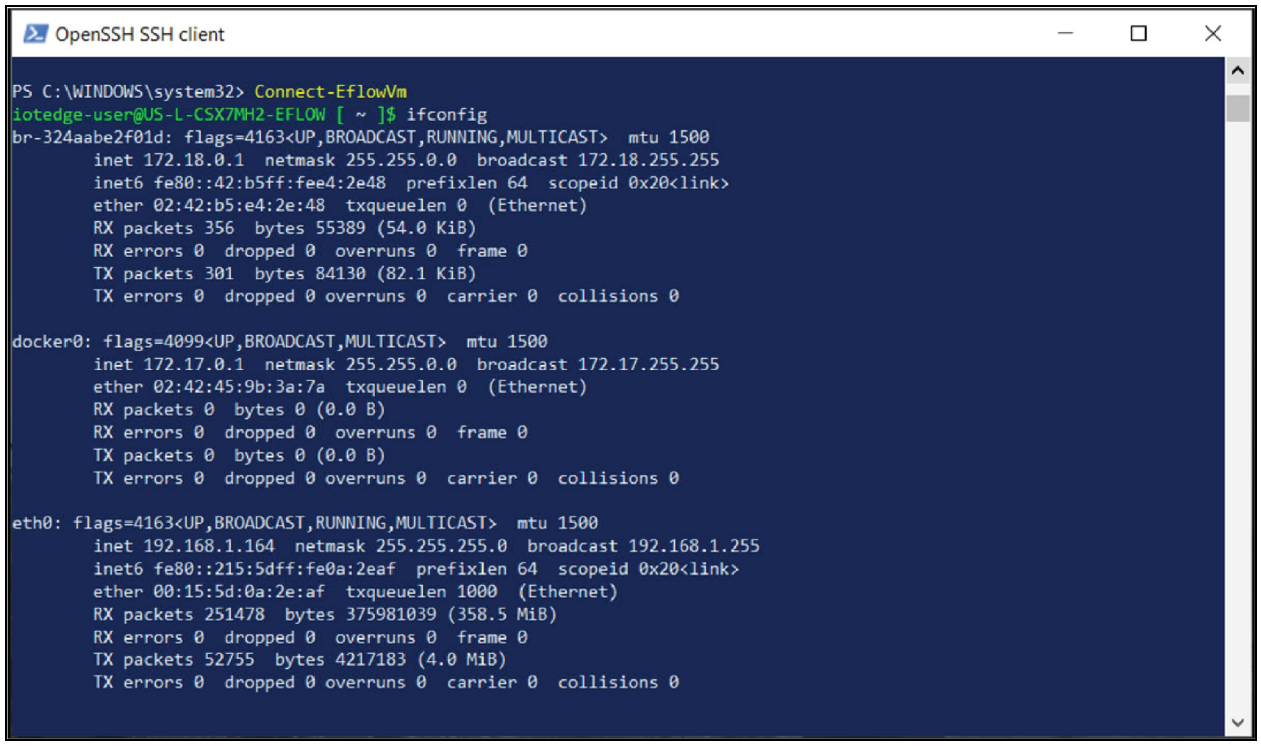
```
Connect-EflowVm
```

2. Wait for the connection to be made and then type the following:

```
ifconfig
```

3. Look for the **eth0** adapter. The IP address for this adapter can be used as the trap/inform target of the agent. It should also be the IP address used to view the local agent logs.

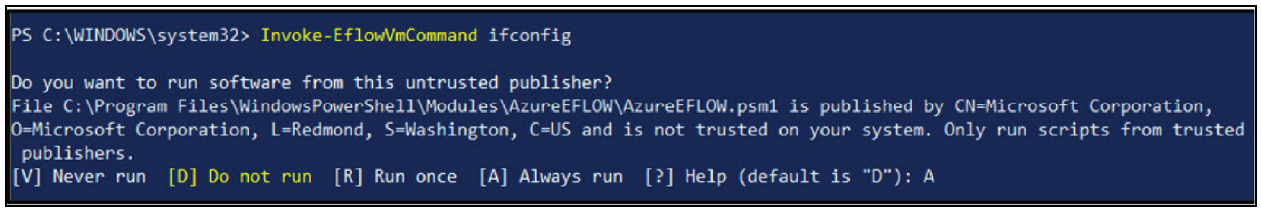
Figure 6.17 Results of Connected ifconfig Command



You may see the warning shown in when trying to run commands. You have two ways to respond:

- Type **R** to run once. This will warn you again the next time you run these commands.
- Type **A** to always run.

Figure 6.18 Command Warning



EFlow Virtual Machine Won't Respond to Ping (ICMP Traffic Requests)

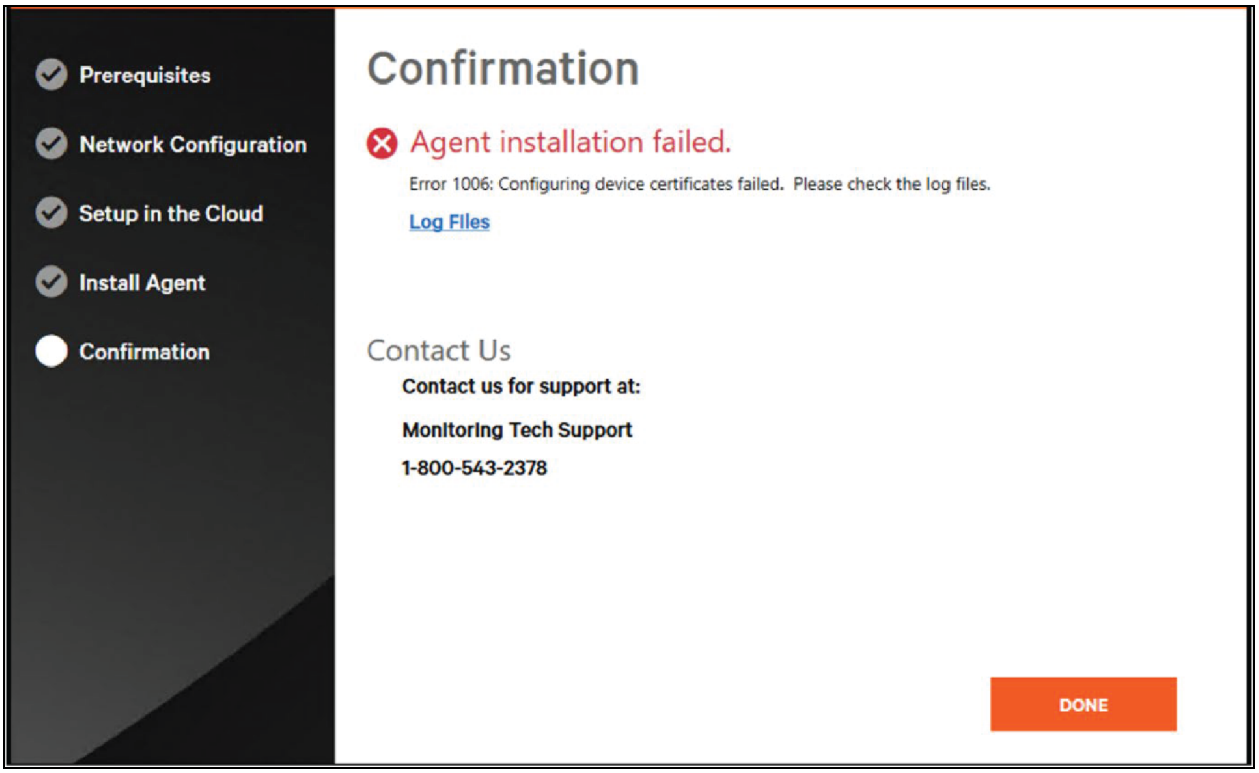
By default, ICMP ping traffic response is disabled on the EFlow VM firewall. To respond to ping requests, allow the ICMP traffic by using the following PowerShell cmdlet:

```
Invoke-EflowVmCommand "sudo iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT"
```

Installation Log Files

If the agent installation fails, you can download the log files by clicking the link in the installer. This opens a file dialog that will ask you to specify a name for the zip file containing the log files. Click **Save** to download.

Figure 6.19 Agent Installation Failed



If you do not download the logs from the link, you can find them in one of these directories:

- C:\Users\<YourUser>\AppData\Local\Temp\LocalAgentInstaller\logs
- C:\Users\<YourUser>\AppData\Local\Temp\<#>\LocalAgentInstaller\logs (# will increment with each attempt to download)

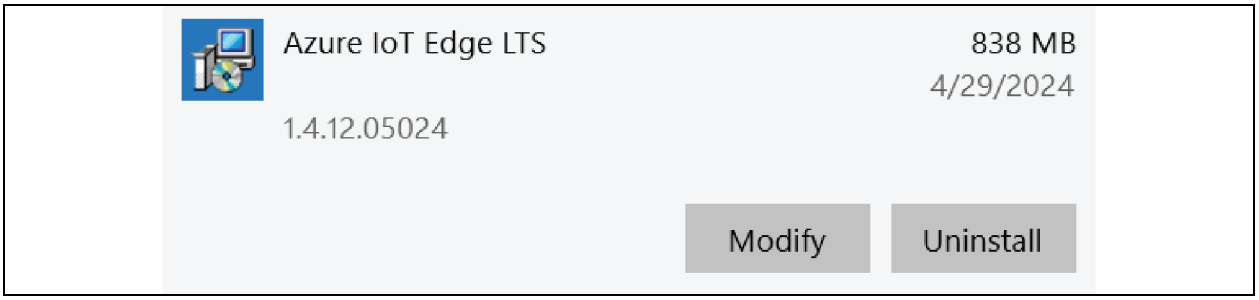
Archived logs from previous installation attempts are stored in the archives folder under the LocalAgentInstaller root folder. Up to the 10 previous installation attempts are kept, with sub-folders for logs and scripts. The scripts folder contains scripts used by the installer to configure the EFlow VM.

Retrying Installation

Depending on where your installation failed, take the following:

1. Uninstall Azure IoT Edge LTS.

Figure 6.20 Uninstall Azure IoT LTS

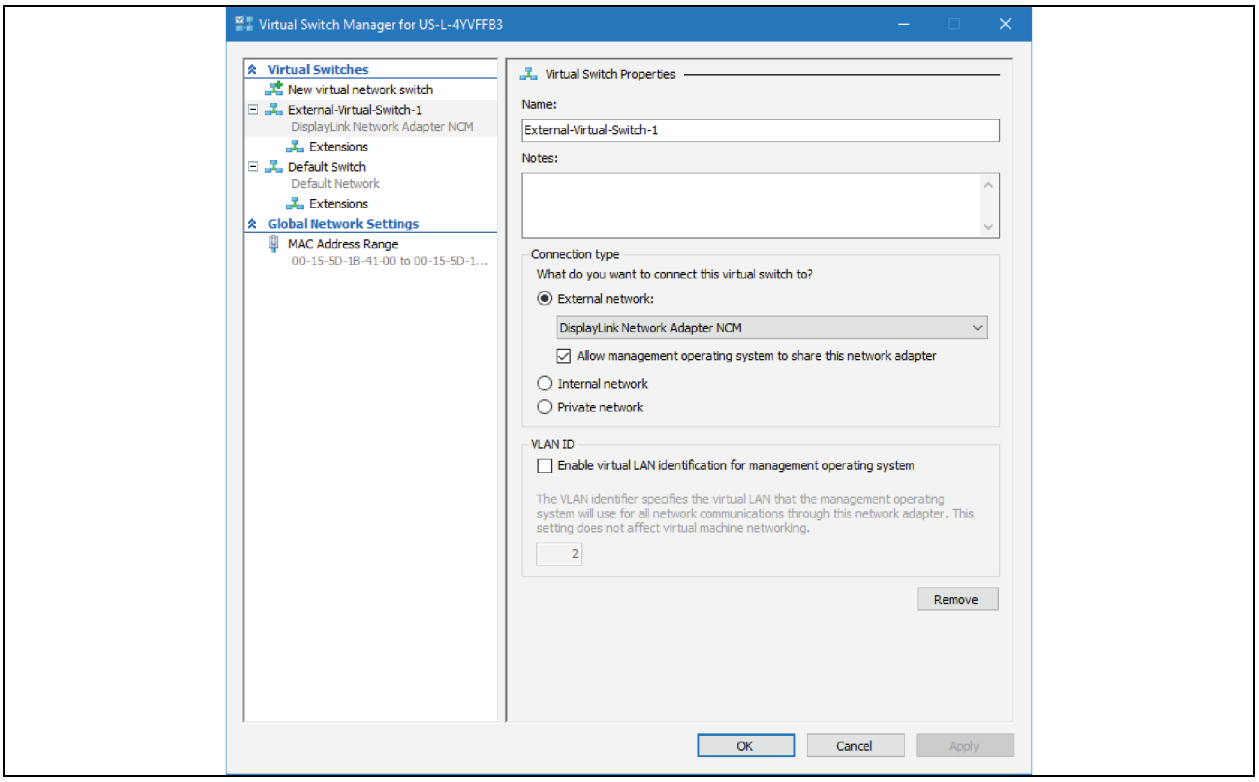


2. Remove any virtual switches created by the agent.
   - Two NIC setup only:
     - External Virtual Switch 1
     - External Virtual Switch 2
   - If broadcast discovery was not enabled:
     - Internal Virtual Switch 1
     - Internal Virtual Switch 2

   The easiest way to do this is to use the Hyper-V Virtual Switch Manager. If you used Wi-Fi as the NIC for the agent, you may also need to manually delete a network bridge.

NOTE: You will only be able to remove virtual switches via the Hyper-V GUI if the Hyper-V installation is successfully completed.

Figure 6.21 Virtual Switch Manager



Alternatively, you can run the following PowerShell command (as an administrator) to remove the switch:

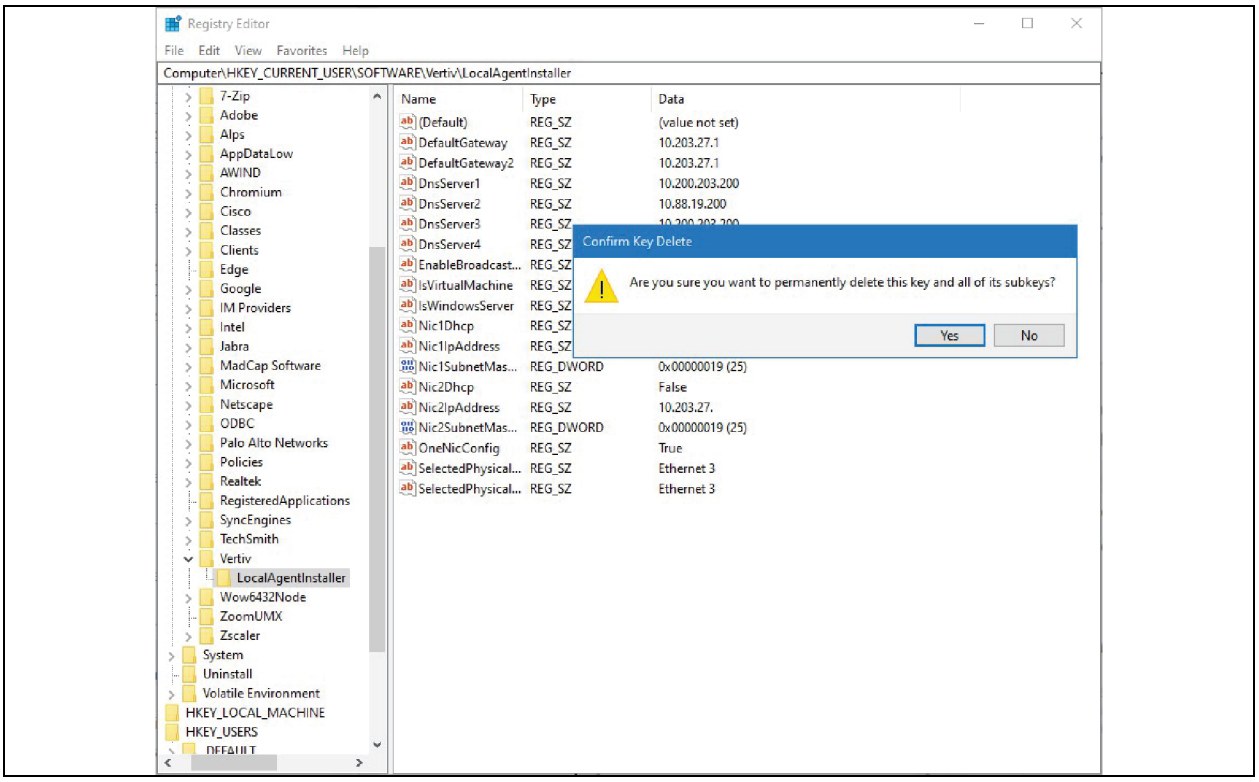
```
Remove-VMSwitch “<NameOfSwitch>”
```

3. Optional. Remove installer reference data from registry.

CAUTION: We recommend that you complete this step only if you have had multiple failed installations.

- Open the Registry Editor. From the Windows Start menu, go to Search, and enter Registry Editor.
- With in the Registry Editor, find this folder**: Computer\HKEY_CURRENT_USER\SOFTWARE\Vertiv\LocalAgentInstaller**
- Delete this folder. When prompted to confirm the deletion, click **Yes**.

Figure 6.22 Registry Editor, Deleting Folder



4. Delete the failed agent from Connect Cloud. You can do this by selecting the agent in the local agent list and clicking the

   Delete icon

   or

   by clicking the

   Pull down menu

   After completing these steps, you can now re-try installation.

6.4 Linux Installation

6.4.1 System Requirements

The Linux Agent minimum requirements are listed in Table 6.4 below

Table 6.4 Linux Minimum Requirements

Requirement		Detail
Supported Linux Distros	Ubuntu 22.04 LTS Desktop "Jammy Jellyfish"	Note: Not server versions.
Hardware	Memory	• Minimum Free Memory: 2GB, 4GB recommended. Memory used exclusively by the agent process. • Total Minimum Memory: 4 GB, 8 GB recommended. Total memory required for the VM or bare metal machine (based on OS minimum + agent minimum).
	Disk Space	• Minimum Free Disk Space: 27 GB, 60 GB recommended. Disk space used exclusively by the agent. • Total Minimum Disk Space : 60 GB, 100 GB recommended. Size of virtual or physical hard drive used by the OS and installed agent.
	CPU Cores	2+ Intel Xeon CPU E5-2673 v3 at 2.40 GHz or equivalent

The agent is not supported on distro forks such as Lubuntu, Linux Mint, etc.

Additional distributions may be added in future releases.

6.4.2 Installation Steps

Installation Preparation

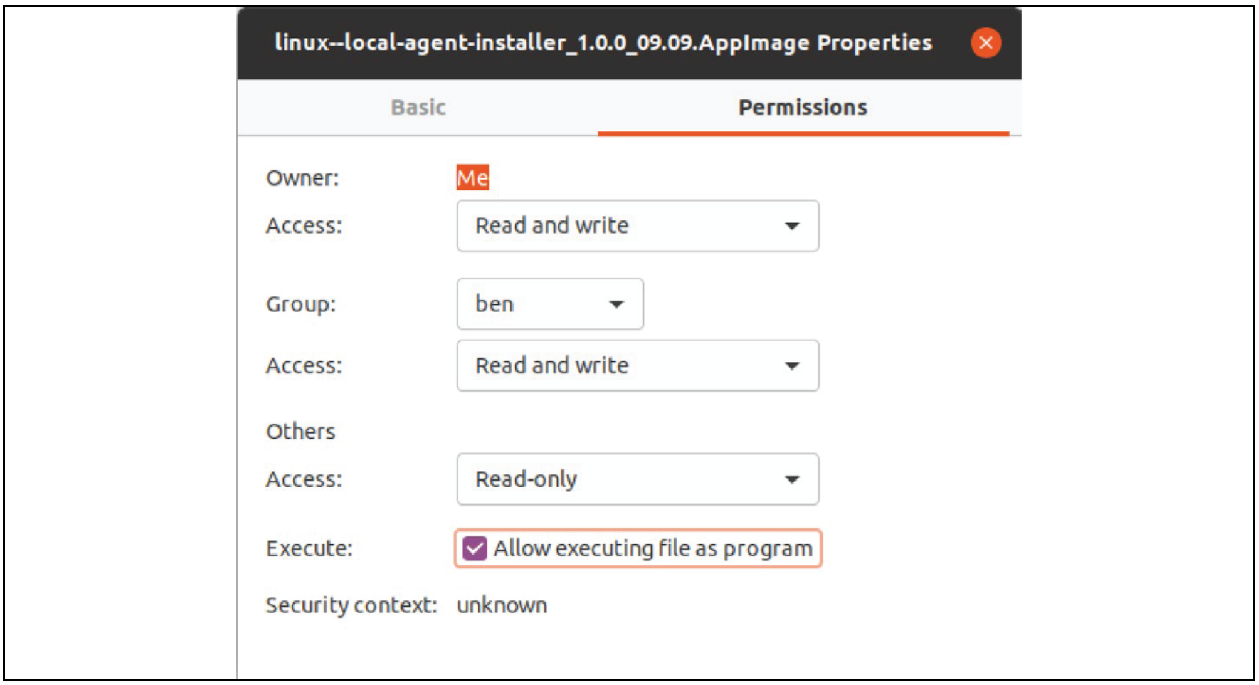
Before installing the Linux Agent, complete the following prerequisite steps.

- Grant the agent installer execution rights.
- Modify sudoers file to allow passwordless execution.
- **Optional.** Install Libfuse2. **This step is required if the Ubuntu distro is FUSE 3.**
- **Optional.** Install recommended packages.

Step 1: Grant Installer Execution Rights

The Linux installer requires execution rights before running. To grant execution rights, right-click on the installer and on the Permissions tab select **Allow executing file as a program**.

Figure 6.23 Grant Execution Rights



Alternatively, you can run the following shell command from a terminal:

```
chmod a+x linux--local-agent-installer_<Version>.AppImage
```

Step 2: Modify the sudoers file to allow passwordless execution

The Linux agent installer requires the ability to execute and run commands as root (sudo). Currently, this requires direct modification of the sudoers file to allow for passwordless execution.

1. Run the following command in a terminal to modify this file:

```
sudo nano /etc/sudoers
```

2. The subdoers file opens in the nano editor. Append the following to the end of the subdoers file.

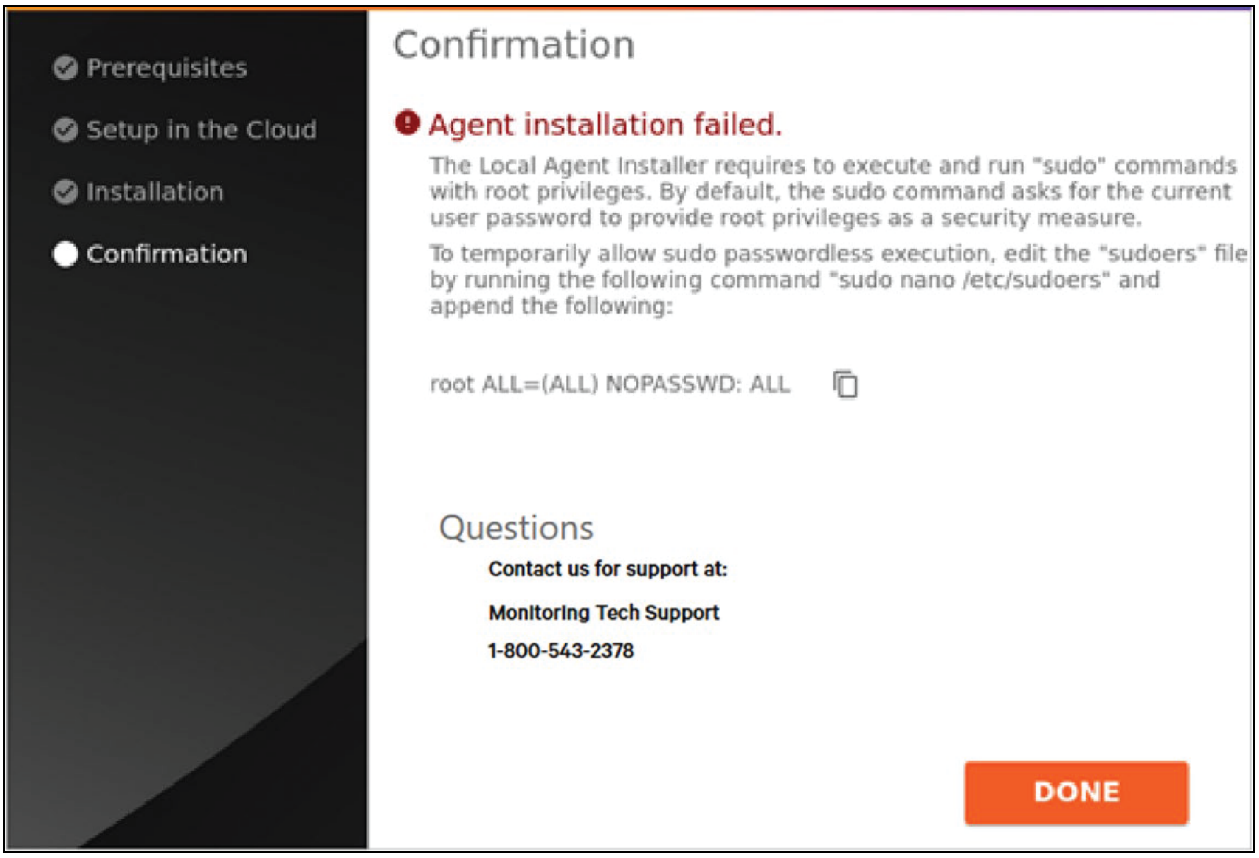
```
<<adminuser>> ALL=(ALL) NOPASSWD:ALL
```

NOTE: Replace <<adminuser>> with the admin/root user.

NOTE: Vertiv recommends attempting installation before modifying the file. The installer should display the required line for modification which you can copy/paste into the sudoers file.

3. Save changes to the file and then run the installer. If you fail to complete this step, the agent installation will fail and prompt you to make this modification.

Figure 6.24 Failed Installation Prompt



IMPORTANT! When you have finished installing the agent, we highly recommend removing the line you added from the sudoers file as a security measure.

Step 3: Install libfuse2 (if Required)

Ubuntu distros that are greater than the initial release of 22.04 LTS may include FUSE3 by default, not libfuse2. As of the date of the publication, libfuse2 is required for running AppImage installers.

NOTE: When AppImage is updated to support FUSE3 we will modify this document and the installer accordingly.

To install libfuse2 alongside the existing FUSE3 distro, run the following commands in a terminal.

```
sudo add-apt-repository universe
```

```
sudo apt install libfuse2
```

WARNING! Be certain to install *libfuse2* and not *fuse*. Installing the fuse package may break your systems. If you installed fuse, refer to Troubleshooting on page 82.

Step 4: (Optional) Install Additional Recommended Packages

Vertiv recommends installing net-tools (used to run commands like ifconfig to determine networking information).

- net-tools can be installed using the following command in a terminal.

```
sudo apt-get install net-tools
```

Vertiv also recommends you run all updates to your Ubuntu installation before running the installer.

Once you have completed the above steps, you can run the agent installer.

Registering the Linux Agent

The Linux agent does not require network configuration. Azure IoT Edge is designed to run natively in a Linux environment. However, you will still need to register the agent with the cloud. This process is the same as in the Windows Agent. See Downloading the Agent on page 56.

Figure 6.25 Registering the Linux Agent Access Code

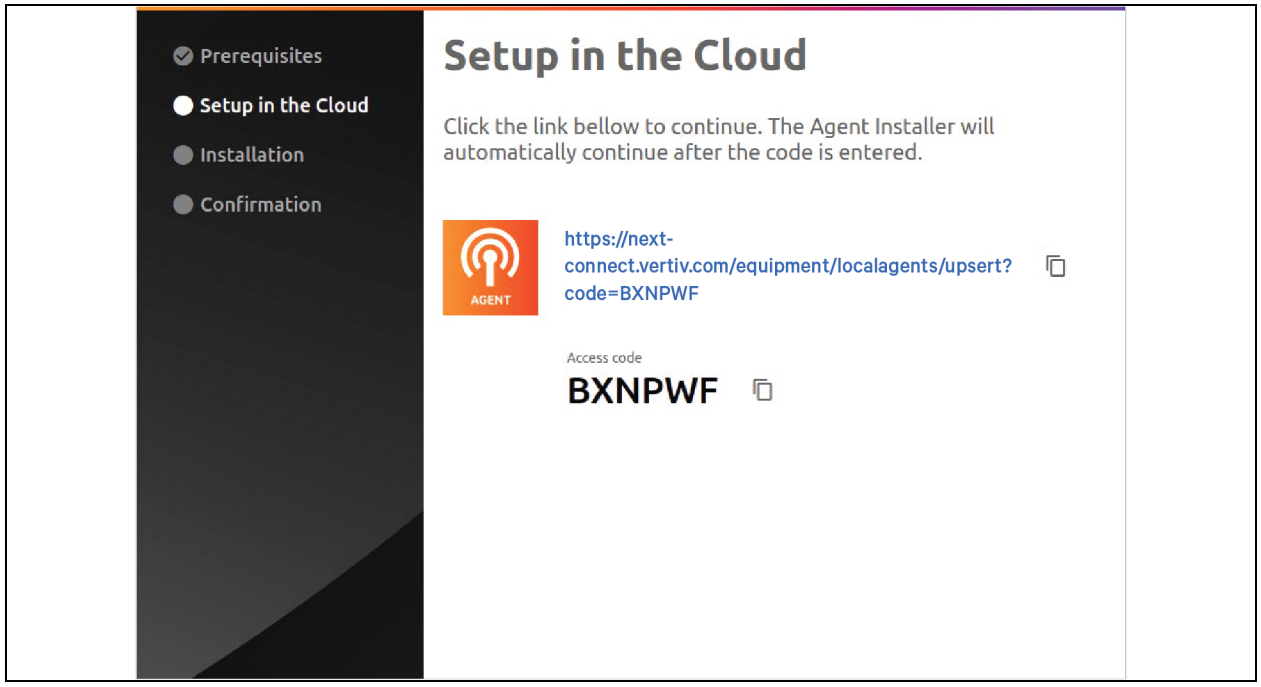
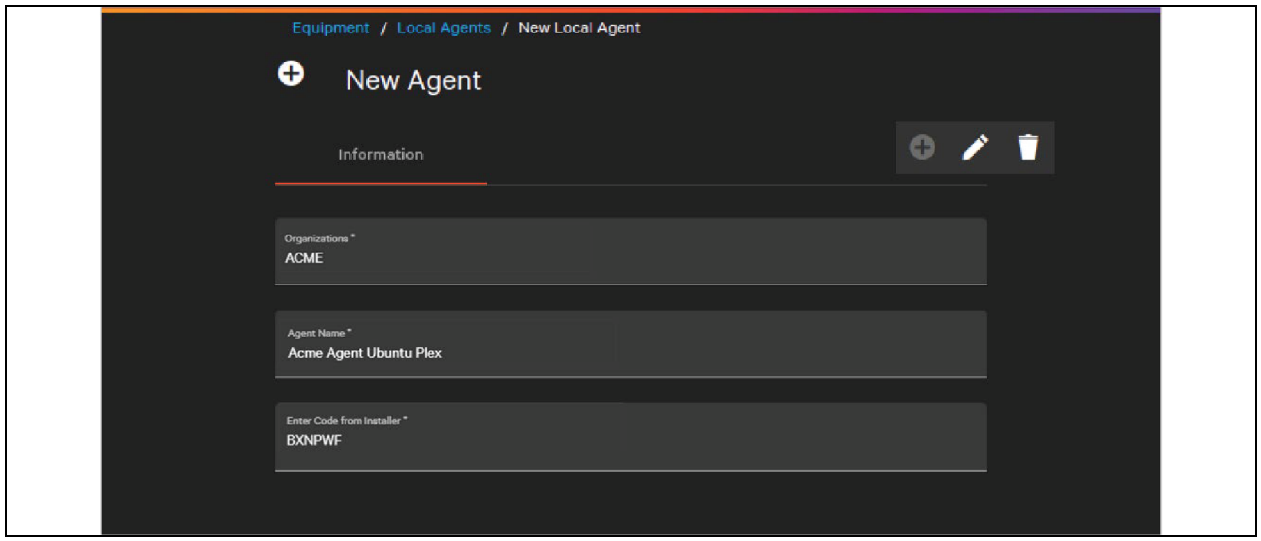


Figure 6.26 Registering Linux Agent



The installer will generate a temporary code for registering the agent with the Connect platform.

IMPORTANT! This code is good for 15 minutes. If it expires you will need to restart the installation process.

Click the link in the installer and you are automatically directed to the Connect platform. Login and you will be directed to the New Agent dialog. The code is auto filled when the link is clicked, but it can also be copied and pasted from the installer. Choose the customer (if not auto filled) and a name for the agent. Click **Save**. When the agent is created, the installation continues.

When installation is complete, the agent downloads additional components and updates. This process can take 10-15 minutes. Afterward the agent will be fully online and ready to scan for and poll devices.

Figure 6.27 Installation Progress

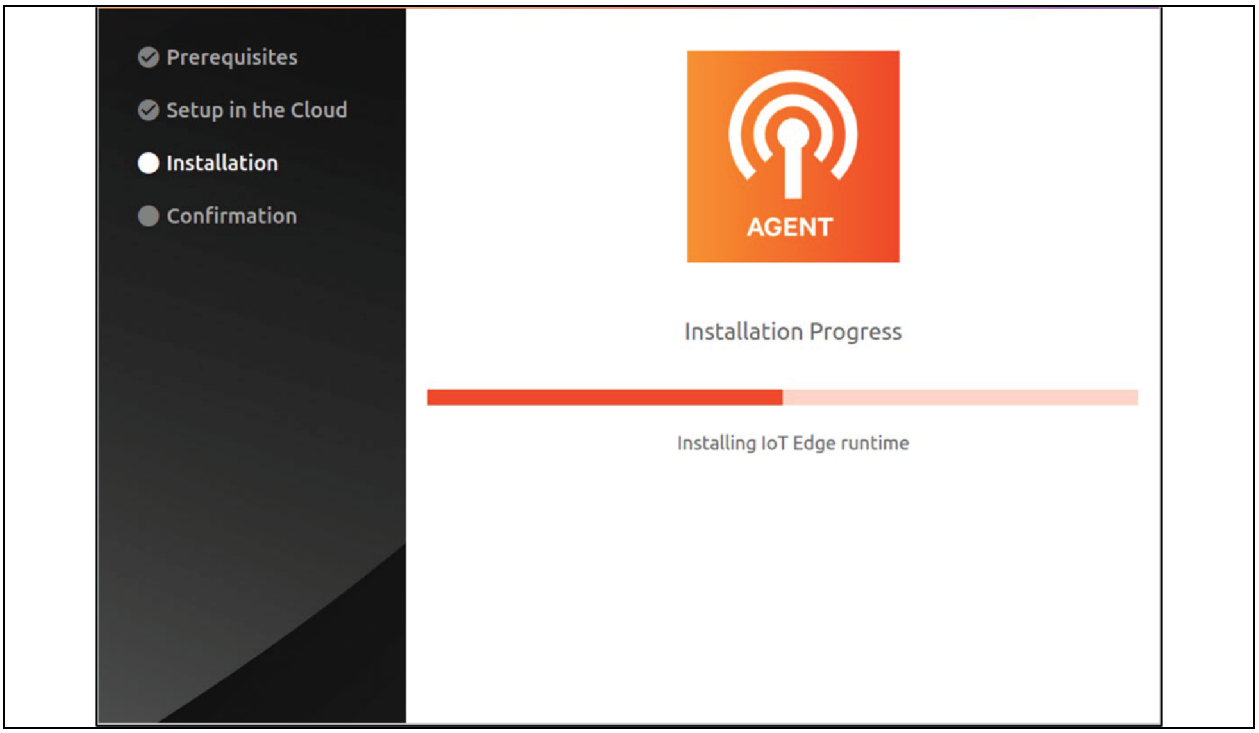
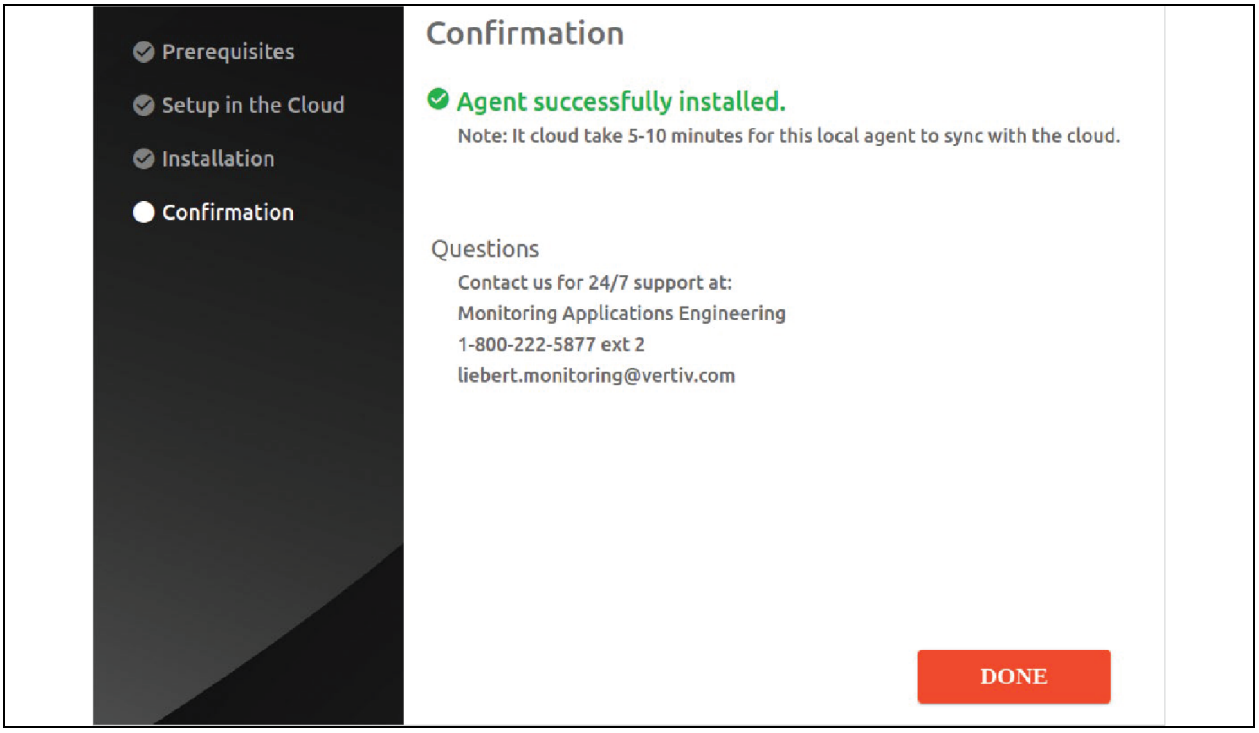


Figure 6.28 Successful Installation Confirmation



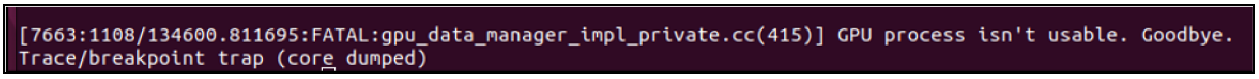
6.4.3 Troubleshooting

Resolving GPU Error

Some users when running the installer have encountered the following error message:

FATAL:gpu_data_manager_impl_private.cc(415)] GPU process isn't usable. Goodbye.

Figure 6.29 GPU Error in Command Window



1. To resolve this, run the agent installer from a terminal and add the **disable gpu sandbox** flag.

```
./linux--local-agent-installer_<Version>.AppImage --disable-gpu-sandbox
```

2. Alternatively, use the **no sandbox** flag.

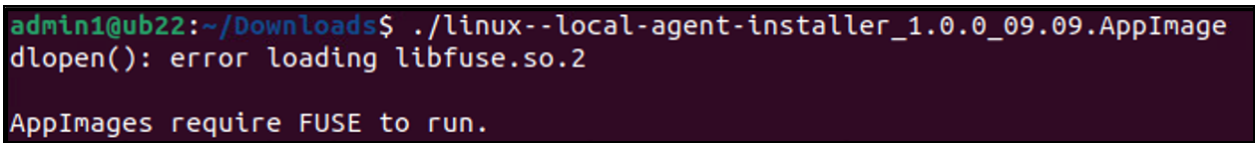
```
./linux--local-agent-installer_<Version>.AppImage --no-sandbox
```

Installing Missing Library Dependencies

As an AppImage, the local agent requires libfuse2 to run. On some operating systems (Ubuntu 22.04.3+), FUSE3 is installed by default, resulting in the following error when running the installer:

dlopen(): error loading libfuse.so.2

Figure 6.30 Error Loading Libfuse in Command Window



Run the older version of FUSE by running this command in a terminal:

```
sudo add-apt-repository universe
```

```
sudo apt install libfuse2
```

Fixing OS after Installation of Older Fuse Library

If the wrong fuse library is installed, the GNOME settings functionality of the OS may be broken. If you have completed installation of the agent, revert to the newer FUSE3 to repair the broken settings dialog with the following commands.

```
sudo apt-get update
```

```
sudo apt-get install --reinstall gnome-control-center
```

This uninstalls the older fuse, and as part of the GNOME installation restores FUSE3 .

For further reference, please see https://askubuntu.com/questions/1420736/settings-window-does-not-open-in-ubuntu-22-04

Uninstalling the Linux Agent

To retry installation of the Linux agent, it may be necessary to remove a previous installation. The procedure below removes IoT Edge and any downloaded docker containers, users, and certificates.

NOTE: This procedure was derived from Microsoft documentation available here: https://learn.microsoft.com/en-us/azure/iot-edge/how-to-provision-single-device-linux-symmetric?view=iotedge-1.4&tabs=azure-portal%2Cubuntu#uninstall-iot-edge

1. Remove the IoT Edge runtime. Open a terminal and run the following:

```
sudo apt-get autoremove --purge aziot-edge
```

2. Removing IoT Edge stops the agent docker containers but these still need to be manually removed. See a list of the downloaded containers by running the following command:

```
sudo docker ps -a
```

A list of docker containers, as shown in Figure 6.31 below is displayed.

Figure 6.31 Agent Docker Containers

3. Deleting the containers by running the commands below from a terminal. These commands must be run in the order shown.

```
sudo docker rm -f LocalAgentWeb
```

```
sudo docker rm -f LocalAgentLib
```

```
sudo docker rm -f edgeHub
```

```
sudo docker rm -f edgeAgent
```

NOTE: edgeHub and edgeAgent are the two runtime containers provided by Microsoft as part of IoT edge.

To additionally remove any stopped containers and all unused images (not just dangling images), add the -a flag to the command:

```
sudo docker system prune --all --volumes
```

Run the following command after deletion to confirm that all containers have been deleted correctly. You should see any empty list:

```
sudo docker ps -a
```

4. Remove the container runtime from your device using the following command from a terminal. You do not need to complete this step is you use something else with containers on the agent machine.

```
sudo apt-get autoremove --purge moby-engine
```

5. Delete the **installer-logs folder. (This folder should be in your home directory.)**

IMPORTANT! If you do not delete this folder, future installation logs will be appended to the end of the current log.

6. Delete the **linux--local-agent-installer** folder. Open a terminal and navigate to the config directory. Run **ls** to see folders at this level.

```
cd .\config
```

```
ls
```

In this folder should be another folder that contains settings used by the previous installation. Delete this folder and its contents by running the following command:

```
sudo rm -r linux--local-agent-installer/
```

7. Delete the **iotedge-user** folder. From a terminal, navigate to your home directory. Run ls to see users at this level. You will see a folder named **iotedge-user**. Delete this folder and its contents by running this command:

```
sudo rm -r iotedge-user/
```

This removes any stray certs and logs used by the agent.

Once you have completed the steps above you can attempt to install the agent as normal.

6.5 Configuring Polling Rates

As of the latest release, the Local Agent supports two polling groups: fast and slow.

- The fast polling group is intended for data that regularly changes such as temperature, load, and current.

- The slow polling group is intended for more static data such as serial number and manufacturer.

Currently, which points are in which polling groups are defined in the device templates supplied by Vertiv.

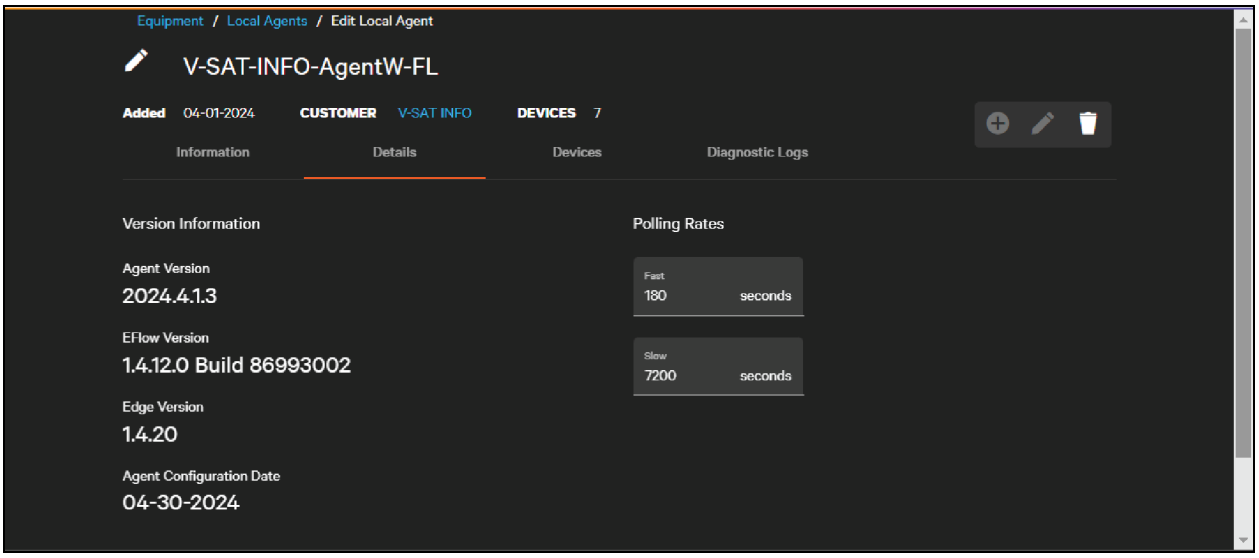
Users can adjust at an agent level how slow or fast data is collected.

1. To edit the polling rates, navigate to an individual agent and click the

   Edit icon.

2. Click on the **Details** tab. The two polling rates on the right-hand side.

Figure 6.32 Editing Polling Rates



3. By default, the fast group is polled every 180 seconds (3 minutes). The slow group's default is 7200 seconds (2 hours). Currently, polling cannot be set faster than 3 minutes.
4. Polling rates can be adjusted (in seconds) up or down as desired. Click **Save** to apply the new polling rates to **all** devices sending data through this agent.

NOTE: This does not affect SNMP trap/inform data speeds. Traps/informs are sent from the device when the inciting event occurs and are processed and sent by the agent immediately.

6.6 Diagnostic Logging

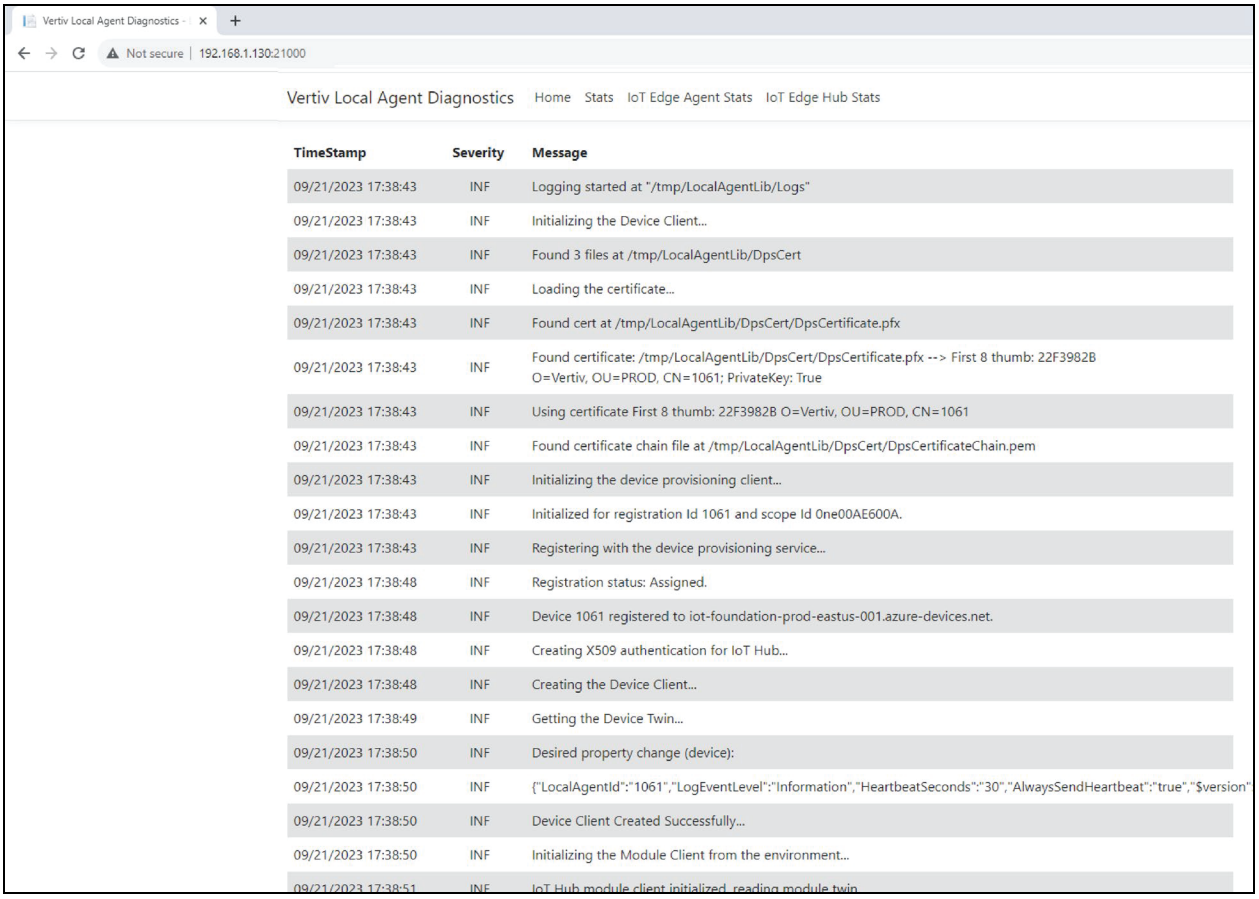
Both the Windows and Linux Agents have locally available and cloud accessible logs.

6.6.1 Local Agent Local Webpage

On the agent machine or within the customer network, you can access a local agent webpage containing logging and metric information. The webpage runs on port 21000 and can be accessed via this URL: http://<ipAddressOfAgent>:21001. See Retrieving Local Agent IP Address on page 69 to see the steps to retrieve the IPv4 address of the agent.

The Linux agent runs directly on the host Linux OS without virtualization, so the IP address of the agent should match that of the host machine. You can retrieve this address by running ifconfig in a terminal.

Figure 6.33 Local Agent Webpage



If you can see the webpage, this means the agent has finished downloading its post installation files and is actively running. Latest log entries are at the bottom of the webpage. All times are in UTC.

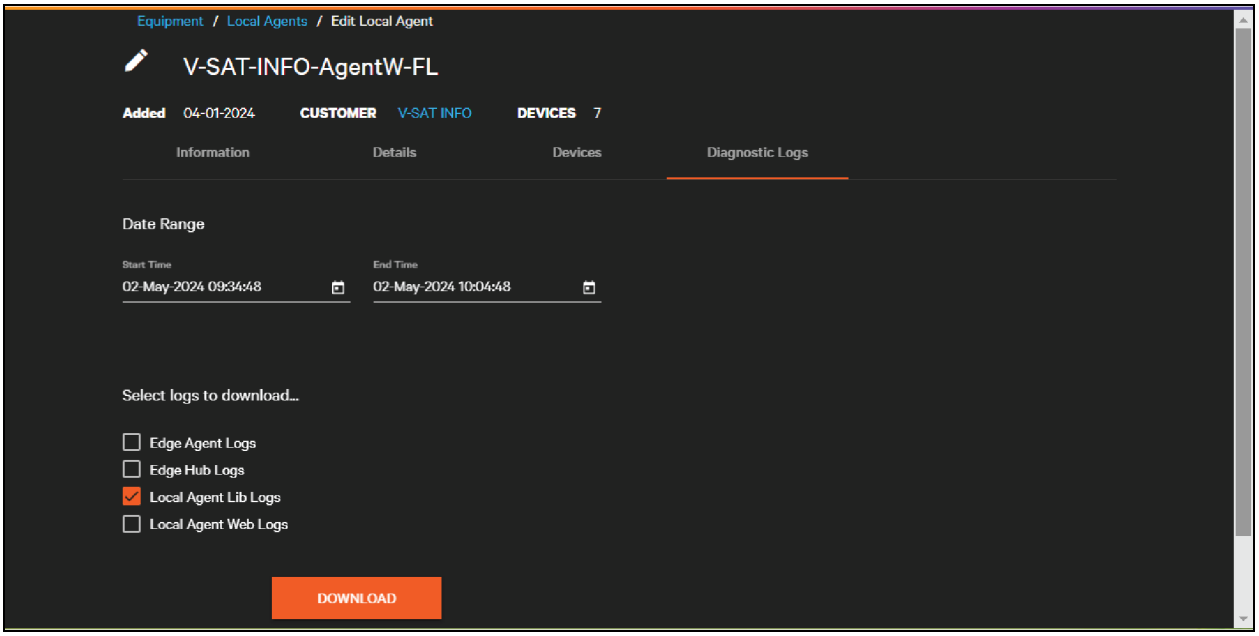
The stats tab shows the message throughput for the agent and when the last messages were sent. The agent sends regular heartbeat messages to the Connect platform every 30 seconds and sends telemetry in compressed format.

The other two tabs contain statistics for the Microsoft made containers inside the agent. Edge Agent is the container orchestrator and runs all the other docker containers within the agent. Edge Hub is the container that manages the message connection to the Connect platform.

6.6.2 Retrieve Agent Logs from the Cloud

You also retrieve agent logs directly from the Connect web application. Navigate to the individual agent by going to the Local Agents list (under the Equipment menu) and click on the name of the agent. If the agent is online, you can retrieve logs on the Diagnostic Logs tab.

Figure 6.34 Diagnostic Logs Tab



The local agent has four logs, one for each of the container running inside the agent. By default, Local Agent Lib logs is selected, which contains most of the relevant information on device polling, discovery operations, provisioning operations, and other statistics.

The full description of logs:

- **Edge Agent Logs**—Microsoft component. Orchestrates other containers.
- **Edge Hug Logs**—Microsoft component. Logs communication with cloud.
- **Local Agent Lib Logs**—Vertiv component. Information about polling, operations, and other troubleshooting.Typically, this is the log most needed by tech support.
- **Local Agent Web Logs**—Contains information about the local agent webpage.

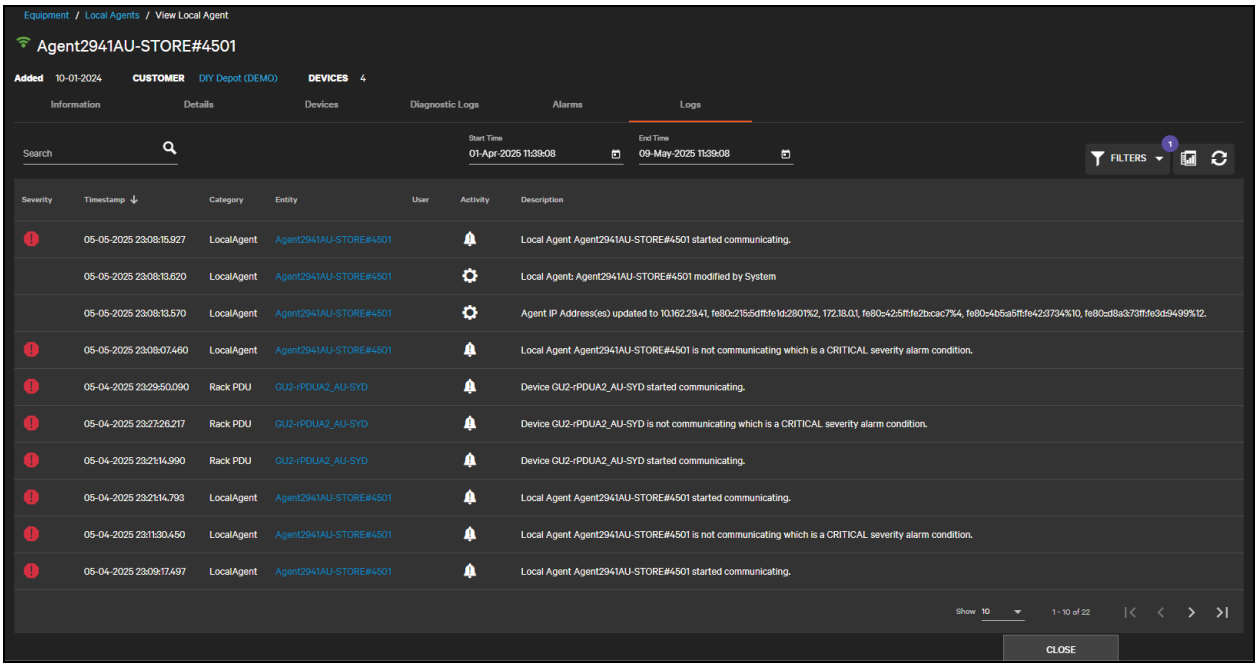
You can select one or more logs by ticking the boxes next to each log. By default, the page will retrieve logs for the past 30 minutes, but you can adjust this time as needed . If you are troubleshooting an issue, be sure to pull the logs for when you are having the issue as soon as possible. Click download to Download an individual log, or a zip file containing multiple logs.

NOTE: Log history is only retained for a short period in the Connect cloud. At most, data is retained for a few hours, although this time limit can be shorter if an operation is particularly noisy.

6.6.3 Local Agent Events and Alarms

The Logs tab of the local agent contains events, alarms and audit records for the agent itself and any devices monitored by that agent. These records are retained on the same cycle as other event logs in the platform and will not roll-over as quickly as the diagnostic logs, but they have a less granular level of detail.

Figure 6.35 Local Agent Events



All columns can be sorted, filtered, or searched. The date range is the last day by default but this can be adjusted.

NOTE: Since device events can be frequent, longer date ranges may take longer for the page to load.

The logs for the agent can be exported to a CSV by clicking the

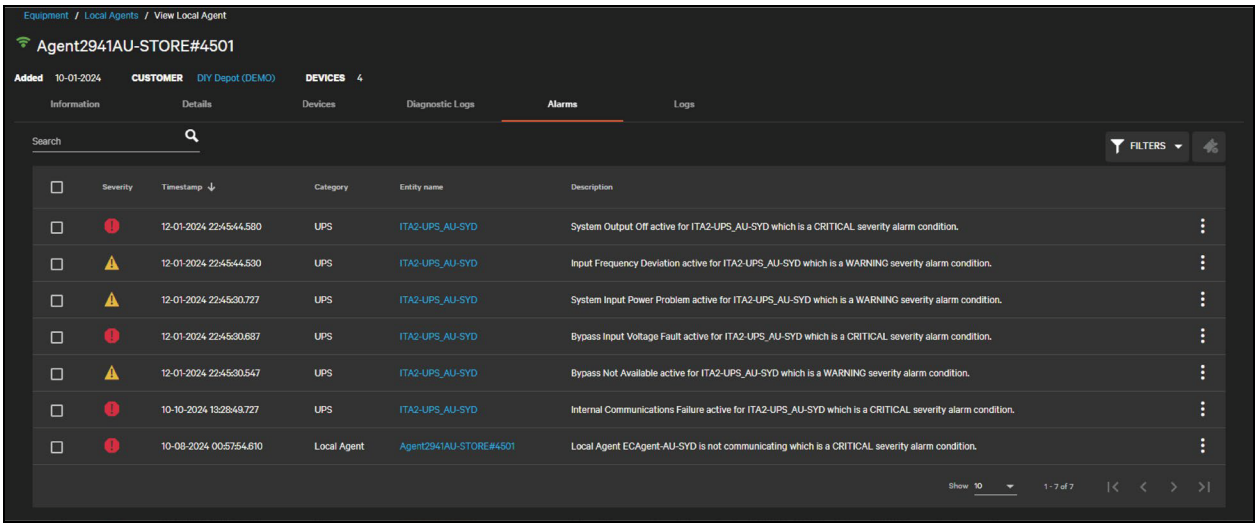
 Export to CSV icon.

The date range can be refreshed back to current by clicking the

 Refresh icon.

You can view the active alarms for any device monitored by the agent, or for the agent itself, by clicking on the Alarms tab. Currently an alarm will be created for the agent when it goes offline that will clear when communication is restored.

Figure 6.36 Local Agent Alarms



Alarms can be sorted, filtered, or searched. You can also manually clear one or more alarms by clicking the box next to the alarm and clicking the

 **Clear alarm** icon.

See Manually Clearing Alarms on page 141 for more information about manually clearing alarms.

This page intentionally left blank

7 Device Management

With the Local Agent installed, users can add devices for monitoring. See Installing the Local Agent on page 55.

There are two ways to add devices for monitoring:

- Run a Discovery Scan of the network. This locates and identifies devices. The user can then add for monitoring in bulk.
- Devices can also be added manually. This can be used to pre-load devices into the system prior to installation.

This section covers adding devices to monitoring to the system, device details pages, and the device dashboard. It will also cover grouping devices into Sites and Device Groups.

7.1 Adding Devices via a Discovery Scan

Users can add devices from several places within the Connect platform. Users can add devices from the Devices List (under the Equipment menu) which shows all the devices a user can access. If the user is a partner or Vertiv user, this will include devices across multiple customers. Users can also add devices from the Devices tab of a local agent.

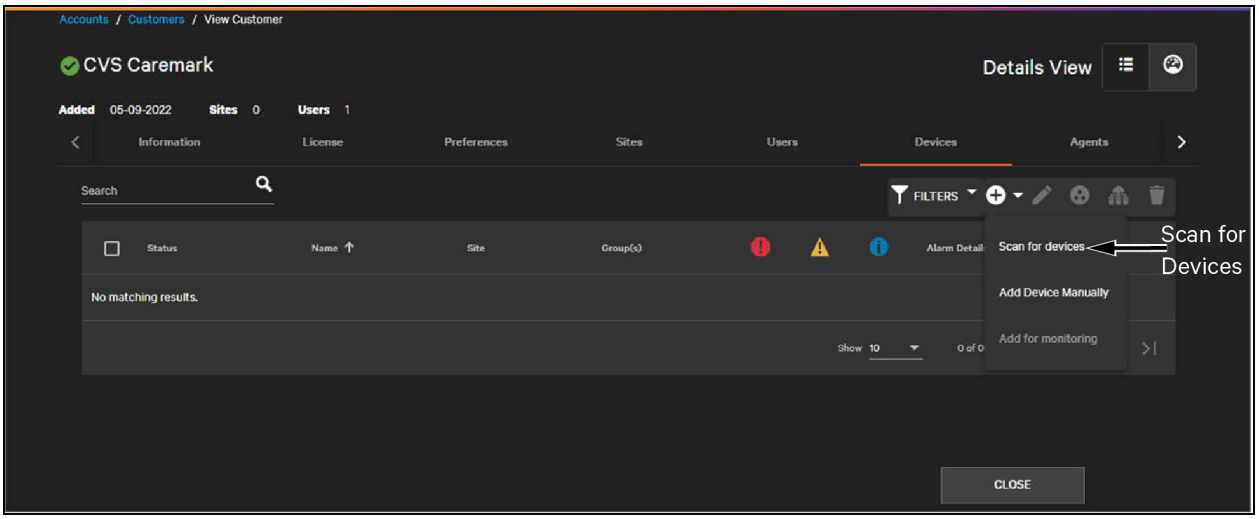
For most users, the simplest place to add devices is on the Assets tab under a specific customer. This allows a user with a wider scope of responsibility to be sure they are adding devices to the right place.

To begin discovering devices, click the Devices tab under a customer and then click the

Add icon.

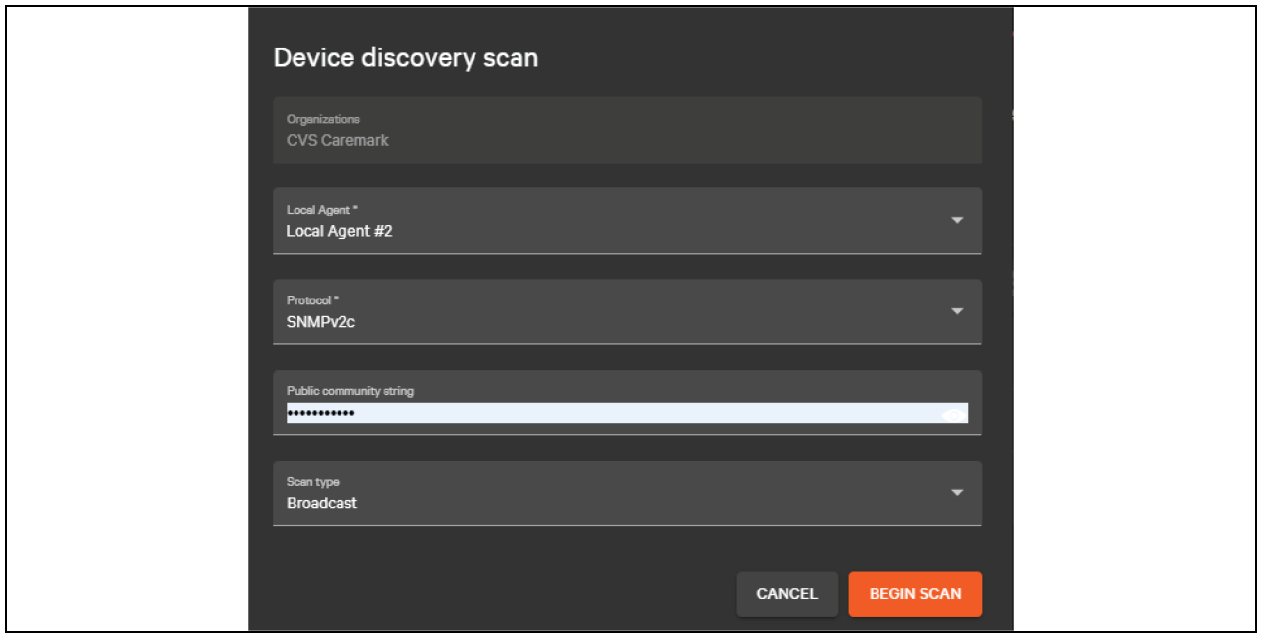
Then click **Scan for devices** from drop down menu.

Figure 7.1 Adding a Device Under a Customer



When you select **Scan for devices**, a dialog box opens with discovery scan options.

Figure 7.2 Broadcast Discovery Scan



Since the user in this case initiated the scan from under a customer, the Organization (Customer) is auto selected . If the customer has only one local agent, this is auto-selected as well. If the customer has multiple local agents, they can select the one from which they wish to scan from the drop down.

NOTE: If you start a scan from the Devices List, you'll need to select the organization manually.

For most devices , the discovery scan uses SNMP polling to identify a device using common fields such as manufacturer and model. From the scan dialog the user can provide the SNMP credentials for the devices to be scanned.

There are two scan options: **Broadcast** and **IP Range**. Choose the scan type by selecting the **Scan Type** from the drop down.

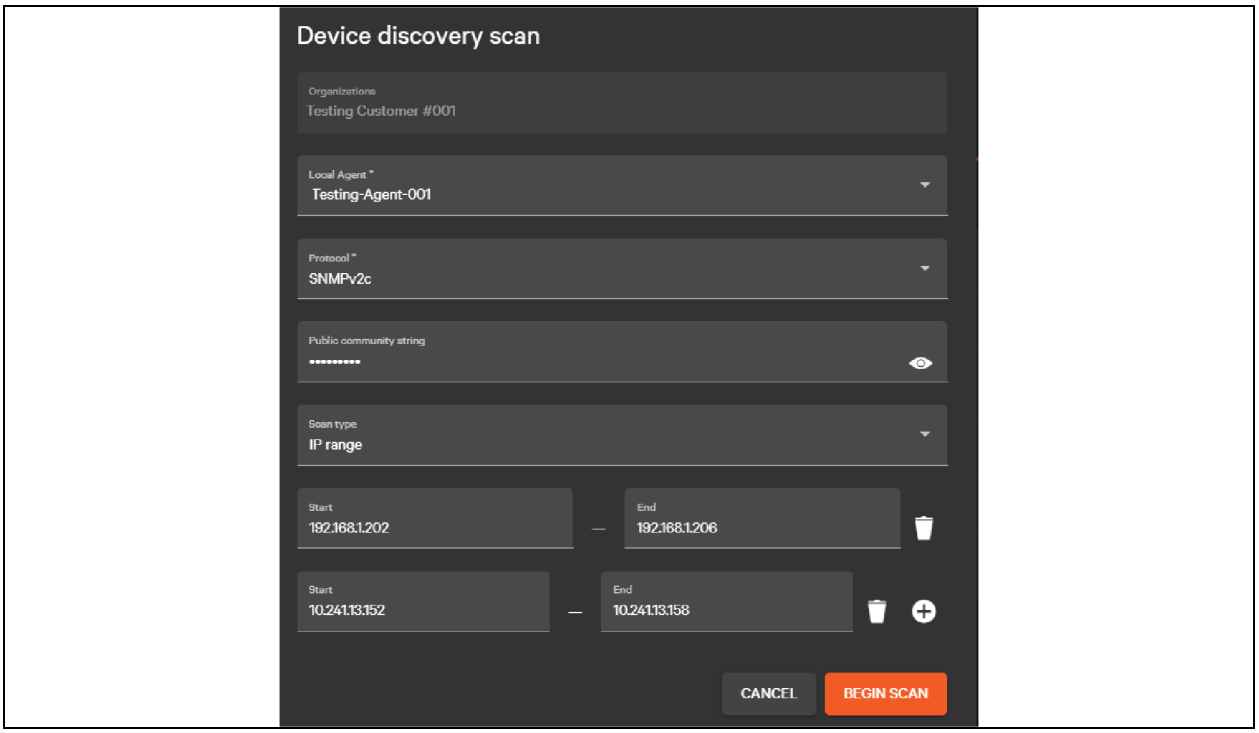
If default credentials are provided at the customer level, these will be populated in the Discovery dialog. See SNMP Credentials on page 34.

IMPORTANT! Currently devices communicating through an Intellislot card (Unity/RDU101) and third party devices require SNMP to be enabled to be identified via a scan. Geist devices (Watchdogs, Geist Upgradeable rPDUs, etc.) can be identified via proprietary protocols that do not require SNMP.

Broadcast scans can take a longer than IP range scans (15 to 90 minutes) but can find both configured and factory-fresh cards and devices on the customer network. This is required for provisioning factory fresh devices that do not have a configured IPv4 address. See Provisioning a Factory Fresh Device on page 143. For the Windows Agent the user will need to have specified a fixed IP address for the agent to run a broadcast scan. See System Requirements on page 58.

IP Range scans can scan one or multiple ranges of IPv4 addresses on different subnets. An IP range scan will only find devices with a configured IPv4 address, either statically defined or assigned by a DHCP server.

Figure 7.3 IP Range Scan with Multiple Ranges



Additional IPv4 ranges can be added by clicking the

Add icon.

Delete an undesired range by clicking the

Delete icon next to the range.

After the customer, agent, specified SNMP credentials, and set the type of scan have been selected, click **Begin Scan** to run the discovery scan. Discovery scans run as a background process, so the user can conduct other activities in the platform while the scan is running.

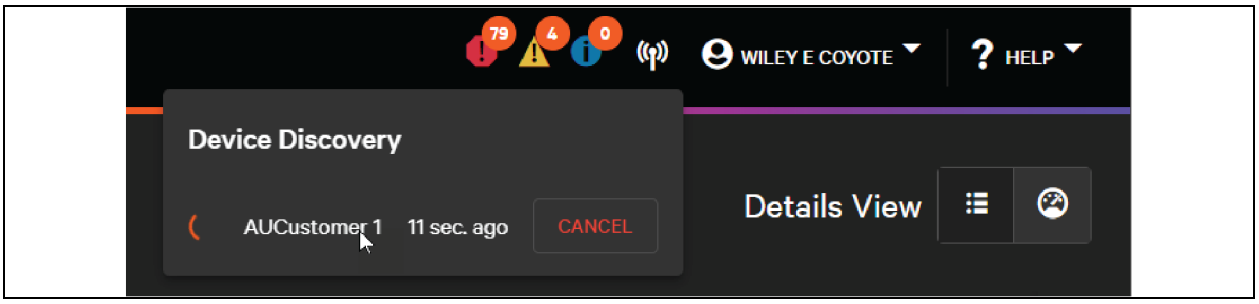
IMPORTANT! IPv6 range scan is not supported.

Check the status of a running scan or cancel a discovery by clicking the

Discovery icon

in the top right corner of the header bar.

Figure 7.4 Running a Scan

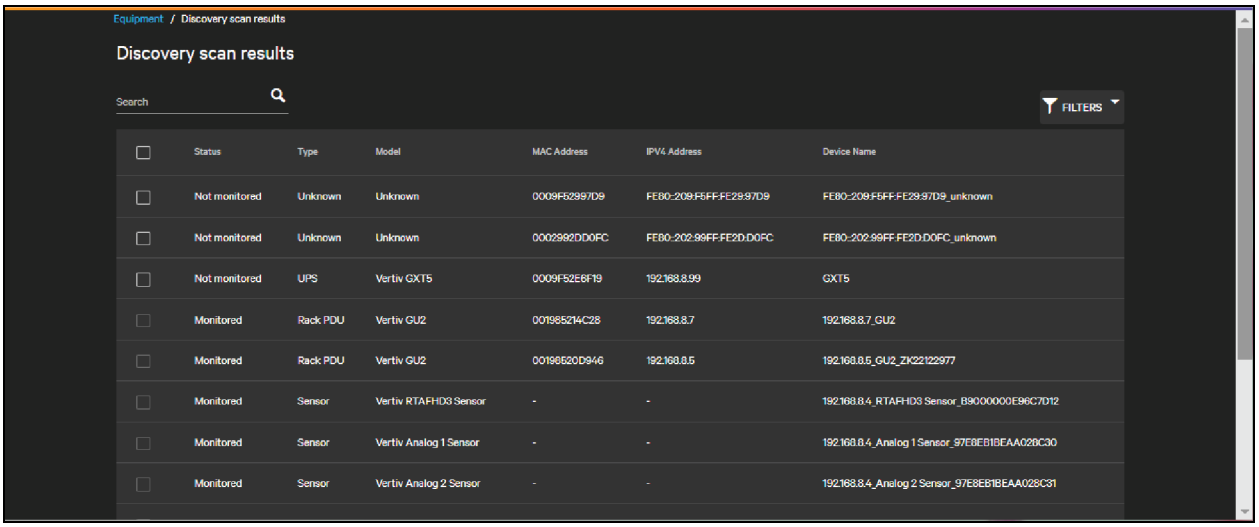


The platform pushes a toast notification when the scan has completed. Additionally, a number is displayed next to the Discovery icon. If the scan failed, try to repeat the asset discovery scan.

When the scan is successful, view the results of the scan by clicking the **Discovery** icon and then clicking **View**.

When the Discovery scan results screen opens, it updates information about discovered devices and devices that have been previously monitored.

Figure 7.5 Loading Discovery Results



NOTE: Multiple simultaneous discovery scans are not supported currently. We also recommend the user remain logged-in during the scan.

Devices that have been monitored previously are indicated in the Status column. If the device model is recognized, information about the type of model of the discovered device is provided.

Devices that cannot be identified are listed as type and model unknown.

NOTE: Connect supports both Vertiv and 3rd party equipment, with new devices supported frequently. If a device is not currently supported, you can request a new template see Request a New Template on page 188.

The MAC address for the device, if applicable, is also stored as a unique identifier.

Select devices to add for monitoring by selecting the checkbox to the left of each device and selecting an asset group for the devices. Click **Add Selected** to add the devices.

A few default asset groups are created for each customer, including **Unassigned** and **New Devices**. Or users can create their own asset group by clicking the

Add icon.

Figure 7.6 Selecting Devices for Monitoring

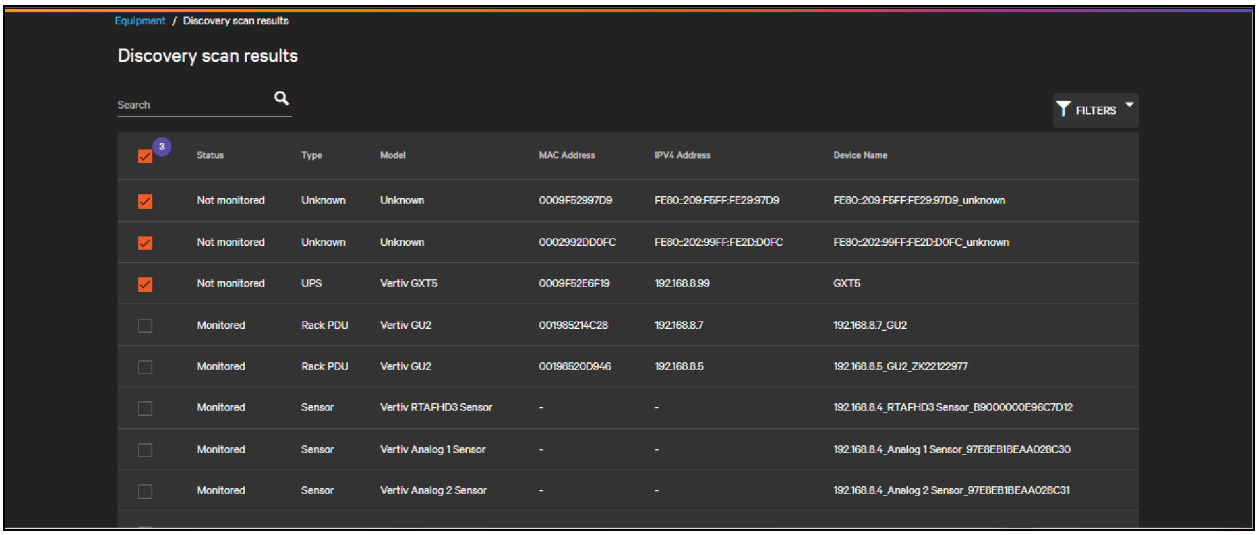
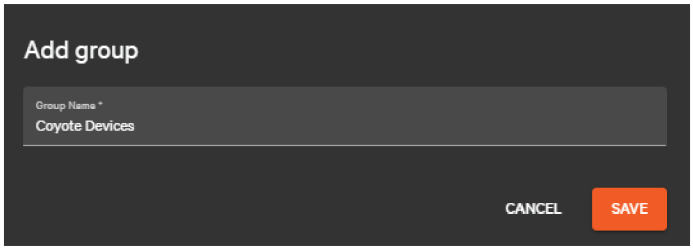


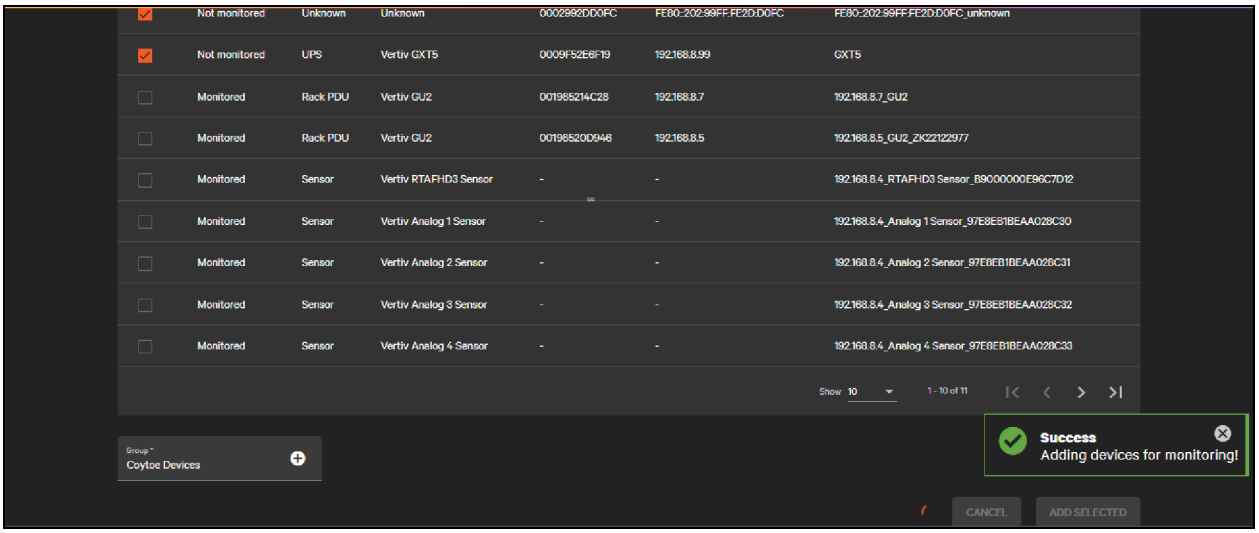
Figure 7.7 Adding a Device Group from Discovery



NOTE: Each device that is to be added for monitoring must have a unique IPv4 address (within the customer). It must have SNMP enabled. Unknown devices can be added for monitoring and users can later select the type, manufacturer, model, and template when editing the device.

Once the devices have been added for monitoring their status will change to **Monitored**. Connect stays on the scan results screen to allow for adding multiple devices. To close the scan results screen, either select **Cancel** or navigate to elsewhere in the product using the menu.

Figure 7.8 Devices Successfully Added for Monitoring

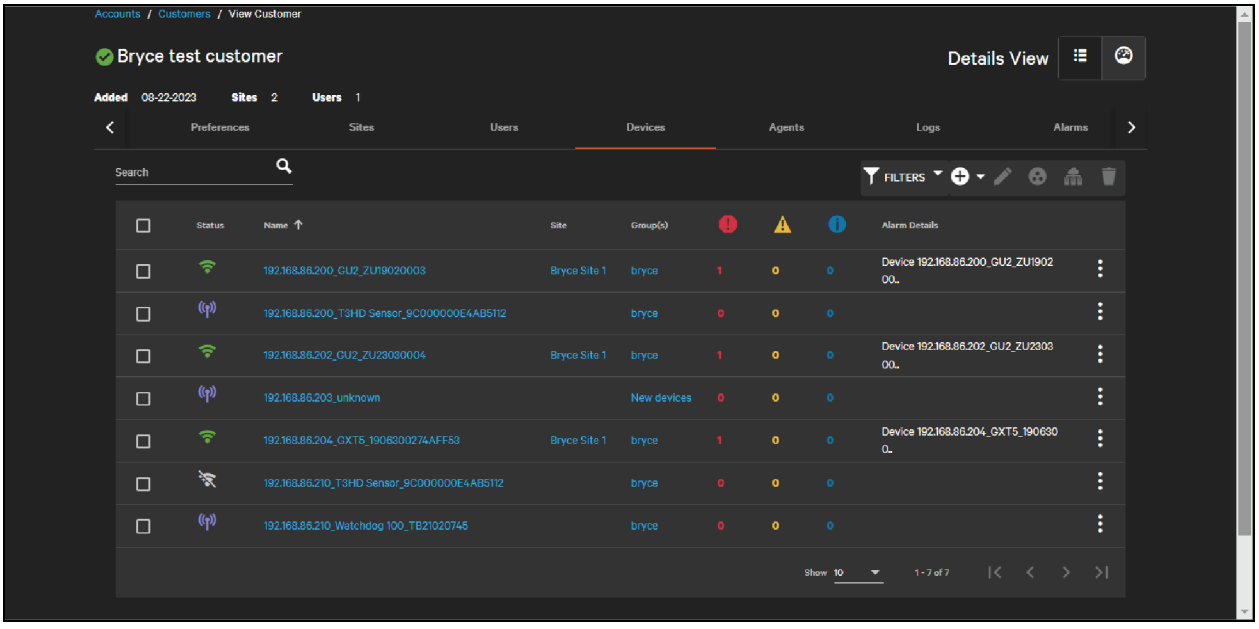


From the Devices tab, you can see devices selected for monitoring as well as unmonitored devices found by the scan.

Unmonitored devices are indicated by a

Discover icon.

Figure 7.9 Device List with Monitored and Unmonitored Devices



Unmonitored devices may be devices that do not have a configured IPv4 address or SNMP credentials, or they may simply be devices the user chose not to add for monitoring.

NOTE: Unmonitored devices do not collect data or create alarms. They can be provisioned (see Provisioning on page 143) or added for monitoring later. Only monitored devices count against the Partner's or Customer's license since unmonitored devices do not collect data or send alarms.

To add these devices later for monitoring, select the checkbox next to the unmonitored device and select **Add for Monitoring** from the

Add icon drop down menu.

Another discovery scan is not needed to be run. This option is only available for unmonitored devices. A device can also be added for monitoring by editing the device and clicking **Add for monitoring in the device details.**

Unmonitored devices can also be deleted by selecting the checkbox next to each device and clicking the

Delete icon.

Monitored devices show their online and offline status with the **Online** and **Offline** icons. Monitored devices collect data, send trap notifications, and can create alarms and will count against the partner or customer's device and datapoint licenses/allocations. See Creating Customers on page 25.

Online icon **Offline** icon

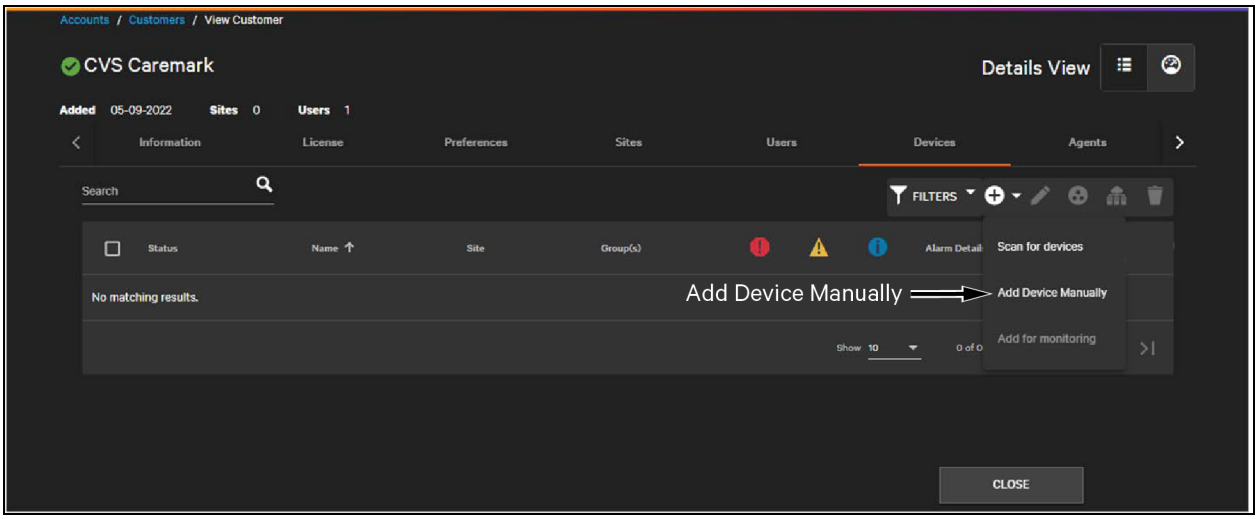
7.2 Adding Devices Manually

Add a device manually by navigating to the Device tab of a specific customer, click the

Add icon

and then select **Add Device Manually**.

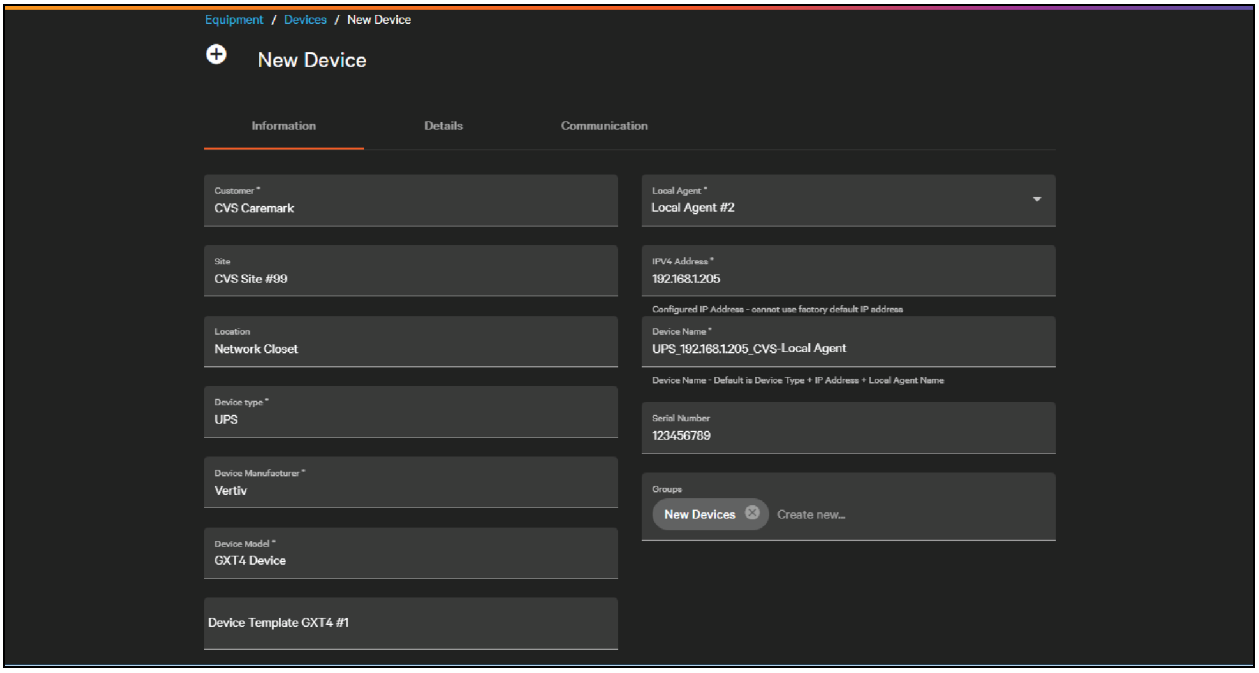
Figure 7.10 Add Device Options from Device Tab Under Customer



The required information for a device is on two tabs: **Information** and **Communication**.

7.2.1 Information Tab

Figure 7.11 New Device Information Tab



The Information tab provides basic identifying information about the device (model, location, IP, etc.) and has fields as listed in Table 7.1 below.

Table 7.1 Information Tab Fields

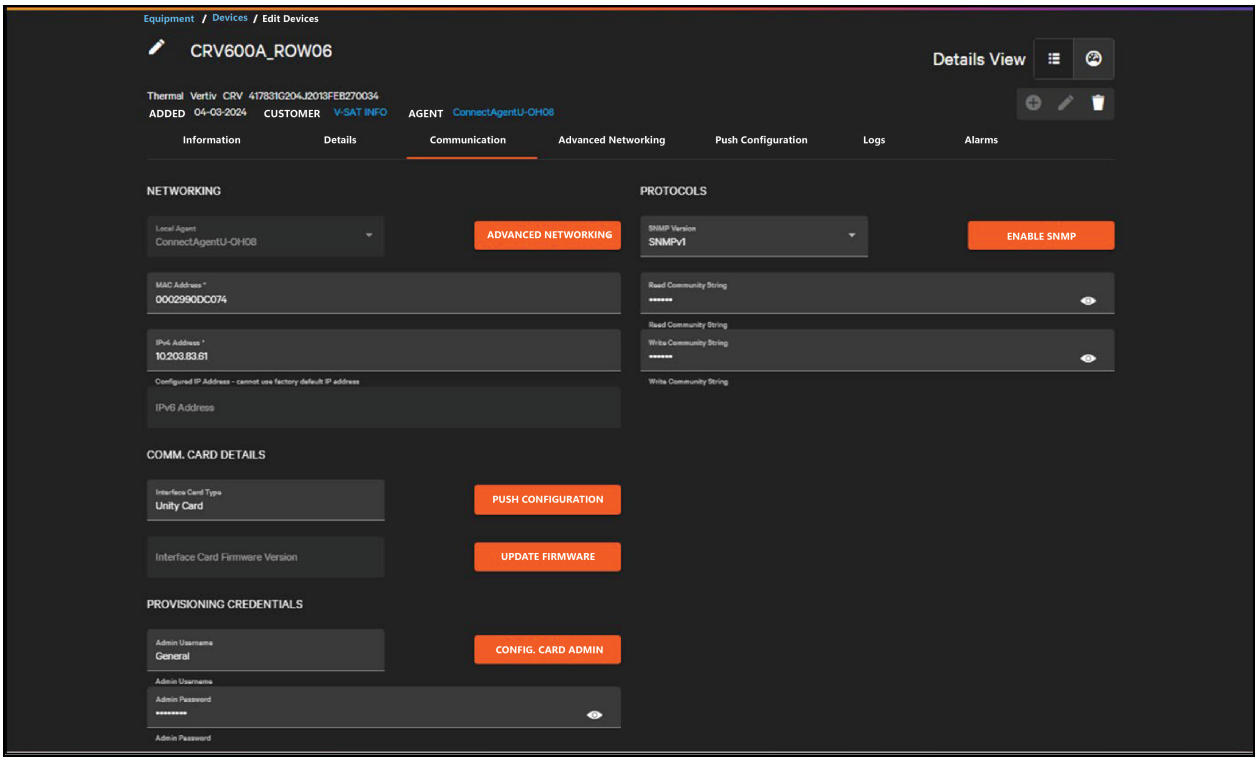
Field	Required or Optional	Description
Customer	Required	Drop down list for the customer that owns the device. This field auto-populates if adding the device from a customer or agent.
Site	Optional	The site where the device is physically located. Drop down list is populated by the sites created in the customer.
Location	Optional	Free form text field for detailed information about the device's location, such as the 2nd floor network closet.
Device Type	Required	Drop down list for the type of device (UPS, Thermal, etc.) being monitored.
Device Manufacturer	Required	Drop down list of manufacturers for supported devices.
Device Model	Required	Drop down list of supported models. Model is a broader category than a specific SKU, more akin to a model family.
Device Template	Required	Drop down list of templates available for the selected model.
Local Agent	Required	The local agent monitoring the device. This auto-populates if adding the device from an agent. Currently, Connect requires a local agent for all monitored devices.
IPv4 Address	Required	IPv4 address of the monitored device. Must be unique within the customer.

Table 7.1 Information Tab Fields (continued)

Field	Required or Optional	Description
Device Name	Required	Free-from text field to enter the device name. A default name is built from the Device Type, Agent, IPv4 address selected.
Serial Number	Optional	Serial number of the device. This is also polled from the device (if available) after communication is established.
Groups	Optional	The device groups to which the device belongs. A single device can be a part of multiple device groups. See Device Groups on page 110.

7.2.2 Communications Tab

Figure 7.12 Device Communications Tab



The Communication tab includes more advanced network information (including SNMP credentials, MAC address, comm. card, and provisioning credentials). The fields on this screen are detailed in Table 7.2 below.

Table 7.2 Communications Tab Fields

Field	Required or Optional	Description
Local Agent	Required	Synced with the selection on the Information tab.
MAC Address	Required	Used to uniquely identify a device within the customer's network This is especially relevant where multiple factory-fresh devices have the same default IPv4 address.
IPv4	Required	Synched with the value on the Information tab.
IPv6	Optional	This is read-only when adding a device manually. It is populated when a broadcast scan finds a device.

Table 7.2 Communications Tab Fields (continued)

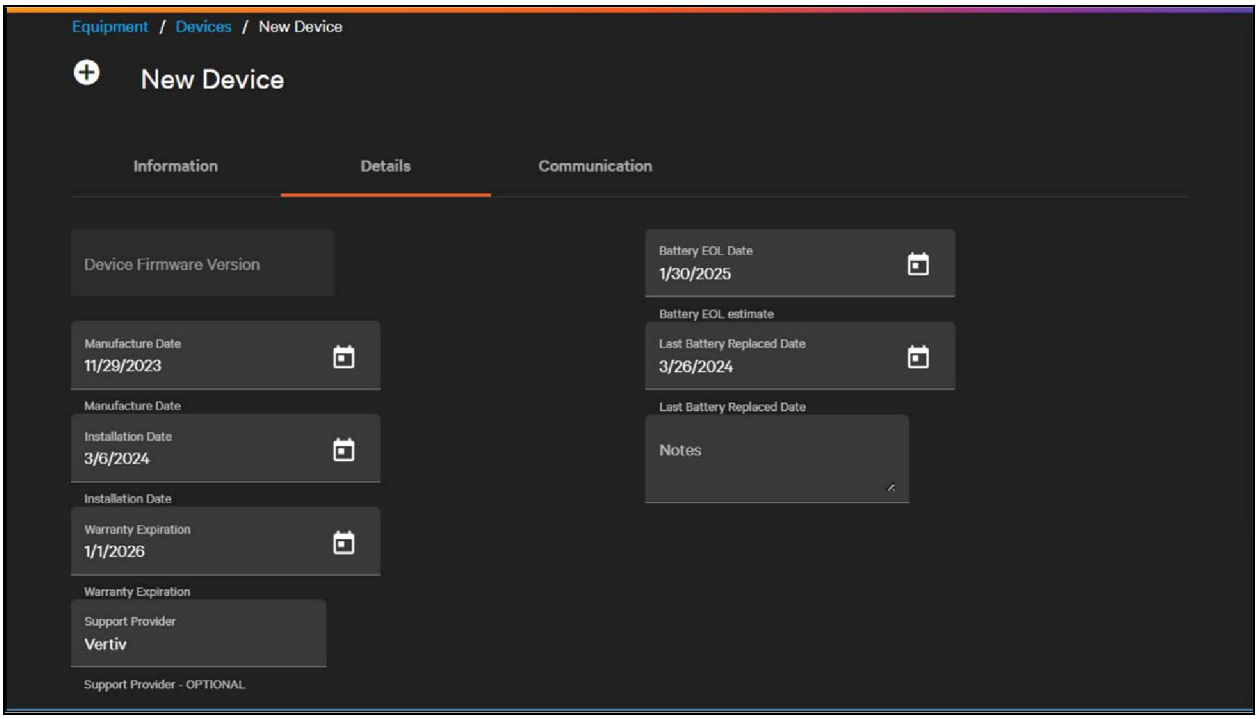
Field	Required or Optional	Description
Interface Card Type	Required	The communications card of interface used to connect a device to the customer network. For Geist devices (Watchdogs, Geist Upgradeable rPDUs, etc.), select **Integrated**.
Interface Card Firmware Version	Read-only	This is populated after the communications card/interface is communicating with the Connect platform.
Provisioning Credentials (Admin Username)	Optional	Used to authenticate provisioning actions or to create an admin user on a factory-fresh device. See Provisioning a Factory Fresh Device on page 143.
Provisioning Credentials (Admin Password)	Optional	Used to authenticate provisioning actions or to create an admin user on a factory-fresh device. See Provisioning a Factory Fresh Device on page 143.
SNMP Version	Required	Connect supports SNMPv1, v2c, and v3.
Read Community String	Required	SNMP v1, v2c only. Used to poll data from the edge device.
Write Community String	Optional	SNMP v1, v2c only. Used for pushing device configurations on devices that communicate via an Intellislot communications card. See Pushing Configurations to Cards and Edge Devices on page 156.
Authentication Type	Required	SNMP v3 only. Drop-down menu of authentication type options for SNMP v3. Possible values: None, MD5, SHA-1, SHA-256, SHA-384, SHA-512., Not all devices supported by Connect support all possible authentication types.
SNMP Username	Required	SNMP v3 only. Used with authentication secret to authenticate and poll data for SNMP v3. See SNMP Credentials on page 34
Privacy Type	Required	SNMP v3 only. Drop down menu of privacy type options for SNMP v3. Possible values: None, DES, Triple DES, AES, AES-192, AES-256. Not all devices supported by Connect support all possible privacy types. See SNMP Credentials on page 34 to confirm privacy type is supported on the specific device.
Authentication Secret	Required	SNMP v3 only. Required if Authentication Type is not None. Used with username to authenticate and poll data for SNMP v3.
Privacy Secret	Required	Required if Privacy Type is not None. Used to authenticate and poll data for SNMP v3.

SNMP and provisioning credentials auto-populate if the customer has provided default credentials at the customer level. See Customer Preferences on page 33.

7.2.3 Details Tab

The Details tab contains optional information used for device and lifecycle management tracking.

Figure 7.13 Device Details Tab



Details on the Detail tab are listed in Table 7.3 below

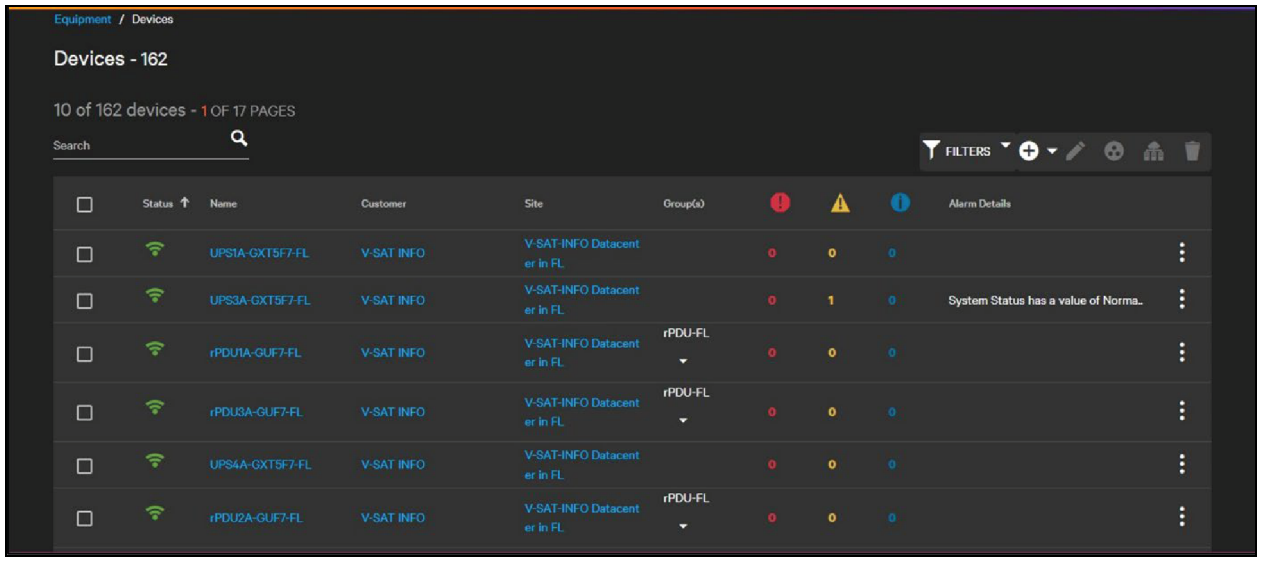
Table 7.3 Detail Tab Fields

Field	Required or Optional	Description
Device Firmware Version	Read Only	Reported from the device after it is communicating with Connect.
Manufacture Date	Optional	Manual date picker entry for when the device was manufactured. Some MIBs provide this a pollable information. However, for the current version of Connect, the field is set with manual entry.
Installation Date	Optional	Manual date picker entry for when the device was installed.
Warranty Expiration	Optional	Manual date picker entry for when the warranty will expire for the device.
Support Provider	Optional	Free-form text entry field for an organization task providing service to the specific device (repair companies, preventative maintenance, etc.).
Battery EOL Date (UPS Only)	Optional	Manual date picker entry for when the UPS battery is expected to expire.
Last Battery Replaced Date (UPS Only)	Optional	Manual date picker entry for when the battery was last replaced in the UPS.
Notes	Optional	Free-form text entry for any device information not captured by other fields.

7.3 Device List

The device list shows a list of the devices that have been added to the system, either manually or via discovery. It includes devices added for monitoring and unmonitored devices. Many context-specific device lists exist underneath other entities in the system. The local agent, customer, asset group, and site entities all have device lists as a tab, and there is also a general device list under the Equipment menu. The functionality of all these lists is the same, and devices can be added from any of these places.

Figure 7.14 Device List in the Equipment Menu



The Device list columns are described in Table 7.4 below.

Table 7.4 Device List in Equipment Menu

Column	Description
Status	Has four possible values: • Online • Offline • Unmonitored • Disabled
Name	Name of the device. Clicking Name takes you to the details page.
Model	Model of the device. In the form <<Manufacturer>><<Model>>(<<Device Type>>)
Customer	The customer who owns the device. **NOTE: On some tabs, this column is hidden since the customer is known from context.**
Site	If a site has been assigned to the device, it is displayed here.
Group(s)	If the device has been assigned to 1-n groups, they are displayed here. This field is a drop down.
Alarm Counts	Shows the count of active alarms on each device, split by severity (critical, warning, informational). Each count can be sorted individually.
Added	The date the device was added for monitoring.

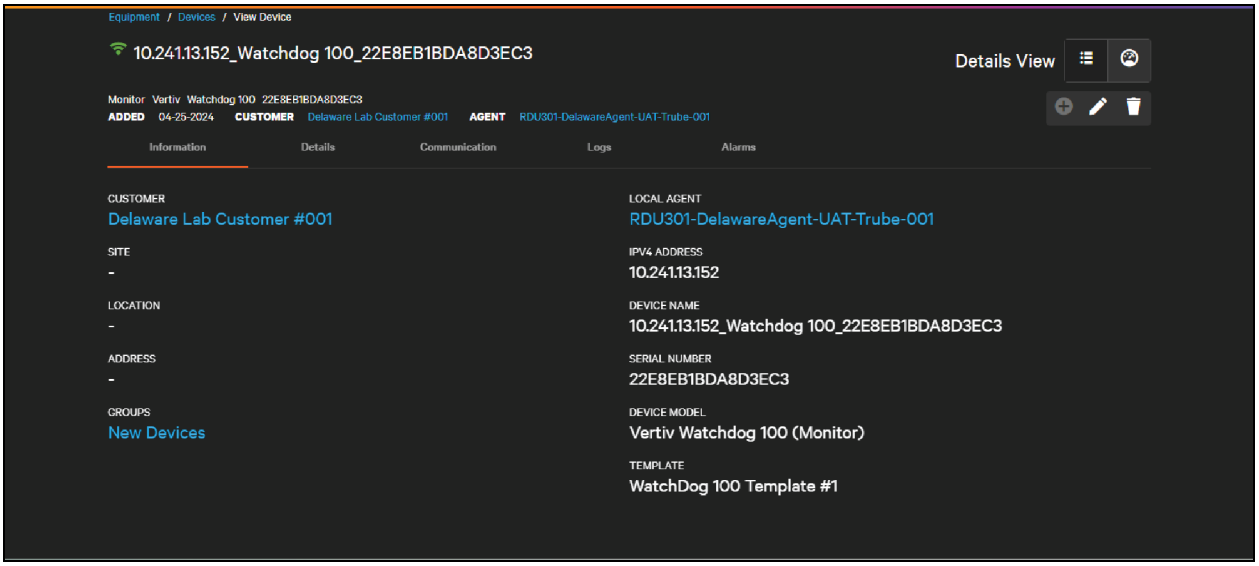
Like other lists in Connect, each column is searchable, sortable, and filterable.

From the device list, these actions can be completed: adding new devices, editing existing devices, adding/removing devices from device groups, and deleting devices. These actions are available by clicking an individual device, clicking the pull down menu, or clicking an action button in the top right.

7.4 Device Details

Clicking on an individual device takes you to its read-only device details page.

Figure 7.15 Information Tab Read-Only Devices



See Information Tab on page 98, Device Details above, and Details Tab on page 101

After a device has been added to the system, logs for any event that have occurred on the device (including audit logs for changes to device configurations) and a list of active alarms can be seen. You can toggle between the details view and the visual view (dashboard) by clicking the

Details icon

Dashboard icon

7.5 Device Dashboard

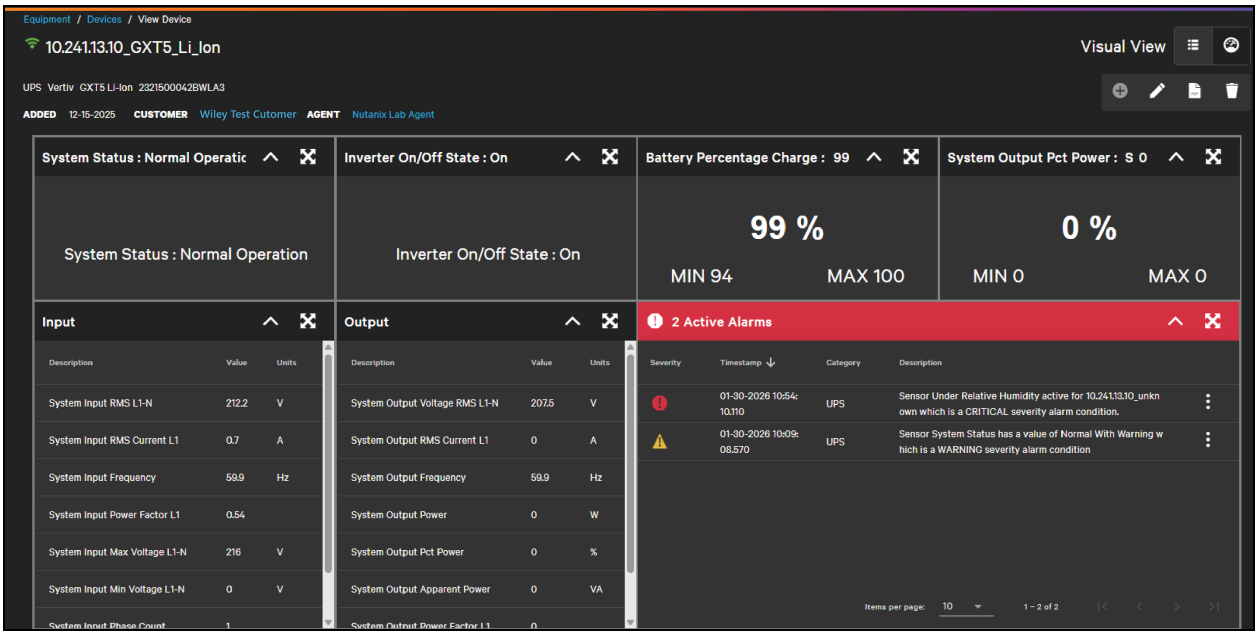
Users can toggle to the dashboard from the device details page by clicking the

Dashboard button.

The device dashboard is a collection of widgets showing important current values, graphs of trended information, active alarms, and logs. The exact dashboard is determined by the model and template selected. Devices of the same model and template will have the same dashboard configuration.

NOTE: Device dashboards are not editable or customizable.

Figure 7.16 Example Dashboard with an Active Alarm

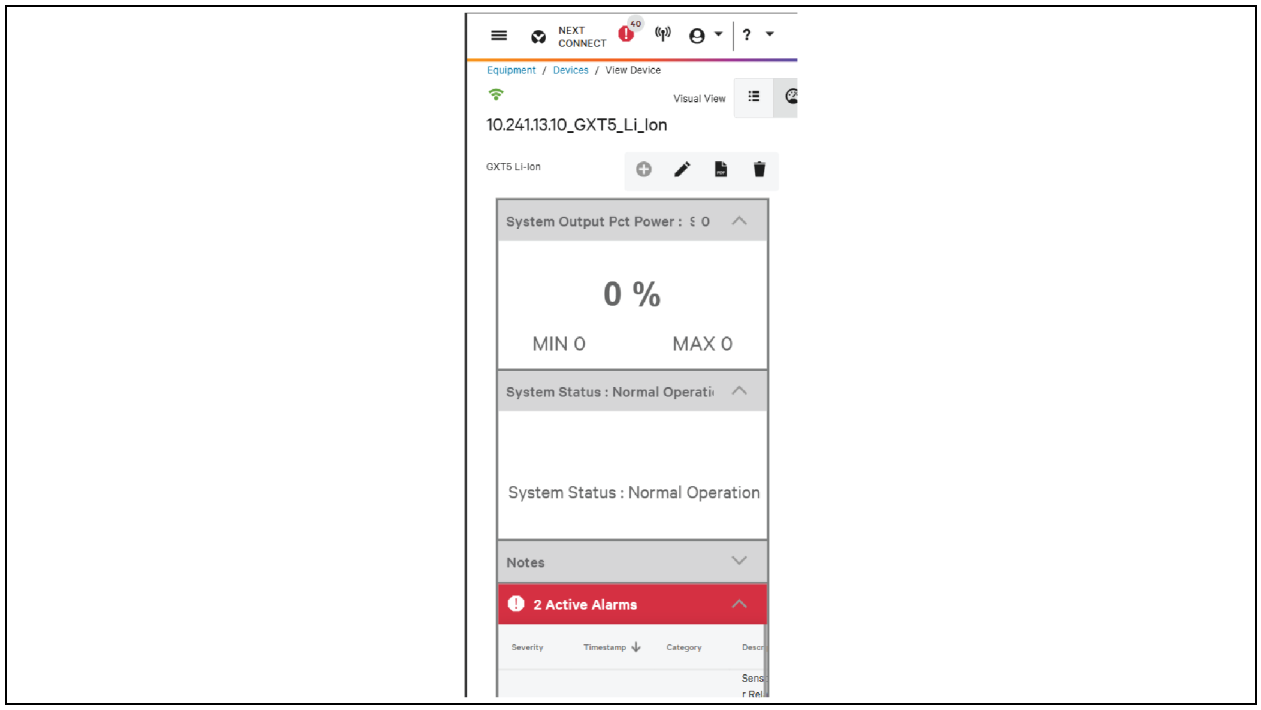


For this current release, device dashboards can include:

- **Value Widgets**—These highlight a critical value on the device and can be numeric or text.
- **Group Widgets**—Show a related data (text and numeric) in a single widget.
- **Active Alarms**—Shows any alarm that is active on the device.
- **Notes**—Provide area to enter notes about the device directly from the dashboard.
- **Line Graph**
- **Bar Graph**

Additional widgets and capabilities will be added in future releases.

Figure 7.17 Mobile Dashboard View



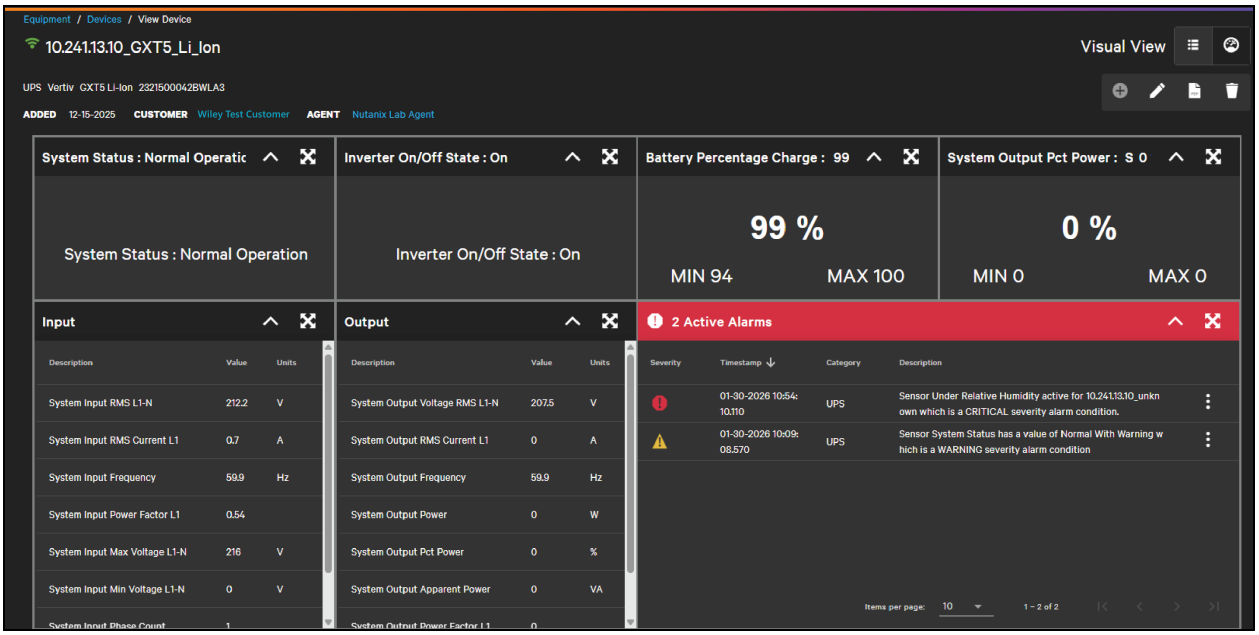
Connect is designed to be viewed on both desktop and mobile devices. On mobile devices, you can minimize/maximize individual widgets by clicking the **Minimize** and **Maximize** icons.

Minimize icon

Maximize icon

The headers of value widgets show the current value when minimized widget headers will also change color if alarm conditions are active.

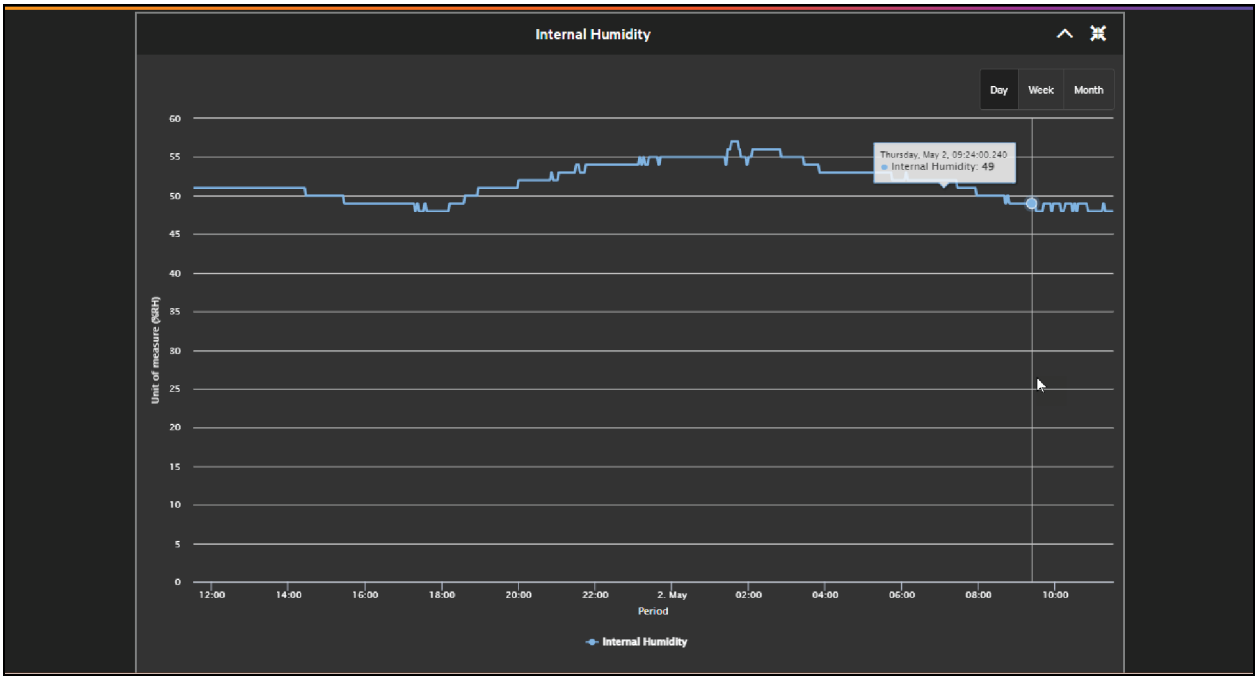
Figure 7.18 Dashboard with Normal Widgets



Some information, like maps, graphs, or lists, are best viewed when expanded. Users can expand an individual widget, so it takes up the full view. Toggle back to the normal view by clicking the collapse button.

Expand icon Collapse icon

Figure 7.19 Dashboard with Expanded Graph Widget



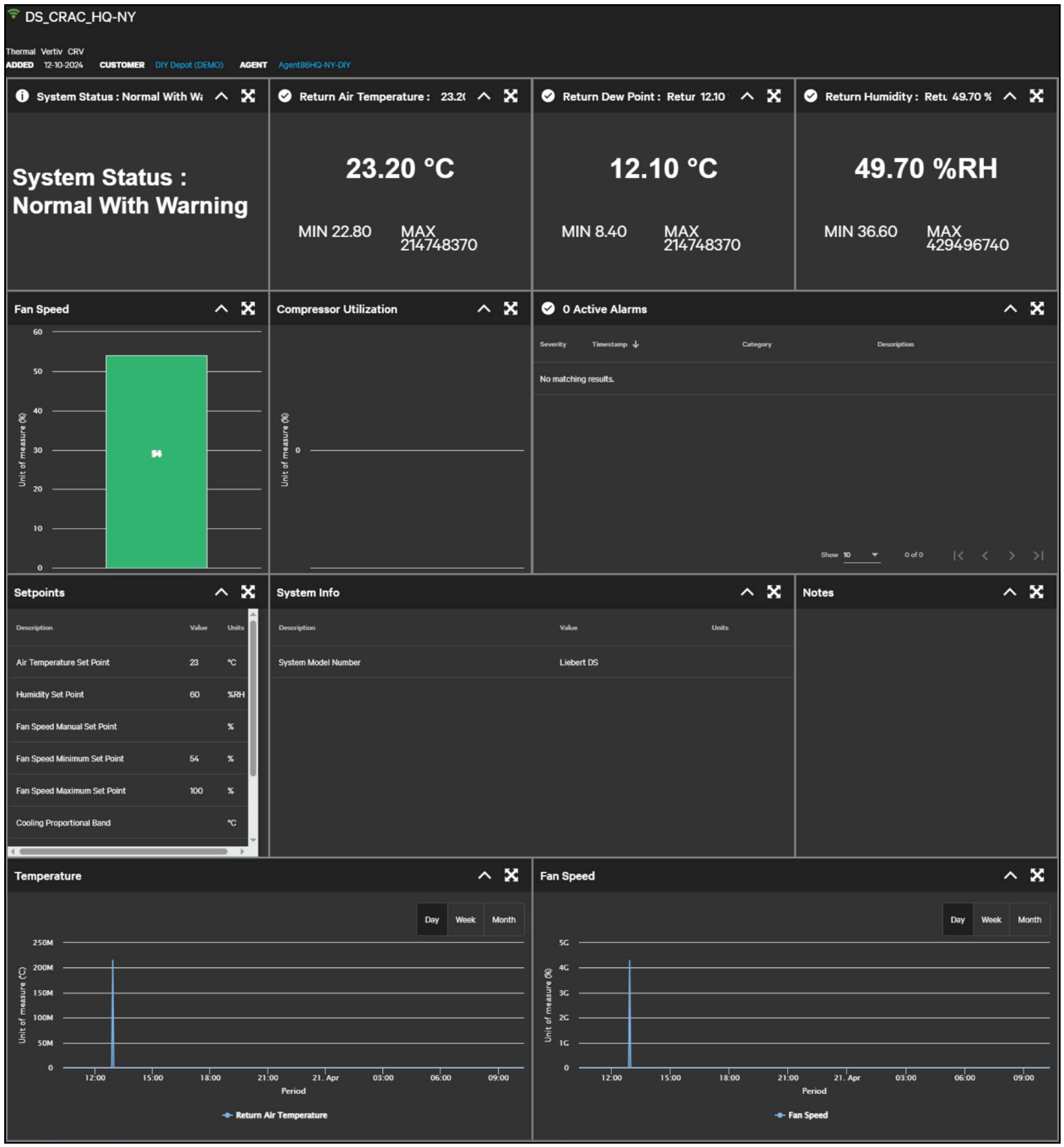
A snapshot of the device dashboard can be exported to PDF. This can be helpful in sharing diagnostic information with a third-party who might not have access to Connect, or for documenting problem states for error reporting.

To save a device dashboard to PDF, click the

 **PDF Export** icon

in the top right-hand corner of the dashboard (between the edit and delete icons). The buttons will disappear momentarily while Connect takes a snapshot of the page, and then a file with a name in the form ***{device_name}_Dashboard_{datetime}.pdf*** will be created and downloaded.

Figure 7.20 Dashboard Exported to PDF

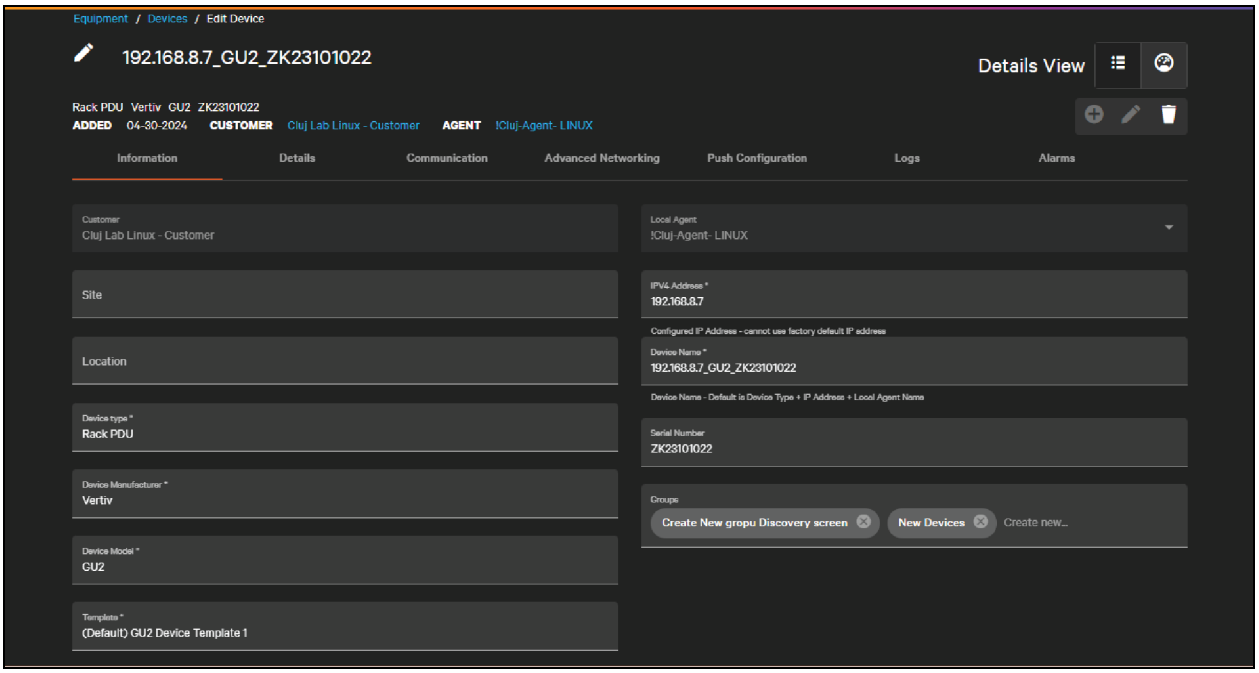


7.6 Editing Devices

Users can edit the details of their existing devices by clicking the **Edit** icon from the device details or visual views.

Edit icon

Figure 7.21 Editing a Device



The customer and local agent fields cannot be changed after a device has been added to the system. Devices can be moved from one site to another and can be added/removed from groups. Devices cannot be moved from one agent to another or to one customer to another and retain historical data. To move a device, you must delete it from the system and then re-add it manually or via a scan to a different agent or customer.

If the device was first discovered as an unknown device, the user can set the device type, manufacturer, model, template, and comm. card to correctly identify the model (if the model is supported by Connect).

NOTE: Changing the IPv4 address using the field on the Information or Communications tab does not change the IP address on the edge device. Changing the IP address on the Information or Communications tab changes the IP address that the agent polls for this specific device. Users can change the IP address via the provisioning process. See Provisioning on page 143. Changes to the serial number may be reverted to a value for the serial number is polled from the edge device.

7.7 Deleting Devices

Delete devices by selecting one or more devices from the device list and clicking the

Delete icon

Individual devices can also be deleted from its device details page or by using the

Pull down menu

Deleting a device deletes device asset data such as name, model, and installation date but also historical data stored for that device. It also clears active alarms pertaining to that device. The device and its associated datapoints are freed up from license utilization. Historical data such as alarms, logs, and trends are removed when deleting a device. Re-adding a device will have history from the point it was re-added.

Only users with access to a specific device and the Device management permission can delete devices.

Deleting a device is irreversible. However, if the device is still communicating on the customer network, it can be re-added to the system manually or via a device discovery.

NOTE: If an unmonitored device is deleted, it may be re-added to the system via another discovery if the device is still active on the network.

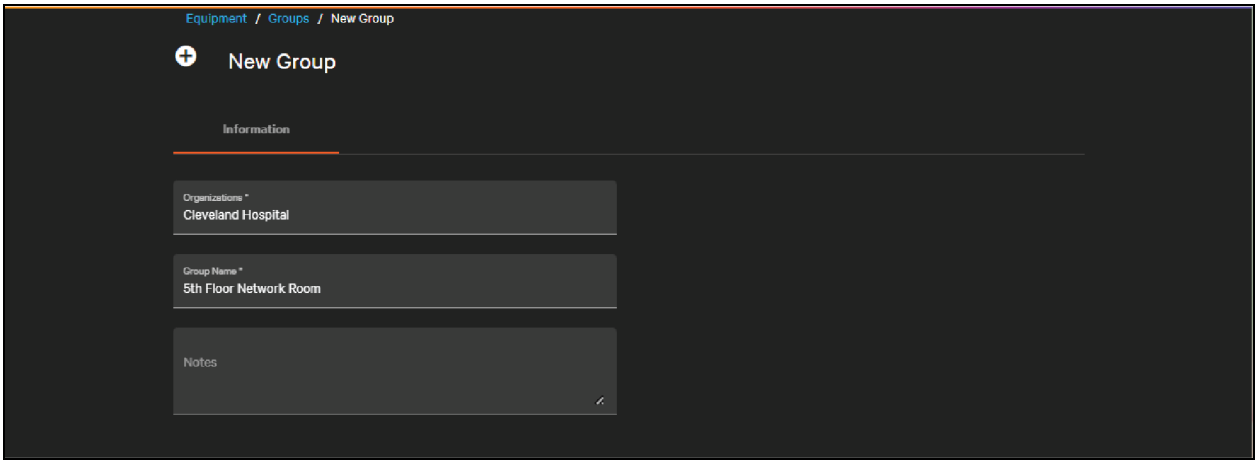
7.8 Device Groups

Device groups are a generic grouping mechanism for signifying sets of devices.

They can be used to signify device in the same physical location such as a specific row/rack or even devices working together as a single device.

Device groups can also be used generically to classify or group devices in such ways as "noisy devices" or "Steve's devices." Groups are contained within a specific customer. A single group cannot contain devices from multiple customers.

Figure 7.22 New Device Group

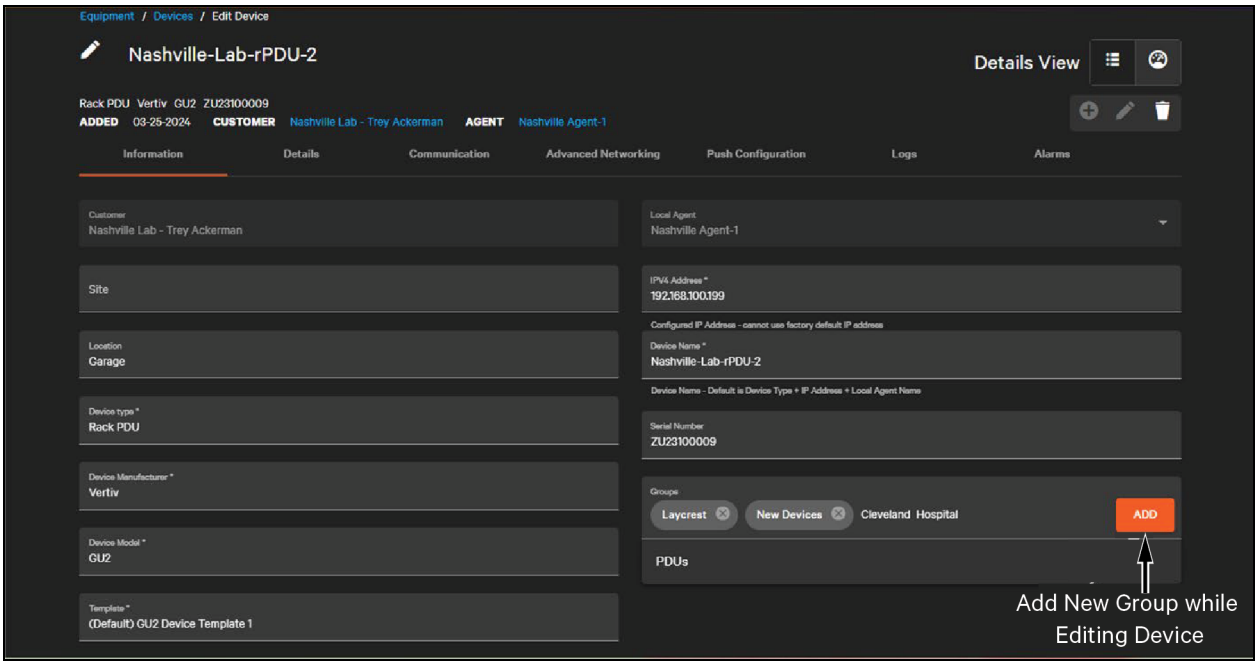


Add groups from the Device Groups list under the Equipment menu by clicking the

Add icon

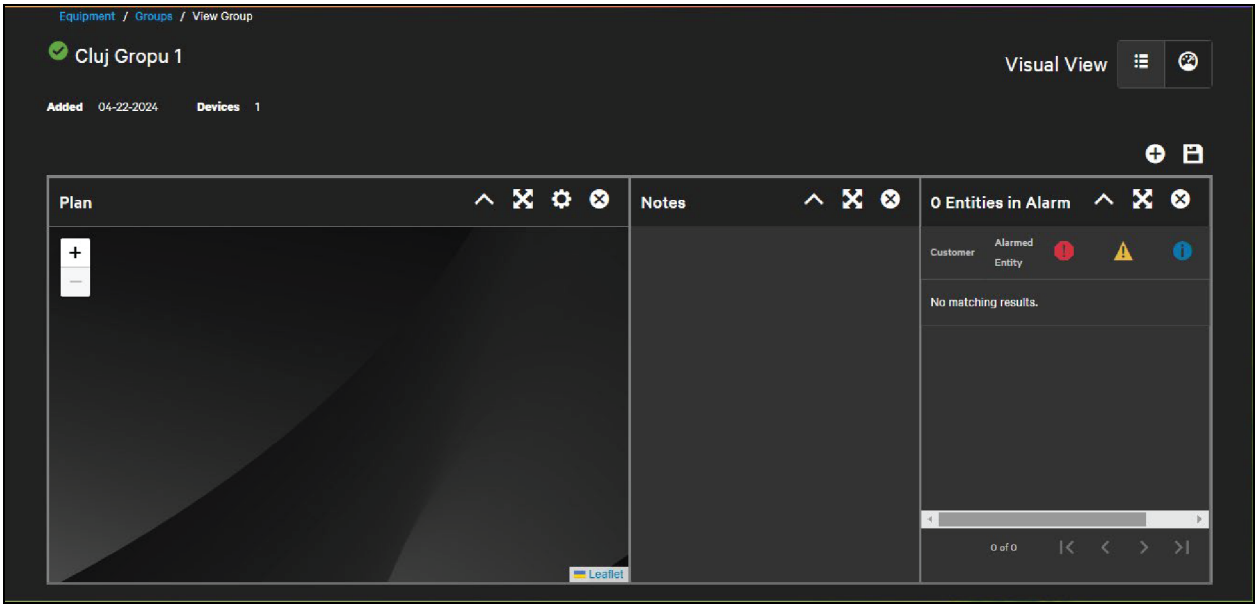
Groups can also be created when editing a device by typing a new group name in the groups field for the device and then clicking **Add**.

Figure 7.23 Add Group from the Groups Field in a Device



The only required field for a group is **Name**. There is an option to add notes and an option to customize the dashboard for the group.

Figure 7.24 Default Group Dashboard



See Basic Dashboard Editing on page 121 and Widgets on page 124 for further details on configuring dashboards.

A device can belong to one or more asset groups. Users can add devices to groups in multiple ways. The easiest for an individual device is to go to its device details page and select the group(s) it is part of from existing groups or to add more as shown in Figure 7.23 on the previous page.

If multiple devices need to be added to a group there are two ways to accomplish this:

- Grouping Devices from the Device List below
- Grouping Devices from a Device Group on the facing page

7.8.1 Grouping Devices from the Device List

On the device list the user can select one or more devices, then click the group button to add or remove groups from those devices.

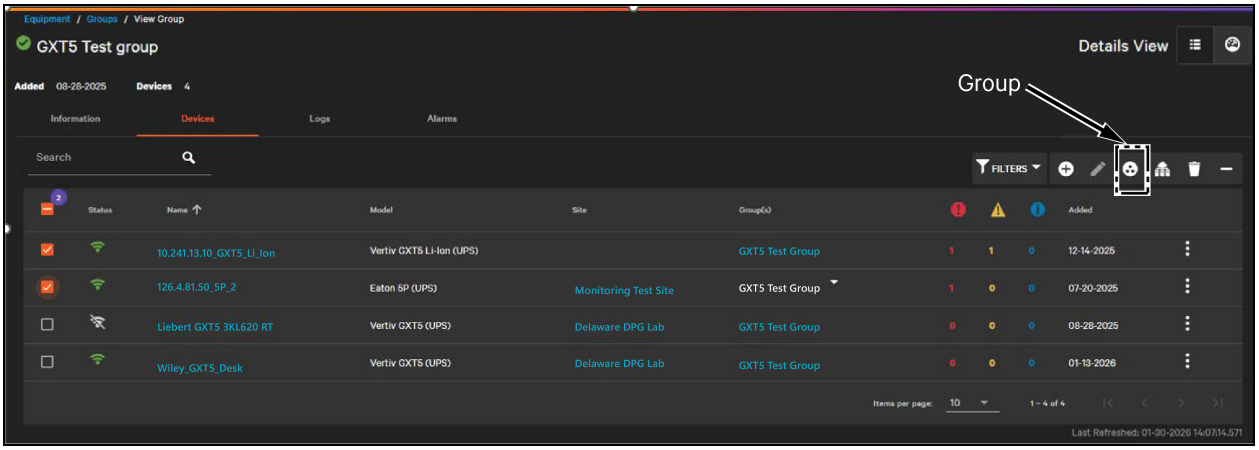
Select one or more devices on the device list and then click the

Group icon

to add or remove groups from those devices.

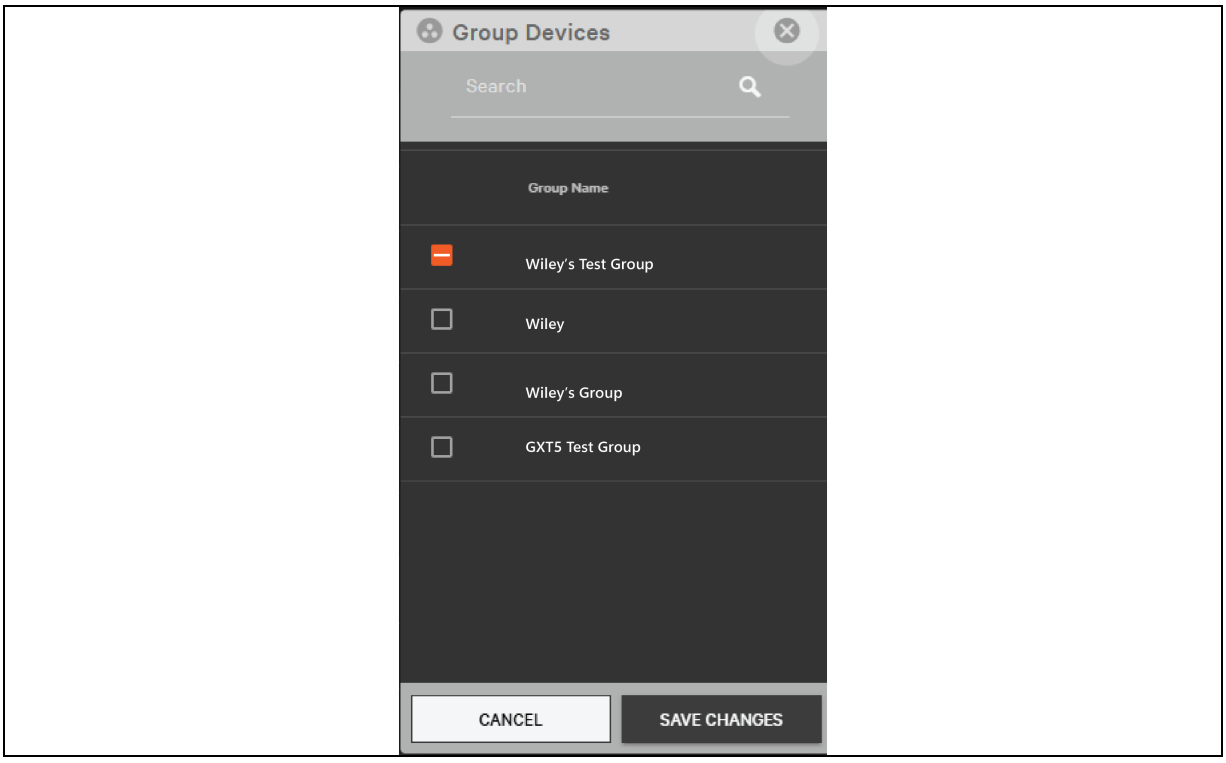
The selected devices must be all under the same customer, otherwise the Group icon is unavailable.

Figure 7.25 Multiple Devices Selected to Add to a Group



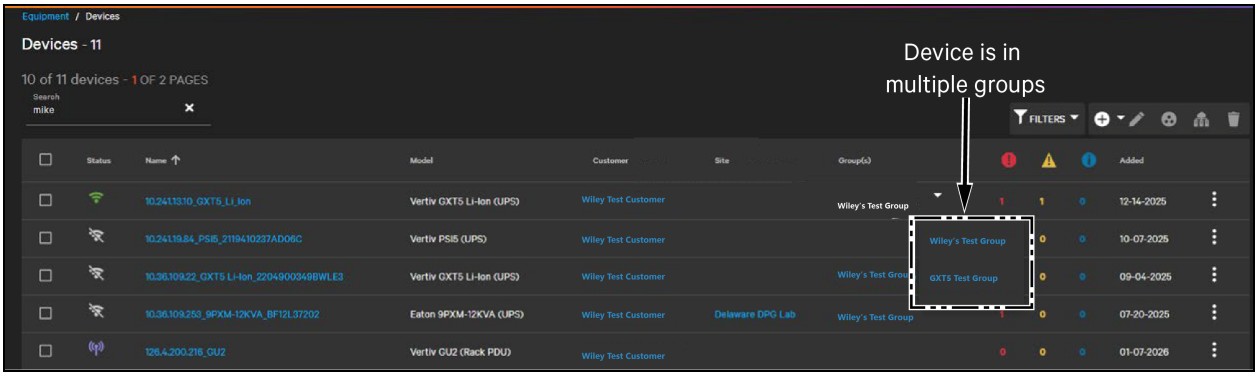
A dialog opens to show the available groups for the devices selected. Select one or more groups to assign to the selected devices and click **Save Changes**.

Figure 7.26 Adding Select Devices to a Group



If a device has been added to multiple groups, click the drop down Groups(s) field on the device list. This will show all groups that contain the device.

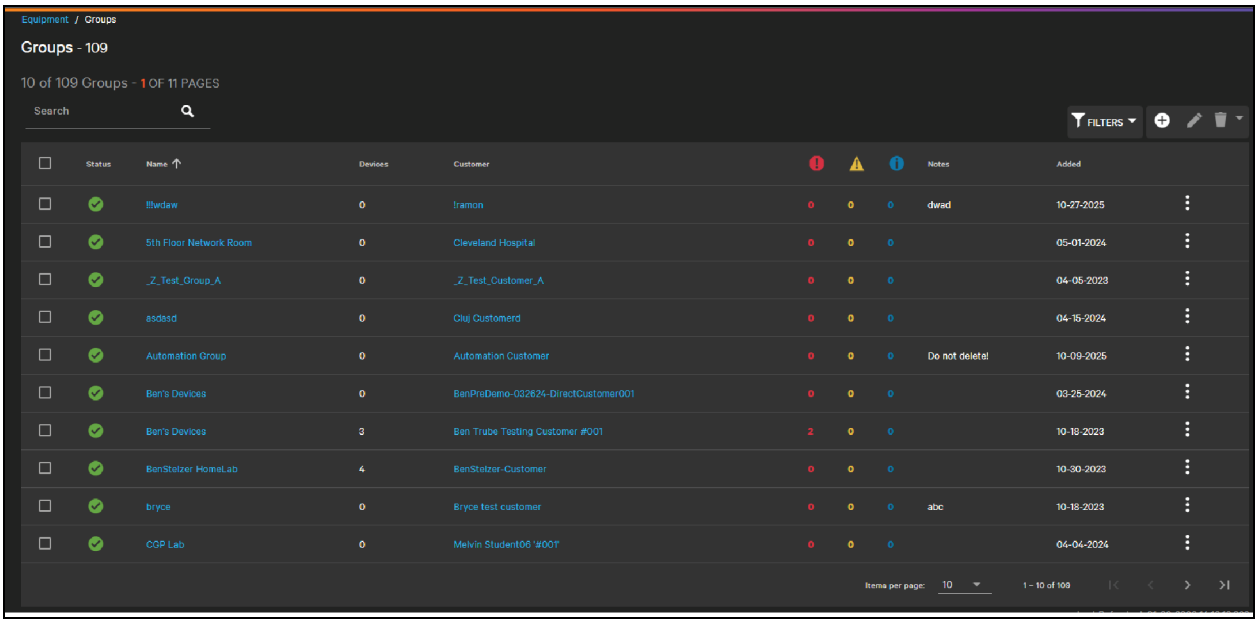
Figure 7.27 Device within Multiple Groups



7.8.2 Grouping Devices from a Device Group

Devices can also be added to a group by going to the Device Groups list and clicking on a specific Device Group.

Figure 7.28 Device Groups List

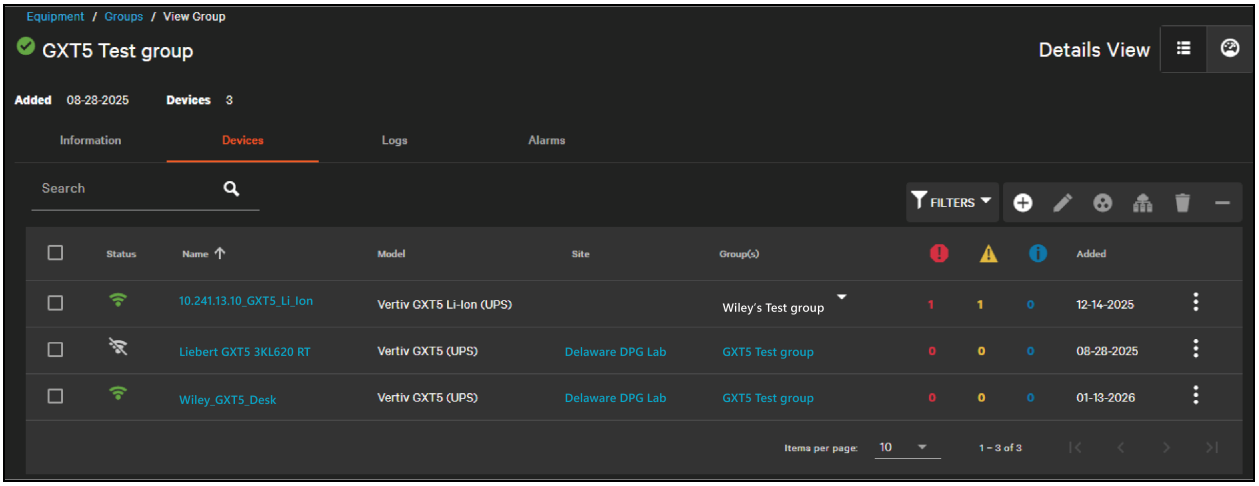


From the Devices tab of the group, click the

Add icon

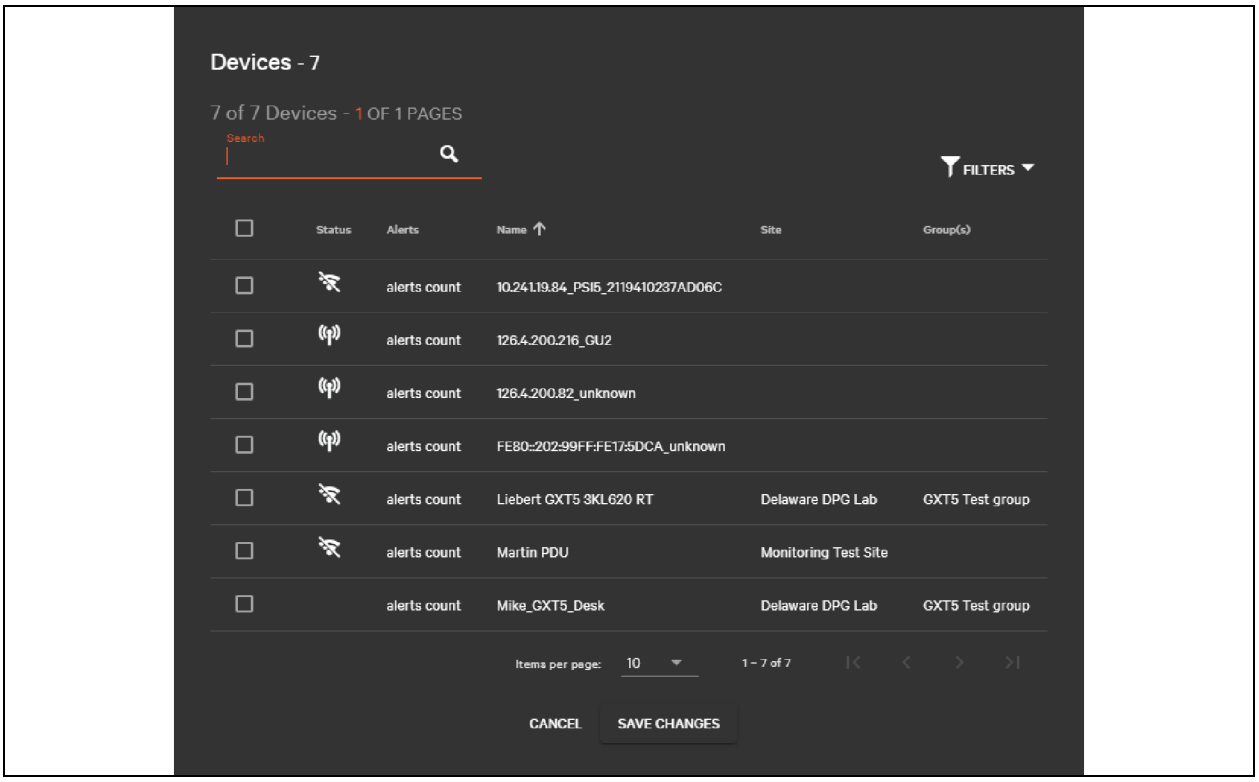
to add existing devices to the group.

Figure 7.29 Device Tab for a Group



The list of devices includes devices that are not already a part of the group is provided. Select one or more devices and scroll down to click **Save Changes** to add the devices to the group.

Figure 7.30 Adding Existing Devices to Group



Remove devices from the group by selecting one or more devices and clicking the

Remove icon.

7.8.3 Deleting Device Groups

Delete device groups created from an individual group or from the device group list by selecting one or more groups and then clicking the

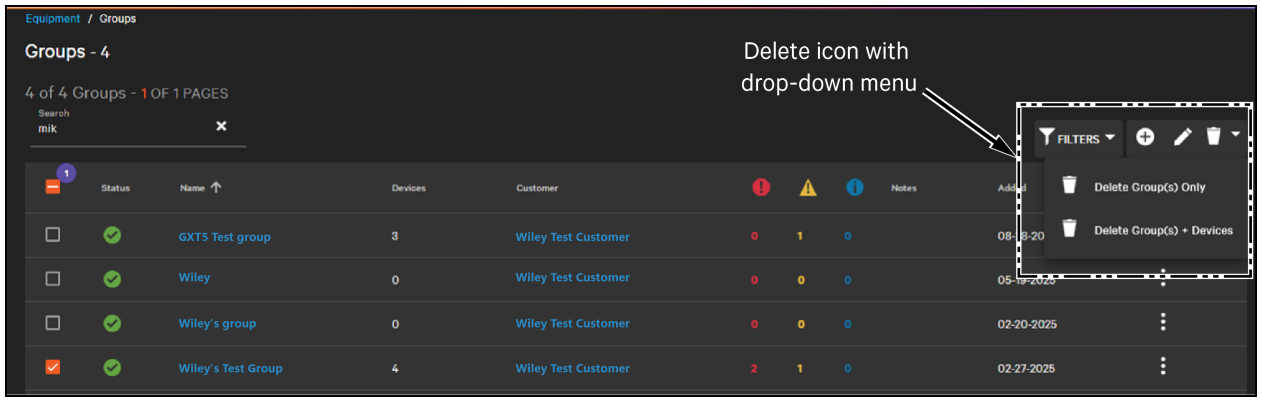
Delete icon

and then selecting the Delete option from the drop down menu.

When deleting a group, there are two choices:

- Delete Groups Only
- Delete Groups + Devices

Figure 7.31 Deleting Groups



When choosing **Delete Group(s) Only**, devices in that group are removed from the group and the group is deleted. The device asset, historical, and alarm data is retained.

When choosing **Delete Group(s) + Devices**, all devices in the group are deleted including historical, asset, and alarm data and then the group itself is deleted.

To delete a group, you must have access to the group and to the devices within that group as well as the Device Management permission.

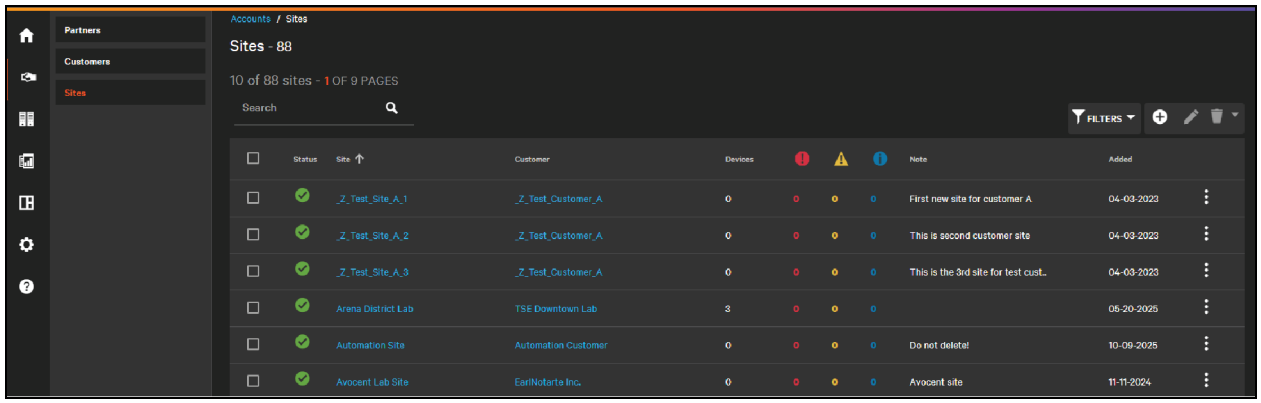
NOTE: Users cannot delete system groups.

7.9 Sites

Sites are a grouping mechanism within Connect that is intended to correspond to physical customer locations with an address. A device can only be physically located within one site, unlike groups which can span across sites, with devices that can be part of multiple groups.

The sites list is located under the Accounts menu and can also be accessed for a specific customer on the Sites tab of that customer.

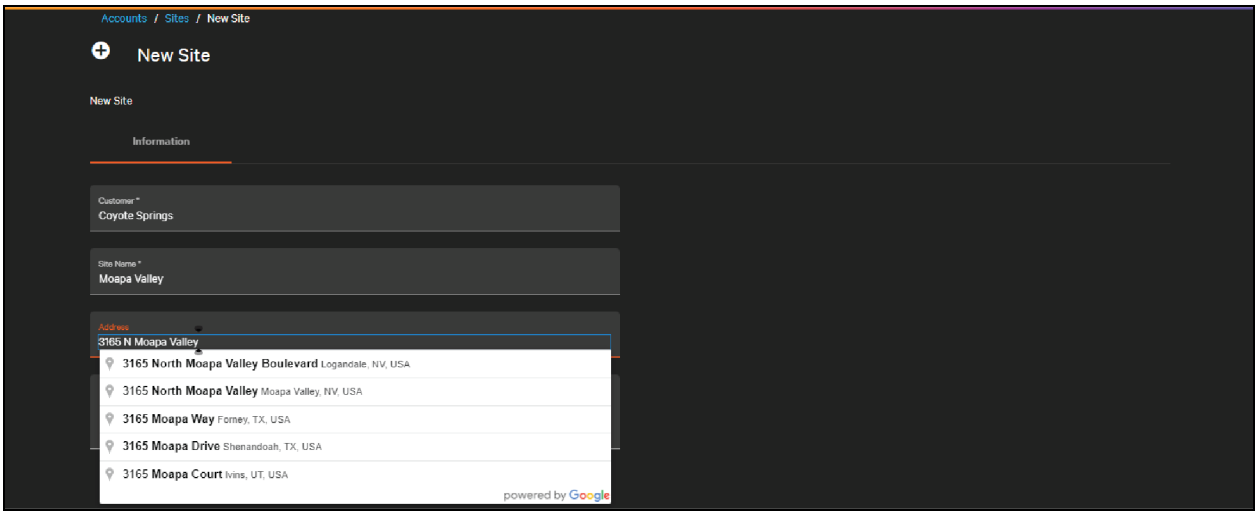
Figure 7.32 Sites List



Add a new site by clicking the

Add icon

Figure 7.33 New Site with an Address

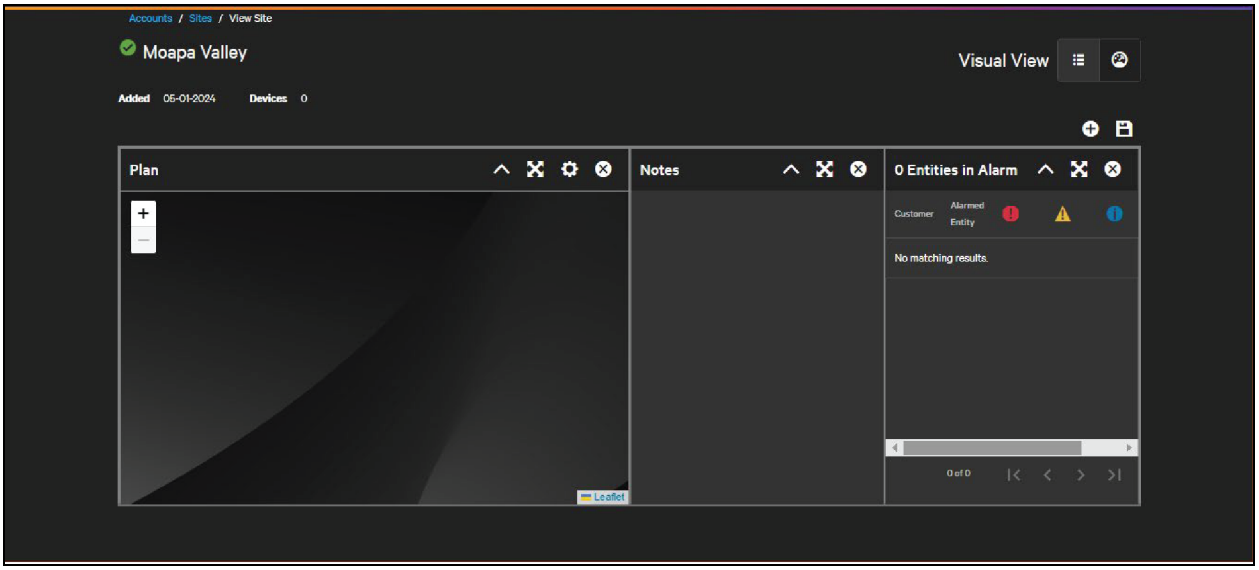


A site requires a name and the parent customer to be created. Sites are contained within a single customer. However, most sites will also have an address. Connect supports searching for addresses using the Google API, which recognizes both street addresses and place names.

When a new site has been added, it can be selected on an individual device level by clicking the sites field and selecting the site from the drop down. This will also populate an address for the device if the address for that site is specified.

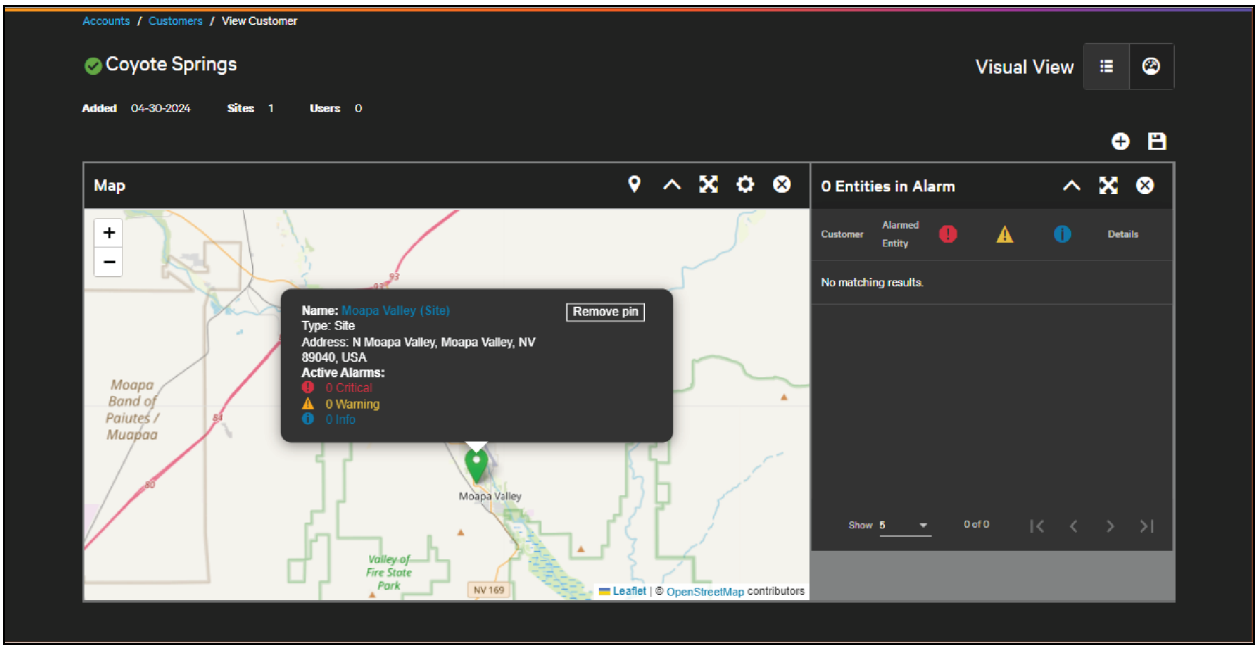
Sites are created with a default dashboard that can be customized to better match the site layout. See Basic Dashboard Editing on page 121.

Figure 7.34 Default Site Dashboard



If the site has an address, it is automatically added to the map widget for the customer and partner dashboards. Clicking on the pin shows information about the site, as well as the counts for any alarms that may be active for devices in the site.

Figure 7.35 New Site Pin on Customer Dashboard



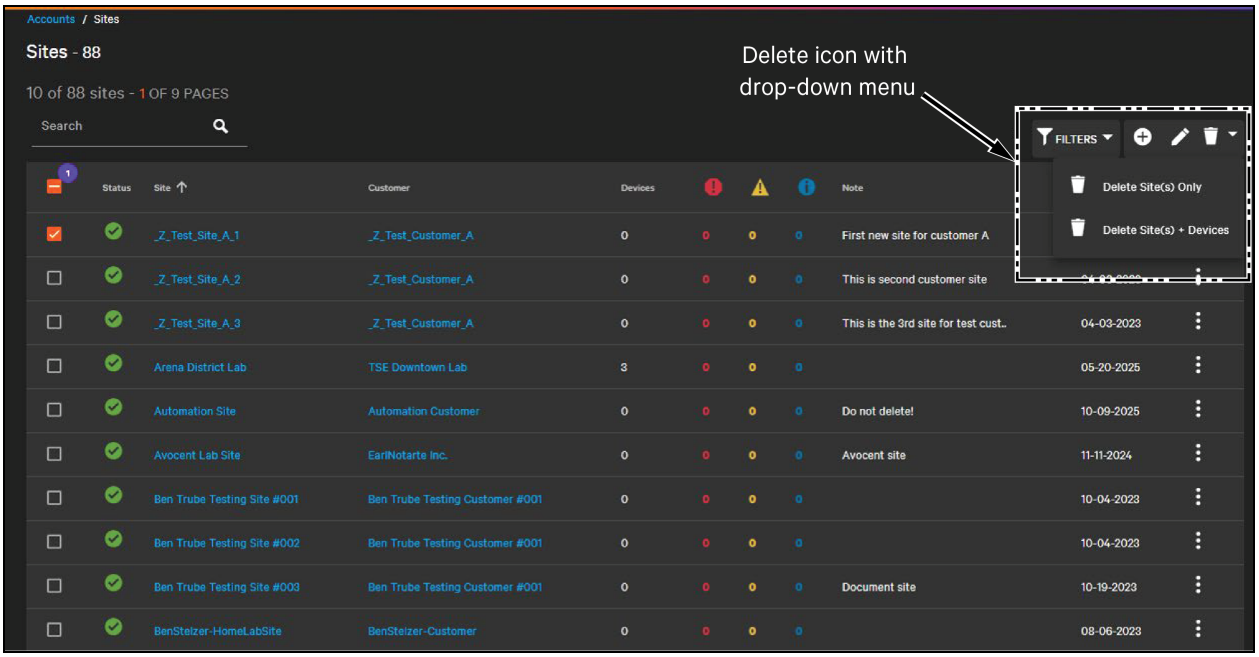
7.9.1 Deleting Sites

Sites have two delete options:

- Delete Site(s) Only
- Delete Site(s) + Devices

Access to the site and all devices is required in order to delete the site.

Figure 7.36 Deleting a Site



When choosing **Delete Site(s) Only**, only the sites selected are deleted. Devices within that site and related data—asset, historical, and alarm data—is retained.

When choosing **Delete Sites(s) + Devices**, the sites selected and any devices within that site are deleted. Related device data—asset, historical, and alarm data—is deleted.

To delete a site, you must have access to the site and to the devices within that group as well as the Device Management permission.

This page intentionally left blank

8 Dashboard Management

Dashboards are visual views that provide an at-a-glance view of the Connect product and can show a partner or customer a high-level perspective of what is going on with their devices.

Dashboards consist of widgets that have different capabilities. Widgets can be sized and moved, can be configured, and can be expanded to fill the whole view or minimized so that only the header is visible.

As Connect is developed to provide new capabilities, the set of available widgets will grow.

When a partner, customer, site, or group is created, they are created with a default dashboard that can be customized. For partners and customers, this dashboard serves as their home dashboard.

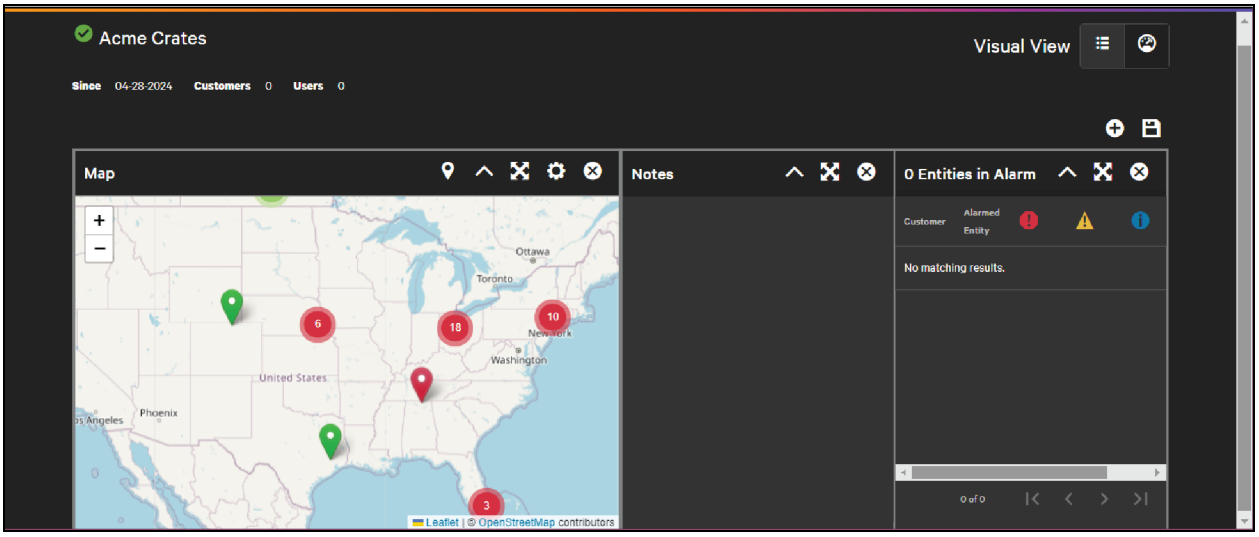
NOTE: Devices also have a dashboard that is part of the device template. Unlike the dashboards for partners, customers, sites, and groups, dashboards that are part of the device template cannot be customized.

8.1 Basic Dashboard Editing

To edit their organization's dashboard and the dashboards of any customers, sites, and groups, users must have Dashboard Management permission.

A dashboard can be modified from the single entity view (partner, customer, site, group). For example, as a partner to edit their home dashboard, the user goes to the partners list, clicks their partner, and toggles to the visual view.

Figure 8.1 Partner Dashboard

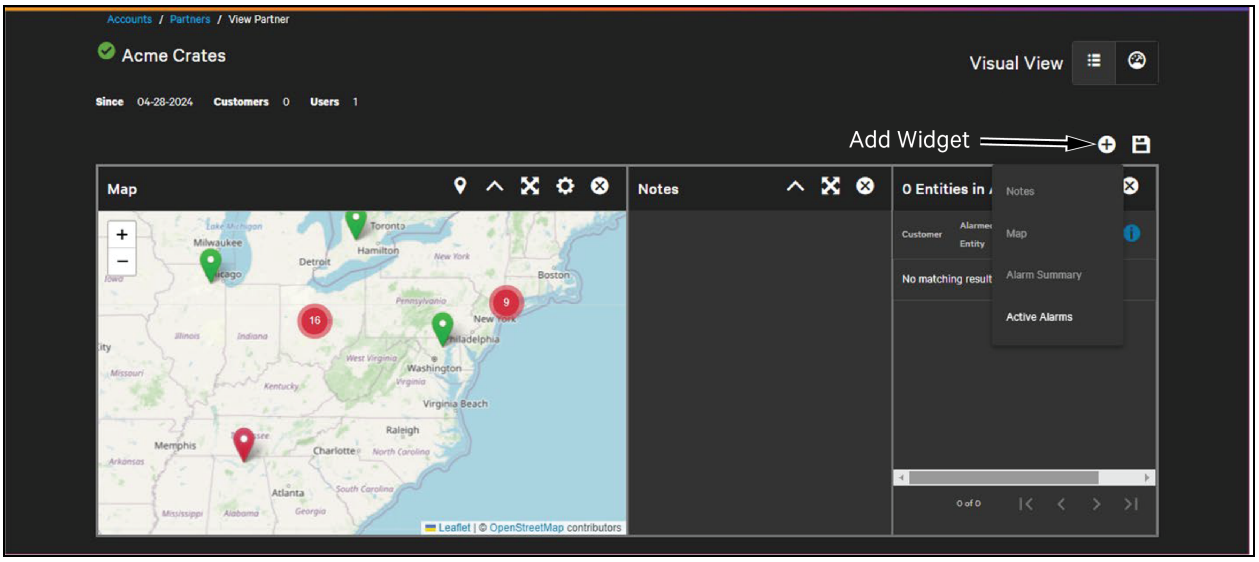


To add a widget, click the

Add icon

and select a widget from the drop down menu.

Figure 8.2 Adding a Widget



Some widgets can only be added once to a dashboard:

- Map
- Notes
- Alarm Summary
- Active Alarm

When one of these widgets has been added once to the dashboard, the option is grayed out.

Other widgets like the Plan widget can be added multiple times.

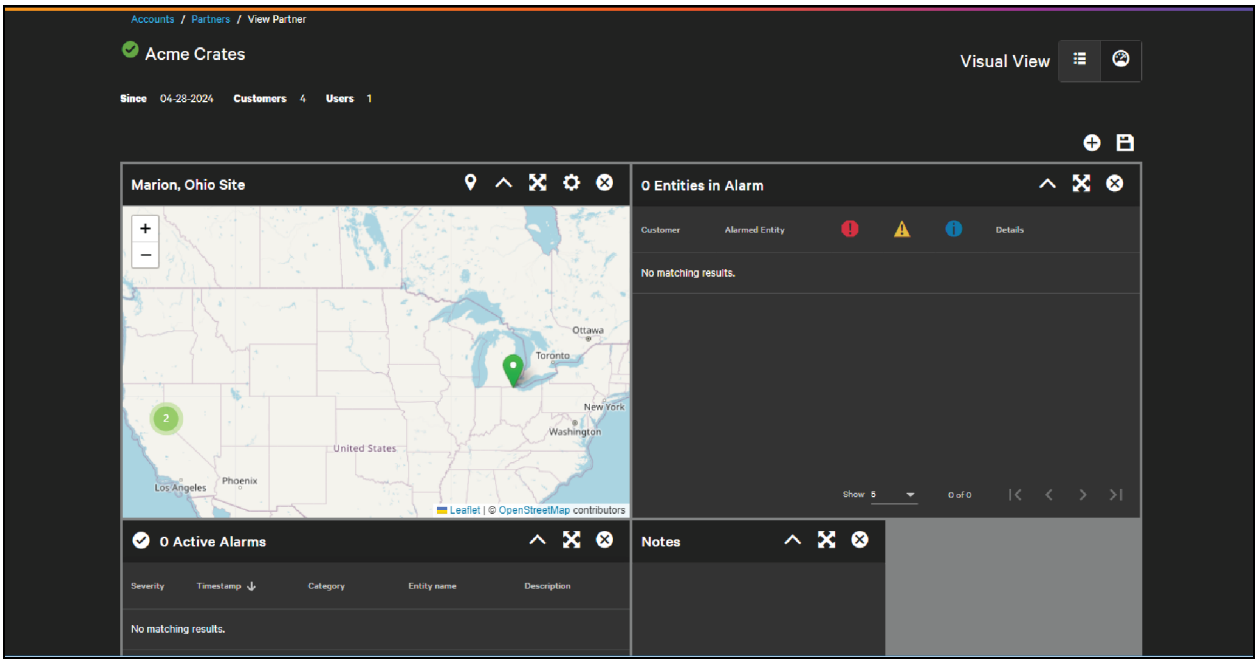
Delete a widget by clicking the

Delete icon

at the top right-corner of the widget. When the widget is removed, the remaining widgets may auto-arrange to fill the gap left by the widget that was removed.

Resize the widget by dragging the edge of the widget. This may also resize adjacent widgets. The dashboard fits a maximum of four widgets per row. A row is typically one widget tall although widgets can be arranged so that some widgets in the row are stacked.

Figure 8.3 Two Widgets Stacked in a Row



Widgets can be moved by clicking and dragging the widget by the header.

Some widgets can be configured by clicking the

Settings icon

in the top-right corner of the widget.

To save changes to the widgets or to the arrangement or configuration of the widgets, or any widgets that may have been added or removed click the

Save icon

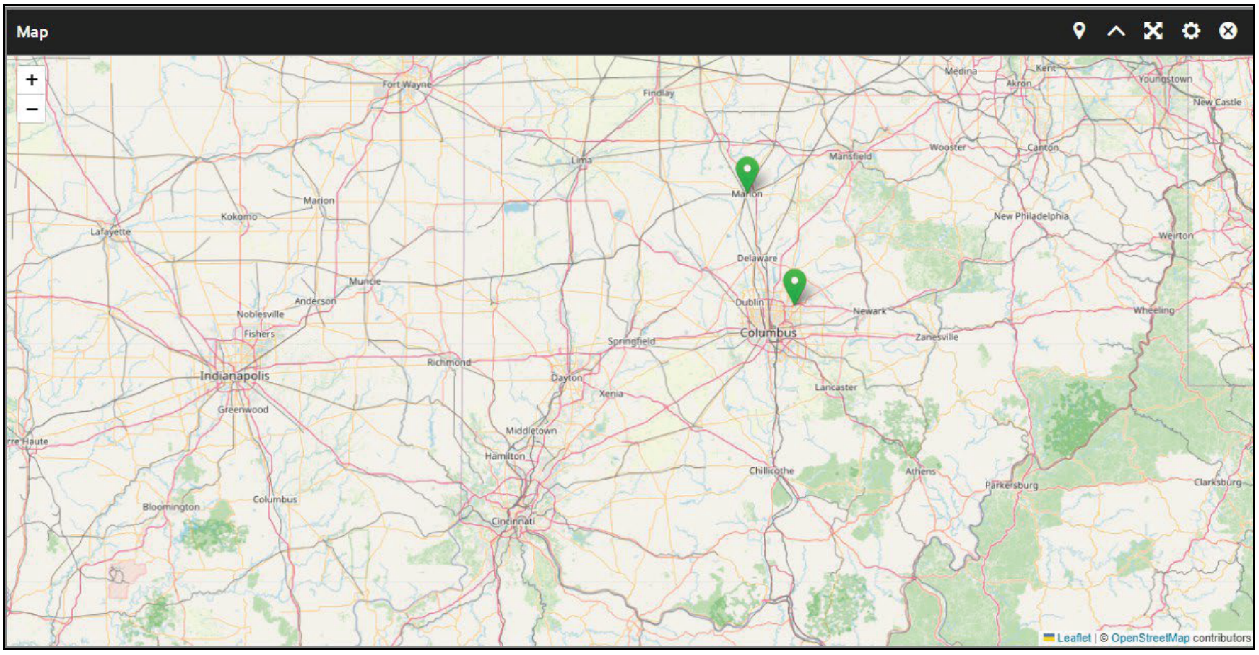
8.2 Widgets

8.2.1 Map Widget

IMPORTANT! The Map Widget is only available on the Partner and Customer dashboards. Groups and devices are not shown on the map widget.

The Map widget is a geographic view of the partners, customers, and sites to which the user has access. If the partner, customer, or site has an address saved, a pin will automatically appear on the map.

Figure 8.4 Map Widget

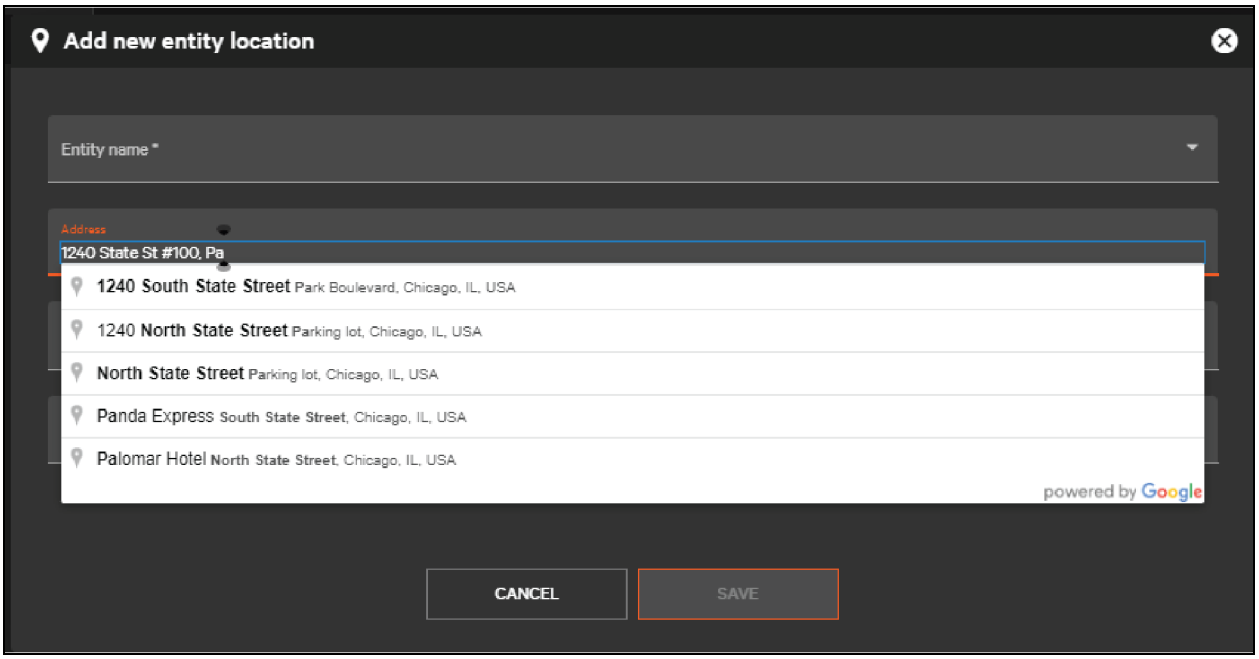


If an address has not been specified or if the partner, customer, or site has been removed from the map, add a pin for the entity by clicking the

Pin icon

A dialog pops up to choose the entity from a drop down menu and to specify an address.

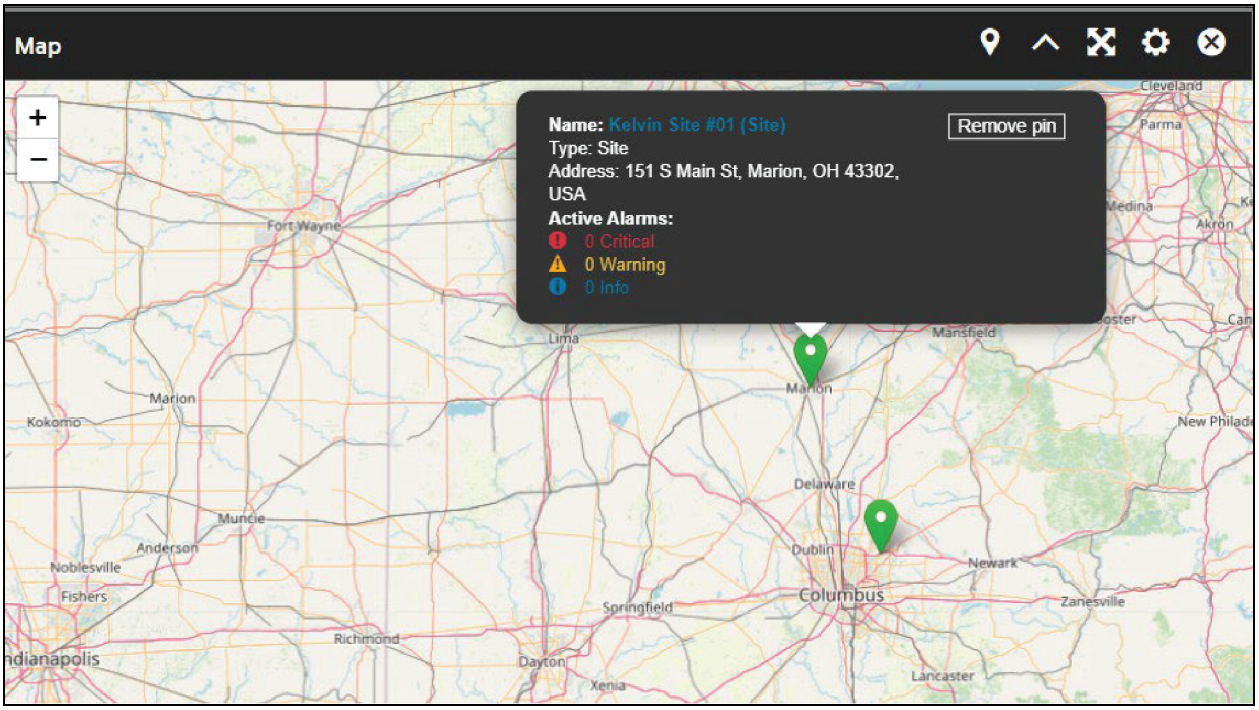
Figure 8.5 Address Search to Add Pin



If the location does not have a precise address, double click a location on the map and select an entity from the drop down. A pin will be placed where the map was clicked.

To remove a pin, click **Remove Pin**. This removes the pin only. It does not affect the entity.

Figure 8.6 Remove Pin

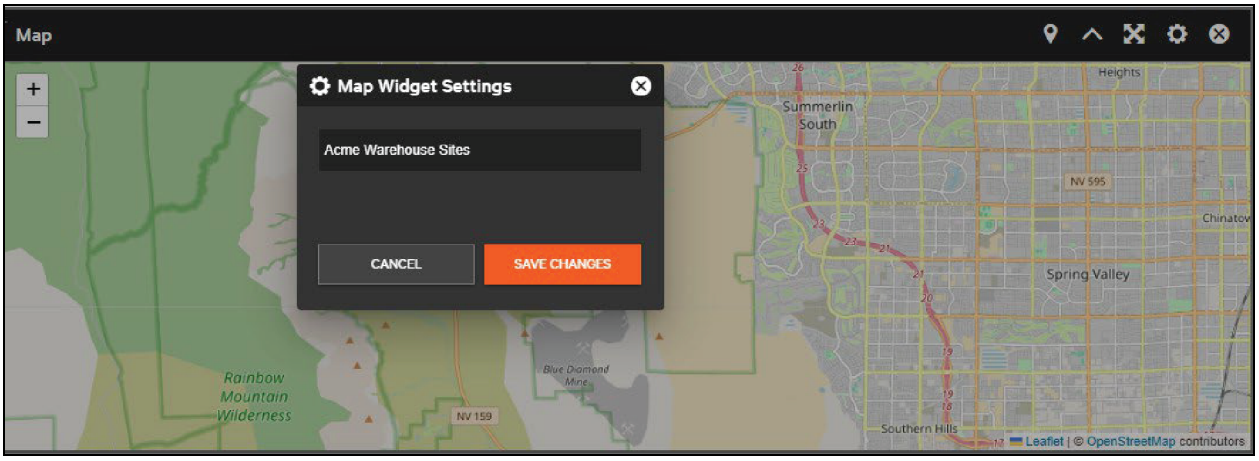


The map widget has a configurable title. To change the title, click the

Settings icon

at the top-right corner of the widget.

Figure 8.7 Map Widget Settings



Change the map title and click **Save Changes**.

8.2.2 Floorplan Widget

The Floorplan widget shows the physical locations of devices or groups of devices. The widget permits .PNG and .JPEG images to be uploaded to the Connect platform. Pins can be placed on the floorplans, similarly to how pins can be placed on the Map widget.

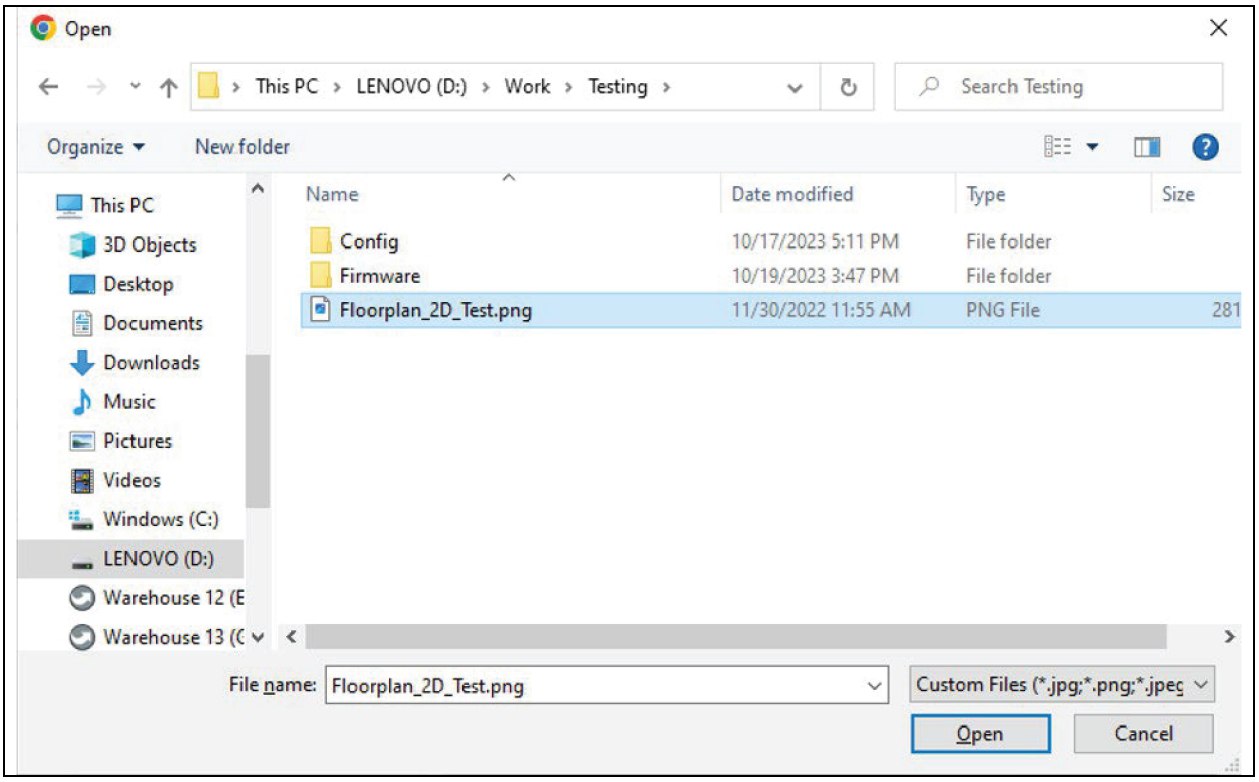
Floorplan widgets can be added only to site or group dashboards. Multiple floorplans can be added to the same site or group. Only groups or devices are available to add as pins to the dashboard.

To upload a floorplan image, click the

Settings icon

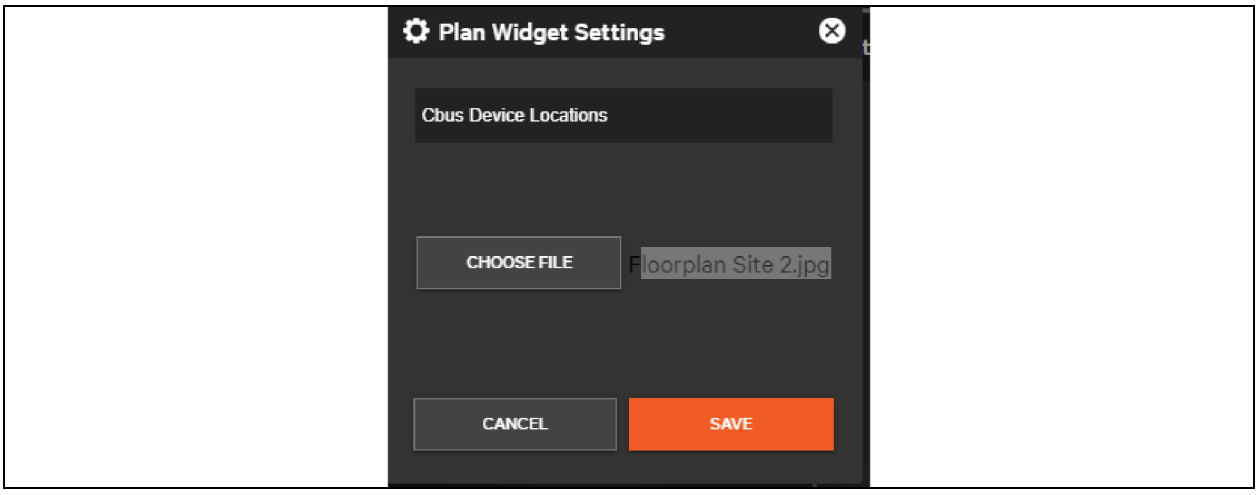
in the top right-hand corner of the widget. A dialog box opens to let you navigate to find the file on your hard drive. Select the image file and click **Open**.

Figure 8.8 Upload a Floormap Image



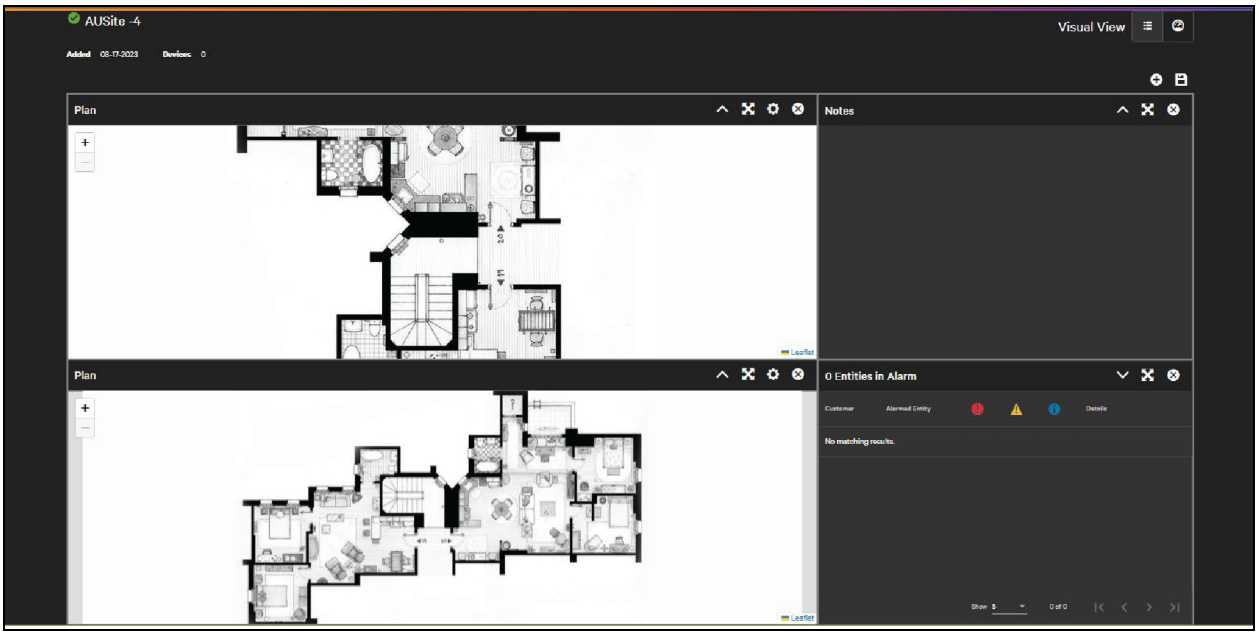
After choosing the file, the Plan Widget Settings dialog opens. You can change the title of the widget here as well. Click **Save** to upload the file to Connect and place it in the widget.

Figure 8.9 Plan Widget Settings



Like the Map widget, uploaded images can be zoomed in and out. Multiple floorplan widgets can be added to the same dashboard.

Figure 8.10 Site with Multiple Plan Widgets



To place devices or groups on the plan widget, double-click the location of the device or group you wish to add. A dialog opens to select the device or group to be added. Groups and devices are categorized within the drop down. After the entity has been added, click **Save** to add the pin to the floorplan.

Pins can be picked up and dragged after they have been added.

- If the floorplan is in a site, only devices that are in that site or groups within the customer can be added.
- If the floorplan is in a group, devices contained within the group or other groups within the customer can be added.

Pins cannot be added multiple times to the same floorplan, but they can be added to multiple floorplans.

Figure 8.11 Floorplan Widget with Pins Added

8.2.3 Other Widgets

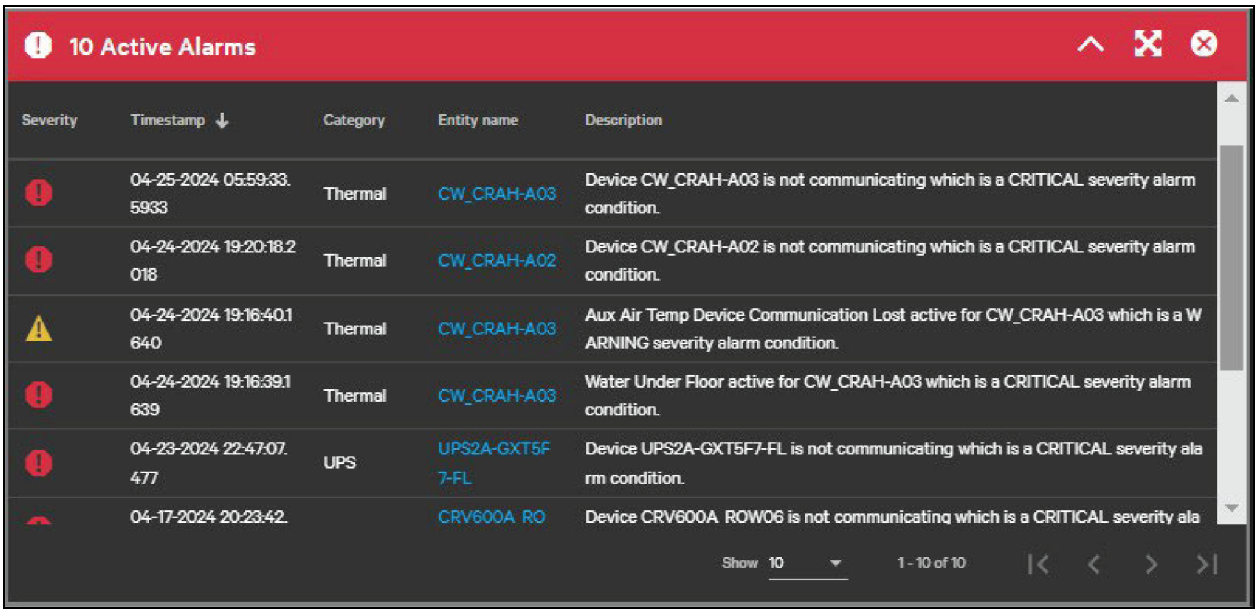
Active Alarm Widget

The Active Alarm widget shows a list of active alarms for the devices at the current level and below.

- At the partner level, the Active Alarm widget shows alarms for devices for all customers managed.
- At the customer level, the Active Alarm widget shows alarms for all their devices.
- For sites, the Active Alarm widget shows alarms for devices in the site.
- For groups, the Active Alarm shows alarms for devices within the group.

Each active alarm is shown as an individual row.

Figure 8.12 Active Alarm Widget



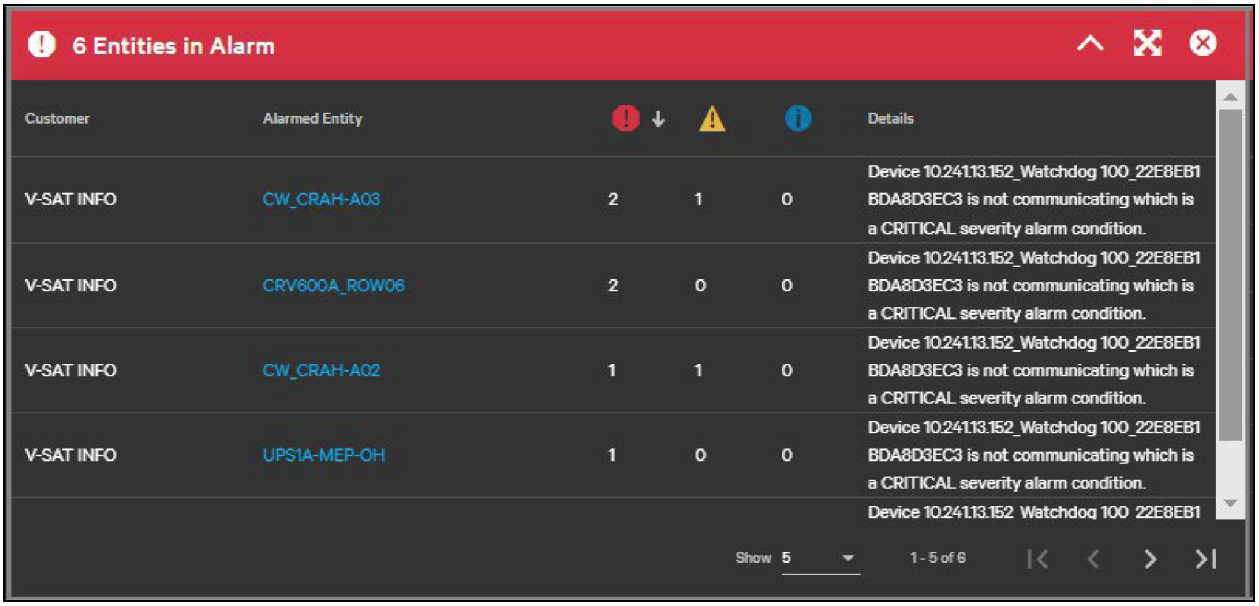
Only one active alarm widget can be added to a partner, customer, site, or group dashboard. This widget requires no configuration.

The widget shows only alarms that are currently active. If the alarm clears it will be removed from the widget. If no alarms are active the header will be neutral (gray), otherwise it reflects the severity of the highest active alarm.

Alarm Summary Widget

The Alarm Summary widget is a summary of devices with active alarms. It displays counts of alarms on each device. Each device with an alarm is an individual row in the widget.

Figure 8.13 Alarm Summary Widget



Only one alarm summary widget can be added to a partner, customer, site, or group dashboard. This widget requires no configuration.

The Alarm Summary widget shows only devices with active alarms. If all alarms are cleared for a device, they are removed from the widget. If no alarms are active the header will be neutral (gray), otherwise it reflects the severity of the highest active alarm.

This page intentionally left blank

9 Alarms

Alarms notify users of bad conditions in their units. The Connect platform highlights alarms in many ways throughout the product and via external notifications. The general goal is to highlight problem areas and drive the user to the details of the problem as quickly as possible.

9.1 How Alarms Work

Connect handles two types of data: polled data and asynchronous data. Polled data includes readings and events that are checked on the device at regular intervals. Asynchronous data includes traps (or informs) for SNMP, which are sent as soon as error conditions are present.

Many devices have alarms that are specified on the edge device itself. In these cases, it's the edge device that looks at readings and fires an event when conditions are not normal. Connect sees the event fired by the device and creates an alarm. How to set edge device alarms is covered in Use Case: Setting Agent as the Trap Target on page 158 and in Use Case: Setting Alarms on page 166.

In other cases, Connect looks at device readings and can create an alarm based on those readings. These alarm rules are specified in templates which are currently supplied by Vertiv. Finer grain control of alarms in Connect including creating different rules for different devices and/or customers building their own templates will be introduced with later versions of the platform.

NOTE: For Geist devices, users need to specify alarms on the edge device as none are specified in the templates.

Whether an alarm is device generated or Connect platform generated, it shows in the same places and trigger the same notifications. When conditions return to normal, Connect will close the alarm. Alarm history is logged and can be queried on log pages and widgets.

9.2 Alarm Counts

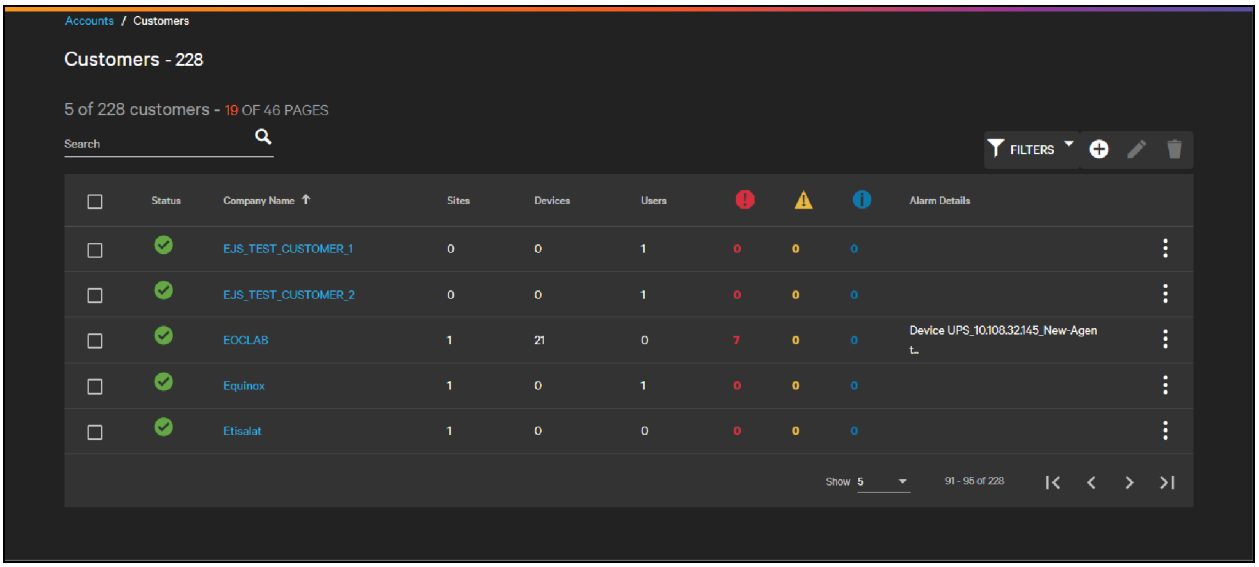
Alarm counts display current active alarms, categorized by severity. Alarms are displayed in the top header bar on lists and on pins within floorplans and maps.

Figure 9.1 Alarm Counts Top Header

The header bar alarm counts reflect current active alarms for the user's organization and for organizations managed by the user. For partners this is a roll-up of all their customers' alarms, and for an individual customer this is a roll-up of all alarms for all their devices. Clicking the alarm counts in the header bar takes the user to the active alarm tab of their parent organization.

Alarm counts are seen on most lists either as a tab of one entity or in the standalone list.

Figure 9.2 Alarm Counts on a List



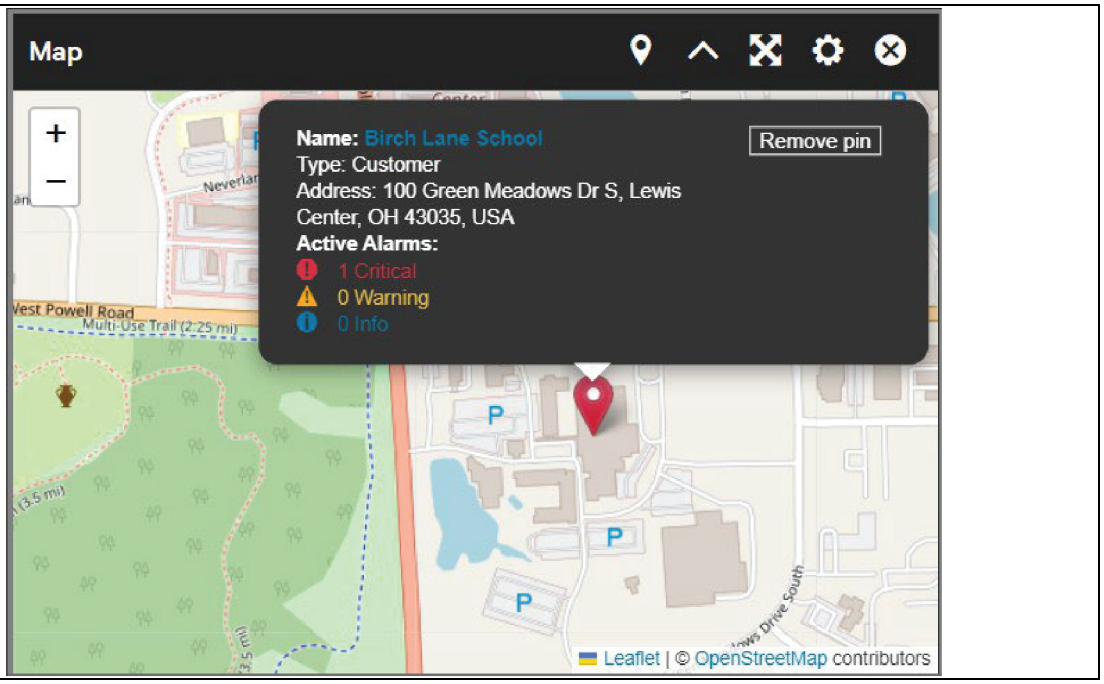
In a list alarm counts can be sorted and filtered by severity. The alarm detail column shows the description of the most recent highest severity alarm.

On a mobile display, the informational severity count column is hidden, but the details of the alarm can be seen in the active alarm log.

9.3 Alarms on Widgets

Alarming is a central feature of most widgets. At the partner or customer level, the map widget will show a pin for the sites managed by the partner or customer.

Figure 9.3 Map with Pin and Mouse Over



If there are no alarms present, the pin is green.

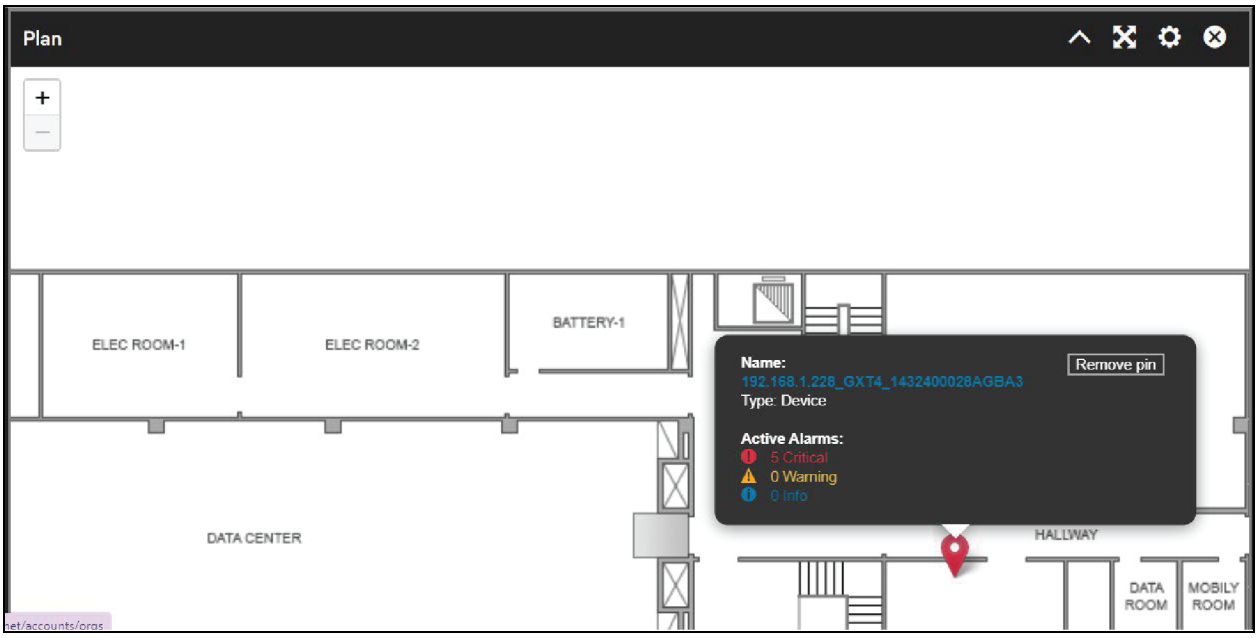
If alarms are active:

- The pin is red, indicating a critical alarm.
- The pin is orange, indicating a warning.
- The pin is blue, indicating informational.

Clicking a pin to show a count of active alarms and provides navigation to the object by clicking the name.

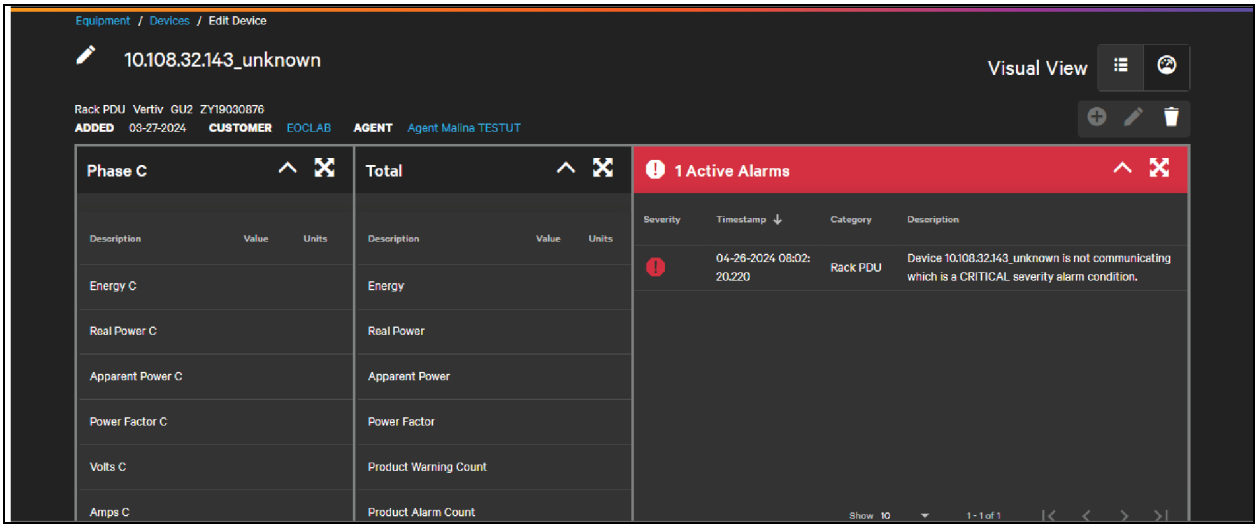
Floorplans on sites and groups works much the same.

Figure 9.4 Pin on a Floorplan



On a device dashboard, Connect uses header color and text color to highlight alarm conditions.

Figure 9.5 Device Dashboard with Active Alarms



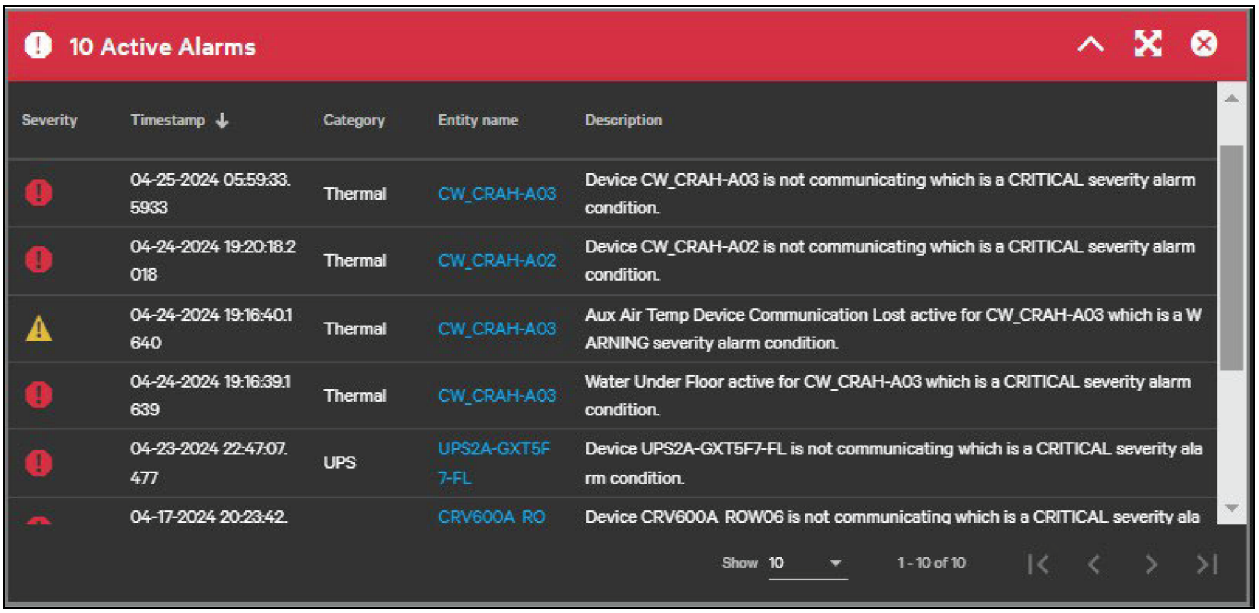
The header color on individual readings will be highlighted if there are active alarms. For group widgets the text color will change if an alarm is active for that reading.

There are two widgets specifically dedicated to alarms:

- Active Alarm widget
- Alarm Summary widget

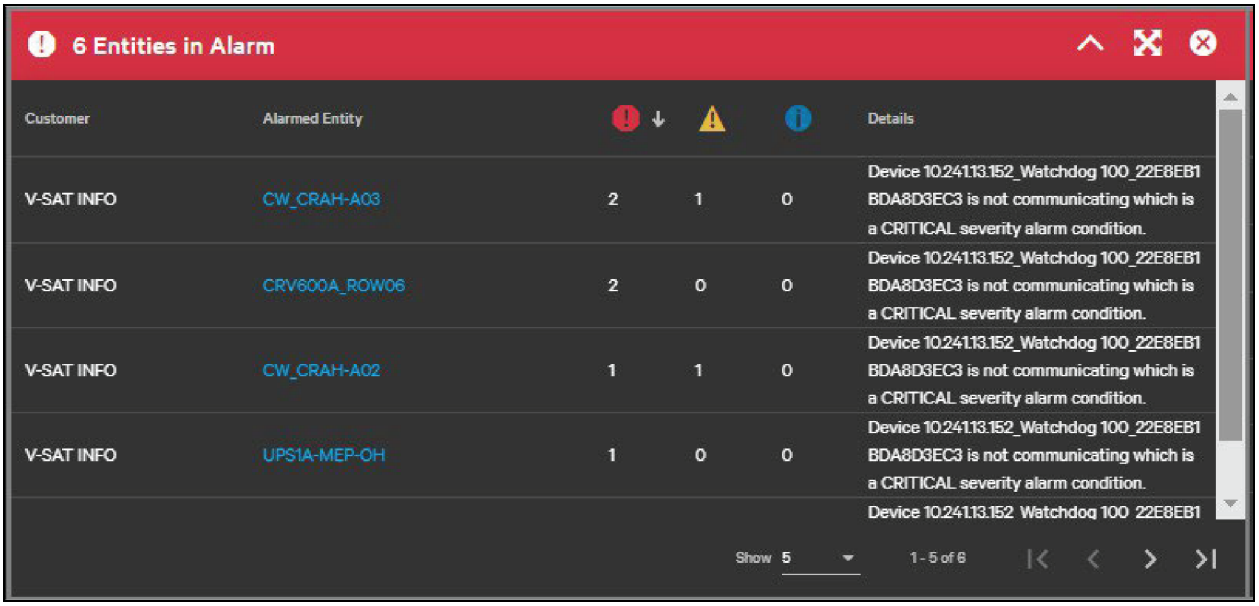
See Other Widgets on page 129.

Figure 9.6 Active Alarm Widget



The active alarm widget shows each active alarm in a separate row. On a device dashboard, an active alarm widget contains active alarms for that device only. If the widget is included on a site, group, customer, or partner, it shows all active alarms contained within that area and includes navigation to the affected device. The view is sorted to show the most recent alarm first by default.

Figure 9.7 Alarm Summary Widget



The alarm summary widget shows alarm counts for devices in alarm, with one row for each device. Both widgets include pagination and sorting controls and can be expanded to fill the whole screen.

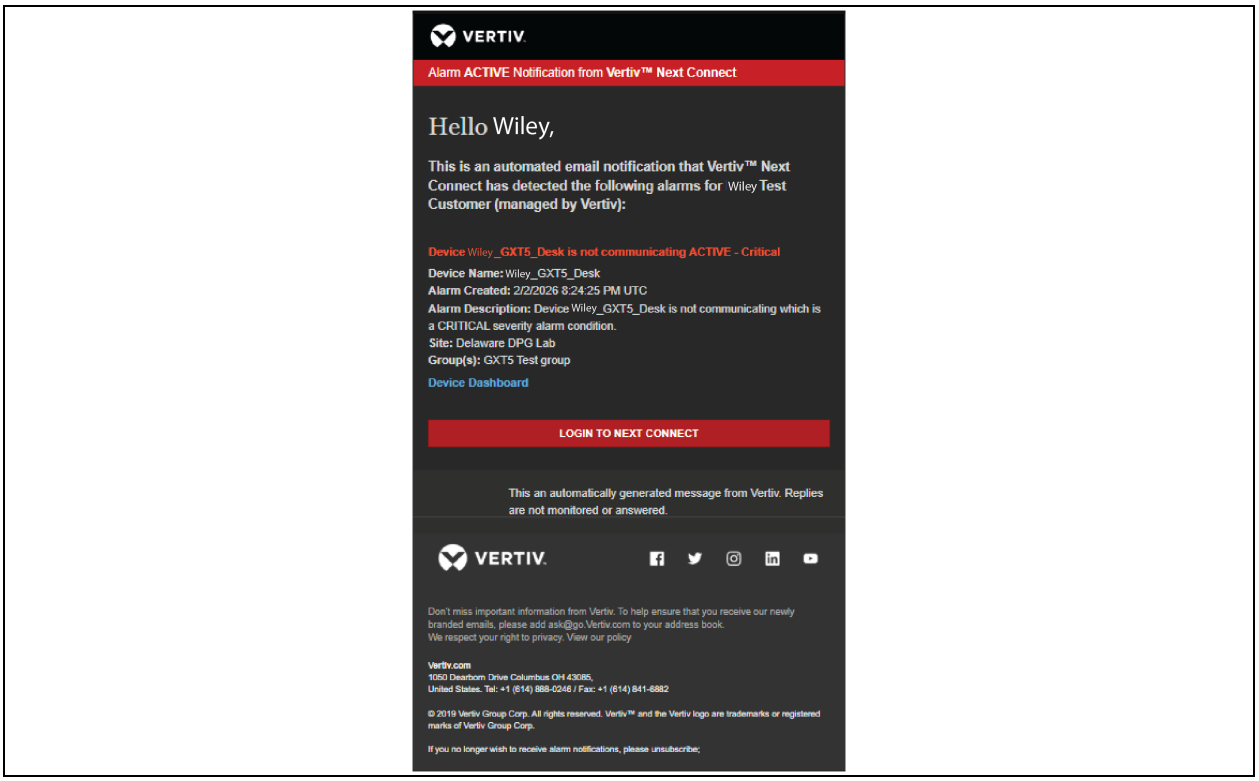
9.4 Alarm Notifications

Connect supports external notifications for alarms via email and SMS. User Notification Preferences on page 50.

NOTE: SMS requires an SMS phone number to be entered for the customer. Message and data rates may apply.

Emails from the Connect platform contain details for one or more active alarms on multiple devices.

Figure 9.8 Alarm Notification Message



There is usually a short delay (about 10 seconds) between the time that an alarm is shown on the platform and the time that a notification is sent to the user. This is to allow for the roll-up of multiple alarms that are received in a short period of time. In addition to the alarm details, each alarm entry will include a direct link to the alarming device's dashboard as well as a general prompt to log into Connect.

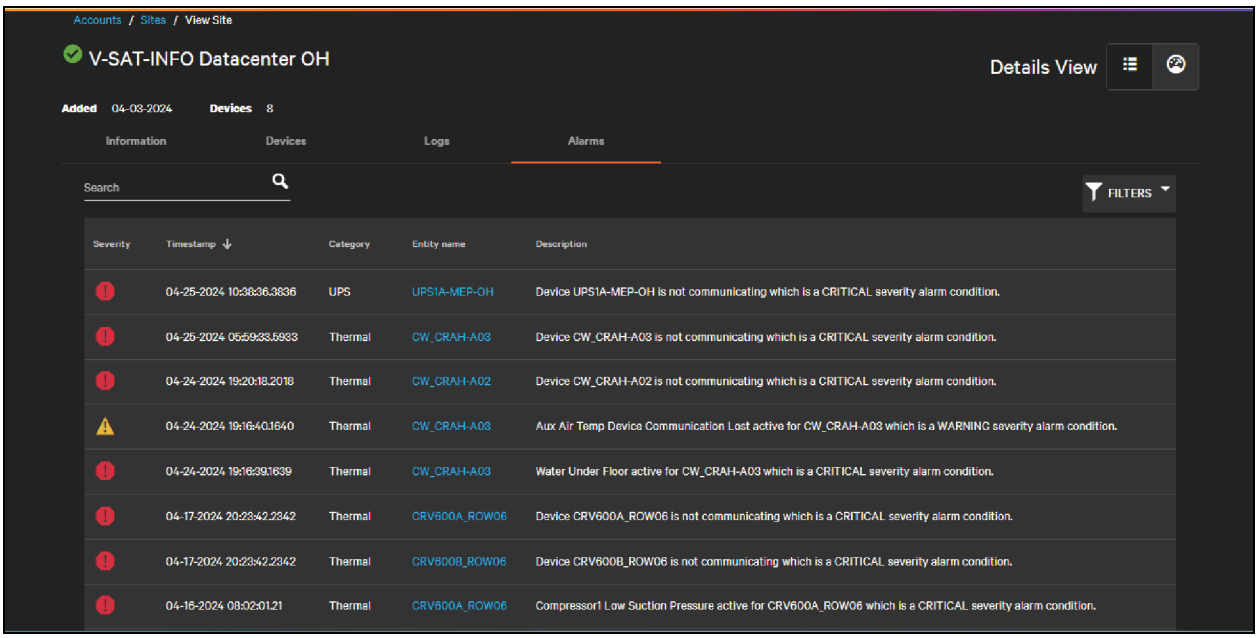
Text messages follow a similar format but contain only active counts without additional detail.

9.5 Alarm Logs

There are two main alarm logs:

- Active alarm table shows alarms that are currently active (when alarms are cleared this table is empty).
- Alarm/event log shows a time stamped historical view of alarms as well as events and audit actions in context with those alarms. It shows both alarm activation and the alarm clearing.

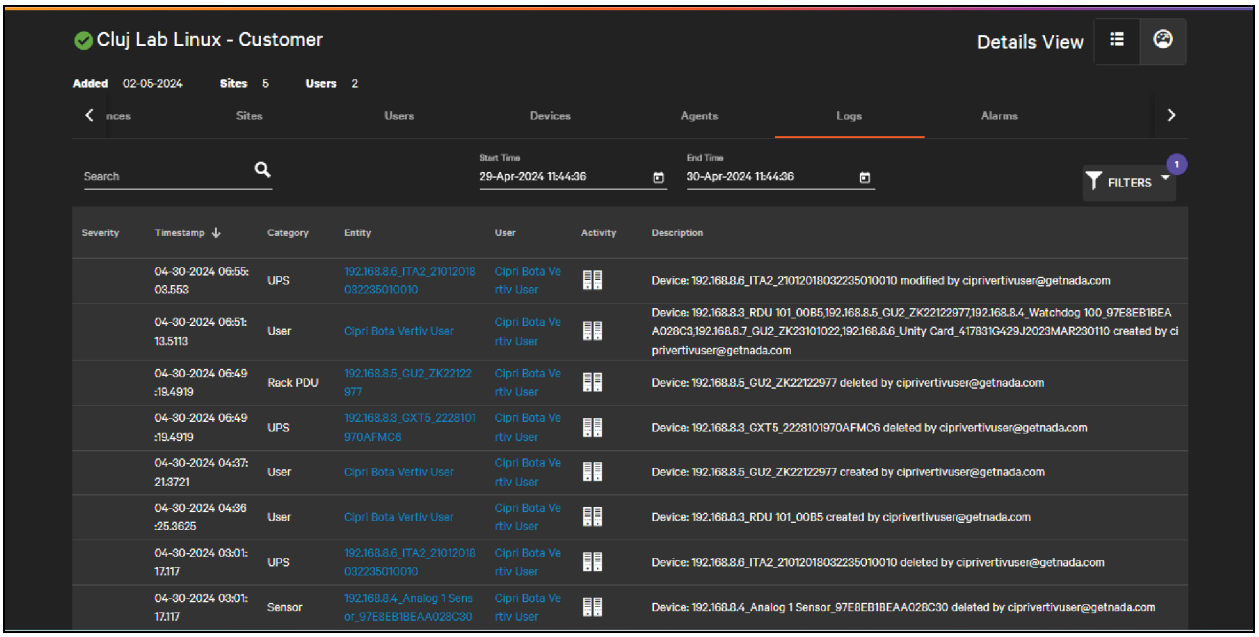
Figure 9.9 Active Alarms Tab



The Active Alarms list can be viewed on the Alarms tab of the Details view of most entities and unlike the active alarm widget, filters can be applied to the list of alarms and search within fields. The widget can only be sorted.

The Logs tab shows historical alarm data and events that triggered alarms.

Figure 9.10 Alarm Logs



This list can be queried by date as well as by standard filter and search options. If the audit log permission is active, this table will also show user actions on the device in context with other events.

Rows in this log can be filtered by type: alarm, audit, event.

NOTE: Showing event data may result in longer loading times, particularly at higher levels such as partner and customer.

You can refresh the log view to see any events, alarms, and so on. that may have occurred since the page was loaded, by clicking the

 **Refresh** Icon

in the top-right (next to the Export to CSV button). This will update the time range to one day ago through now.

The current log view (with filters and the time range applied) can also be exported to CSV.

To export the logs to CSV, click the

 **Export to CSV** Icon

in the top-right hand corner (next to the filters drop-down). This will create and download a CSV file of the form ***{device_name}_LogExport_{datetime}.csv***. This file can be viewed in Excel or other comparable software.

9.6 Manually Clearing Alarms

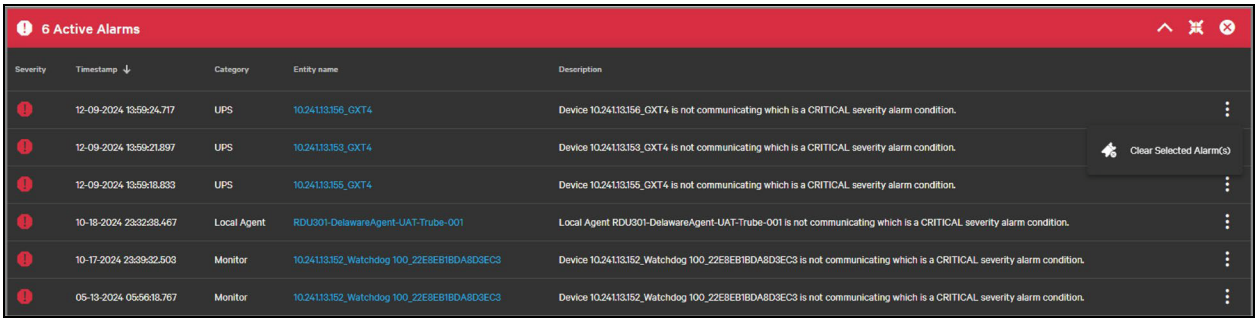
Most alarms will clear on their own when the conditions that created the alarm return to normal. However, sometimes the alarm conditions remain active even though the device is in normal working order. Users may also determine that the alarm condition no longer needs to be shown in Connect. For these and other similar situations, Connect offers the capability to manually clear alarms singly or in bulk.

On partner, customer, site, group, or device dashboards, you can clear individual alarms from the Active Alarm widget by clicking the vertical 3-dots menu next on the row of the alarm you want to clear, then clicking the

 **Clear Selected Alarm(s)** button.

NOTE: Clearing an alarm manually will create a clear event in the log and will send out "alarm cleared" notifications to subscribed users.

Figure 9.11 Clearing a Single Alarm on the Active Alarm Widget



IMPORTANT! Manually clearing an alarm does NOT change the conditions on the edge device. Threshold based alarms (like overload or high temperature) will become active again on their next polling cycle.

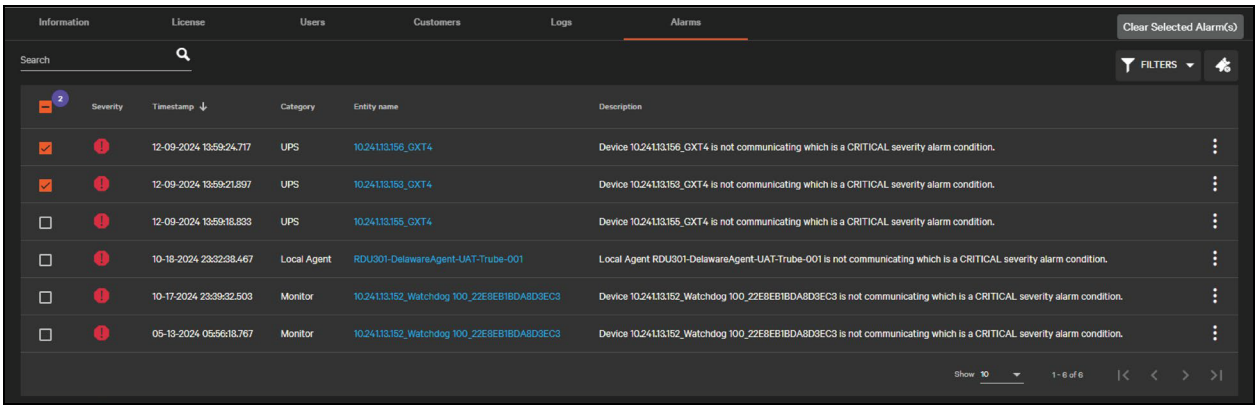
You can clear multiple alarms from the alarms tab on partners, customers, sites, groups, devices, or agents. Select one or more rows and click the

 **Clear Selected Alarm(s)** button

to clear the selected alarms. Each alarm will be cleared separately in the event log, though notifications should be batched.

NOTE: You can also clear alarms individually from the 3-dots menu on each row.

Figure 9.12 Clearing Multiple Alarms from the Alarm Log



10 Provisioning

Provisioning is a powerful capability of the Connect product that enables lifecycle management during device commissioning and operation. It is available exclusively for Vertiv-manufactured devices and includes two major areas: configuration and firmware update. The product specifically calls out basic configuration actions for initial setup such as creating an admin user, configuring the device's network, and enabling SNMP. Advanced configuration actions such as NTP settings, alarm thresholds, and device metadata are managed through configuration files.

10.1 Provisioning a Factory Fresh Device

Connect can take devices that have just been connected to the customer network and configure them from factory-fresh to fully monitored. The process can also be applied to already configured devices, though most Vertiv devices only allow the setting of an admin user once.

IMPORTANT! Configuring a factory fresh device requires that the local agent to be installed with Broadcast Scan enabled (Windows Agent only) and that the device and agent are in an environment that supports IPv6 multicast. See Installing the Local Agent on page 55.

10.1.1 Running a Broadcast Scan

The first step in configuring a factory-fresh device is a discovery scan.

Start a discovery scan from the device list by clicking the

 **Add** icon

and select **Scan for devices** from the drop down. The Discovery Scan dialog opens.

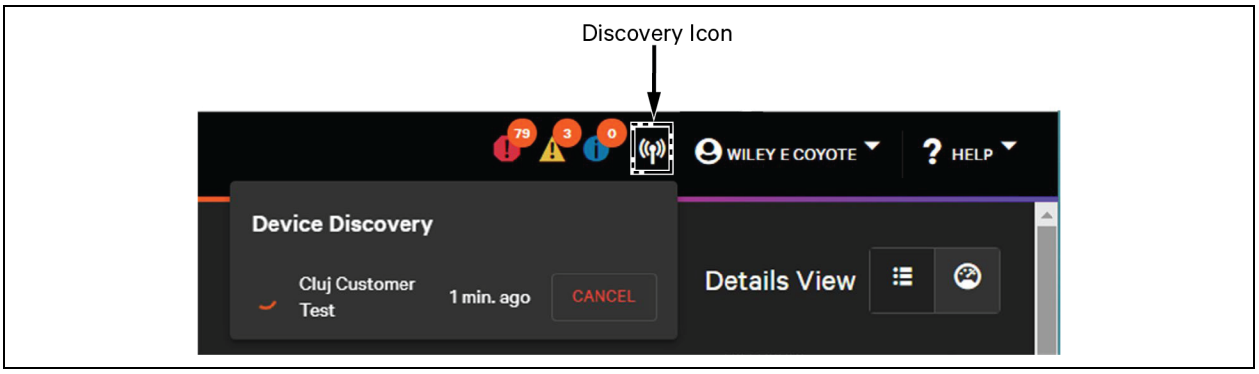
Devices in their default configuration use a default IPv4 address if DHCP is not enabled on the customer network. An IP range scan will not be able to uniquely distinguish new devices from each other. If IPv6 is implemented on the network, each device has a unique IPv6 address based on their MAC address in the network which can then be used to tell the devices apart.

After selecting the customer, agent, and specifying SNMP credentials, select Scan Type **Broadcast** and then click **Begin Scan to** run the discovery scan.

Broadcast scans can take 15 – 90 minutes to complete, depending on the number of devices in the customer network. While the scan operation is running, you can check the status of the running scan by clicking the

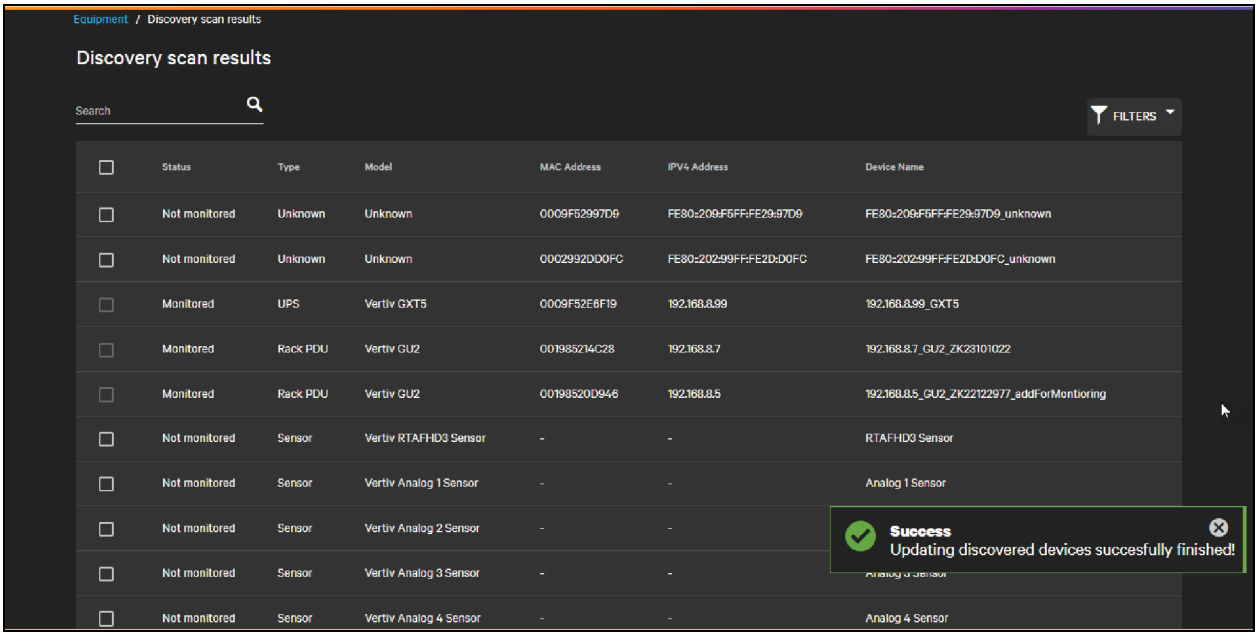
 **Discovery** scan icon in the top right header bar.

Figure 10.1 Running Broadcast Scan



When the scan is complete, a notification toast pops up in the bottom right. Click **View** to see the broadcast discovery results.

Figure 10.2 Broadcast Discovery Scan Results



When the results page load there are notification toasts update Connect's inventory of any devices found. This allows Connect to retain device information, even if a device is not added for monitoring.

For a device to be added for monitoring, it must have the following:

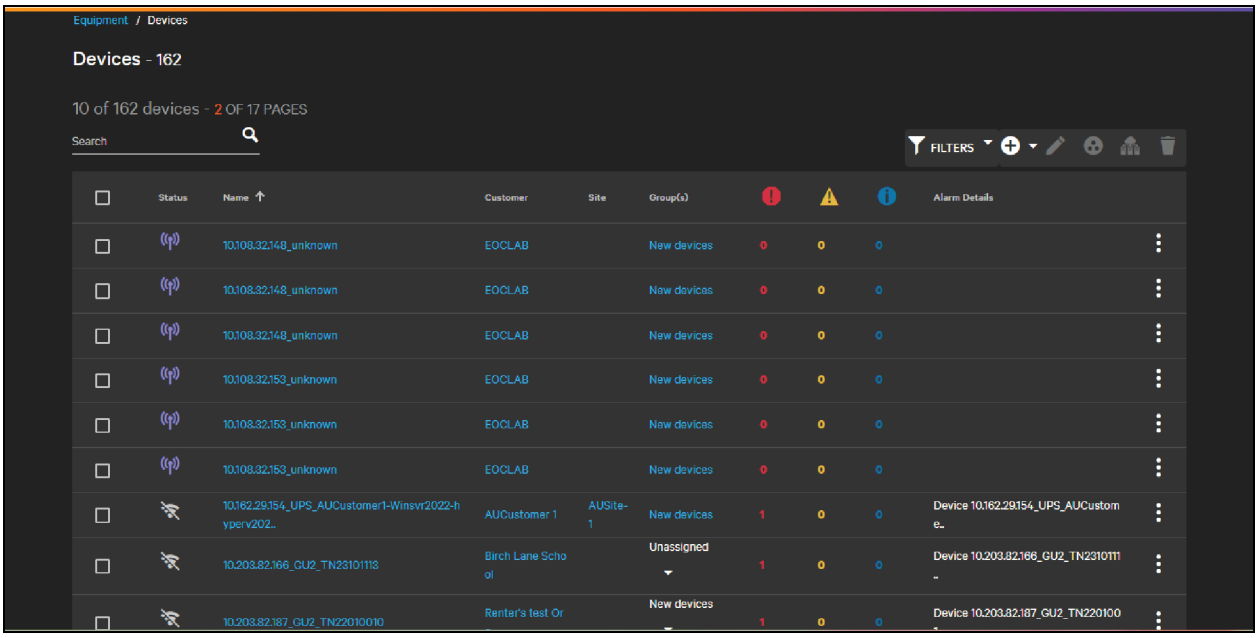
- An IPv4 address that is unique within the Customer's environment
- SNMP credentials
- An admin user, if using Connect to configure the IPv4 addresses and SNMP credentials

A factory-fresh device will not meet the above criteria, but the system can still retain information about the device as an unmonitored device, which allows the user to provision and configure the device for monitoring.

After the Discovery Scan page has loaded, press **Cancel** to return to the Assets screen. Assets that were found by the scan are added as unmonitored devices which are indicated with a purple

Discovery icon.

Figure 10.3 Unmonitored Devices in Device List



Interact with these device records and save details as you would with a monitored device. The main difference is that unmonitored devices will not collect data or create alarms, but they also do not count against the license for the partner or customer.

10.1.2 Creating an Admin User

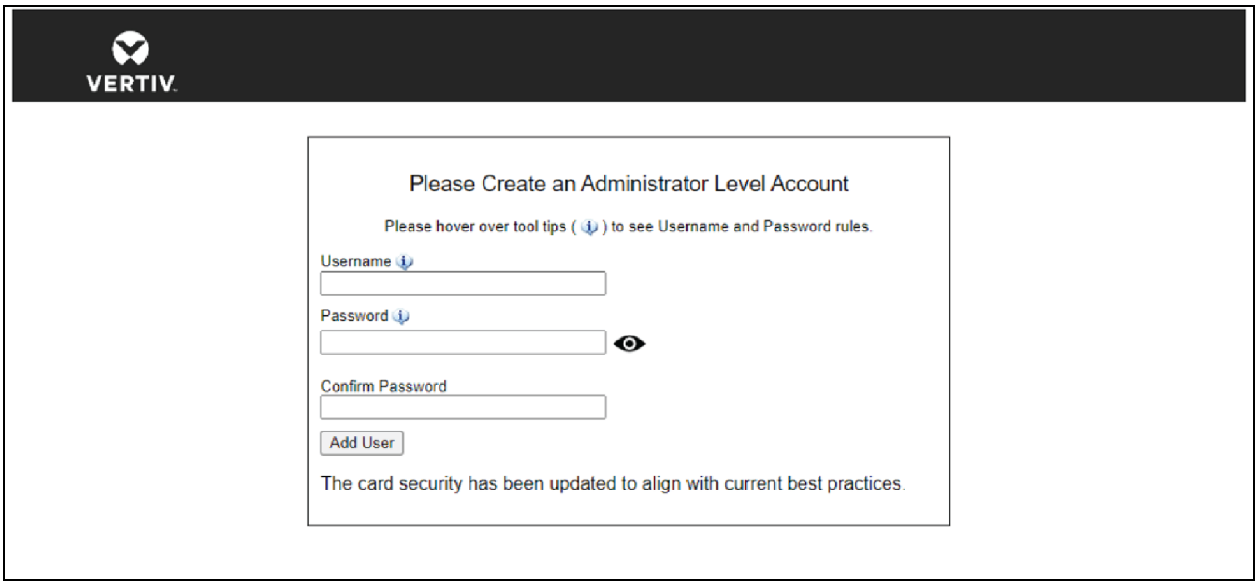
A factory fresh communication card or controller running the latest firmware requires a configured administrative user before you are able to log into the web page for that device. An admin user also authenticates significant configuration or firmware updates taken on that card.

NOTE: The admin user is not the same user that is used to login to Connect. The admin user is used to log into and authenticate with the edge device.

Connect provides the ability to configure the admin user from the cloud rather than setting up an admin user locally on each edge device. Connect retains administrative credentials to authenticate any other configuration actions. This permits Connect to be the central point of configuration for all customer equipment.

When logging into an Intellislot card (Unity, RDU101, and RDU120), the screen to create an admin user is shown in Figure 10.4 on the next page.

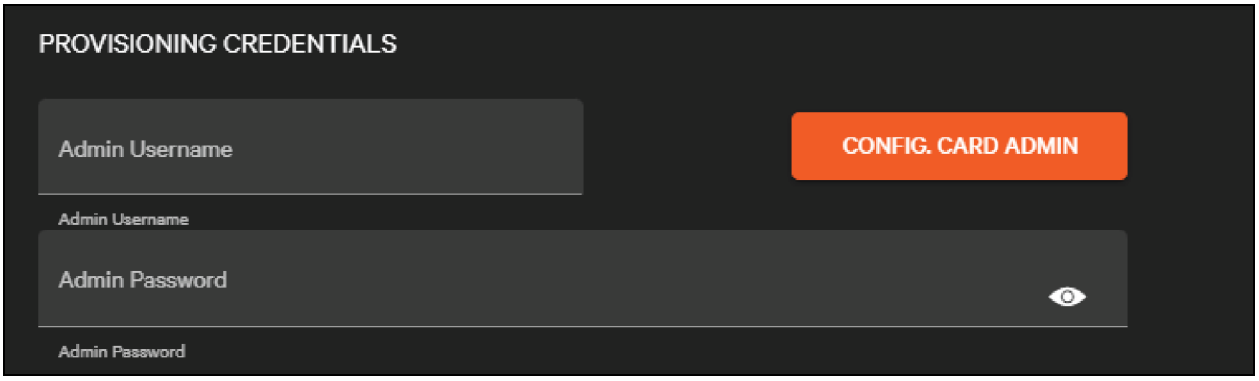
Figure 10.4 Creating an Administrator Account on a Unity Card



Instead of configuring this information locally, you can instead enter it in the Connect cloud on the Communications tab of single devices, or in bulk as we'll see in Update Firmware on page 169.

The information can be entered in the Connect cloud on the Communications tab of a single device or in bulk. See Bulk Actions on page 172 for further details.

Figure 10.5 Provisioning Credentials Section on a Communications Tab on a Device



To configure the edge device credentials, go to device edit mode by clicking the

Edit icon

on the Communication tab. Type in a user name and password and click **Config Card Admin**. When complete, a success toast will pop up in Connect and you are able to log into the device using those credentials.

IMPORTANT! Admin credentials can usually only be set once on the edge device. If admin credentials are already set on the edge device, Connect will display a failure toast notification indicating that credentials are already in place.

If an admin user already exists on the edge card, save your credentials to Connect so that you can authenticate any further actions. Enter a user name and password in the Provisioning Credentials and click the device **Save** button or icon.

Configuring or saving admin credentials is not required to monitor devices but is required for any of the provisioning actions in this section.

10.1.3 Setting Advanced Network

A factory fresh Intellislot card or Geist IMD controller ships with a default IP address and with DHCP enabled. If the device is in a DHCP friendly environment, it picks up an initial unique IPv4 address, though this may not be the address the customer intends to assign to the device long-term. If DHCP is not enabled on the network, the device is inaccessible via its default IPv4 address except by directly connecting to the device, but the local agent can access it via its IPv6 address.

Setting the advanced networking configures the static IPv4 address, subnet mask, gateway information and DNSs in the network on the edge device. This can be done with a factory fresh device, or with an existing device that is being moved.

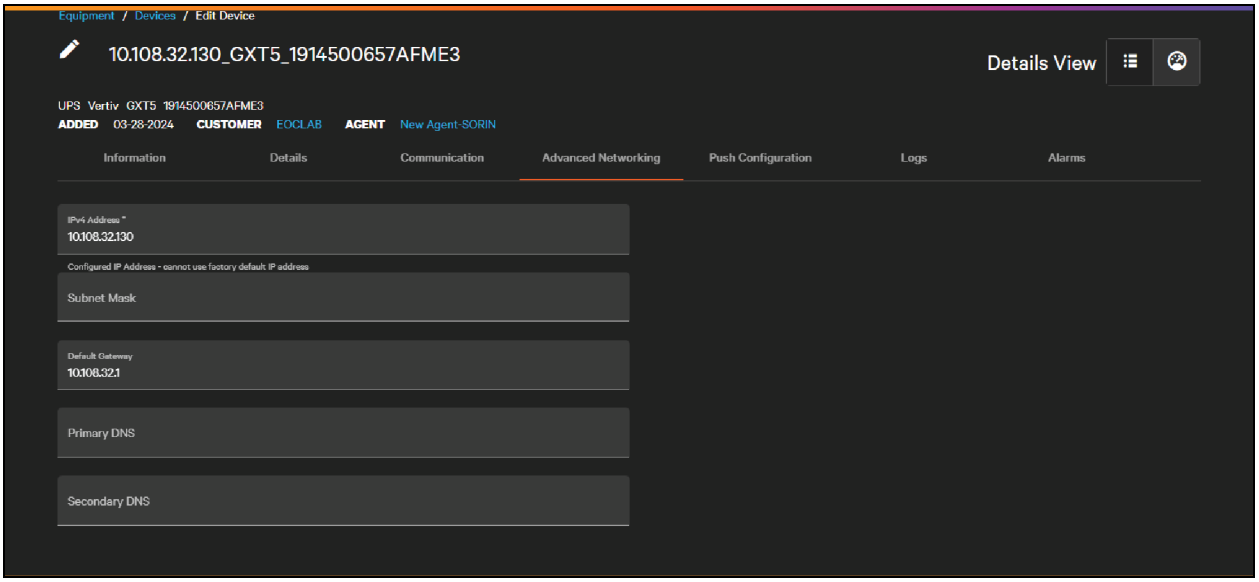
NOTE: You do not need to set the advanced networking on a device that has already been configured; discovery or adding manually prompts for the minimal information required to monitor the device.

To configure the Advanced Networking, enter the edit mode of the device by clicking the

Edit icon

on the Communication tab. Then click the **Advanced Networking** link.

Figure 10.6 Configuring Advanced Networking

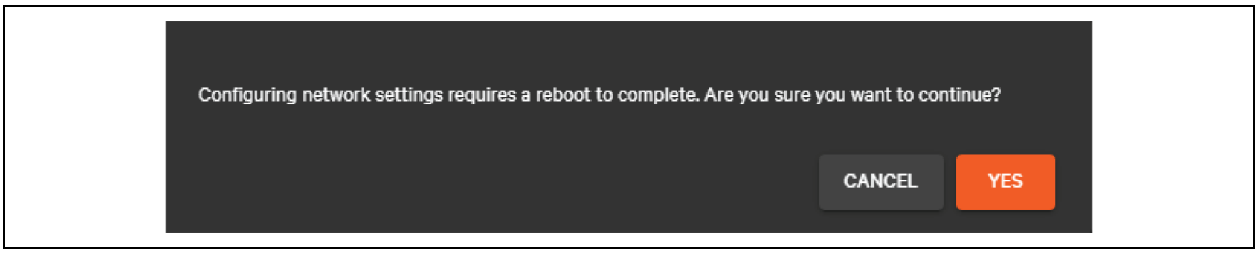


The IPv4 address entered on this page is synchronized to the fields on the Communication and Information tabs. The minimum required fields are the IPv4 Address, Subnet Mask and Default Gateway. It is also recommended to set at least one DNS.

NOTE: Cards may default to the Google DNSs: 8.8.8.8 or 8.8.4.4. However, these DNSs may not be accessible within a customer network.

To configure the networking on the edge device, click the **Config. Card Networking** button. This will pop up a prompt asking if you wish to continue.

Figure 10.7 Networking Reboot Prompt



Configuring network settings requires a reboot for the new settings to be put into effect.

Click **Yes** to apply the network settings to the edge device.

Click **Cancel** to leave existing networking settings in place.

A reboot takes from 3 to 5 minutes to complete and is triggered automatically by the provisioning action.

When the networking settings have been applied, a success toast pops up, notifying the reboot is in progress.

Figure 10.8 Success Toast

NOTE: Connect may briefly lose connectivity with the device during the reboot as the new IP address is put into place.

10.1.4 Enabling SNMP Polling

Connects initial release relies on SNMP polling and trap decoding to collect data from the edge device. Some communication cards do not ship with SNMP enabled by default, but this can be enabled or adjusted from Connect..

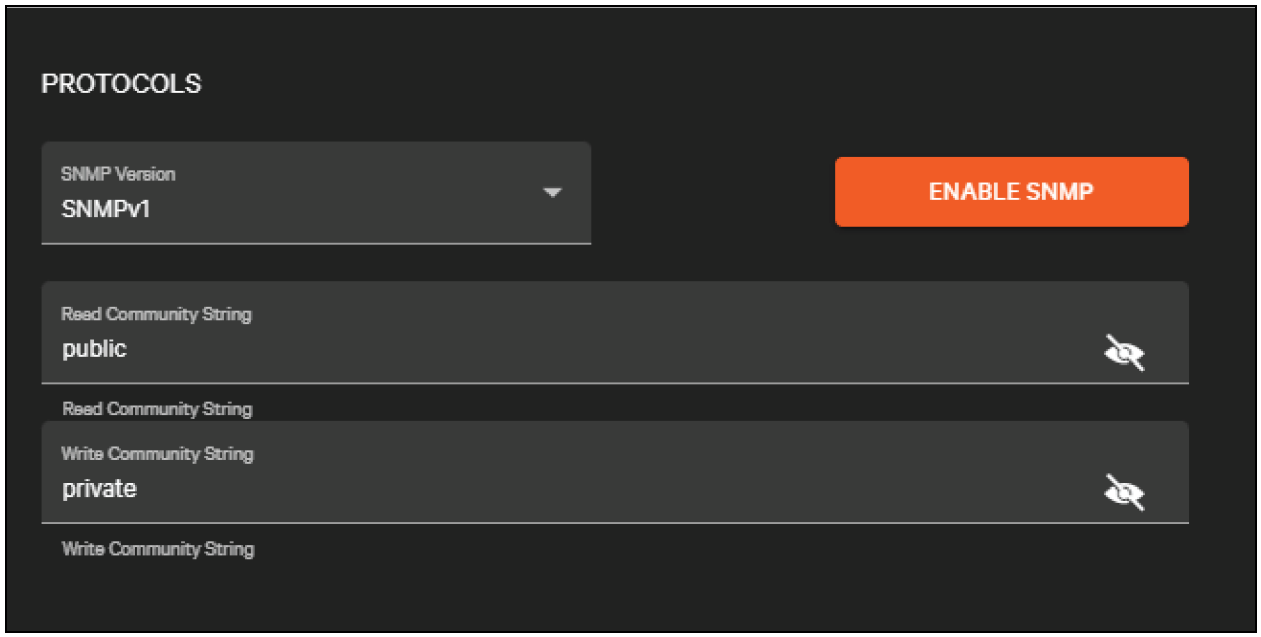
NOTE: There is no need to enable the SNMP credentials to monitor a device, just save the credentials that are already in place to Connect on the individual device. The action is mainly required for factory fresh device where SNMP is disabled, or if a user wishes to change the credentials used to poll devices.

To enable SNMP on the edge device, click the

Edit icon

on a device's communication tab. The SNMP credentials saved on the individual device are what will be sent to the edge device. In this case, the same form is used.

Figure 10.9 SNMP Protocol Section of the Communication



NOTE: Connect supports setting on v1, v2c, or v3 credentials. While v3 is supported on Vertiv communication cards, not all available encryption and privacy methods may be implemented. Check the communication card documentation for supported encryption.

Click the Enable SNMP button to set the SNMP credentials on the edge device. A warning pops up to ask to reboot the card. Rebooting the card is required for the new SNMP credentials to be applied.

- Click **Yes** to continue.
- Click **Cancel** to leave the SNMP settings as they are.

NOTE: Connect may briefly lose connectivity with the device during the reboot and as the new SNMP credentials are being put into place.

10.2 Advanced Configuration

Connect incorporates some device settings directly into its user interface. However, communication cards and edge devices can support an array of configurations. These configurations can be enhanced with new firmware versions. Connect supports generic ways of setting all other device settings on the communication cards and edge devices. The goal is to enable Connect to set communication cards and edge device settings via the device webpage or the device API.

Exact methods and formats can vary depending upon the type of equipment. The following subsections walk through some of the variations and indicate where samples can be found in the Connect product. In general the process is the same: upload a configuration file to the Connect platform that was modified locally and push the file to the edge device. A sample in the platform can be used or a configuration from an already configured device can be used and applied to devices in your site.

10.2.1 Configuration File Types

Configuration files come in three main variations, driven primarily by model and communication card.

Card Configuration File

Depending on the model of Communication card. The card configuration files follow two formats for the Unity and the RDU101 the files will be a text file download that acts as an .ini file and the file will be either

- Card Config – Unity
- Card Config – RDU101

depending upon the model of communication card. When you export the file from the card, it will have a .txt extension. This file includes documentation within the file on the format and possible values for each reading. These files apply only to Unity or RDU101 Comm. Card settings and will NOT affect settings on the edge device.

Configuration files for the RDU120 follow a JSON format similar to the Geist Configuration files discussed later in this section. Vertiv has provided sample files for the most common operations. These files follow the card supplied API and additional documentation is available from Vertiv in the https://www.vertiv.com/493ad4/globalassets/shared/av-50017_reva_10-25_weblocked_liebert-intellislot-rdu120-api-specifications.pdf. These files will be upload to the Connect Platform as

- Card Config – RDU120

Device Configuration - Generic Via SNMP writes

When uploading or selecting files this is a Device Config – Generic via SNMP writes configuration type. These files apply only to devices communicating through SNMP that support SNMP write capability. Vertiv supplies sample files that include all the points that can be configured on the Vertiv models. Values are set using SNMP writes from the local agent, so valid SNMP credentials are required to change device configuration values.

The format is CSV with the following columns:

- Label
- OID
- Data Type
- Value
- Description

When modifying files provided by Vertiv, only the value column needs to be modified. The data type column offers a guide to the sorts of values that are valid but you may need to review the device manual for a full list of valid ranges.

Gauge and Integer are numbers. The device may scale the value automatically. For example: CRV High Supply Air Temperature Threshold is divided by 10. OctetString is text.

Device Configuration Geist (Host/Device/Alarm)

In the Connect platform this will be one of the following

- Device Config – Geist Device Configuration
- Device Config – Geist Host Configuration
- Device Config – Geist Alarm Configuration

Configuration files for Geist devices are in JSON format. They are split by functional area, with communication values in host files, device specific settings/labels in device files, and alarm configurations in alarm files. These correspond to JSON files that can be retrieved from the edge device. See Pulling Configuration Files from the Edge Device below.

The format of these JSON files is described in detail in the Geist Public API document.

Download the latest version from https://www.vertiv.com/49e32f/globalassets/products/critical-power/power-distribution/geist-api-specification-api-specifications-sl-70874.pdf

It is recommend to set one device manually using the device's webpage, extracting the JSON settings from the device, then making any minor adjustments needed to apply the file more broadly to other devices.

10.2.2 Pulling Configuration Files from the Edge Device

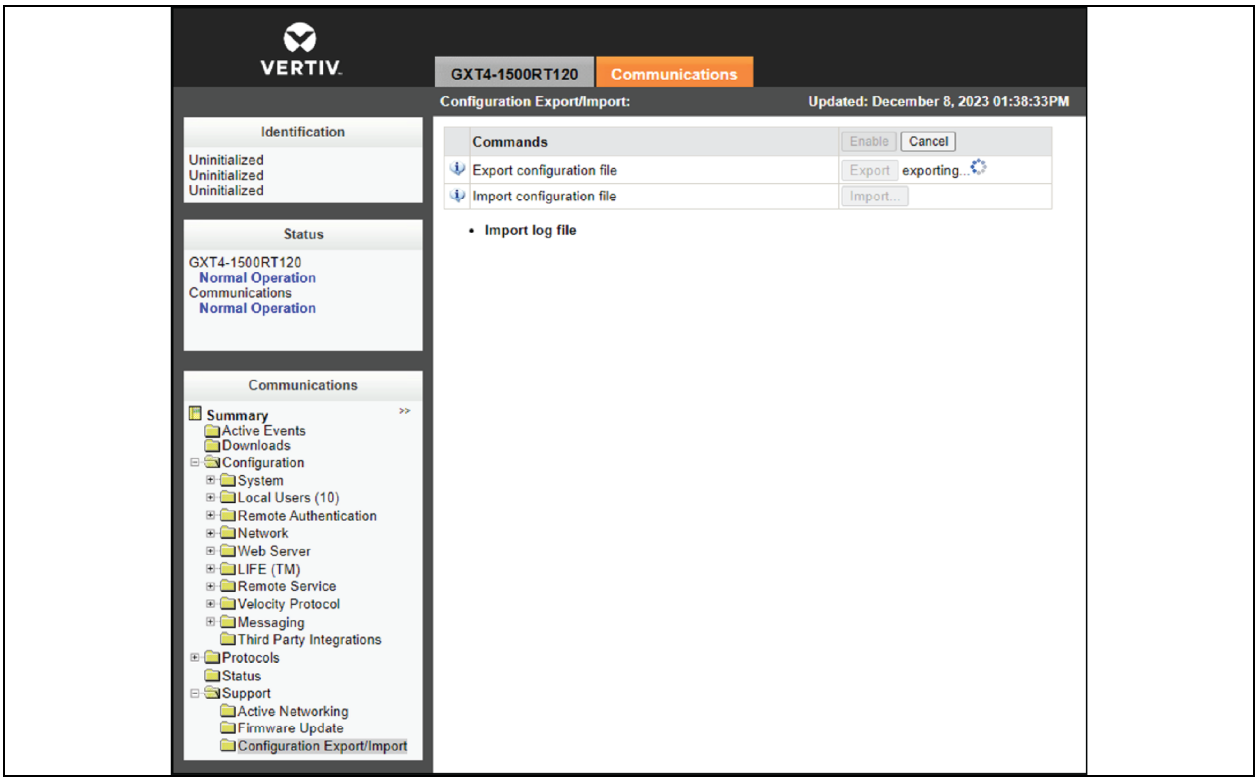
There are several methods used to pull configurations. These methods are based on the model and type of configuration.

Card Configuration File – Unity and RDU101

On the Communications tab of the card, navigate to the Support, Configuration Export/Import sub-menu. From there, enable the Export/Import commands. You may need to log in with the card's admin credentials to do this. Export the current running configuration from the card by clicking **Export**. A file will be downloaded in your browser.

The file for Unity and RDU101 cards will be an INI file you can directly edit. From the card webpage, the RDU120 exports a backup file that is not intended for direct editing. But you can export a .json of the configuration using the method outlined in Card Configuration – RDU120. The configuration of RDU120 settings is very similar to Geist JSON files, and examples are available in the configuration files published by Vertiv.

Figure 10.10 Configuration Export on Intellislot Card



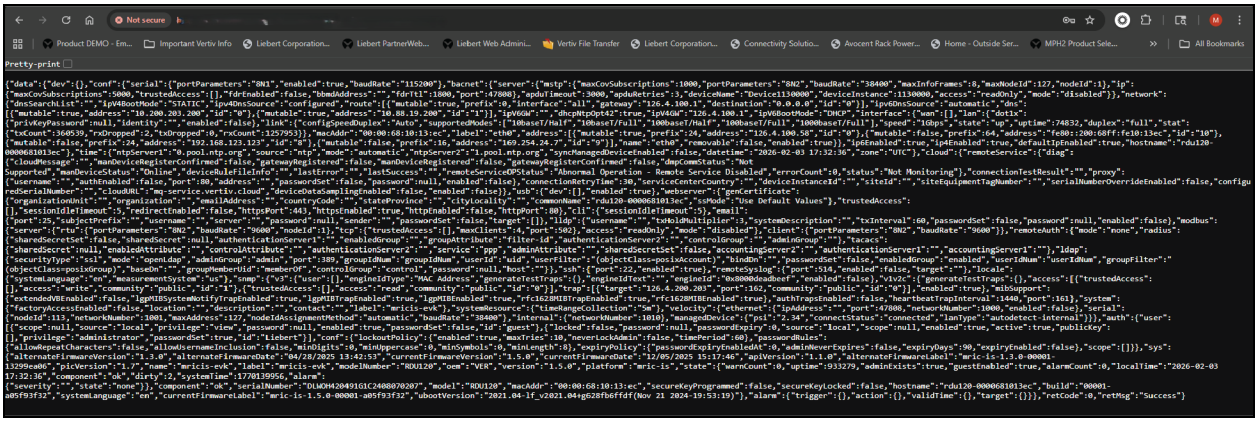
Card Configuration – RDU120

The method for the RDU120 is similar and can be done from the browser. Navigate to the web page of the edge device or you can paste its IPv4 address into a browser if you are on the same network.

To see the full configuration of the RDU120, From the webpage add the following URL you will need to include your username and password in the appropriate fields

<IPAddress>/api?username=<username>&password=<password>

Figure 10.11 RDU120 Configuration



Geist Device Configuration (Host/Device/Alarm)

The method for all Geist configurations is similar and can be done from the browser. Navigate to the web page of the edge device or you can paste its IPv4 address into a browser if you are on the same network.

Host Configuration

From the web page, add this URL to retrieve the configuration file:

Host configuration: <<ipAddress>>\api\conf

Figure 10.12 Example Host Configuration

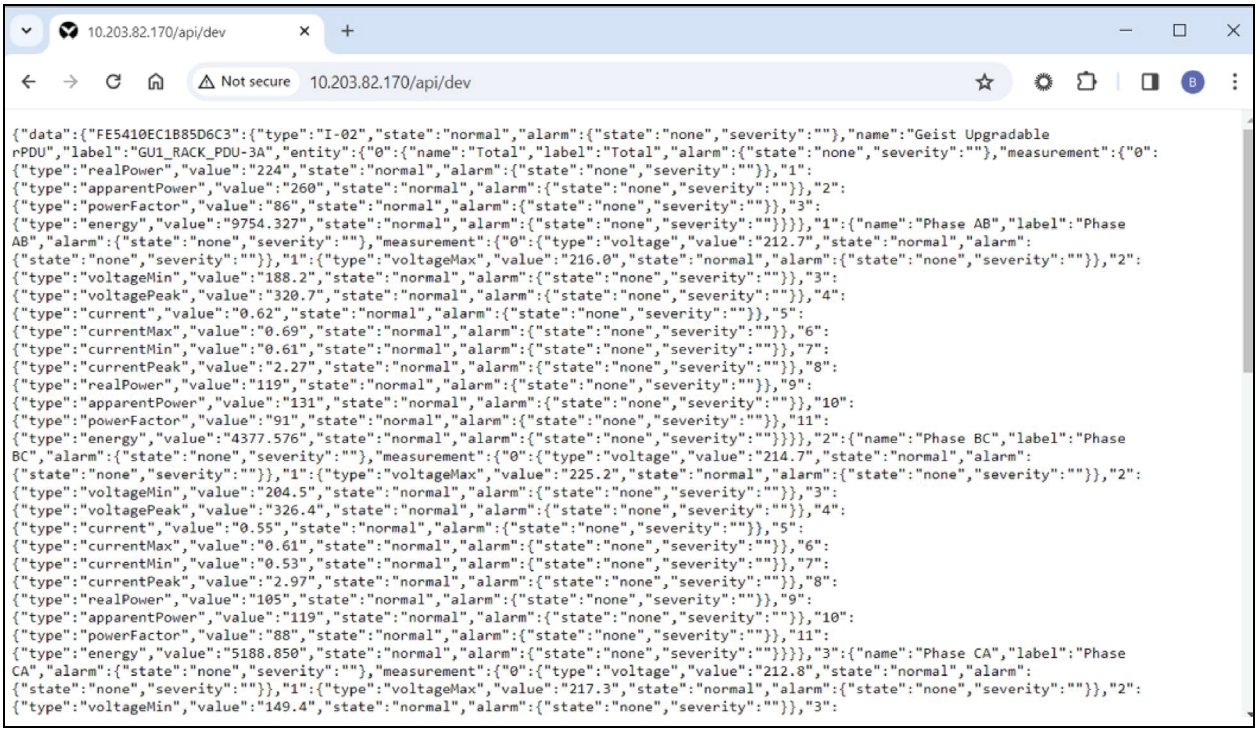

```
{"data":{"network":{"ethernet":{"type":"bridge","name":"Bridge 0","label":"Bridge
0","order":0,"removable":false,"enabled":true,"macAddr":"54:10:EC:1B:85:D6","dhcpOn":false,"ip4GW":"192.168.123.1","ip6GW":"","ports":
["port0","port1"],"address":{"0":{"address":"10.203.82.170","prefix":25,"mutable":true},"1":
{"address":"FE80::5610:ECFF:FE1B:85D6","prefix":64,"mutable":false}},"dns":{"0":{"address":"8.8.8.8","mutable":true},"1":
{"address":"8.8.4.4","mutable":true}},"route":{"0":
{"destination":"0.0.0.0","prefix":0,"gateway":"192.168.123.1","interface":"all","mutable":true}},"link":{"state":"up","uptime":92041},"stp":
{"enabled":false,"maxAge":0,"mode":"stp","forwardDelay":0,"helloTime":0}},"port0":{"type":"port","name":"Port 0","label":"Port
0","order":1,"removable":false,"enabled":true,"bridge":"ethernet","link":
{"state":"up","uptime":90250,"speed":"100Mb/s","duplex":"full","supportedModes":
["10baseT/Half","10baseT/Full","100baseT/Half","100baseT/Full"]},"stp":{"cost":0,"role":"unknown","state":"disabled"}},"port1":
{"type":"port","name":"Port 1","label":"Port 1","order":2,"removable":false,"enabled":true,"bridge":"ethernet","link":
{"state":"down","uptime":90250,"speed":"10Mb/s","duplex":"half","supportedModes":
["10baseT/Half","10baseT/Full","100baseT/Half","100baseT/Full"]},"stp":{"cost":0,"role":"unknown","state":"disabled"}}},"contact":
{"description":"6-branch C13/C19","location":"DCIM Lab","contactEmail":"","contactName":"Jim Hercules","contactPhone":""},"system":
{"label":"GU1_RACK_PDU-3A","hostname":"BB5410EC1B85D6"},"email":
{"server":"","port":25,"sender":"","username":"","passwordSet":false,"password":null,"sslEnabled":false,"target":{},"status":{"0":{"msg":"Email
OK"}}},"snmp":
{"v1v2cEnabled":true,"v3Enabled":true,"port":161,"readCommunity":"public","writeCommunity":"private","trapCommunity":"private","target":{"0":
{"trapVersion":"2c","user":"0","name":"10.207.120.32","port":"162"}},"user":{"0":
{"username":"","privPasswordSet":false,"privPassword":null,"privType":"none","authPasswordSet":false,"authPassword":null,"authType":"none","type":
"Read"},"1":
{"username":"","privPasswordSet":false,"privPassword":null,"privType":"none","authPasswordSet":false,"authPassword":null,"authType":"none","type":
"Write"},"2":
{"username":"","privPasswordSet":false,"privPassword":null,"privType":"none","authPasswordSet":false,"authPassword":null,"authType":"none","type":
"Trap"}},"engineID":"0x80"},"http":{"httpEnabled":true,"httpPort":80,"httpsPort":443},"syslog":{"enabled":false,"target":"","port":514},"locale":
{"defaultLang":"en","units":"imperial"},"camera":{},"display":{"gmsd":{"mode":"totalPower","vlc":{"enabled":false}}}},"retCode":0,"retMsg":""}
```


Device Configuration

From the web page, add this URL to retrieve the configuration file:

Device configuration: <<ipAddress>>\api\dev.

Figure 10.13 Example Device Configuration




```
{"data":{"FE5410EC1B85D6C3":{"type":"I-02","state":"normal","alarm":{"state":"none","severity":""},"name":"Geist Upgradable
rPDU","label":"GU1_RACK_PDU-3A","entity":{"0":{"name":"Total","label":"Total","alarm":{"state":"none","severity":""},"measurement":{"0":
{"type":"realPower","value":"224","state":"normal","alarm":{"state":"none","severity":""}},"1":
{"type":"apparentPower","value":"260","state":"normal","alarm":{"state":"none","severity":""}},"2":
{"type":"powerFactor","value":"86","state":"normal","alarm":{"state":"none","severity":""}},"3":
{"type":"energy","value":"9754.327","state":"normal","alarm":{"state":"none","severity":""}}}},"1":{"name":"Phase AB","label":"Phase
AB","alarm":{"state":"none","severity":""},"measurement":{"0":{"type":"voltage","value":"212.7","state":"normal","alarm":
{"state":"none","severity":""}},"1":{"type":"voltageMax","value":"216.0","state":"normal","alarm":{"state":"none","severity":""}},"2":
{"type":"voltageMin","value":"188.2","state":"normal","alarm":{"state":"none","severity":""}},"3":
{"type":"voltagePeak","value":"320.7","state":"normal","alarm":{"state":"none","severity":""}},"4":
{"type":"current","value":"0.62","state":"normal","alarm":{"state":"none","severity":""}},"5":
{"type":"currentMax","value":"0.69","state":"normal","alarm":{"state":"none","severity":""}},"6":
{"type":"currentMin","value":"0.61","state":"normal","alarm":{"state":"none","severity":""}},"7":
{"type":"currentPeak","value":"2.27","state":"normal","alarm":{"state":"none","severity":""}},"8":
{"type":"realPower","value":"119","state":"normal","alarm":{"state":"none","severity":""}},"9":
{"type":"apparentPower","value":"131","state":"normal","alarm":{"state":"none","severity":""}},"10":
{"type":"powerFactor","value":"91","state":"normal","alarm":{"state":"none","severity":""}},"11":
{"type":"energy","value":"4377.576","state":"normal","alarm":{"state":"none","severity":""}}}},"2":{"name":"Phase BC","label":"Phase
BC","alarm":{"state":"none","severity":""},"measurement":{"0":{"type":"voltage","value":"214.7","state":"normal","alarm":
{"state":"none","severity":""}},"1":{"type":"voltageMax","value":"225.2","state":"normal","alarm":{"state":"none","severity":""}},"2":
{"type":"voltageMin","value":"204.5","state":"normal","alarm":{"state":"none","severity":""}},"3":
{"type":"voltagePeak","value":"326.4","state":"normal","alarm":{"state":"none","severity":""}},"4":
{"type":"current","value":"0.55","state":"normal","alarm":{"state":"none","severity":""}},"5":
{"type":"currentMax","value":"0.61","state":"normal","alarm":{"state":"none","severity":""}},"6":
{"type":"currentMin","value":"0.53","state":"normal","alarm":{"state":"none","severity":""}},"7":
{"type":"currentPeak","value":"2.97","state":"normal","alarm":{"state":"none","severity":""}},"8":
{"type":"realPower","value":"105","state":"normal","alarm":{"state":"none","severity":""}},"9":
{"type":"apparentPower","value":"119","state":"normal","alarm":{"state":"none","severity":""}},"10":
{"type":"powerFactor","value":"88","state":"normal","alarm":{"state":"none","severity":""}},"11":
{"type":"energy","value":"5188.850","state":"normal","alarm":{"state":"none","severity":""}}}},"3":{"name":"Phase CA","label":"Phase
CA","alarm":{"state":"none","severity":""},"measurement":{"0":{"type":"voltage","value":"212.8","state":"normal","alarm":
{"state":"none","severity":""}},"1":{"type":"voltageMax","value":"217.3","state":"normal","alarm":{"state":"none","severity":""}},"2":
{"type":"voltageMin","value":"149.4","state":"normal","alarm":{"state":"none","severity":""}},"3":
```

Alarm Configuration

From the web page, add this URL to retrieve the configuration file:

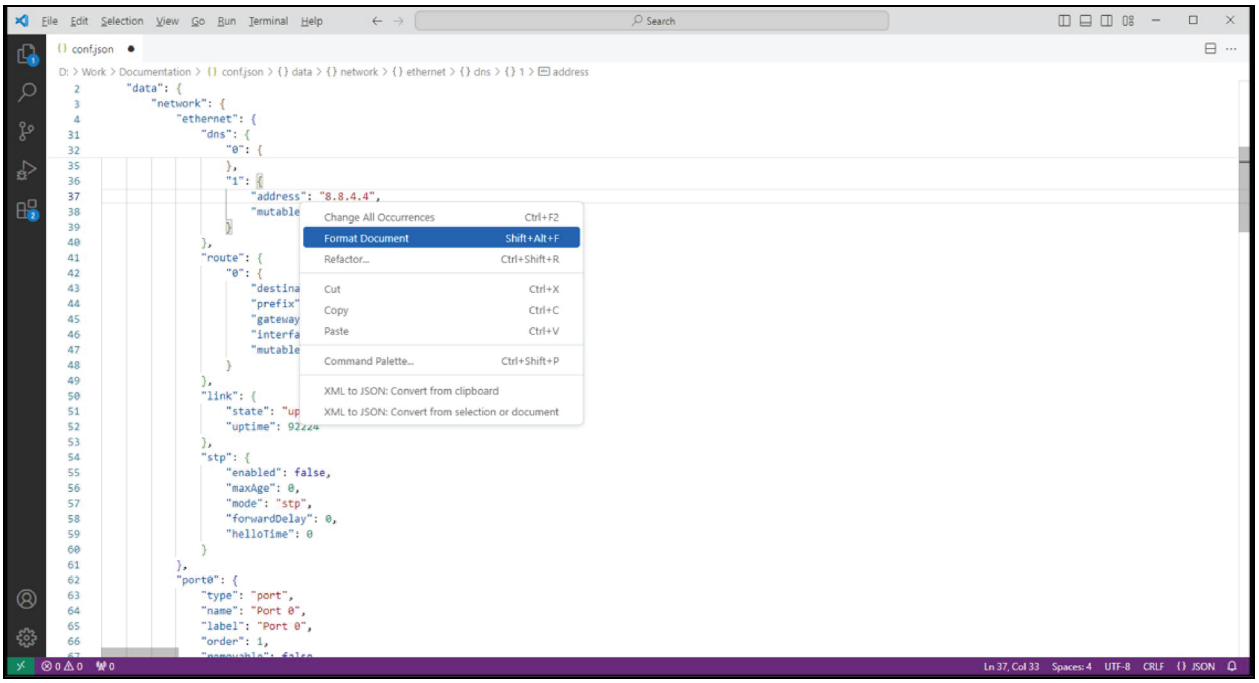
Host configuration: <<ipAddress>>\api\alarm

Figure 10.14 Example Alarm Configuration

To save the configuration locally to your computer, right click the browser window and choose **Save As**. The file is automatically named conf.json, but it can be renamed although the .json extension must be kept. For example, new-conf.json.

The file can be cleaned up using tools such as JSON Beautify, Notepad ++, or Visual Studio Code. Visual Studio Code has a Format Document option that adds indenting and context highlight to the configuration file.

Figure 10.15 Cleaning Up a Configuration File



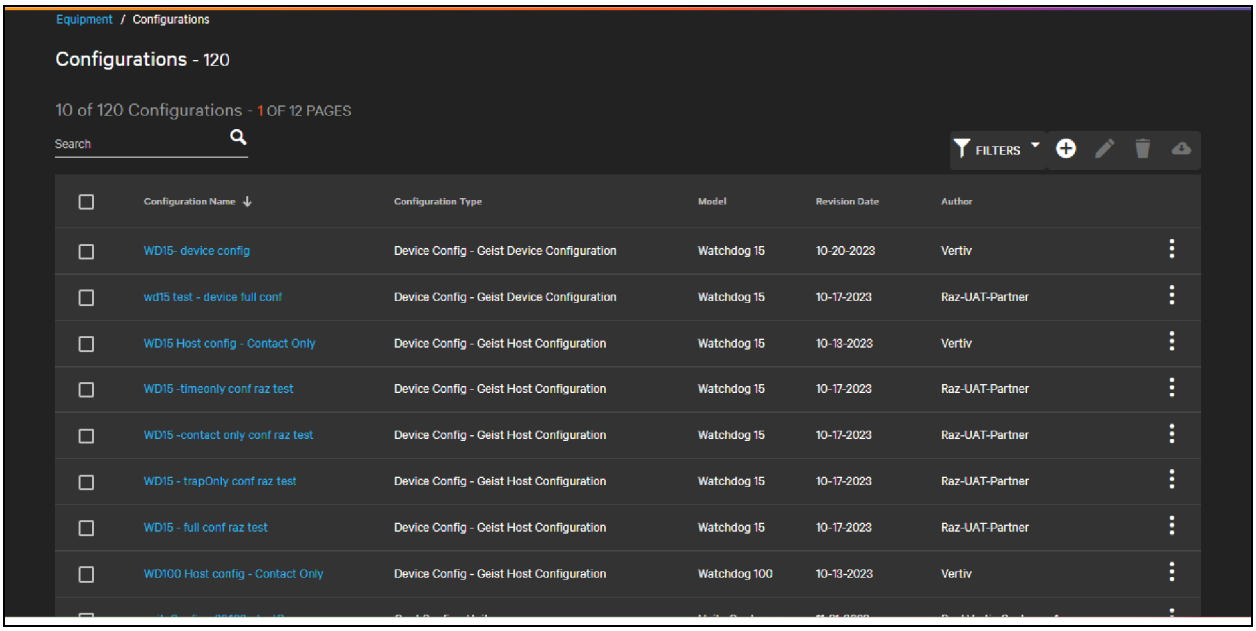
Cleaning up the file is not required to upload to Connect. It is suggested to make modifications to the file directly as it is easier to read and to see formatting issues.

10.2.3 Uploading Configuration Files

Vertiv provides sample configuration files for each configuration file type, but you may also upload your own configuration files specific to a partner or customer. These will be available only to you, or if you are a partner only to you and the customers you manage.

To upload configuration files to the Connect platform go to the **Equipment, Configurations** menu to see a list of available configurations. By default, this will be filtered to show only configurations uploaded by you or others in your organization, though you can change this filtering to show configurations available from Vertiv.

Figure 10.16 Configuration Library

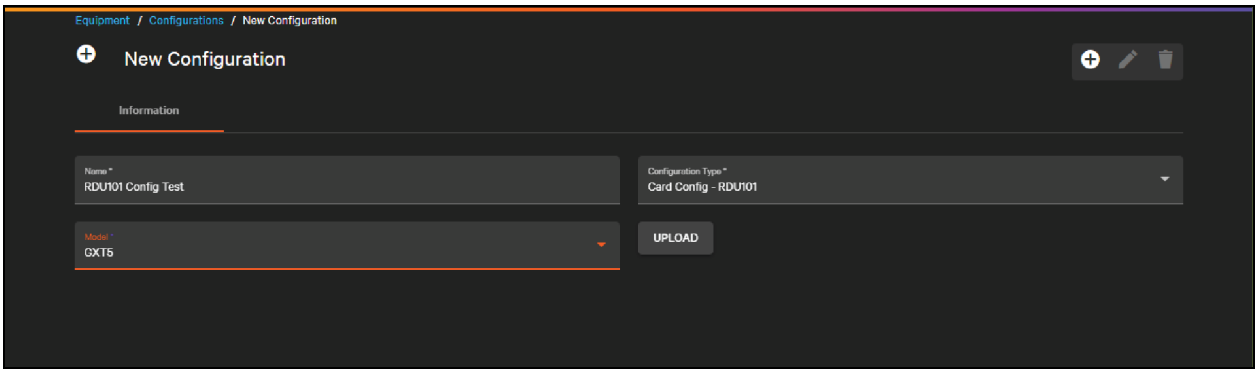


To upload a new file, click the

Add icon

The new Configuration Dialog opens. All fields are required.

Figure 10.17 New Configuration Dialog



Enter a name for the configuration file and select a configuration type from the drop down.

CAUTION: Select the configuration type carefully. The type of configuration you select affects the devices to which the configuration file can be pushed. If you are unsure of which configuration type to select, see Configuration File Types on page 150.

Select a model. Depending on the configuration type, choose this by either model of the edge device or the model of Intellislot card (Unity, RDU101, or RDU120) in the case of card configurations. Be sure to select the correct model.

To upload the configuration file, click **Upload** to browse for the location and to choose the file on your local hard drive where the configuration file is stored. Select the file and click **Open** to upload to the platform.

When all fields are completed and the configuration file is uploaded, click **Save** to finalize the configuration file record in the configuration library.

Like other lists with in Connect, files can be managed individually or in bulk. To edit the name or upload a replacement file, click **Edit** from the


Pulldown icon.

To delete one or more files, select the checkbox next to the file and click the


Delete icon.

NOTE: You may only edit or delete configuration files that have been authorized by your organization.

To download a configuration file, click the **Pulldown** menu and choose the


Download icon

You can download any configuration file that you have access to, including samples from Vertiv.

10.2.4 Pushing Configurations to Cards and Edge Devices

Configuration files that are uploaded to the platform on each device can be pushed to each individual device or in bulk action. See Bulk Actions on page 172 for further information.

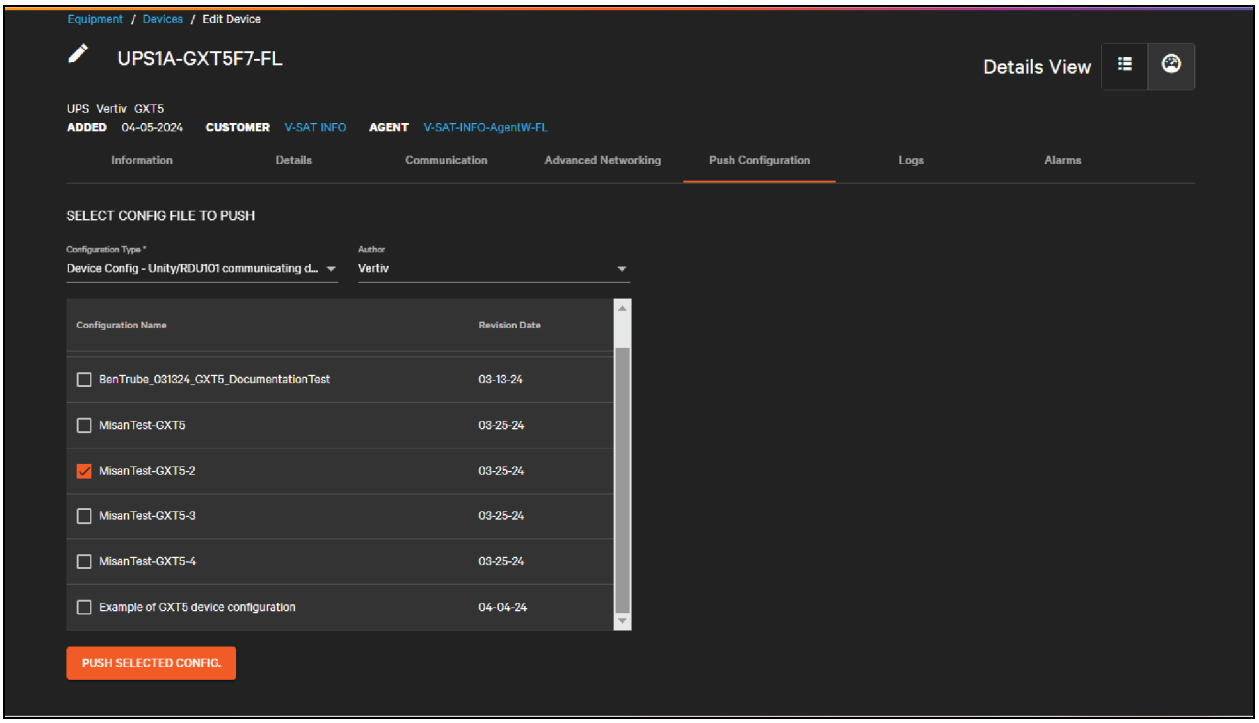
NOTE: Use only configuration files you or a managing partner have uploaded. Vertiv files are intended as examples and should be modified and saved as new, unique configuration files before uploading to a device.

To push a configuration file to a card or a device, enter the edit mode for the device by clicking the


Edit icon.

Click either the **Push Configuration** button or **Push Configuration** tab to push the configuration to the edge card or device.

Figure 10.18 Card Configuration File Example



The push configuration dialog has several drop down options that narrows the files available. The configuration type corresponds to the configuration file types covered in Configuration File Types on page 150 .The values of these two drop downs filter the list of options available at the bottom of the window.

To push a file, select it from the list and click **Push Selected Config**. Only one file can be pushed to a device at a time.

Like other settings, pushing a device or card configuration may require a reboot for the settings to be applied. A dialog warning you that the card will pop up asking if you wish to continue. Click **Yes** to apply the selected file or **Cancel** to go back to the previous dialog.

Once the configuration file has been applied, a status toast notifies the user whether the operation has succeeded or failed. If the operation has failed, this may be due to a lack of communication with the edge device or a formatting error in the configuration file.

NOTE: Review any configuration files thoroughly before applying to the edge devices to check for any formatting or value errors.

10.3 Use Case: Setting Agent as the Trap Target

For the local agent to receive traps from the edge device, the IPv4 Address of the agent must be configured as a trap target on the device. This is done via configuration files for both Intellislot Card communicating devices and for Raven-Based Geist devices.

Intellislot Cards (Unity or RDU101)

Configuration files for Intellislot cards (Unity and RDU101) are text-based .ini files. For more details, refer to Device Configuration on page 153.

When exporting a configuration .ini file, protected fields like passwords, community strings, or authentication secrets are not displayed by default, but they can be manually entered into the file.

Figure 10.19 Intellislot .ini Configuration File: SNMPv1 Trap

```
[SNMPv1 Trap.1]

# SNMP Trap Target
#   Configure a network host destination for SNMPv1 Traps. The trap target may be a
hostname or an IP address. Note: Maximum length is 125 characters.
#   maximum length: 125

SNMP Trap Target: "192.168.1.125"

# SNMP Trap Port
#   Port on the trap target to which to send SNMPv1 traps.
#   range: 1 to 65535

SNMP Trap Port: 162

# SNMP Trap Community String
#   Password string used by the trap target to authenticate traps. Printable
characters are allowed with the exception of <, >, comma, semicolon, and space. Note:
Maximum length is 32 characters.
#   maximum length: 32
# ** Protected value not displayed.  Uncomment following line to import new value:

SNMP Trap Community String: "public"
```

The Intellislot card supports up to 20 trap targets for v1/v2c traps. Each target consists of three values:

- SNMP Trap Target (an IPv4 address)
- Trap Port
- Trap Community String

NOTE: The community string must be set to public for the local agent to receive and interpret the trap. This will be revised in the future.

SNMP v3 Traps/Informs are also supported (up to 20). The trap target information is embedded as an attribute of the SNMPv3 user.

Figure 10.20 Intellislot .ini Configuration File: SNMPv3 Username, Access Type, and Authentication

```
[SNMPv3 User.1]

# SNMPv3 User Enable
#   Enable or disable reading, writing, or sending traps with the user's credentials.
#   0: disabled
#   1: enabled

SNMPv3 User Enable: 0

# SNMPv3 Username
#   Username for authentication and privacy settings. Printable characters are
allowed with the exception of <, >, colon, semicolon, space, tab, double quote, and
question mark.
#   maximum length: 32

SNMPv3 Username: ""

# SNMPv3 Access Type
#   Select the SNMPv3 access type: Read Only, Read/Write, or Traps Only.
#   0: Read Only
#   1: Read/Write
#   2: Traps Only

SNMPv3 Access Type: 0

# SNMPv3 Authentication
#   Algorithm used for authentication: None, MD5, or SHA-1.
#   0: None
#   1: MD5
#   2: SHA

SNMPv3 Authentication: 0
```

Figure 10.21 Intellislot .ini Configuration File: SNMPv3 Authentication and Authentication Secret

```
SNMPv3 Authentication Secret: ""

# SNMPv3 Privacy
#   Algorithm used for encryption: None, DES or AES128.
#   0: None
#   1: DES
#   2: AES

SNMPv3 Privacy: 0

# SNMPv3 Privacy Secret
#   Password for generation of the SNMPv3 privacy key. Printable characters are
allowed with the exception of <, >, colon, tab, double quote, and question mark.
Note: The entry must be 8 to 64 characters.
#   maximum length: 64

SNMPv3 Privacy Secret: ""

# SNMPv3 Trap Targets
#   Configure one or more network host destinations for SNMPv3 Traps. Each trap
target may be a hostname or an IP address. Multiple targets must be separated by
commas ','. Note: Maximum length is 125 characters.
#   maximum length: 125

SNMPv3 Trap Targets: ""

# SNMPv3 Trap Port
#   The IP port number for SNMPv3 traps.
#   range: 1 to 65535

SNMPv3 Trap Port: 162
```

After modifying the configuration file, upload it to the Connect platform and push it to the edge device. Refer to Uploading Configuration Files on page 155 and Pushing Configurations to Cards and Edge Devices on page 156.

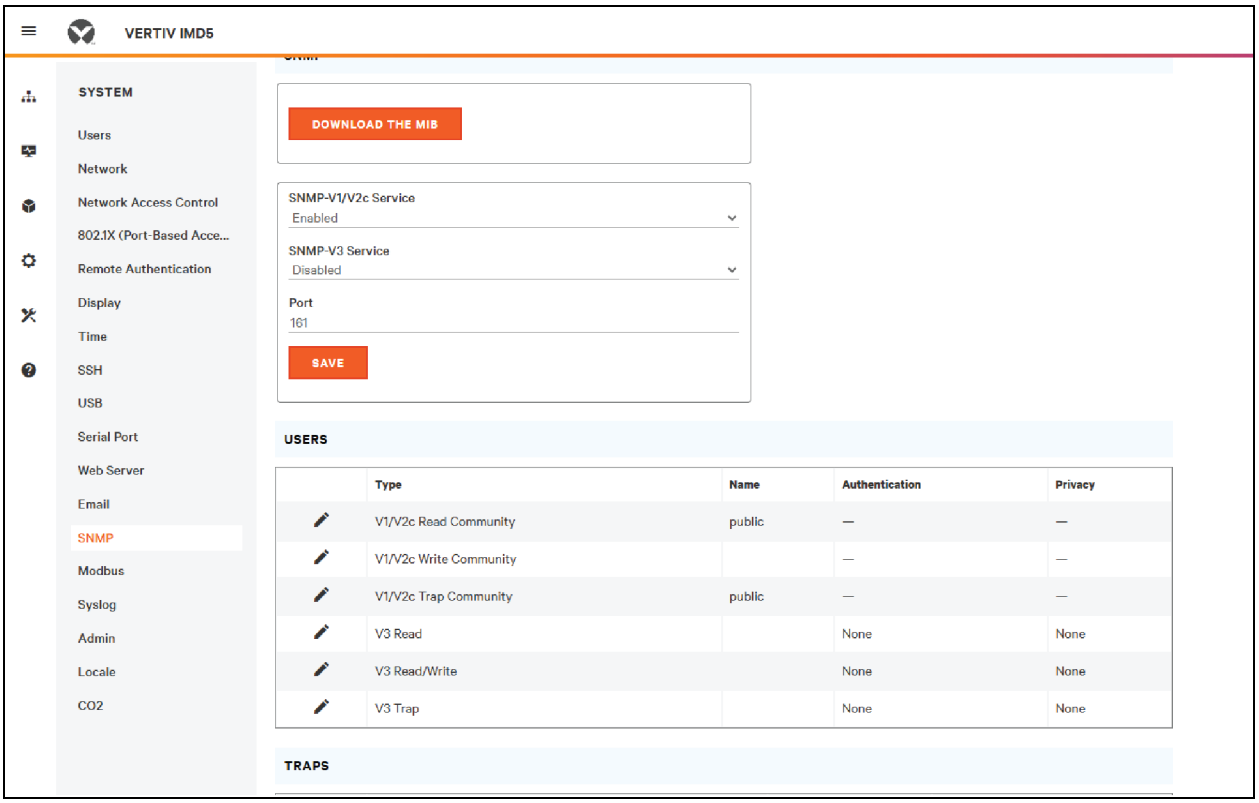
Geist Configuration

For Geist Raven-based devices, Vertiv recommends that you manually configure the first device via the device's local webpage, export the configuration, and then apply the settings to multiple devices.

WARNING! Older Blackbird-based devices (GU1 with an IMD2 or the Watchdog 15/100) are not supported.

Configure SNMP settings by clicking **System Menu** and selecting **SNMP**.

Figure 10.22 IMD SNMP Settings

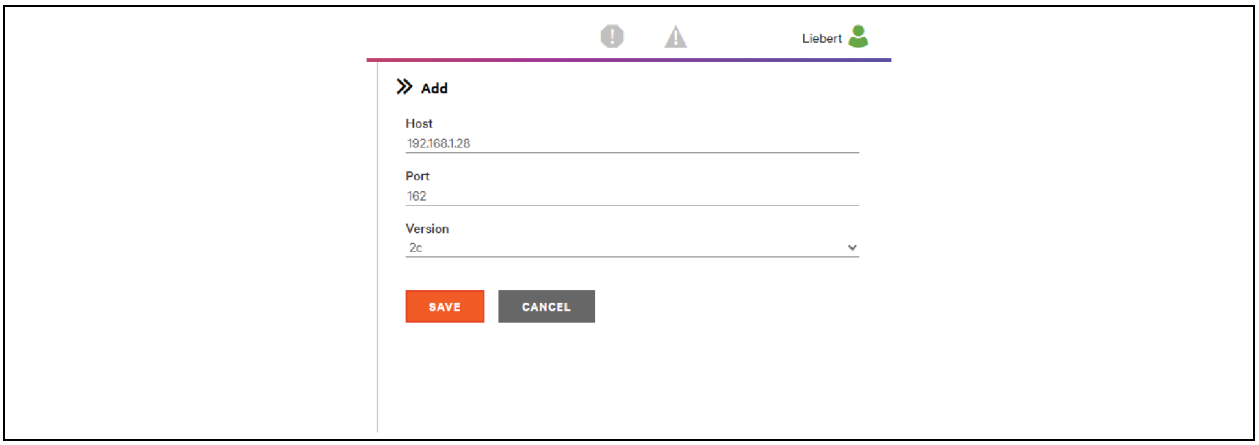


Trap targets are added at the bottom of the page. Click the

Add icon

to open the Add Trap Target dialog.

Figure 10.23 Add Trap Target



Geist devices can have both v1/v2c SNMP credentials and v3 credentials active. Unlike Intellislot, they have a single set of credentials for each version but can have multiple targets.

Selecting the SNMP version associates the trap with specific SNMP credentials. Click **Save** to add the new target.

The SNMP configuration including trap targets is in the Host configuration file. Retrieve the host configuration via this URL:

<<ipAddress>>**\api\conf**

Replacing <<ipAddress>> with the IPv4 address of the edge device. Paste this address into a browser window. Refer to Pulling Configuration Files from the Edge Device on page 151.

Figure 10.24 Host Configuration in a Browser

Right-click the file and Save As a JSON file to your local computer.

Geist configuration files are not export with any credentials, although the configuration file will include community strings. If you import the file and credentials are blank, existing credential remain in place.

Figure 10.25 SNMP Configuration Geist Host File

IMPORTANT! Modify the JSON file to look like the example above so as not to import other settings when applying the configuration file to multiple devices. Include everything between the SNMP braces { } and the wrapping attributes as shown above.

After you have modified the configuration file, upload it to the Connect platform and push it to the edge device. See Uploading Configuration Files on page 155 and Pushing Configurations to Cards and Edge Devices on page 156.

NOTE: Format of JSON files is described in detail in the Geist Public API document. You can download the latest version of the API document here: https://www.vertiv.com/49e32f/globalassets/products/critical-power/power-distribution/geist-api-specification-api-specifications-sl-70874.pdf.

The URL for the API is here: https://www.vertiv.com/en-us/products-catalog/critical-power/power-distribution/vertiv-geist-updu-universal-power-distribution-unit/#/downloads.

10.4 Use Case: Setting Intellislot Device Parameters via SNMP Writes

For all devices that support SNMP writes, Connect allows users to set values using a formatted CSV file. Vertiv provides CSV formatted example device parameter files for all Vertiv devices supported by Connect allow SNMP writes. Users can apply all the settings in the file or a subset.

To download an example configuration file, go to the **Configurations** sub-menu under **Equipment**. Change the **Author** filter to Vertiv. Configurations supplied by Vertiv are located here.

For this section you are looking for the configuration type **Device Config – Generic (via SNMP Writes)**. Click on the name of the configuration to load its details, then click the download link to download the file. You then edit the .CSV file in Excel, Notepad++, or another editor.

NOTE: Data parameters can be modified when opened in Excel.

Figure 10.26 Example CSV for GXT5, Outlet Group Settings

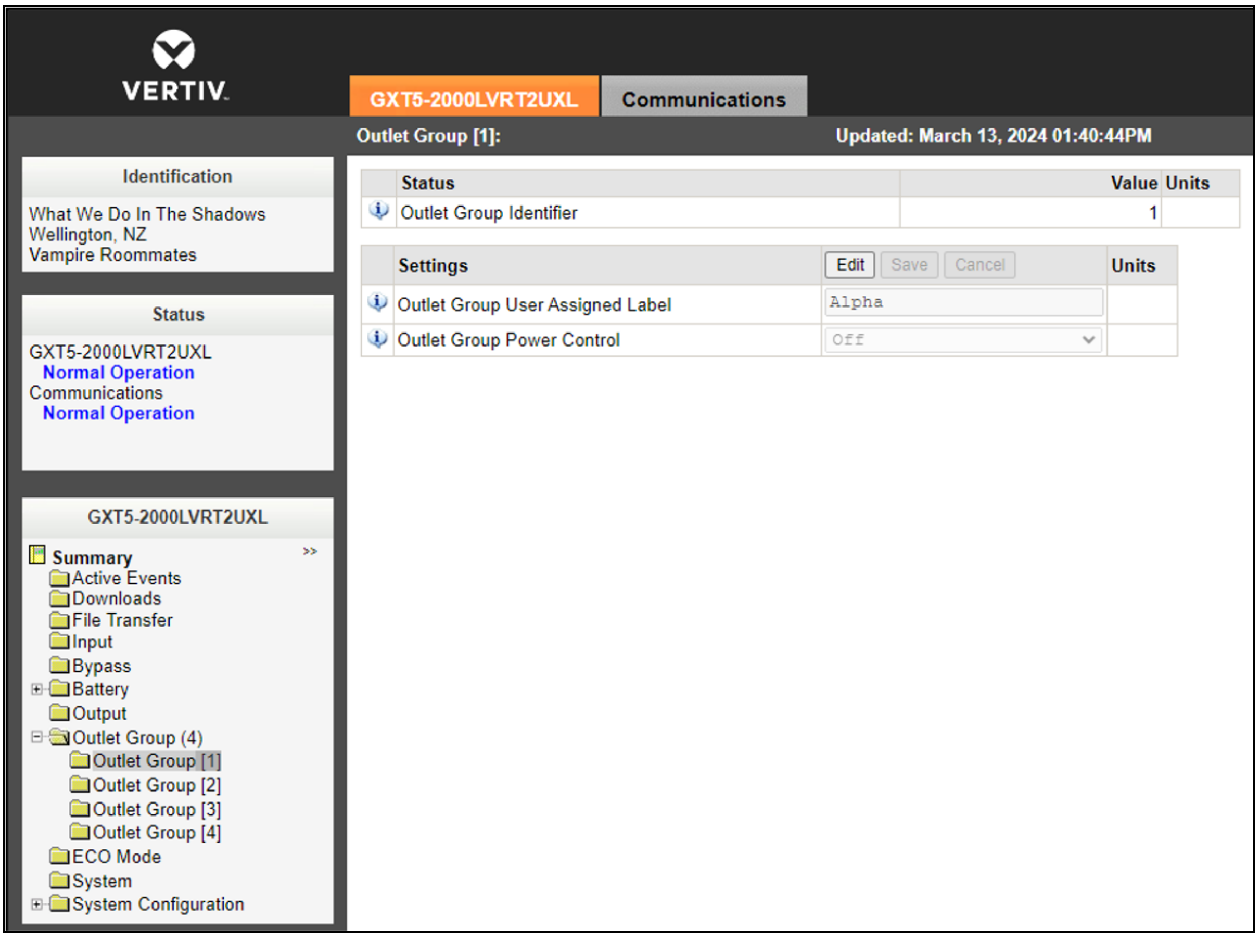
	A	B	C	D	E
1	Outlet Group User Assigned Label	.1.3.6.1.4.1.476.1.42.3.9.20.1.20.1.2.1.4359.1	OctetString	Alpha	The user assigned outlet group name
2	Outlet Group User Assigned Label	.1.3.6.1.4.1.476.1.42.3.9.20.1.20.1.2.1.4359.2	OctetString	Beta	The user assigned outlet group name
3	Outlet Group User Assigned Label	.1.3.6.1.4.1.476.1.42.3.9.20.1.20.1.2.1.4359.3	OctetString	Charlie	The user assigned outlet group name
4	Outlet Group User Assigned Label	.1.3.6.1.4.1.476.1.42.3.9.20.1.20.1.2.1.4359.4	OctetString	Delta	The user assigned outlet group name
5	Outlet Group Power Control	.1.3.6.1.4.1.476.1.42.3.9.30.1.20.1.2.1.4365.1	Gauge	0	Outlet Group Power Control (OFF, ON, Cycle, etc)
6	Outlet Group Power Control	.1.3.6.1.4.1.476.1.42.3.9.30.1.20.1.2.1.4365.2	Gauge	1	Outlet Group Power Control (OFF, ON, Cycle, etc)
7	Outlet Group Power Control	.1.3.6.1.4.1.476.1.42.3.9.30.1.20.1.2.1.4365.3	Gauge	1	Outlet Group Power Control (OFF, ON, Cycle, etc)
8	Outlet Group Power Control	.1.3.6.1.4.1.476.1.42.3.9.30.1.20.1.2.1.4365.4	Gauge	2	Outlet Group Power Control (OFF, ON, Cycle, etc)

The CSV file format includes these columns:

- Point Name
- OID
- DataType
- Value
- Description

You only need to modify the Value column. The type and description columns offer additional information on valid values, though you may adjust these settings on one edge device before applying to multiple.

Figure 10.27 Outlet Group 1 Settings after Applying Configuration



If an invalid value is put in the CSV, that parameter will be ignored. If the CSV file format is corrupted, the configuration file cannot be applied and pushing the configuration will fail.

IMPORTANT! Vertiv recommends that you apply this configuration file to a single device before applying in bulk.

After modifying the configuration file, upload it to the Connect platform and push it to the edge device. See Uploading Configuration Files on page 155 and Pushing Configurations to Cards and Edge Devices on page 156.

CAUTION: Device parameters use SNMP writes to set the parameters. Ensure that you have proper write credentials specified for your device or the parameter setting will fail.

10.5 Use Case: Setting Alarms

For Raven-based Geist devices (GU2 or GU1s with the IMD3 controller), use Connect to push alarm configurations to the edge device.

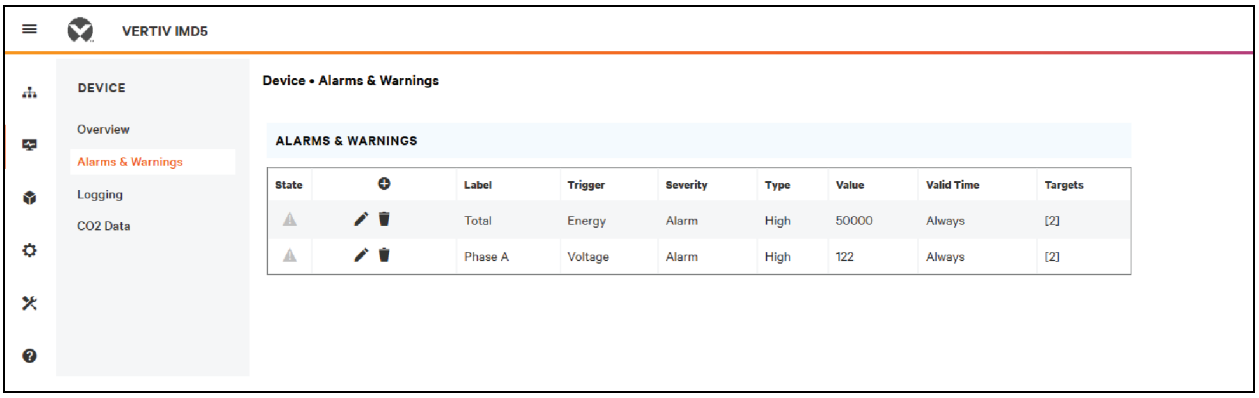
WARNING! Older Blackbird-based Geist devices, GUI1 with an IMD2 and the Watchdog 15/100 are not supported.

NOTE: For Intellislot devices, well-known alarms are already configured. Some of these alarms have thresholds that can be set using device parameters. See Use Case: Setting Intellislot Device Parameters via SNMP Writes on page 164.

Vertiv recommends configuring alarms as desired on one device via the device's local webpage, then exporting that configuration and applying it to other devices. This is to ensure correct formatting and that all necessary parameters are in place.

To manually configure an alarm, click the **Sensors** menu on the local device web page and select **Alarms & Warnings**.

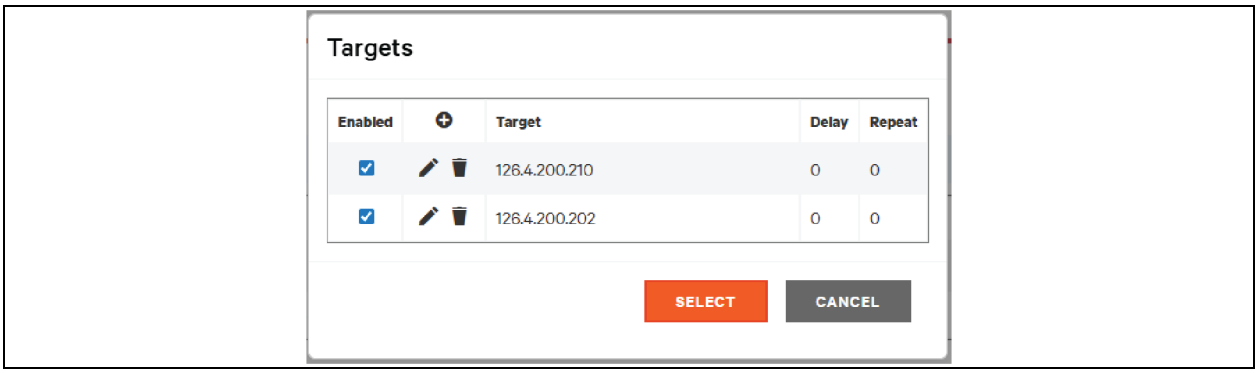
Figure 10.28 Alarms & Warnings Page



To add an alarm, click the

Add icon to open the Add dialog.

Figure 10.29 Add Dialog to Add Another Trap Target

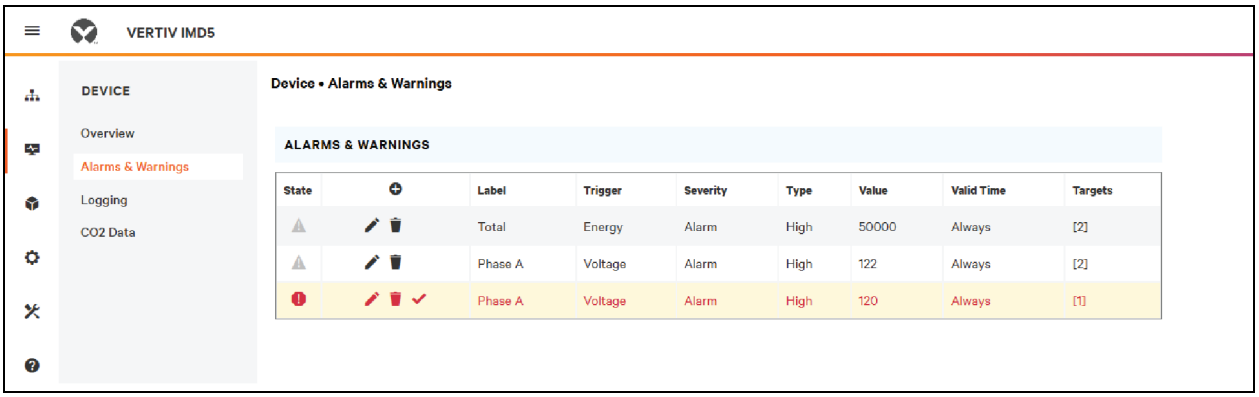


The targets shown in this dialog must be added in the SNMP configuration section first before being able to be added as an alarm target. Refer to Use Case: Setting Agent as the Trap Target on page 158.

NOTE: Be sure to select the checkbox next to each trap target when configuring the alarm. Otherwise, those targets will not be associated with the alarm.

Click Save to add the alarm to the edge device. When the alarm is active, it is evaluated to see if alarm conditions are met and will trigger active alarms.

Figure 10.30 New Alarm Added



The SNMP configuration including alarms is in the Alarm configuration file. Retrieve the alarm configuration via the following URL:

<<ipAddress>>**\api\alarm**

Edit the URL to replace <<ipAddress>> with the IPV4 address of the edge device.

Refer to Pulling Configuration Files from the Edge Device on page 151.

Figure 10.31 Extract Alarm Configuration

Right-click the file and save as a JSON file to your local computer. Figure 10.32 on the next page shows the contents of an extracted alarm configuration. Maximized sections are for the alarm added in previous screenshots.

Figure 10.32 JSON Alarm Configuration Example

```
{
    "data": {
        "trigger": {
            "0": {…
            },
            "1": {
                "state": "tripped",
                "latching": false,
                "type": "high",
                "severity": "alarm",
                "path": "FE5410EC1B85D6C3/entity/1/measurement/8",
                "threshold": "110.00",
                "clearDelay": "0",
                "tripDelay": "0",
                "selectedActions": [
                    1
                ]
            }
        },
        "action": {
            "0": {…
            },
            "1": {
                "target": "11",
                "delay": 0,
                "repeat": 0
            }
        },
        "target": {
            "10": {…
            },
            "11": {
                "name": "192.168.1.125",
                "group": "trap",
                "type": "trap",
                "enabled": true,
                "path": "api/conf/snmp/target/1"
            }
        }
    },
    "retCode": 0,
    "retMsg": ""
```


Alarm configurations can be applied to multiple units as long as both units have the same configuration (i.e., the same number of outlets, phases, are both WYE or DELTA based, etc.). All three sections (trigger, action, target) are required and are interconnected.

When an alarm or device file is extracted, it has a specific serial number for the component. For example, FE5410EC1B85D6C3 in Figure 10.32 above. Replace this with 16 zeroes (0000000000000000) in all places within the file when using generically across multiple devices.

NOTE: Alarms have a tie back to host configurations for SNMP trap targets. Be sure that the configuration file for alarms is applied with its companion host file (ideally sourced from the same original first device).

After you have modified the configuration file, upload it to the Connect platform. See Uploading Configuration Files on page 155 and Pushing Configurations to Cards and Edge Devices on page 156.

NOTE: Format of JSON files is described in detail in the Geist Public API document. You can download the latest version of the API document here: https://www.vertiv.com/49e32f/globalassets/products/critical-power/power-distribution/geist-api-specification-api-specifications-sl-70874.pdf.

The URL for the API is here: https://www.vertiv.com/en-us/products-catalog/critical-power/power-distribution/vertiv-geist-updu-universal-power-distribution-unit/#/downloads.

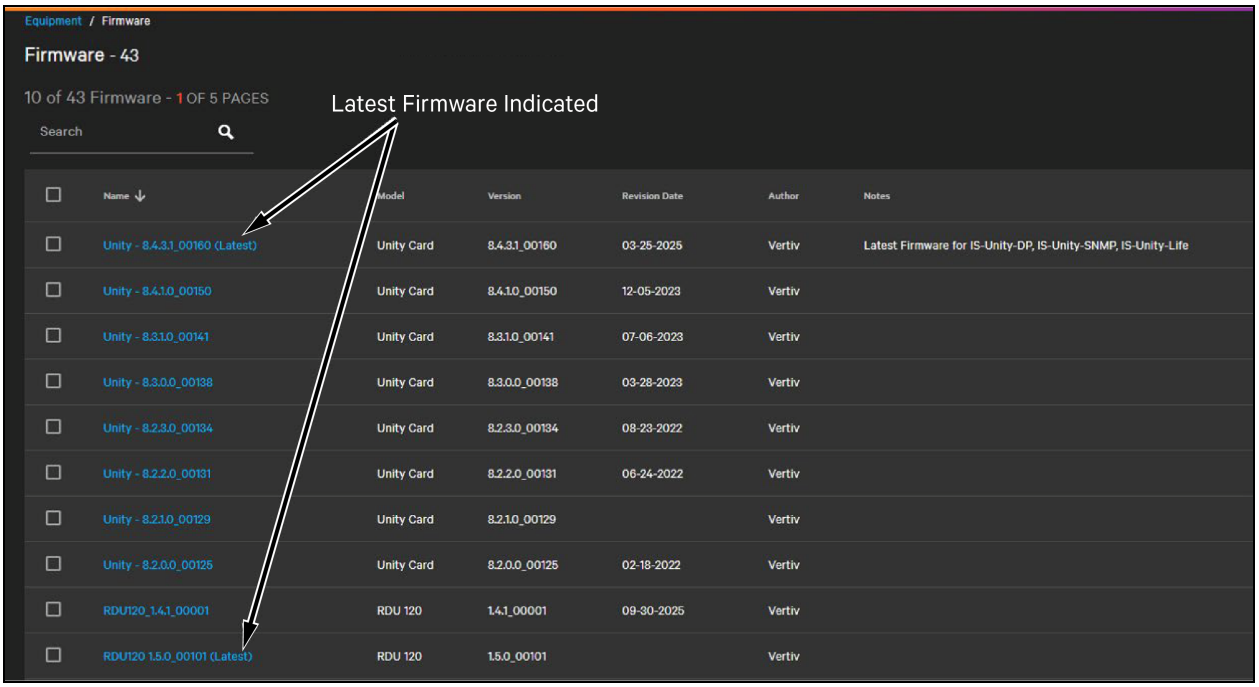
10.6 Update Firmware

Connect can update the communication card and device firmware for a limited set of Vertiv devices. Connect requires devices to be upgraded to a base level of firmware before supporting all provisioning capabilities.

Refer to Supported Devices on page 174 for further details.

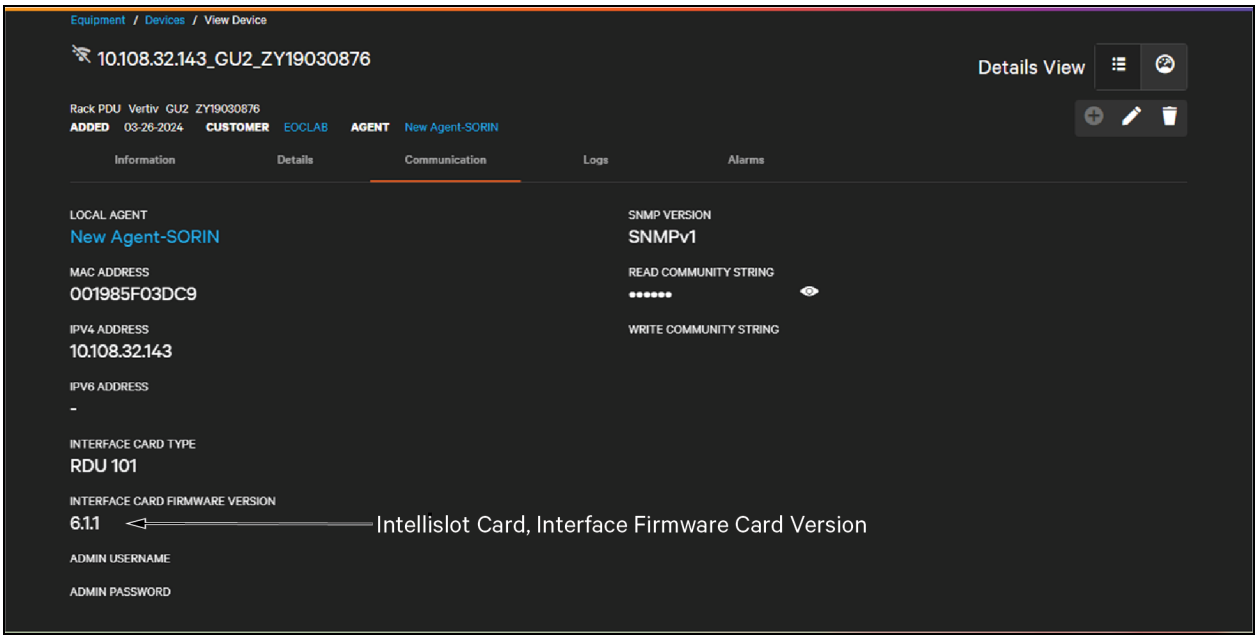
Vertiv maintains a library of firmware available to all users. The latest firmware is marked **(latest)**.

Figure 10.33 Firmware List



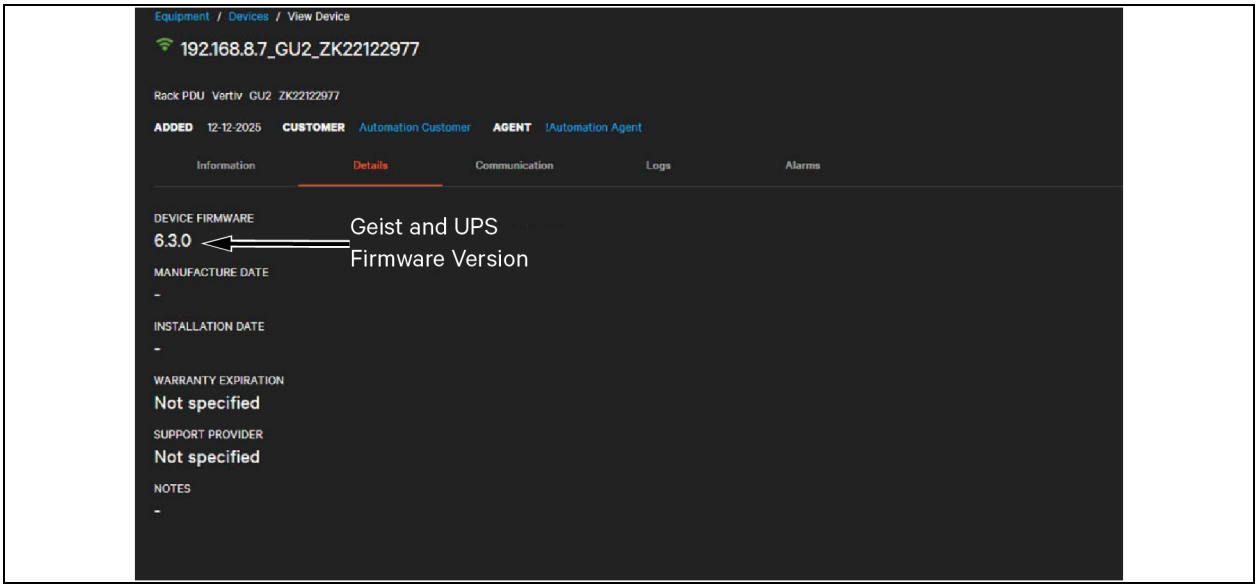
The firmware version that is currently running for Intellislot cards is reported on the **Communications** tab, under **Interface Card Firmware Version**.

Figure 10.34 Intellislot Card Device, Interface Card Firmware Version



For Geist devices, the firmware currently running is reported on the **Details** tab and the **Communications** tab.

Figure 10.35 Geist Device Firmware

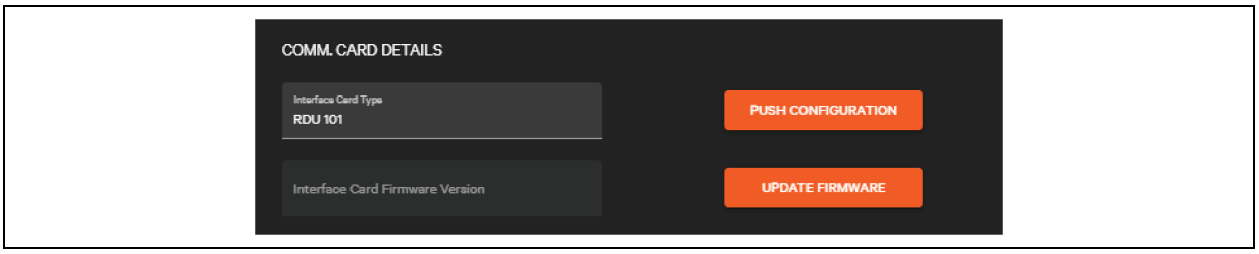


To update the firmware of an individual device, go to the individual details of that device, click the **Communications** tab, and then click the

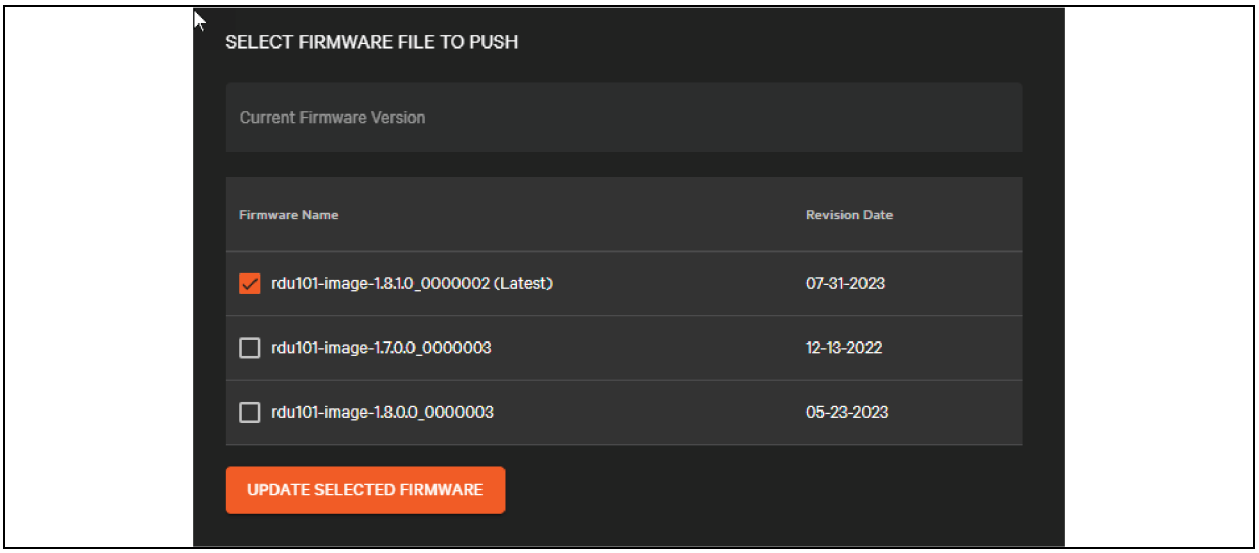
Edit icon.

Locate the Comm. Card Details

Figure 10.36 Update Firmware for a Communication Card



Click **Update Firmware**. A list of available firmware opens.

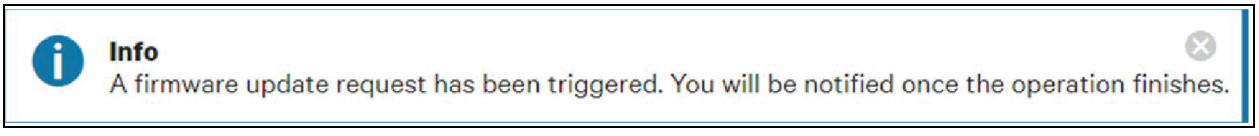


Select a single firmware from this list to apply to the edge devices. The list of available firmware will not include all released firmware but will include the last few public releases.

NOTE: Vertiv recommends to always update to the latest firmware, unless card documentation or market memo indicates that an interim upgrade version is required.

After selecting the firmware versions, click Update Selected Firmware to start the update and confirm when asked to proceed. Firmware updates can take 10 - 15 minutes per device. This includes sending the new firmware to the device, flashing the device memory, and rebooting the device if the flash was successful.

Figure 10.37 Firmware Operation Start Toast

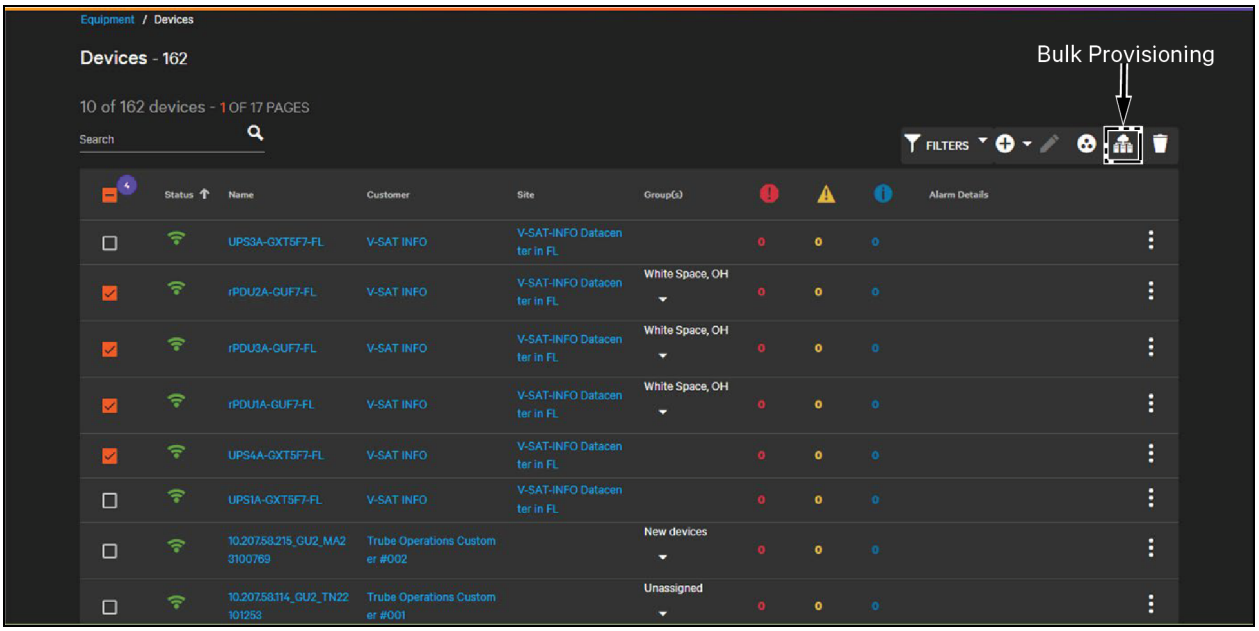


IMPORTANT! Firmware updates can be applied to monitored and unmonitored devices, including those with only an IPv6 address. However, it is recommended to specify a unique IPv4 address before upgrading firmware in most cases.

10.7 Bulk Actions

All the provisioning actions described in this section can be taken singly or in bulk. Trigger provisioning actions from any device list, under a partner, customer, site, or group in the **Devices** sub-menu under **Equipment**.

Figure 10.38 Selecting Devices to Bulk Provision



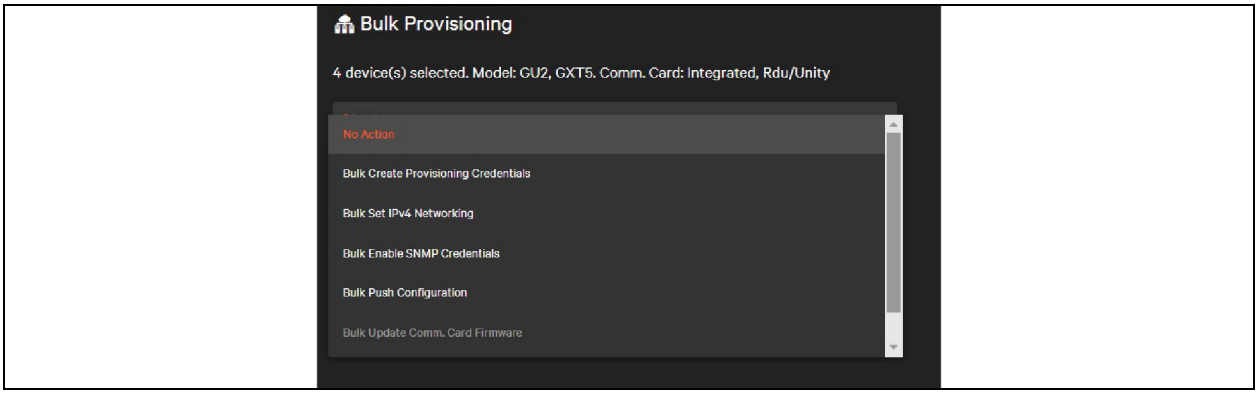
To trigger actions in bulk, select two or more devices from the list and click the

Bulk Provisioning icon

The Bulk Provisioning dialog opens. If you are a partner user, all devices must be in the same customer.

IMPORTANT! Pushing configuration files and firmware updates require that all devices be the same model. Other actions can be taken on a mix of devices.

Figure 10.39 Bulk Provisioning Dialog, Select Provisioning Action



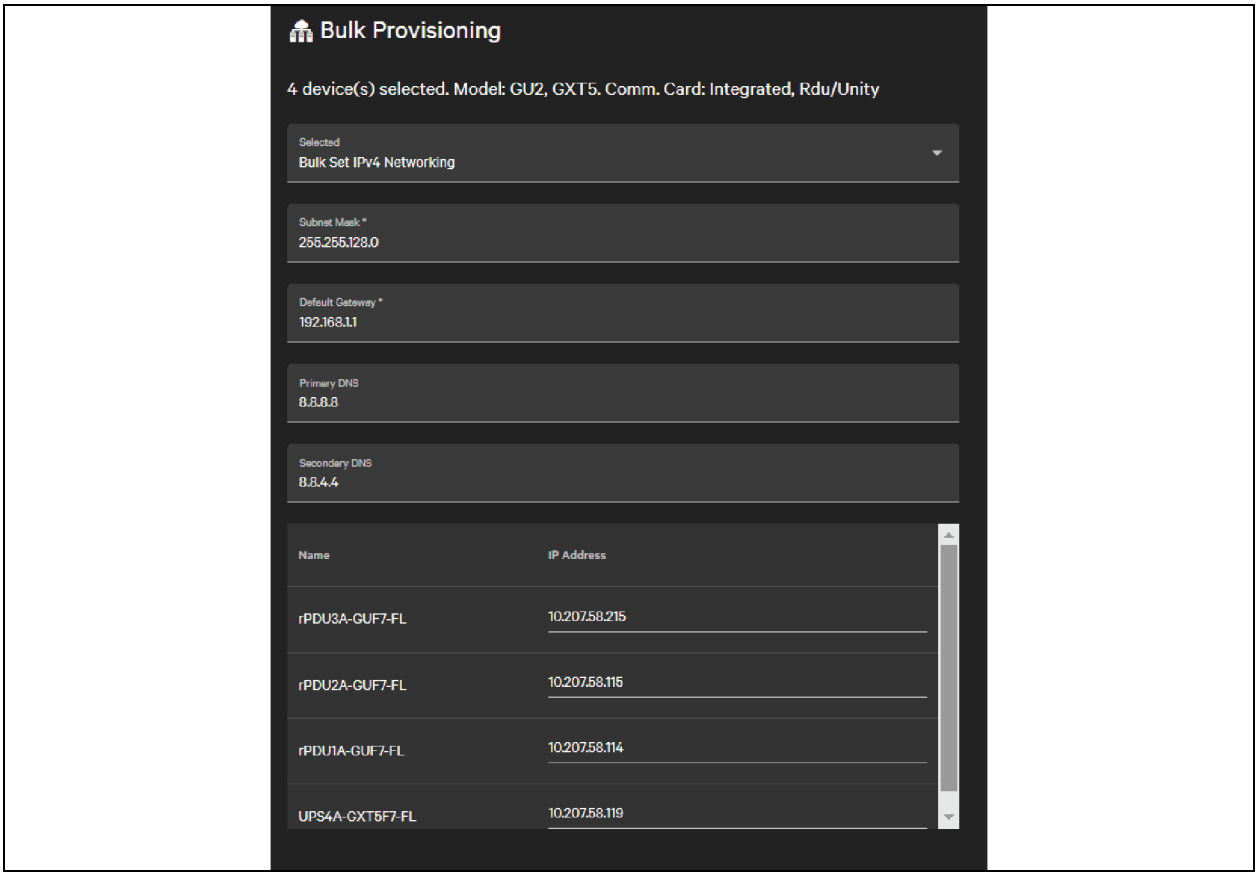
The Bulk Provisioning dialog provides a summary of the models and devices selected. Check to ensure it matches your intention.

Select a provisioning action. Some actions are disabled based on the devices selected. Some actions apply the same settings to all devices:

- Creating Provisioning Credentials
- SNMP Credentials
- Pushing Configurations
- Applying firmware

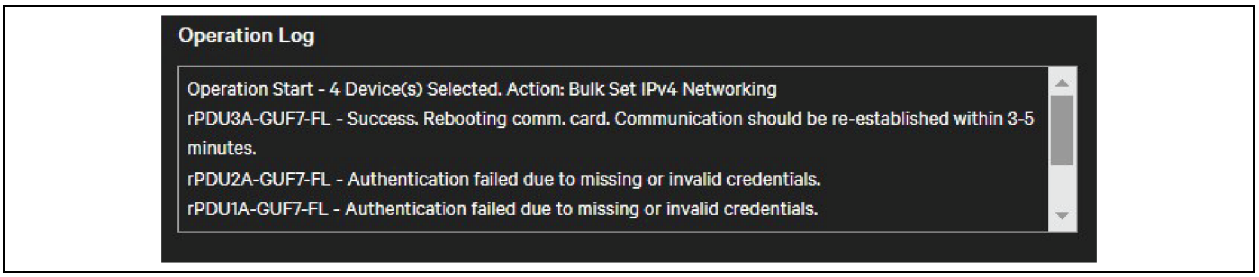
Networking permits setting some common values such as subnet DNS, and default gateway while applying a unique value to each device selected (IPv4 address).

Figure 10.40 Bulk Provisioning Networking



Complete all fields and click **Run Action** to run the provisioning action. An operation log opens to show the status of each action.

Figure 10.41 Operation Log



WARNING! While running provisioning actions, do not navigate away from the page while the operation is running. If you navigate away, the operation will be halted and not completed. To continue making changes in the product, open a new tab. The only exception to this is updating firmware, which will allow you to navigate away.

10.8 Supported Devices

Table 10.1 Device Configuration and Firmware Updates Supported on Vertiv Devices

Type of Action	Supported Models	Base Firmware Required	Comments
Intellislot Card Configuration	Unity and RDU101 cards	Unity: 8.2.0.0_00125+ RDU101: 1.7.0.0_0000003+	
Device Configuration via SNMP Writes	Vertiv and third party devices	N/A	
Card Firmware Update	Unity, RDU101 and RDU120 cards	Unity: 8.2.0.0_00125+ RDU101: 1.7.0.0_0000003+ RDU120: 1.4.0_00001+	
Device Firmware Update	GXT5 VRLA and Li-Ion Variants	See **Table 10.2** below for more details	Supported on applicable GXT5's manufactured 2021 or later. See **Table 10.2** below.
Geist Configuration (Raven-Based Models)	GU2 (with IMD-05 or IMD-03 controller), GU1 (with IMD-03 controller)	Raven 5.9.0+	
Geist Firmware Update (Raven-Based Models)	GU2 (with IMD-05 or IMD-03 controller), GU1 (with IMD-03 controller	Raven 5.9.0+	

Table 10.2 Supported GXT5 Model Families that are Currently Supported for GXT5 UPS Firmware Update.

Supported Model Family	Base Firmware required	Notes
GXT5 VRLA UPS 500-3KVA (LV, HV, I) GXT5 VRLA UPS 5KVA-10KVA (MV) GXT5 VRLA UPS 15KVA-20KVA (MV) GXT5 VRLA UPS 5KVA-10KVA (HV, I) GXT5 VRLA UPS 16KVA-20KVA (I)	Base firmware must be MCUv180 or greater	Required to be Manufactured in 2021 or later. S/N will start with 21
GXT5 Lithium-Ion UPS 1000-3000VA (LV, I) GXT5 Lithium-Ion UPS 5KVA-10KVA (MV)	Base firmware must be MCUv130 or greater	

11 Reports

Next Connect offers predefined reports designed to help users manage their fleet of monitored devices. Reports can be run on an ad hoc basis by the user and can be found under the

 Reports menu.

These reports include:

- Device Report: Designed for Basic Life Cycle management of monitored devices.
- UPS Fleet Management Summary Report: Designed to pinpoint problems within your UPS fleet.
- UPS Fleet Management Detailed Report: Designed to act as a Detailed overview of your existing fleet.

New reports will be added with upcoming versions of Connect.

Based on their permissions these reports allow the end user to customize the scope of the report based on the following hierarchy:

- Partner
- Customer
- Site
- Group

NOTE: The Device Report, and the UPS Fleet Management Report can be sorted and filtered based on the predefined drop-down lists.

11.1 Device Reports

Device reports are located under the

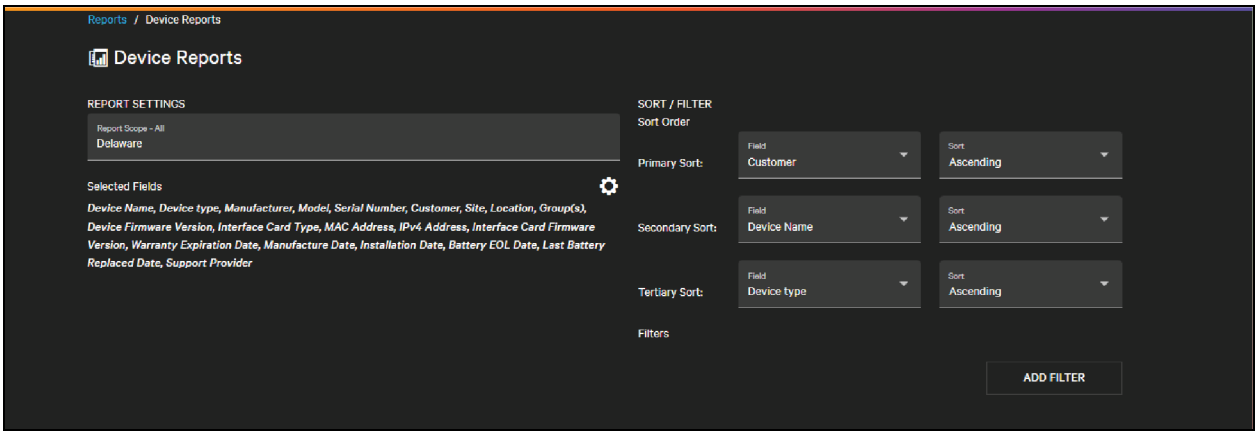
 **Reports** icon

within Connect. Connect supports exporting device lifecycle information on an ad hoc basis. Reports cannot be scheduled. Reports are scoped to device metadata that is either static or changes infrequently (for example, serial number or firmware version). Users with Device Reporting permission are able to generate reports.

The report is generated as a comma separated (.csv) file that can be opened in Excel or a report processor for more detailed analysis and presentation.

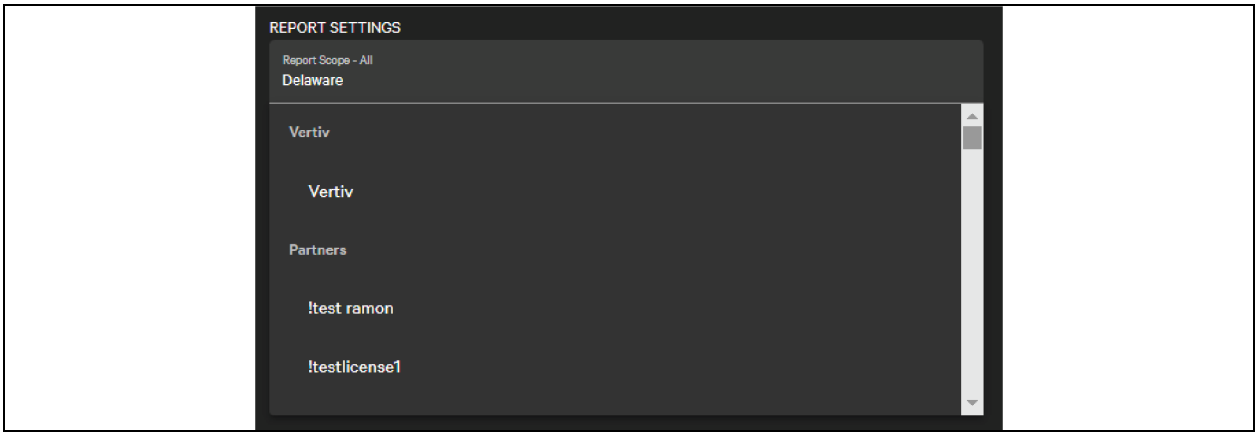
Additional reports will be provided in future releases of Connect.

Figure 11.1 Device Report Screen



To run a device report, select the report scope from the drop down. The can be all customers to which you have a view or the devices or a specific customer. By default, the report gathers data for all devices to which you have visibility.

Figure 11.2 Selecting a Customer to Scope the Device Report



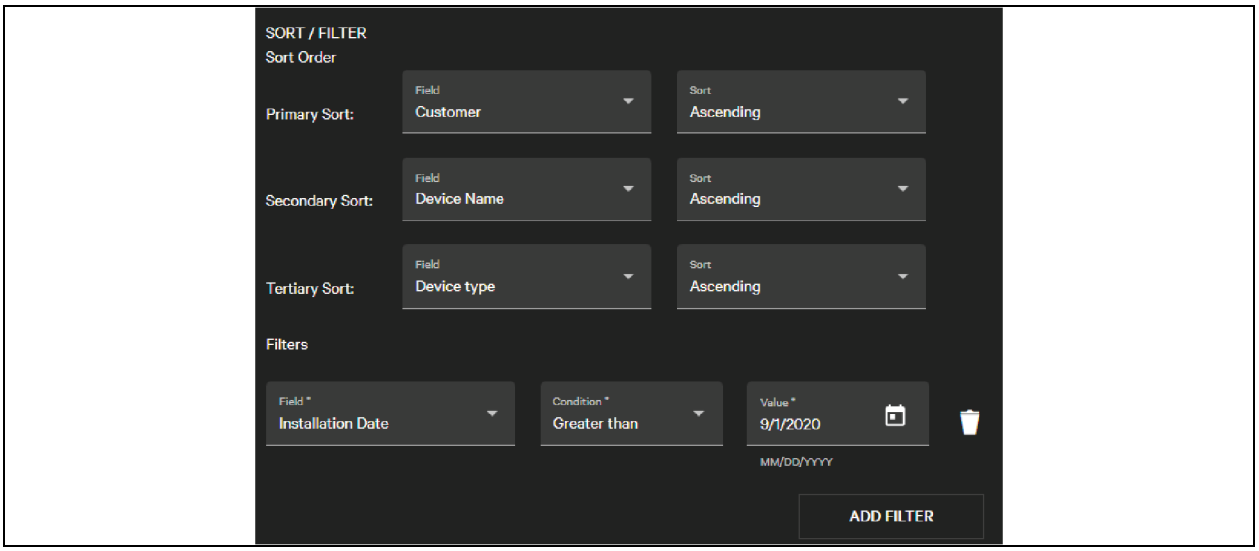
By default, all device fields are selected for the report. The information gathered for the report can be narrowed by clicking the

Gear icon.

This opens a dialog showing all available fields that can be included in the report. Select or deselect fields as needed. Some fields may not contain a value for all devices, such as manually entered values like installation date. Save the fields to include in the report by clicking **Save**. Click **Cancel** to keep the original selected fields.

Options to sort and filter are on the right side of the report screen. The device report supports up to three sorts to allow sorting within categories. Any field can be sorted.

Figure 11.3 Report Sort and Filter



Only the following fields can be filtered:

- Device Type
- Manufacturer
- Model
- Warranty Expiration Date
- Battery EOL Date
- Installation Date
- Support Provider

Additional filters can be added by clicking **Add Filter**. An unlimited number of filters can be added.

To remove a filter, click the

Delete icon next to the filter.

11.2 UPS Fleet Management Summary Report

The UPS Fleet Management Summary Report is designed to help the user proactively detect issues with their UPS Fleet. The report supports both UPS using valve regulated lead acid batteries (VRLA) and lithium ion (Li-Ion) batteries. This report analyzes system data and UPS readings to identify the following critical conditions:

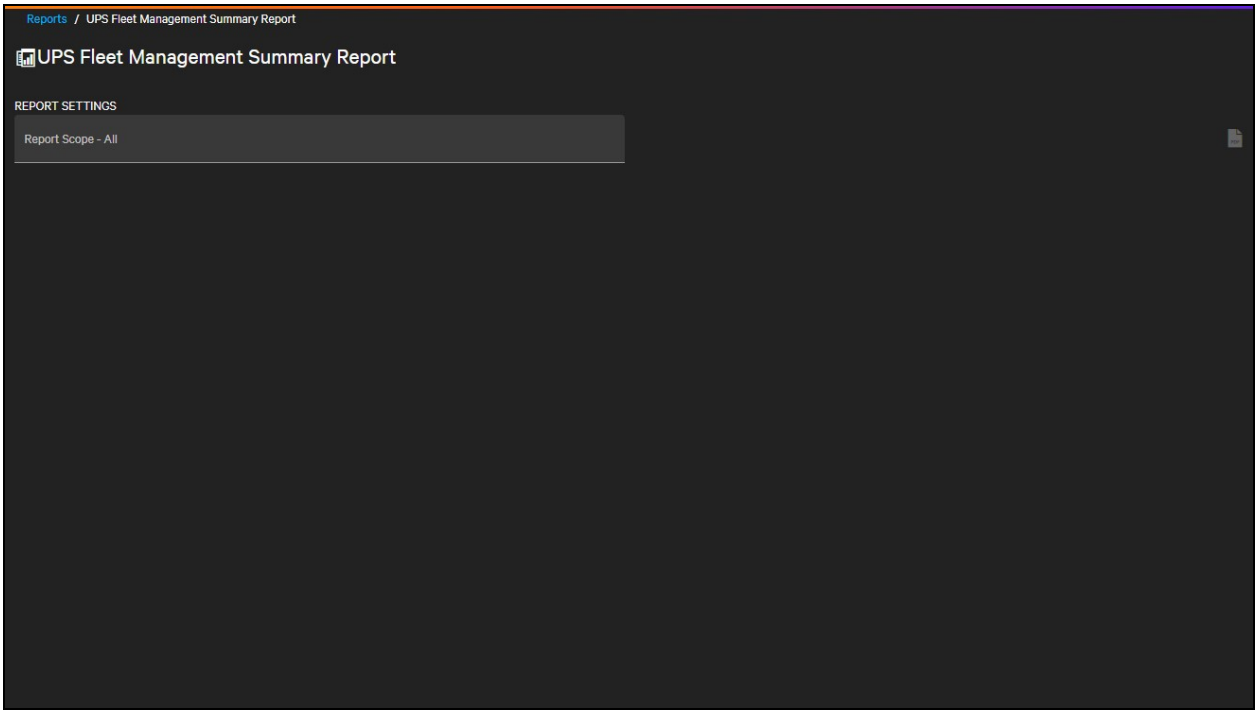
- UPSs where the load is at risk due to the UPS being On Battery or Bypass, or where the last battery self-test failed.
- UPSs with VRLA batteries greater than 3 years old.
- UPSs with Li-Ion Batteries greater than 5 years old.
- UPSs older than 7 years with VRLA batteries.
- UPSs older than 10 years with Li-Ion batteries.
- UPS with VRLA Batteries in high temperature environments greater than 27 °C.
- UPS with Li-Ion Batteries in high temperature environments greater than 50 °C.

- UPS with greater than 80% load.

The UPS Fleet Summary Report is located under the

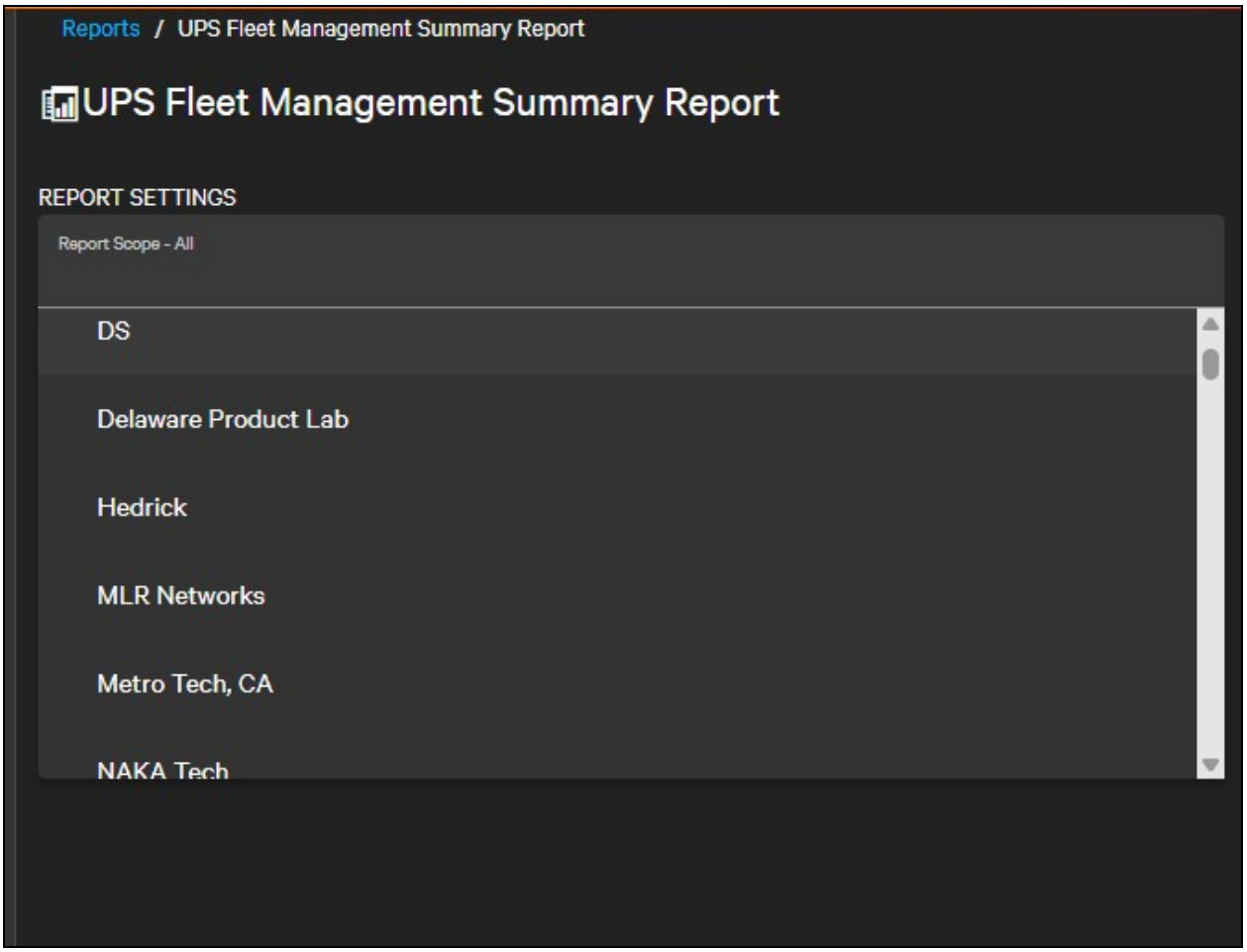
 **Reports** menu.

Figure 11.4 UPS Fleet Management Summary Report Screen



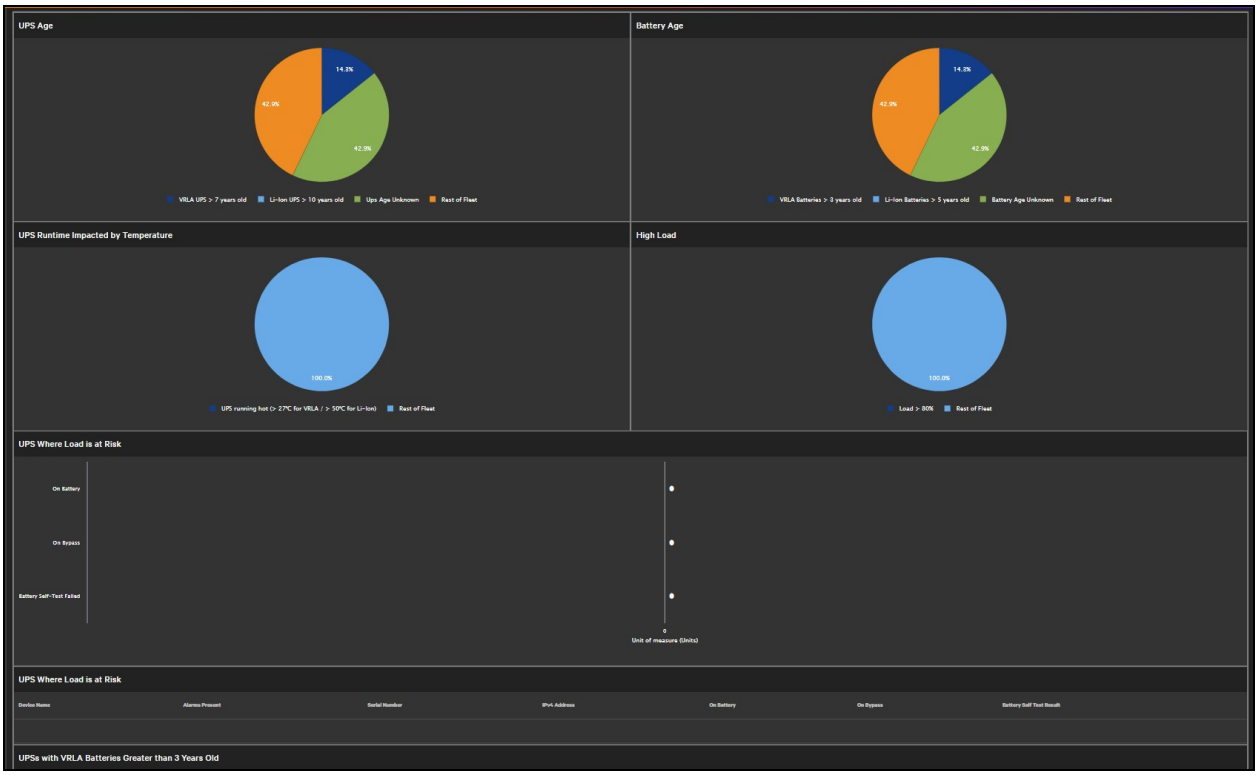
To run this report, you will need to select the scope of the report from the drop-down menu. The default scope is all devices to which you have access, but this can be narrowed down to specific customers, sites, or groups.

Figure 11.5 UPS Fleet Management Report Scope



After selecting the scope, the report will begin gathering data to populate the results in the Web browser.

Figure 11.6 UPS Fleet Management Report



This report can be exported to PDF for distribution or use later. To export the report, click the

Export To PDF icon

in the upper right-hand corner of the report view.

NOTE: This button will be inactive until you select a report scope.

11.3 UPS Detailed Report

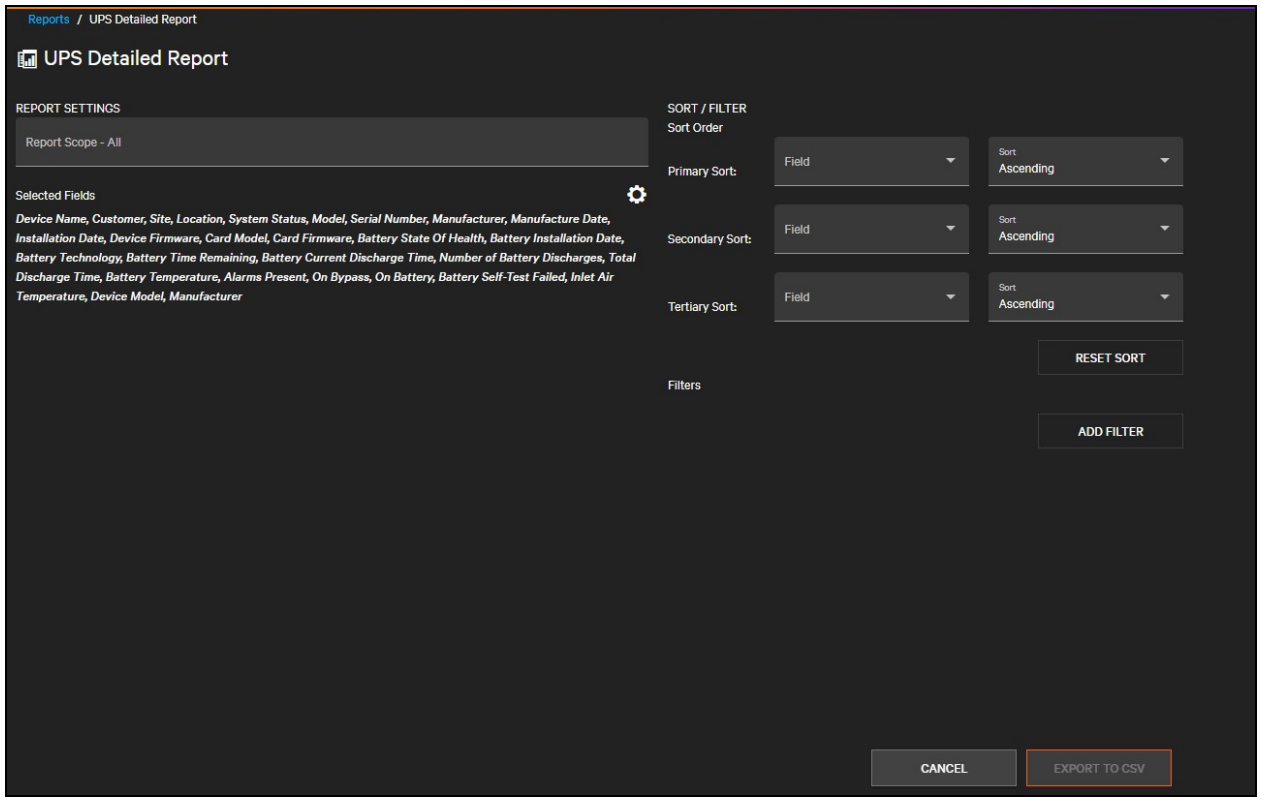
The UPS Detailed Report is designed to give users a clear view of the UPS devices deployed across their environment. It includes key details such as device specifications, network configuration, physical location, firmware versions, and battery lifecycle status. The report supports both VRLA and Lithium-Ion UPS systems and helps users manage their fleet more effectively by providing the information needed for maintenance planning, support coordination, and risk mitigation.

The UPS Detailed Report is generated as a comma separated (.csv) file that can be opened in Excel or a report processor for more detailed analysis and presentation.

The UPS Detailed Report is located under the

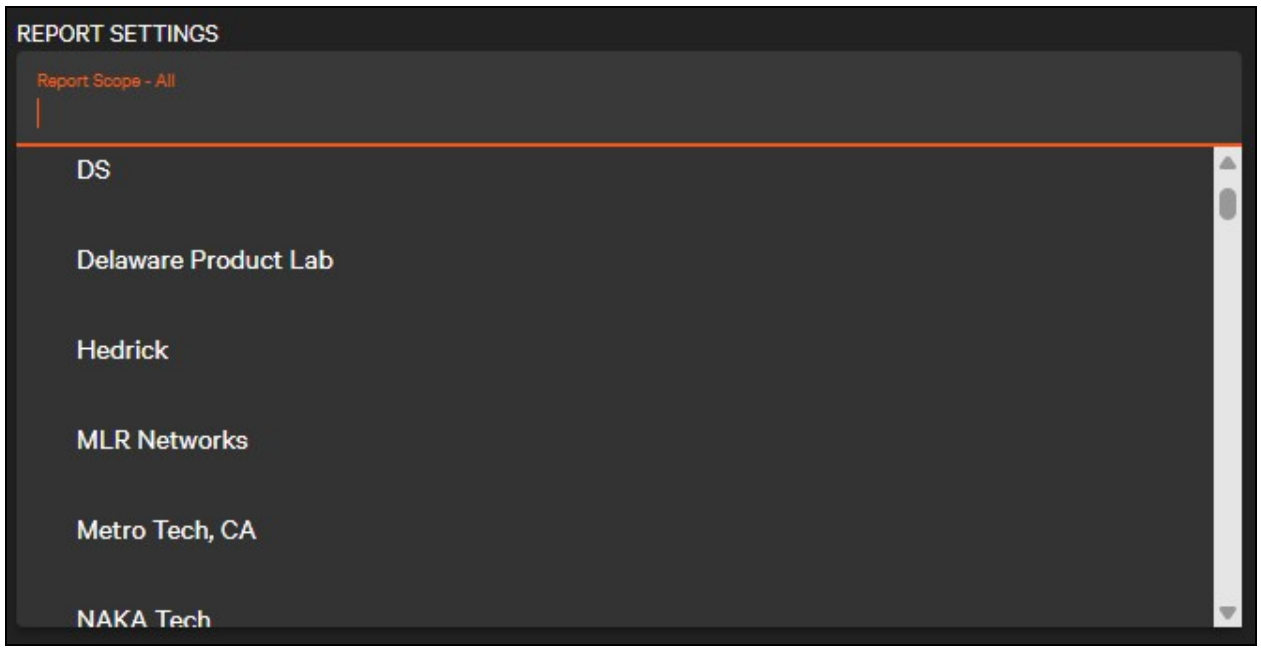

Reports menu.

Figure 11.7 UPS Detailed Report Screen



To run the UPS Detailed Report, select the report scope from the drop-down. The scope will include the customers, sites, or groups to which you have visibility. Every device at or below your chosen scope will be included in the report.

Figure 11.8 Selecting Report Scope



By default, all UPS device fields are selected. The information gathered for the report can be narrowed by clicking the

Settings button.

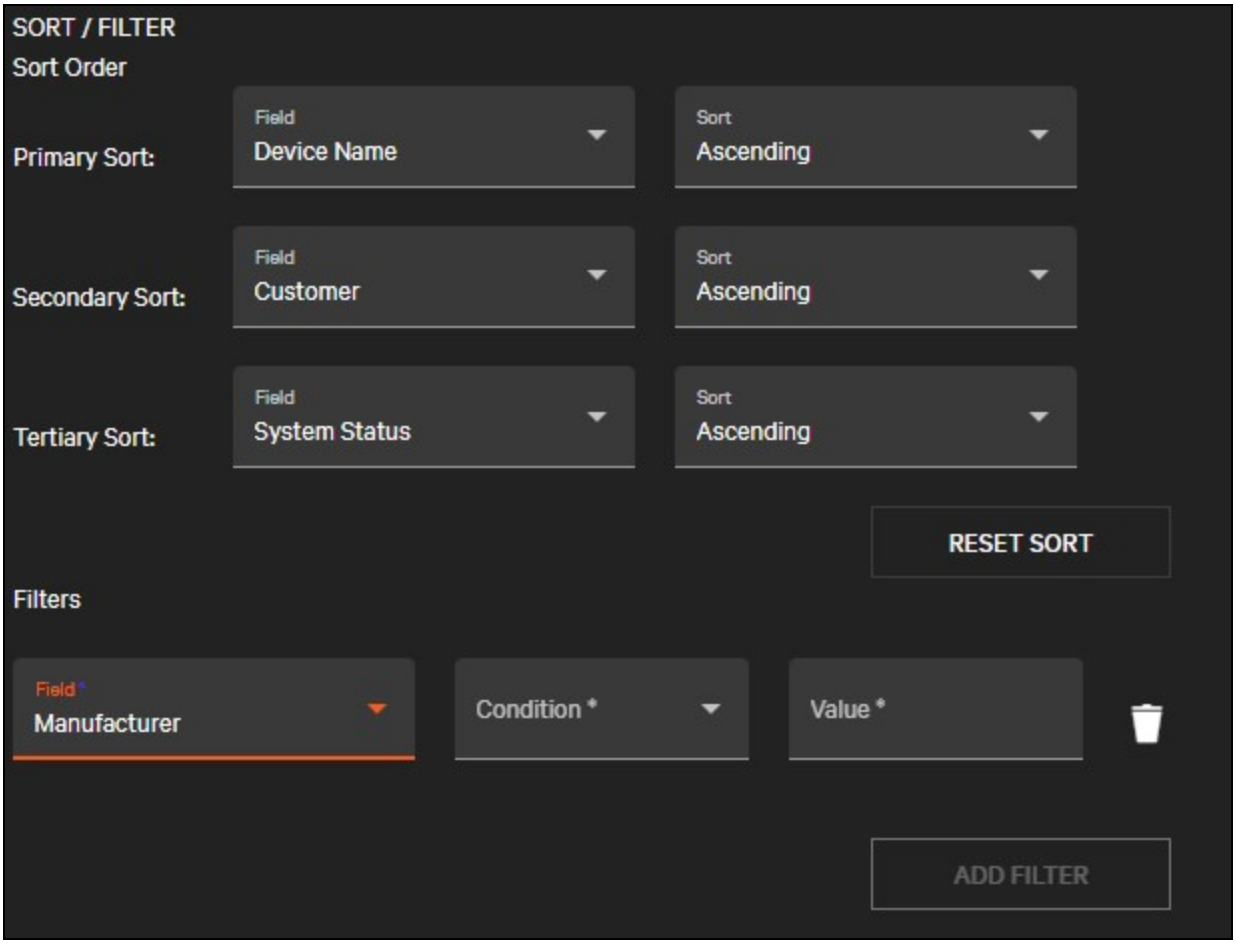
This will open a dialog box displaying all the available fields that can be included in the report and allow you to select or deselect the fields as needed. Some fields may not contain a value for all devices, such as manually entered values or values not supported by the device being monitored.

Save the fields to include in the report by clicking **Save**.

Click **Cancel** to keep the originally selected fields.

User can apply the various filter by using sort/filter options from the right side of the report screen. See **Figure 11.9** below for more information. The UPS Detailed Report supports up to three sorts to allow sorting within categories. Any field can be sorted. Click the Reset Sort to reset the sorts/filter.

Figure 11.9 Report Sort and Filter



Filters can be added for only the following fields:

- Battery Technology
- Device Model
- Card Model
- Manufacturer

- Manufacture Date
- Installation Date
- Battery Installation Date

An unlimited number of filters can be added by clicking Add Filter. To remove a filter, click the

 **Delete** icon next to the filter.

This page intentionally left blank

12 Support

12.1 Documentation and Resources

Documentation for Connect can be downloaded from the product page on Vertiv.com. Within Connect you can access the following documents and resources. These documents are accessible within Connect from the **Support** menu.

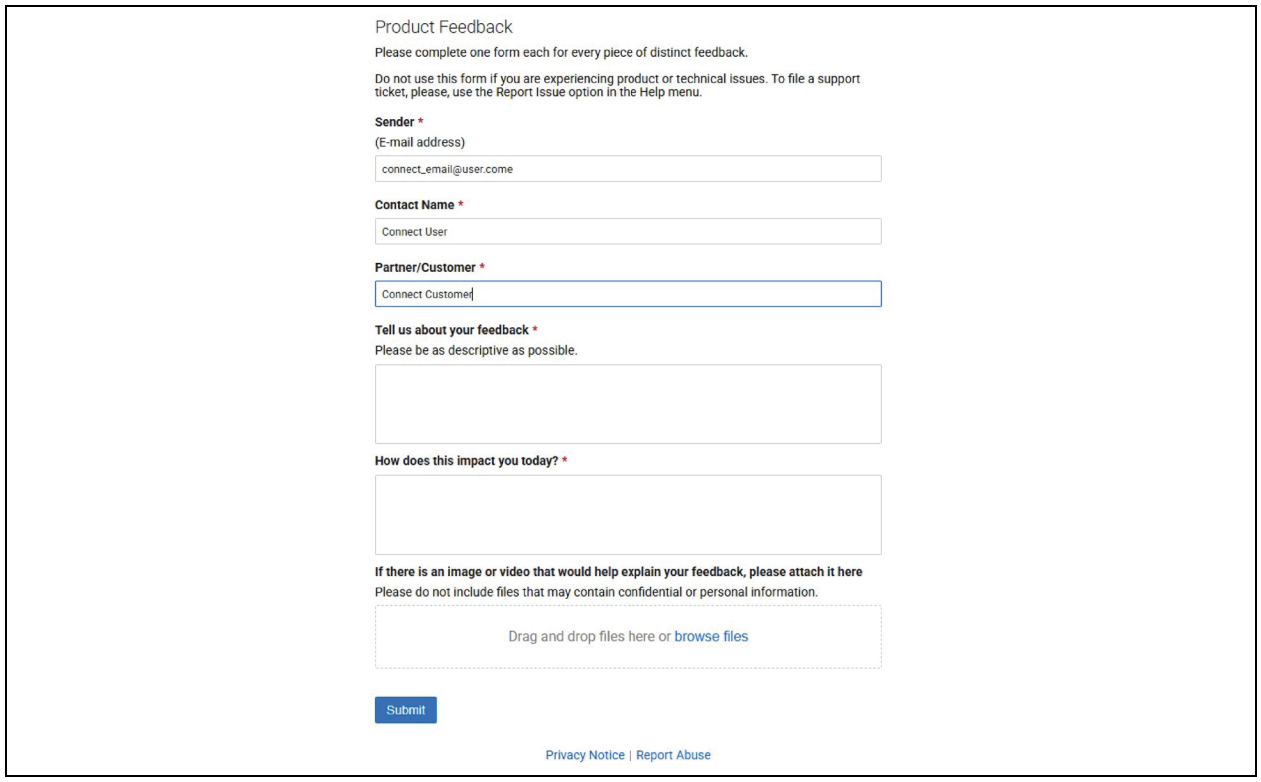
- Get Started — Quick start guide which walks the user through registering with Connect and initial setup steps.
- User Guide — This document.
- Training Videos — Instructional videos that walk the user through the most common features used in the Connect Platform.
- Release Notes — Details about the latest updates and patches to Connect.
- Report an Issue — Allows users to submit support tickets from within the platform.
- Feedback/Suggestions — Allows users to provide Feedback on Enhancements or suggestions to improve the platform.
- Request a new template — Allows users to request new device support from Vertiv. Users will need to provide documentation regarding the requested device.
- EULA — End User License Agreement.

12.2 Sending Feedback

Connect provides a direct feedback mechanism for questions or for issues you encounter while using the product.

From the Support menu or Help menu click **Feedback** to open a new tab with our feedback form.

Figure 12.1 Feedback Form



The feedback form records your Connect email and organization so the support team can respond to your issue. You can modify these as necessary.

Select the category of issue (Application – General, Device, Local Agent, Communication) to classify the problem you are having.

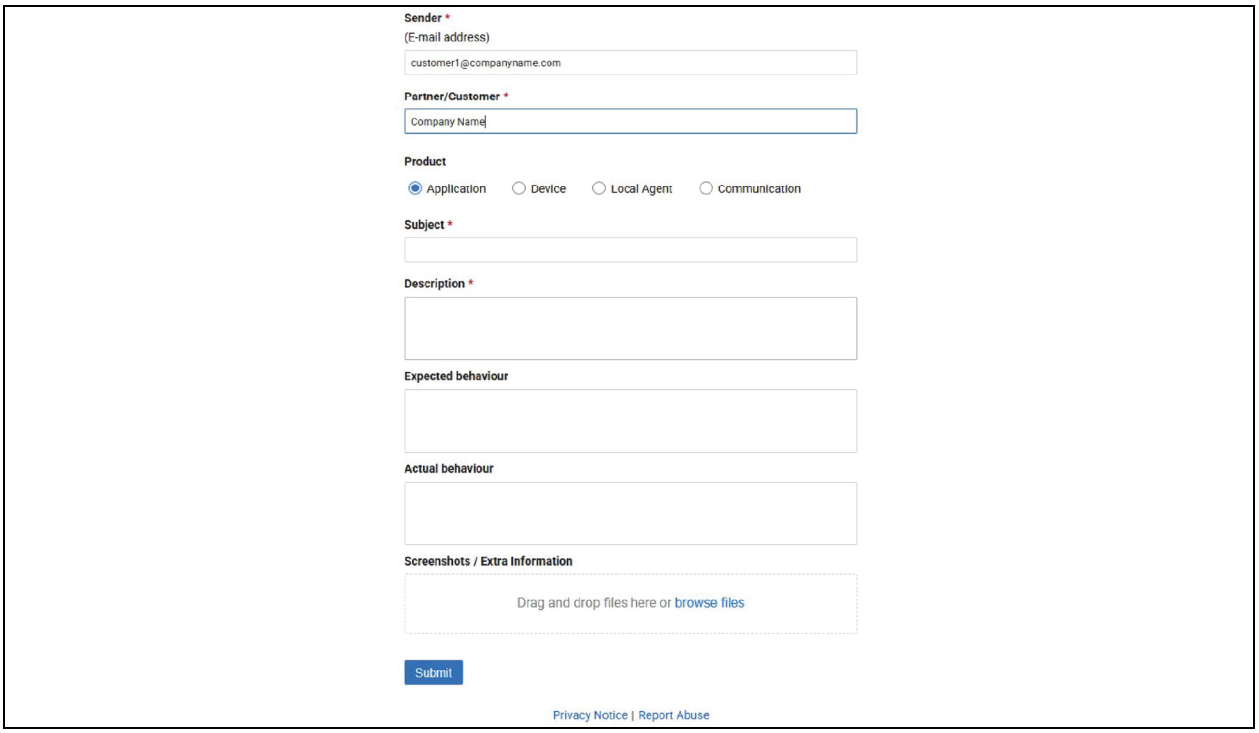
Enter a subject with a high-level description, then a more detailed description below. If Connect behaves in a way you do not expect, you can record your expected and actual behavior (though this is not required). You can also upload any screenshots or additional information for context.

When you have completed the form, click **Submit** and our operations team will triage and respond to the issue. As always you can also contact the direct support line or any contacts from whom you purchased Connect.

12.3 Report an Issue

When a user encounters an issue, they can request support from within Connect. To access the support form, click Report an Issue from either the Support or Help menus.

Figure 12.2 Report an Issue



To complete this form (see Figure 12.2 above), do the following:

1. First you need an email address and organization name for the support team to respond to the issue. These should be auto populated by Connect, but you can modify as necessary.
2. Select the category of issue (Application – Application, Device, Local Agent, Communication) to classify the problem.
3. Enter a subject with a high-level description, then a more detailed description below. If Connect behaves in a way you do not expect, you can record your expected and actual behavior (though this is not required). You can also upload any screenshots or additional information for context.
4. When you have completed the form, click Submit and our operations team will triage and respond to the issue.

As always you can also contact the direct support line or any contacts from whom you purchased Connect.

12.4 Training Videos

Next Connect includes built-in access to end user training videos. These videos are designed to guide users through key features and configuration steps, to help them use the platform more effectively. Training videos can be accessed on the Support menu under Training Videos. Topics discussed in the training videos include:

- Provisioning a Device
- Managing Users
- Managing Dashboards
- Installing the Agent
- Getting Help
- Discovering a device

- Deleting a User
- Creating a report
- Creating an Account
- Bulk updates
- Adding a User

Figure 12.3 Training Videos

NOTE: The list of topics will be expanded as new features become available.

12.5 Request a New Template

While Vertiv maintains a library of supported devices, users may encounter a device that is not currently supported in Connect. Connect allows end users to request new device support for any SNMP compatible device from within the product interface.

When requesting new device support, users should be prepared to submit at minimum:

- All Device MIB files
- An SNMP walk of the device
- Device documentation

The Request a new template form can be found under either the Support or Help menu. This form will automatically populate the name of the Connect user that is Requesting the template, the user's email, and the organization's name. This information will be used by Vertiv to contact the user should any additional information be required. These fields can be modified as needed.

To submit the request, users must complete all required fields on the form.

Appendices

Appendix A: Technical Support and Contacts

A.1 Technical Support/Service in the United States

Vertiv Group Corporation

24x7 dispatch of technicians for all products.

1-800-543-2378

Liebert® Thermal Management Products

1-800-543-2378

Liebert® Channel Products

1-800-222-5877

Liebert® AC and DC Power Products

1-800-543-2378

A.2 Locations

Vertiv Americas Headquarters

505 N Cleveland Ave

Westerville, OH 43082

Vertiv EMEA Headquarters

Victor-von-Bruns Strasse 21,

8212 Neuhausen am Rheinfall, Switzerland

Vertiv Asia Headquarters

Singapore

151 Lorong Chuan, Lobby D #05-04

New Tech Park, Singapore 556741

India

Vertiv Energy Private Limited

Plot No. C 20, Road No. 19

Wagle Industrial Estate, MIDC

Thane (West), Maharashtra 400604, India

China

Vertiv Technology Co., Limited

Floors 1–4 and 6–10,

Building B2, Nanshan I Park

No. 1001 Xueyuan Road, Nanshan District

Shenzhen, Guangdong 518055, China

Connect with Vertiv on Social Media

 https://www.facebook.com/vertiv/

 https://www.instagram.com/vertiv/

 https://www.linkedin.com/company/vertiv/

 https://www.x.com/Vertiv/

Vertiv.com | Vertiv Headquarters, 505 N Cleveland Ave, Westerville, OH 43082 USA

SL-71242_REVC_04-26