GE VERNOVA

GE LaunchNET

User Guide

Version 6.0

Table of Contents

Overview

GE LaunchNET is a graphical front-end program that offers provisioning of device configuration at the beginning of a device’s life cycle. It consists of two components:

GE LaunchNET: The web application, which allows for the creation/staging of device templates, management of device inventory, and GE PulseNET Integration.

Radio Admin: This client acts as the conduit between the application and the device being configured.

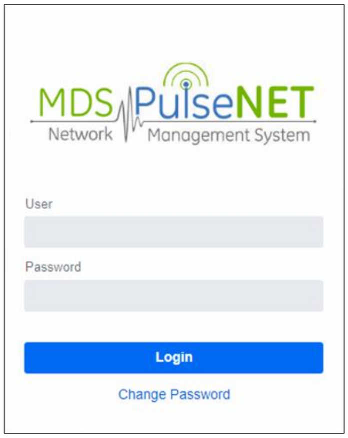
LaunchNET Roles

LaunchNET uses the underlying User/Role system of GE PulseNET, which contains two default roles, by default Administrators have access to all views and groups, Operators have no access to views or groups.

Administrative LaunchNET users are granted API access by default. If additional users require API access, they must be assigned the 'Device Administrator' role within their user group by an Administrator. This can be accomplished via Access Control. Please see the section ‘Adding an Access Control Record’ in this guide for more information.

Login

Before the login menu will display, the GE PulseNET services must be running.



To log in to GE PulseNET using a Web browser:

1. Open a Web browser.
2. Navigate to the URL with the following syntax:

```
http[s]://<hostname>:<port>/
```

Where *<hostname>* is the name of the machine that has a running instance of GE PulseNET and *<port>* is the HTTP or HTTPS port specified during installation (the defaults are 8080 and 8443).

3. On the login screen that appears, enter the **Username** and **Password**.
4. Click **Login**.

Operator users are automatically taken to the Summary dashboard because access to other menus must be granted by an Admin first.

The appearance of GE PulseNET and the variety of accessible dashboards will vary depending on the role and permissions assigned. Administrators can access advanced dashboards and configuration workflows, while Operators have access to a restricted set of dashboards, based on the permissions they have been granted.

Admin Overview

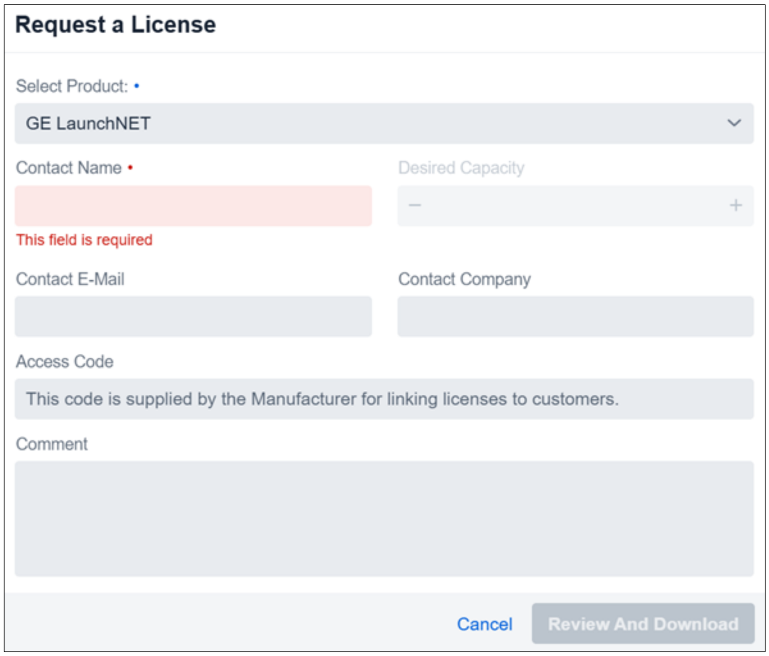
The following section relates to tasks exclusive to Administrator users. Multiple Administrator users can be created, and any Administrator can create additional administrators and operators. The Administrator configures the integration of the system with other systems such as external databases and Microsoft CA servers and is responsible for creating and staging the templates that Operators will employ to configure the devices.

Licensing

LaunchNET is integrated with GE PulseNET Enterprise and will require a separate license before the LaunchNET menu will appear on the Administration page.

One of the first administrative tasks is to request and install a valid

GE LaunchNET license. Once in place, a second **LaunchNET Devices** license must be requested which will provide GE LaunchNET with the capacity to stage devices for provisioning. Follow the PulseNET licensing instructions below to generate a GE LaunchNET request, then a subsequent LaunchNET Device request.



Request a License

Select Product: • GE LaunchNET

This field is required

Access Code: This code is supplied by the Manufacturer for linking licenses to customers.

To request a license:

1. Navigate to **Administration > Licensing > Request a License**. A dialog box will appear.
2. Select required product from the dropdown list of **Available Products.**
3. In the **Contact Name** field, type the name of the person at the company who will be the contact.
4. In the **Company E-Mail** field, type the email address of the primary contact.
5. In the **Access Code** field, type the access code obtained from the GE Sales team.
6. In the **Desired Capacity** field, type the total number of licenses required. **Note:** LaunchNET is an activation license and does not require a quantity. However, subsequent

LaunchNET Device license will require a quantity value.

7. In the **Comment** field, enter any comments which would help the Licensing team fulfill the license request.
8. Click **Save Request to a File** to create a licenseRequest.txt file.

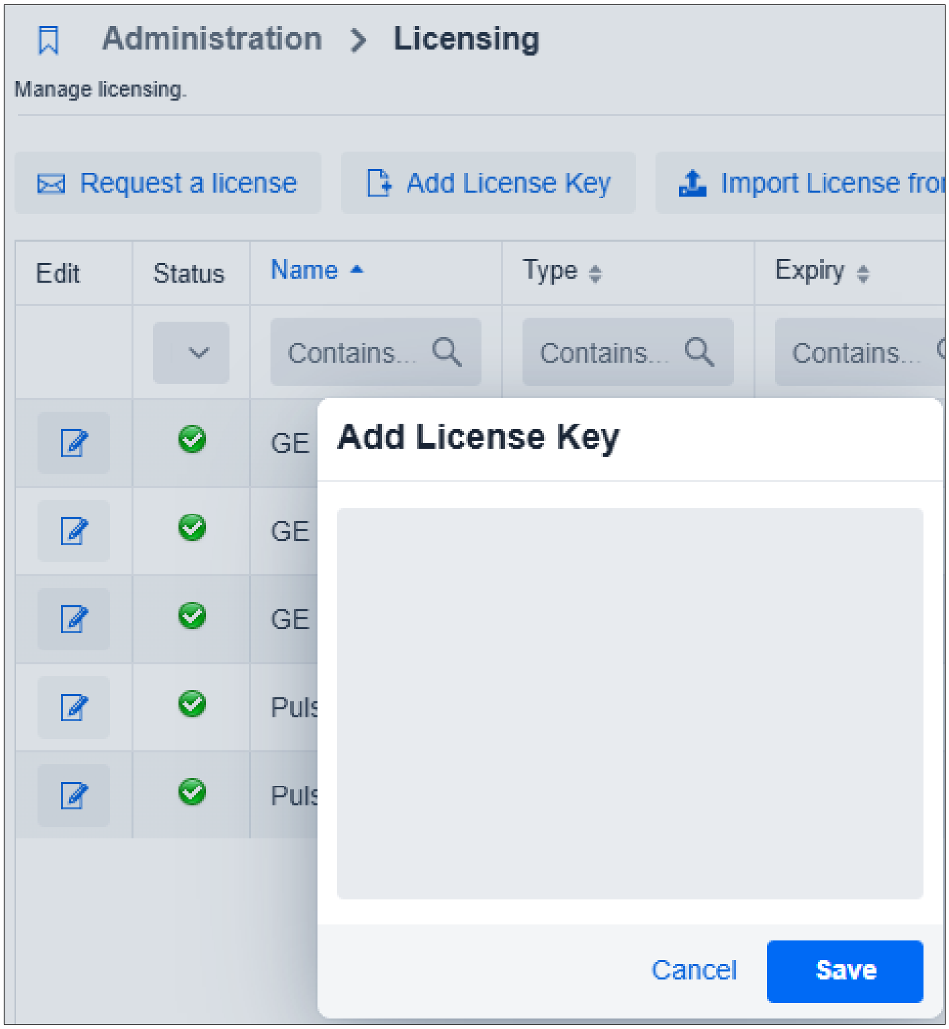
This must be sent directly to the GE Licensing Team at: gemds.pulsenet@ge.com

When the request is approved, the new license will be sent via email by GE.

Adding Licenses

After receiving the new licenses, they must be added to the LaunchNET instance.

1. From **Administration > Licensing**, click Add License Key and directly paste the received license key into the provided field and click Save.

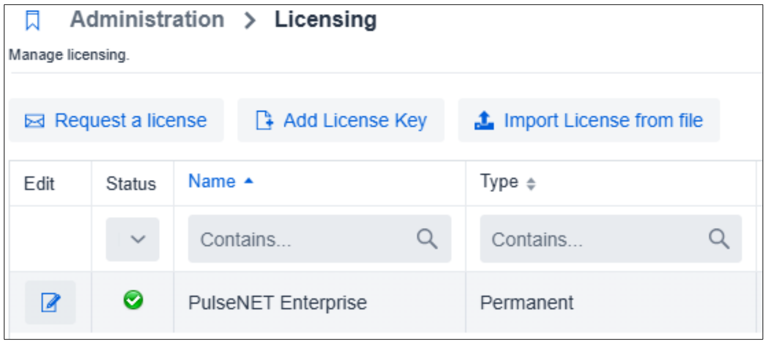


2. Or click **Import License from File** to locate the license file on the computer (the .txt file must be on the machine where the browser is running.) Then click Import.

If the license is valid, it is added to GE LaunchNET. Otherwise, a message will appear stating that the license key is invalid. Contact the GE Licensing team if this occurs.

Managing Licenses

Installed licenses appear under **Administration > Licensing**. This menu allows deletion of expired licenses, migrating devices to new licenses, or requesting replacement licenses.



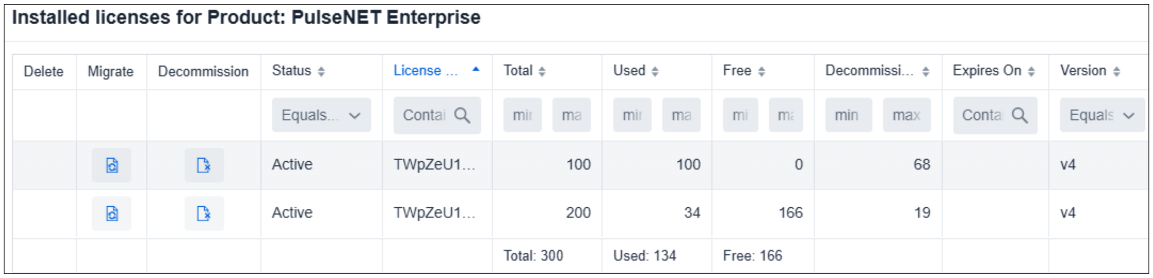
Administration > Licensing

Manage licensing.

Edit	Status	Name ▲	Type ⇕
	⌄	Contains...	Contains...
✎	✓	PulseNET Enterprise	Permanent

Click the Edit icon on any license row to view the details for a specific license. Here the Hardware ID that identifies the server to GE PulseNET is displayed. Click the checkbox on a row to select it. Selected rows may be deleted from the system. Click on the **License Key** field to view the GE PulseNET license key associated with this license.

The **Used** column provides the option to migrate devices that have been associated with this license. Click the **Migrate** link to view the list of devices and select them for migration. Once selected, choose another GE PulseNET license to which the selected devices should be migrated.



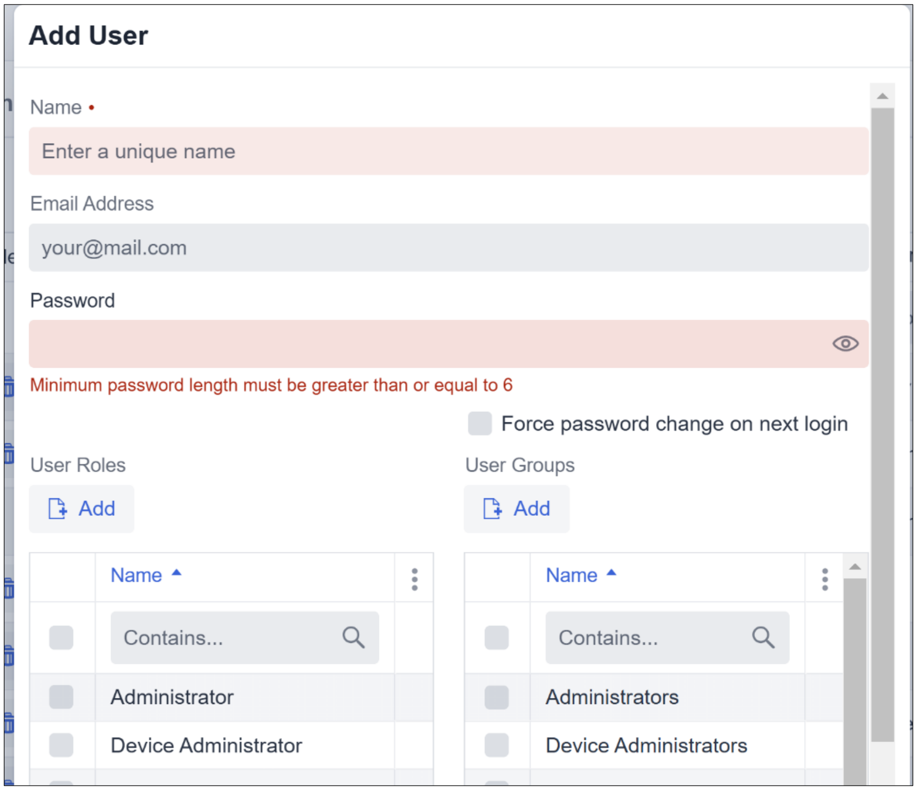
Installed licenses for Product: PulseNET Enterprise

Delete	Migrate	Decommission	Status ⇕	License ... ▲	Total ⇕	Used ⇕	Free ⇕	Decommissi... ⇕	Expires On ⇕	Version ⇕
			Equals... ⌄	Contai	mi ma	mi ma	mi mi	min max	Conta	Equals ⌄
			Active	TWpZeU1...	100	100	0	68		v4
			Active	TWpZeU1...	200	34	166	19		v4
					Total: 300	Used: 134	Free: 166			

Working with Users

GE PulseNET controls user access to the web interface using the concept of users, groups, and roles. When administrators create new users, a role and/or group can be assigned to the user. The assigned role/group determines the features and views that users can access when they log in to GE PulseNET.

Creating Users



Add User

Name •

Enter a unique name

Email Address

your@mail.com

Password

Minimum password length must be greater than or equal to 6

□ Force password change on next login

User Roles	User Groups
Add	Add

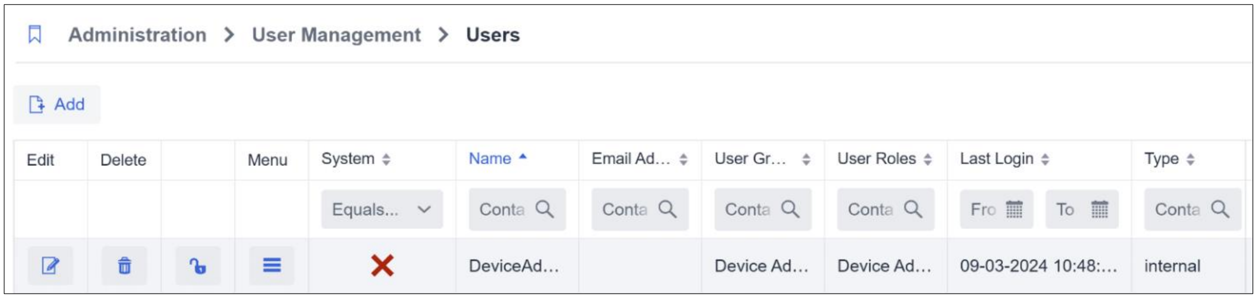
□	Name ▲
□	Contains...
□	Administrator
□	Device Administrator

□	Name ▲
□	Contains...
□	Administrators
□	Device Administrators

1. Navigate to **Administration** > **User Management** > **Users**
2. Click the **Add** button
3. Enter a unique name for the new user
4. Enter the user’s email address (if desired)
5. Enter a GE PulseNET password for this user, then confirm the password on the next line
6. Assign the new user one or more roles. Administrators also have access to all operator functionalities.
7. Optionally assign the new user to one or more user groups
8. Click **Save**.

   The new user now appears in the users table.

Managing Users



Administration > User Management > Users

Add

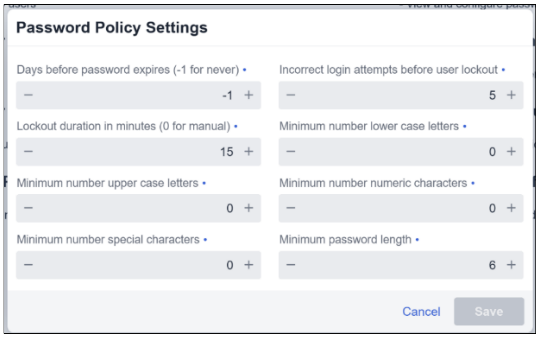
Edit	Delete		Menu	System	Name	Email Ad...	User Gr...	User Roles	Last Login	Type
				Equals...	Conta	Conta	Conta	Conta	Fro To	Conta
				✗	DeviceAd...		Device Ad...	Device Ad...	09-03-2024 10:48:...	internal

All users are listed in the **Users** table. Each contains options to lock the account, edit the settings, or delete the user.

- Click the **Lock** icon to lock or unlock a user account
- Click the **Copy** icon to make a duplicate of an existing user account
- Click the **Edit** icon to change account details (name, role, password)
- Click the **Delete** icon to remove an account from GE PulseNET
- Click the **Audit Logs** icon to view the GE PulseNET activity by this user

Configuring Password Policy

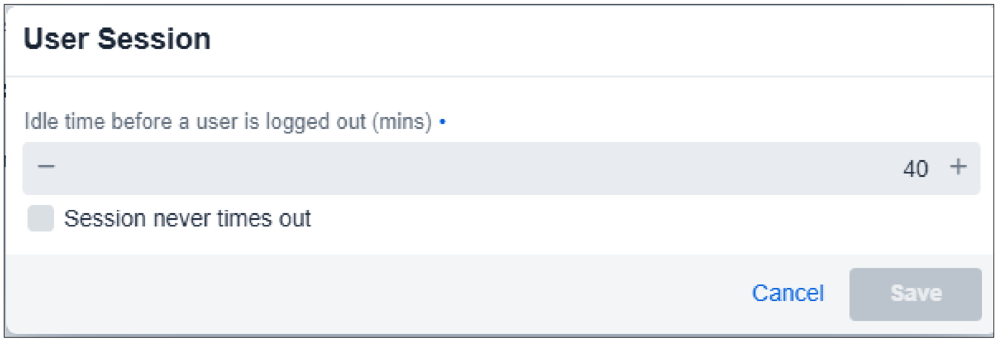
An Administrator can configure the global default password policy for user accounts.



Password Policy Settings

Days before password expires (-1 for never) •	-1
Incorrect login attempts before user lockout •	5
Lockout duration in minutes (0 for manual) •	15
Minimum number lower case letters •	0
Minimum number upper case letters •	0
Minimum number numeric characters •	0
Minimum number special characters •	0
Minimum password length •	6

Setting User Session Timeout



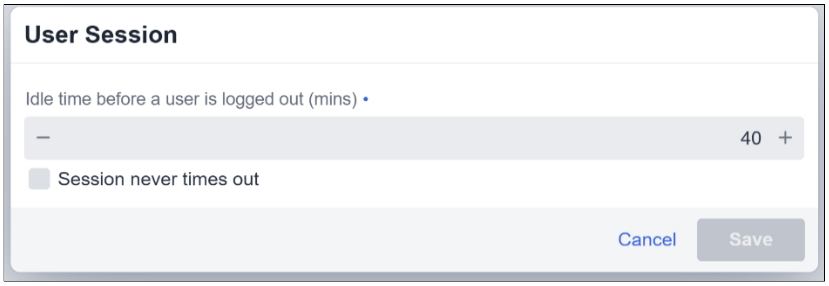
User Session

Idle time before a user is logged out (mins) •

− 40 +

□ Session never times out

An Administrator can set the user session timeout in minutes. Or check the box which disables session timeout.



User Session

Idle time before a user is logged out (mins) •

− 40 +

□ Session never times out

Configuring LDAP - Enterprise Only

Instead of duplicating the existing Lightweight Directory Access Protocol (LDAP) or Active Directory users in GE PulseNET, it can be configured to authenticate directly to the LDAP or Active Directory server. GE PulseNET supports LDAP version 3 compatible directory services, including Active Directory, Sun Java Systems Directory Server, and OpenLDAP.

Familiarity with the details of the LDAP Directory Service, and related parameters is required to configure the feature in GE PulseNET. The following considerations are important when planning to integrate an external directory service with the GE PulseNET:

- Secure LDAP is supported, but not required

- LDAP with Transport Layer Security is not supported
- A persistent connection to the LDAP server is not required

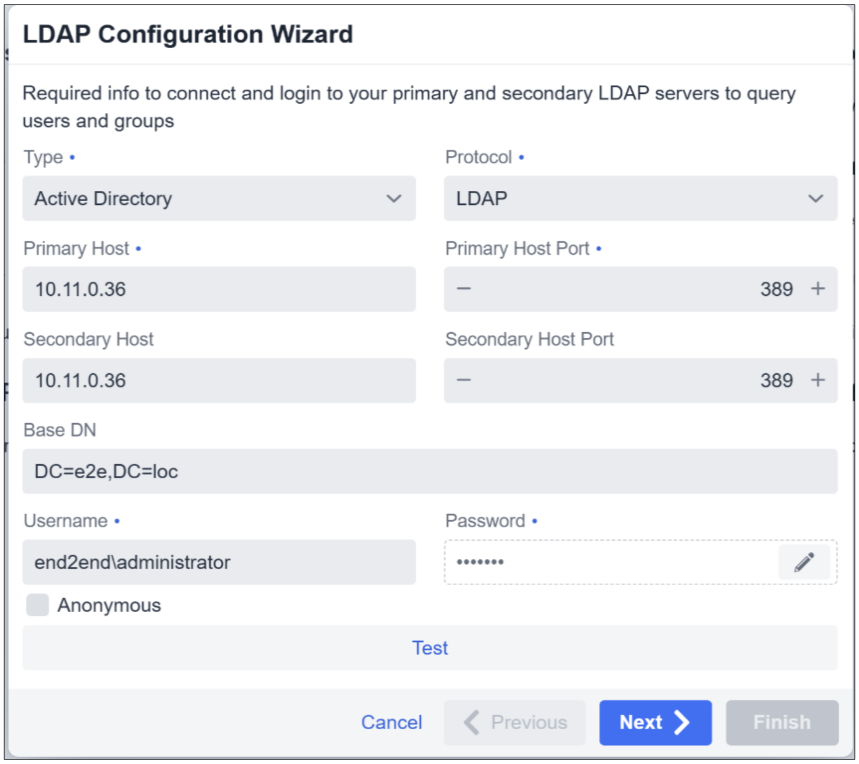
LDAP groups can be imported into GE PulseNET and assigned GE PulseNET roles. This allows users who have been granted special permissions within an organization to have associated permissions in GE PulseNET.

User credentials continue to be managed on the LDAP server. Any password changes in the LDAP directory service are transparent to GE PulseNET. After a password change in the directory service, that user can log into GE PulseNET with the new password, while any attempts to use the old password will fail. If a user account is removed from the directory service, any login requests with those credentials result in a login failure in GE PulseNET.

Similarly, if the LDAP authentication service is down, GE PulseNET cannot authenticate users whose accounts are defined there. At the same time, any internal GE PulseNET users, such as the built-in *admin* user or any accounts created manually using the **Manage Users** dashboard, are unaffected during LDAP authentication service interruptions.

Configure LDAP Server Information

The first window in the **LDAP Configuration Wizard** allows configuration of connectivity and login with the LDAP server.



LDAP Configuration Wizard

Required info to connect and login to your primary and secondary LDAP servers to query users and groups

Type •	Protocol •
Active Directory	LDAP
Primary Host •	Primary Host Port •
10.11.0.36	389
Secondary Host	Secondary Host Port
10.11.0.36	389
Base DN	
DC=e2e,DC=loc	
Username •	Password •
end2end\administrator	•••••••

□ Anonymous

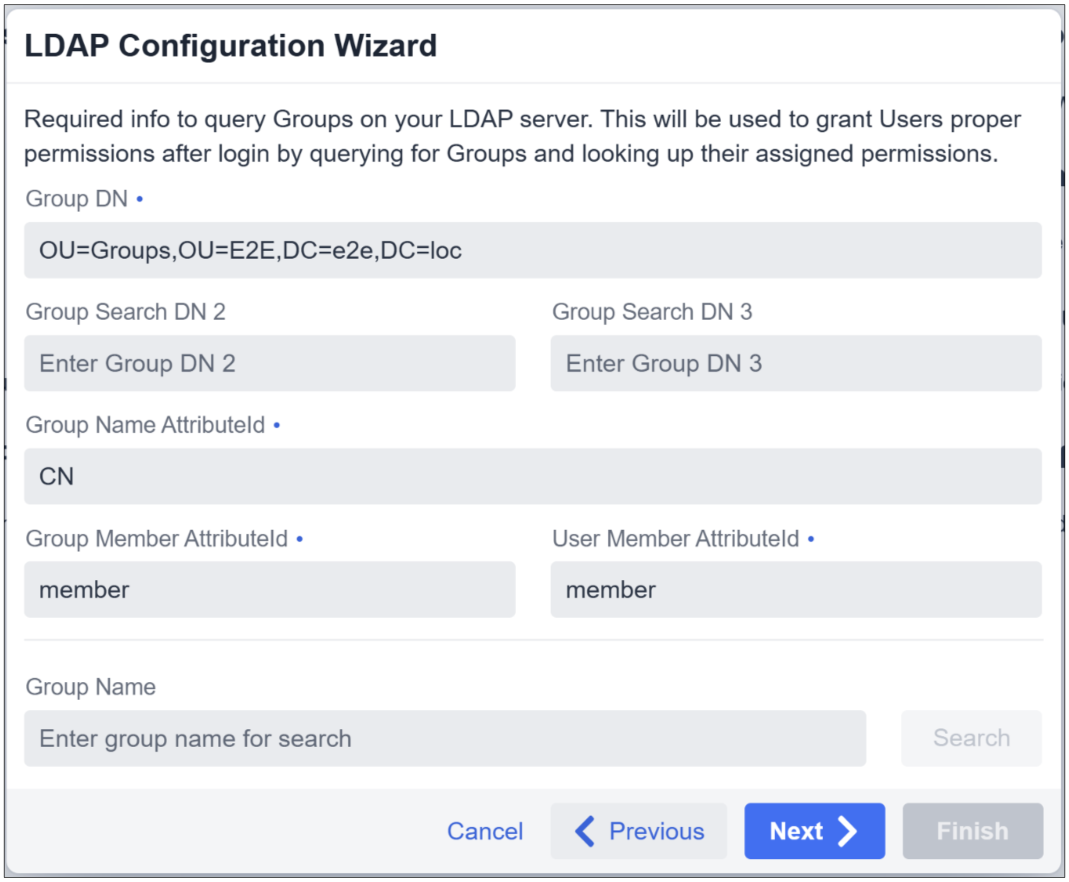
1. In the **LDAP Configuration Wizard** window, select the Type of LDAP server, either Active directory or other.
2. In the **Primary Host** field, select LDAP or LDAP over SSL.
3. In the **Primary Host Port** field, the default port will appear.
4. If using a failover server, enter the details in the **Secondary Host and Secondary Host Port** fields.
5. In the **Base DN** field, enter the distinguished name (DN) of the service account to fetch users and groups. In Active Directory, typically a common name (CN) is used instead of DN. For example: CN=John Smith, OU=Employees, DC=company, DC=com.
6. If the **Anonymous** checkbox is enabled, GE PulseNET will use an anonymous service account to search for users in the extended directory. The default username for anonymous service accounts is _anonymous_ and enabling this option sets the Distinguished Name of the service account to _anonymous_.
7. In the **Username** and **Password** fields, enter the username and password of the

service account used for user searching in the external directory.

8. Click the **Test** button to test the system connection and login credentials for the LDAP server. If the Test is successful, proceed to the next step.
9. Click the **Next >** button.

Find LDAP User Groups

Once configured, the second window in the **LDAP Configuration Wizard** will grant Users proper permissions after login by querying for Groups and looking for their assigned permissions.



LDAP Configuration Wizard

Required info to query Groups on your LDAP server. This will be used to grant Users proper permissions after login by querying for Groups and looking up their assigned permissions.

Group DN •: OU=Groups,OU=E2E,DC=e2e,DC=loc

Group Search DN 2: Enter Group DN 2

Group Search DN 3: Enter Group DN 3

Group Name AttributeId •: CN

Group Member AttributeId •: member

User Member AttributeId •: member

Group Name: Enter group name for search

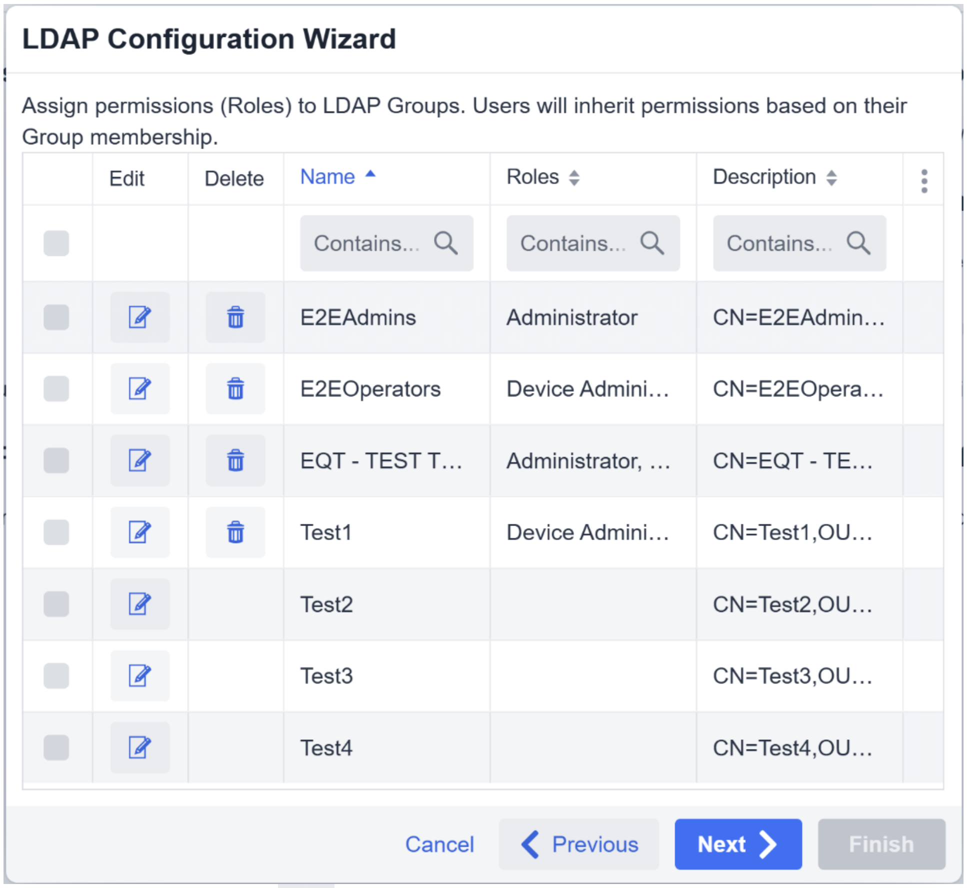
1. In the **Group DN** field, enter the search path for groups identified in the LDAP server. For example: OU=Groups,DC=2k3,DC=dom. The order in which the groups are searched is determined by the order of the groups listed in these settings. The **Group Search DN 2** and **3** fields are optional.

2. In the **Group Name Attribute-ID** field, enter the Attribute-ID for finding Groups in the external directory. The default for Active Directory is “CN.”
3. In the **Group Member Attribute-ID** field, enter the Attribute-ID for finding Group Members in the external directory. The default for Active Directory is “member.”

   In the **User Member Attribute-ID** field, enter the Attribute-ID for finding Users in the external directory. The default for Active Directory is “member.”
4. To ensure the paths are correct for finding Groups, in the **Group Name** field, enter the name of a Group to search. Click the **Search** button. If the search is successful, the **Test Search for Group** dialog box will indicate “Group found!” and list the Group Members including the Users and any Subgroups.

Assign Permissions (Roles) to LDAP Groups

The third window in the **LDAP Configuration Wizard** allows for assigning permissions (roles) to LDAP Groups.

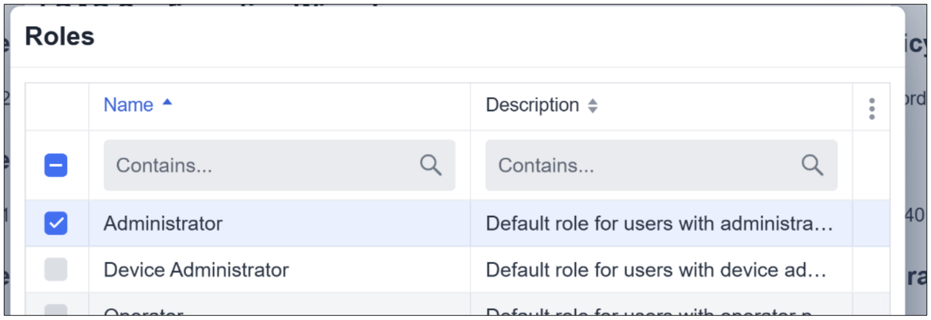


LDAP Configuration Wizard

Assign permissions (Roles) to LDAP Groups. Users will inherit permissions based on their Group membership.

	Edit	Delete	Name ▲	Roles ⇕	Description ⇕
☐			Contains...	Contains...	Contains...
☐	✎	🗑	E2EAdmins	Administrator	CN=E2EAdmin…
☐	✎	🗑	E2EOperators	Device Admini…	CN=E2EOpera…
☐	✎	🗑	EQT - TEST T…	Administrator, …	CN=EQT - TE…
☐	✎	🗑	Test1	Device Admini…	CN=Test1,OU…
☐	✎		Test2		CN=Test2,OU…
☐	✎		Test3		CN=Test3,OU…
☐	✎		Test4		CN=Test4,OU…

1. Select the edit icon ✎ of the LDAP Group to which roles will be assigned.

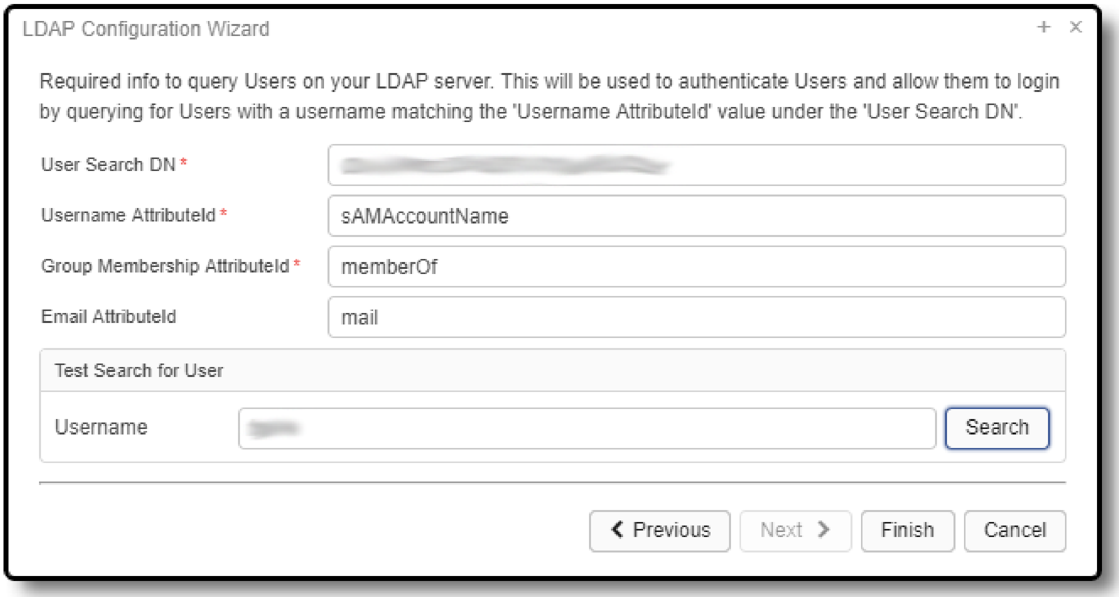


Roles

	Name ▲	Description ⇕
⊟	Contains...	Contains...
☑	Administrator	Default role for users with administra…
☐	Device Administrator	Default role for users with device ad…
☐	Operator	Default role for users with operator p…

Finding LDAP Users

The fourth window in the **LDAP Configuration Wizard** provides a means to search for and test the connection of LDAP Users.



LDAP Configuration Wizard

Required info to query Users on your LDAP server. This will be used to authenticate Users and allow them to login by querying for Users with a username matching the 'Username AttributeId' value under the 'User Search DN'.

User Search DN * [redacted]

Username AttributeId * sAMAccountName

Group Membership AttributeId * memberOf

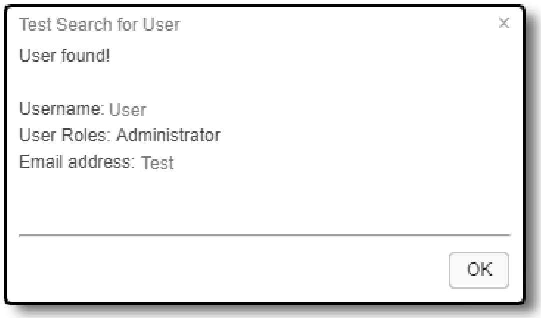
Email AttributeId mail

Test Search for User

Username [redacted]

1. In the **User Search DN** field, enter the search path for users identified in the LDAP server. For example, in Active Directory, if the CN user accounts are defined in the sAMAccount=Users group, and the Active Directory domain is example.com, apply the following: CN=Users,DC=example,DC=com
2. In the **Username Attribute-ID** field, enter the Attribute-ID which contains the Username. For example, in Active Directory, the default is sAMAccountName.
3. In the **Group Membership Attribute-ID** field, enter the Attribute-ID which includes the Group Membership. For example, in Active Directory, the default is memberOf.
4. In the optional **Email Attribute-ID** field, enter the Attribute-ID which includes the User's Email. For example, in Active Directory the default is mail.
5. To ensure the paths are correct for finding Users, in the **Username** field, enter the name of a User to search. Click the **Search** button. If the search is successful, the **Test Search for User** dialog box will indicate "User found!" and list the

Username, User Roles, and Email Address.


Test Search for User

User found!

Username: User
User Roles: Administrator
Email address: Test

6. In the **LDAP Configuration Wizard** window, click the **Finish** button.

> **NOTE:** All credentials and permissions are controlled by the LDAP server. Each time a user logs in, GE PulseNET will check the credentials and User Roles designated by LDAP, and update their permissions in PulseNET.

If GE PulseNET is being configured to use secure LDAP, an additional step is required.

GE PulseNET makes use of the standard Java LDAP service provider using *Java Secure Socket Extension (JSSE)* software for SSL support. To configure secure communication between GE PulseNET and the LDAP server, ensure that the GE PulseNET LDAP client trusts the LDAP server by installing the LDAP server's root certificate (CA) in GE PulseNET's database of trusted certificates.

1. Navigate to <pulsenet_home>\jre\lib\security
2. Obtain the CA certificate for the secure LDAP server and make sure it is accessible under <pulsenet_home>
3. Use the Java keytool program to import the LDAP server's root CA certificate into the keystore. Refer to the documentation for the Java keytool command if needed

(docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html). If the *jssecacerts* keystore does not exist, the following commands will create it. If it already exists, ensure the existing keystore password is known, and it can be accessed.

   a. <pulsenet_home>\jre\bin\keytool -import -file <path_to_ldap_server_CA_file>\<root_CA_Cert_filename>.crt-keystore jssecacerts
   b. Enter the *jssecacerts* keystore password, or enter a new password if none previously existed.
   c. Look at the files in the security folder to verify that the *jssecacerts* keystore exists.

4. Restart the GE PulseNET service and log in as an admin user to retest LDAPS connectivity.

GE PulseNET can now send requests to the secure LDAP server.

LDAP User Groups

To manage the roles assigned to LDAP User Groups navigate to **Administration > User Management > LDAP** User Groups.

1. Select the LDAP Groups to which roles will be assigned by clicking the checkbox.
2. Click the **Assign** button.
3. In the **Select Role** window, select the role that will be assigned to the selected LDAP Groups by clicking the checkbox.
4. Click **Save**.
5. To remove a role from a Group, select the LDAP Group by clicking the checkbox. Then, click the **Unassign** button.

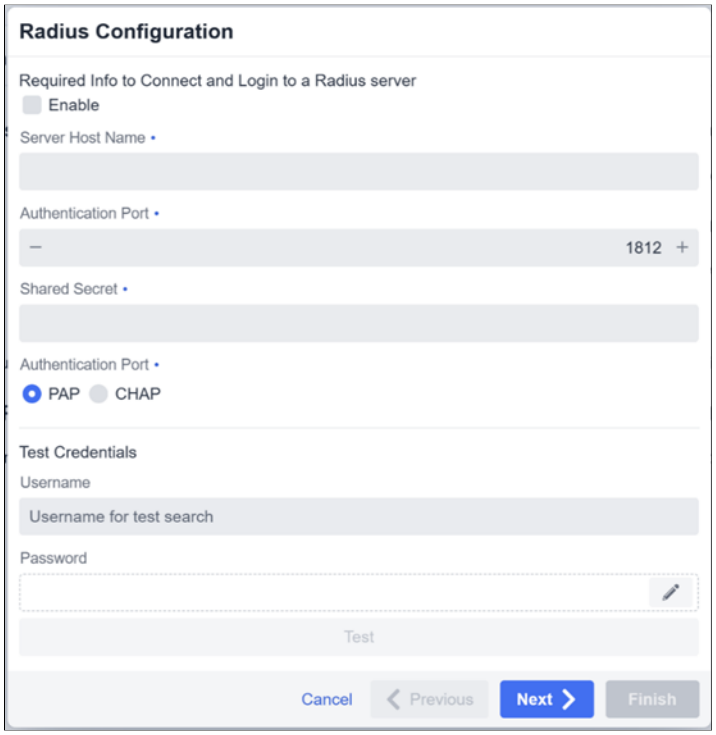
Enabling RADIUS Authentication

If using “Remote Authentication Dial In User Service” (RADIUS) to manage user access to the network, RADIUS server authentication can be enabled in GE PulseNET. When the GE PulseNET server is configured to access the RADIUS server, it is able to authenticate GE PulseNET users, which allows management of user credentials with RADIUS.

Enable RADIUS Authentication

1. Navigate to **Administration > User Management > RADIUS Configuration**.
2. In the dialog box that appears, select the **Enable** check box.
3. In the **Server Host Name** box, type the hostname or IP address of the RADIUS server.
4. In the **Authentication Port** box, type the port number.
5. In the **Shared Secret** box, type the authentication key for the RADIUS server.
6. Select the **Authentication Port** — PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol) are both supported.
7. To ensure that all values are correct, enter the username and password before clicking the Test button. After the test connection is successful, close the dialog box.
8. In the **Radio Configuration Wizard** window, click the **Next >** button.

After the RADIUS server connectivity is configured, default roles for users can be defined.



Radius Configuration

Required Info to Connect and Login to a Radius server

□ Enable

Server Host Name •

Authentication Port •

– 1812 +

Shared Secret •

Authentication Port •

● PAP ○ CHAP

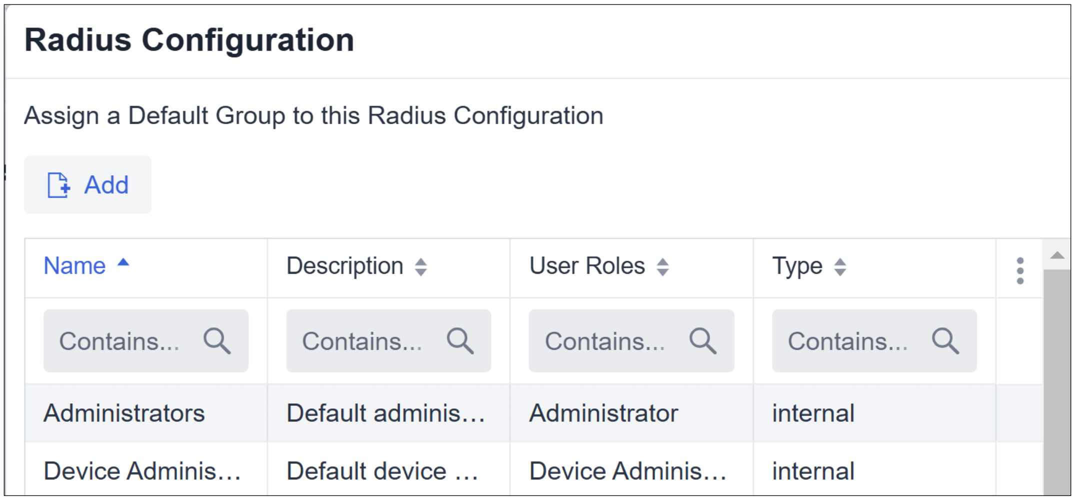
Test Credentials

Username

Username for test search

Password

Define User Roles

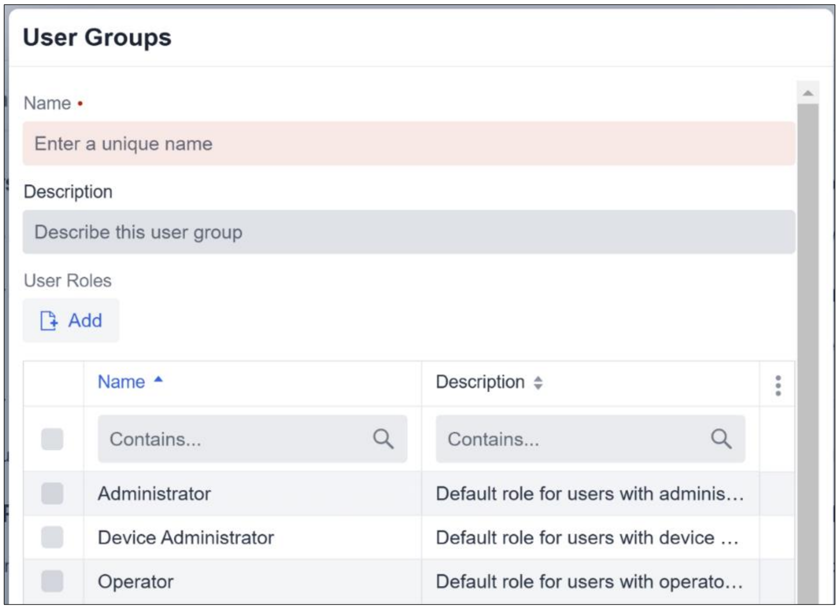


Radius Configuration

Assign a Default Group to this Radius Configuration

Name	Description	User Roles	Type
Contains...	Contains...	Contains...	Contains...
Administrators	Default adminis…	Administrator	internal
Device Adminis…	Default device …	Device Adminis…	internal

1. In the second **Radio Configuration Wizard** window, click the **Add** button to create a new user group. See **Managing User Groups** for more information on creating new groups.



User Groups

Name •

Enter a unique name

Description

Describe this user group

User Roles

	Name ▲	Description ⇕
□	Contains...	Contains...
□	Administrator	Default role for users with adminis…
□	Device Administrator	Default role for users with device …
□	Operator	Default role for users with operato…

2. Alternatively, select a default user group from the list of predefined options, select the "Administrators" or "Operators" group. Once a user logs onto GE PulseNET, they will be assigned this predefined group automatically. For instructions on changing that user group after the user logs in, visit **Managing User Groups > Managing Users**.
3. Click the **Finish** button.

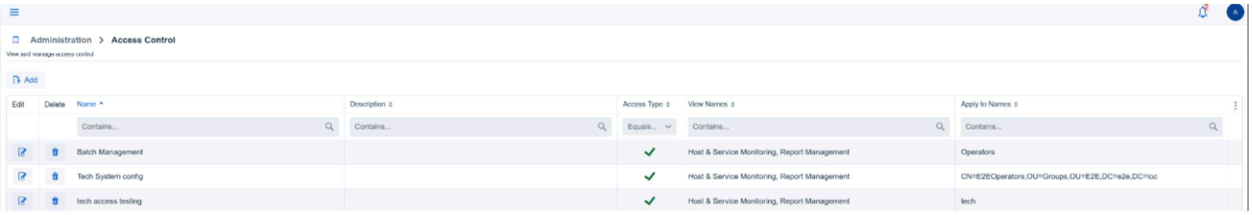
NOTE: GE PulseNET only supports RADIUS usernames that have more than four characters.

ACCESS CONTROL

The Access Control feature allows administrators to grant unprivileged users the ability to view dashboards which would normally only be accessible to administrators. This provides a way for GE PulseNET administrators to delegate some of their routine tasks to power users that they have identified. These extra privileges can be granted by specific User Name, by User Group, or by User Role.

View Access Control Properties

Navigate to **Administration > Access Control**.



Administration > Access Control

View and manage access control

Edit	Delete	Name	Description	Access Type	View Names	Apply to Names
		Contains...	Contains...	Equals...	Contains...	Contains...
		Batch Management		✓	Host & Service Monitoring, Report Management	Operators
		Tech System config		✓	Host & Service Monitoring, Report Management	CN=E2EOperators,OU=Groups,OU=E2E,DC=e2e,DC=loc
		tech access testing		✓	Host & Service Monitoring, Report Management	tech

Delete Access Control Records

- Select the checkbox on one or more rows which are to be deleted
- Click the **Delete** button and then confirm deletion of the selected rows
- Individual rows can also be deleted by clicking the **Delete** icon in the **Actions** section

Edit Access Control Records

Click the **Edit** icon on the row that will be edited. Any property except the unique Access Control Name can be edited.

Add Access Control Records

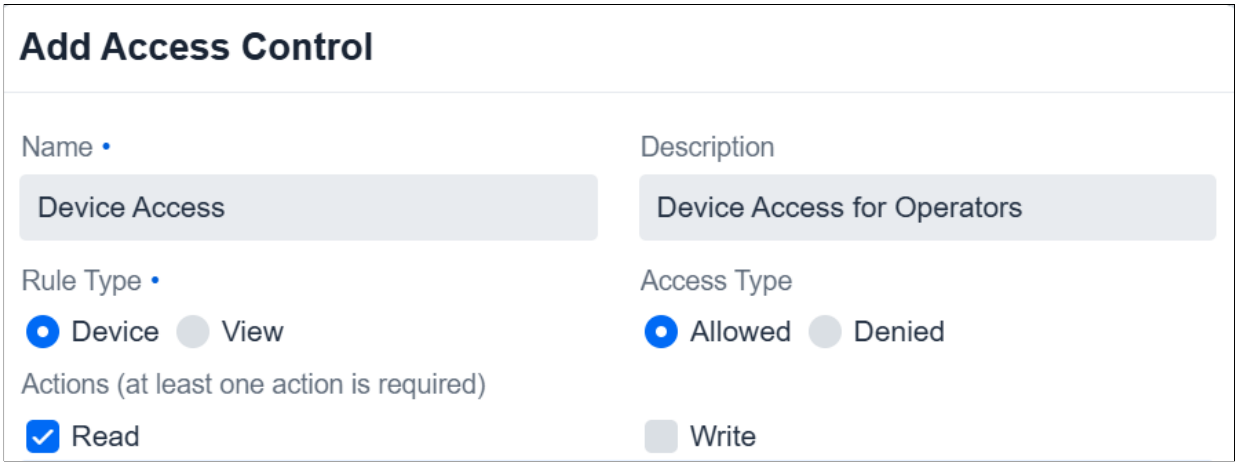
Click the **Add** button and enter the information for the new Access Control

Adding an Access Control Record

To add a new record, click the **Add** button at the top left of the Access Control table.

Enter a unique **Name** for this Access Control record and provide a detailed **Description**.

There are two options under **Rule Type** - **Device** and **View**. Note: LaunchNET does not use Device Rule Type.



Add Access Control

Name • Device Access

Description Device Access for Operators

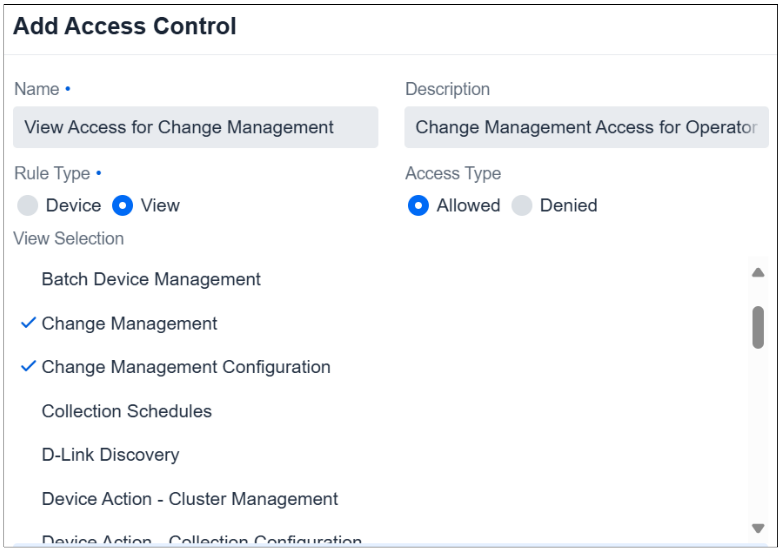
Rule Type • ● Device ○ View

Access Type ● Allowed ○ Denied

Actions (at least one action is required)

☑ Read □ Write

Rule Type: View is used to provide access to specific dashboards or control features.



Add Access Control

Name • View Access for Change Management

Description Change Management Access for Operator

Rule Type • ○ Device ● View

Access Type ● Allowed ○ Denied

View Selection

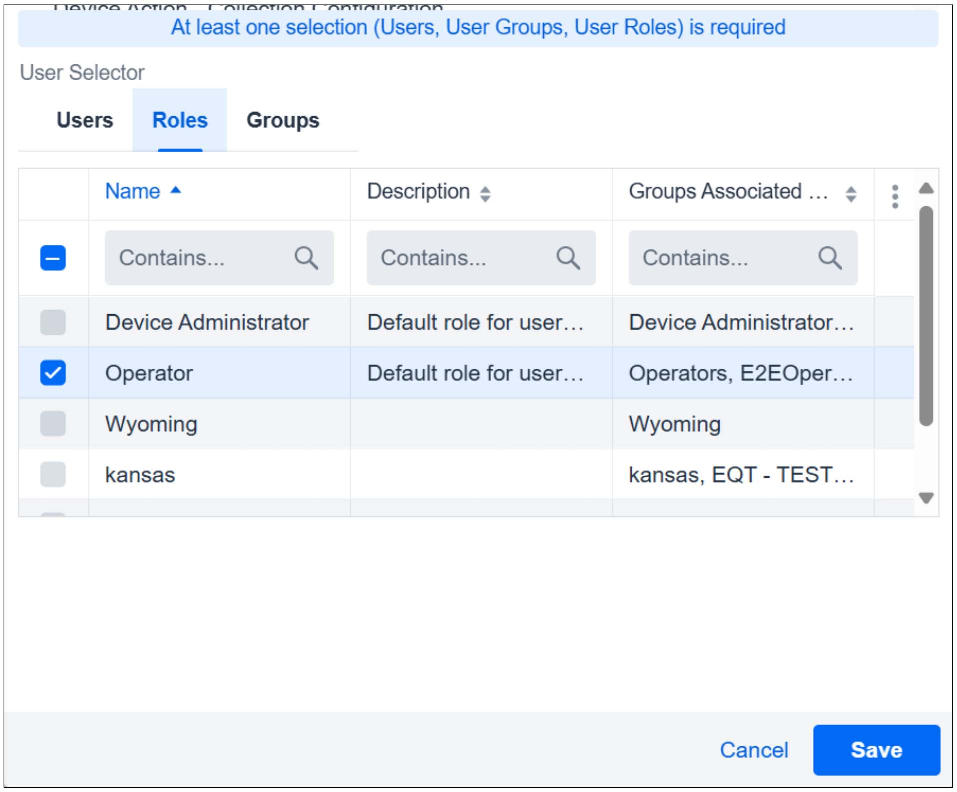
- Batch Device Management
- ✓ Change Management
- ✓ Change Management Configuration
- Collection Schedules
- D-Link Discovery
- Device Action - Cluster Management
- Device Action - Collection Configuration

Access Type contains the options Allowed or Denied. **Allowed** will provide view access for the selected users, while **Denied** will prevent the selected users from accessing the selected menu/feature. This provides the flexibility to add features for users who need them, or remove features for users who should not be allowed to access them. Note: administrators cannot be denied access to views.

The **View Selection** menu contains all features that can be allowed or denied for users. Select one or more Views from the left menu, and use the arrows to move desired features over to the right menu, Selected Views. Any feature in the

Selected Views menu will be Allowed/Denied.

On the User menu below, select at least one option from the Users, User Roles, or User Groups section to which the Selected Views will be applied.



Device Action   Collection Configuration

At least one selection (Users, User Groups, User Roles) is required

User Selector

	Name ▲	Description ⬍	Groups Associated … ⬍
⊟	Contains...	Contains...	Contains...
□	Device Administrator	Default role for user…	Device Administrator…
☑	Operator	Default role for user…	Operators, E2EOper…
□	Wyoming		Wyoming
□	kansas		kansas, EQT - TEST…

When finished, click **Save** to save the changes and view the new control in the **Access Control** table. Since each record can only grant access to one view at a time for one set of selected user(s), several different Access Control records may be required for each dashboard or user group.

Access Control for LaunchNET

For a LaunchNET-specific example, let's assume a new user titled: "Test Operator" has just been created using the instructions above, and must now be given access to LaunchNET features.

Navigate to Access Control, and click **Add**. Provide a name, i.e. "Test

Operator LaunchNET Access" Then select Rule Type - **View**. This will display the View Selection menu. Ensure Access Type - **Allowed** is also selected. Now scroll through the left-hand **Views** column to find the LaunchNET feature items, which appear as below:

- LaunchNET Inventory – Gives access to the internal inventory view.
- LaunchNET Management – Gives access to configuration and properties
- LaunchNET Report - Gives access to the reporting inside LaunchNET.
- LaunchNET Provisioning – Gives access to LaunchNET Templates and LaunchNET Staging

NOTE: An additional API Token can be created so that the Users/Admins can Provision devices.

MANAGING DEVICE GROUPS

The Device Groups dashboard allows for management of device group definitions, which are built using GE PulseNET filters. To manage device group settings, navigate to **Administration > Device Groups**. From the Device Groups table view, edit, or delete existing device groups, or add new device groups.

GE PulseNET device groups consist not only of associated devices, but also of associated users and time windows during which changes to the group's devices will be allowed. Each of these components are described in the **Adding Device Groups** section below.

View Device List for a Group

Click the play icon in the **Actions** section of the row for the group that will be examined. A popup list will show the devices included in this group. Click the **Information** icon on any of the devices to view a detailed list of device properties that are available. Click the gray **X** to close the popup window.

Edit Device Group Definition

Click the **Edit** icon on the row for the group that will be edited. See **Adding Device Groups** for an explanation of the components that can be edited in a device group.

Delete Device Group

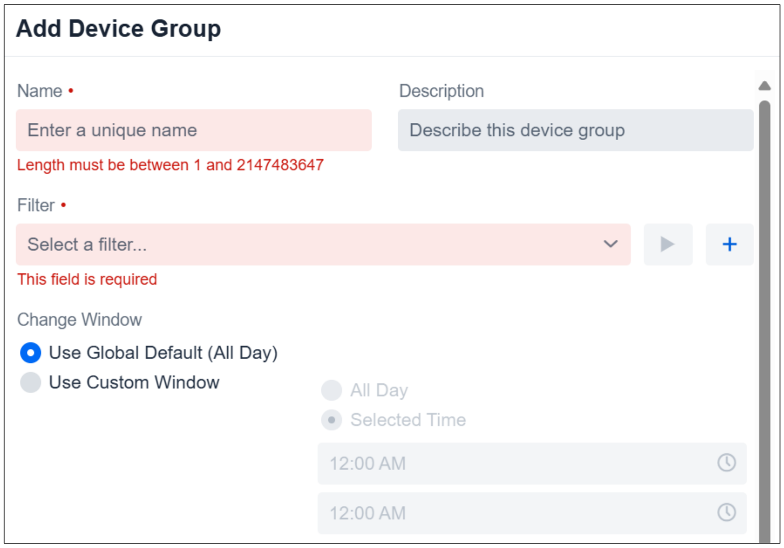
Click the **Delete** icon on the row for the group that will be removed. Click **Yes** to confirm the deletion, or **Cancel** to cancel this action.

Adding Device Groups

Click the **Add** button to add a new device group. Enter a unique device group name and a description of the devices that will be included in the group.

Next, select a device filter to be used to define the devices which are members of this group. If there is no appropriate filter in the dropdown list, click the **Add** icon to add a new filter. See the **Managing Device Filters** section for more information. Once a filter is selected, click the play icon to view a list of the devices that will be included in this device group.

Next select the **Change Window**, which is the period of time during which changes will be allowed on this group of devices. The global default change window setting can be used, or a custom time range can be defined. Finally, select the GE PulseNET users who are the owners for any change requests on this group of devices. Click **Save** to save the new device group.



Add Device Group

Name •

Enter a unique name

Length must be between 1 and 2147483647

Description

Describe this device group

Filter •

Select a filter...

This field is required

Change Window

● Use Global Default (All Day)

○ Use Custom Window

○ All Day

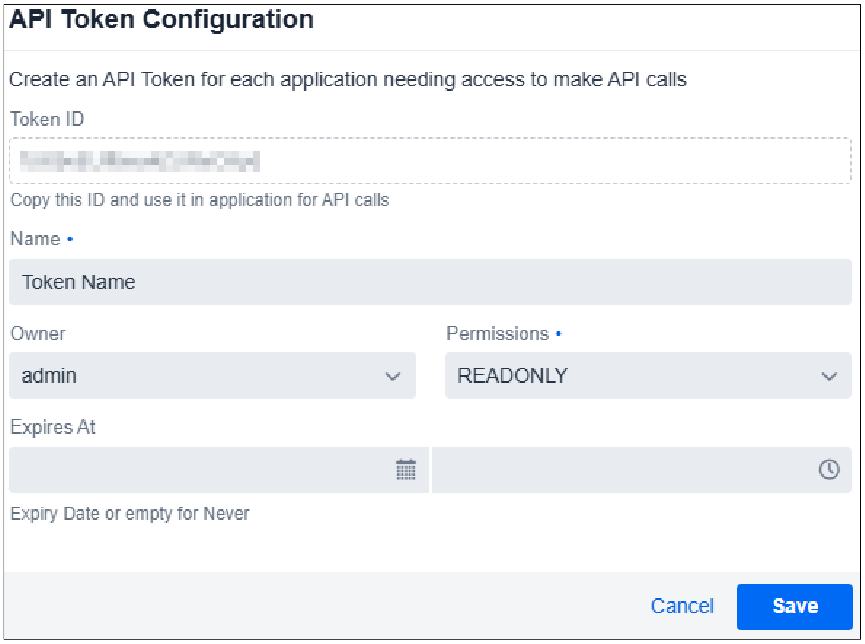
● Selected Time

12:00 AM

12:00 AM

API Tokens

An API token is a unique identifier created by GE PulseNET for other applications to request access. To integrate with PulseNET, generate an API token and provide that token to the other application. To generate an API Token, navigate to **Administration > System Configuration > API Tokens**. Click Add to create a random Token ID.



API Token Configuration

Create an API Token for each application needing access to make API calls

Token ID

[redacted]

Copy this ID and use it in application for API calls

Name •

Token Name

Owner

admin

Permissions •

READONLY

Expires At

Expiry Date or empty for Never

In the **API Token Configuration** dialog box, view the unique **Token ID** in the first field. The **Name** field adds a descriptive name to the token ID to help identify it. The **Expires At** field sets an expiry date for the token to determine when it expires. Use the **Permissions** drop-down menu, to determine which privileges the token will provide.

> ***Readonly:*** The software will only be allowed to view information. For example, it will be able to gather device information or view the current system debug level.
>
> ***Device:*** The software will be able to perform modifications to devices. For example, it will be able to add a new device to the system or trigger a configuration poll.
>
> ***System:*** The software will be able to perform modifications to the PulseNet system itself. For example, it will be able to change the system debug level or add a new license.

Click **Save** to return to the **Token ID** table, which lists and describes the unique token IDs that have been generated. The table contains all of the above information for each token and each column is sortable by clicking on the heading title. The **Last Used** category is useful when setting up an API token to ensure it is working properly. It will display the last date GE PulseNet received a call from that specific token ID and the status of the last call.

GETTING SUPPORT

If problems arise, diagnostic data can be gathered and saved in a group of files called a support bundle. Support bundles can then be forwarded to the GE MDS Technical Support team to aid in identifying and correcting any issues. Each support bundle contains a diagnostic snapshot of the GE PulseNET services and log files.

Generating a Support Bundle

It is not difficult to generate a support bundle. The time it takes to generate a support bundle depends on the number of monitored devices and the length of time the system has been monitoring those devices.

Generate a Support Bundle

1. Navigate to **Administration > Support**.
2. On the Support view, click **Generate Support Bundle**.

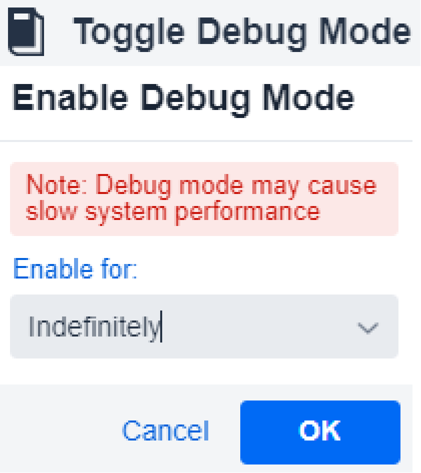
3. The **Include Observations** checkbox is an optional field this option gathers data for only those devices (limit 10 devices).
4. When prompted, either view the support bundle using a local archive manager or download it to the local machine.

In order to conserve storage space, support bundles are not stored on the GE PulseNET machine.

Note: If the user interface of PulseNET is unable to be reached. An offline support bundle can be generated from running the support_log_bundle.bat from the PulseNET home directory where PulseNET is installed.

Enabling Debug Mode

Click on the Toggle Debug Mode button to enable. In the dialogue box that appears, select a maximum runtime for Debug Mode from the drop-down menu. Click OK. Please keep in mind that Debug Mode may cause slowdowns in system performance.



Toggle Debug Mode

Enable Debug Mode

Note: Debug mode may cause slow system performance

Enable for: Indefinitely

LaunchNET Menu

The LaunchNET menu item can be located on the **PulseNET > Administration** page, provided that a LaunchNET license has been applied. Sub-menus explained below.

Provisioning

The provisioning process has two main functions: **Template** and **Staging**.

During the template creation process, an Administrator user chooses the set of parameters for each template and determines which groups and devices that template should be applied to.

Once a template has been fully created, it is Staged, making it available as a provisioning option to the chosen device groups.

Template

Templates are GE LaunchNET's key components, dictating what devices can be provisioned with what features by which users. They are where the User creates the features of how each set of devices will be configured.

After selecting GE and the device model the template applies to (thus removing options that don't apply to that specific device set), the User selects which features to include on the template. Some features, such as SNMP Location, can only appear once on the template. Other features, such as NAT entries for a router, are not unique and can be used multiple times on the same template to collect different data.

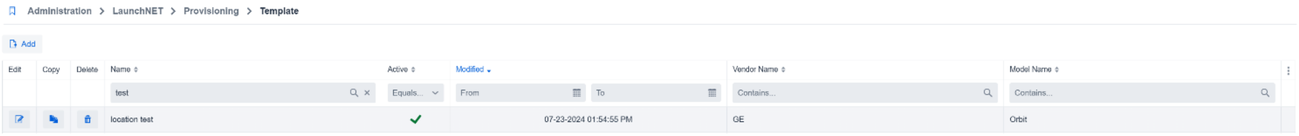
Once saved, a template can be edited to add additional features, but the existing features of that saved template cannot be deleted (to prevent a template from being overwritten). The best way to "delete" features is to copy an existing template and create a brand new template with the desired changes. Copying a template duplicates the selected features, but offers the freedom to add, edit, or delete features as needed. This is extremely useful when creating a set of templates with very similar feature sets.

A User may delete a template entirely. Before complying, however, the **Delete** feature checks to see if the template has been staged. If it has not been staged, the template is removed. If it has been staged, and especially if devices have been provisioned based on that template, GE LaunchNET will warn of the ramifications of deleting the template and suggest steps to properly return the provisioned devices to inventory before deleting the template they were using.

NOTE: An IP Address for at least one interface in the template must be supplied in order for a GE Orbit device to be provisioned. Also, when provisioning a GE Orbit and selecting the LO1 or GRE1 interfaces in the templates, those interfaces must be in the golden config in order to provision those interfaces. If additional interfaces are required (i.e. LOx or GREx), please contact a sales representative to have them added.

Template List menu:

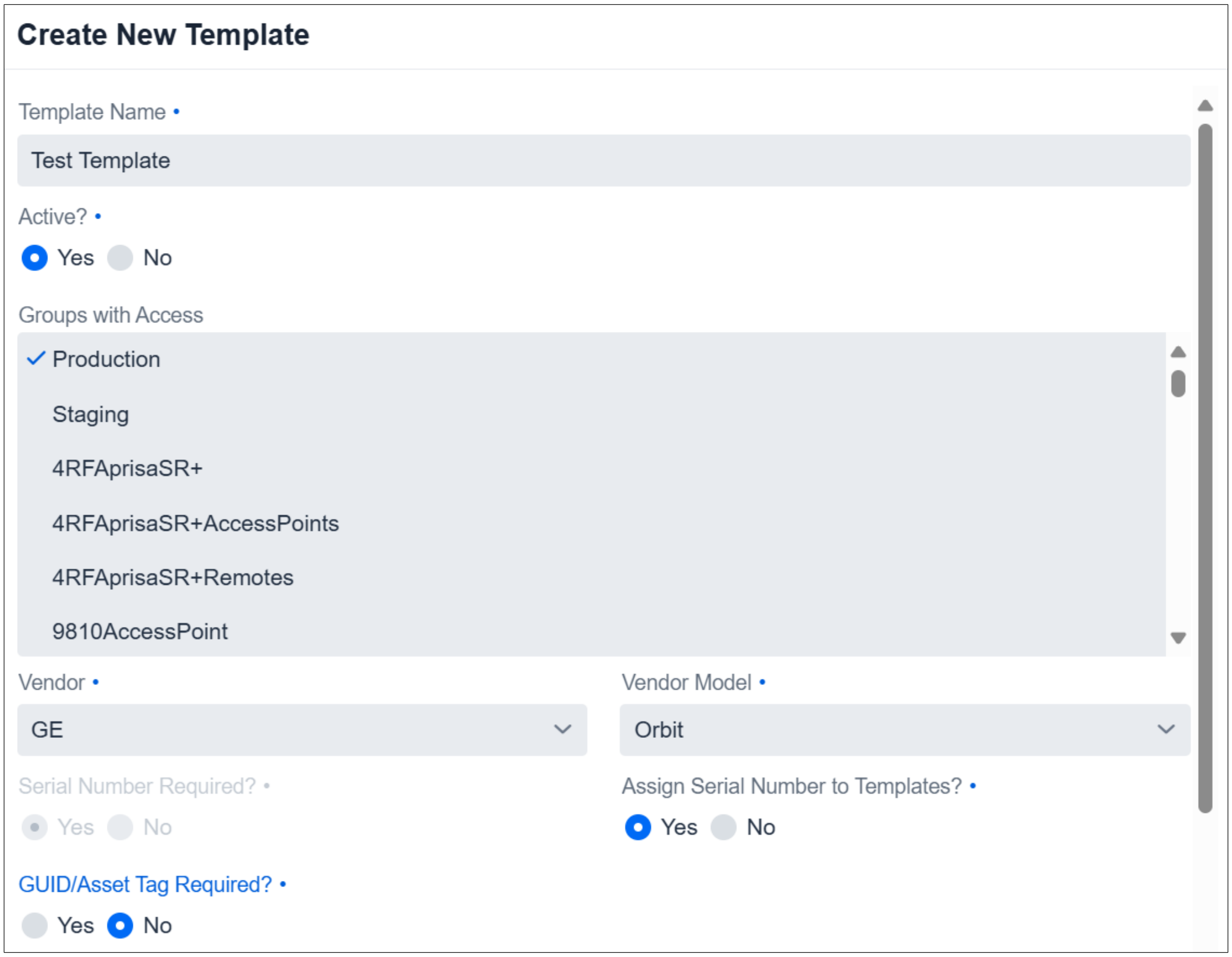
- Add a new template
- Edit, copy, or delete an existing template
- Search for existing templates using column filters



Edit	Copy	Delete	Name	Active	Modified	Vendor Name	Model Name
			test	Equals...	From To	Contains...	Contains...
			location test	✓	07-23-2024 01:54:55 PM	GE	Orbit

Click ***Add*** *to access the Create New Template menu:*

- Provide a Template Name
- Mark that template as Active (i.e. ready for Staging - Y/N)
- Select which device group(s) the template will be associated with
- Select GE and Model of the devices that will use this template



Create New Template

Template Name •

Test Template

Active? •

● Yes ○ No

Groups with Access

✓ Production

Staging

4RFAprisaSR+

4RFAprisaSR+AccessPoints

4RFAprisaSR+Remotes

9810AccessPoint

Vendor •

GE

Vendor Model •

Orbit

Serial Number Required? •

● Yes ○ No

Assign Serial Number to Templates? •

● Yes ○ No

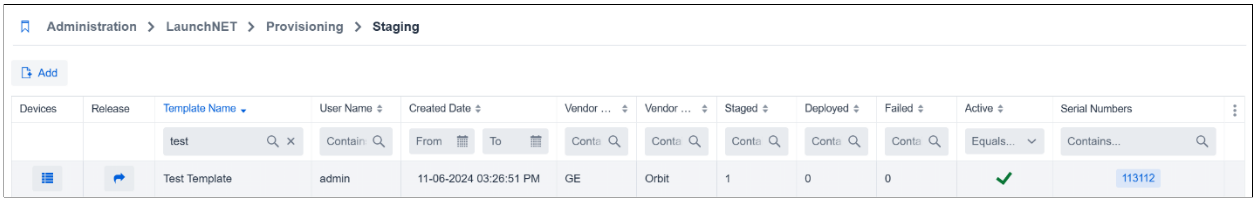
GUID/Asset Tag Required? •

○ Yes ● No

Created Templates can be edited at any time by clicking the notepad "edit" icon to the left of the template name in this menu.

Staging

The Staging menu is where Administrator users can release or publish created templates so that Operator users can use the Radio Admin client to configure the device.



Administration > LaunchNET > Provisioning > Staging

Add

Devices	Release	Template Name	User Name	Created Date	Vendor ...	Vendor ...	Staged	Deployed	Failed	Active	Serial Numbers
		test	Contain	From To	Conta	Conta	Conta	Conta	Conta	Equals...	Contains...
		Test Template	admin	11-06-2024 03:26:51 PM	GE	Orbit	1	0	0	✓	113112

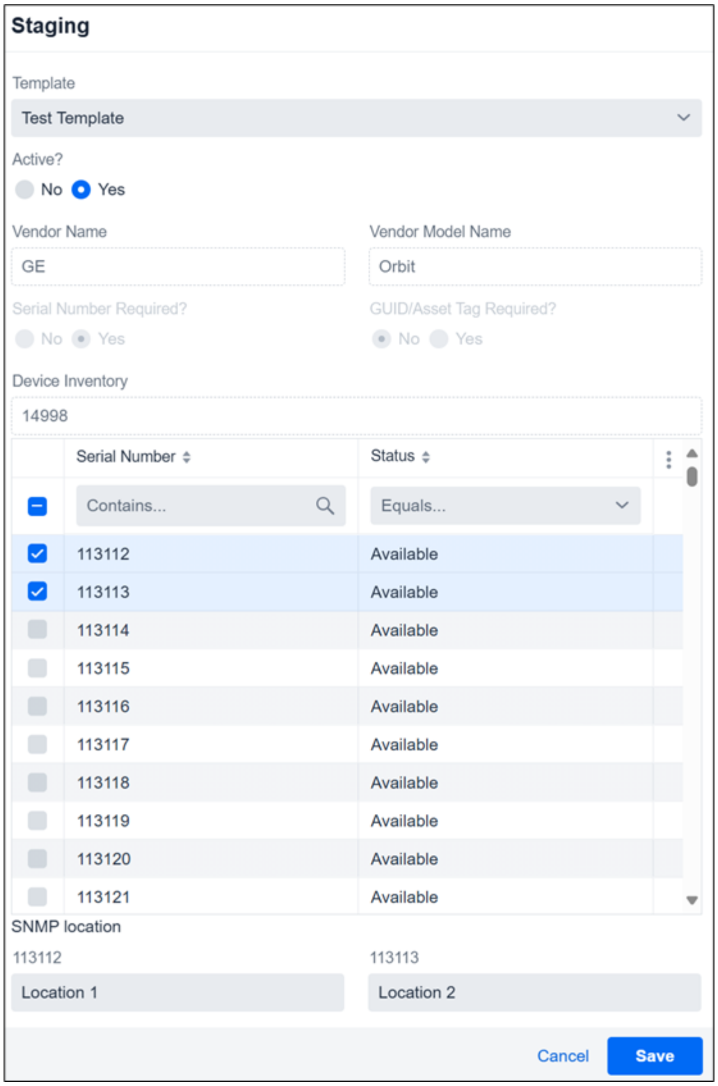
Click the **Add** button, then on the Template dropdown select a template.

Active – determines if this Staging item can be selected for Provisioning.

The Vendor Name, Vendor Model Name, Device Inventory is dictated by the underlying template and cannot be modified from this menu but is provided for reference.

In the Device Inventory menu, select which serial numbers will be associated with the template selected in this staging.

Users can allow users to provision radios multiple times within a single template. If the **"Allow Re-provisioning of Inventory"** box has been set to **Active - YES** (instead of the default **NO**) on the Company Information page, a specific serial number can be staged and restaged multiple times. This option allows specific serial numbers to be reprovisioned without having to restage the full template.



Staging

Template

Test Template

Active?

○ No ● Yes

Vendor Name: GE

Vendor Model Name: Orbit

Serial Number Required?

○ No ● Yes

GUID/Asset Tag Required?

● No ○ Yes

Device Inventory

14998

	Serial Number	Status
⊟	Contains...	Equals...
☑	113112	Available
☑	113113	Available
☐	113114	Available
☐	113115	Available
☐	113116	Available
☐	113117	Available
☐	113118	Available
☐	113119	Available
☐	113120	Available
☐	113121	Available

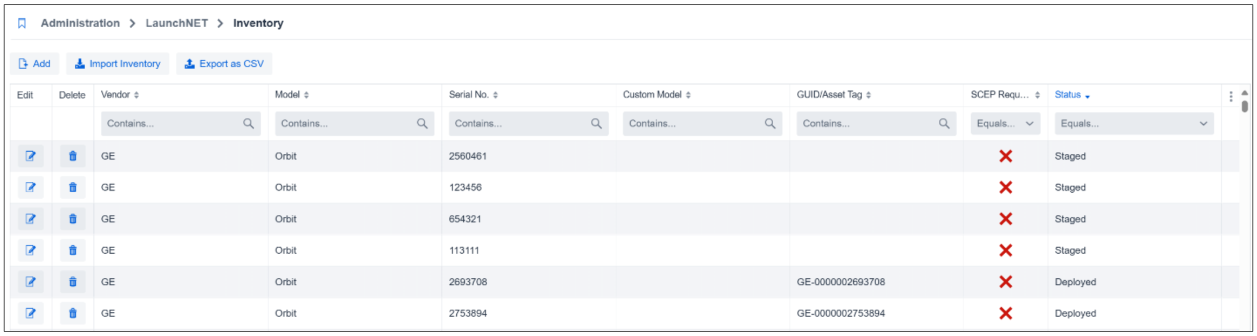
SNMP location

113112: Location 1

113113: Location 2

Device Inventory

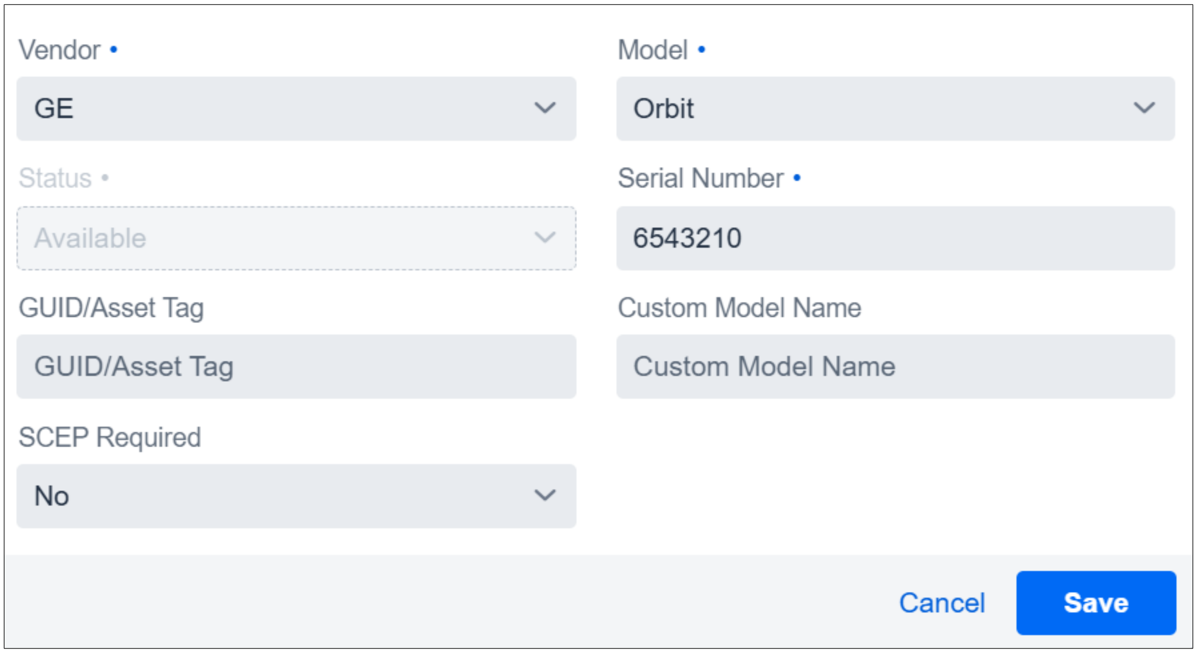
The **Device Inventory** allows authorized users to manually add one device at a time or import/export a list of devices from a CSV file as a batch action.



Edit	Delete	Vendor	Model	Serial No.	Custom Model	GUID/Asset Tag	SCEP Requ...	Status
		Contains...	Contains...	Contains...	Contains...	Contains...	Equals...	Equals...
		GE	Orbit	2560461			✗	Staged
		GE	Orbit	123456			✗	Staged
		GE	Orbit	654321			✗	Staged
		GE	Orbit	113111			✗	Staged
		GE	Orbit	2693708		GE-0000002693708	✗	Deployed
		GE	Orbit	2753894		GE-0000002753894	✗	Deployed

Click **Add** to create a new device entry. Select a Vendor and Model from the dropdown menus, then provide the Serial Number. Click **Save** when ready. The following additional information can be added, but is not required:

- GUID/Asset Tag
- Custom Model Name
- SCEP Required [Y/N]



Vendor •
GE

Model •
Orbit

Status •
Available

Serial Number •
6543210

GUID/Asset Tag
GUID/Asset Tag

Custom Model Name
Custom Model Name

SCEP Required
No

Once a device has been added to the Inventory, it can be edited.
The following statuses can be edited from the edit in the device inventory view:

Staged > Available - This will unstage the device from a staging.

Deployed > Available - This will remove all staging information and set the device to Available to be provisioned again.
Completed > Available -This will remove all staging information and set the device to Available to be provisioned again.

The full device list can be exported using the **Export as CSV** option. The export will be created in **GE_MDS\PulseNET\reports**.

To Import a **Device Inventory** list, select the **Import Inventory** option.

Import Menu:

- Select the device Vendor and Model
- Select whether the uploaded table has header rows
- Select which column contains the serial number/guid/asset tag (or ignore)
- Upload file*

NOTE:** The **Upload File** must be in a comma separated format that includes the following fields: ***serial/GUID, model name, and ***SCEP flag***.

The **SCEP flag** tells GE LaunchNET to configure the device with X.509 RSA certificates prior to device configuration with configuration templates, and must be in the following format:

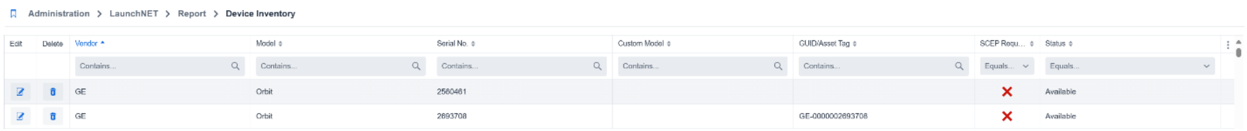
- Values to set the field false: 0,f,F,false,False,FALSE,n,N,no,No,NO
- Values to set the field true: 1,t,T,true,True,TRUE,y,Y,yes,Yes,YES

Report

All the reports in this section are predefined with some search options. Hyperlinks in the deployments completed section give more details on each deployment. The Company Admin may clink on the **Export** button to see these details.

Device Inventory

This menu acts as a live report of the current inventory, allowing the user to search or sort the list by vendor, model, serial number, GUID/Asset tag, or staging status.



Administration > LaunchNET > Report > Device Inventory

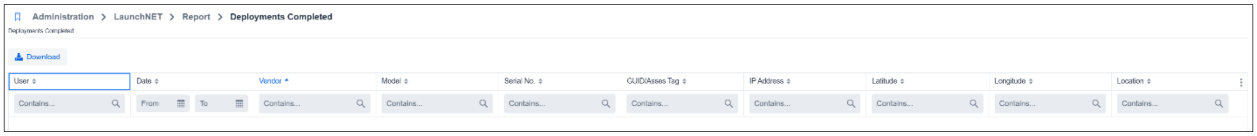
Edit	Delete	Vendor	Model	Serial No.	Custom Model	GUID/Asset Tag	SCEP Requ...	Status
		Contains...	Contains...	Contains...	Contains...	Contains...	Equals...	Equals...
		GE	Orbit	2560461			✗	Available
		GE	Orbit	2693708		GE-0000002693708	✗	Available

Deployments Completed

This section allows the Administrator to:

- Generate a Deployment Detail Report which will display information sent between Radio Admin, ZTP, and LaunchNET.
- Search deployments by template name, vendor name, or vendor model name
- Sort recent deployments by template, vendor, or model
- Show the status of recent deployments (staged or provisioned)
- View deployments released back into inventory (highlighted in pink)
- Export the data to a CSV file
- Export deployment details to a CSV file (user, timestamp, vendor, model, serial number, GUID/Asset Tag, and IP addresses)

  Note: If a Staging attempt is later deleted, the Deployments Completed history for that staging attempt will also be removed.



Administration > LaunchNET > Report > Deployments Completed

Deployments Completed

User	Date	Vendor	Model	Serial No.	GUID/Asses Tag	IP Address	Latitude	Longitude	Location
Contains...	From To	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...	Contains...

Management

Integrations

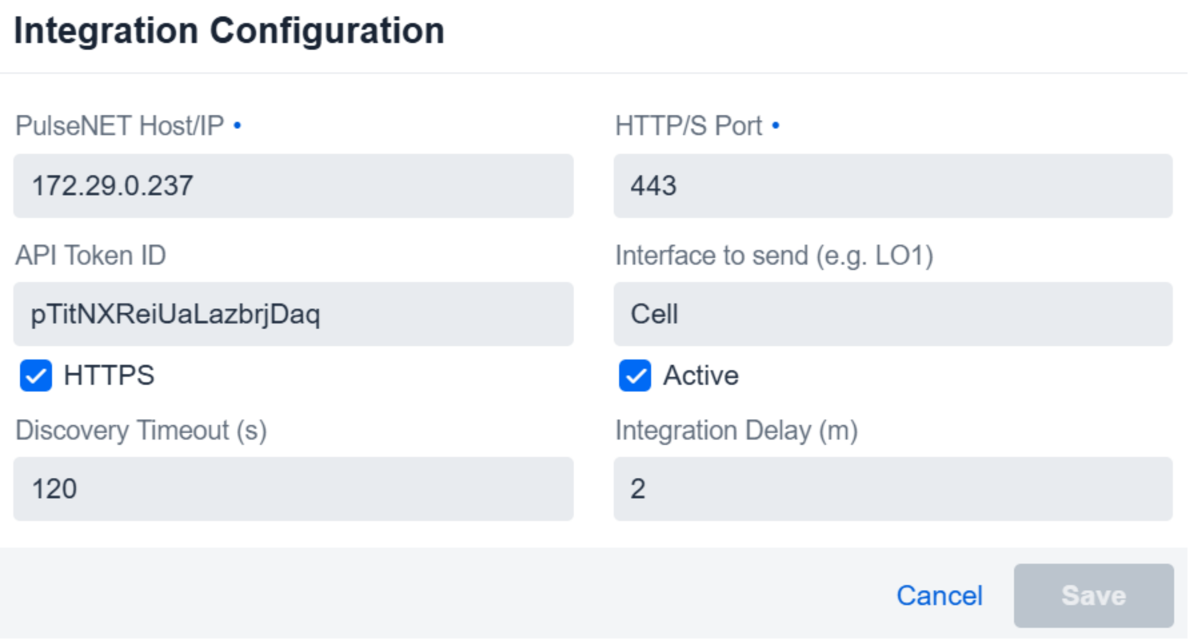
Configuration

After GE LaunchNET has configured a new SNMP device, it can automatically discover and authorize it in PulseNET. (NOTE: SNMP Credentials must be entered in PulseNET and the device must be online in order to accomplish).

This feature will auto-instantiate the new device in PulseNET Enterprise and trigger a configuration/performance collection in PulseNET. If this feature is active, then every new provisioned device will be sent to PulseNET Enterprise.

Note: Integration in this version is compatible with GEMDS Orbit devices only.

To enable Integration, navigate to: **Administration > LaunchNET > Management > Integrations > Configuration:**



Integration Configuration

PulseNET Host/IP • 172.29.0.237

HTTP/S Port • 443

API Token ID pTitNXReiUaLazbrjDaq

Interface to send (e.g. LO1) Cell

☑ HTTPS

☑ Active

Discovery Timeout (s) 120

Integration Delay (m) 2

Enter the PulseNET server Hostname or IP, and a PulseNET API token.

Interface to Send allows the required interface (LO1, GRE1, Bridge, etc...) to be selected.

If the PulseNET instance was installed as HTTPS Secure Server only, check **HTTPS**, otherwise leave as is.

Default ports are: **HTTP 8080 - HTTPS 8443**

Discovery Timeout sets the amount of time GE PulseNET waits for device response during discovery.

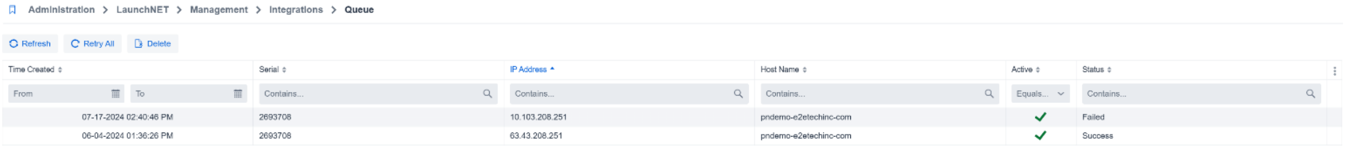
Integration Delay - Customizable delay is the time taken for a device to be discovered in PulseNET after the device has been provisioned.

Once configured, compatible devices provisioned by GE LaunchNET will now automatically be added to the Integration Queue.

Queue

To review the Integration Queue, navigate to **Administration > LaunchNET > Management > Integrations > Queue.**

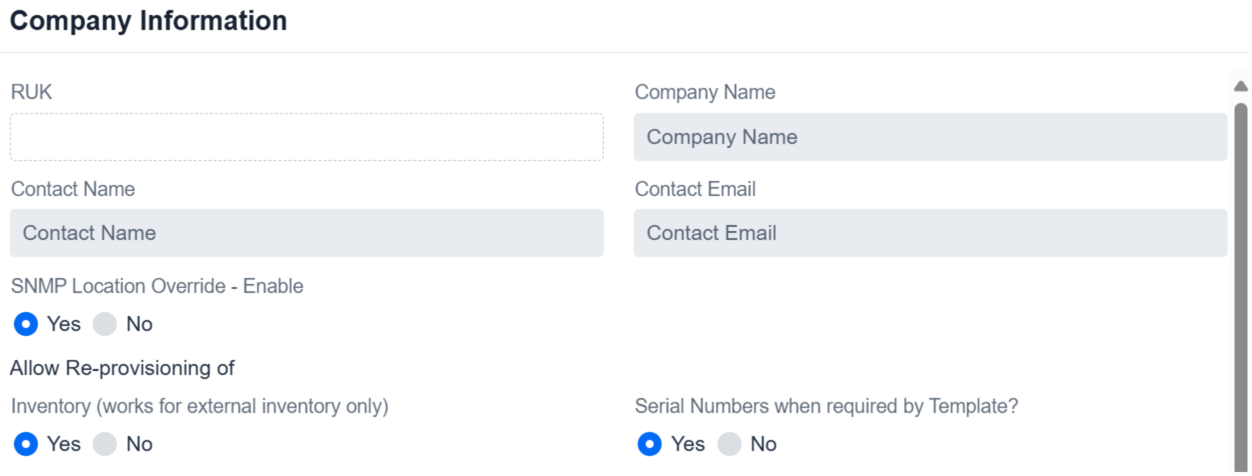
Here, view any pending Integration discovery request, or review past Integrations. Devices that have the status of error or failed can be set to retry for auto-instantiate by clicking the "Retry All" button. The Delete button will become available if any record(s) are selected. Keep in mind any record, whether pending or not can be deleted. Please verify before confirming the action.


Administration > LaunchNET > Management > Integrations > Queue
Refresh
Retry All
Delete

Time Created	Serial	IP Address	Host Name	Active	Status
From / To	Contains...	Contains...	Contains...	Equals...	Contains...
07-17-2024 02:40:46 PM	2693708	10.103.208.251	pndemo-e2etechinc-com	✓	Failed
06-04-2024 01:36:26 PM	2693708	63.43.208.251	pndemo-e2etechinc-com	✓	Success

Company Information

The Company Information menu allows Administrator users to manage company contact/account and Microsoft CA server information.



Company Information

RUK

Company Name

Company Name

Contact Name

Contact Name

Contact Email

Contact Email

SNMP Location Override - Enable

● Yes ○ No

Allow Re-provisioning of

Inventory (works for external inventory only)

● Yes ○ No

Serial Numbers when required by Template?

● Yes ○ No

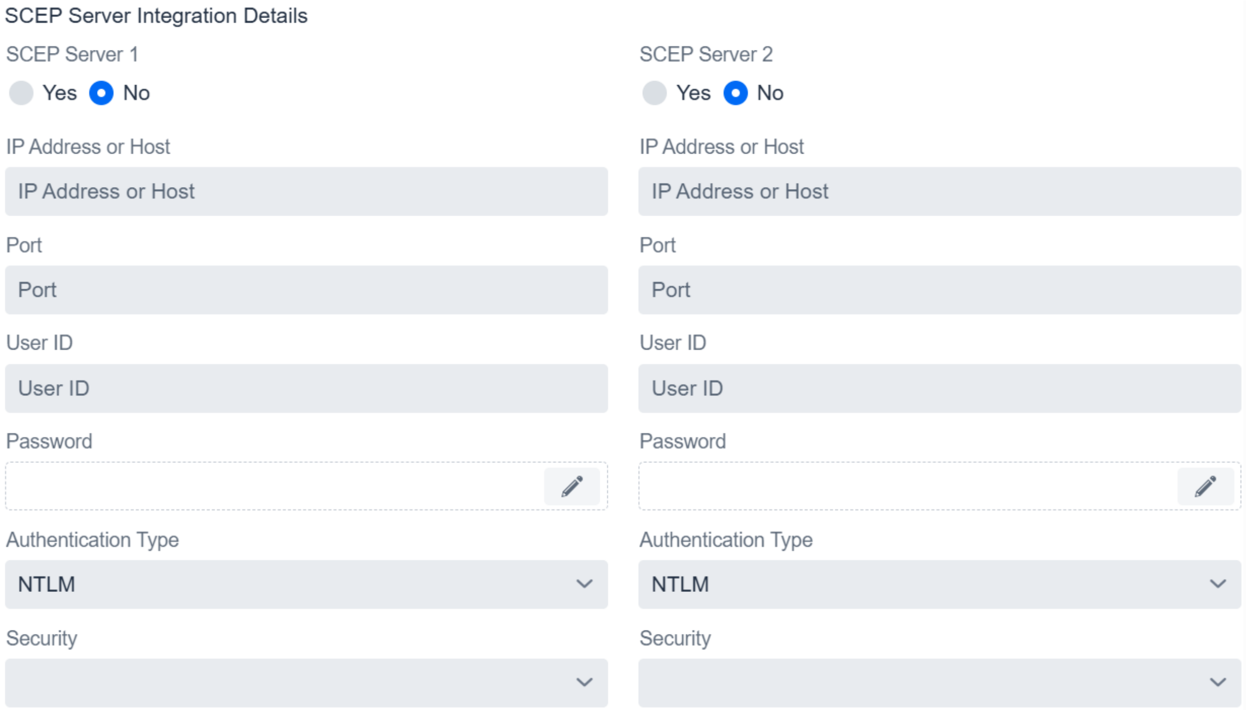
RUK - [Field is not used in this release.]

Enter Company and Contact information as needed in **Account Details**.

SNMP Location Override will activate the option to enter a custom location name for each device serial number during the Template creation process.

Allow Re-provisioning of Serial Numbers - if checked, allows radios to be provisioned multiple times within a single template, overriding the “once provisioned, don’t do it again” approach. If set to **Yes**, a specific serial number can be staged and restaged multiple times without issue using the same template, or inventory. This option is designed for customers using external inventories that limit changes to the inventory system, and allows specific serial numbers to be reprovisioned without actually having to restage the full template. Note: This only works when the Serial Numbers are Required and correctly checked in the Template.

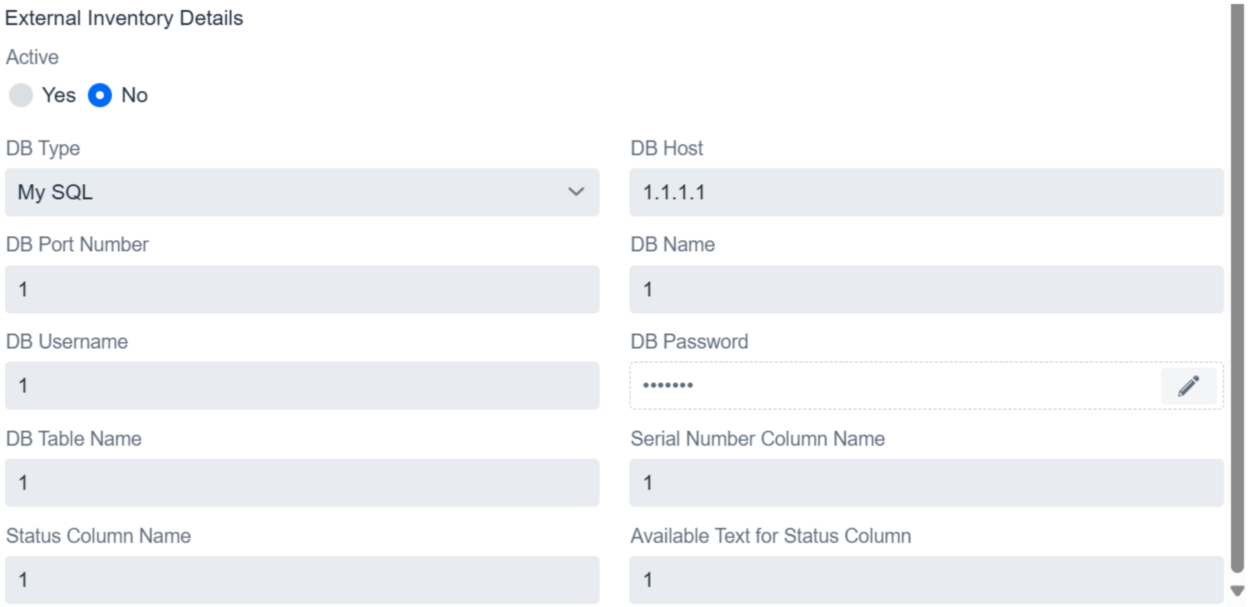
The lower menu is used to enter SCEP server, connection, and redundant/backup server information.



SCEP Server Integration Details

SCEP Server 1	SCEP Server 2
○ Yes ● No	○ Yes ● No
IP Address or Host: IP Address or Host	IP Address or Host: IP Address or Host
Port: Port	Port: Port
User ID: User ID	User ID: User ID
Password:	Password:
Authentication Type: NTLM	Authentication Type: NTLM
Security:	Security:

External Inventory Details allows a customer to import a device inventory from an external MySQL or MSSQL database. Fill in the fields with the external database information and save. Note: Doing this will disable internal device inventory.



External Inventory Details

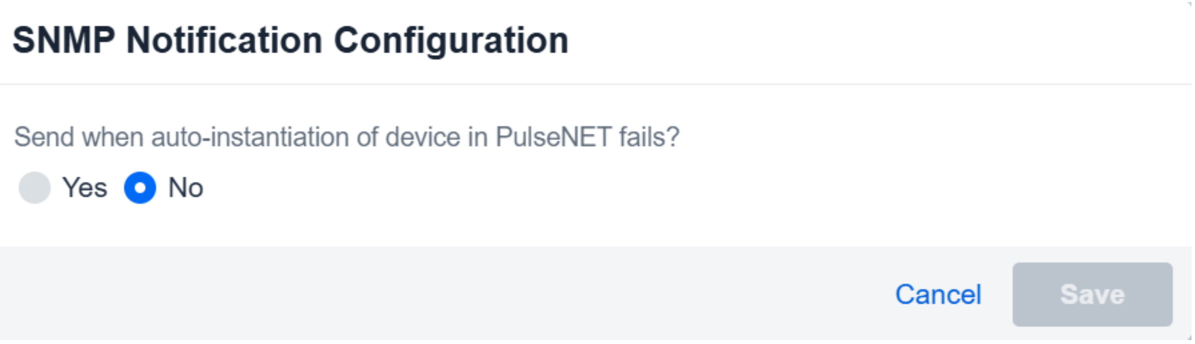
Active

○ Yes ● No

DB Type: My SQL	DB Host: 1.1.1.1
DB Port Number: 1	DB Name: 1
DB Username: 1	DB Password: •••••••
DB Table Name: 1	Serial Number Column Name: 1
Status Column Name: 1	Available Text for Status Column: 1

Notifications

If for some reason a PulseNET Integration should fail, the Notifications feature can activate an SNMP trap that will be sent to a Manager of Managers system. Select “Yes” and **Save** to enable.

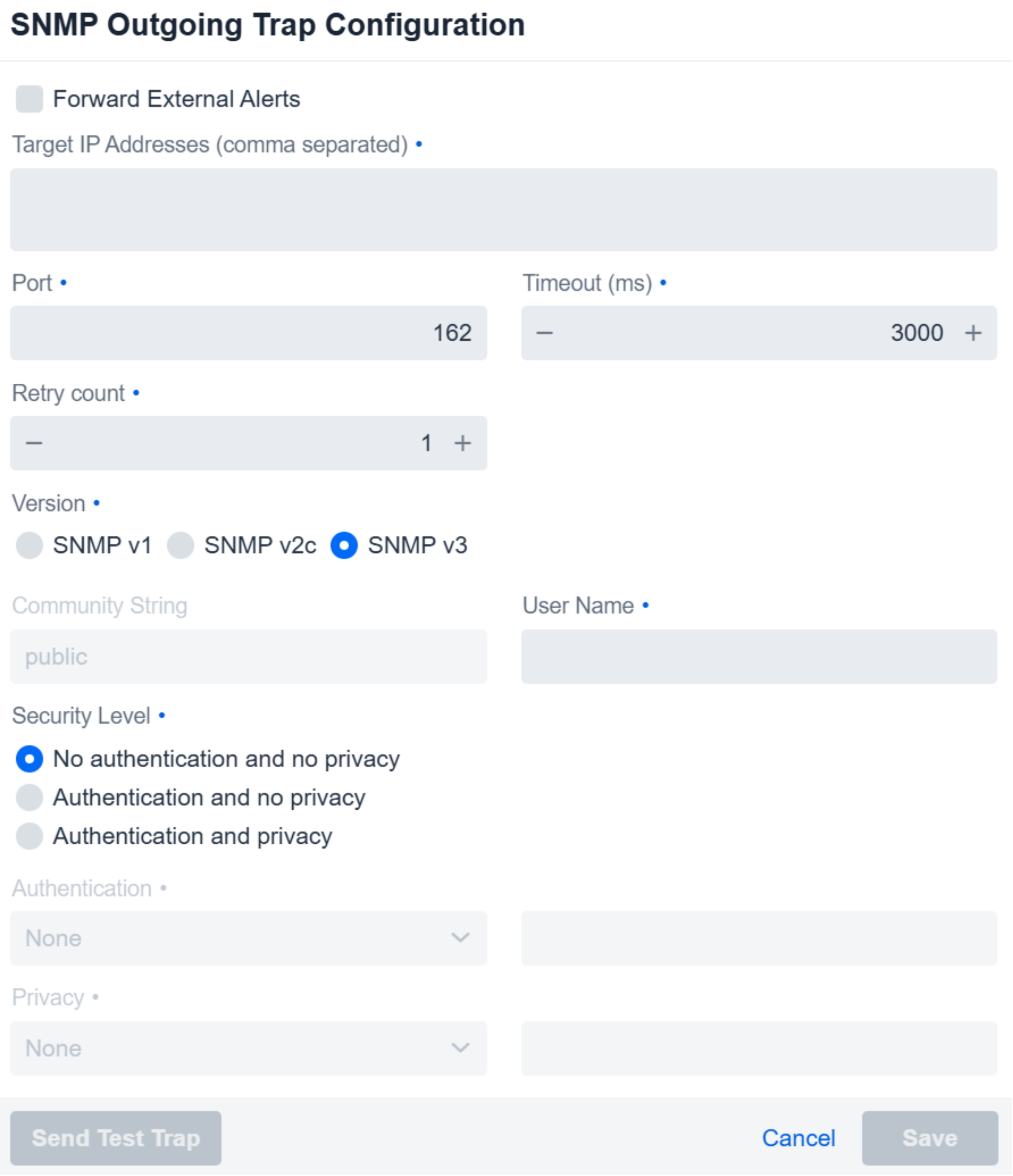


SNMP Notification Configuration

Send when auto-instantiation of device in PulseNET fails?

○ Yes ● No

This notification will use the GE PulseNET SNMP Trap Settings which can be found by navigating to **Administration > System Configuration > SNMP Outgoing Trap Configuration**.



SNMP Outgoing Trap Configuration

□ Forward External Alerts

Target IP Addresses (comma separated) •

Port • 162

Timeout (ms) • 3000

Retry count • 1

Version • ○ SNMP v1 ○ SNMP v2c ● SNMP v3

Community String: public

User Name •

Security Level •

● No authentication and no privacy

○ Authentication and no privacy

○ Authentication and privacy

Authentication • None

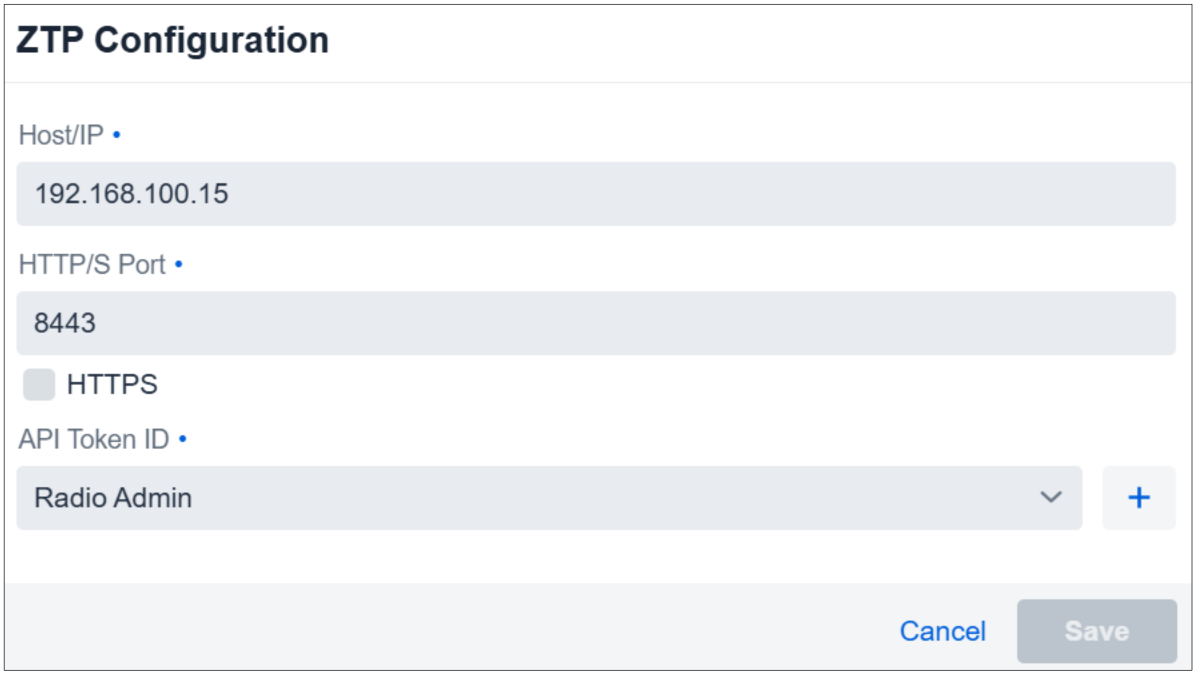
Privacy • None

In the SNMP **Outgoing Trap Configuration view**, enable and define where to send outgoing alerts, including the destination and credentials for messages. When the **Forward External Alerts** checkbox is not selected, trap messages are sent only when PulseNET Enterprise rules generate alerts. When the **Forward External Alerts** checkbox is selected, PulseNET Enterprise will also send alerts received from the external devices.

Click the **Send Test Trap** button to test the trap message. To confirm trap messages are being sent, verify the test message has been received.

ZTP Configuration

Zero-Touch Provisioning (ZTP) is an advanced automation feature that allows devices to be provisioned and configured automatically.



ZTP Configuration

Host/IP •

192.168.100.15

HTTP/S Port •

8443

□ HTTPS

API Token ID •

Radio Admin

ZTP Logs

Logs for Zero Touch Provisioning are kept here and can be updated using the Refresh button to pull the latest between ZTP and the device.

Provisioning with Radio Admin

Radio Admin Client for Provisioning

To accomplish field deployments of new devices using the GE LaunchNET templates, field technicians will have a local copy of the Radio Admin software on their computers. The Provisioner tab on the Tools menu will allow field technicians to contact the Provisioning server and select the list of deployment options that are available to them.

For Radio Admin software installation and configuration, please refer to the full Radio Admin User guide that is delivered with the software. The GE LaunchNET currently supports the following GE MDS device models:

- Orbit
- SD
- TransNET

Settings for Provisioning with Radio Admin

Navigate to the **Tools > Provisioner > Settings** tab to provide the GE LaunchNET Server credentials. This tells Radio Admin how to connect to the LaunchNET Server in order to get the list of configuration templates that have been provided for the specific field technician who is deploying a specific device on the network.

- Enter the server name or IP address of the Provisioning server on which the staged entries reside
- Enter the field technician username for the Provisioning server
- Enter the field technician password for authenticating to the Provisioning server
- Enter the RUK for this user and company
- Select whether secure HTTPS protocol is used to connect to the Provisioning server

Radio Admin will connect to the local device that is being provisioned using either an Ethernet cable (Orbit) or a serial cable (SD & TransNET). If connecting to the device serially, enter the COM port, baud rate, data bits, stop bits, and parity.

Save the Radio Admin settings by clicking the **Save Changes** button.

Radio Admin Provision Tab

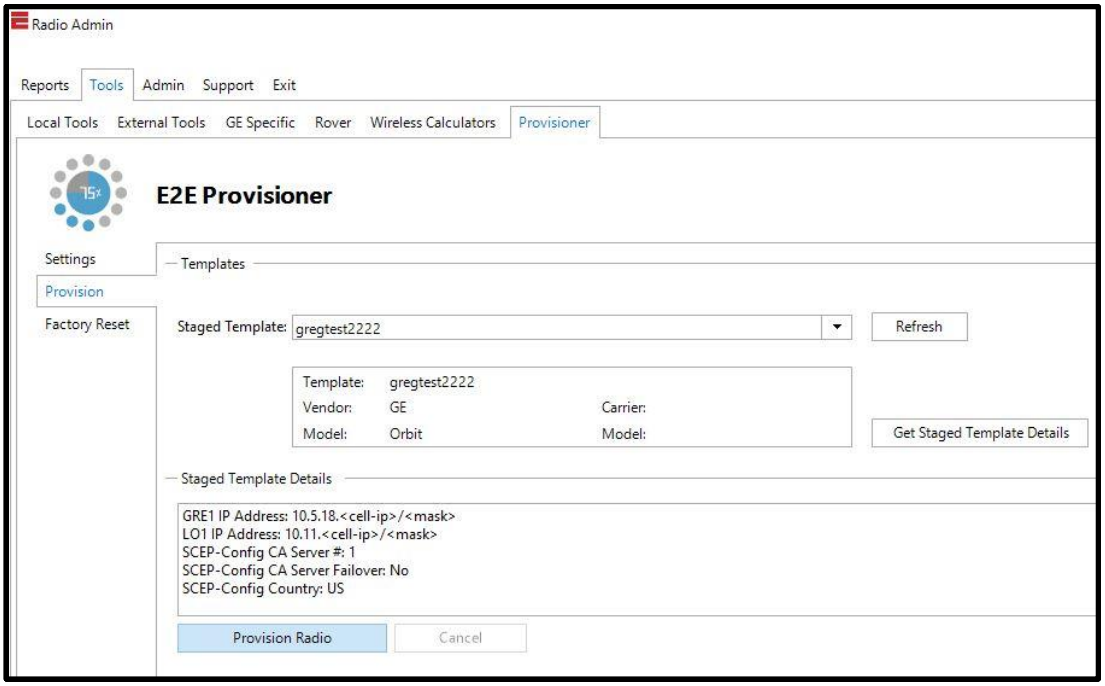
Once the settings have been saved, click on the **Provision** tab and **Radio Admin** will attempt to connect with the Provisioning server using the credentials provided.

> NOTE: Administrators MUST create an Device Level API Token in order for the user to communicate with LaunchNET. This API Token is tied to the user so that the user will only be able to see provisions in which they have access.

If successful, the list of available templates for this user will be displayed in the Staged Templates drop-down list. If unsuccessful, an error message will appear suggesting validation of the GE LaunchNET account and connection settings.

If “Use secure connections (HTTPS)” was selected on the **Settings** tab, an error message indicating Radio Admin could not establish a trust relationship for the SSL/TLS secure channel may appear. To resolve this issue, ensure that the Radio Admin CA certificate includes an entry for the Provisioning Server. Ask an IT Admin to add a certificate to the Windows computer.

Click on the drop-down list to select the template that will be applied to the device that is being deployed. To view the details of the selected template, click on the **Get Staged Template Details** button. This will show any unique configuration settings that are included in the template for deployment to the device. Once satisfied that the correct template for the device being deployed has been selected, and that the configuration settings appear to be correct, click the **Provision Radio** button to start the process of deploying the template settings to the device. Status messages will be displayed during each step of the configuration process.



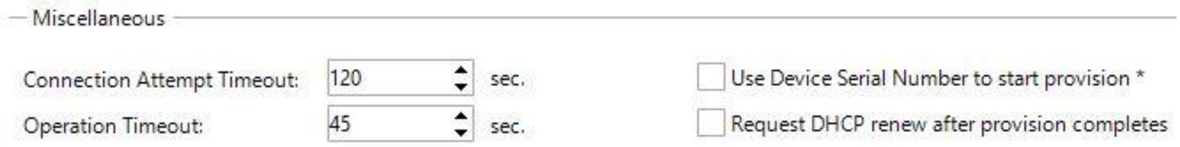
Staged Template: gregtest2222

Template: gregtest2222
Vendor: GE
Model: Orbit
Carrier:
Model:

```
GRE1 IP Address: 10.5.18.<cell-ip>/<mask>
LO1 IP Address: 10.11.<cell-ip>/<mask>
SCEP-Config CA Server #: 1
SCEP-Config CA Server Failover: No
SCEP-Config Country: US
```

Radio Admin Serial # Orbit AutoProvision

If the Provisioning Server administrator has locked specific device serial numbers to templates for deployment, the option to "Use Device Serial Number to Start Provision." is enabled for GE Orbit radios.



Connection Attempt Timeout: 120 sec.
Operation Timeout: 45 sec.

□ Use Device Serial Number to start provision *
□ Request DHCP renew after provision completes

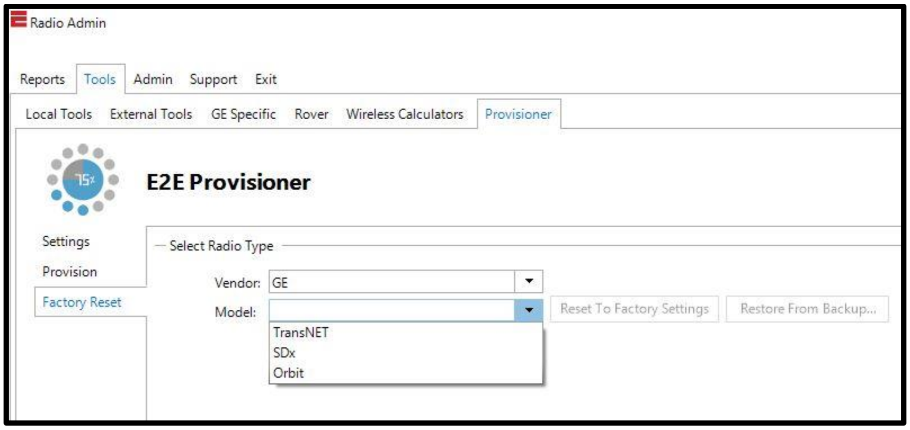
If this checkbox is selected, Radio Admin assumes a connection to an Orbit radio via Ethernet cable and that the Orbit has the factory default IP address (192.168.1.1). **Save Changes** must be clicked before the option will take effect.

Radio Admin will automatically connect to the Orbit radio, send its serial number to the Provisioning Server to obtain the correct template (where the serial number is staged in a template), and immediately begin applying the template settings to the Orbit device.

Radio Admin Factory Reset

To reset a GE MDS device to its factory default configuration values, navigate to the **Factory Reset** tab and select the vendor and model. Reset the device to its factory configuration settings by clicking on **Reset to Factory Settings**. Restore the configuration settings from a backup file by clicking **Restore from Backup**.

NOTE: If using an IP device, it must be set to the default of the device from the factory (i.e. 192.169.1.1).



Vendor: GE

How to Provision Devices

The initial steps for provisioning devices need to be done within GE LaunchNET using an Administrator user. This allows an administrator to create and stage company templates with the required parameters. Once the templates are set, any user can deploy them to the desired networks without fear of changing or tampering with the company-wide settings. The device inventory, template creation, and staging happens within GE LaunchNET, while the actual deployment happens within Radio Admin using the provisioner tooltab.

Zero-Touch Provisioning (ZTP) is a feature that allows devices to be provisioned and configured automatically. It eliminates most of the manual labor involved in adding radios or sensors to the network. Once the hardware is powered on, it will be automatically added to the network and instantly configured. This advanced network automation saves time and streamlines updates.

Create Device Inventory

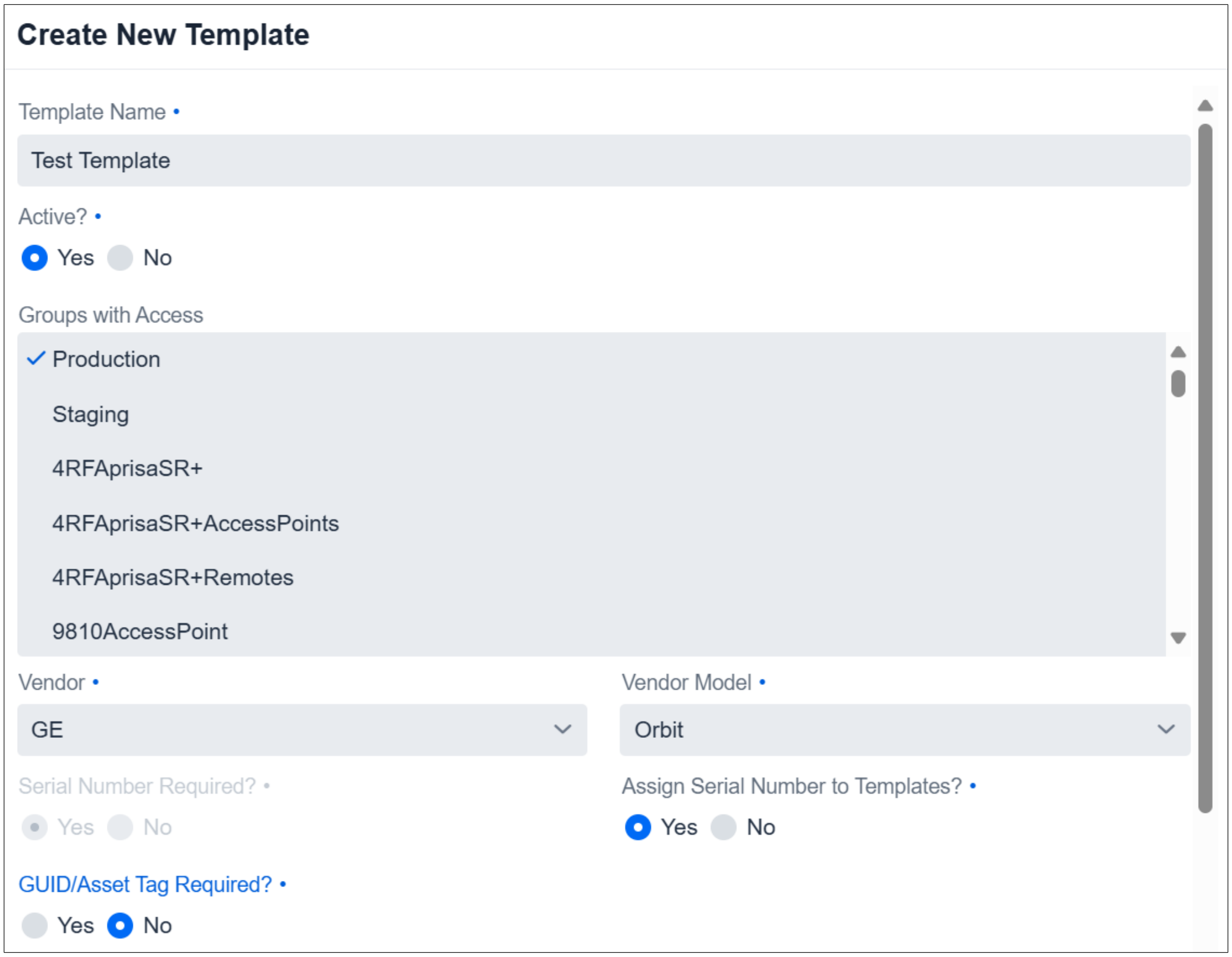
There are three ways to create a device inventory:

1. Connect to an existing external database (instructions for this are found in the Company Information section).
2. Import a CSV file of serial numbers or GUID tags using the **Import Inventory** button (instructions for this are found in the Device Inventory section).
3. Add device details manually using the **Add New** button (instructions for this are found in the **Device Inventory** section).

If the device inventory doesn't yet exist or doesn't contain the desired devices for the current deployment, use one of these methods to create the inventory of devices for provisioning. If the device inventory is already in the list of existing inventories, simply verify that it contains the specific devices that will be provisioned and that they are available (i.e., not marked as inactive or already provisioned elsewhere.)

Create Template

1. Under **LaunchNET > Provisioning > Template > Add**, input details, such as template name, groups that will have access, and device types/models. If needed, ensure "Serial Number Required" and "Assign Serial Number to Templates?" are set to **Yes**, and the template is marked "Active".



Create New Template

Template Name •

Test Template

Active? •

● Yes ○ No

Groups with Access

✓ Production

Staging

4RFAprisaSR+

4RFAprisaSR+AccessPoints

4RFAprisaSR+Remotes

9810AccessPoint

Vendor •

GE

Vendor Model •

Orbit

Serial Number Required? •

● Yes ○ No

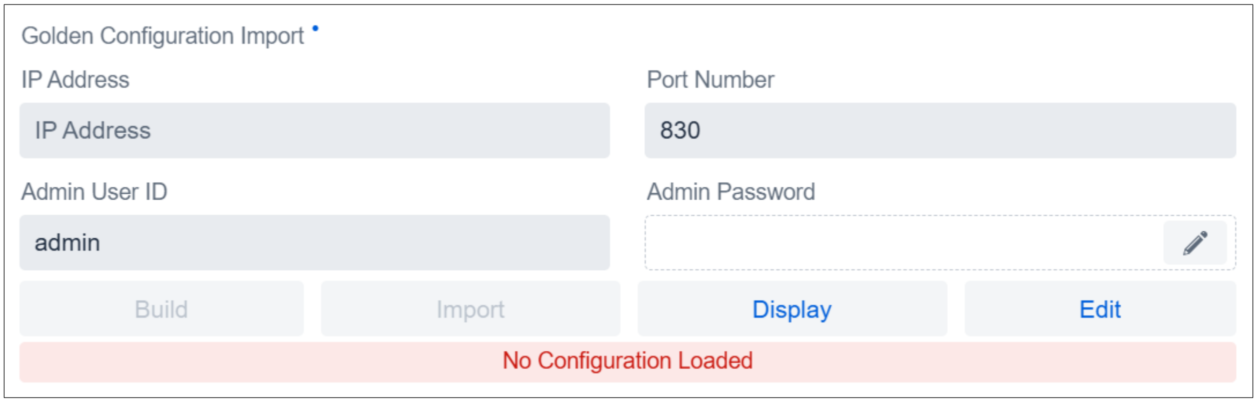
Assign Serial Number to Templates? •

● Yes ○ No

GUID/Asset Tag Required? •

○ Yes ● No

2. Under the **Golden Config** section, type the connection information for the reference device. These details will then be pushed out to all other selected devices in the network.



Golden Configuration Import •

IP Address

IP Address

Port Number

830

Admin User ID

admin

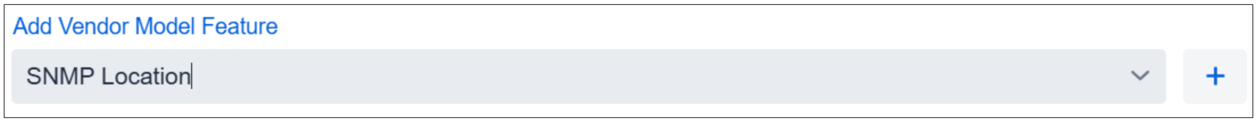
Admin Password

No Configuration Loaded

3. Once the connection details are set, click the **Build Golden Config** button. This will open the GE MDS Device Manager interface in a new window. Input desired changes and parameters here to set up the Golden Config device exactly the way the whole network is to be arranged. When finished, click **Save** to be returned to the **Provisioner Template** tab.

4. Click the **Import Golden Config** button to retrieve the new parameters from the poster child device. Click the **Display Golden Config** button to verify that all the updated changes have successfully been brought over from the poster child device.

5. From the **Vendor Model Feature List** drop-down menu, select any additional parameters not already included in the template or the GE MDS device manager window and fill in the required data. Once satisfied that all desired parameters and information have been set, click **Save**. The template is now prepared and ready to be released for provisioning.

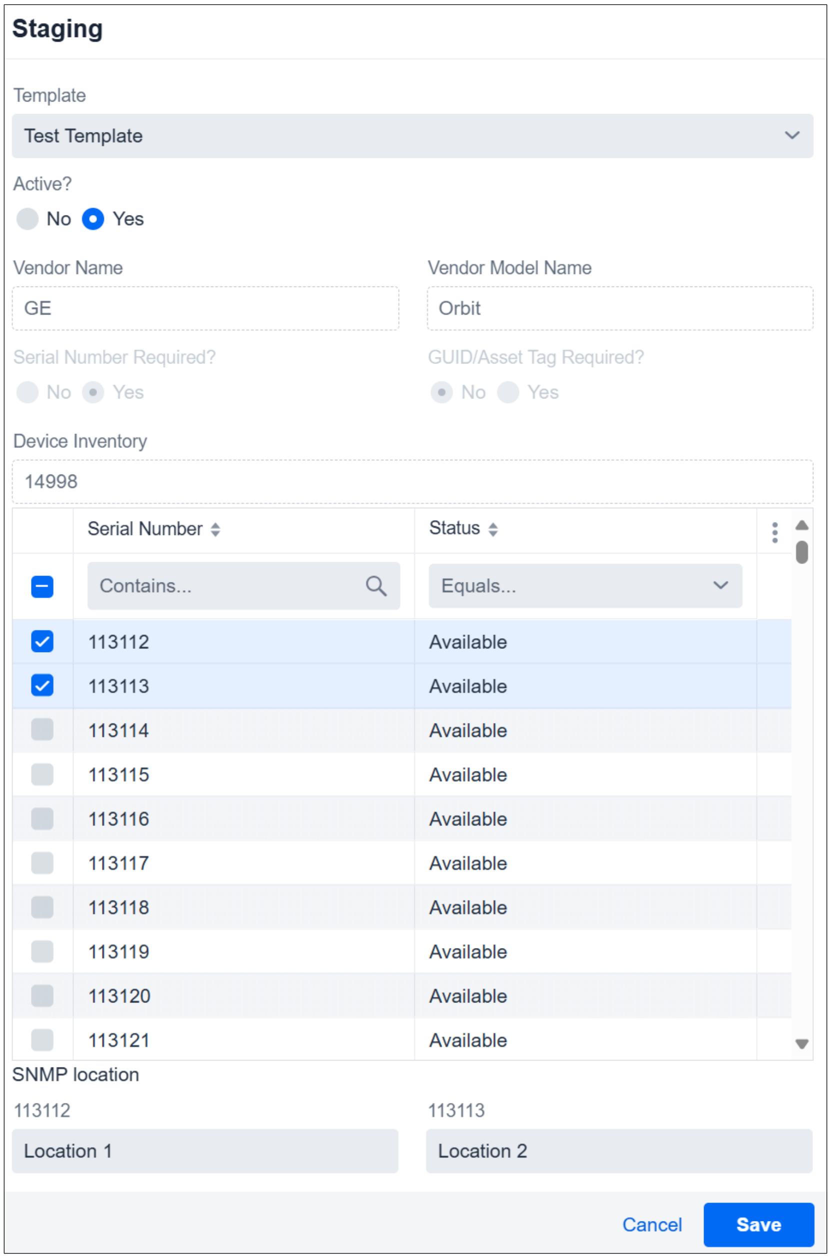

Add Vendor Model Feature

SNMP Location

Stage Template

All templates need to be staged (released for provisioning) before they will appear in the **Radio Admin Provisioner** tooltab. Only an Admin can create and stage templates.

1. Under **LaunchNET > Provisioning > Staging > Add**, select the desired template from the list of existing templates. (If not in the list, the template may not have been saved in the previous step or may not have been marked as **Active**.) Fill in the desired parameters and verify that existing parameters are correct. If attempting to re-run a previously staged or deployed template, it may need to be released first. This essentially resets the template to allow for a new deployment.



Staging

Template

Test Template

Active?

○ No ● Yes

Vendor Name: GE

Vendor Model Name: Orbit

Serial Number Required?

○ No ● Yes

GUID/Asset Tag Required?

● No ○ Yes

Device Inventory

14998

	Serial Number	Status
⊟	Contains...	Equals...
☑	113112	Available
☑	113113	Available
☐	113114	Available
☐	113115	Available
☐	113116	Available
☐	113117	Available
☐	113118	Available
☐	113119	Available
☐	113120	Available
☐	113121	Available

SNMP location

113112: Location 1

113113: Location 2

2. In the table select serial numbers to assign to the template in this staging.

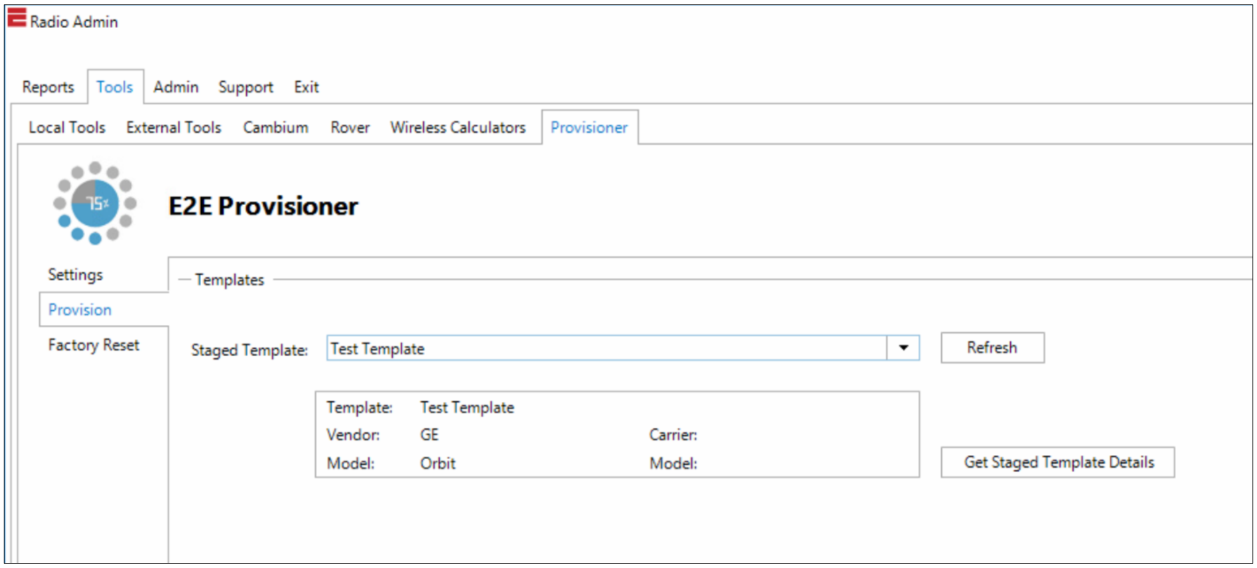
3. Verify that all information is correct, and click **Save**. The template has now been matched with the specific devices required for the provision, and those serial numbers will show up as “Staged” in the device inventory list. All

further steps will be taken care of by a User within the Radio Admin provisioner tooltab.

Provision Devices Using Radio Admin

1. Within Radio Admin, under **Tools > Provisioner > Settings**, enter the connection details. Ensure a correct username and password in order to connect the Radio Admin system to GE LaunchNET.

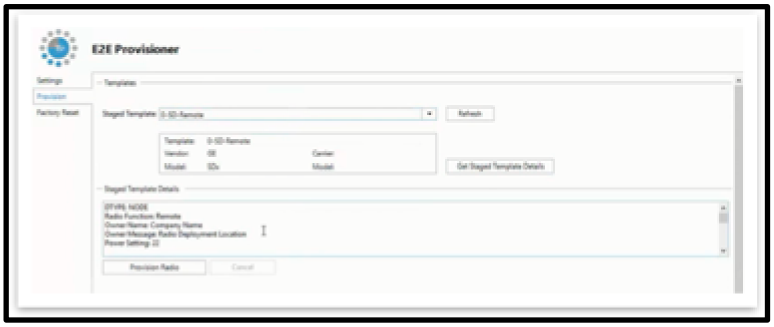
2. Under **Tools > Provisioner > Provision**, select the staged template to use to provision the devices from the **Staged Template** dropdown menu. (If the required template does not appear, the staged templates list may need to be refreshed. If it still does not appear, it may not have been properly staged.)



Staged Template: Test Template

Template: Test Template
Vendor: GE
Carrier:
Model: Orbit
Model:

All information should be contained in the staged template—device parameters, serial numbers, etc.—and can't be changed at this step. In the **Staged Template Details** box, verify that the parameters of the Golden Config are correct for the current provisioning attempt.



Staged Template: 0-SD-Remote

Template: 0-SD-Remote
Vendor: GE
Carrier:
Model: SDx
Model:

DTYPE: NODE
Radio Function: Remote
Owner Name: Company Name
Owner Message: Radio Deployment Location
Power Setting: 22

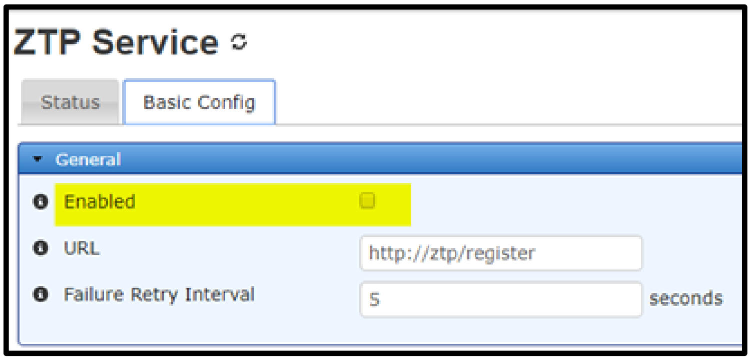
3. Once everything has been confirmed, click the **Provision Device** button. This will provision the required data to the selected devices. Depending on the number of devices being provisioned, the process may take several minutes.

Provision Devices Using ZTP

Zero Touch Provisioning (ZTP) is an advanced option using LaunchNET along with the capability of the GE Orbit radio. The customer will work with GE to include in the shipped radio a URL that the radio will access when it is powered on and with the ZTP option enabled as shown below.

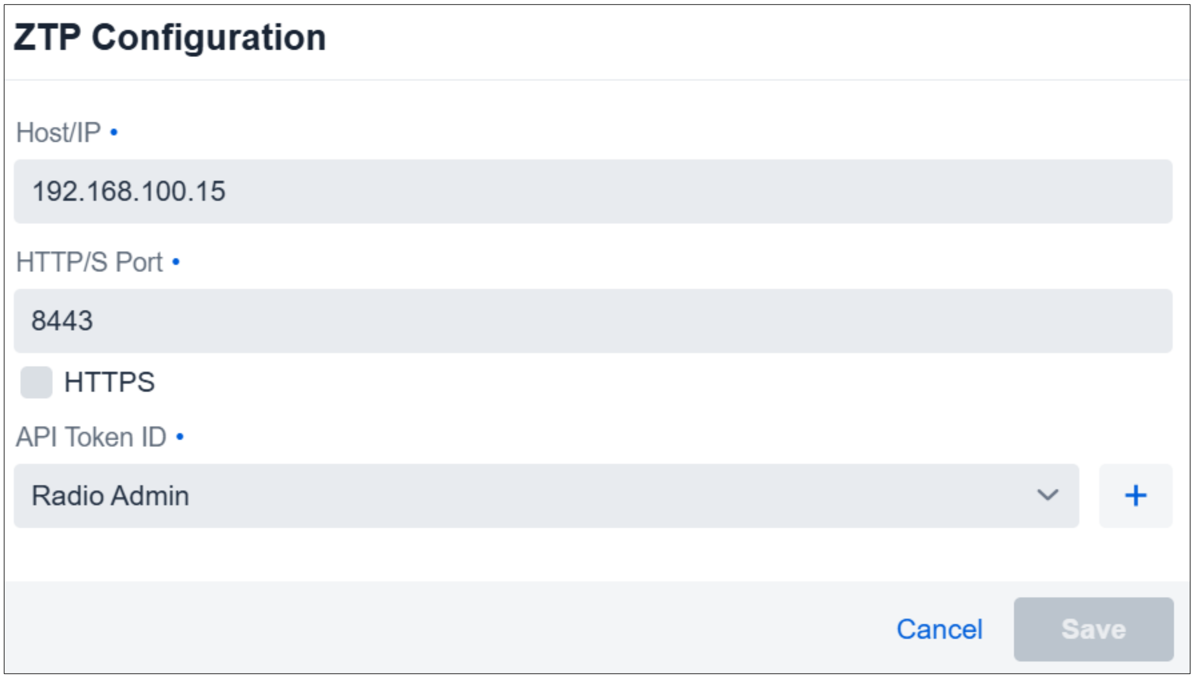
Orbit Radios

The Orbit radio must have the ZTP service enabled, and the URL must be pointed to the ZTP service (For example: http://192.168.1.1:8080/api/orbit/register):



Enabled ☐
URL http://ztp/register
Failure Retry Interval 5 seconds

On LaunchNET, navigate to **Administration > LaunchNET > Management > ZTP Configuration**. Here enter the host credentials that will be used for provisioning devices.



ZTP Configuration

Host/IP •

192.168.100.15

HTTP/S Port •

8443

□ HTTPS

API Token ID •

Radio Admin

Host: The IP where the ZTP Service is running.

HTTP/S Port: The Port where ZTP Service is running.

HTTPS: Enabled or Disabled. (Not supported)

API Token Name: The API Token that ZTP will use to communicate with LaunchNET (See API Tokens.)

NOTE: The API Token MUST have device level permissions to Provision a device Successfully.

In the **LaunchNET > Report > Deployments Completed** menu; history is kept for each provision attempt. **Note:** If a Staging attempt is later deleted, the Deployments Completed history for that staging attempt will also be removed.

ZTP will decrement the license count configured within GE LaunchNET/PulseNET as each radio is provisioned.

Addendum

Introduction

This document is intended for customers that have purchased the LaunchNET product and are wanting to interact with the LaunchNET's web services programmatically. The requests must be in the `Content-Type: application/json` with https.

The different endpoints are listed in the document and require authentication. The samples will have a "X-Sting-API-Key" that is associated with the user account per company. A device level API Token will need to be generated in order to make these calls. Please see Creating an API Token for information. The <> symbols show where customers will enter their own specific information.

Below is an example of a endpoint command:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @acstagedtemplates.json
<https://ipORhost:port>/api/e2em2m/userapi/acstagedtemplates
```

Insert the API token with device level privileges in the <insert API token here>

Insert LaunchNET's host and port information in the <https://ipORhost:port>

At the end of the url after "userapi/" is the endpoint in which is being called. The example above is using the acstagedtemplate (Auto-create Staged Templates) endpoint. This endpoint uses a request. To run this endpoint save a text file and insert the json formatted text from the Request. Save the json file where the call is being run.

Request:

```
{
  "templatename": "For Demo Use",
  "numbertobestaged": "1",
  "Serial_Number": "462346",
  "SNMP_Location": "North Pole”
}
```

Disclaimer

This software is provided “as is” and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

List of Staged Templates

This endpoint will respond with a list of templates that have been staged for provisioning. The response shows two templates.

Type: POST

CURL:

```
curl -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json" -X
POST -d"{}" <https://ipORhost:port>/api/e2em2m/userapi/templates
```

Sample Response:

```
{
  "status": "success",
  "payload": [
    {
      "tmpl_name": "For Demo Use",
      "vendor_name": "GE",
      "tmpl_id": "5fa31838487e092a4469e598",
      "vendor_need_guid": "No",
      "vendor_orbit_userid": "admin",
      "vendor_orbit_ipaddress": "192.168.1.1",
      "vendor_id": "5e78c57a8379a45944cefc80",
      "ext_inventory": "No",
      "vendor_model_name": "Orbit",
      "vendor_orbit_password": "admin",
      "assign_sernum": "Yes",
      "vendor_need_serial": "Yes",
      "vendor_orbit_portnum": "830"
    },
    {
      "tmpl_name": "Set Firewall Configuration",
      "vendor_name": "GE",
      "tmpl_id": "5fb56433306fba5bc86c5311",
      "vendor_need_guid": "No",
      "vendor_orbit_userid": "admin",
      "vendor_orbit_ipaddress": "192.168.1.1",
      "vendor_id": "5e78c57a8379a45944cefc80",
      "ext_inventory": "No",
      "vendor_model_name": "Orbit",
      "vendor_orbit_password": "admin",
      "assign_sernum": "Yes",
      "vendor_need_serial": "Yes",
      "vendor_orbit_portnum": "830"
    }
  ]
}
```

The information in the response informs the user of the name of the template, vendor name, vendor model, and if any serial number or GUID/Asset tags are required. In the response, the information that is relevant to the user is the “tmpl_id” value, as it will allow the user to get the staging details later.

List of Configured Templates

This endpoint will respond with a list of templates that are configured and ready to be staged.

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d"{}" <https://ipORhost:port>/api/e2em2m/userapi/configtemplates
```

Sample Response:

```
{
  "status": "success",
  "payload": [
    {
      "tmpl_name": "For Demo Use",
      "vendor_name": "GE",
      "tmpl_id": "5fa31838487e092a4469e598",
      "vendor_need_guid": "No",
      "vendor_orbit_userid": "admin",
      "vendor_orbit_ipaddress": "192.168.1.1",
      "vendor_id": "5e78c57a8379a45944cefc80",
      "ext_inventory": "No",
      "vendor_model_name": "Orbit",
      "vendor_orbit_password": "admin",
      "assign_sernum": "Yes",
      "vendor_need_serial": "Yes",
      "vendor_orbit_portnum": "830"
    },
    {
      "tmpl_name": "Set Firewall Configuration",
      "vendor_name": "GE",
      "tmpl_id": "5fb56433306fba5bc86c5311",
      "vendor_need_guid": "No",
      "vendor_orbit_userid": "admin",
      "vendor_orbit_ipaddress": "192.168.1.1",
      "vendor_id": "5e78c57a8379a45944cefc80",
      "ext_inventory": "No",
      "vendor_model_name": "Orbit",
      "vendor_orbit_password": "admin",
      "assign_sernum": "Yes",
      "vendor_need_serial": "Yes",
      "vendor_orbit_portnum": "830"
    }
  ]
}
```

Staged Template Details

This endpoint will respond with details of a specific template that has been staged for provisioning. The ‘tmpl’ (in the command in bold below) is from the previously requested list of templates.

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d"{\"tmpl\" :\"5fa31838487e092a4469e598\"}"
https://192.168.1.5:8443/api/e2em2m/userapi/provisions
```

Sample Response:

This response is for template id 5fa31838487e092a4469e598 and gives the vendor model features that will be set and to what value. Additionally, it will provide a placeholder for the serial numbers assigned as the devices are provisioned in the `vendormodelserialandguid` property. This shows how many are left for allocation. The “rpid” is also used in other endpoint’s requests.

```
{
  "status": "success",
  "payload": {
    "tmpl_name": "For Demo Use",
    "vendor_name": "GE",
    "tmpl_id": "5fa31838487e092a4469e598",
    "vendormodelserialandguid": [
      {
        "radio_serial": "2693708",
        "radio_guid": "",
        "rpid": "5fb6e1b2b6cd8e38dc402962"
      }
    ],
    "vendor_need_guid": "No",
    "vendor_orbit_userid": "admin",
    "vendor_orbit_ipaddress": "192.168.1.1",
    "vendor_id": "5e78c57a8379a45944cefc80",
    "ext_inventory": "No",
    "vendor_model_name": "Orbit",
    "vendor_orbit_password": "admin",
    "assign_sernum": "Yes",
    "vendor_need_serial": "Yes",
    "vendor_orbit_portnum": "830",
    "vendormodelfeatures": {
      "SNMP_Location": {
        "SNMP_Location_only_entered_if_assigned_by_Provisioner": {
          "0": "Saint Paul MN",
          "Comment": "data/system/location"
        },
        "SNMP_Location_Use_Selected_Interface": [
          "NA"
        ],
        "SNMP_Location_Assignment": [
          "Provisioner"
        ]
      },
      "GE-Orbit-Production-APN": [
        "mw01.VZWSTATIC"
      ],
      "GE-Orbit-Network_Interfaces_IP_Address_List_Settings_1": {
        "GE-Orbit-Network_Interface_IP_Address_List_Netmask_1": {
          "0": "30",
          "Comment":
"data/interfaces/interface[name='INTERFACEREPLACEME']/ipv4/address/prefix-length"
        },
        "GE-Orbit-Network_Interface_List_1": [
          "Cell"
        ],
        "GE-Orbit-Network_Interface_IP_Address_List_1": {
          "Comment":
"data/interfaces/interface[name='INTERFACEREPLACEME']/ipv4/address/ip",
          "Available": "192.168.1.1"
        }
      },
      "GE-Orbit_Generate_One-Time-Password": {
        "0": "Yes",
        "Comment_2": "<rpc xmlns=\\\"urn:ietf:params:xml:ns:netconf:base:1.0\\\" message-
id=\\\"0\\\"><otp-create xmlns=\\\"com:gemds:mds-
system\\\"><function>login</function></otp-create></rpc>"
      },
      "GE-Orbit-Tech-Password": {
        "0": "RosesAreRed123",
        "Comment": "rpc/change-password/password",
        "Comment_2": "<rpc xmlns=\\\"urn:ietf:params:xml:ns:netconf:base:1.0\\\" message-
id=\\\"0\\\"><change-password xmlns=\\\"com:gemds:mds-
system\\\"><user>tech</user><password></password></change-password></rpc>"
      },
      "GE-Orbit-Core": [
        "<data><logging xmlns=\"com:gemds:mds-logging\"><debug><devel-log-
enabled>false</devel-log-enabled></debug></logging><services xmlns=\"com:gemds:mds-
services\"><dhcp xmlns=\"com:gemds:dhcp-
service\"><enabled>true</enabled><v4subnet><network>192.168.1.0/24</network><range-
start>192.168.1.2</range-start><range-end>192.168.1.10</range-end><broadcast-
address>192.168.1.255</broadcast-
address><router>192.168.1.1</router></v4subnet></dhcp><serial xmlns=\"com:gemds:mds-
serial\"><ports><name>COM1</name></ports><ports><name>COM2</name></ports><ports><name>USB
1</name></ports><console><serial-ports>COM1</serial-ports><serial-ports>COM2</serial-
ports><serial-ports>USB1</serial-ports></console></serial><remote-management
xmlns=\"com:gemds:mds-service-remote-management\"><shared-
secret>$8$GkYKxwVhFROclh4EM1OMN8dRDyQQc1mEa6bCxq99f94=</shared-secret></remote-
management><firewall
xmlns=\"com:gemds:services:firewall\"><enabled>false</enabled><address-set><name>LOCAL-
NETS</name><addresses>192.168.1.0/24</addresses></address-
set><filter><name>IN_TRUSTED</name><rule><id>10</id><match><protocol>all</protocol></matc
h><actions><action>accept</action></actions></rule></filter><filter><name>IN_UNTRUSTED</n
ame><rule><id>1</id><match><protocol>icmp</protocol></match><actions><action>accept</acti
on></actions></rule><rule><id>2</id><match><protocol>udp</protocol><src-
port><services>dns</services></src-
port></match></rule><rule><id>3</id><match><protocol>tcp</protocol><dst-
port><services>https</services><services>netconf</services><services>ssh</services></dst-
port></match><actions><action>accept</action></actions></rule><rule><id>10</id><match><pr
otocol>all</protocol></match><actions><action>drop</action></actions></rule></filter><fil
```

```
ter><name>OUT_TRUSTED</name><rule><id>10</id><match><protocol>all</protocol></match><acti
ons><action>accept</action></actions></rule></filter><filter><name>OUT_UNTRUSTED</name><r
ule><id>1</id><match><src-address><address-set>LOCAL-NETS</address-set><add-interface-
address>true</add-interface-address></src-
address></match><actions><action>accept</action></actions></rule><rule><id>10</id><match>
<protocol>all</protocol></match><actions><action>drop</action></actions></rule></filter><
nat><source><rule-set><name>MASQ</name><rule><id>1</id><source-nat><interface/></source-
nat></rule></rule-set></source></nat></firewall><netconf
xmlns=\"com:gemds:services:netconf\"><enabled>true</enabled><port>830</port></netconf><sn
mp
xmlns=\"com:gemds:services:snmp\"><agent><enabled>true</enabled><port>161</port><version>
<v1/><v2c/><v3/></version><engine-id><enterprise-number>4130</enterprise-number><from-
text>00:06:3d:09:94:b3</from-text></engine-id><max-message-size>50000</max-message-
size><debug-enabled>false</debug-
enabled></agent><system/><community><index>public</index><sec-name>public</sec-
name></community><vacm><group><name>all-rights</name><member><sec-name>public</sec-
name><sec-model>v1</sec-model><sec-model>v2c</sec-model><sec-model>usm</sec-
model></member><access><sec-model>any</sec-model><sec-level>no-auth-no-priv</sec-
level><read-view>internet</read-view><write-view>internet</write-view><notify-
view>internet</notify-
view></access></group><view><name>internet</name><subtree><oids>1.3.6.1</oids><included/>
</subtree></view></vacm></snmp><ssh
xmlns=\"com:gemds:services:ssh\"><enabled>true</enabled><port>22</port></ssh><web
xmlns=\"com:gemds:services:web\"><http><enabled>false</enabled><port>80</port></http><htt
ps><enabled>true</enabled><port>443</port></https></web></services><interfaces
xmlns=\"urn:ietf:params:xml:ns:yang:ietf-interfaces\"><interface><name>Bridge</name><type
xmlns:mds_bridge=\"com:gemds:mds-if-bridge\">mds_bridge:bridge</type><bridge-settings
xmlns=\"com:gemds:mds-if-
bridge\"><members><port><interface>ETH1</interface></port><port><interface>ETH2</interfac
e></port><port><interface>ETH3</interface></port><port><interface>ETH4</interface></port>
<wifi-ap><ssid>GEMDS_2693708</ssid></wifi-ap></members><stp-mode>disabled</stp-
mode></bridge-settings><filter
xmlns=\"com:gemds:services:firewall\"><input>IN_TRUSTED</input><output>OUT_TRUSTED</outpu
t></filter><ipv4                                 xmlns=\"urn:ietf:params:xml:ns:yang:ietf-
ip\"><address><ip>192.168.1.1</ip><prefix-length>24</prefix-
length></address></ipv4></interface><interface><name>Cell</name><type
xmlns:mds_cell=\"com:gemds:mds-if-cell\">mds_cell:cellular</type><cell-config
xmlns=\"com:gemds:mds-if-cell\"><connection-profile><name>Production</name><bearer-
config><apn>mw01.VZWSTATIC</apn></bearer-config></connection-profile></cell-
config><filter
xmlns=\"com:gemds:services:firewall\"><input>IN_UNTRUSTED</input><output>OUT_UNTRUSTED</o
utput></filter><nat xmlns=\"com:gemds:services:firewall\"><source>MASQ</source></nat><ipv4
xmlns=\"urn:ietf:params:xml:ns:yang:ietf-ip\"><dhcp                  xmlns=\"com:gemds:mds-
interfaces\"><point-to-point-connection>true</point-to-point-
connection></dhcp></ipv4></interface><interface><name>ETH1</name><type
xmlns:mdsif=\"com:gemds:mds-
interfaces\">mdsif:ethernet</type></interface><interface><name>ETH2</name><type
xmlns:mdsif=\"com:gemds:mds-
interfaces\">mdsif:ethernet</type></interface><interface><name>ETH3</name><type
xmlns:mdsif=\"com:gemds:mds-
interfaces\">mdsif:ethernet</type></interface><interface><name>ETH4</name><type
xmlns:mdsif=\"com:gemds:mds-
interfaces\">mdsif:ethernet</type></interface><interface><name>Wi-Fi</name><type
xmlns:mds_wifi=\"com:gemds:mds-if-ieee80211\">mds_wifi:wifi</type><wifi-config
xmlns=\"com:gemds:mds-if-ieee80211\"><mode>access-point</mode><ap-
config><ap><ssid>GEMDS_2693708</ssid><broadcast-ssid>true</broadcast-ssid><privacy-
mode>wpa2-personal</privacy-mode><psk-
```

```
config><psk>$8$ILYU6U/5ztK/DJ8dPflflXMHDq0kEKzFc7fs+cnOgAc=</psk></psk-config></ap></ap-
config></wifi-config></interface></interfaces><system
xmlns=\"urn:ietf:params:xml:ns:yang:ietf-system\"><ntp><use-ntp>false</use-
ntp></ntp><simple-web-mode               xmlns=\"com:gemds:mds-system\">false</simple-web-
mode></system></data>"
      ],
      "SNMP_Contact": {
        "SNMP_Contact_only_entered_if_assigned_by_Provisioner": {
          "0": "Brandon",
          "Comment": "data/system/contact"
        },
        "SNMP_Contact_Assignment": [
          "Provisioner"
        ]
      }
    }
  }
}
```

Auto-Create Staged Template Entry

This endpoint will allow an external system to automatically create a staged template entry.

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @acstagedtemplates.json
<https://ipORhost:port>/api/e2em2m/userapi/acstagedtemplates
```

Request:

```
      {
        "templatename": "For Demo Use",
        "numbertobestaged": "1",
        "Serial_Number": "2693708",
        "SNMP_Location": "North Pole”
      }
```

Required:

- “templatename” is the name of the template to be staged
- “numbertobestaged” is the number of the devices for the template to stage [this is a value of “1” for devices where the serial number is being sent –if no serial number, then it can be up to a value of “9999”]

Optional:

Each of the features may be selected in the request. If the feature has an option for LaunchNET or Radio Admin, the feature must be set to LaunchNET to allow for the API to function correctly:

- “Serial_Number” is for the device to be created and assigned to the template (if the template requires a serial number)
- “SNMP_Location” is for the SNMP Location text (if the template has this feature)
- “SNMP_Contact” is for the SNMP Contact text (if the template has this feature

Additional Notes:

1. SNMP Location has a drop-down for “Use Selected Interface”, except for the value “NA”. If the contents equal one of the selections (i.e., “Bridge”), then the value for the “SNMP Location (Use Selected Interface)” would be set to the value sent. Otherwise, the “SNMP Location (only entered if assigned by LaunchNET)” would have the sent value. Default value is “NA” for the “SNMP Location (Use Selected Interface)” field.
2. When the SNMP Contact and SNMP Location are added, the admin has the option to have Radio Admin set the value or use the value that is in LaunchNET in the template. Those feature entries must be in the template AND they must be set to LaunchNET to be processed via the API. For serial number (the other optional property), if it is required by the template and the web request doesn’t have it, the web request will be ignored. Also, SNMP Location and SNMP Contact will be ignored if the template doesn’t contain those features.

Sample Response:

```
{
        "status": "success",
        "message": "<On success, return the record number. On failure, message for failure>"
}
```

Status can be ‘success’ or ‘failure’.

Import Inventory

This endpoint will allow the user to import inventory as ‘Available’ to LaunchNET.

Type: POST

URL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @importinventory.json
<https://ipORhost:port>/api/e2em2m/userapi/importinventory
```

Request:

```
{
        "vendor": "GE",
        "model": "Orbit",
        "Inventory": [{
                        "serial": "25501318",
                        "guid": "GE-0000002550138"
                },
                {
                        "serial": "25501319",
                        "guid": "GE-0000002550139"
                }
        ]
}
```

Note that the payload is listed in pairs of serial and guid (which can be an asset tag as well) whether they are populated or not. However, one of them must be populated. Additionally, if you are populating GE Orbits for the guid, it must be in the format of a GE asset tag (i.e., GE-000000<serial number>).

The vendor name and vendor model name must be populated correctly. Please review your user interface for your appropriate selection options, spelling, and syntax. If these are not correct, your import will fail.

```
{
        "vendor": "GE",
        "model": "Orbit",
        "Inventory": [{
                        "serial": "25501318",
                        "guid": ""
                },
                {
                        "serial": "25501319",
                        "guid": ""
                }
        ]
}
```

Where guid may be “” if not being used.

Sample Response:

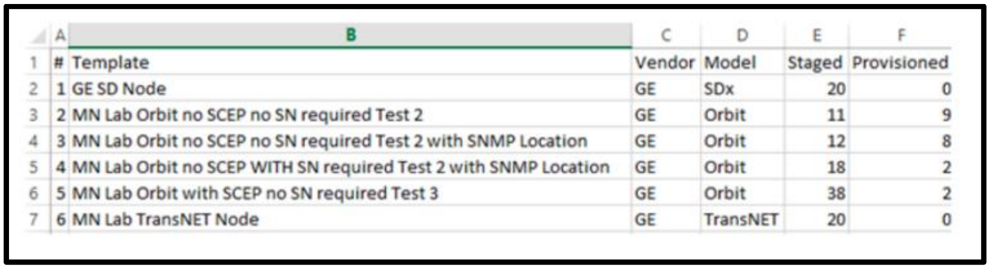
```
{
        "status": "success"
}
```

OR

```
{
        "status": "failure"
}
```

Export Deployments List

This endpoint allows the user to export the information just as they can in the UI for the ‘Export List as CSV’ in the Deployments Completed of the Reports section. Below is a sample of the output from the UI as a CSV.



	A	B	C	D	E	F
1	#	Template	Vendor	Model	Staged	Provisioned
2	1	GE SD Node	GE	SDx	20	0
3	2	MN Lab Orbit no SCEP no SN required Test 2	GE	Orbit	11	9
4	3	MN Lab Orbit no SCEP no SN required Test 2 with SNMP Location	GE	Orbit	12	8
5	4	MN Lab Orbit no SCEP WITH SN required Test 2 with SNMP Location	GE	Orbit	18	2
6	5	MN Lab Orbit with SCEP no SN required Test 3	GE	Orbit	38	2
7	6	MN Lab TransNET Node	GE	TransNET	20	0

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @exportdeploymentlist.json
<https://ipORhost:port>/api/e2em2m/userapi/exportdeploymentlist
```

Request:

```
{
        "template": "For Demo Use"
}
```

If all deployments are needed in a report run the following command without using a json:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d {} <https://ipORhost:port>/api/e2em2m/userapi/exportdeploymentlist
```

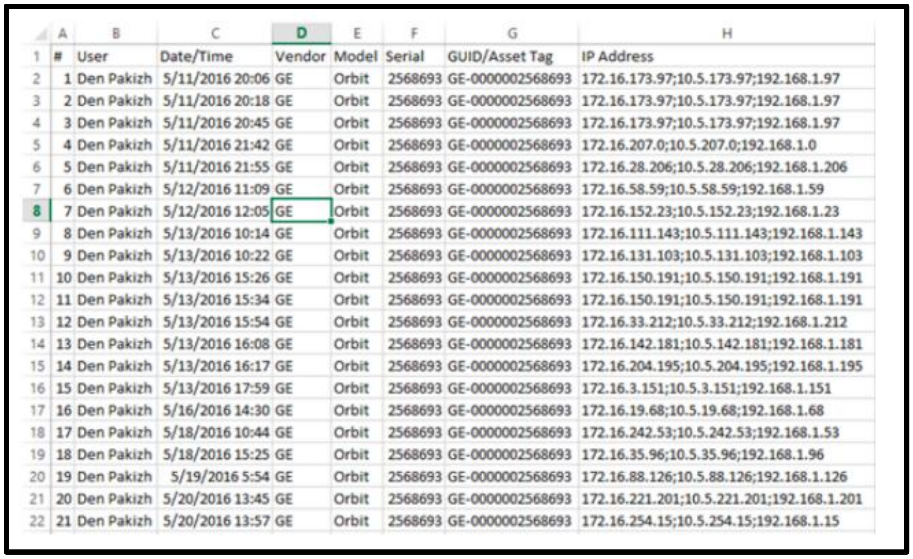
Sample Response:

This response below tells the user that there are 2 templates and lists how many devices were staged & provisioned.

```
{
  "status": "success",
  "payload": [
    {
      "Staged": 2,
      "Failed": 0,
      "Model": "Orbit",
      "Vendor": "GE",
      "Provisioned": 1,
      "Template": "For Demo Use"
    },
    {
      "Staged": 1,
      "Failed": 0,
      "Model": "Orbit",
      "Vendor": "GE",
      "Provisioned": 0,
      "Template": "For Demo Use"
    }
  ]
}
```

Export Deployment Details

This endpoint allows the user to export the information just as they can in the UI for the 'Export Details as CSV' in the Deployments Completed of the Reports section. Below is a sample of the output from the UI as a CSV.



	A	B	C	D	E	F	G	H
1	#	User	Date/Time	Vendor	Model	Serial	GUID/Asset Tag	IP Address
2	1	Den Pakizh	5/11/2016 20:06	GE	Orbit	2568693	GE-0000002568693	172.16.173.97;10.5.173.97;192.168.1.97
3	2	Den Pakizh	5/11/2016 20:18	GE	Orbit	2568693	GE-0000002568693	172.16.173.97;10.5.173.97;192.168.1.97
4	3	Den Pakizh	5/11/2016 20:45	GE	Orbit	2568693	GE-0000002568693	172.16.173.97;10.5.173.97;192.168.1.97
5	4	Den Pakizh	5/11/2016 21:42	GE	Orbit	2568693	GE-0000002568693	172.16.207.0;10.5.207.0;192.168.1.0
6	5	Den Pakizh	5/11/2016 21:55	GE	Orbit	2568693	GE-0000002568693	172.16.28.206;10.5.28.206;192.168.1.206
7	6	Den Pakizh	5/12/2016 11:09	GE	Orbit	2568693	GE-0000002568693	172.16.58.59;10.5.58.59;192.168.1.59
8	7	Den Pakizh	5/12/2016 12:05	GE	Orbit	2568693	GE-0000002568693	172.16.152.23;10.5.152.23;192.168.1.23
9	8	Den Pakizh	5/13/2016 10:14	GE	Orbit	2568693	GE-0000002568693	172.16.111.143;10.5.111.143;192.168.1.143
10	9	Den Pakizh	5/13/2016 10:22	GE	Orbit	2568693	GE-0000002568693	172.16.131.103;10.5.131.103;192.168.1.103
11	10	Den Pakizh	5/13/2016 15:26	GE	Orbit	2568693	GE-0000002568693	172.16.150.191;10.5.150.191;192.168.1.191
12	11	Den Pakizh	5/13/2016 15:34	GE	Orbit	2568693	GE-0000002568693	172.16.150.191;10.5.150.191;192.168.1.191
13	12	Den Pakizh	5/13/2016 15:54	GE	Orbit	2568693	GE-0000002568693	172.16.33.212;10.5.33.212;192.168.1.212
14	13	Den Pakizh	5/13/2016 16:08	GE	Orbit	2568693	GE-0000002568693	172.16.142.181;10.5.142.181;192.168.1.181
15	14	Den Pakizh	5/13/2016 16:17	GE	Orbit	2568693	GE-0000002568693	172.16.204.195;10.5.204.195;192.168.1.195
16	15	Den Pakizh	5/13/2016 17:59	GE	Orbit	2568693	GE-0000002568693	172.16.3.151;10.5.3.151;192.168.1.151
17	16	Den Pakizh	5/16/2016 14:30	GE	Orbit	2568693	GE-0000002568693	172.16.19.68;10.5.19.68;192.168.1.68
18	17	Den Pakizh	5/18/2016 10:44	GE	Orbit	2568693	GE-0000002568693	172.16.242.53;10.5.242.53;192.168.1.53
19	18	Den Pakizh	5/18/2016 15:25	GE	Orbit	2568693	GE-0000002568693	172.16.35.96;10.5.35.96;192.168.1.96
20	19	Den Pakizh	5/19/2016 5:54	GE	Orbit	2568693	GE-0000002568693	172.16.88.126;10.5.88.126;192.168.1.126
21	20	Den Pakizh	5/20/2016 13:45	GE	Orbit	2568693	GE-0000002568693	172.16.221.201;10.5.221.201;192.168.1.201
22	21	Den Pakizh	5/20/2016 13:57	GE	Orbit	2568693	GE-0000002568693	172.16.254.15;10.5.254.15;192.168.1.15

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @exportdeploymentdetails.json
<https://ipORhost:port>/api/e2em2m/userapi/exportdeploymentdetails
```

Request with json information:

```
{
  "template": "For Demo Use"
}
```

If all deployments are needed in a report run the following command without using a json:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d {} <https://ipORhost:port>/api/e2em2m/userapi/exportdeploymentdetails
```

Sample Response:

This response tells you what the users have deployed and associated details.

```
{
  "status": "success",
  "payload": [
    {
      "Serial": "2693708",
      "IP Address": "Bridge - 192.168.1.1",
      "User": "admin",
      "GUID/Asset Tag": null,
      "Date/Time": "11/19/2020 01:26:16 PM",
      "Model": "Orbit",
      "Vendor": "GE"
    }
  ]
}
```

Release a Staged Device

This endpoint will release a device from being staged and if a local inventory, set it to a status of ‘Available’.

It can work in two scenarios. It can work on "rpid" as well as serial number, requiring only one of them at a time. If both are passed then "rpid" is used. So, at least one of "rpid" or "serial" is always required. "guid" is always optional.

"rpid": - Lookup by "rpid" is the best bet for the job so this should be used whenever possible. If passed then other two params would be skipped. The “rpid” is found in the provisions endpoint.

"serial": If "rpid" is not available then this is the only other option "serial" is required if "rpid" key is not present.

"guid": This is optional but can be passed with "serial" to make the lookup stronger. This should be passed whenever possible with serial even if it’s optional.

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @releaseserial.json <https://ipORhost:port>/api/e2em2m/userapi/releaseserial
```

Request:

```
{
      "rpid":"5fb6c45eb6cd8e4b7c726970",
      "serial":"4353522",
      "guid":"4353522"
}
```

Sample Response:

This response simply tells you success or failure on releasing the device.

Success Response:

```
{
   "status":"success",
   "payload":""
}
```

Error Response:

```
{
   "status":"error",
   "payload":"<error message>"
}
```

Report a Failed Deployment

This endpoint allows a report of a failed provision deployment.

Type: POST

CURL:

```
curl -k -H "X-Sting-API-Key: <Insert API Token Here>" -H "Content-Type: application/json"
-X POST -d @reportfaileddeployment.json
<https://ipORhost:port>/api/e2em2m/userapi/reportfaileddeployment
```

Request:

```
{
      "rpid":"5fb6e1b2b6cd8e38dc402962",
      "serial":"2693708",
      "remarks":"Testing reporting of deployment failure."
}
```

Sample Response:

This response simply tells you success or failure reporting a failure of a deployment.

Success Response:

```
{
   "status":"success",
   "payload":""
}
```

Error Response:

```
{
   "status":"error",
   "payload":"<error message>"
}
```

DisengageSerial Endpoint Commands

The "disengageserial" endpoint marks all stagings that match the serial number as "Released". By default, the endpoint works only on "Staged" stagings, but it has an optional input variable named "include_deployed", which expects a boolean value string, and if that variable is given a true/positive value then the endpoint works on "Deployed" stagings as well. The endpoint also marks inventory as "Available" if the serial number is present in inventory and also increments the license count as per the number of stagings released.

URL: https://<hostname>/e2em2m/index.php/userapi/disengageserial

The input json structure is given below:

```
{
"payload": {
"serial": "xxxxxx",
"include_deployed": <optional, a boolean value as given below>
},
"username": "xxxxx",
"password": "xxxxx",
"ruk": "xxxxx"
}
```

Valid values for "include_deployed" can be any value that can be resolved to a corresponding boolean value. The valid values are: 0, f, F, false, False, FALSE, n, N, no, No, NO, 1, t, T, true, True, TRUE, y, Y, yes, Yes, YES.

This returns a Json with the below structure:

```
{
"status": "success" OR "error",
"payload": "<a description in case of error, blank if success>"
}
```

Below is a release stagings sample as a reference.

Release a Staged Device

This endpoint will release a device from being staged and if a local inventory, set it to a status of ‘Available’.

It can work in two scenarios. It can work on "rpid" as well as serial number, requiring only one of them at a time. If both are passed, then "rpid" is used. So, at least one of "rpid" or "serial" is always required. "guid" is always optional.

"rpid": Lookup by "rpid" is the best bet for the job so this should be used whenever possible. If passed, then the other two parameters would be skipped.

"serial": If "rpid" is not available then this is the only other option "serial" is required if "rpid" key is not present.

"guid": This is optional but can be passed with "serial" to make the lookup stronger. This should be passed whenever possible with serial even if it’s optional.

Type: POST

URL: https://<hostname>/e2em2m/index.php/userapi/releaseserial

Request:

```
{
"username":"username",
"password":"userpassword",
"ruk":"rukchr",
"payload":{
"rpid":"66",
"serial":"XXXX",
"guid":"YYYY"
}
```

Sample Response:

This response simply tells you success or failure on releasing the device.

Success Response:

```
{
"status":"success",
"payload":""
}
```

Error Response:

```
{
"status":"error",
"payload":"<error message>"
}
```

E2E Copyright Notice

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use without the written permission of End 2 End Technologies, LLC.

The information in this document is provided in connection with E2E products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of E2E products.

EXCEPT AS SET FORTH IN E2E'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, E2E ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED, OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL E2E BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF E2E HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

E2E makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. E2E does not make any commitment to update the information contained in this document.

About End 2 End Technologies

End 2 End (E2E) Technologies offers a unique combination of wireless communications and information technology expertise. We improve efficiency, reduce risk, and lower the cost of industrial field operations via modernization and management of our customer's wireless communications networks. From initial planning through lifecycle support, we assist your team in adopting a wireless solution that keeps communication costs low while maximizing network reliability and performance. For more information visit us at www.e2etechinc.com.

E2E TECHNOLOGIES

License Credits

LaunchNET and Radio Admin contain several third-party components, which are credited here.

Apache License 2.0

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Brainboxes.IO: Copyright 2015 by Brainboxes Limited

This is free and unencumbered software released into the public domain. Anyone is free to copy, modify, publish, use, compile, sell, or distribute this software, either in source code form or as a compiled binary, for any purpose commercial or non-commercial, and by any means. In jurisdictions that recognize copyright laws, the author or authors of this software dedicate any and all copyright interest in the software to the public domain. We make this dedication for the benefit of the public at large and to the detriment of our heirs and successors. We intend this dedication to be an overt act of relinquishment in perpetuity of all present and future rights to this software under copyright law.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION

Newtonsoft: Commercial Software License

OpenSSL License

PHP License

RENCI SSH.net: Copyright 2010 RENCI

Licensed under the terms of the new BSD license Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of RENCI nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Syslog Sharp

Licensed under the terms of the GNU LESSER GENERAL PUBLIC LICENSE, Version 3, 29 June 2007; https://www.gnu.org/licenses/lgpl.html.

SharpSNMPlib: Copyright 2008 Malcolm Crowe, Lex Li, and other contributors

Licensed under the terms of the MIT License. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON INFRINGEMENT.

IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Telerik UI for WinForms

Subject to the terms of this Agreement, You are granted a limited, non-transferable, royalty-free license to redistribute and sublicense the use of the Programs solely to Authorized End-Users: (i) in object code form only; (ii) as embedded within Your Integrated Product for internal company use, hosted applications, websites, commercial solutions deployed at Your Authorized End Users sites, or shrink- or click-wrapped software solutions; and (iii) pursuant to an end user license agreement or terms of use that: imposes the limitations set forth in this paragraph on Your Authorized End-Users; prohibits distribution of the Programs by Your Authorized End-Users; limits the liability of Your licensors or suppliers to the maximum extent permitted by applicable law; and prohibits any attempt to disassemble the code, or attempt in any manner to reconstruct, discover, reuse or modify any source code or underlying algorithms of the Programs, except to the limited extent as is permitted by law notwithstanding contractual prohibition. In no event are You allowed to distribute the Software or sublicense its use (a) in any format other than in object form, (b) as a standalone product, or (c) as a part of any product other than Your Integrated Product.