Digi Remote Manager

User Guide

Trademarks and copyright

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Digi International. Digi provides this document "as is," without warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of fitness or merchantability for a particular purpose. Digi may make improvements and/or changes in this manual or in the product(s) and/or the program(s) described in this manual at any time.

Warranty

To view product warranty information, go to the following website:

www.digi.com/howtobuy/terms

Customer support

Gather support information: Before contacting Digi technical support for help, gather the following information:

- Product name and model
- Product serial number (s)
- Firmware version
- Operating system/browser (if applicable)
- Logs (from time of reported issue)
- Trace (if possible)
- Description of issue
- Steps to reproduce

Contact Digi technical support: Digi offers multiple technical support plans and service packages. Contact us at +1 952.912.3444 or visit us at www.digi.com/support.

Feedback

To provide feedback on this document, email your comments to

techcomm@digi.com

Include the document title and part number (Digi Remote Manager User Guide, 90002349 n) in the subject line of your email.

Contents

Welcome

Map

Alerts

Reports

Data Streams

Health

Devices

Configurations

Automations

Subscriptions

Users and accounts

Notifications

Logs

API explorer

Monitors

Previous release notes

Welcome

Welcome to the Digi Remote Manager®

Click What's new in February 2024 for details on what's new in the latest release of Digi Remote Manager.

This chapter contains the following topics:

What's new in February 2024

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There were no security related changes.

Enhancements

For February 27, 2024

- Account Selector doesn't save reset state
- Fetch data and show single device results
- Kick off Ookla Speedtest and show test running modal
- Allow specifying minimum device version when uploading/modifying device firmware
- API Explorer should pass error body back to the caller
- Confusing language in header message | Out of date firmware

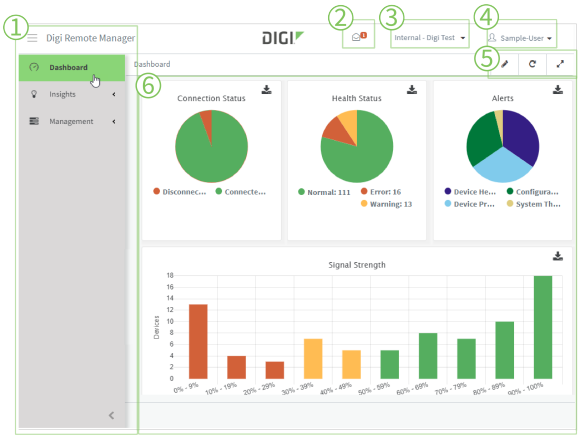
About Digi Remote Manager

Digi Remote Manager is a cloud-based device management and data enablement platform that makes it easy to connect your application to the data on which your business relies. With Remote Manager, you can efficiently interact with any device or device data in your Remote Manager inventory. You can:

- Ensure your devices are up to date by automatically applying security patches, firmware, and configurations.
- Monitor the state of all of your devices to quickly identify, assess, and respond to issues.
- Set up custom alerts to inform you that an issue requires your attention.
- Automate remediation for devices out of compliance.
- Deploy application logic to any devices, such as routers and gateways.

Dashboard

When you log into Digi Remote Manager, the **Dashboard** appears. The Dashboard contains menus to access Remote Manager operations, and widgets that display device health and status information.



Components common to every page in Remote Manager

#	Component	Description
1	Remote Manager main menu	Provides quick access to Remote Manager functionality. Click or to show/hide the main menu.
2	Notifications	Click to display notifications. ▪ Click the notification to mark it as read. ▪ Click **Mark all as read** to mark all notifications as read. ▪ For each notification, click to access a menu: • **Open Notification** opens the **Notifications** window. • If a notification has been read, **Mark as Unread** marks the notification as unread. • **Save** the notification. • **Delete** the notification
3	Account menu	If there are sub-accounts associated with this account, search or select a sub-account.
4	User menu	Provides access to additional Remote Manager functionality, including: ▪ The legacy Classic Remote Manager user interface. ▪ Remote Manager documentation. ▪ User configuration options. ▪ Feedback. ▪ Terms of Service ▪ **Logout**.

Components specific to the Dashboard

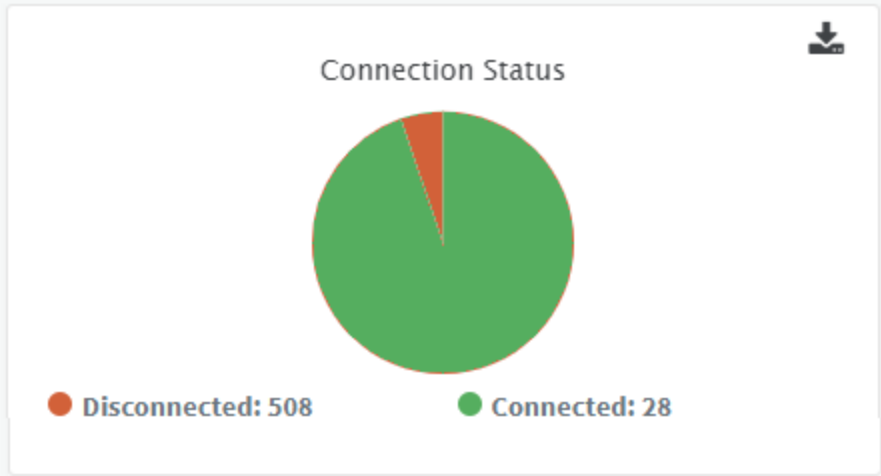
#	Component	Description
5	Toolbar	Edit the widgets displayed in the dashboard. Refresh the information displayed by the widgets. Make the widget display full screen.
6	Widgets	See Dashboard widgets.

Dashboard widgets

Several widgets are available for display in the Remote Manager dashboard. You can add, remove and resize widgets, and you can restore the default widget display. See Customize your dashboard for information about customizing the dashboard.

Connection Status widget

The **Connection Status** widget shows a summary of the number of devices connected, disconnected, or never connected. Never connected denotes a registered device that has not yet connected to Remote Manager.



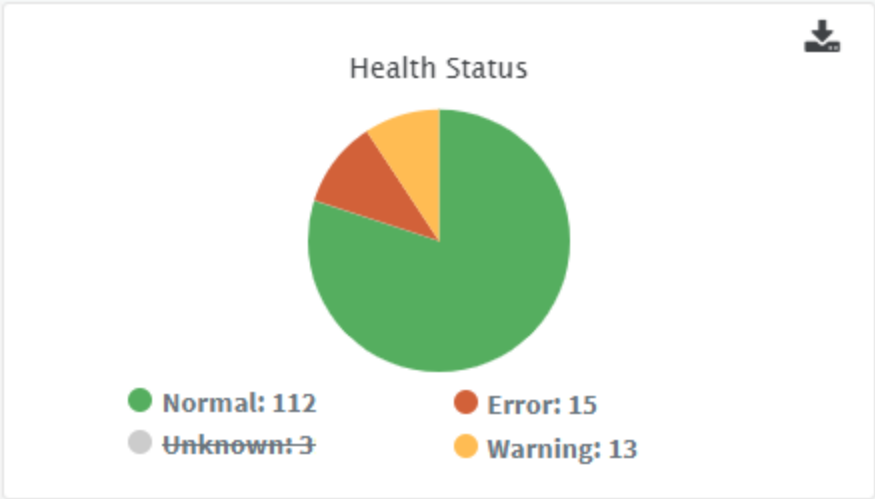
- Click a data label beneath the chart to include or exclude that data from the display. For example, to display only disconnected devices, click **Connected** to exclude connected devices.
- Click on an slice in the chart to open the **Device** page, filtered by the type of devices represented by the slice that was clicked. For example, to display a list of all disconnected devices, click on the **Connected** slice of the **Connection Status** chart.
- Click to download a local copy of the chart in PNG format.

Heath Status widget

The **Health Status** widget displays a summary of the health of all devices in your inventory. Health status is determined by a set of metrics reported by your devices. Sample health metrics include cellular signal strength and quality, CPU and memory usage, and local network performance statistics. See View health status definitions for health status definitions.

The overall health of a device is reported as an aggregate of all health metrics for the device:

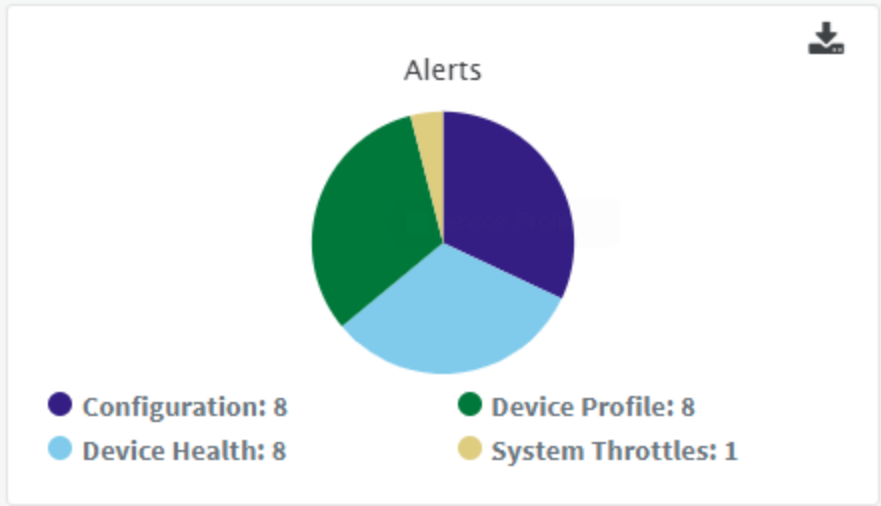
- **Normal:** All health metrics for the device are within configured normal thresholds.
- **Warning:** At least one health metric for the device is within a configured warning threshold, and no health metrics are within a configured error threshold.
- **Error:** At least one health metric for the device is within a configured error threshold.
- **Unknown:** Device health information is not found and the device state is unknown.



- Click a data label beneath the chart to include or exclude that data from the display. For example, to exclude devices with a normal health status from the display, click **Normal**.
- Click on an slice in the chart to open the **Device** page, filtered by the type of devices represented by the slice that was clicked. For example, to display a list of devices with a health status of error, click on the **Error** slice of the **Health Status** chart.
- Click to download a local copy of the chart in PNG format.

Alerts widget

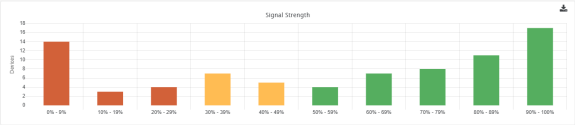
The **Alerts** widget shows a summary of all alert events by alert type. For a list and definitions of all alert types, in the main menu, click **Alerts** > **Definitions**.



- Click a data label beneath the chart to include or exclude that data from the display. For example, to exclude configuration alerts, click **Configuration**.
- Click on an slice in the chart to open the **Alerts** page, filtered by the type of devices represented by the slice that was clicked. For example, to display a list of **Device Health** alerts, click on the **Device Health** slice of the **Alerts** chart.
- Click to download a local copy of the chart in PNG format.

Signal Strength widget

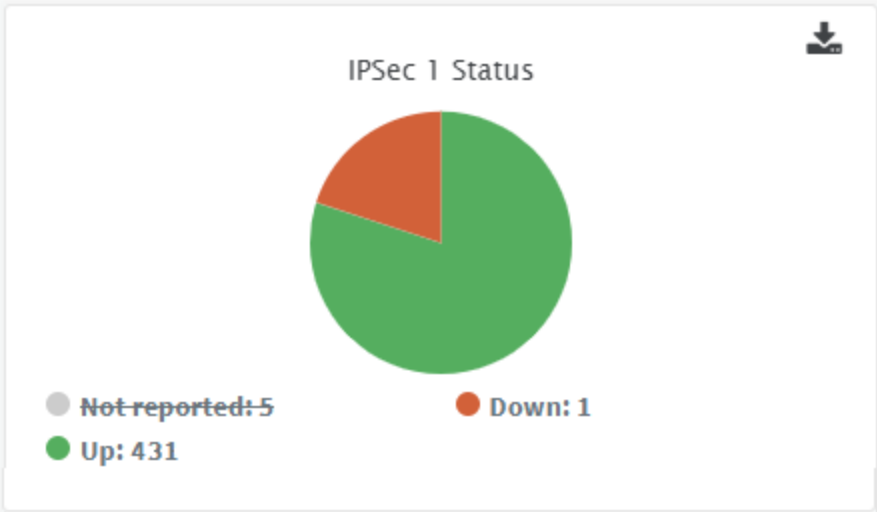
The **Signal Strength** widget shows a bar graph with the reported signal strength percentage of all devices in your inventory.



- Click on an bar in the chart to open the **Device** page, filtered by the type of devices represented by the bar that was clicked. For example, to display a list of devices with a signal strength of **0%-9%** devices with IPsec tunnels that are down, click on the **0%-9%** bar of the **Signal Strength** chart.
- Click to download a local copy of the chart in PNG format.

IPSec Status widgets

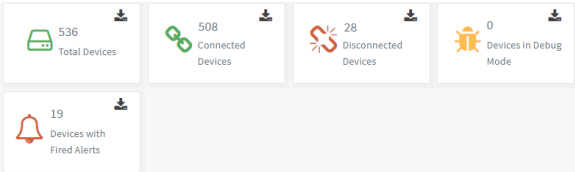
There are four IPsec Status wigets that display the current status of IPsec VPN tunnels.



- Click a data label beneath the chart to include or exclude that data from the display. For example, to display only devices with IPsec tunnels that are down, click **Down**.
- Click on an slice in the chart to open the **Device** page, filtered by the type of devices represented by the slice that was clicked. For example, to display a list of devices with IPsec tunnels that are down, click on the **Down** slice of the **IPSec Status** chart.
- Click to download a local copy of the chart in PNG format.

Inventory Status widgets

The **Inventory Status** widgets provide a quick, at-a-glance summary of your device inventory:



- Click on a chart to open the **Device** page, filtered by the type of devices represented by the chart that was clicked.
- Click to download a local copy of the chart in PNG format.

Customize your dashboard

Add a widget to your dashboard

1. Click
2. Click **Widgets** to display the list of available dashboard widgets.
3. Click the widget you want to add to the display.
4. Click to save your edits.

Remove a widget from your dashboard

1. Click
2. Each widget is now in edit mode.
3. In the top right of the widget you want to remove, click .
4. Click to save your edits.

Change the size or position of dashboard widgets

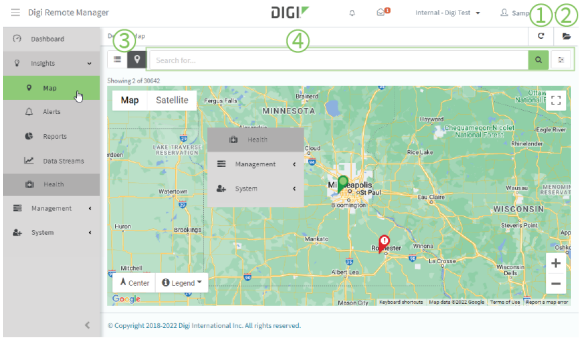
1. Click
2. Resize and position each of the widgets in your dashboard.
3. Click to save your edits.

Restore the default widgets

1. Click
2. Click **Widgets** to display the list of available dashboard widgets.
3. Click **Restore Default Widgets**.
4. Click to save your edits.

Map

The **Map** page displays a graphical display of the location of your devices.
From the main menu, click **Insights** > **Map**.



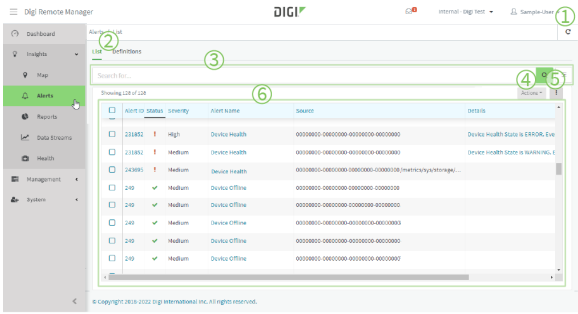
#	Component	Description
1	Refresh	Click to refresh the map.
2	Groups list	Click to toggle on or off a list of available groups. When a group is selected, only devices for that group will be displayed on the map.

#	Component	Description
3	Views	■ Click to display devices in tabular list view. ■ Click to display device location on a map view.
4	Device filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ■ Click to filter the display. ■ Click to clear the filter criteria.

Alerts

The Alerts page provides a list of alerts that have fired, as well as a tab to view and configure alert definitions.

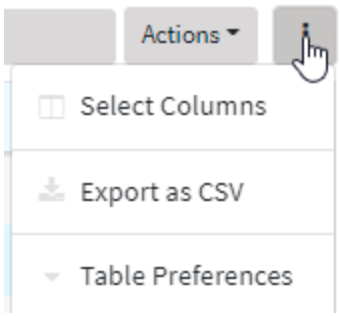
From the main menu, click **Insights** > **Alerts**.



Alerts are fired when certain events occur, such as when a device is disconnected or a device is out of compliance with its configuration.

You can acknowledge an alarm, manually reset an alarm that has been fired. The status of the alarm is cleared and returned to the normal state.

#	Component	Description
1	Refresh	Click to refresh the alert list.
2	Tabs	▪ **List**: Provides a list of alerts that have fired. ▪ **Definitions**: Provides a list of alert definitions.
3	Alert filter	▪ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:

#	Component	Description
		 ▪ Click to filter the display. ▪ Click to clear the filter criteria.
4	**Actions** menu	Select an alert to: ▪ View Alert Details. ▪ **Acknowledge** the alert. The system will stop devoting resources to an alarm while still leaving it in a fired state. ▪ **Reset** the alert. The status of the alarm is cleared and returned to the normal state.
5	Customize display menu	Click to customize the display.  ▪ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column.

#	Component	Description
		• Click **Use Defaults** to return to the default display. • Click **Close** when finished. ▪ Click **Export as CSV** to export a list of the devices in CSV format. ▪ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
6	Alert list	▪ Click to select an activity. ▪ Click an **Alert ID** or **Alert Name** view Alert Details. Alert list details: **Column** — **Description** **Alert Id** — Unique identifier for the alert. **Status** — Status of the alert: Fired, Normal, Acknowledged, Reset. **Severity** — Severity level of the alert definition. **Alert** — Name of the Alert.

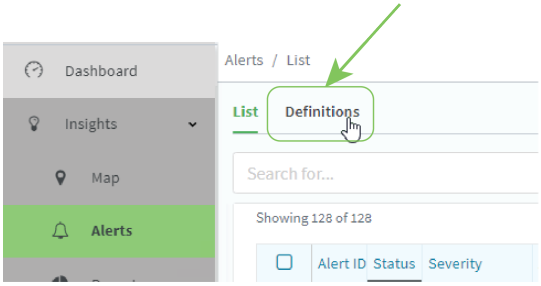
#	Component	Description
		<table><tr><th>Column</th><th>Description</th></tr><tr><td>**Name**</td><td></td></tr><tr><td>**Source**</td><td>Data source for the alert.</td></tr><tr><td>**Details**</td><td>Message describing the details of the alert.</td></tr><tr><td>**Device Id**</td><td>Id of the device for which the alert was fired.</td></tr></table>

This chapter contains the following topics:

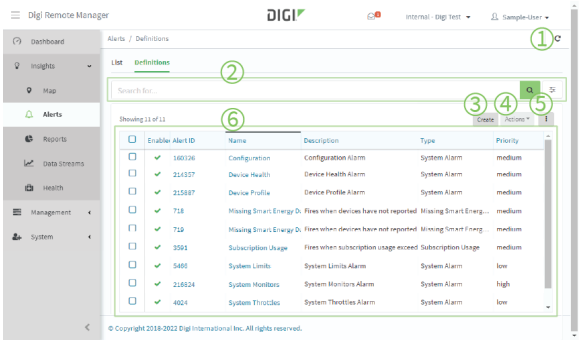
View alert definitions

To view alert definitions:

1. From the main menu, click **Insights** > **Alerts**.
2. Click **Definitions**.



The **Definitions** page displays.



#	Component	Description
1	Refresh	Click to refresh the alert definition list.
2	Alert definitions filter	▪ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ▪ Click to filter the display. ▪ Click to clear the filter criteria.

#	Component	Description
3	**Create**	Click to create an alert definition.
4	**Actions** menu	Select an alert definition to: ▪ **Delete** the alert. ▪ **Edit** the alert. You can change the name, description, and priority of the alert definition, and you can enable or disable it. You cannot edit system alerts.
5	Customize display menu	Click to customize the display. ▪ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ▪ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
6	Alert definition list	▪ Click to select an activity. ▪ Click an **Alert ID** or **Name** edit the alert. You can change the name, description, and priority of the alert definition, and you can enable or disable it. You cannot

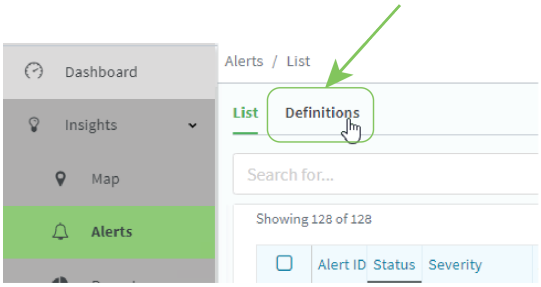
#	Component	Description
		edit system alerts. Alert definition list details: **Column** / **Description** **Enabled** — indicates that the alert is enabled. ! indicates that the alert is disabled. **Alert Id** — Unique identifier for the alert. **Name** — Name of the Alert. **Description** — Severity level of the alert definition. **Type** — Alert type: ▪ Device Offline ▪ XBeeNode offline ▪ Device Excessive Disconnects ▪ XBeeNode excessive deactivations ▪ DIA channel data point condition match ▪ Smart energy data point condition match ▪ Data point condition match ▪ Subscription Usage ▪ SystemAlarm ▪ Missing data point ▪ Missing DIA channel data

#	Component	Description
		Column / **Description** point ▪ Missing Smart Energy DataPoint **Priority** / Priority assigned to the alert definition: High, Medium, or Low. The Priority determines the severity level of the fired alarm.

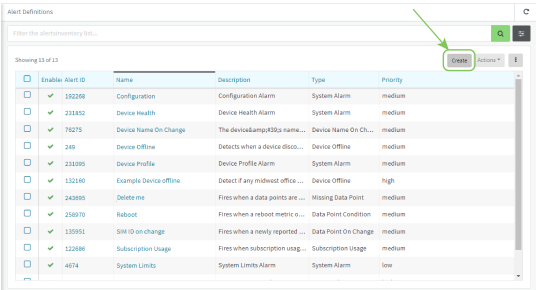
Create an alert

To create an alert:

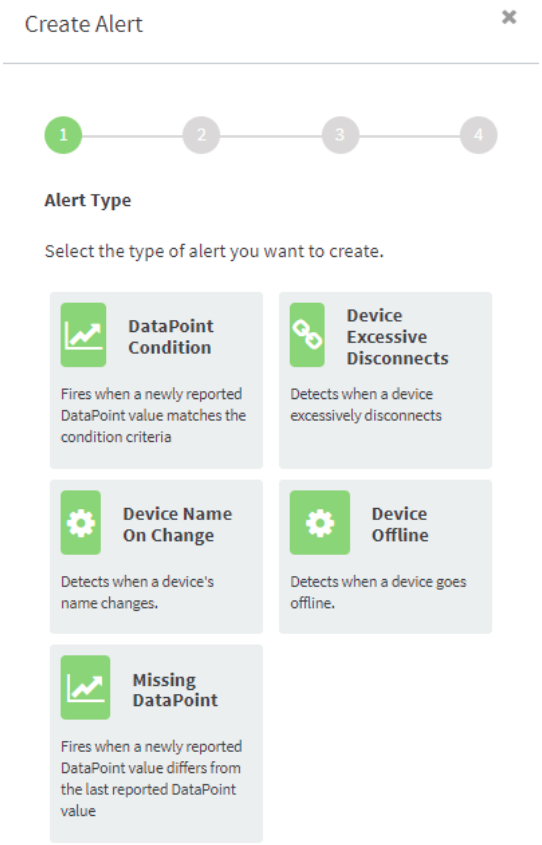
1. From the main menu, click **Insights** > **Alerts**.
2. Click **Definitions**.



3. Click **Create**.



The Create Alert dialog displays:

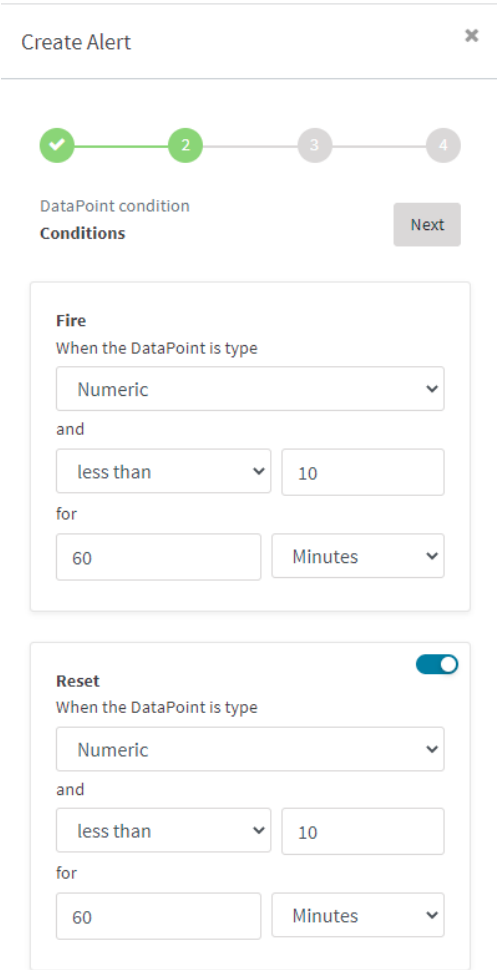


4. Click the applicable **Alert Type**.

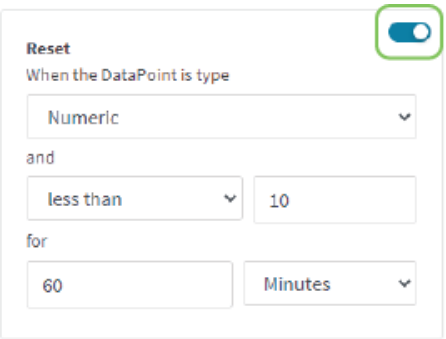
   The **Conditions** page displays. The **Conditions** page varies depending on the type of alert being created:

   DataPoint Condition:

   Fires when the specified datapoint usage conditions are met. When using this option, you must specify a data stream path that should be monitored for the alarm conditions configured for this alarm.



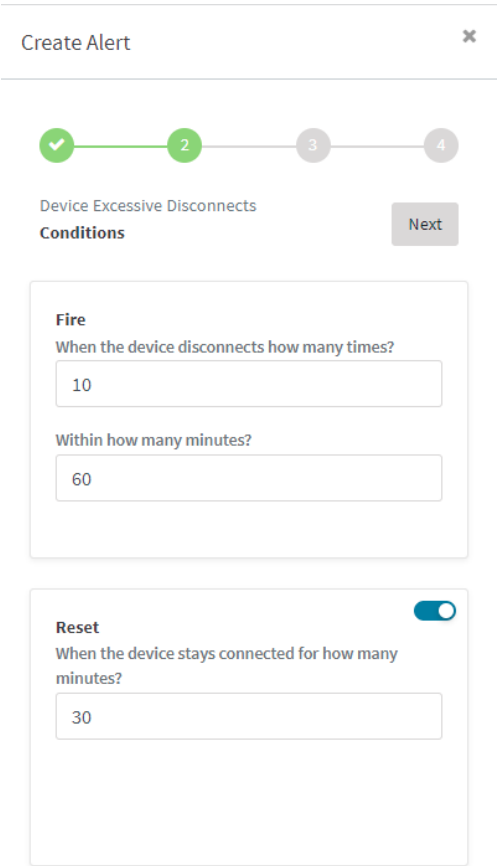
- The **Fire** section defines the conditions that will cause the alert to be generated:
  a. Select the type of DataPoint, either **String** or **Numeric**.
  b. Define the matching criteria that determines if the reported DataPoint is considered a match, so that the alert will be fired.
  c. Define the amount of time that the reported DataPoint should match the matching criteria in order for the alert to be fired.
- The **Reset** section defines when the alert will be automatically reset:
  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



b. Select the DataPoint type, matching criteria, and amount of time to define when the alert will be automatically reset.

Device Excessive Disconnects:

Defines a threshold for excessive disconnects and generates an alert when a device's disconnects exceed the threshold.



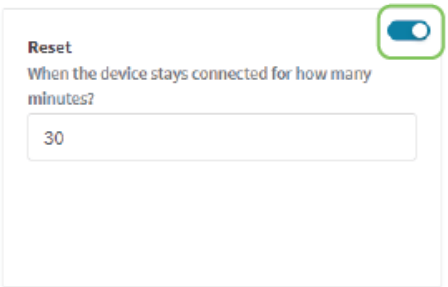
- The **Fire** section defines the number of disconnects within a period of time that will be considered excessive and will therefore fire the alert:

a. Define the number of disconnects.

b. Define the number of minutes during which the defined number of disconnects should take place to be considered excessive.

- The **Reset** section defines when the alert will be automatically reset:

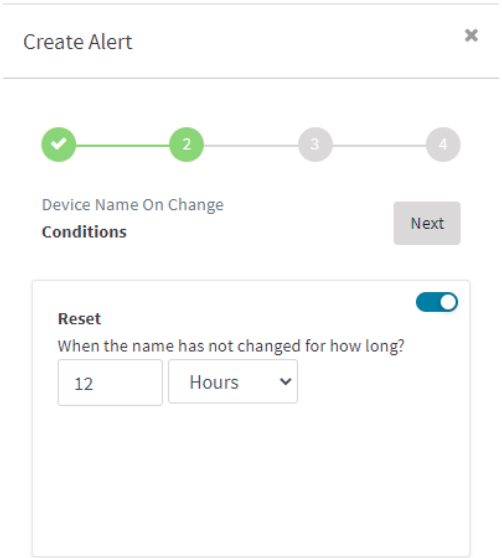
  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



  b. Select the number of minutes that the device should stay connected before the alert is automatically reset.

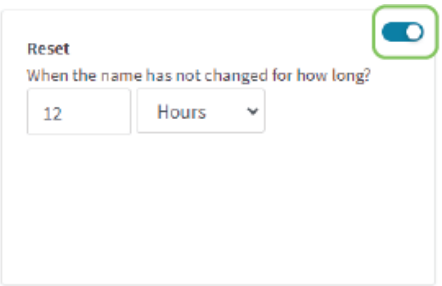
Device Name On Change:

Generates an alert when a device's name changes.



- The **Reset** section defines when the alert will be automatically reset:

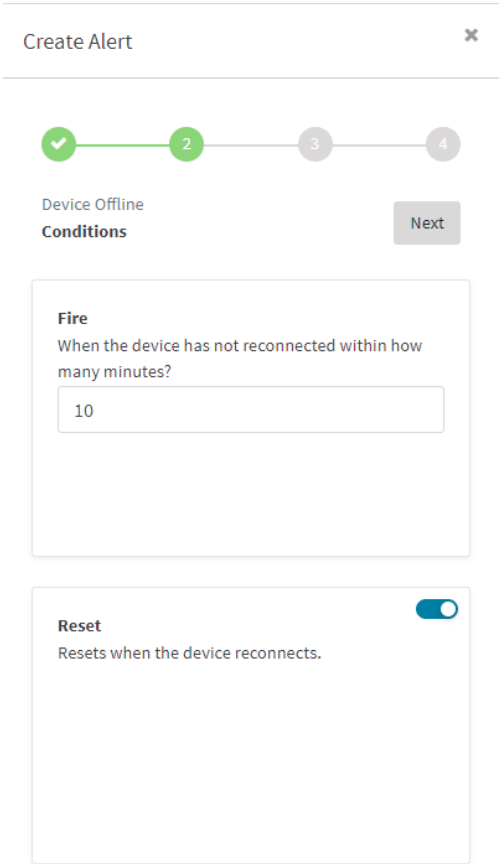
  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



b. Select the amount of time that the device name should stay the same after a device name change, before the alert is automatically reset.

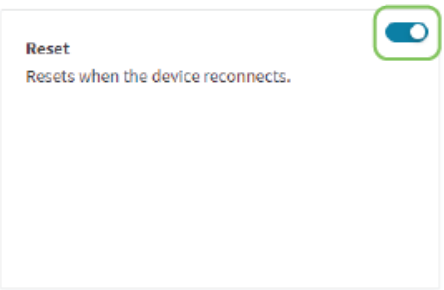
Device Offline:

Detects when a device goes offline.



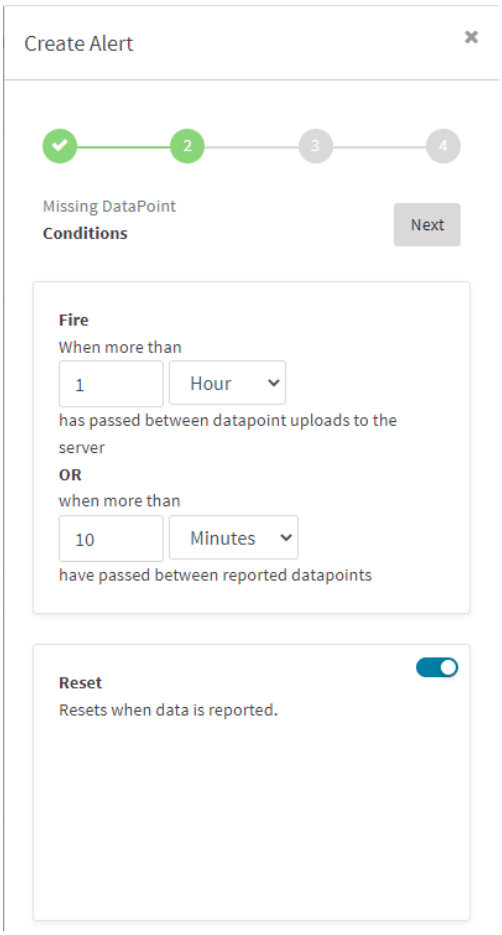
- The **Fire** section defines the conditions that will cause the alert to be generated:
  a. Select the number of minutes that the device has not been connected.
- The **Reset** section defines when the alert will be automatically reset:

a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



Missing DataPoint:

Generates an alert when DataPoint values have not been uploaded or reported for a defined period of time.



- The **Fire** section defines the conditions that will cause the alert to be generated:
  a. Select the amount of time between datapoint uploads from the device, after which Remote Manager will consider the datapoint to be missing and the alert

will fire.

b. Select the amount of time between when the device reports the datapoint, after which Remote Manager will consider the datapoint to be missing and the alert will fire.

- The **Reset** section defines when the alert will be automatically reset:

  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.

5. Click **Next**.

   The **Scope** page displays.

   - For **DataPoint Condition** and **Missing DataPoint** alerts, specify a data stream path you want to scope to. A resource scope can include an asterisk (*) to match to any element in the path, for example, */tx/bytes.
   - For **Device Excessive Disconnects**, **Device Name on Change**, or **Device Offline** alerts, identify either the group or the device that the alert will be scoped to.

6. Click **Next**.

   The **Information** page displays.

   a. (Optional) Type a **Name** for the alert.

   b. (Optional) Type a **Description** for the alert.

   c. Alerts are enabled by default; click to toggle off **Enabled** to disable the alert.

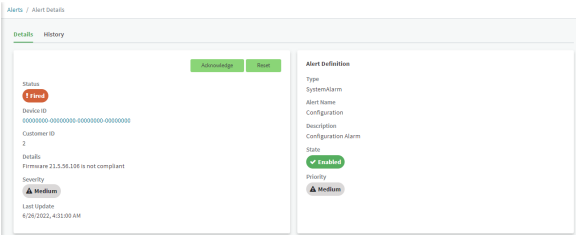
   d. Select a **Priority** for the alert.

7. Click **Create**.

View alert details and history

To view alert details and alert definition

1. From the main menu, click **Insights** > **Alerts**.
2. Click on the alert you want to view.
3. Click **Actions** > **Alert Details**.



Alert details

Click the **Details** tab to view details about the alert and the alert definition. You can also click **Acknowledge** or **Reset** from the Details tab to acknowledge or reset the alert.

Item	Description
Status	Status of the alert: Fired, Normal, Acknowledged, Reset.
Device ID	ID of the device for which the alert was fired.
Customer ID	ID of the customer account that the alert was fired on.
Details	Message describing the details of the alert.
Severity	Severity level of the alert definition.
Last Update	The date and time that the alert was last updated.
Alert Definition	
Type	Alert type: ▪ Device Offline ▪ XBeeNode offline ▪ Device Excessive Disconnects ▪ XBeeNode excessive deactivations ▪ DIA channel data point condition match ▪ Smart energy data point condition match ▪ Data point condition match ▪ Subscription Usage ▪ SystemAlarm ▪ Missing data point ▪ Missing DIA channel data point ▪ Missing Smart Energy DataPoint
Alert Name	Name assigned to the alert.
Description	Description for the alert.
State	State of the alert definition: Enabled or disabled.
Priority	Priority assigned to the alert definition: High, Medium, or Low. The Priority determines the severity level of the fired alarm.

Alert History

Click the **History** tab to view a bar graph representation of the history of when the alert was fired, acknowledged, and reset.

Click to export the graph as an image or a CSV or Excel file.

Acknowledge an alert

You can acknowledge an alert when you want Remote Manager to stop devoting resources to an alert while still leaving it in a fired state.

To acknowledge an alert:

1. From the main menu, click **Insights** > **Alerts**.
2. Select one or more alerts to acknowledge.
3. Click **Actions > Acknowledge**.

Reset an alert

You can manually reset an alert that has been fired. The status of the alert is cleared and returned to the normal state.

To reset an alert:

1. From the main menu, click **Insights** > **Alerts**.
2. Select one or more alerts you want to reset.
3. Click **Action** > **Reset**.

System alerts

System alerts automatically trigger for Remote Manager processing conditions for which a customer may want to be notified. The alerts are automatically created as needed and automatically reset when the condition is resolved.

System alerts types include the following:

- **System monitor alarms:** Fire for events such as a monitor disconnecting, or when Remote Manager is unable to send messages to a monitor.
- **System limits alarms:** Fire for events such as the device limit being reached, the size of a list of DataPoints exceeds the maximum, and so on.
- **System throttle alarms:** Fire for data being received at a rate that exceeds a threshold, such as sending too many web service requests in a time period.
- **Device profile alarms:** Fire when a profile scan runs and finds a device out of compliance with the profile.
- **Device health alarms:** Fire when a device reports a metric that is outside of the bounds of the device health profile.

Reports

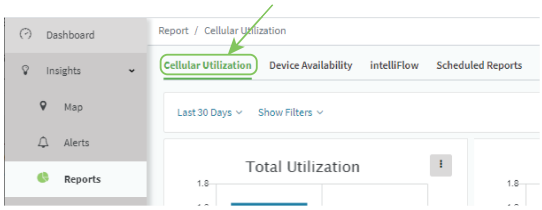
From the main menu, click **Insights** > **Reports**.

The **Reports** page provides the following report types:

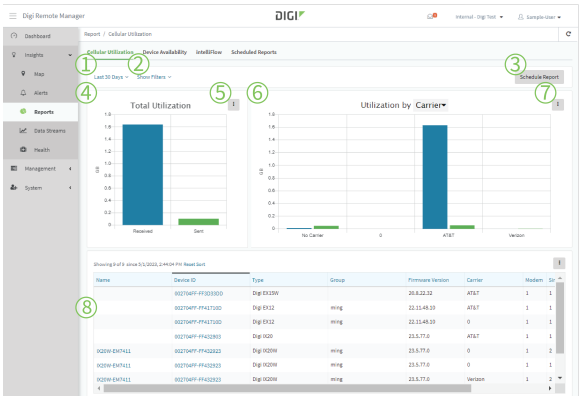
Cellular Utilization

The **Cellular Utilization** report provides views of your total cellular utilization and utilization based on carrier type, device type, group, and several other filter categories.

1. From the main menu, click **Insights** > **Reports**.
2. Click the **Cellular Utilization** tab.



The **Cellular Utilization** report page displays:



#	Component	Description
1	Date and time selector	Select a relative time, such as within the **Last Hour** or **Last 30 Days**. Or, enter a **Start** and **End** date.
2	Filters	1. Click to expand **Show Filters** ☒ 2. Type or select values for the appropriate filters. 3. Click **Generate Report** when finished.
3	**Schedule Report**	Click **Schedule Report** to open the **Scheduled Report Options** dialog.
4	**Total Utilization** graph	Bar graph that displays the total data received and sent by all matching devices.

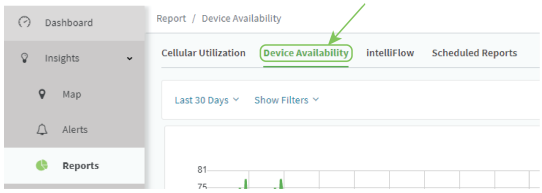
#	Component	Description
5	**Total Utilization** graph menu	Click next to **Total Utilization** to: ▪ Set the unit of data to be displayed by the **Total Utilization** graph. Available values are **KB**, **MB**, **GB**, and **TB**. ▪ Download a copy of the chart in **PNG**, **JPEG**, or **SVG** format.
6	**Utilization by...** graph	Bar graph that displays the data received and sent by selected category.Click to select the category to display in bar graph form. Available categories are: **Modem**, **SIM**, **Carrier**, **Device Type**, **Firmware Version**, and **Group**.
7	**Utilization by...** graph menu	Click next to **Utilization by...** to: ▪ Set the unit of data to be displayed by the **Total Utilization** graph. Available values are **KB**, **MB**, **GB**, and **TB**. ▪ Download a copy of the chart in **PNG**, **JPEG**, or **SVG** format.
8	Cellular Utilization tabular view	Displays cellular utilization in tabular form. Click to customize the display. ▪ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and

#	Component	Description
		dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ▪ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)

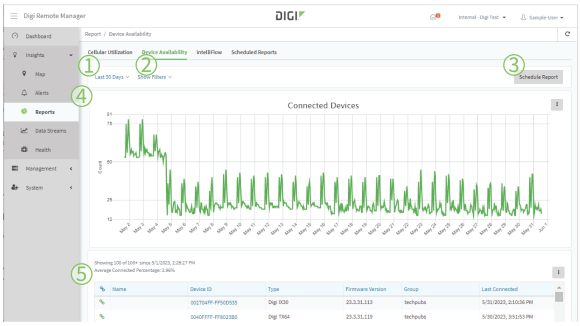
Device Availability

The **Device Availability** report provides a pie chart of the percentage of currently connected devices, and a line graph of connection percentage over time.

1. From the main menu, click **Insights** > **Reports**.
2. Click the **Device Availability** tab.



The **Device Availability** report page displays:



#	Component	Description
1	Date and time selector	Select a relative time, such as within the **Last Hour** or **Last 30 Days**. Or, enter a **Start** and **End** date.
2	Filters	1. Click to expand **Show Filters** ☒ 2. Type or select values for the appropriate filters. 3. Click **Generate Report** when finished.
3	**Schedule Report**	Click **Schedule Report** to open the Scheduled Report Options dialog.
3	**Connected Devices** graph	Line graph that displays connection statistics for all matching devices. Click next to the graph to: ▪ Download a copy of the chart in **PNG**, **JPEG**, or **SVG** format. ▪ Set the **Unit** to display either the total **Count** or the **Percentage** of connected devices.
4	Device availability tabular view	Displays device availability in tabular form. Click to customize the display. ▪ Click **Select Columns** to open a list of columns. • Click to select the columns that will be

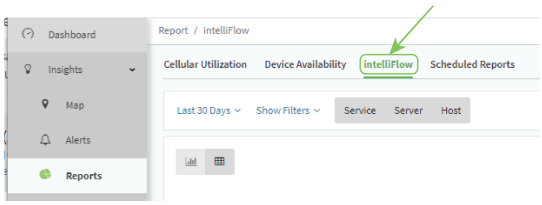
#	Component	Description
		displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ▪ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)

intelliFlow

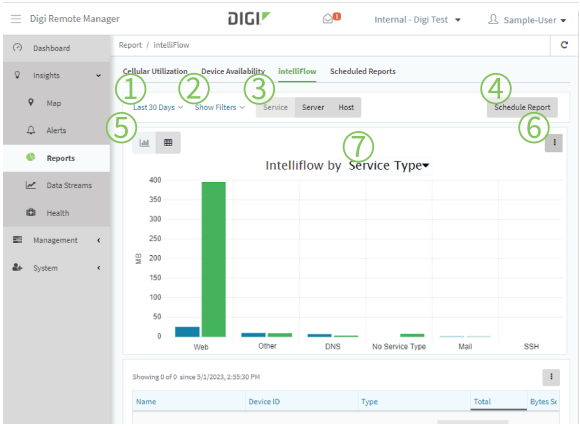
Digi intelliFlow is a reporting and graphical presentation tool for visualizing your network's data usage and network traffic information.

intelliFlow can be enabled on Digi Remote Manager to provide a full analysis of all Digi devices on your network. Contact your Digi sales representative for information about enabling intelliFlow on Remote Manager.

1. From the main menu, click **Insights** > **Reports**.
2. Click the **intelliFlow** tab.



The **intelliFlow** report page displays:

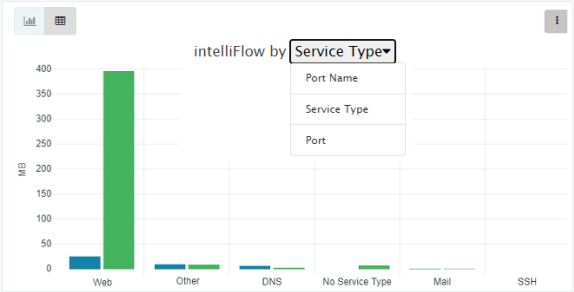


#	Component	Description
1	Date and time selector	Select a relative time, such as within the **Last Hour**, **Last 30 Days**, or **Year to Date**. Or, enter a **Start** and **End** date.
2	Filters	1. Click to expand **Show Filters** ☒ 2. Type or select values for the appropriate filters. 3. Click **Generate Report** when finished.
3	Report type	Select the type of categorization for the report: ▪ **Service**: Displays intelliFlow data by **Service type** or **Port**. ▪ **Server**: Displays intelliFlow data by the destination server being contacted. ▪ **Host**: Displays intelliFlow

#	Component	Description
		data by the internal host that the traffic originated from.
4	**Schedule Report**	Click **Schedule Report** to open the Scheduled Report Options dialog.
5	Views	▪ Click to view the data in chart format. ▪ Click to view the data in tabular format.
6	Display options (chart view only)	Click to: ▪ Set the unit of data to be displayed. Available values are **KB**, **MB**, **GB**, or **TB**. ▪ Set the number of top sources to be displayed. Available values are **5**, **10**, **20**, or **all**. ▪ Set the sorting order. Available values are **Total**, **Bytes Sent**, **Bytes Received**, or **Server Address**. ▪ Download a copy of the chart in **PNG**, **JPEG**, or **SVG** format. ▪ Export the chart in comma separated value (CSV) format.
7	x-axis (chart view only)	▪ Service view: Change between **Service Type** and **Port** number. See Service type for further details. ▪ Server view: Change between **Server Domain** and **Server Address**. ▪ Host view: Change between **Host Domain** and **Host Address**.

Service type

In chart view, you can select to view the network traffic by either **Service Type**, or **Port**.



Service Type is used to categorize several ports under one service. For example, port numbers 80, 443, and 8080 are included in the **Web** service type.

There are several predefined service types:

- Web: Ports 80, 443, and 8080.
- FTP: Ports 20, 21, 989, and 990.
- SSH: Port 22.
- Telnet: Ports 23 and 992.
- Mail: Ports 25, 110, 143, 220, 993 and 995.
- DNS: Port 53.
- IRC: Ports 194 and 994.
- RSYNC: Ports 873.

You can add and remove ports from the predefined service port types, and you can also define your own service types. This is done at the device level, or as part of a configuration. For example, in a configuration, to define a service type called "MyService" using ports 9000 and 9001:

1. From the main menu, click **Insights** > **Reports**.
2. **Monitoring** > **intelliFlow**.
3. Click to expand **Ports**.
4. Yto add a port.
5. **Label** is optional.
6. For **Port number**, type **9000**.
7. For **Service name**, type **MyService**.
8. Click Yto add a another port.
9. For **Port number**, type **9001**.
10. For **Service name**, type **MyService**.

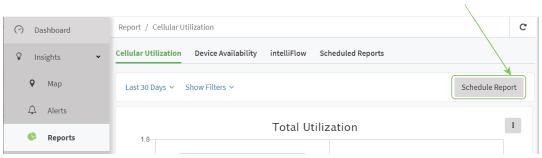
IntelliFlow is also available on the local device for device-specific visualization of network use. To use intelliFlow on the local device, you must have access to the local WebUI. By default, intelliFlow is disabled on the local device.

Schedule a report

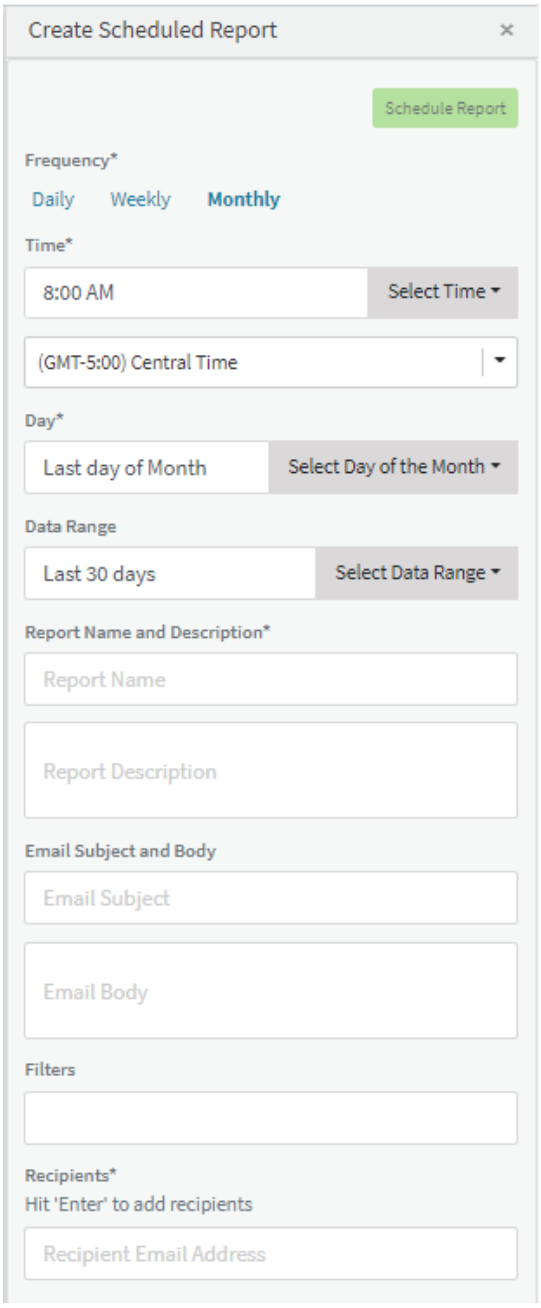
To schedule a report:

1. From the main menu, click **Insights** > **Reports**.
2. Select a report type, either Cellular Utilization, Device Availability, or intelliFlow.

3. Click **Schedule Report**.



The **Create Scheduled Report** dialog opens.



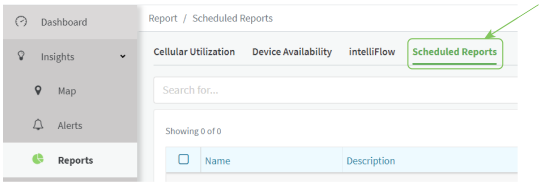
4. For **Frequency**, select either **Daily**, **Weekly**, or **Monthly**.

5. For **Time**, type the time or click **Select Time** and select a time from the menu.
6. Select the **Timezone**.
7. For **Date Range**, select range of dates that should be included in the report.
8. Type a **Report Name and Description**.
9. (Optional) Type an **Email Subject and Body**.
10. Include a list of **Recipients** for the email. Press Enter between each recipient.
11. Click **Schedule Report**.

View scheduled reports

To view a tabular list of scheduled reports:

1. From the main menu, click **Insights** > **Reports**.
2. Click **Scheduled Reports**.



- To edit a scheduled report, select the report and select **Actions** > **Edit Report**.
- To manually run a scheduled report, select the report and select **Actions** > **Run Report**.
- To delete scheduled reports, select one or more reports and select **Actions** > **Delete Reports**.

Data Streams

Within the data streams page, you can view a list of all your data streams as well as create, edit, and delete them. You can select a data stream from your list and view a chart of that data stream's data points based on several options and using several pre-defined time periods, or simply view the raw data associated with a data stream.

What is a data stream?

Time-series data involves two concepts:

- **Data points**: Data points are the individual values which are stored at specific times, while data streams are containers of data points.
- **Data streams**: Data streams contain metadata about the data points held within them. Data streams and the data points they hold are addressed using hierarchical paths (much like folders), for example:

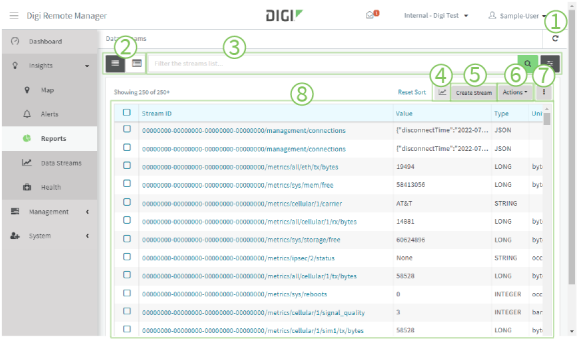
  00000000-00000000-11223344-55667788/metrics/sys/storage/tmp/used

Remote Manager data streams

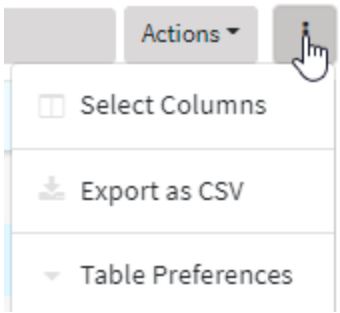
Remote Manager data streams can store and access time-series data. Virtually any type of data can be stored, and you can create real-time charts to visualize and monitor the data streams. Data streams are fully searchable and the data can also be rolled up into time interval summaries.

Data streams are primarily intended for numeric data and typically hold data points for a specific attribute on a device, such as the temperature from a specific thermostat. However, data streams can be used for virtually any type of data. Smart Energy attribute data and DIA channel data can be configured to automatically store their data via the time series data feature. Additionally, any data previously accessible via the DIA or XBee APIs is automatically replicated and available for historical query via the v1/streams API. See the

Your data is completely protected; it is stored and replicated in multiple secure, commercial-grade storage systems. If at any time you choose to cancel your data streams subscription, you will need to first download your data.



#	Component	Description
1	Refresh	Click to refresh the data stream list.
2	Views	■ Click to display each data stream in list view. ■ Click to group data streams by Device ID.
3	Data stream filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category: 

#	Component	Description
		▪ Click to filter the display. ▪ Click to clear the filter criteria.
4	**Chart** button	See Display a data stream in chart or tabular format.
5	**Create Stream** button	See Create a data stream.
6	**Actions** menu	▪ **Stream Details**: Display further information about the selected data stream. ▪ **Copy Properties** (JSON): Copy the selected data stream's properties in JSON format. ▪ **Delete**: Delete the selected datastream. ▪ **Create Alert**: Create a **DataPoint Condition** or **Missing DataPoint**. If a data stream is selected, the alert's resource scope will be auto-filled with the data stream's Stream ID.
7	Customize display menu	Click to customize the display.  ▪ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the

#	Component	Description
		column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click **Export as CSV** to export a list of the devices in CSV format. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
8	Datastream list	■ Click to select a datastream. ■ Click a **Stream ID** to open the datastream in chart view. See Display a data stream in chart or tabular format for more information.

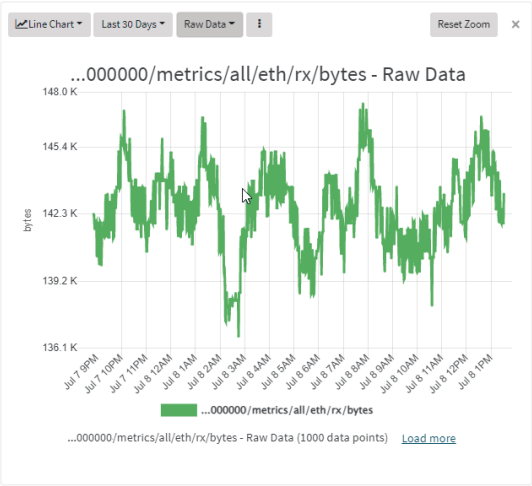
This chapter contains the following topics:

Display a data stream in chart or tabular format

You can display data points for a selected data stream in table or chart format. You can also configure the time line and the type of data displayed, and save or export the data.

1. From the main menu, click **Insights** > **Data Streams**.
2. Click the Stream ID, or select the appropriate data stream and click .

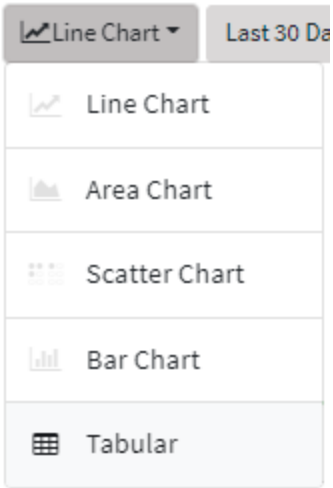
   The data stream is displayed in chart format:



Change the chart type

To change the type of chart that is used to display the data stream:

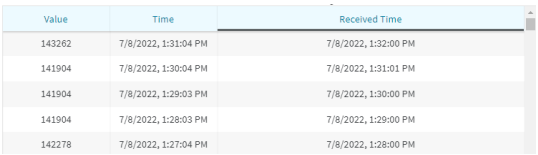
1. Click the **Chart** menu
2. Select the appropriate type of chart.



Display the data stream in tabular format

To display the data stream in tabular format, listing each individual data point:

1. Click the **Chart** menu.
2. Select **Tabular**.

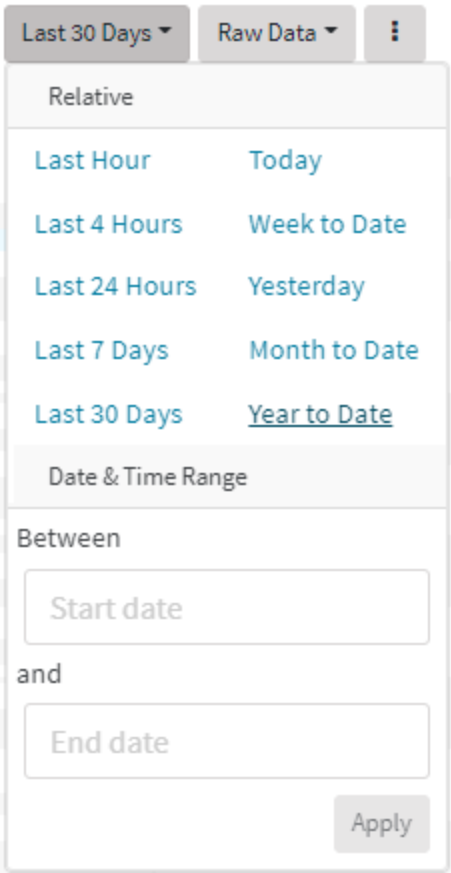


Value	Time	Received Time
143262	7/8/2022, 1:31:04 PM	7/8/2022, 1:32:00 PM
141904	7/8/2022, 1:30:04 PM	7/8/2022, 1:31:01 PM
141904	7/8/2022, 1:29:03 PM	7/8/2022, 1:30:00 PM
141904	7/8/2022, 1:28:03 PM	7/8/2022, 1:29:00 PM
142278	7/8/2022, 1:27:04 PM	7/8/2022, 1:28:00 PM

Change the time line for the chart

To change the time line displayed by the chart or table:

1. Click the **Time line** menu.

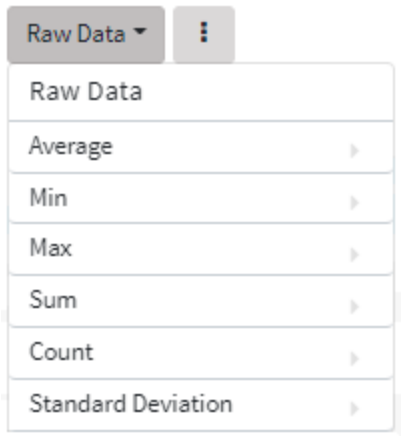


2. Click a relative timeline, or select the date and time range.
3. Click **Apply**.

Change the type of data being displayed

To change the type of data being displayed:

1. Click the **Data** menu.

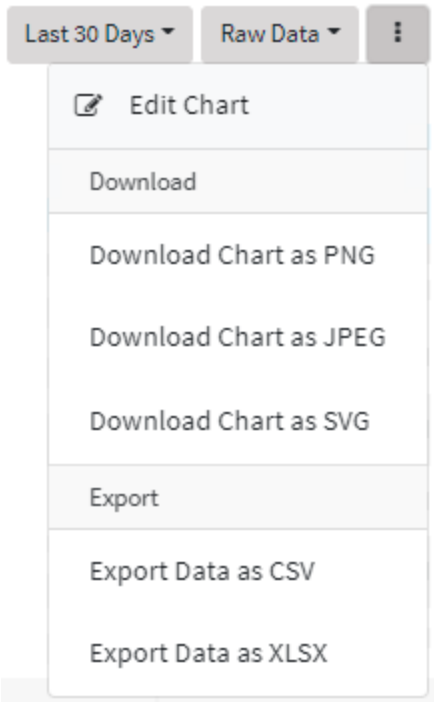


2. Select the appropriate type of data to be displayed.

Edit the chart

You can change the chart title and related chart settings.

1. Click .



2. Select **Edit Chart**.
3. Change the appropriate chart options.
4. Click **Apply**.

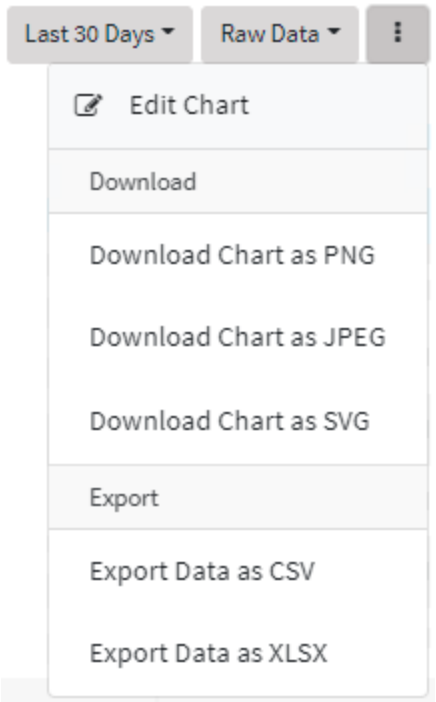
Zoom in and out in chart view

When viewing a data stream in a chart, you can zoom in and out of the data by using the mouse wheel. Click **Reset Zoom** to return to the original display.

Download the chart or export data

You can download the data stream chart as a PNG, JPEG, or SVG, and you can export the chart's data in CSV or Excel formats.

1. Click .



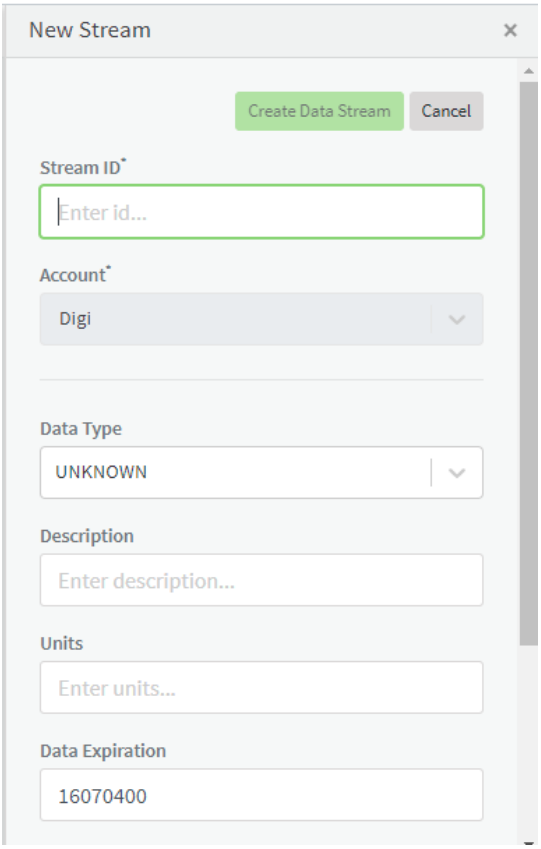
2. To download the chart, select the appropriate filetype to download.
3. To export the data used to create the chart in CSV or XLSX formats, select the appropriate filetype to export to.
4. The chart or file will be downloaded using your browser's download functionality.

Create a data stream

Data streams contain metadata about the data points held within them. Remote Manager users and administrators can create data streams.

To create a data stream:

1. From the main menu, click **Insights** > **Data Streams**.
2. Click **Create Stream**.

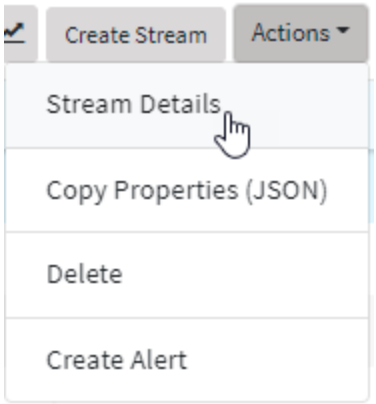


   a. For **Stream ID**, type a name for a container for data.
   b. For **Data Type**, select the data type that will be stored in the data stream.
   c. For **Description**, type a description of the data.
   d. For **Units**, type a user-defined description of the unit of measure for the reported data.
   e. For **Data Expiration**, enter the length of time the data point is stored. The value is measured in seconds. The value can be between 0 and 16,070,400 seconds, which is 6 months. You can manually enter a value or select an option from the drop-down list.
   f. For **Rollups Expiration**, enter the length of time the data rollup is stored. The value can be between 0 and 16,070,400 seconds, which is 6 months. You can manually enter a value or select an option from the drop-down list.
   g. For **Forward To**, select additional data streams to forward the data to when it is received:
      i. Click in the **Forward To** field to open a list of existing data streams.
      ii. Click a data stream.
      iii. To add another data stream, click in the **Forward To** field again.
3. Click **Create Data Stream**.

Edit data stream properties

To edit the properties for a data stream:

1. From the main menu, click **Insights** > **Data Streams**.
2. Select the appropriate data stream.
3. Click **Actions** > **Stream Details**.



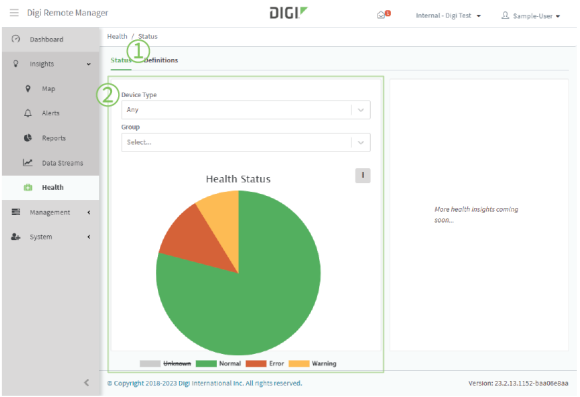
The **Stream Details** dialog appears.

4. Modify information in the dialog as necessary. See Create a data stream for a description of the fields.
5. Click **Update Data Stream**.

Health

The **Health** page displays the health status view and allows users to view the definitions for health status metrics.

From the main menu, click **Insights** > > **Health**.



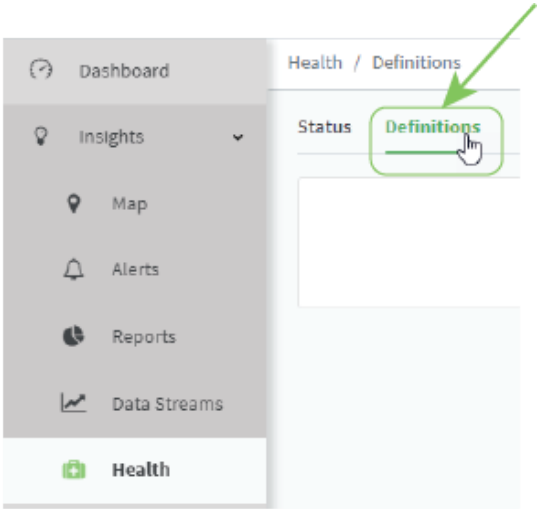
#	Component	Description
1	Tabs	▪ **Status**: Provides a health status chart. ▪ **Definitions**: Provides health status

#	Component	Description
		definitions.
2	**Health status chart**	The **Health Status** chart displays a summary of the health of devices in your inventory. Health status is determined by a set of metrics reported by your devices. ▪ Click **Device Type** to limit the displayed health status to all devices in your inventory of the selected device types. ▪ Click **Group** to limit the displayed health status to all devices in the selected group.

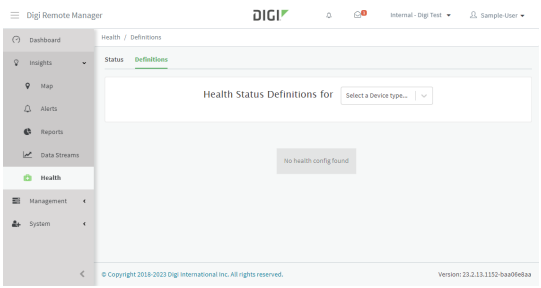
View health status definitions

To view health status definitions:

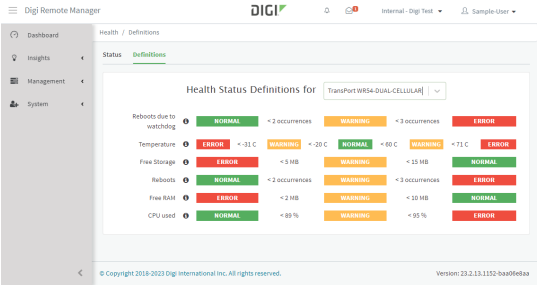
1. From the main menu, click **Insights** > > **Health**.
2. Click **Definitions**.



The **Definitions** page displays.



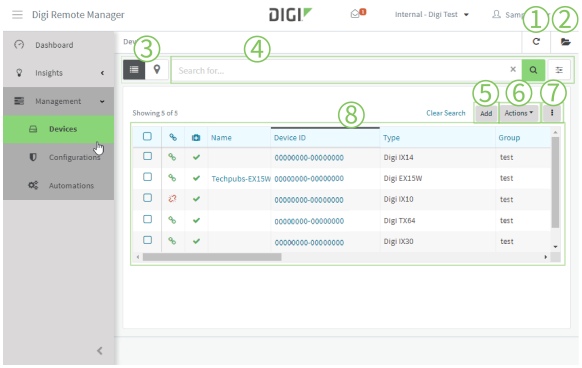
3. **Select a Device type** to display the health status definitions for that device.



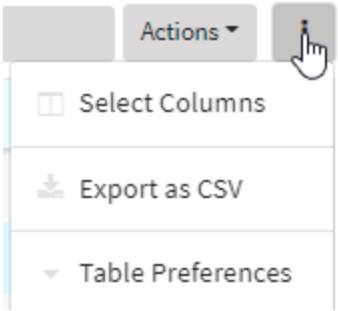
Devices

The **Devices** page lists all devices registered in your Remote Manager account.

From the main menu, click **Management** > **Devices**.



#	Component	Description
1	Refresh	Click to refresh the device list.
2	Groups list	Click to toggle on or off a list of available groups.
3	Views	▪ Click to display devices in tabular list view. ▪ Click to display device location on a map view.
4	Device filter	▪ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for.

#	Component	Description
		• Advanced filtering: click in the filter bar to select a filtering category:  ▪ Click to filter the display. ▪ Click to clear the filter criteria.
5	**Add** button	See Add a device.
6	**Actions** menu	See Device actions.
7	Customize display menu	Click to customize the display.  • Click **Select Columns** to open a list of columns. ◦ Click to select the columns that will be displayed in the device list. ◦ Click and select whether to send the column to the top or bottom of the list. ◦ Click to reorder the listing by dragging and dropping a column. ◦ Click **Use Defaults** to return to the default display. ◦ Click **Close** when finished. • Click **Export as CSV** to export a list of the devices

#	Component	Description
		in CSV format. • Click Table Preferences to set your table view preferences: ◦ Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. ◦ Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
8	Device list	▪ Click to select a device . ▪ Click a device **Name** or **Device ID** to open Device Details for the device.

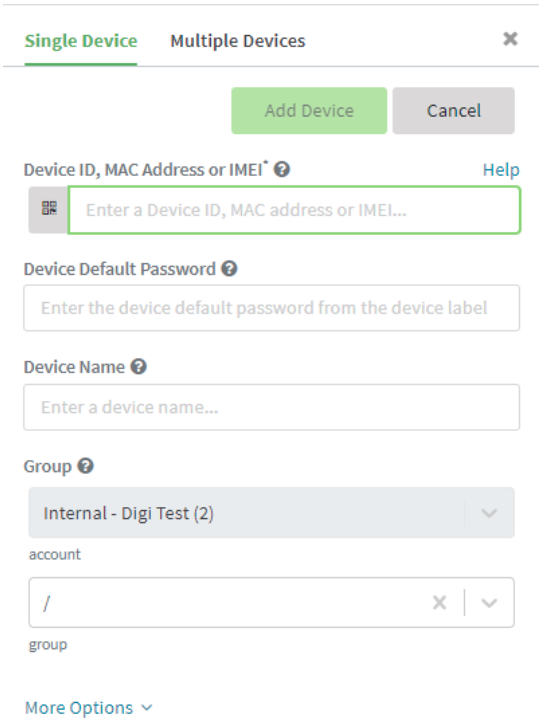
This chapter contains the following topics:

Add a device

To manage a device, add the device to your Remote Manager inventory. Once a device is in your inventory, you can view and manage the device using any Remote Manager feature.

To add a device:

1. From the main menu, click **Management** > **Devices**.
2. Click **Add**.



- To add a single device:
  1. Either scan the device's QR code or enter device information.
     - If your device's label has a QR code:
       a. Click
       b. When prompted, allow Remote Manager to use your camera.
       c. Position the QR code on the device's label in front of your camera.

       The **Device ID** And **Device Default Password** will be filled automatically.
     - To enter device information:
       a. Type the **Device ID, MAC Address, or IMEI**.
       - The device ID is a unique 16-byte number used to identify a device within Remote Manager. See Device IDs for more information.
       - The MAC address must be in the format 00:00:00:00:00:00. The colon separators are optional.
       - If the device has both a MAC address and an IMEI number, you must use the MAC address.

b. Type the **Device Default Password** printed on the device label. This field is optional, but some devices may require the default password to add the device to Remote Manager.

2. (Optional) Enter a name for the device.
3. Select an account and group that the device will be added to.
4. (Optional) Click **More Options** to enter notes and tags for the device.
5. Click **Add Device**.

- To add multiple devices:
  1. Click **Multiple Devices**.
  2. Click **Browse** to upload a comma-separated values (CSV) file containing information for multiple devices.

     A description of the CSV file format and an example file is provided in the help message. See Create a CSV file to add multiple devices for more information.
  3. (Optional) Click to enable **Update existing devices** to update information for devices listed in the CSV file that have already been added to Remote Manager.
  4. Click **Add Devices**.

Create a CSV file to add multiple devices

You can add one or more devices to Remote Manager by importing the devices from a Comma Separated Values (CSV) file.

The first row of the CSV file contains comma-separated column names. Subsequent rows identify individual devices by Device IDs or MAC address. For example:

```
id,install_code,name
00000000-00000000-11111111-22222222,1234567890,device-1
00000000-00000000-11111111-22222222,1234567891,device-2
```

Allowed column names are:

Column name	Description
id	The Device IDs. Either the Device ID or the MAC address is required.
install_code	The device's default password, printed on the device label. Depending on the device, the default password may be required.
mac	The device's MAC address. Either the MAC address or the Device ID is required.
type	(Optional) The device model type. Depending on the device, this may be completed automatically when the device connects to Remote Manager.
description	(Optional) A description of the device.
restricted_status	(Optional) One of:

Column name	Description
	▪ **Untrusted**: The device can be auto-provisioned, but is not fully operational until validated. ▪ **Restricted**: The device cannot be fully managed until the restriction status is changed to unrestricted. ▪ **Unrestricted**: There are no restrictions on the device. If not set, your configured default restricted status (available in the Classic Remote Manager user interface only) will be used.
contact	The name of the contact for this device.
location	(Optional) A description of the device's location.
geoposition	(Optional) The geoposition of the device. Should be comma-separated using the format "*latitude*,*longitude*,[*altitude*]" for example: **"44.92646,-93.39752"**.
vendor_id	(Optional) The system-assigned vendor ID registered for your account. Normally this should not be changed.
notes	(Optional) Notes related to the device.
tags	(Optional) Tags to help categorize the device. Should be comma-separated, for example **"tag1,tag2"**.
group	(Optional) The group to which the device should be added.
name	(Optional) A name of the device.
maintenance_mode	Whether the device should be in debug mode. Allowed values are **On** and **Off**.
cellular_modem_id	(Optional) The IMEI of the device's cellular modem.

Note

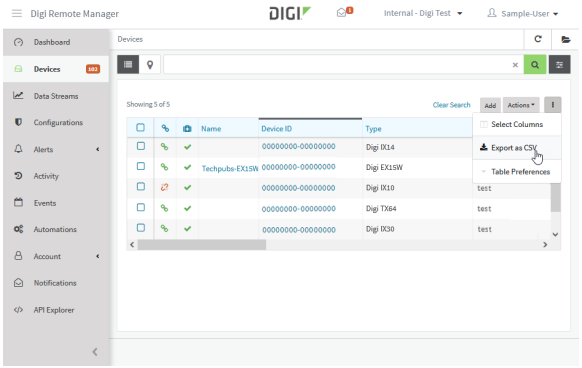
- Blank lines, empty values, or leading and trailing white space in values and column names are ignored.
- Values containing commas must be enclosed in double quotes.
- If **Update existing devices** is disabled, existing devices will not be updated with values from the file. The **type** and **vendor_id** values cannot be updated.

Export device list to a CSV file

To export the device list to a CSV file:

1. From the main menu, click **Management** > **Devices**.
2. Click .
3. Select **Export to CSV**.

A CSV file will be downloaded to your local file system.



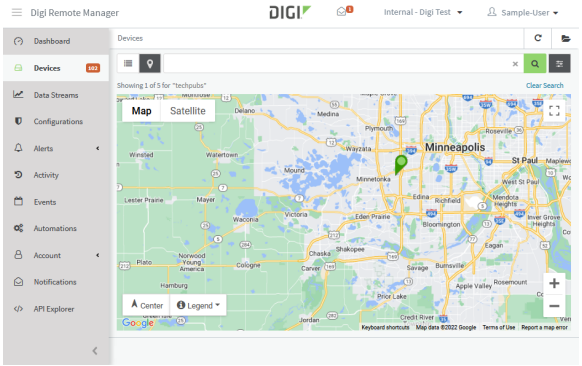
Show devices on map

You can show devices as pins on a map from the **Devices** page.

Note Only devices that have connected to Remote Manager can be shown. Remote Manager cannot plot devices that have never connected.

To show devices on a map:

1. From the main menu, click **Management** > **Devices**.
2. Click
3. You can select **Map** (with or without Terrain) or **Satellite** (with or without labels).
4. To switch back to list view, click



Update device firmware

You can update device firmware on one or more devices in two ways:

- Update using a firmware file available in the Remote Manager firmware repository.
- Update using a firmware file on you local device. Visit Digi firmware to download firmware.

Update firmware from the firmware repository

To update firmware from the Remote Manager firmware repository:

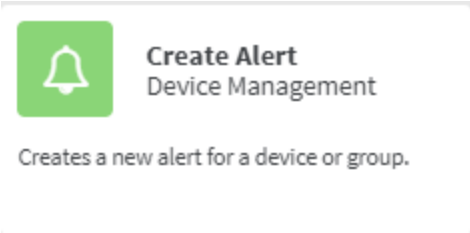
1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to have their firmware updated, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Update Firmware**.

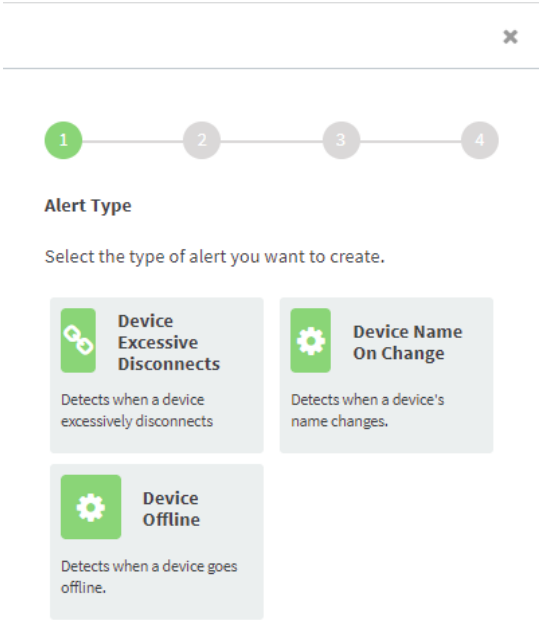
4. For each selected device, select the firmware version to update the device firmware.
5. Click **Update**.

Update firmware by using a local firmware file

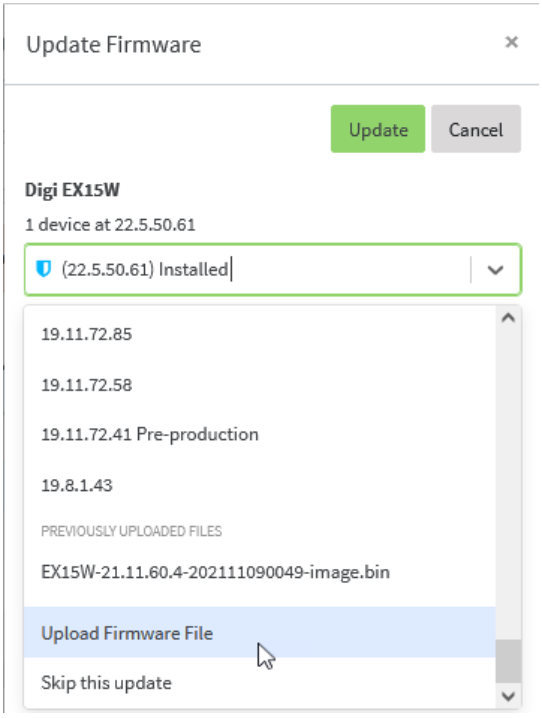
To update firmware from a local file:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to have their firmware updated, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Update Firmware**.





4. For each selected device, select **Upload Firmware File**.



5. Click **Browse** and select the file from your local file system.
6. Click **Update**.

View the status of device firmware updates

To view the status of device firmware updates

1. Click **Activity**

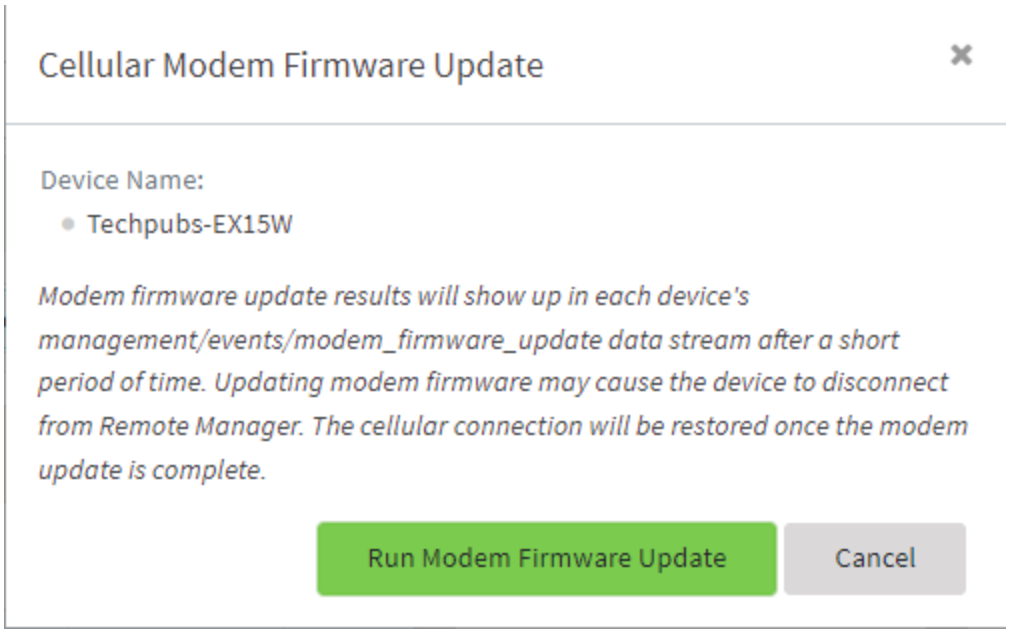
   Each update is represented as a job in the **Activity** page.
2. Select the update firmware activity and click **Actions** > **Activity Details** to view detailed information about the firmware update.

Update cellular modem firmware

To update cellular modem firmware:

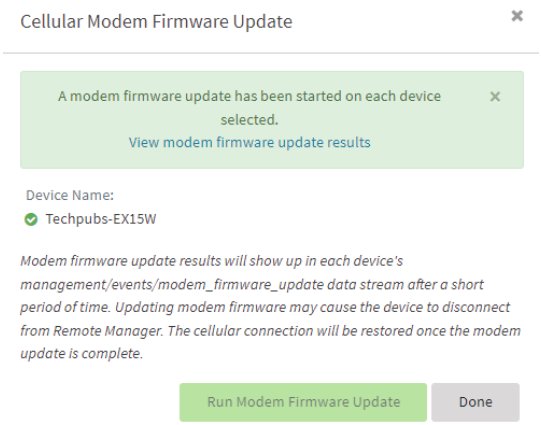
1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to have their modem firmware updated, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Cellular Modem Firmware Update**.

The **Cellular Modem Firmware Update** dialog is displayed.



4. Click **Run Modem Firmware Update**.

   The dialog is updated to indicate that the modem firmware update is taking place:



5. Click **View modem firmware update results** to open the Data Streams page filtered for this activity.

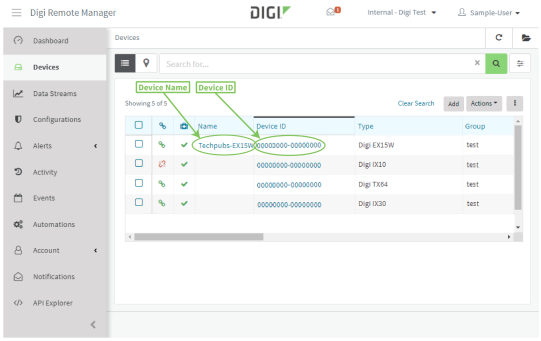
View and edit device details

Device details include:

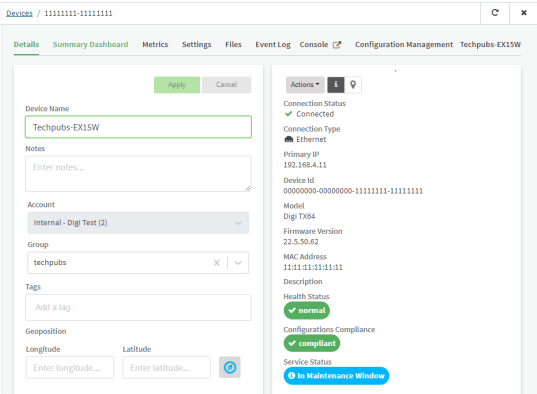
- **Device metadata**: **Device Name**, **Notes**, **Group**, and **Tags**. You can edit device metadata for connected and disconnected devices and the data is stored in Remote Manager, not on the device.
- **Device status**: **Connection Status**, **Device ID**, **Model**, **Primary IP**, **Firmware Version**, **MAC Address**, and **Health Status**.
- **Device alerts**: Lists of fired alerts for the device. Click on an alert to view the alert in the **Alerts** page.

To view device details:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



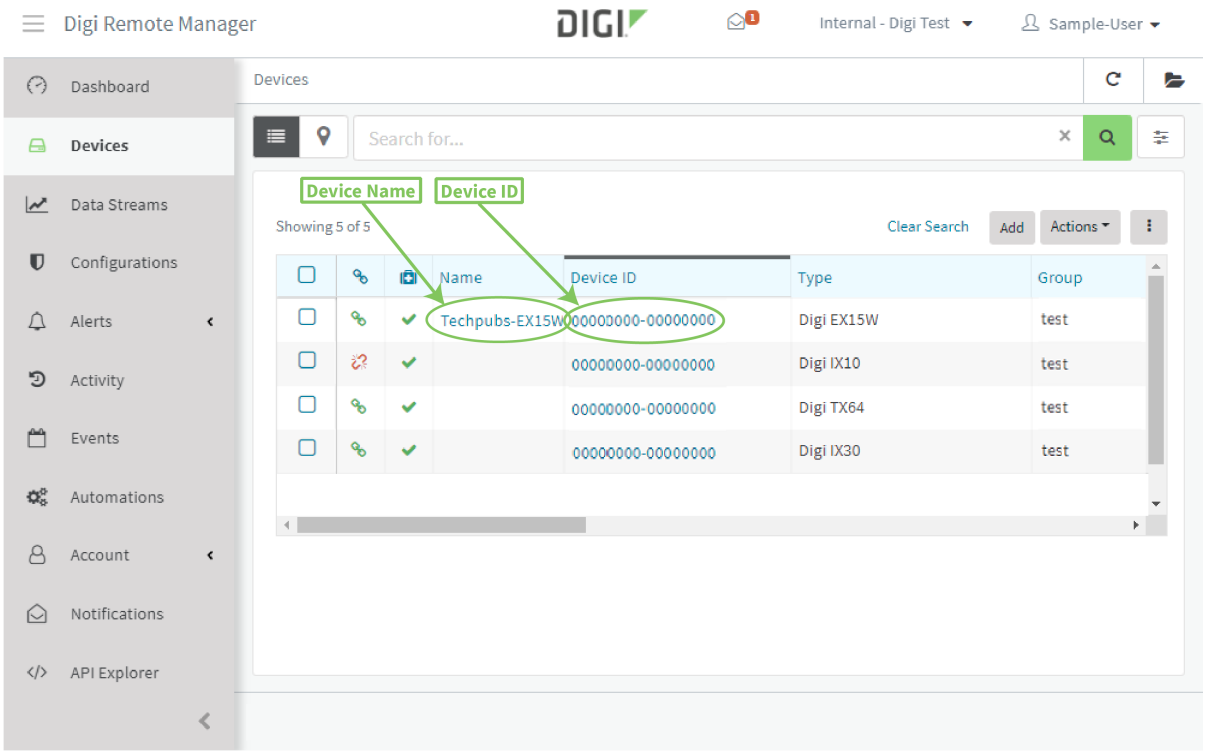
This section contains the following topics:

View device summary dashboard

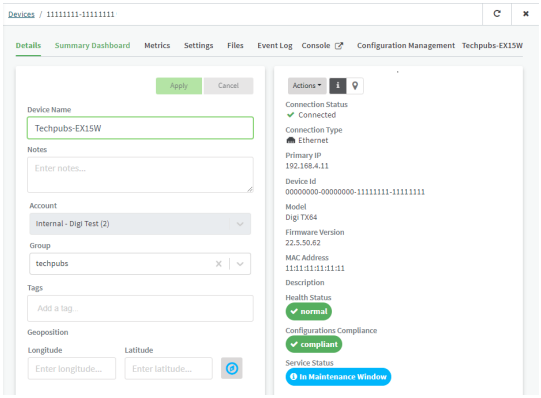
The device summary dashboard shows bar and table charts for the device connection history.

To view the device summary dashboard:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.

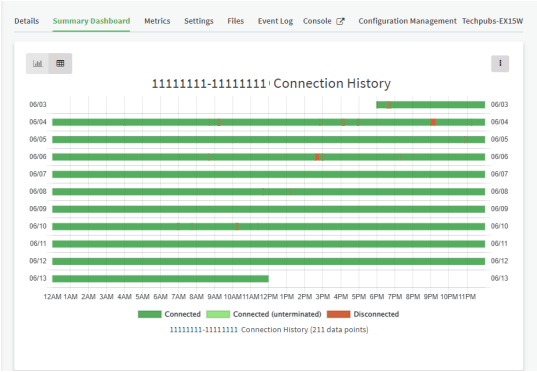


The device's **Details** page is displayed.



3. Click **Summary Dashboard**.

   The summary dashboard is displayed.



   - To view a bar chart of connection history, click ⓪
   - To view tabular data for connection history, click ⌀

The connection status displayed is one of:

- **Connected**
- **Disconnected**
- **Connected (unterminated)** —The device connected at the beginning of the session, but there was no session end. The device has since reconnected. As a result, there is a new connection event, but no previous disconnect event.

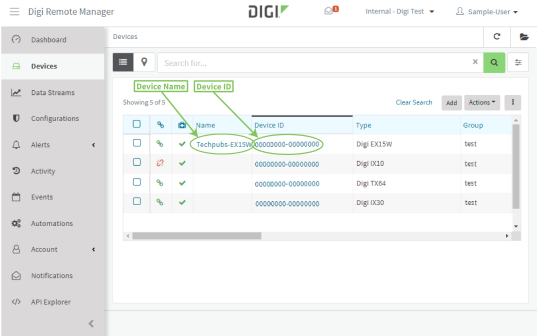
  This may be the result of infrastructure problems that sever the connection between Remote Manager and the device.

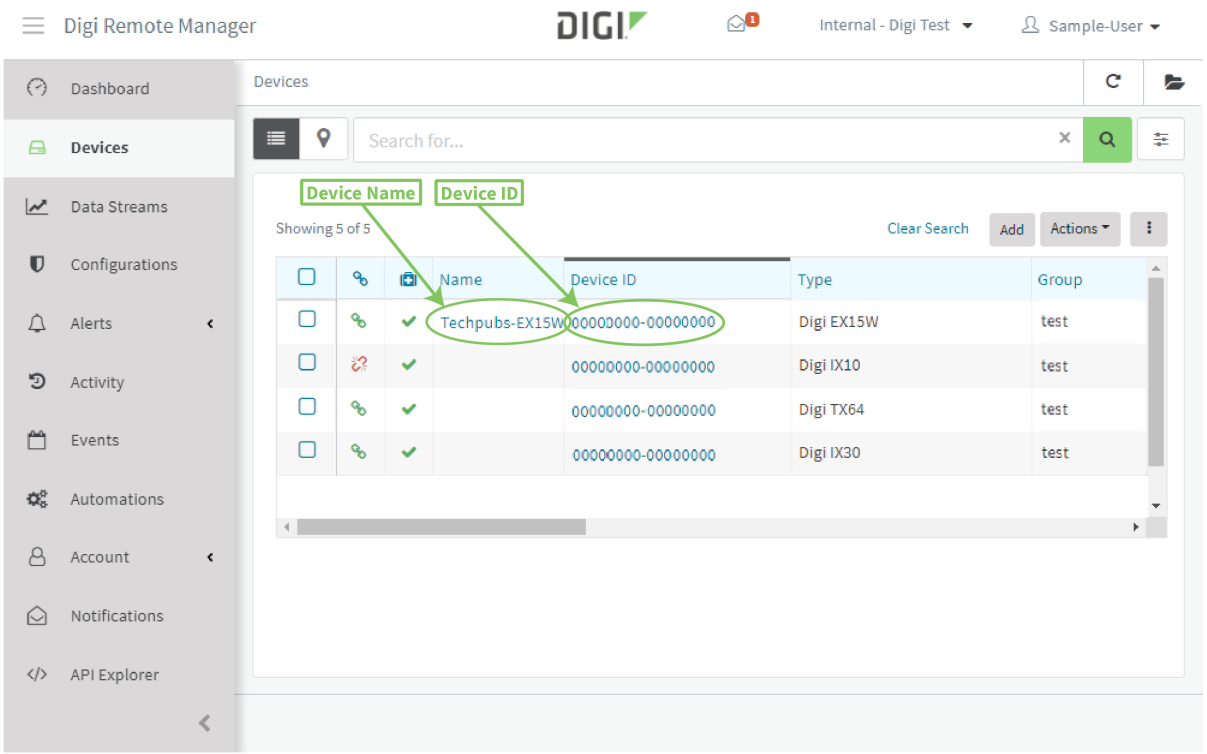
View and manage device metrics

If a device supports metrics reporting, the device **Metrics** page provides a detailed view of the latest metrics reported by the device to Remote Manager.

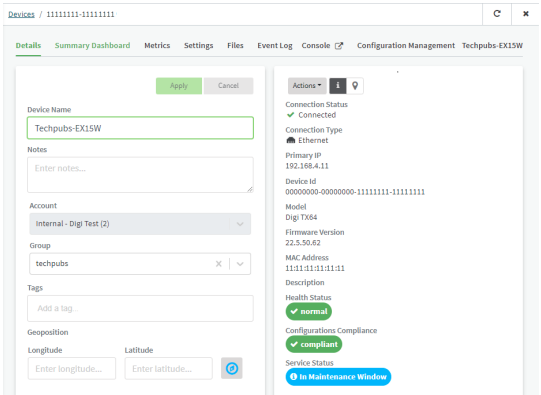
To view device metrics:

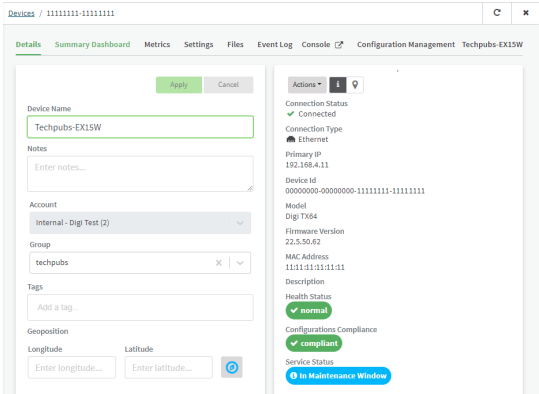
1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.





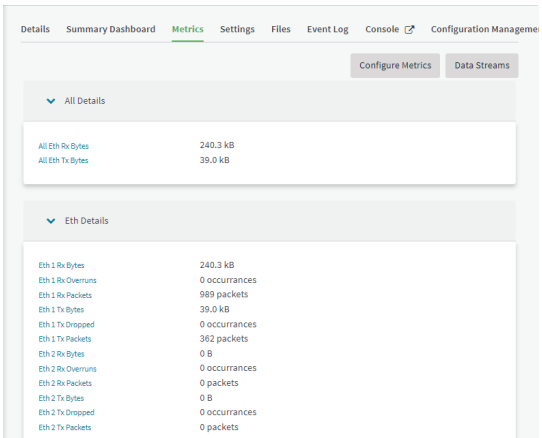
The device's **Details** page is displayed.





3. Click **Metrics**.

   The Device Metrics page displays.



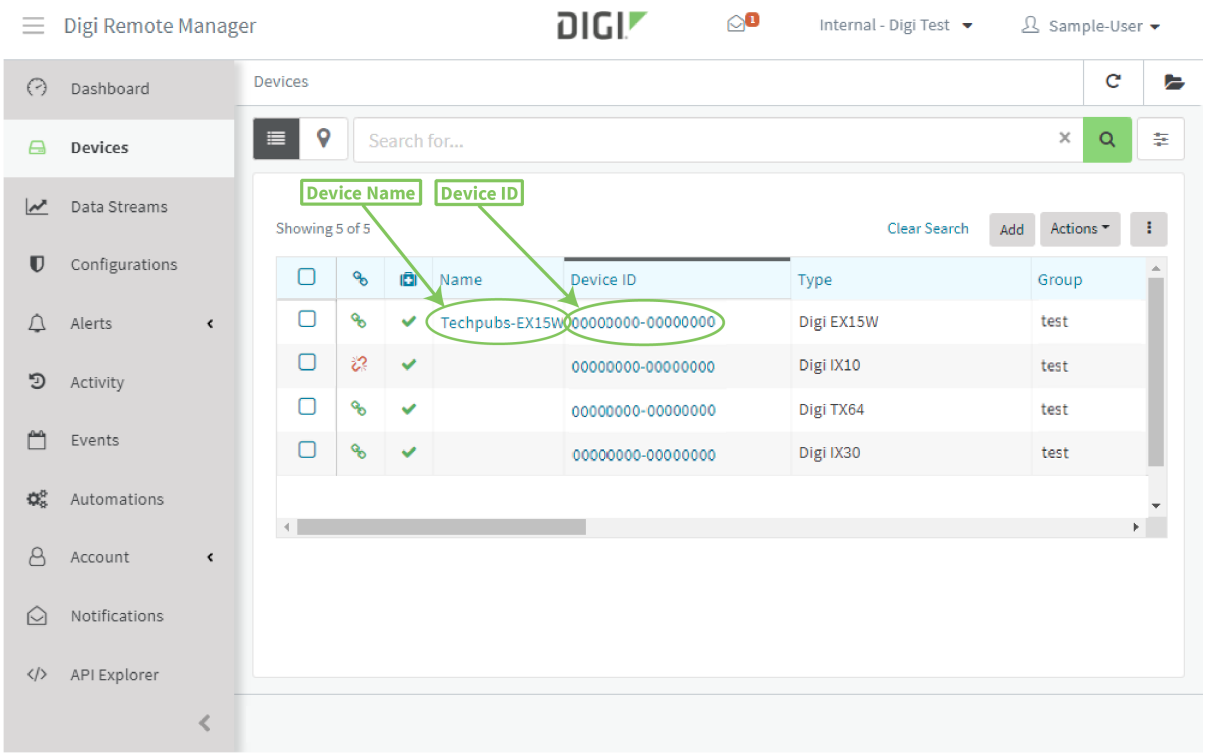
- Click **Configure Metrics** to go to the **Settings** > **Config** > **Monitoring** > **Device Health**, where you can configure the devices's metrics upload settings. See the documentation for the specific device for details about configuration of metrics uploads.
- Click **Data Streams** to go to the device's **Data Streams** page. See Data Streams for more details.

Edit a device's local settings

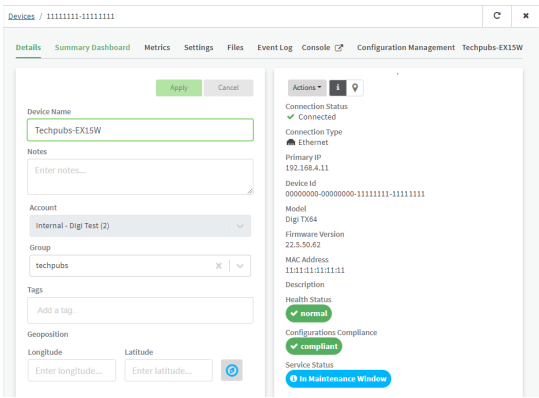
Note Use **Settings** page to create an initial configuration for a device type, or to configure devices that are not controlled by a Remote Manager configuration. If a device's configuration settings are controlled by a Remote Manager configuration, you should edit the configuration through **Configurations**. Digi recommends that you use Remote Manager configurations to manage your device configuration. See Configurations for more information.

To edit the configure for a device:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.

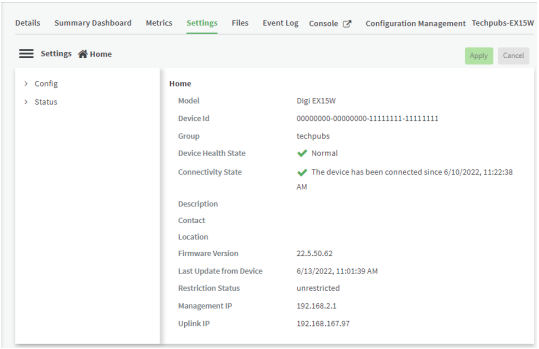


The device's **Details** page is displayed.

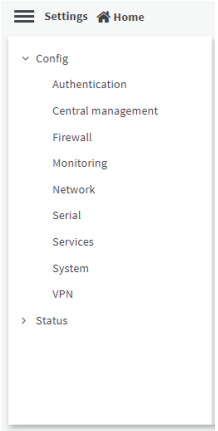


3. Click **Settings**.
4. Click **Config**.

   The **Settings** page is displayed.



5. Click to expand **Config**.



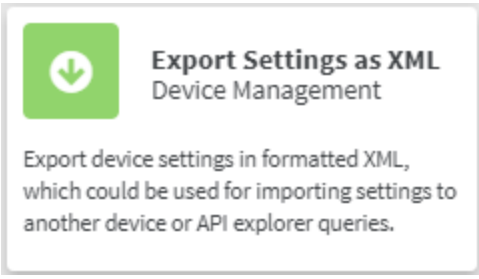
6. Click a configuration node to edit the settings for that node. For example, to edit user authentication settings, click **Authentication**.
7. Click **Apply** when finished.

Import and export device settings in XML format

You can export the settings for a device in XML format, and import those settings to other devices.

Export devices settings as XML

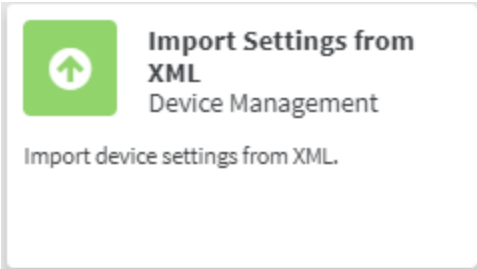
1. From the main menu, click **Management** > **Devices**.
2. Select a device to export its settings to XML, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Export Settings as XML**.



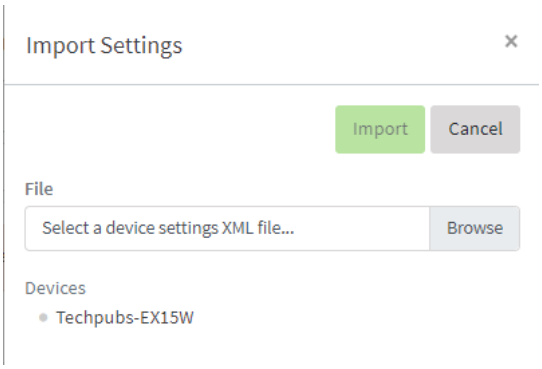
The XML file is downloaded to your local filesystem, using the filenaming convention device_settings_*mac_address*.xml.

Import devices settings as XML

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to import XML settings to, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Import Settings from XML**.



The **Import Settings** pane displays.



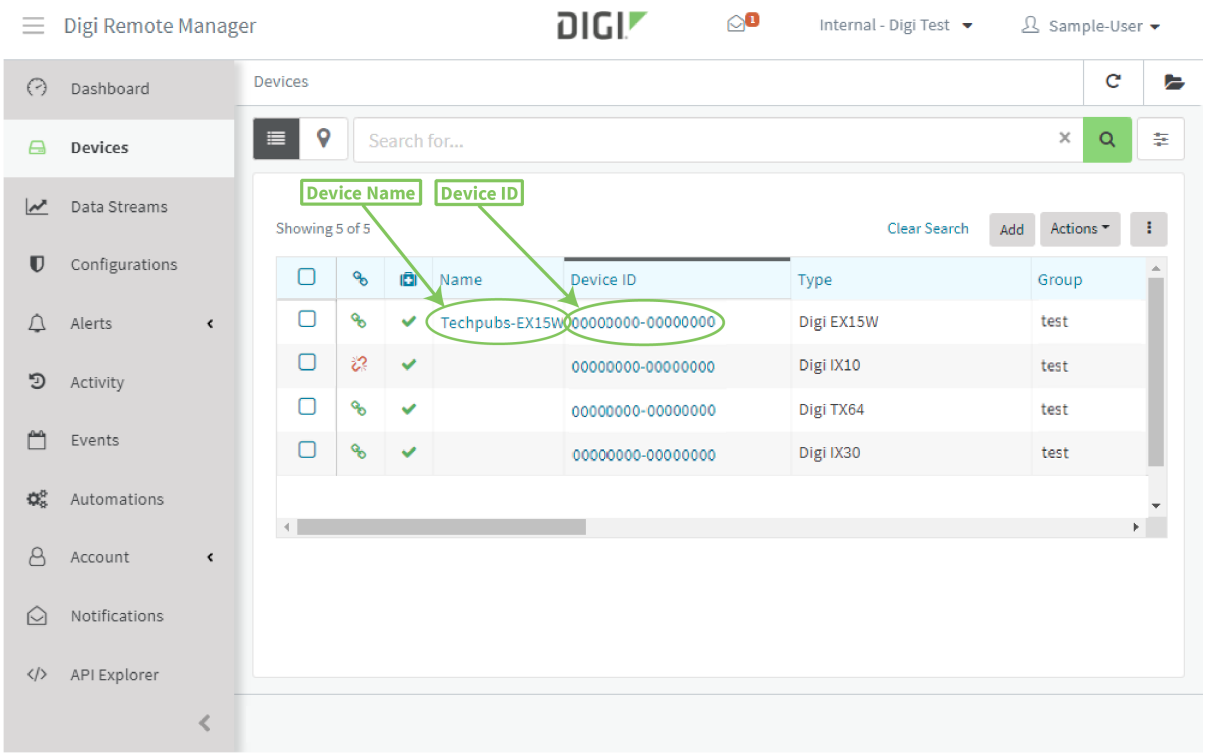
4. Click **Browse** and select the appropriate XML file from your local filesystem.
5. Click **Import**.

View and manage device files

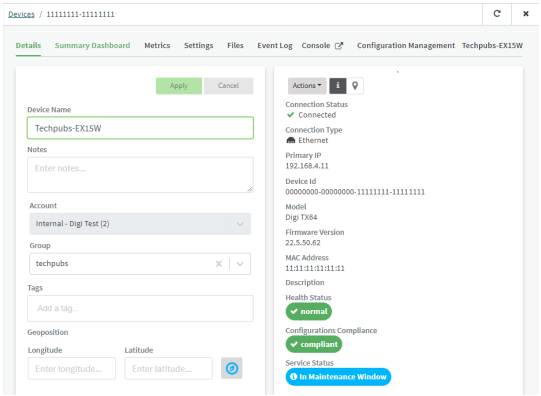
For devices that provide a file system, Remote Manager allows you to view and manage device files for connected devices. If you attempt to view files for a device that is not currently connected to Remote Manager, the message Device Not Connected is displayed.

To view and manage device files:

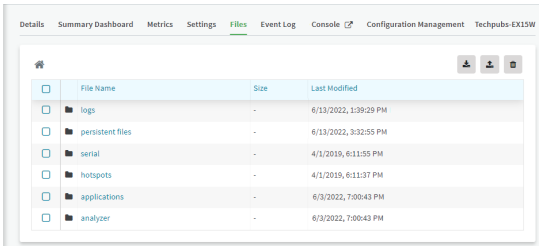
1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



3. Click **Files**.



- To download a file from the device to your local computer, click .
- To upload a file from your local system to the device, click ❽
- To delete a file or directory, select the item, and click .
- To return to the home directory, click .

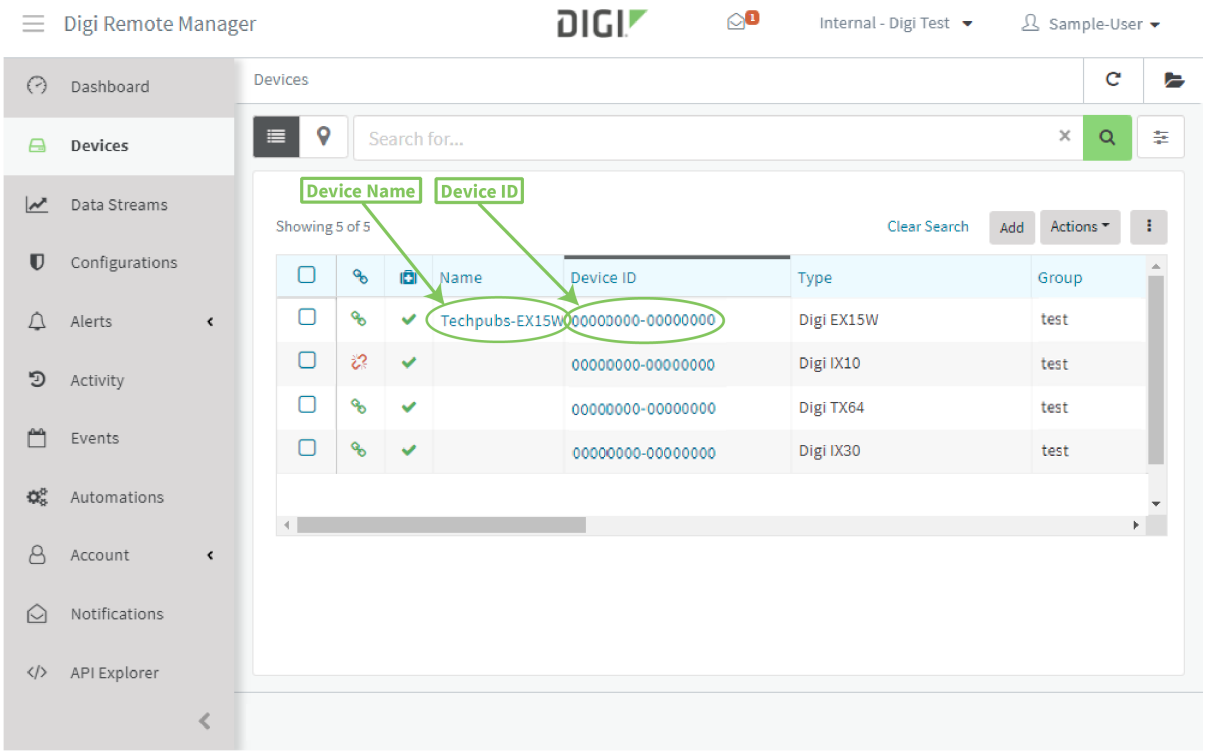
View and manage device event logs

Devices that support uploading event logs to Remote Manager Can be configured to upload their event logs on a periodic basis.

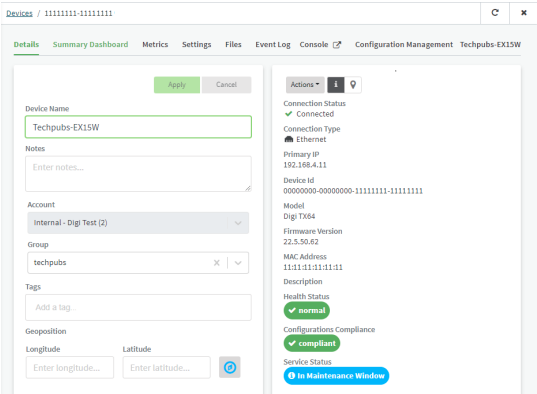
Note Event logging may affect your data plan.

To view and manage device event logs:

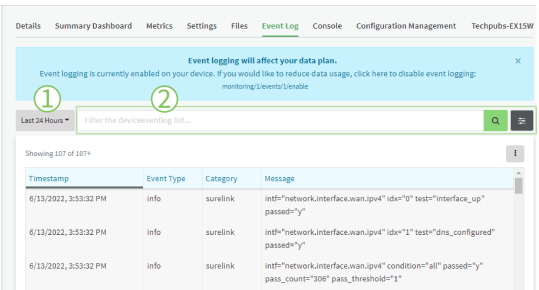
1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



2. Click **Event Logs**.



#	Component	Description
1	Date range	Select the range of dates that you would like to view event logs from, or enter a range in **Start date** and **End date**. 
2	Event log search	▪ Click ▇ to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in

#	Component	Description
		the filter bar to select a filtering category:  ▪ Click to filter the display. ▪ Click to clear the filter criteria.

Use a device console

For devices that provide terminal access, Remote Manager allows you to access a device console and execute commands. If you attempt to access a console for a device that is not currently connected to Remote Manager, the message Device Not Connected is displayed.

You can open a console connection to a device in a new browser tab from the **Devices** page, or you can open a console connection in the same browser tab from **Device Details**.

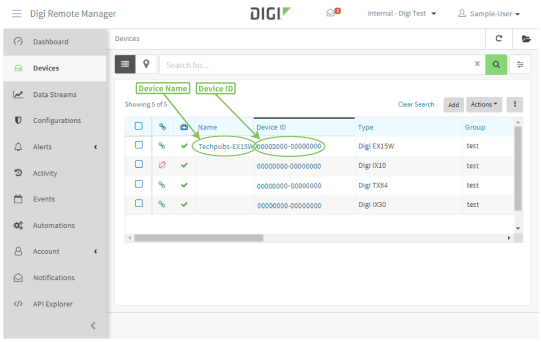
Open a device console in a new browser tab

1. From the main menu, click **Management** > **Devices**.
2. Select a device.
3. From the **Actions** menu, select **Open Console**.

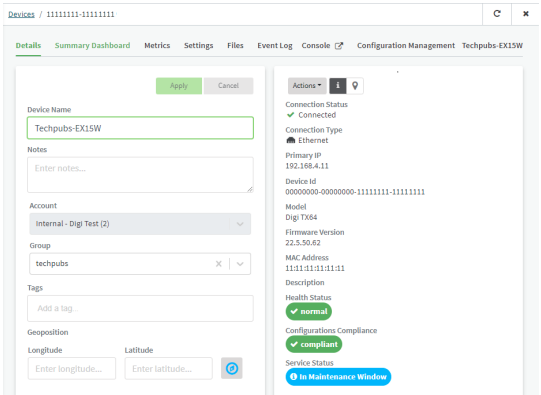
A console connection is opened in new browser tab.

You can also open the device console in a new browser tab from the device details page:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



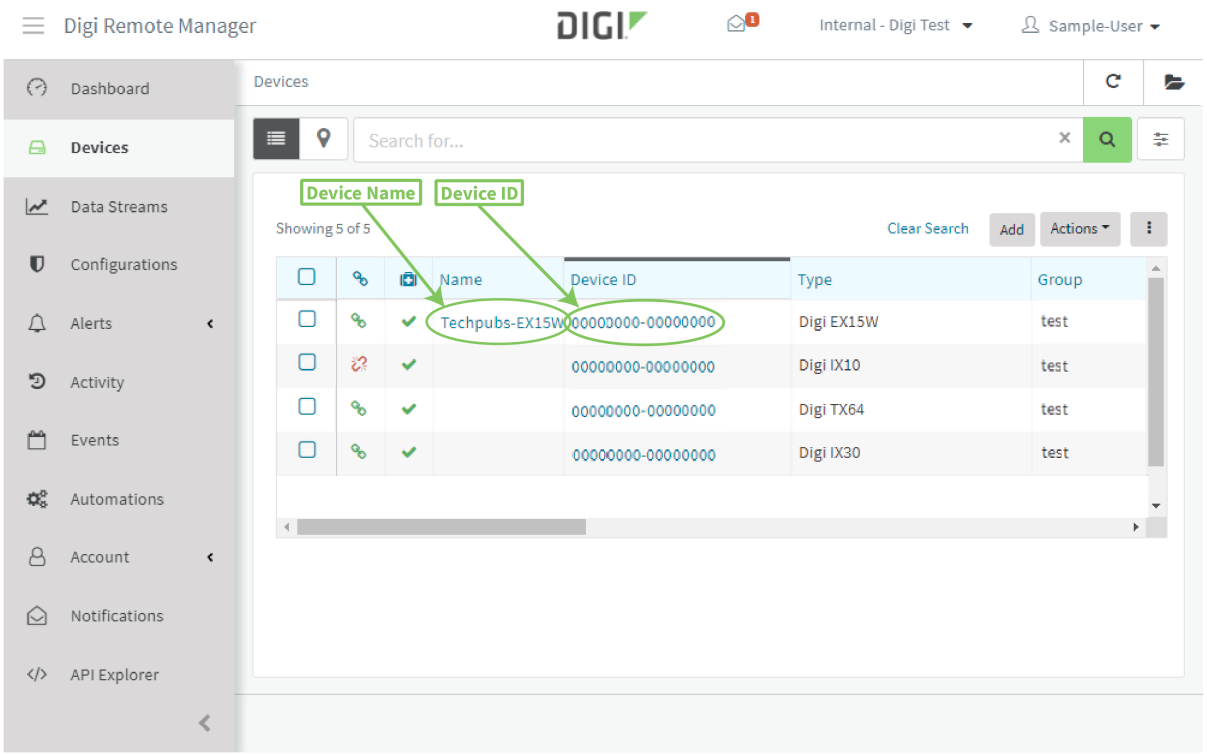
The device's **Details** page is displayed.



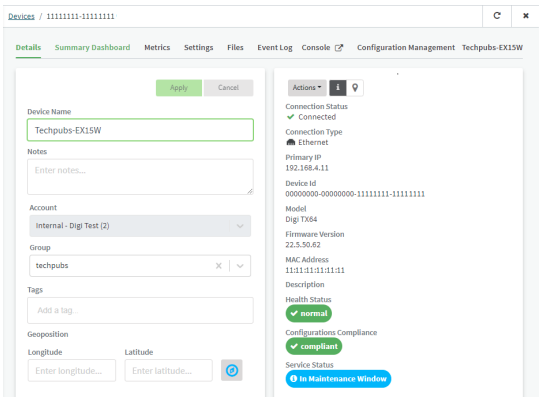
3. Click ❸ next to **Console**.

Open a device console in the same tab

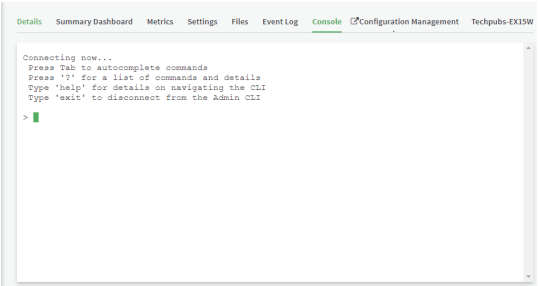
1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



3. Click **Console**.

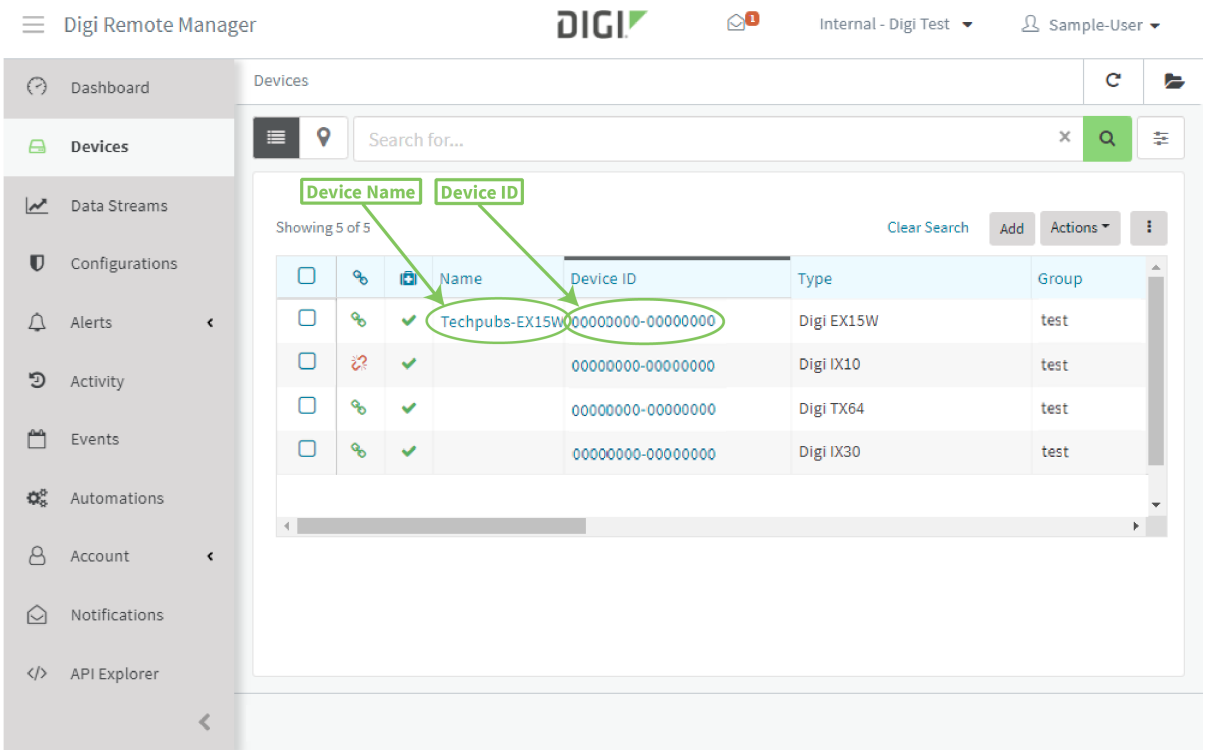


4. Once you have opened the device console, you can open it in a new window by clicking ❸next to **Console**.

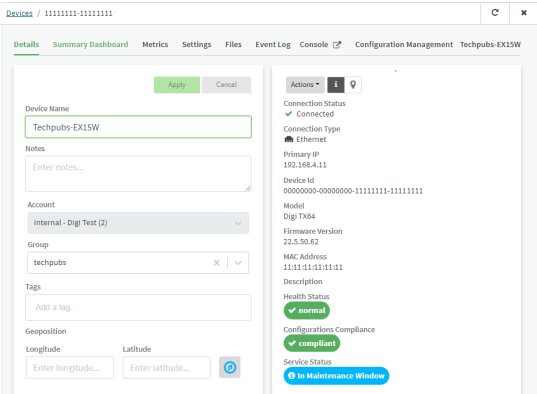
View a device's configuration

If the device is being controlled by a Remote Manager configuration, you can view the configuration:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



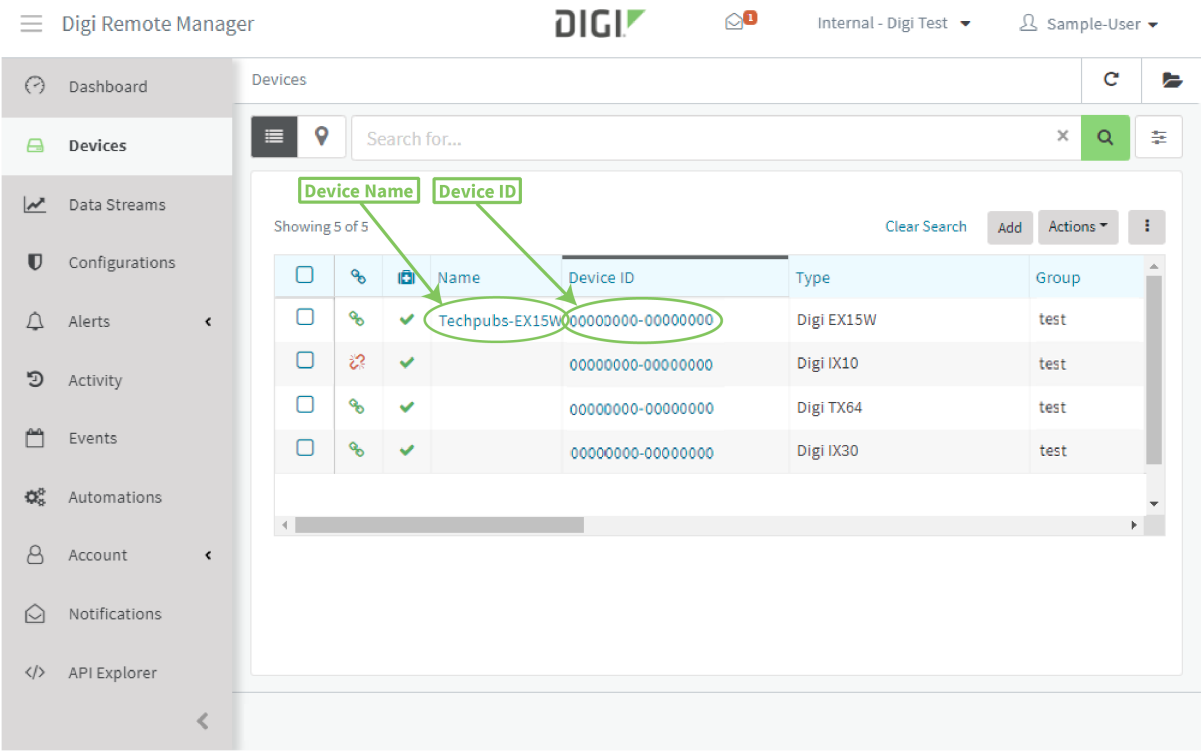
3. Click **Configuration Management**.

This will take you to the configuration that controls the device's settings.

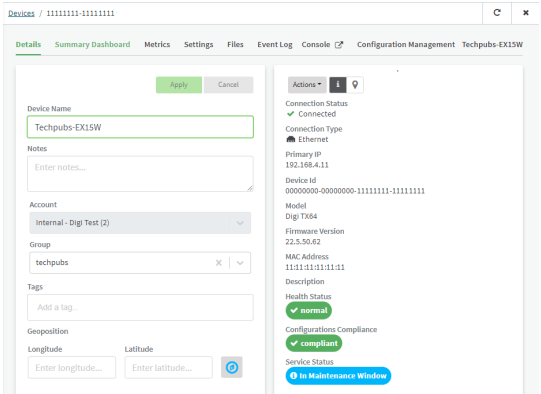
View configuration scan history for a device

From the device details page, you can view the configuration scan history for a device.

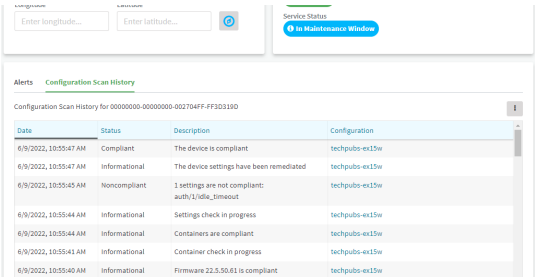
1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



The device's **Details** page is displayed.



3. Scroll down and click **Configuration Scan History**.



Organize devices: groups, tags, and notes

This section describes how to organize devices using device groups, device tags, and metadata.

Device groups

You can create groups within Remote Manager to organize and manage your devices.

- To organize devices, create a hierarchical structure of groups and then move devices into the desired groups.
- To manage devices, create a Configuration for a group and then move devices into the group with the desired Configuration. In this way, all devices of the same type within the group will automatically comply with the Configuration for the group. See Configurations.

Device tags

Remote Manager uses tags to categorize devices. You can sort devices by tags in screens that have a device list, such as the **Devices** page or when adding a schedule. This feature is useful if you want to create a set of devices that are in different device groups.

Device notes

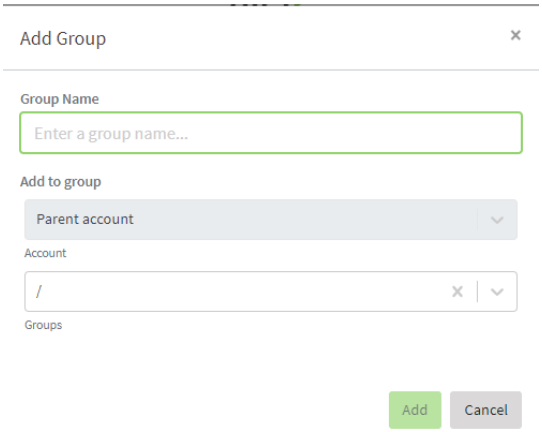
Notes provide unstructured information associated with a device and can help to identify a device, find a device, or simply provide additional information about a device.

This section contains the following topics:

Create device groups

The groups feature allows you to add or create a group and assign a list of devices to that group. You can create a hierarchical structure of device groups to help organize your device inventory.

1. From the main menu, click **Management** > **Devices**.
2. Click to display device groups.
3. Click
   The **Add Group** dialog displays.



4. For **Group Name**, type a name for the group.
   The group name can contain letters, numbers, as well as dashes, periods and spaces.
   A forward slash will create a subgroup.
5. (Optional) For **Groups**, select an existing group that the group you are creating will be a subgroup of.
6. Click **Add**.

Add devices to a group

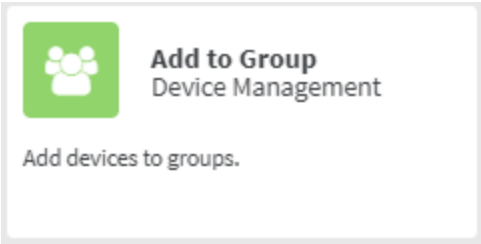
You can add one or more devices to a device group, and can add up to 500 devices to a group at one time. Create at least one device group before adding devices to groups.

CAUTION! Some groups are managed by one or more Configurations. If a group is managed by an active configuration, use caution when adding a device to the group because the device configuration will be automatically updated to match the group configuration for that device type. If you do not intend to change the device configuration, do not move the device to a group associated with a managed configuration.

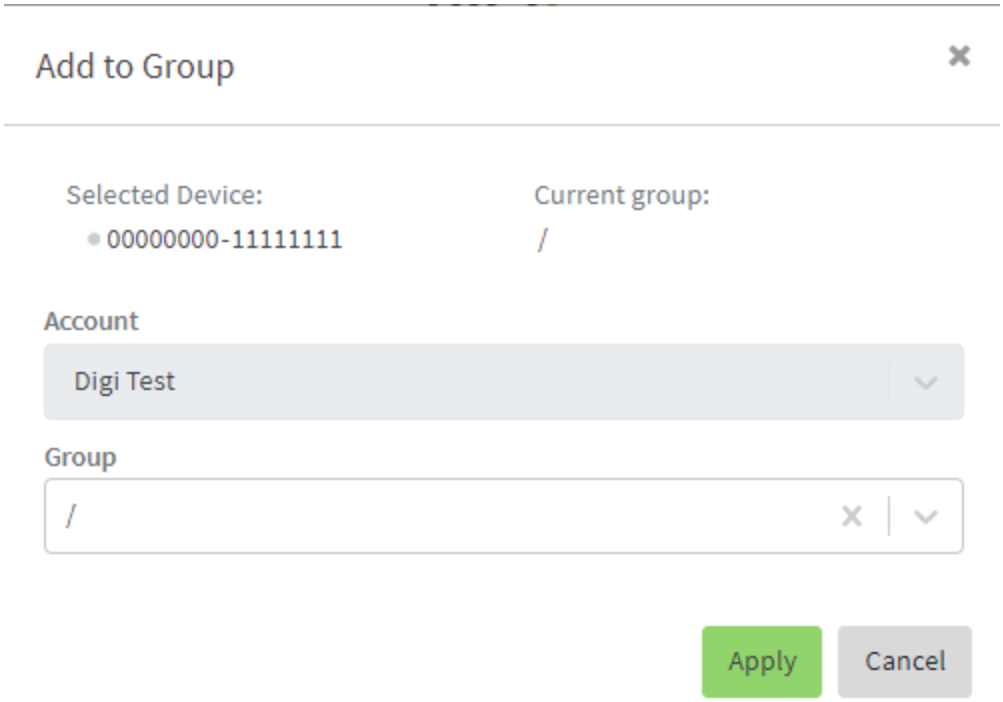
To add a device to a group

1. If needed, create the device group. See Create device groups.
2. From the main menu, click **Management** > **Devices**.
3. Select one or more devices to add to a group.

4. From the **Actions** menu, click **Add To Group**.



The **Add To Group** dialog is displayed.



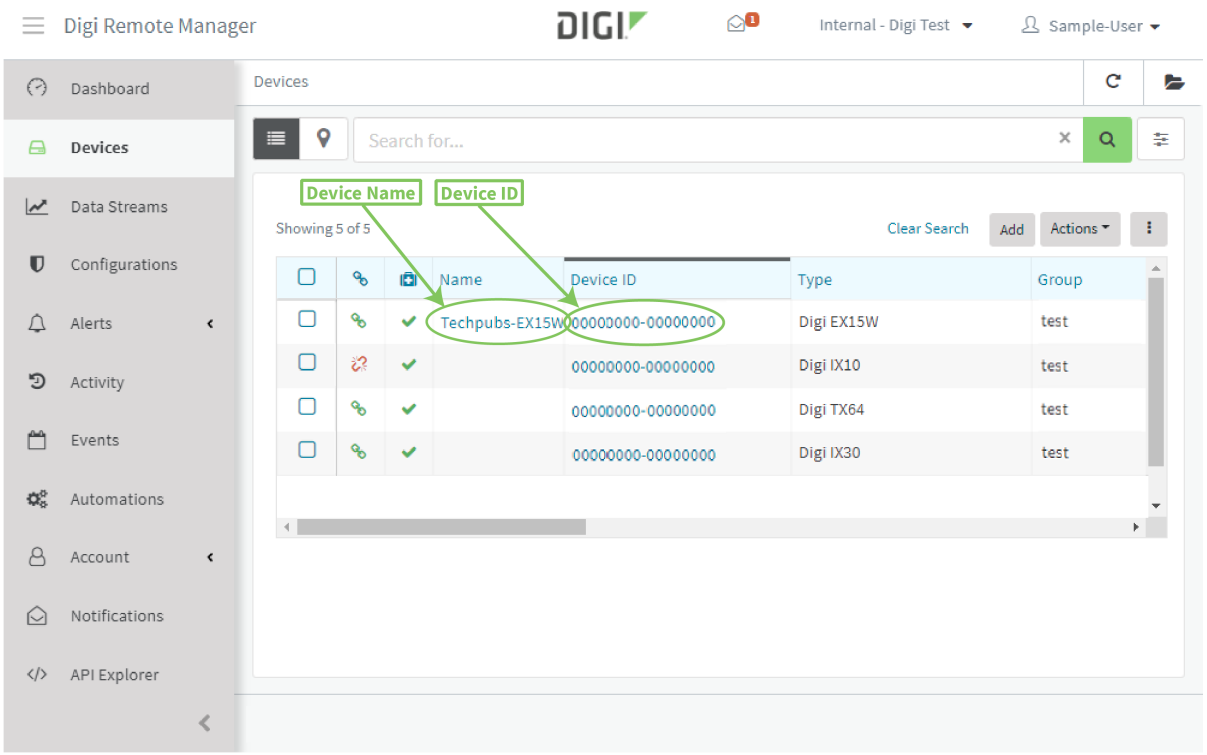
5. For **Group**, select the group that the device will be added to.
6. Click **Apply**.

You can also:
Drag-and-drop devices into a group:

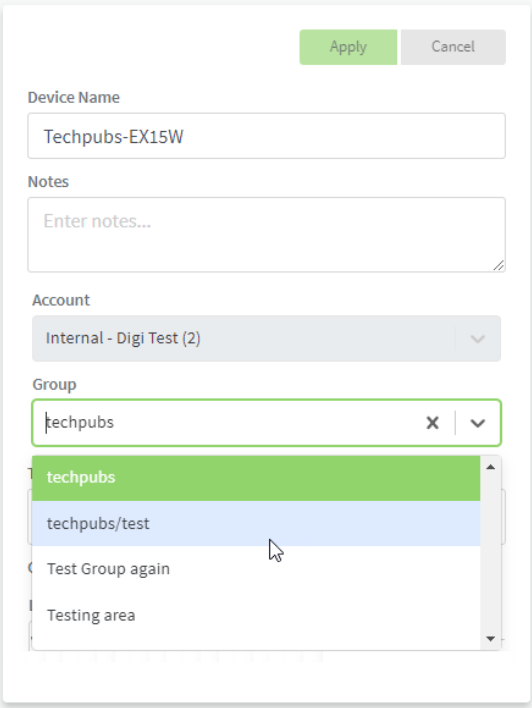
1. At the Devices page, click to display device groups.
2. Drag-and-drop devices onto a group in the **Groups** list. Select devices to drag-and-drop multiple devices at the same time.
3. Click **Apply** to confirm.

Change the group for an individual device from the **Device Details** view:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



3. In the device's **Details** view, change the **Group** to the appropriate group:



4. Click **Apply**.

Edit a device group name

You can edit device group properties, including the group name and its parent in the groups hierarchy.

To edit the name of a device group:

1. From the main menu, click **Management** > **Devices**.
2. Click to display device groups.
3. Select the group you want to rename
4. Click
5. Type a new name for the group and click **Save**.

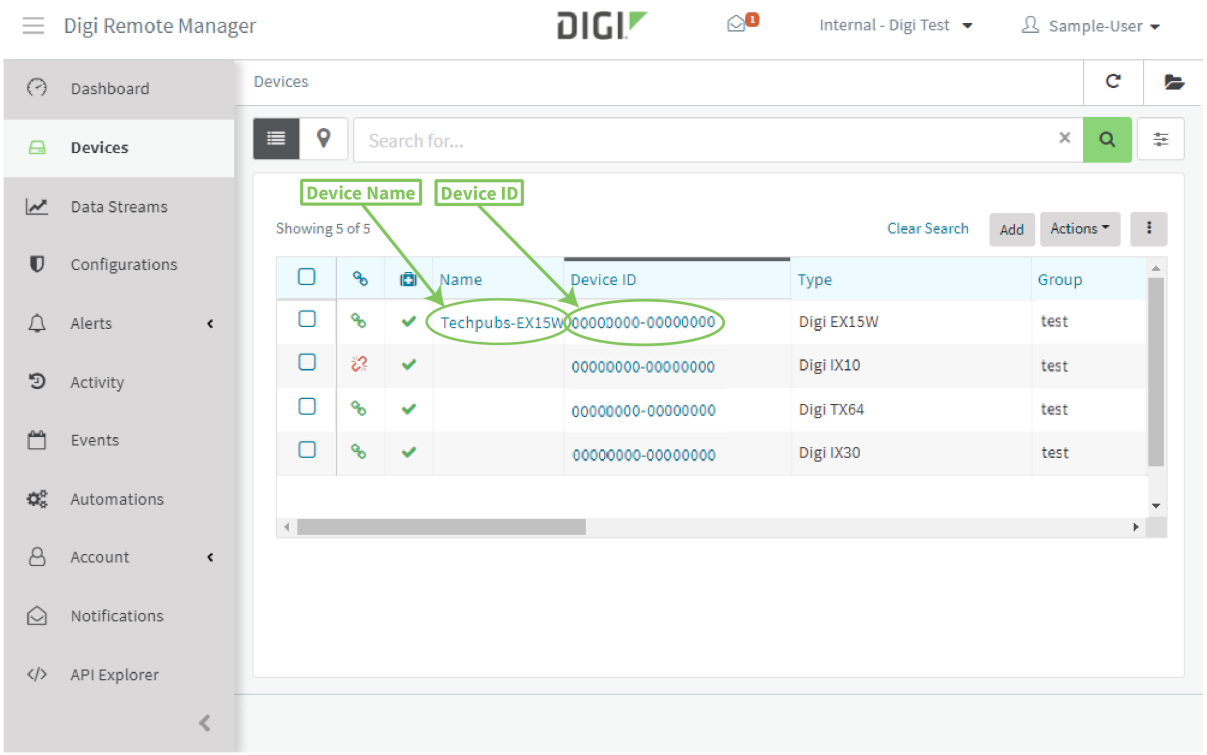
Remove a device from a device group

You can remove a device group by moving it to the root folder or to another device group.

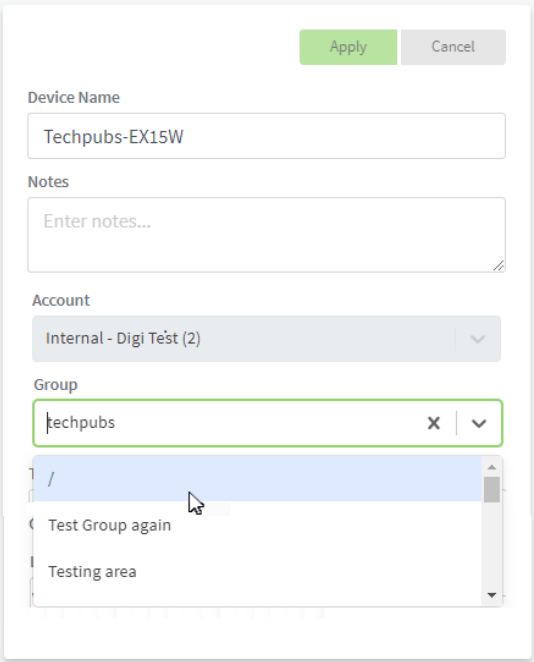
CAUTION! Some groups are managed by one or more Configurations. If a group is managed by an active configuration, use caution when removing a device from the group because the device configuration will cease to be managed. If you want to continue managing the device configuration using the group, do not remove the device from the group.

To remove a device from a group:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



3. In the device's **Details** view, change the **Group** to **/** (slash) to remove the device from the group:



4. Click **Apply**.

Show or hide device groups

To show or hide device groups

1. From the main menu, click **Management** > **Devices**.
2. Click to display device groups.
3. Click again to hide the device groups.

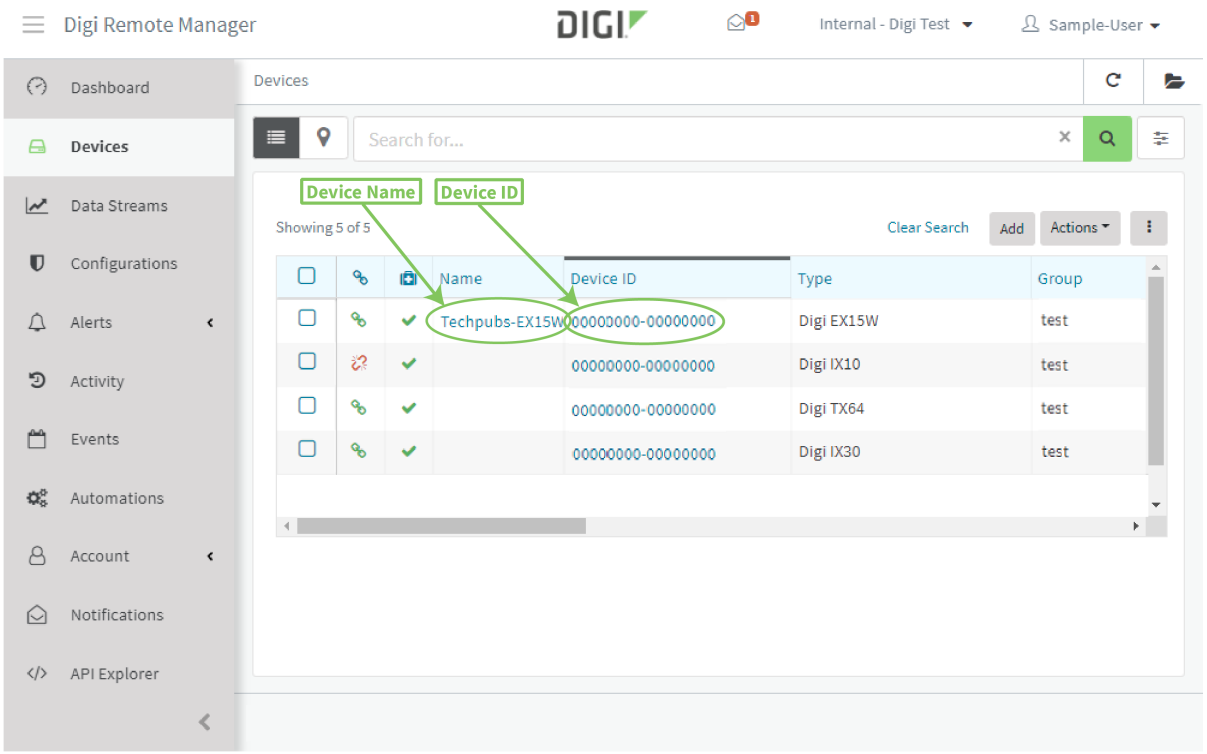
Add or edit device tags

You can add tags to a device to help categorize that device.

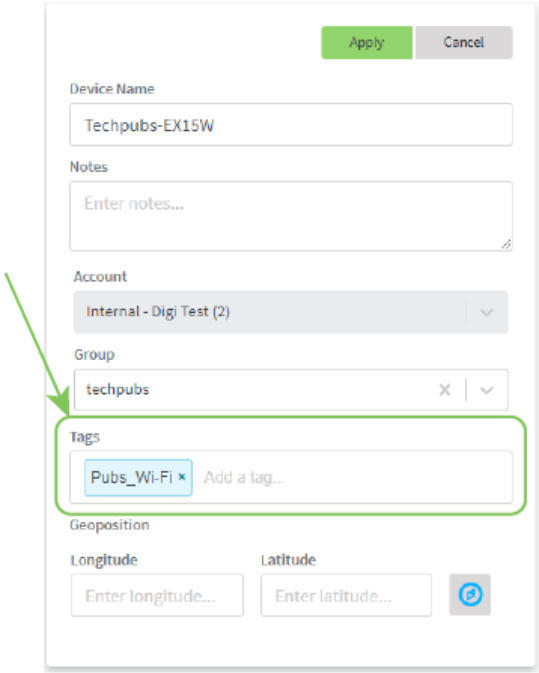
Note Device tags are stored in Remote Manager, not on the device.

To add or edit a device tag:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



3. In the device's **Details** view, type one or more **Tags** for the device:



4. Click **Apply**.

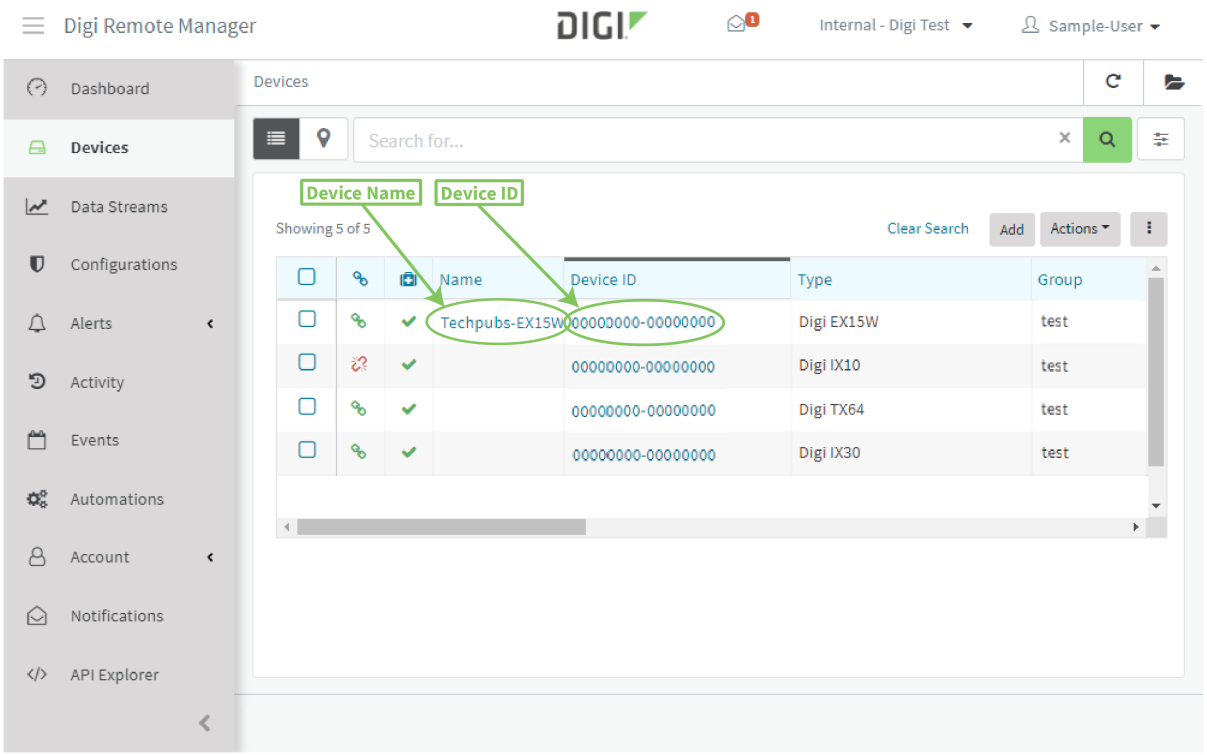
Add or edit device notes

You can add notes to a device to help categorize or identify the device.

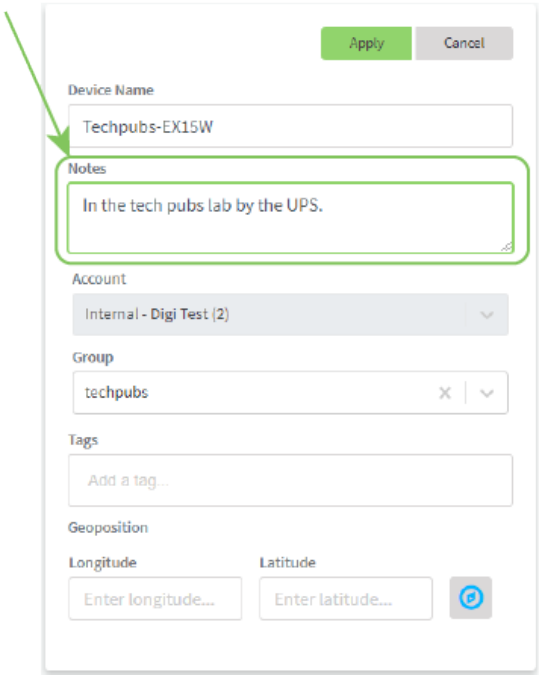
Note Device notes are stored in Remote Manager, not on the device.

To add or edit device notes:

1. From the main menu, click **Management** > **Devices**.
2. In the device list, click the device **Name** or **Device ID**.



3. In the device's **Details** view, type **Notes** for the device:

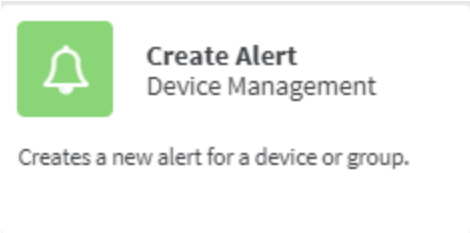


4. Click **Apply**.

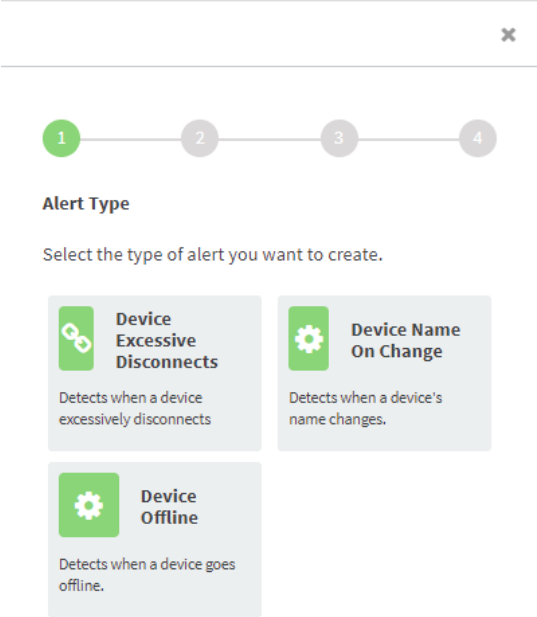
Download a support report

To download a support report for a device:

1. From the main menu, click **Management** > **Devices**.
2. Select a device to download a support report from, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Download Support Report**.



The **Download Support Report** dialog is displayed.



4. Click **Generate and Download**.

The support report is downloaded to your local file system.

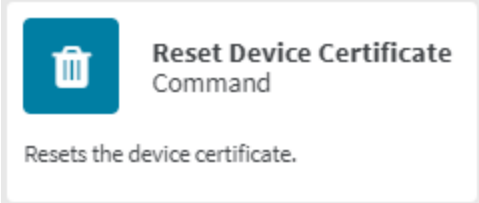
Reset the device's client side certificate

For cellular routers and related products using the Digi Accelerated Linux (DAL) firmware with firmware version 22.2.9.x and above, the default URL for the device's Digi Remote Manager connection is edp12.devicecloud.com. This URL is required to utilize the client-side certificate support. Prior to release 22.2.9.x, the default URL was my.devicecloud.com. The new URL of edp12.devicecloud.com is for device communication only. Use my.devicecloud.com for user interaction with remote manager.

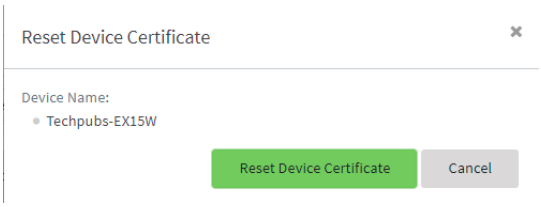
- If you perform a factory reset on the DAL device by pressing the **Reset** or **Erase button** twice, the client-side certificate will be erased and you must use the Remote Manager interface to reset the certificate.
- If you downgrade your firmware from version 22.2.9.x to version 21.11.x or previous, your device will no longer be able to communicate with Remote Manager and you must use the Remote Manager interface to reset the certificate.

To reset the device's client side certificate:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to have their device certificates reset, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Reset Device Certificate**.



The **Reset Device Certificate** dialog is displayed.



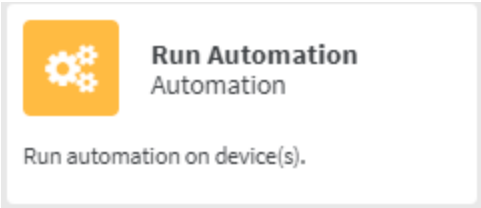
4. Click **Reset Device Certificate**.

Run an automation for a device

Automations are commands and scripted events that can be run against a device, or against multiple devices. See Automations for more information, including how to create automations.

To run an automation:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to run an automation against, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Run Automation**.



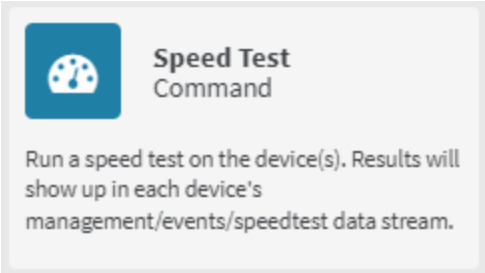
4. Select an automation and click **Run**.

Click **Automation Runs** to view the results of the automation.

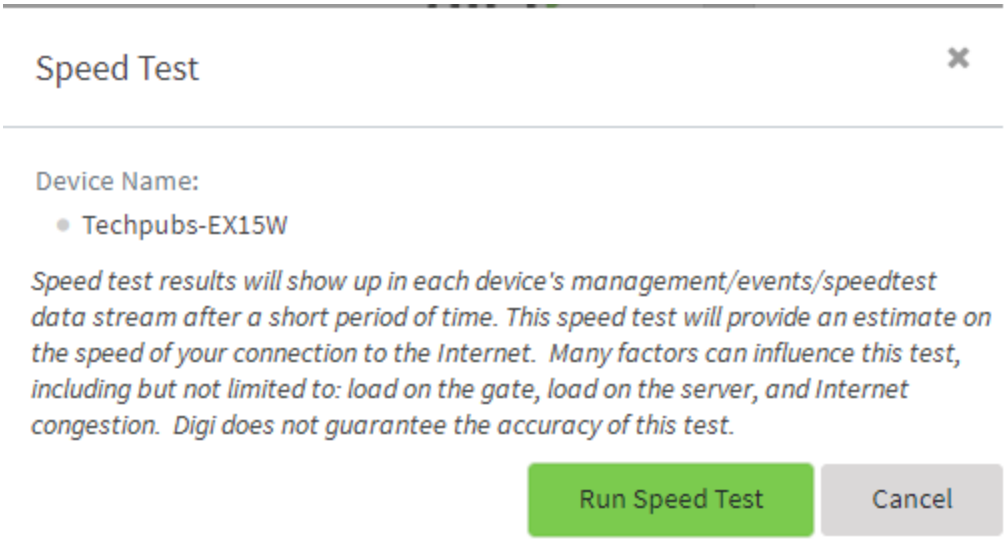
Run a speed test for a device

To run a speed test for a device:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to run a speed test for, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Speed Test**.



The **Speed Test** dialog is displayed.



4. Click **Run Speed Test**.
5. Click **View Speed Test data streams**.

   The Data Streams page displays, filtered for the speed test.

   a. Select the data stream.

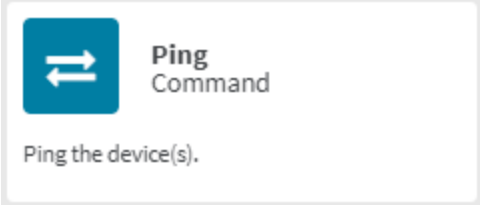
   b. Click to view the results in tabular format.

Ping a device

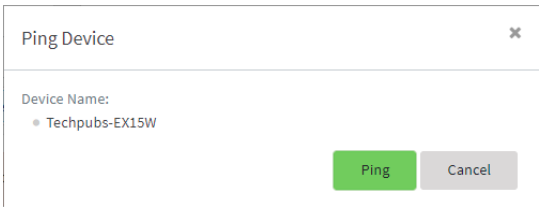
You can ping a device from your Remote Manager account to determine the round trip latency of a device connection. The result gives the actual time used to send a simple command to the device and receive a reply.

To ping a device:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to ping, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Ping**.



The **Ping** dialog is displayed.



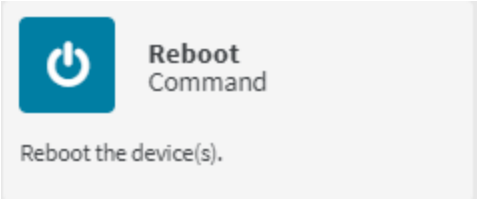
4. Click **Ping**.

The response time of the ping is displayed, or, if the ping was unsuccessful, an error message is displayed.

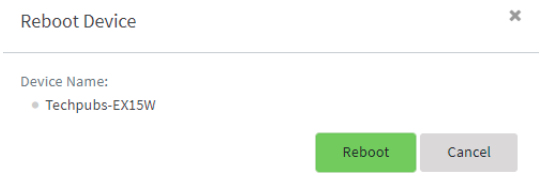
Reboot a device

To reboot one or more devices:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to reboot, or click a device **Name** or **Device ID** to open the **Device Details** view.
2. From the **Actions** menu, click **Reboot**.



The **Reboot** dialog is displayed.

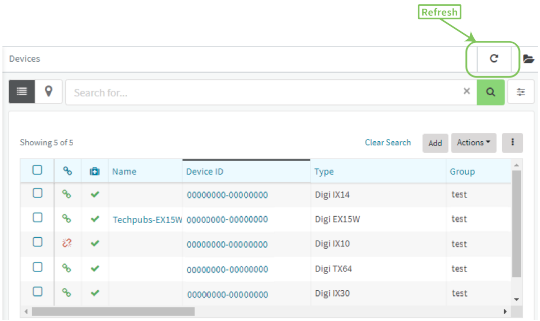


3. Click **Reboot**.

Refresh device information

To refresh device information

1. From the main menu, click **Management** > **Devices**.
2. Click .

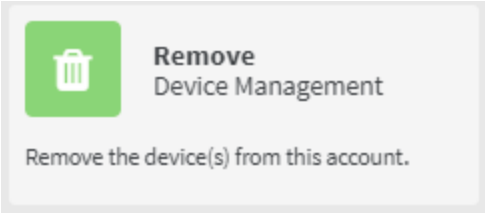


Remove a device

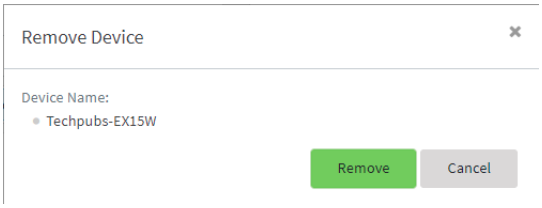
If you no longer need to monitor or manage a device in your Remote Manager inventory, you can remove the device from Remote Manager.

To remove a device:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to remove, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Remove**.



The **Remove** dialog is displayed.



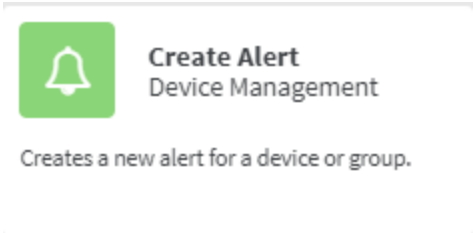
4. Click **Remove**.

Create an alert for a group or device

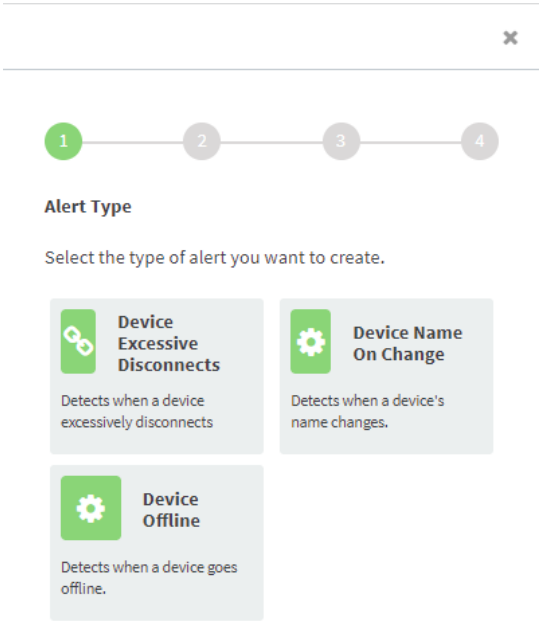
You can create an alert for the group or device from the **Devices** page.

- If you select a group to filter the device display, the group will be automatically used for the scope of the alert.
- If you select a device, or create an alert from the **Device Details** page, the device ID will be automatically used for the scope of the alert.

1. From the main menu, click **Management** > **Devices**.
2. From the **Actions** menu, click **Create Alert**.



The **Create Alert** dialog is displayed.

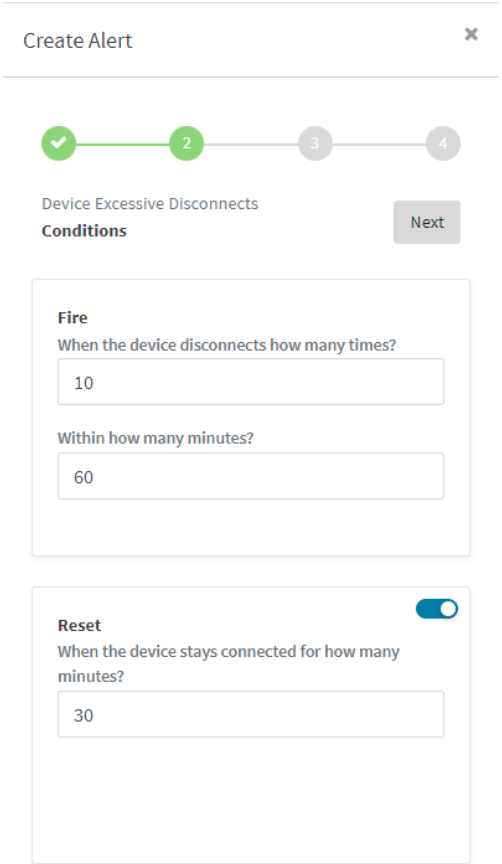


3. Click the applicable **Alert Type**.

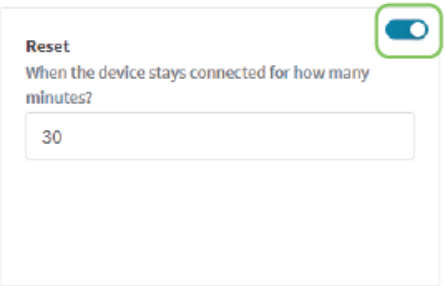
   The **Conditions** page displays. The **Conditions** page varies depending on the type of alert being created:

   Device Excessive Disconnects:

   Defines a threshold for excessive disconnects and generates an alert when a device's disconnects exceed the threshold.



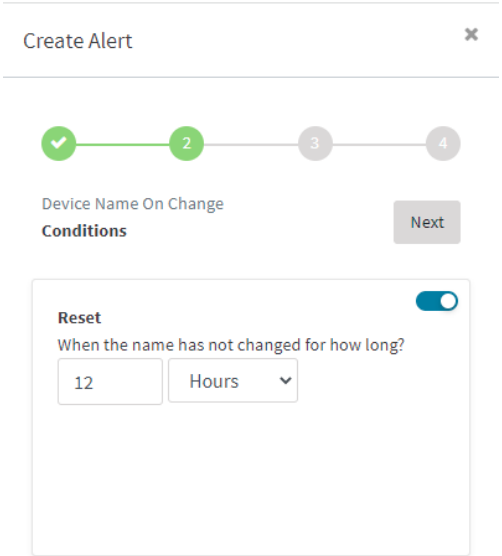
   - The **Fire** section defines the number of disconnects within a period of time that will be considered excessive and will therefore fire the alert:
     a. Define the number of disconnects.
     b. Define the number of minutes during which the defined number of disconnects should take place to be considered excessive.
   - The **Reset** section defines when the alert will be automatically reset:
     a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



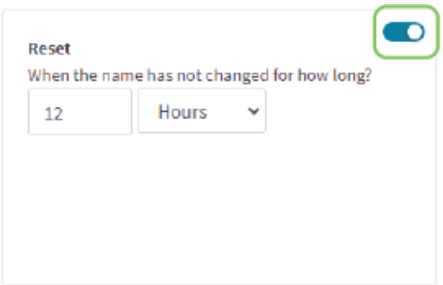
b. Select the number of minutes that the device should stay connected before the alert is automatically reset.

Device Name On Change:

Generates an alert when a device's name changes.



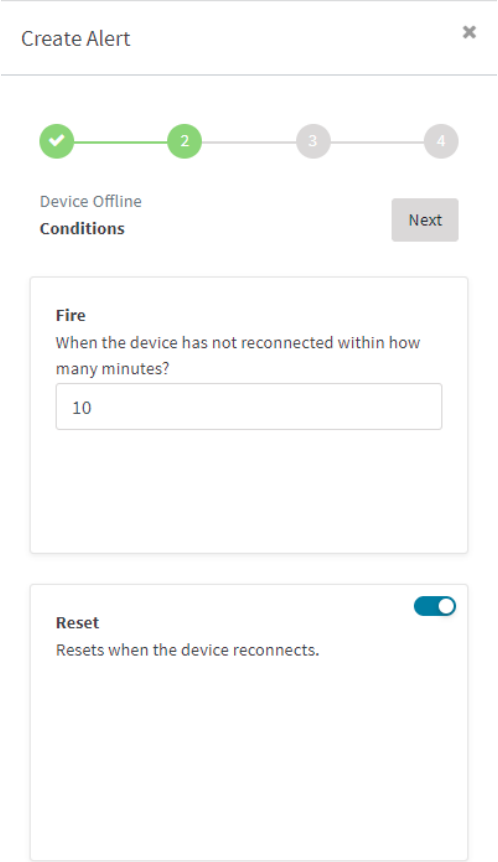
- The **Reset** section defines when the alert will be automatically reset:
  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



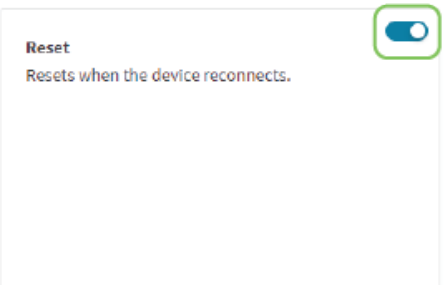
b. Select the amount of time that the device name should stay the same after a device name change, before the alert is automatically reset.

Device Offline:

Detects when a device goes offline.



- The **Fire** section defines the conditions that will cause the alert to be generated:
  a. Select the number of minutes that the device has not been connected.
- The **Reset** section defines when the alert will be automatically reset:
  a. If the alert should not be automatically reset, click the reset toggle button to disable automatic resets.



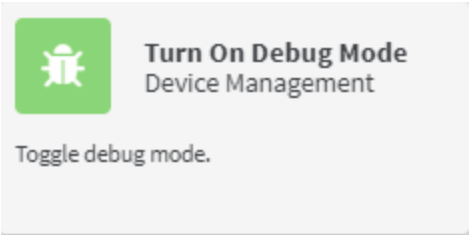
Turn on/off debug mode

In Remote Manager, devices can be put into debug mode. When a device is in debug mode, alerts for the device fire and reset, but alert notifications for the device are not sent. Devices in debug mode show a ✱ in the **Connection Status** column and the message **Debug Mode On** in device details for connection status.

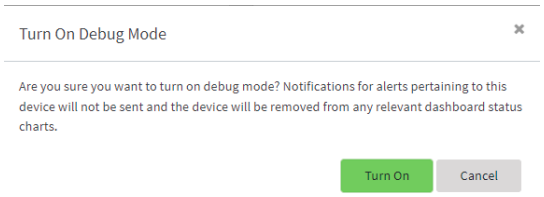
Note Devices in debug mode are excluded from all dashboard charts.

Turn on debug mode for a device

1. From the main menu, click ✱**Management** > ▪ **Devices**.
2. Select a device to turn the debug mode to on.
3. From the **Actions** menu, click **Turn On Debug Mode**.



The **Turn On Debug Mode** dialog is displayed.

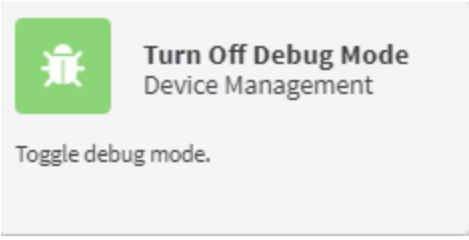


4. Click **Turn On**.

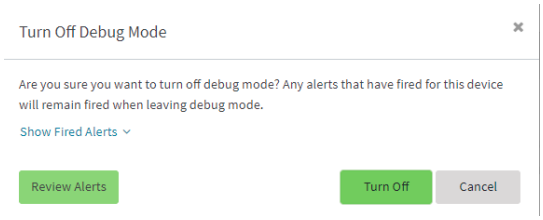
To turn on debug mode for additional devices, repeat this procedure for each device.

Turn off debug mode for a device

1. Click **Devices**.
2. Select a device to turn the debug mode to off.
3. From the **Actions** menu, click **Turn Off Debug Mode**.



The **Turn Off Debug Mode** dialog is displayed.



4. (Optional) To review alerts for this device prior to turning off debug mode:
   a. Click **Review Alerts**.

      The **Alerts** page, filtered for the selected device, is displayed.
      - To review details for an alert, select the alert and click **Actions** > **Alert Details**.
      - To **Acknowledge** or **Reset** an alert, select the alert and click **Actions** > **Acknowledge** or **Actions** > **Reset**.
   b. After reviewing alerts, click **Devices** to return to the **Device** page.
   c. Select the device and click **Actions** > **Turn Off Debug Mode** again..
5. Click **Turn Off**.

If you want to turn off debug mode for additional devices, repeat this procedure for each device.

SMS messaging service

Remote Manager SMS messaging service allows you to send and receive SMS messages between Remote Manager and the devices registered in your inventory. You can use the SMS service for very basic device management tasks as well as to exchange application data between Remote Manager and the connected device. You can subscribe individual connected devices to SMS and can activate SMS messaging on a per-device basis.

You can use SMS messaging services to:

- Send an SMS message to a device, causing it to dynamically establish its EDP connection with Remote Manager
- Send user-defined data between Remote Manager and devices registered in your device inventory
- Perform limited device management tasks, such as pinging the device and provisioning it properly for Remote Manager

Because Remote Manager only needs intermittent connection to your SMS-enabled devices, the SMS messaging service enables you to control your cellular data usage. To collect data, Remote Manager sends an SMS message instructing the device to establish its EDP connection to Remote Manager. Once the device has uploaded its data to Remote Manager, Remote Manager then disconnects the EDP connection.

The Remote Manager SMS messaging service provides a reliable way to send data between Remote Manager and the devices in your inventory, and is an improvement over the limitations of basic SMS messages in several ways. For example:

- You can send request/response pairs allowing message receipt confirmation; this also allows devices to respond to user commands sent though Remote Manager.

- You can send messages larger than a single SMS message. Remote Manager automatically splits up and reassembles large messages into a multi-part message without requiring any user intervention.
- You can send binary messages, whereas basic SMS messages are limited to text only.
- Your data integrity is guaranteed, whereas basic SMS messages do not guarantee data integrity.

SMS messaging concepts

SMS messaging uses message compression and raw messages.

SMS message compression

The SMS feature supports sending compressed messages between Remote Manager and a registered device. Message compression allows Remote Manager to pack a user's message into a smaller number of bytes.

Requirements:

- The device must be configured with phone numbers and have cellular service.
- The device firmware must support message compression; otherwise, all communication is uncompressed.

How SMS message compression works:

- Remote Manager compresses message transfers to the device.
- The device compresses messages sent to Remote Manager.
- The amount of compression is determined by the compressibility of the message, and never results in sending a larger message than the original version.
- If compressing the message results in a larger message, Remote Manager sends the original message instead.

Raw SMS messages

In addition to Remote Manager-formatted messages, a user can send an unmodified, or "raw", SMS message. Use raw messages when you want to use every byte of the SMS message (Remote Manager protocol takes approximately 5 bytes per message of overhead), or when using a device that doesn't have Remote Manager protocol support but does have SMS support.

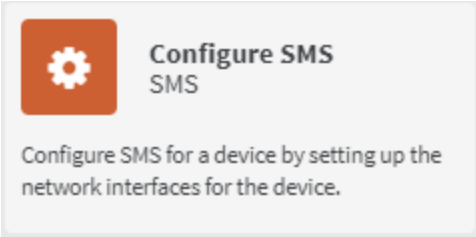
About raw messages:

- Raw messages are not modified by Remote Manager and are subject to the restrictions of the SMS messaging interface.
- They can contain a maximum of 160 characters.
- Specific supported characters are dependent on the carrier but are character only, not binary.
- Raw messages are not guaranteed to be delivered, and may be delivered more than once.
- Since they may be subject to corruption, are not guaranteed to be correct.

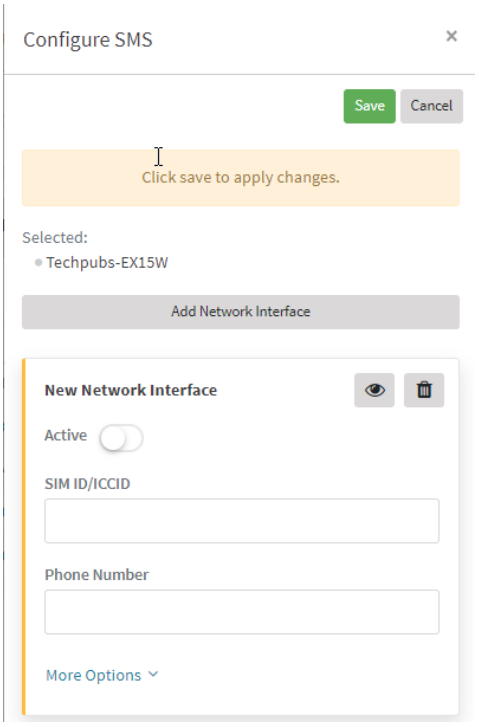
Configure SMS for a device

To configure SMS for a device:

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to configure for SMS messaging, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Configure SMS**.

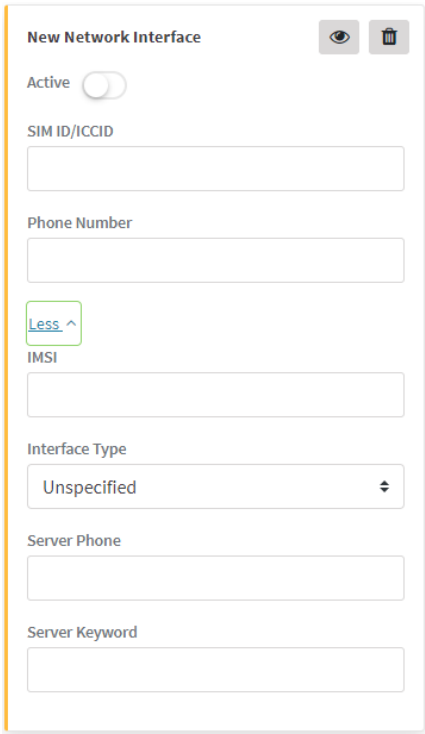


- If there are no network interfaces configured for SMS:
  a. Click **Add** to create an interface.



  b. Click **Active** to enable SMS.
  c. Provide at least one of:
     - **SIM ID/ICCID**: Type the SIM ID or ICCID.
     - **Phone Number**: Type the SIM phone number.
     - IMSI:

i. Click **More Options**.



ii. Type the **IMSI**.

d. (Optional) Click **More Options** to identify:

- **Interface Type**
- **Server Phone**
- **Server Keyword**

- If a network interface already exists:
  - Click to edit the interface.
  - Click to delete the interface.
  - Click **Add Network Interface** to create additional network interfaces.

4. Click **Save**.

SM/UDP messaging service

The SM/UDP (Short Message/User Datagram Protocol) service lets you send and receive SM/UDP messages between Remote Manager and your devices. You must enable SM/UDP support for each device before you can send SM/UDP messages.

SM/UDP uses the very small data footprint of Remote Manager SM protocol over UDP. Devices with limited data plans can keep data traffic to a minimum by only occasionally sending data readings to Remote Manager. For example, you can set up a device to use SM/UDP to send sensor readings to Remote Manager once a night. This type of message is queued because some devices are not publicly addressable.

To keep data usage to a minimum, SM/UDP messages are not guaranteed-delivery. When writing applications that use SM/UDP, build in retry logic.

Pack command for SM/UDP

The pack command for SM/UDP (Short Message/User Datagram Protocol) allows multiple SM commands to be merged and sent in a single datagram to reduce data usage and overhead. Remote Manager supports pack commands once it receives a pack command from a device. You can also configure support with web services.

When Remote Manager receives a message from a device, it will combine the reply (if requested) with any pending requests and send them in a single pack command. If an outstanding request is too large to fit in a single datagram by itself, Remote Manager will send that request as a standalone multipart request. If the pending requests are too large to fit in a single pack command, Remote Manager will batch and send multiple pack commands.

Battery-operated mode with SM/UDP

Some devices need to restrict the number of replies they receive. These devices can immediately shut down their network connection in order to conserve power. To allow for this, use the classic version of Remote Manager to set a device to battery-operated mode. See Send an SM/UDP Reboot message for instructions.

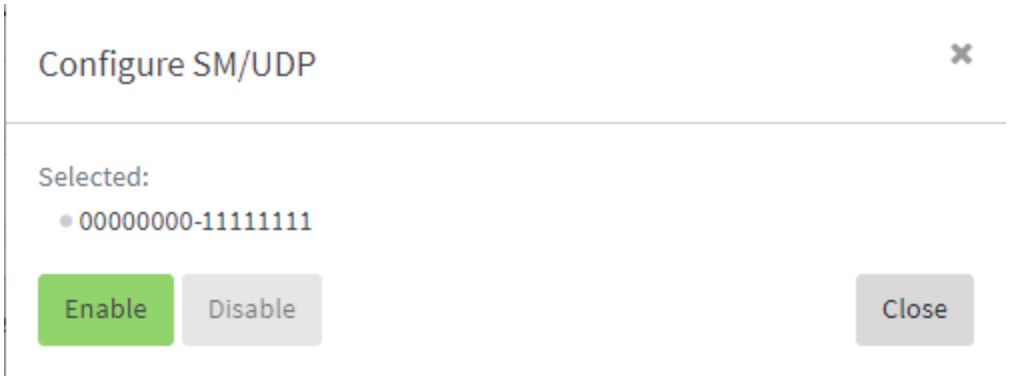
When Remote Manager receives an SM/UDP request from a device that did not explicitly request a reply, it will not send any outstanding requests. If the device requested a reply, the server will pack the reply together with pending requests until it reaches capacity. Any new pending requests will remain queued until the device sends another request. If a queued request is too large to fit in a pack command along with a reply, Remote Manager will not send it.

Note Do not attempt to configure support for battery-operated mode unless the device supports the pack command.

Configure SM/UDP for a device

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to configure for SM/UDP messaging, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Configure SM/UDP**.

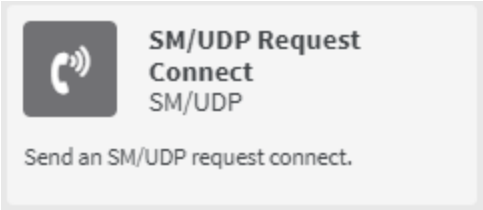
The **Configure SM/UDP** dialog is displayed.



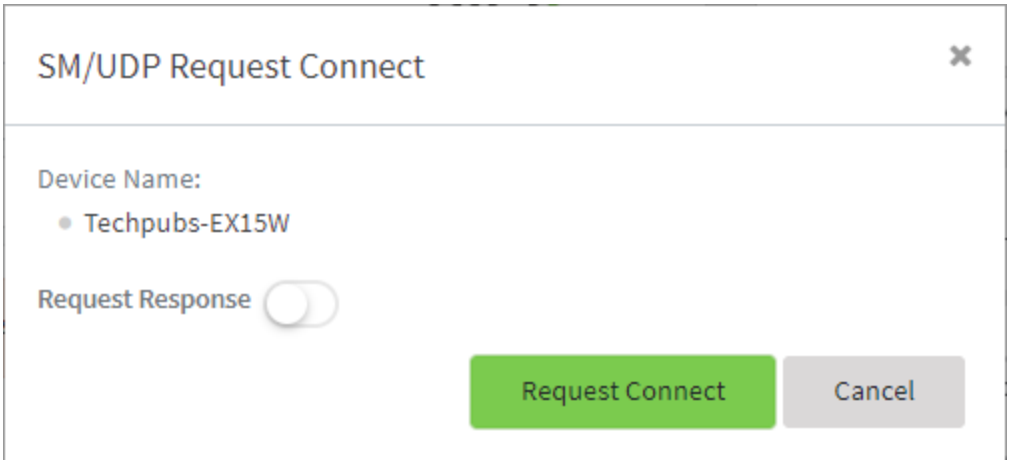
4. Click **Enable**.

Send an SM/UDP request connect

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to request an SM/UDP connection with, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **SM/UDP Request Connect**.



The **SM/UDP Request Connect** dialog is displayed.



4. (Optional) Click **Request Response** if you want to receive a success or failure message from the device.
5. Click **Request connect**.

To view the status of the request:

1. Click **Activity** from the main menu to open the **Activity** page.
2. Select the Sm_udp Request Connect activity.
3. Click **Actions** > **Activity Details**.

Device IDs

A device ID is a unique 16-byte number used to uniquely identify a device within Remote Manager.

Most device IDs are derived from the device MAC address, IMEI number, or ESN number. If a device does not have an assigned MAC, IMEI, or ESN, Remote Manager generates and assigns a random 16-byte number for the device ID. See System-generated device IDs for more information.

Device ID Assignments

A device ID is derived from the unique information from the device, in the order specified in the list below.

1. The Ethernet interface MAC-48. See Device IDs based on MAC addresses.
2. The 802.11 interface MAC-48. See Device IDs based on MAC addresses.
3. The cellular modem IMEI for GSM devices. See Device IDs based on GSM IMEI.
4. The cellular modem ESN (Electronic Serial Number) for CDMA devices. See Device IDs based on CDMA addresses.
5. The auto-generated format. See System-generated device IDs.

For example, if a device has an Ethernet interface and a cellular modem, the device ID is generated from the Ethernet interface. If a device contains multiple interfaces of one type (such as two Ethernet interfaces), a primary interface is selected and used as the source of the device ID.

Full-length device IDs

The full-length device ID is specified as four groups of eight hexadecimal digits separated by dashes. For example:

```
01234567-89ABCDEF-01234567-89ABCDEF
```

Abbreviated device IDs

Device IDs can also be specified in an abbreviated form, without the leading groups of zeros. The following table shows how some device IDs can be abbreviated.

Full device ID	Abbreviated forms
00000000-89ABCDEF-01234567-89ABCDEF	89ABCDEF-01234567-89ABCDEF
00000000-00000000-01234567-89ABCDEF	00000000-01234567-89ABCDEF 01234567-89ABCDEF
01234567-89ABCDEF-01234567-89ABCDEF	No abbreviated form
00000000-00000000-00000000-89ABCDEF	00000000-00000000-89ABCDEF 00000000-89ABCDEF 89ABCDEF

System-generated device IDs

Remote Manager can automatically generate and assign a device ID. Generated IDs are often used for devices that do not have a unique identifier.

Here is a sample system-generated device ID:

0008cccc-eeeeeeee-vvvvvvvv-gggggggg

System-generated value	Description
cccc	Unique value set per cluster, dependent on the generated cluster ID
eeeeeeee	Typically all zeroes, but may be randomly assigned
vvvvvvvv	Represents a provision ID for the customer, currently the vendor ID
gggggggg	Randomly assigned

Device IDs based on MAC addresses

Device IDs can be derived from the 48-bit MAC address.

For example:

MAC address: 112233:445566
Device ID mapping: 00000000-00000000-112233FF-FF445566

Device IDs based on GSM IMEI

Device IDs can be derived from a GSM IMEI address which consists of 14 decimal digits plus a check digit. The check digit is not officially part of IMEI. However, since modems commonly report the IMEI including check digit and it is typically listed on labels, the check digit is included in the device ID mapping.

Example IMEI: AA-BBBBBB-CCCCCC-D
Device ID mapping: 00010000-00000000-0AABBBBB-BCCCCCCD

Device IDs based on CDMA addresses

CDMA (Code Division Multiple Access) device IDs have two addressing schemes:

- 32-bit Electronic Serial Number (ESN) scheme
- 56-bit Mobile Equipment Identifier (MEID) scheme

Both addresses can be specified in hexadecimal or decimal format.

ESN-Hex address: MM-SSSSSS
Device ID mapping: 00020000-00000000-00000000-MMSSSSSS

MEID-Hex address: RR-XXXXXX-ZZZZZZ-C
Device ID mapping: 00040000-00000000-00RRXXXX-XXZZZZZZ

Note A check digit is appended to MEID addresses. The check digit is not part of the MEID and is therefore not included in the device ID mapping.

Device disconnect reasons

A device's connection history, visible from the **Properties** menu, describes the reason a device disconnected.

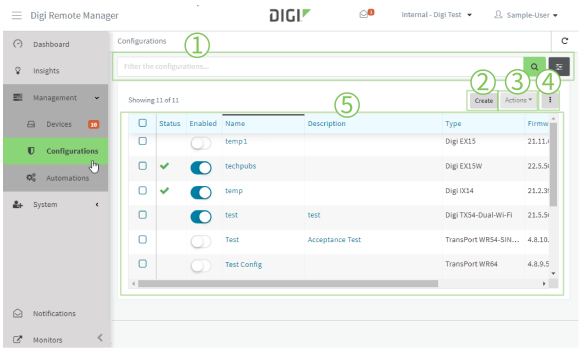
Disconnect Reason	Description
...	The reason for disconnect has become stale, which sets this field to an empty string.
... OR session closed	The device was disconnected by the Remote Manager server but no disconnect reason was given. It is common to see this disconnect around the same time as a server reset.
Closed after reboot	The device was rebooted, automatically disconnecting the device from Remote Manager.
Connection reset: connection ended unexpectedly	The TCP connection was severed remotely from Remote Manager. Typically, a device or piece of networking equipment is causing disconnection. For example: ▪ A NAT device's translation table expired the TCP connection from lack of sufficient keep-alives. This is very common in cellular devices whose EDP keep-alive is set too high. ▪ The device was reconfigured to a new server and a boot action=reset was executed.
Device Certificate Distributed	The device is running firmware that utilizes client-side certificates, and Remote Manager sent it a certificate to use to authenticate itself for subsequent connections. Remote Manager disconnects the device to ensure that it reconnects with the new certificate
Disconnect job submitted	An RCI job was submitted from SCI or the web UI.
Invalid credentials	The device password was set and the device reported an incorrect token.
Invalid device ID supplied	The device ID provided in the security layer was not in the expected format.
No keep-alives in 180 seconds	The device has not responded to keep-alive messages in 180 seconds.
RCI timeout for device	After an RCI timeout, the EDP connection is closed.
Reboot job submitted	An RCI reboot job was submitted either by SCI or the web UI.

Disconnect Reason	Description
Redirect sent	A connection control reset was sent from SCI or the web UI.
Reset sent	An SCI or Web UI has sent a firmware reset command.
Server reset	The Remote Manager server that the device is connected to became unavailable. This can happen during maintenance windows or server failure; in this event, the device can simply connect back in to another system.
Session closed	The session timed out due to a command or inactivity.
SSL handshake failed	The SSL handshake process failed. Causes for this failure may include a bad certificate.
Stale connection found	The connection was dropped due to a new TCP connection to a device reporting this device ID.
Supplied encryption form no supported	The encryption form submitted is not supported.
Unexpected data in security layer	An unexpected opcode appears in the security form, likely due to a corrupted packet.
Vendor ID	The vendor ID reported by the device does not match any registered ID.

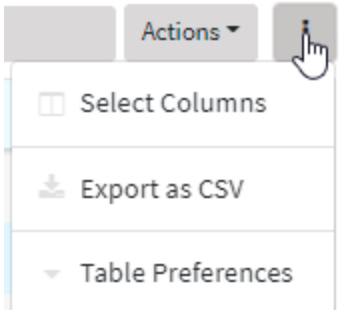
Configurations

Use **Configurations** to automatically manage device firmware, settings, and files. For example, you can automatically provision or update multiple devices with one common configuration which includes firmware, settings, and file systems. In addition to the common settings included in a configuration, you can provide site-specific settings to override one or more settings.

From the main menu, click **Management** > **Configurations**.



#	Component	Description
1	Configurations filter	▪ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ▪ Click to filter the display. ▪ Click to clear the filter criteria.
2	**Create** button	See Create a configuration.
3	**Actions** menu	Accessible only when a configuration has been selected. ▪ **Edit** —Edit the configuration. ▪ **Delete** —Delete the configuration. ▪ **Scan Now** —Scan the devices associated with the configuration for compliance with the configuration. If **Remediate** is selected for the configuration (see Create a configuration), non-compliant devices will be updated to be compliant. ▪ **Copy** —Copy the configuration.
4	Customize display menu	Click to customize the display.

#	Component	Description
		 ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click **Export as CSV** to export a list of the devices in CSV format. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly**

#	Component	Description
		(shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
5	Configurations list	▪ Click to select a configuration. ▪ Click a configuration **Name** or **Description** to display status and configuration information. Click a menu item at the bottom of the display to edit the configuration.

This chapter contains the following topics:

Configurations, device types, and groups

A Remote Manager **configuration** is a named set of device firmware, settings, and file system options. You use the configuration to automatically update multiple devices and to periodically scan devices to check for compliance with the configuration.

Groups are the organizational unit used to apply configurations. First, organize your devices into groups. Then, create configurations for the device types in the group. You can create multiple configurations for a device type in a group, but only one configuration per device type can be enabled at one time.

If you move a device into group that is managed by an active configuration for that device type, the device is immediately scanned for compliance. If the device is not compliant and you have opted to automatically perform remedial action, the device is automatically updated to match the configuration. If you move a device out of a group that is managed by an active configuration, the device is no longer managed.

Create a configuration

You can create a configuration using defaults taken from the device firmware repository.

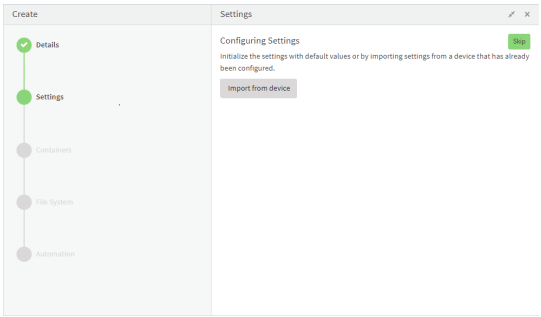
To create a configuration using device defaults:

1. From the main menu, click **Management** > **Configurations**.
2. Click **Create** and enter details for the configuration:

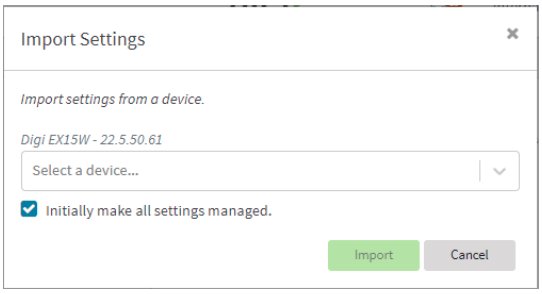
Option	Description
Name	Enter a name for the configuration.
Description	Enter a description for the configuration to help you identify the purpose of the configuration.
Groups	Select one or more groups of devices to manage. You can have multiple configurations for a group, but only one configuration for each device type within the group can be enabled at the same time.
Device type	Select the device type.
Firmware version	Select the firmware version for the device type.

3. Click **Save and Continue**.

Note Once you save the device type and firmware version for a configuration, you cannot change these selections.



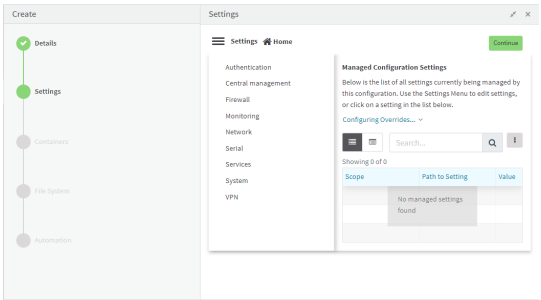
4. Click **Import from Device**.



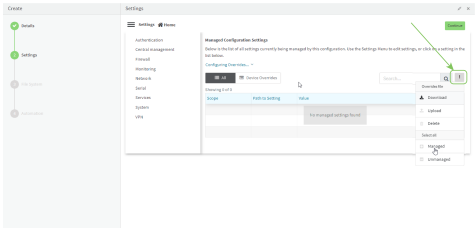
   a. Select a device in your inventory that you have already configured. The selected device will serve as the basis for the configuration of all devices of the same device type that are members of this group.
   b. By default, the **Initially make all settings managed** option is selected. After importing the device's settings, you can deselect some of the settings so that they are no longer managed.

      If you are creating a configuration to manage only a select number of settings, deselect **Initially make all settings managed**. After importing the device's settings, you can select the settings you want to manage one-by-one.

The managed configuration settings appear:



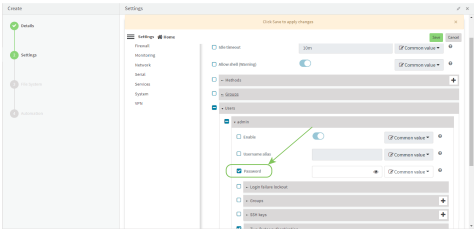
5. Select and configure the settings you want to manage in this configuration:
   - To manage or unmanage all settings:
     a. Click .



     b. Click **Managed** to set all settings to managed.
     c. Click **Unmanaged** to set all settings to unmanged.
   - To manage or unmanage individual settings:
     a. In the **Settings** menu, click a category of settings to access a list of settings.
     b. Select to manage, or deselect to unmanage, individual settings.

     For example, to set the password for the admin user to managed:

     a. In the **Settings** menu, click **Authentication**.
     b. Click **Users** > **admin**.
     c. Click to deselect **Password**.

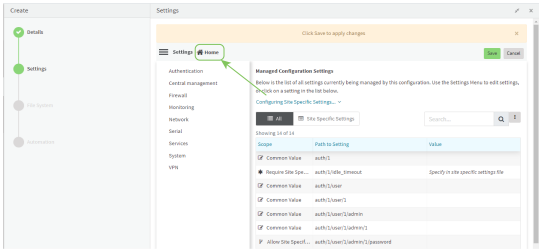


     After you have set a settings to managed, edit the value of the setting by clicking on the setting.

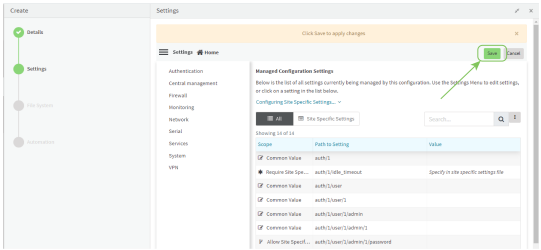
Option	Description
Common value	Use the value as the common value for all devices managed by this configuration. When a device is scanned, Remote Manager compares the device value to this common value.
Allow site-specific settings	Allow individual devices to provide a site-specific setting that overrides the common setting. When a device is scanned, Remote Manager checks to see if the site-specific file provides a value for the device. ▪ If a value is provided in the site-specific file and the value configured

Option	Description
	on the device does not match the value in the site-specific file, then the value on the device will be updated. ▪ If no value is provided in the site-specific file, the common value is used. See Include site-specific settings in a configuration.
Require site-specific settings	Require all devices to provide an site-specific value. You must provide the site-specific values for each device via an site-specific file. When a device is scanned, Remote Manager compares the device value to the value in a site-specific file. If no value is provided in the site-specific file, the scan will fail. See Include site-specific settings in a configuration.
Set default value	Set the value of this option to the default value taken from the firmware version for the device type.

6. To view a list of all managed settings, click **Home**:



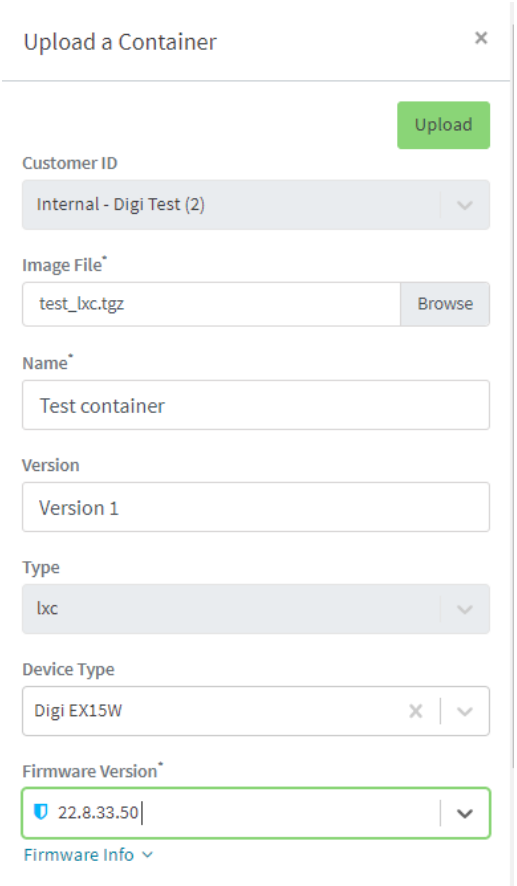
7. Click **Save** when all changes are complete.



8. Click **Continue**.
9. Add containers to the configuration (if available).

Note Container support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

   a. Click Yto add a container to the configuration.
      If no containers have been uploaded, or if Click ❸to upload a container file.



i. Click **Browse** and select the container file.

ii. Type the **Name** of the container.

The **Name** entered here must be the same name as the container .tgz file. This is absolutely necessary, otherwise the container file will not be properly configured on the local devices.

iii. (Optional) Include a version number for the container.

iv. (Optional) Select the **Device Type** and **Firmware Version** that applies to the container.

If set, these options will limit the container to only be included in Configuration templates that match the specified device type and firmware version. If these are left blank, the container can be included in any Configuration template.

v. Click **Upload**.

vi. Repeat to upload additional containers.

b. Select one or more containers to add to the configuration.

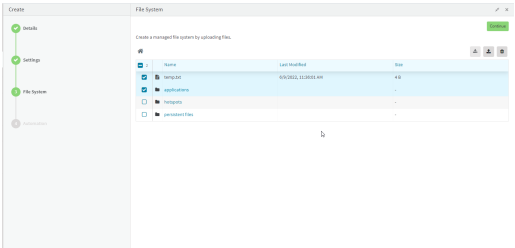
c. Click **Done**.

d. Click **Save**.

e. Click **Continue**.

See Deploy and run containers for additional information about using containers in a Configuration template.

10. Create a managed file system:
    a. Click to upload appropriate files to the configuration.
        - Use the to download files.
        - Use the delete files.
    b. Select files and folders to be managed.



    c. Click **Continue**.
11. At the **Automation** page:
    a. Click **Enable Scanning** to enable this configuration to scan devices for compliance. After enabling scanning, once you save the configuration, Remote Manager will immediately start scanning devices.
    b. For **Frequency**, select the frequency that devices should be scanned for compliance.
    c. For **Action Plan**:
        - **Alert** is enabled by default. This will generate an alert if one or more devices is out of compliance when a scan is performed.
        - Click **Remediate** to update device configuration to bring it into compliance when a scan is performed.
    d. For **Add-ons**, enable any add-ons that apply.
    e. For **Before Scan Options**:
        - To run an automation prior to scanning devices, click **Run Automation** and select the automation. See Automations for more information.
    f. For **Post Remediation Options**:
        - Click **Reboot** to reboot the device after remediation has been performed on the device.

          Note If the device requires a firmware upgrade as part of the remediation, the device will be rebooted as a normal part of the firmware upgrade process, regardless of the setting of the **Reboot** option.

        - Click **Run Automation** and select an automation to run the automation after remediation has been performed on a device. See Automations for more information.
    g. For **On Successful Scan Options**:
        - To run an automation after a scan completes, click **Run Automation** and select the automation. See Automations for more information.

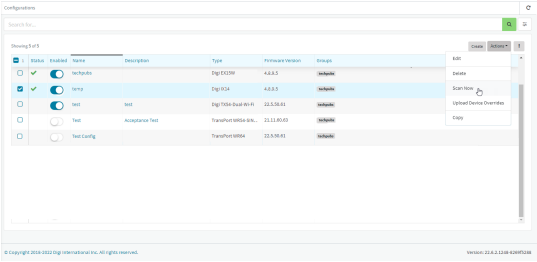
Scan devices

There are two methods to use to scan devices for compliance with a configuration:

- Manual scans
- Scheduled scans

Start a manual scan

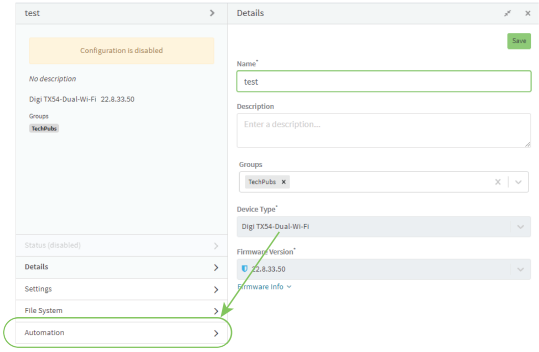
1. From the main menu, click **Management** > **Configurations**.
2. Select a configuration.
3. From the **Actions** menu, click **Scan now**.



Schedule scanning

To set of a schedule for scanning devices and configure remedial actions for non-compliant devices, use the **Automation** options.

1. While creating or editing a configuration, click **Automation**.



2. Select the frequency and action plan for the configuration.

Automation option	Description
Enable scanning	Enable or disable the configuration. After enabling scanning, once you save the configuration, Remote Manager will immediately start scanning devices.
Frequency	Select **Monthly**, **Weekly**, or **Daily**.

Automation option	Description
Action plan	Select **Alert**, **Remediate**, or both. ▪ If you set the plan to alert, Remote Manager triggers an alert for a device that is not compliant when the configuration scan is run ▪ If you set the plan to remediate, Remote Manager updates the device to match the configuration. ▪ If you set the action plan to both, Remote Manager triggers an alert for each non-compliant device and automatically updates devices to match the configuration.

3. If you are ready to scan devices, enable the configuration and click **Save**. Remote Manager will immediately start scanning devices of the specified type.

Include site-specific settings in a configuration

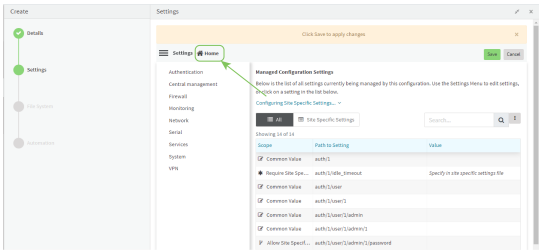
Managed settings can be configured as either **Allow site specific settings** or **Require site specific settings**:

Option	Description
Allow site-specific settings	Allow individual devices to provide a site-specific setting that overrides the common setting. When a device is scanned, Remote Manager checks to see if the site-specific file provides a value for the device. ▪ If a value is provided in the site-specific file and the value configured on the device does not match the value in the site-specific file, then the value on the device will be updated. ▪ If no value is provided in the site-specific file, the common value is used.
Require site-specific settings	Require all devices to provide an site-specific value. You must provide the site-specific values for each device via an site-specific file. When a device is scanned, Remote Manager compares the device value to the value in a site-specific file. If no value is provided in the site-specific file, the scan will fail.

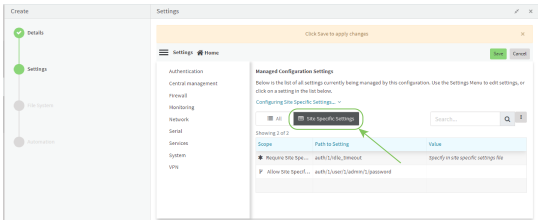
View managed settings that have been configured as site-specific settings

To view a summary of all managed settings that have been configured as site-specific settings:

1. At the **Settings** page for a configuration, click **Home**:



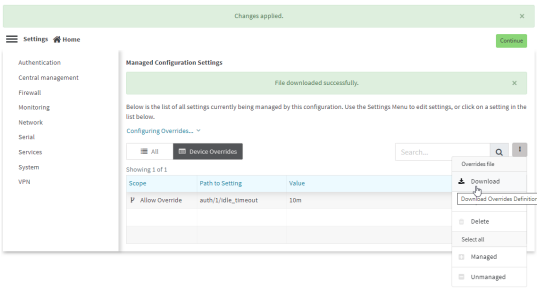
2. Click **Site Specific Settings**.



Provide site-specific settings

To provide site-specific settings for devices:

1. Click and select **Download**. Remote Manager downloads a CSV file to your local filesystem, which you can use to set site-specific values.

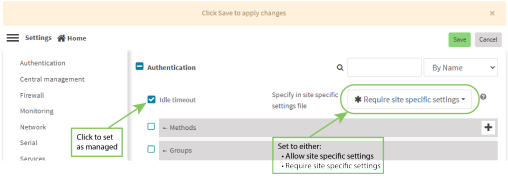


The file consists **key_type** and **key_value** columns, used to identify the specific device that the site-specific value applies to, followed by columns for each setting that you designated as **Allow site specific settings** or **Require site specific settings**.

- **key_type** can be one of **device_name** or **device_id**.
- **key_value** can be either the device name, or the device ID, depending on the value of **key_type**.

For example, to edit the CSV file to set site-specific values for the **Idle timeout** setting for two devices, one named **Device1** and another with the device ID of **00000000-00000000-01234567-01234567**:

a. Set the **Idle timeout** setting to **Managed**, and to **Allow site specific settings** or **Require site specific settings**.



See Create a configuration for more information.

b. Download the CSV file.

c. Add the devices and the appropriate site-specific values:

A	B	C
key_type	key_value	auth/1/idle_timeout
device_name	Device1	5m
device_id	00000000-00000000-01234567-01234567	15m

d. Save the edited CSV file.

2. Click and select **Upload**. Select the edited CSV file from your local filesystem.

   The site-specific settings will be applied to the device the next time that the configuration scanned and remediation performed.

   You an also upload the CSV file via the command line. For example, to upload a CSV file named myoverrides.csv:

```
curl -u username -F upload=@myoverrides.csv
https://devicecloud.digi.com/ws/v1/configs/inventory/configId/settings/device/bulk"
```

   where:

   - *username* is the name of the Remote Manager user. When prompted, enter the user's password to authenticate.
   - *configId* is the ID of the Configuration. the Configuration ID can be determined by using the /ws/v1/configs/inventory API. See the Digi Remote Manager API Reference for further information.

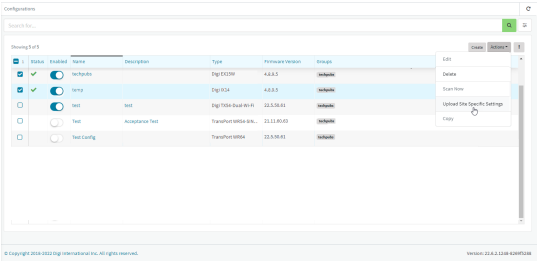
3. To disregard site-specific settings that have been uploaded, click and select **Delete**. This will remove the current specific settings file. You should remove the current-specific settings file before uploading a new one.

Use the same e-specific settings file for multiple configurations

You can also upload the same e-specific settings file for multiple configurations:

1. From the main menu, click **Management** > **Configurations**.
2. Select one or more configurations.
3. From the **Actions** menu, select **Upload Site Specific Settings**. Select the specific settings file

from your local filesystem.



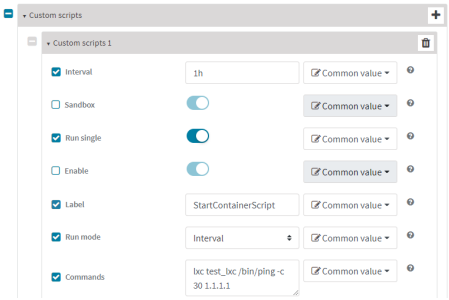
Deploy and run containers

Note Container support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

1. Create a Configuration template. See Create a configuration for instructions.
   a. For the **Settings** step:
      - Click **Import from device** and import settings from an appropriate device.
      - Configure a script to run the container:
        i. Click **System**.
        ii. Click **Scheduled tasks** > **Custom scripts**.
        iii. Click Yes to add a custom script.
        iv. Click the **Label** checkbox and type an identifiable label for the script, for example, **StartContainerScript**.
        v. To ensure that the script is always running:
           i. Click the **Run mode** checkbox and select **Interval**.
           ii. Click the **Interval** checkbox and enter a very short interval (for example, one minute).
           iii. Click the **Run single** checkbox, and toggle on to enable.

           This will configure the device to regularly check if the script is running, but only run if it is currently not running.
        vi. For **Commands**, type the command to run the script. The command will vary depending on how you want to run the script, and what application you want to run inside the script. For example, to run the ping command inside a container, the command would be:

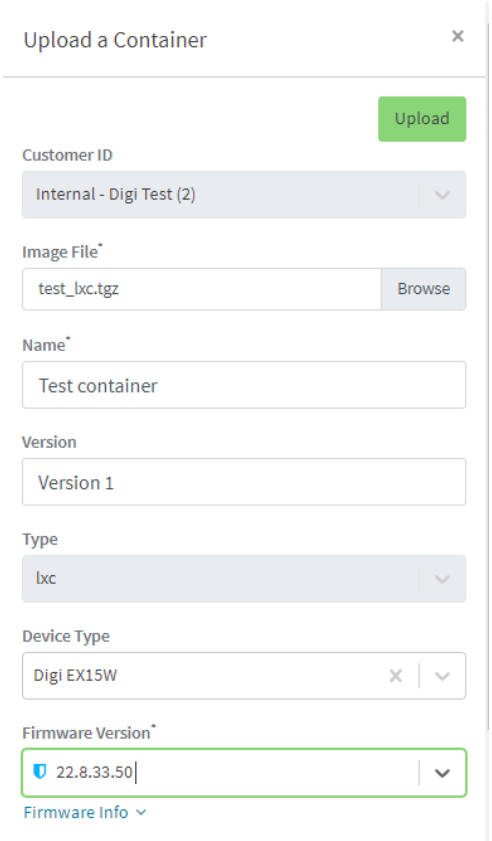
lxc *container_name* /bin/ping -c 30 1.1.1.1



b. For the **Containers** step:

   i. Click ⊕ to add a container to the configuration.

   If no containers have been uploaded, or if Click ⊗ to upload a container file.



   i. Click **Browse** and select the container file.

   ii. Type the **Name** of the container.

   The **Name** entered here must be the same name as the container .tgz file. This is absolutely necessary, otherwise the container file will not be properly configured on the local devices.

   iii. (Optional) Include a version number for the container.

iv. (Optional) Select the **Device Type** and **Firmware Version** that applies to the container.

If set, these options will limit the container to only be included in Configuration templates that match the specified device type and firmware version. If these are left blank, the container can be included in any Configuration template.

v. Click **Upload**.

vi. Repeat to upload additional containers.

ii. Select one or more containers to add to the configuration.

iii. Click **Done**.

iv. Click **Save**.

v. Click **Continue**.

c. For the **Automation** step:

i. Click to toggle on **Enable Scanning**.

ii. Click to toggle on **Remediate**.

2. Run a manual configuration scan to apply the container and configuration settings to all applicable devices.

3. Verify that the container is running on a device:

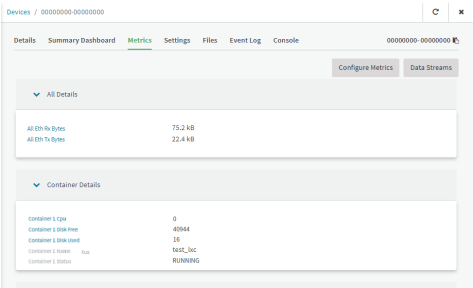
- To verify by using device metrics:

a. From the main menu, click **Management** > **Devices**.

b. Click the **Device ID** to open the device's **Details** page..

c. Click **Metrics**.

d. Information about configured containers is located under the **Container Details** heading.



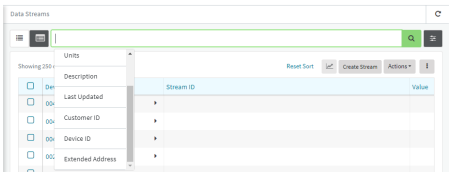
- To verify by using the **Data streams** page:

a. From the main menu, click **Management** > **Data Streams**.

b. Locate the container's data stream:

i. Click to search using advance filtering.

ii. Click in the search text bar and select **Device ID** from the menu.

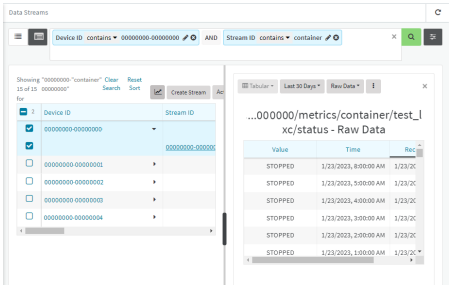


iii. Type the device ID and press the Enter key.

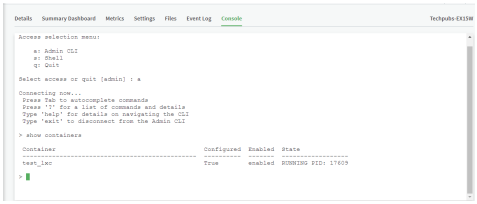
iv. Click in the search text bar again and select **Stream ID** from the menu.

v. Type container and press the Enter key.

vi. Click the **Stream ID** to view container status.



- To verify by using the **show containers** command on the local device:
  a. From the main menu, click **Management** > **Devices**.
  b. Select the device.
  c. From the **Actions** menu, select **Open Console**.
  d. At the prompt, type **show containers**.



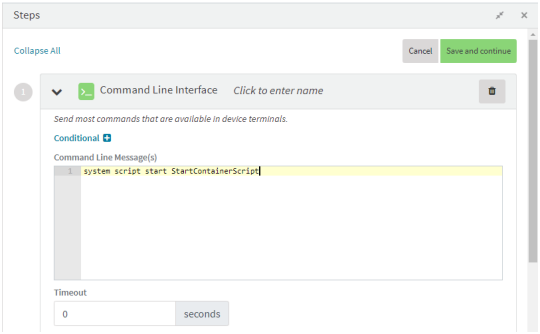
Use an automation to start the container

You can also use an automation to start a container:

1. Follow the steps in the previous procedure, except:
   - For **Run mode**, select **Manual**.
   - Do not set **Interval** or **Run single**.
2. Create an automation that uses a Command Line Interface step.

   For the **Command Line Message**, use the system script start command, using the label provided for the script in the previous procedure:

```
system script start StartContainerScript
```



Once the automation has been created, you can:

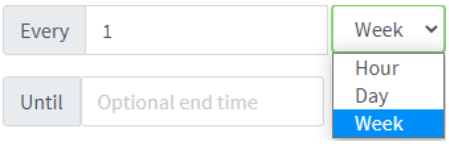
- Run the automation manually.
- Include the automation in a Configuration template as a post-remediation or post-scan step.

  When creating or editing a Configuration template, at the **Automation** page:

  1. For **Post Remediation Options**, click **Run Automation** and select the automation.
  2. For **On Successful Scan Options**, click **Run Automation** and select the automation.
- Include a trigger for the automation.

  When creating or editing an automation, at the **Triggers** page:

  1. Click to enable **Triggered** to configure the automation to be triggered, either on a schedule or by device activity.
     a. To configure the script to be run on a schedule:
        i. Click to enable **By Schedule**.
        ii. Click **Start Time**.
        iii. From the calendar provided, select the date and time that the script should be started for the first time.
        iv. By default, the script will run only once. Click to enable **Repeat** to configure the script to run on a regular basis:



        i. Type or select the number of times, and select the time period.
        ii. (Optional) Click **Until** to select a date and time when the automation schedule will stop repeating.

     b. To configure the automation to be triggered by device activity, click to enable one or more of the following:
        - **Run when a device enters the target scope**
        - **Run when a device in the target scope enters a maintenance window**:
        - **Run when a device in the target scope leaves debug mode**

        Target scope refers to a device that either:

- Is member of a group that was selected on the **Target** page.
- Has a tag that was selected on the **Target** page.
- Is one of the devices included on the **Target** page.

Enable and configure WAN bonding on multiple devices

Note WAN bonding support must be enabled in Digi Remote Manager. Contact your Digi sales representative for information.

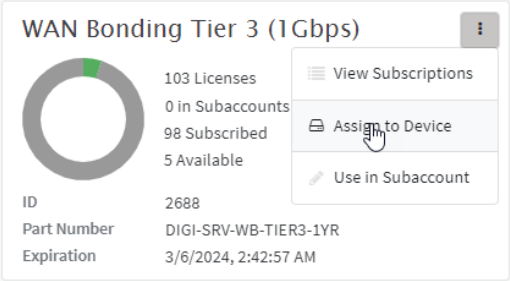
You must also set up the WAN bonding server. This can be done using one of three mechanisms:

- Set up a WAN bonding server on physical hardware or a Virtual Private Server (VPS) in your local environment. See Bondix documentation for instructions.
- Unwired Networks maintains a number of WAN Bonding servers throughout the world, focused mainly on locations in the United States, Europe, and Australia. Contact them for WAN bonding hosting and configuration services.
- Digi Professional Services can setup, manage, and maintain your WAN bonding servers.

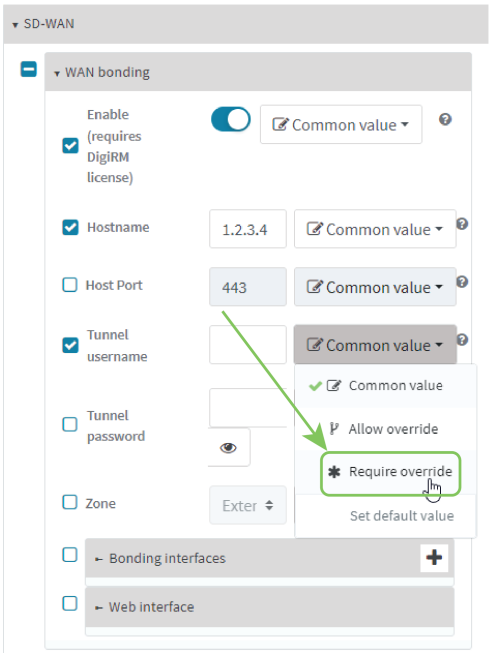
You can also setup a trial server at the Bondix website for testing purposes.

To enable and configure WAN bonding on multiple devices:

1. Add the WAN bonding entitlement to your device:
   a. From the main menu, click **Management** > **Subscriptions**.
   b. In the **WAN Bonding** entitlement card, click and select **Assign to Device**.



   c. Select the appropriate devices.
2. Create a Configuration template. See Create a configuration for instructions.
3. For the **Settings** step in the configuration:
   a. Click **Network** > **SD-WAN** > **WAN bonding**.
   b. Select and toggle on **Enable**.
   c. Select **Hostname** and type the hostname or IPv4 address of the external server hosting the WAN bonding server.
   d. Select **Tunnel username** and **Tunnel password**, and set them to **Require override**. Later in this procedure we will create an override file that includes the username and password that you created when you configure device-specific tunnel settings on the WAN bonding server:
      i. Select **Tunnel username**.
      ii. From the **Common value** menu, select **Require override**:



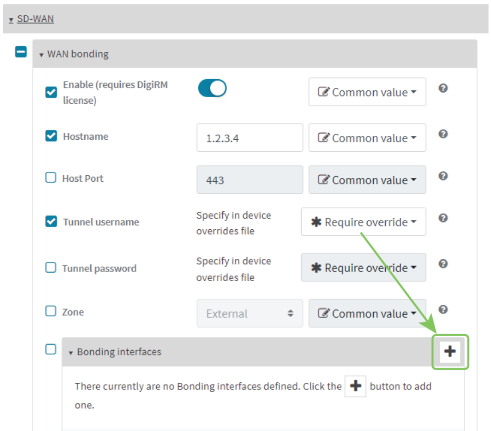
iii. Select for **Tunnel password**.

iv. From the **Common value** menu, select **Require override**:

e. Configure the device's WAN interfaces that will be bonded:

i. Click **Network** > **SD-WAN** > **WAN bonding** > **Bonding interfaces**.

ii. Click to add an interface.

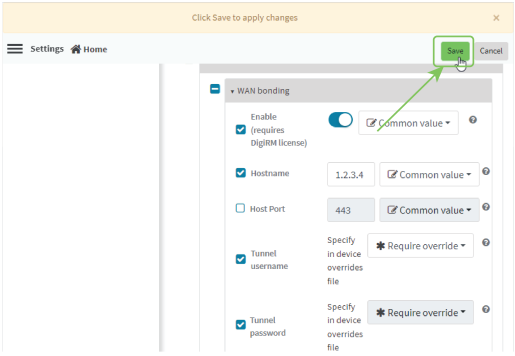


iii. Select **Interfaces** and select a WAN interface to be bonded.

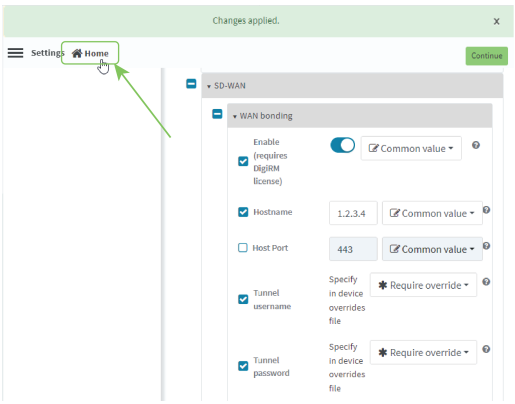
iv. Repeat for additional interfaces.

For example, if you want to bond a wired WAN Ethernet with a cellular modem, add two bonded interfaces: the WAN Ethernet interface and modem cellular interface.

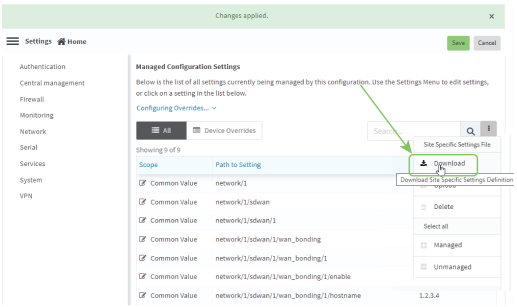
f. Click **Save**.



4. Create a site-specific settings file for the **Tunnel username** and **Tunnel password** options:
   a. Click **Home**.



   b. Click and select **Download** to download a CSV file to your local filesystem, which you can use to set site-specific settings.



   c. Open the CSV file in a spreadsheet editor (such as Excel).

      The file consists **key_type** and **key_value** columns, used to identify the device that the site-specific setting applies to, followed by columns for each setting that you designated as **Require site specific settings**.

      - **key_type** is either **device_name** or **device_id**.
      - **key_value** is either the device name, or the device ID, depending on the value of **key_type**.

   d. Include the username and password in the CSV file:

key_type	key_value	network/1/sdwan/1/wan_bonding/1/password	network/1/sdwan/1/wan_bonding/1/username
device_name	Techpubs-device1	password1	username1
device_name	Techpubs-device2	password2	username2

   e. Save and close the CSV file.
   f. In Remote Manager, click and select **Upload**. Select the edited CSV file.
   g. Click **Continue**.
5. For the **Automation** step in the configuration:
   a. Toggle on **Enable Scanning**.
   b. For **Action Plan**, toggle on **Alert** and **Remediate**.
   c. Click **Save**.
6. To apply these configuration settings immediately to the devices linked to this configuration template, instead of waiting for the next automated scan and remediation to occur:
   a. From the main menu, click **Management** > **Configurations**.
   b. Select the configuration.
   c. Click **Actions** > **Scan Now**.

When are devices scanned?

When you enable a configuration for a device type and within a group, Remote Manager scans devices in the group matching the device type during the next scheduled scan window. The next scan window starts between 7-10 UTC. Devices are rescanned on the interval specified in the configuration.

In addition to scheduled scans, you can initiate a scan immediately using **Scan Now**. When you start a scan using Scan Now, any existing scan for the device is canceled and the new scan starts.

The following table summarizes how changes to the configuration, device group, or device affect scanning operations.

When . . .	Scan operations
Settings, files, or automation values are edited	Depending on the progress the device has made through an existing scan, the device may get the old or the new values. For this reason, we recommend you disable a configuration when you are editing the configuration to prevent scanning devices during the editing. After completing your changes, enable the configuration.
Scan is started via schedule or **Scan Now**	All outstanding jobs from the previous scan are canceled and the scan restarts.
Group the device is in is removed from the configuration	All scans in progress for devices in the group are canceled.
Device name is unset or changed	If the previous device name or new name has site-specific settings, the device is scanned.
Device is removed from an account	All scans in progress are canceled.
Device is moved to a different group	If the new group is part of the same configuration, no change. If the new group has an enabled configuration, any previous scan in progress is canceled and a new scan is started.

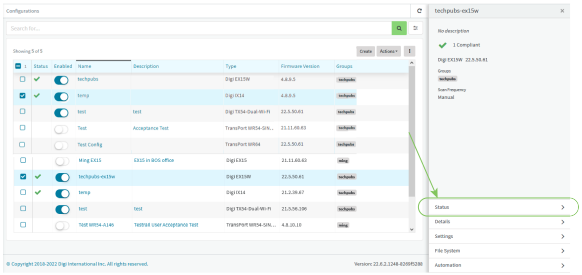
When . . .	Scan operations
Device is in service	Device is not scanned.
Device transitions from in service to in maintenance mode	Device is scanned.
Device is in debug mode	Device is not scanned.
Device is disconnected	Offline jobs are created based on cached data. The offline jobs runs when the device connects.
Device goes into debug mode	All scans in progress are canceled.
Device connects for the first time and the device type is determined to match the configuration	Device is scanned.
Device comes out of debug mode	Device is scanned.
Configuration is disabled or deleted	All scans in progress are canceled.

View configuration status

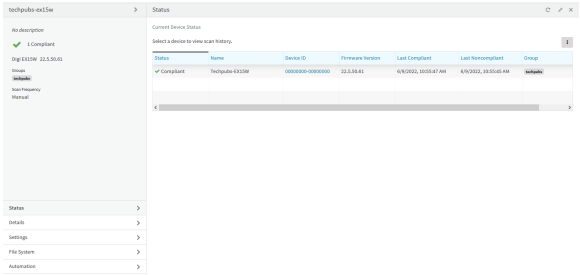
The configuration status display provides a summary list of all devices managed by the configuration.

To view the configuration status:

1. Click **Configurations**.
2. Click a configuration.
3. Click **Status**.



The **Status** page displays:



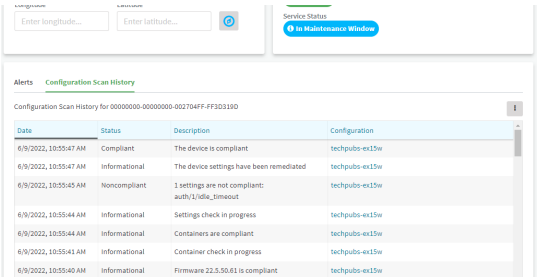
The configuration scan status for a managed device can be one of the following:

- **Compliant**: Device currently complies with the configuration.
- **Non-compliant**: Device currently does not comply with the configuration.
- **Informational**: Remote Manager provides an informational message about scan actions.
- **Unknown**: Configuration scan status is unknown.
- **Canceled**: Configuration scan was canceled.

View configuration scan history for a device

To view the scan history for a device:

1. From the configuration status display, click on a device in the summary list.
2. The **Device Details** page is displayed for the device.
3. Scroll down and click **Configuration Scan History**.

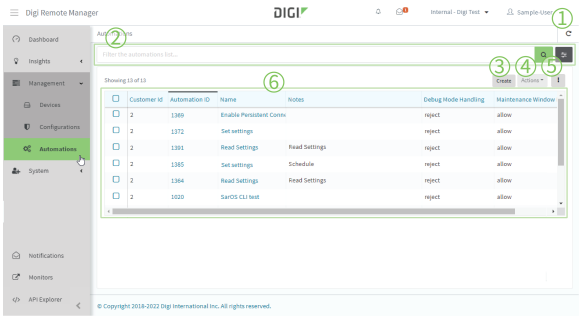


Automations

Automations provides a graphical interface to create complex multi-step operations using features of pseudo-programing like conditional expressions and error handling.

For each step in the process, you can define conditions under which the step will be executed, what should happen when the step is successful or when the step is unsuccessful, and what to do at the end of the step based on the results.

From the main menu, click ❸**Management** > ❺**Automations**.



#	Component	Description
1	Refresh	Click to refresh the automations list.
2	Automations list filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ■ Click to filter the display. ■ Click to clear the filter criteria.
3	**Create** button	See Create an automation.
4	**Actions** menu	Select an automation to: ■ View details about the automation. ■ Run the automation. Select one or more automations to: ■ Delete.
5	Customize display menu	Click to customize the display. ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column.

<table>
<tr><th>#</th><th>Component</th><th>Description</th></tr>
<tr><td></td><td></td><td>
Click Use Defaults to return to the default display.
Click Close when finished.
Click Table Preferences to set your table view preferences:
Click Table Spacing to select Compact, Comfy, or Roomy spacing.
Click Device ID to determine how to display the Device ID, either Friendly (shorter) or Full. (This table preference is not applicable for the Configurations table.)
</td></tr>
<tr><td>8</td><td>Automations list</td><td>
Click to select an automation.
Click an Automation ID or Name to view automation details.
<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Customer ID</td><td>The ID of the customer who created the automation.</td></tr>
<tr><td>Automation ID</td><td>An unique number for the automation.</td></tr>
<tr><td>Name</td><td>The name of the automation.</td></tr>
<tr><td>Notes</td><td>Notes included with the</td></tr>
</table>
</td></tr>
</table>

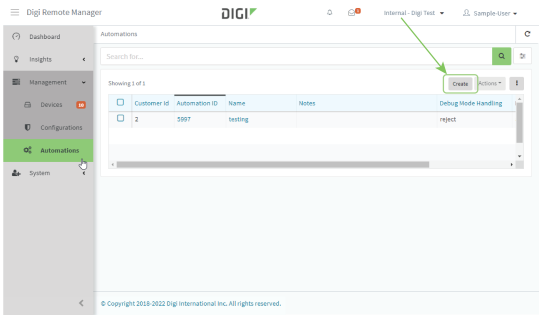
#	Component	Description
		<table><tr><th>Column</th><th>Description</th></tr><tr><td></td><td>automation.</td></tr><tr><td>Debug Mode Handling</td><td>The debug handling used by the automation. See Create an automation for more details.</td></tr><tr><td>Maintenance Window Handling</td><td>The debug handling used by the automation. See Create an automation for more details.</td></tr></table>

This chapter contains the following topics:

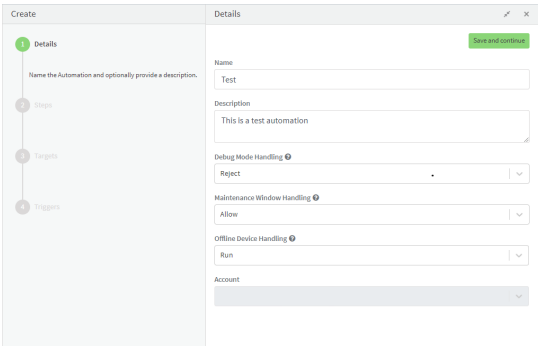
Create an automation

To create an automation:

1. From the main menu, click **Management** > **Automations**.
2. Click **Create**.



The **Details** page displays.



3. Type a **Name** for the automation.
4. Optionally, type a **Description** for the automation.
5. For **Debug Mode Handling**, select one of:
   - **Reject**: The automation fail at the start of the run if any device is in debug mode.
   - **Allow**: The automation will run regardless of the debug mode status of the devices.
   - **Cancel**: The automation will fail during any step in the automation if a device transitions to debug mode.
6. For **Maintenance Window Handling**, select one of:
   - **Reject**: The automation fail at the start of the run if any device is outside of its maintenance window.
   - **Allow**: The automation will run regardless of the devices' maintenance window.
   - **Cancel**: The automation will fail during any step in the automation if a device is outside of its maintenance window.

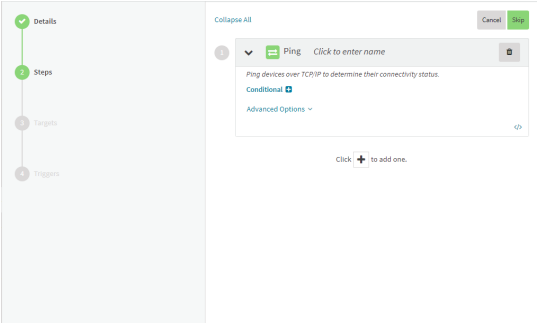
   Note The maintenance window is defined on the device. See your device documentation for information about how to define the maintenance window.

7. For **Offline Device Handling**, select one of:

- **Run**: The automation will run normally if a device is offline at the start of the run. Steps may fail if they required the device to be online.
- **Skip**: The automation will not run on any devices that are offline at the start of the run. Skipped devices are not included in the count, and there are no messages or results generated for the skipped devices.

8. Click **Save and continue** when finished.

   The **Steps** page displays.



   The **Steps** page automatically includes a **Ping** step as the first step.

   - To add another step:
     a. Click Yes repeat to add additional steps as necessary.
   - To remove the **Ping** step:
     a. Click .
     b. Click Yes to add a different step; repeat to add additional steps as necessary.

   For information about each type of step, see Automation steps.

9. Click **Save and continue** when finished with step configuration.

   The **Targets** page displays.

10. (Optional) Select the **Groups**, **Tags**, or **Devices** that the automation will act on.

    Targets are only required if the automation is run automatically. If the automation is run manually, you select the targets at run time.

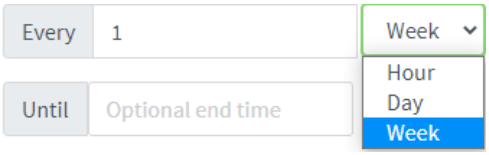
11. Click **Save and continue** when finished.

    The **Triggers** page displays.

12. (Optional) Click to enable **Triggered** to configure the automation to be triggered, either on a schedule or by device activity.

    Triggers are only required if the automation is run automatically. If the automation is run manually, you select the targets at run time.

    a. To configure the automation to be triggered on a schedule:
       i. Click to enable **By Schedule**.
       ii. Click **Start Time**.
       iii. From the calendar provided, select the date and time that the automation should be started for the first time.
       iv. By default, the automation will run only once. Click to enable **Repeat** to configure the automation to run on a regular basis:



i. Type or select the number of times, and select the time period.

ii. (Optional) Click **Until** to select a date and time when the automation schedule will stop repeating.

b. To configure the automation to be triggered by device activity, click to enable one or more of the following:

- **Run when a device enters the target scope**
- **Run when a device in the target scope enters a maintenance window**:
- **Run when a device in the target scope leaves debug mode**

Target scope refers to a device that either:

- Is member of a group that was selected on the **Target** page.
- Has a tag that was selected on the **Target** page.
- Is one of the devices included on the **Target** page.

13. Click **Save** to save the automation, or click **Save and Run Now** to save the automation and run it immediately.

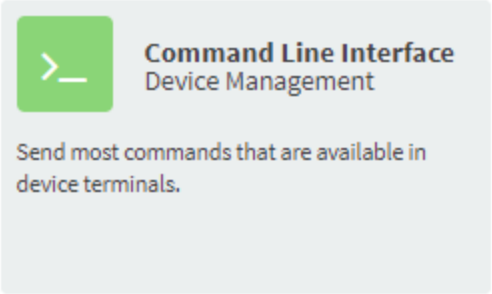
Automation steps

#	Component	Description
1	Keyword search	Type a search string to locate a step in the **Add Step** dialog.
2	Card view	Display cards in detailed or icon view.
3	Sort	Sort the list by name, category, or most recently used. Click ℴ

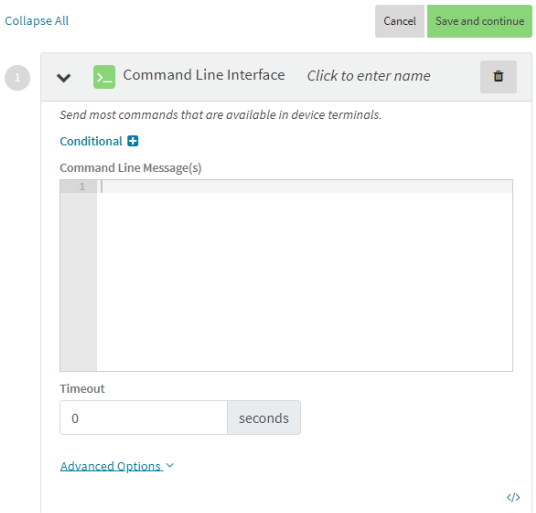
#	Component	Description
		change the order from first to last, or last to first.
4	Step cards or icons	Available steps in card or icon format. Click a step to add it to the automation.
5	**Close** button	Click Close to close the dialog without choosing a step.

This section contains the following topics:

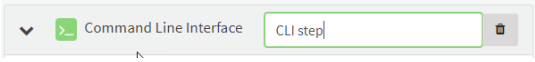
Command Line Interface step



1. Click **Command Line Interface** to add the Command Line Interface step to your automation.



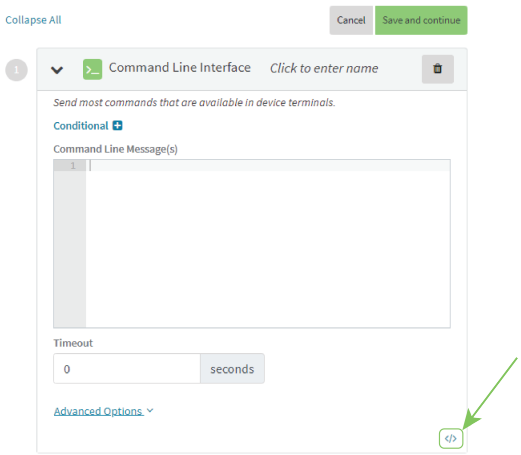
2. Click the header to enter a name for the step.



3. Type the **Command Line Message(s)** that should be executed at the command line as part of this automation.
4. Set the **Timeout** for this step's operation, in seconds. The default is **5**.

You can also view the step in JSON format.

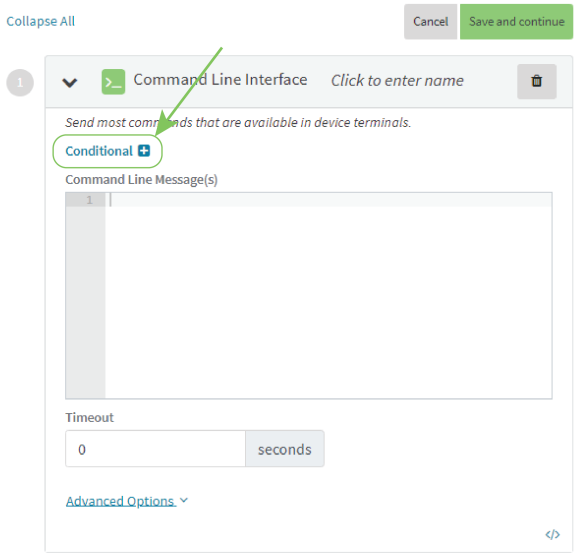
1. Click </>.



2. Click to return to edit mode.

Conditional processing

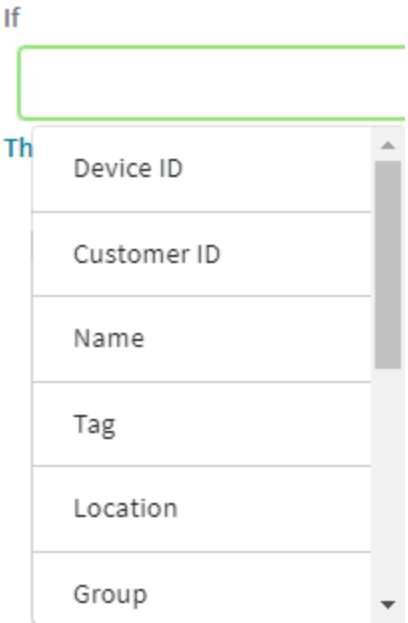
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

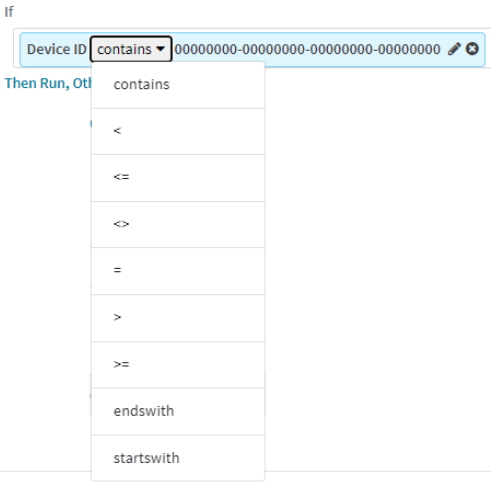
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

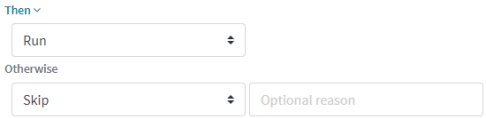
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



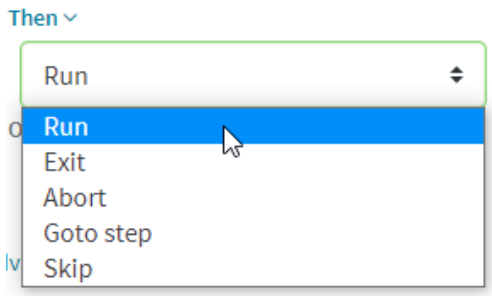
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

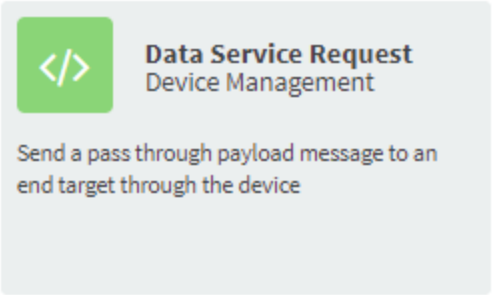
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

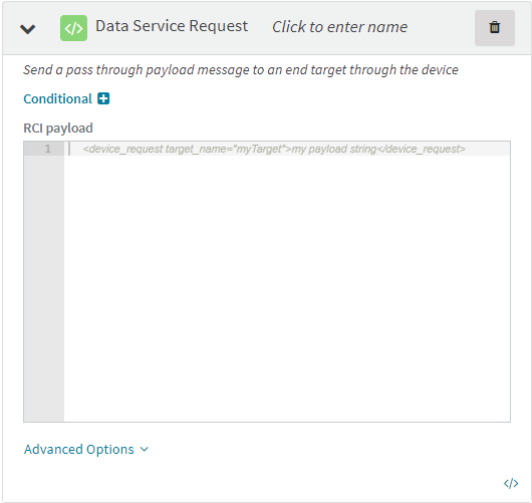
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

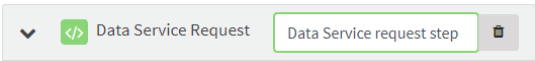
Data Service Request step



1. Click **Data Service Request** to add the Data Service Request step to your automation.



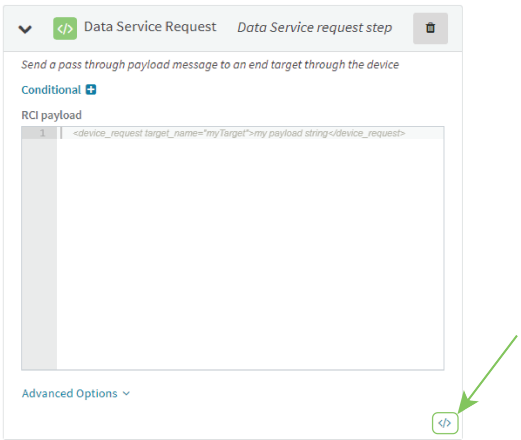
2. Click the header to enter a name for the step.



3. Type the **RCI payload** that should be passed to an end target through the device.

You can also view the step in JSON format.

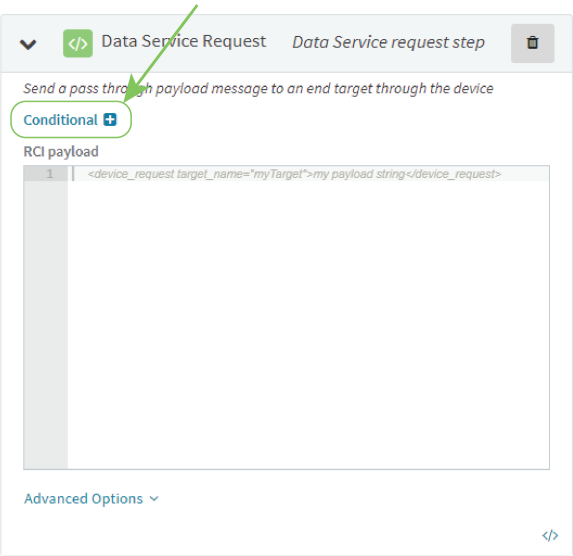
1. Click </>.



2. Click to return to edit mode.

Conditional processing

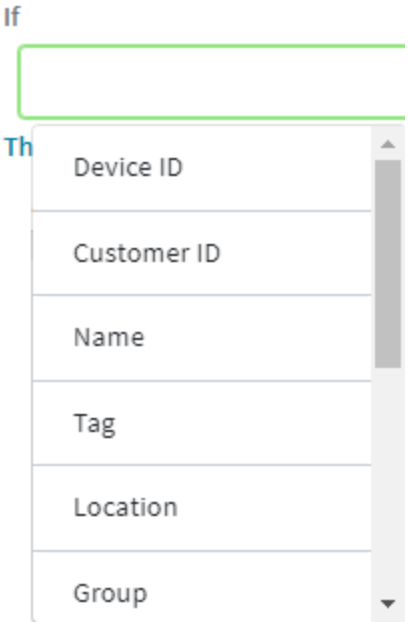
You can optionally set conditions that will determine whether this step should be executed.



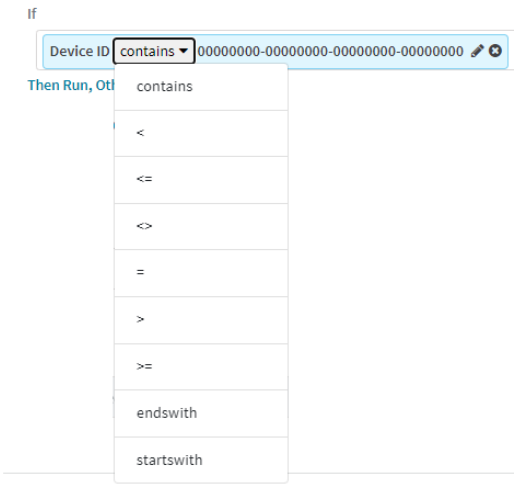
1. Click to expand Conditional.

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



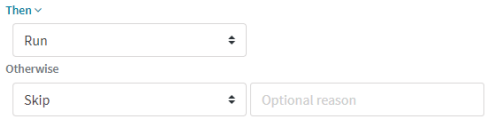
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



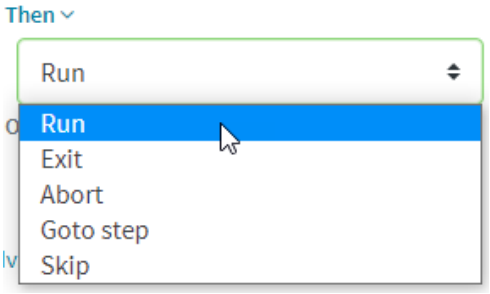
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

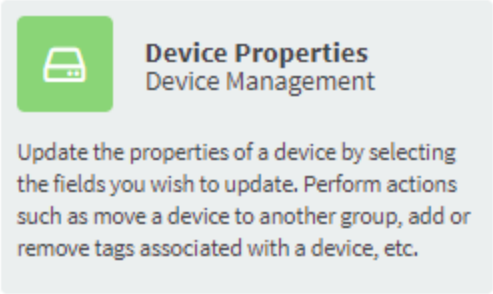
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

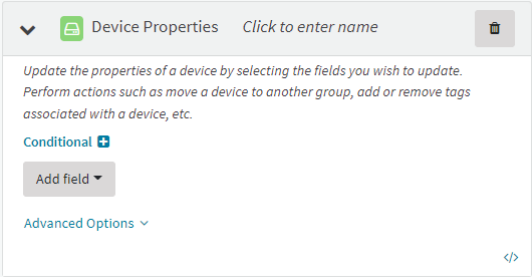
Device Properties step

The **Device Properties** step allows you to update the Remote Manager properties of a device, such as the group that the device is a member of, or device tags. This is helpful to automate device management.

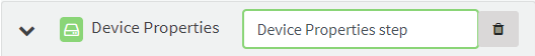
For example, you might create two groups for new devices: Provisional, and Completed. You can then create an automation that runs against all devices in the Provisional group, and when the automation completes successfully for each device, the last step uses the Device Properties step to move the device from the Provisional to the Completed group.



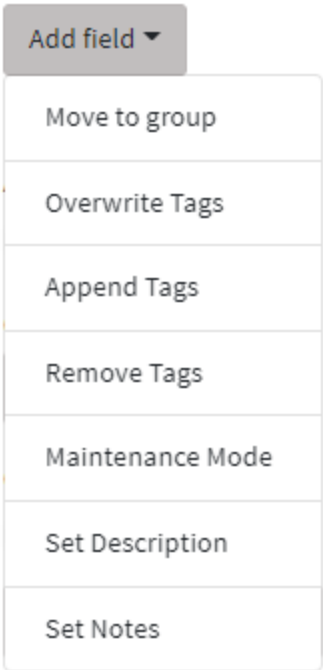
1. Click **Device Properties** to add the Device Properties step to your automation.



2. Click the header to enter a name for the step.



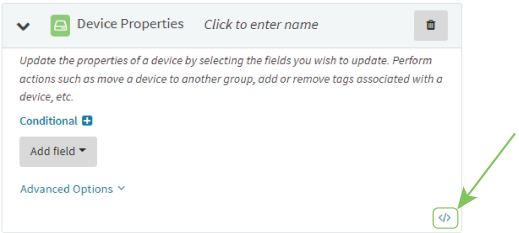
3. Click **Add field** to display a list of device properties that can updated.



- **Move to group**: Select the group that the device should be moved to.
- **Overwrite Tags**: Type the tags will be used in place of existing tags.
- **Append Tags**: Type the tags that will be added to the existing tags.
- **Remove Tags**: Type the tags that will be deleted.
- **Maintenance Mode**: Toggle off to move the device out of Maintenance mode, toggle on to move device into Maintenance mode.
- **Set Description**: Type a description to be added.
- **Set Notes**: Type notes to be added.

You can also view the step in JSON format.

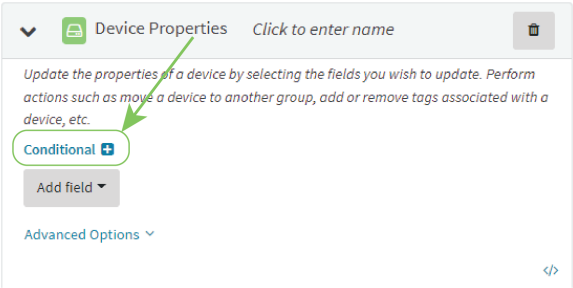
1. Click </>.



2. Click to return to edit mode.

Conditional processing

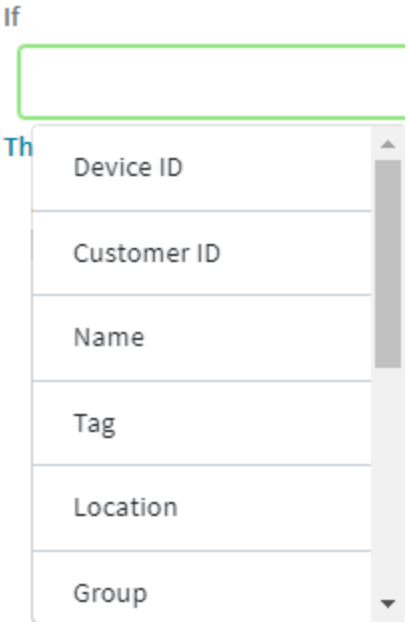
You can optionally set conditions that will determine whether this step should be executed.



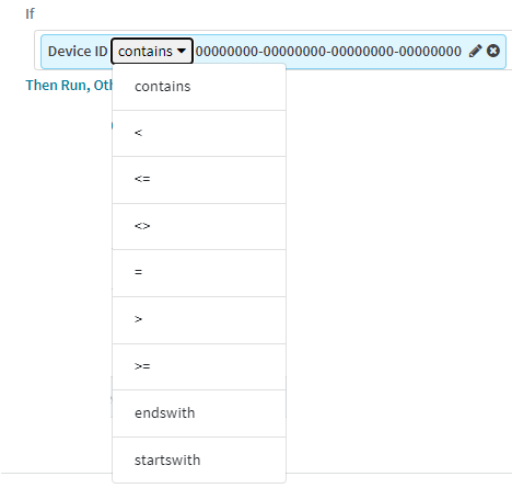
1. Click to expand Conditional.

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



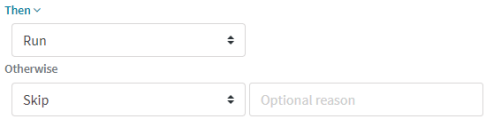
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



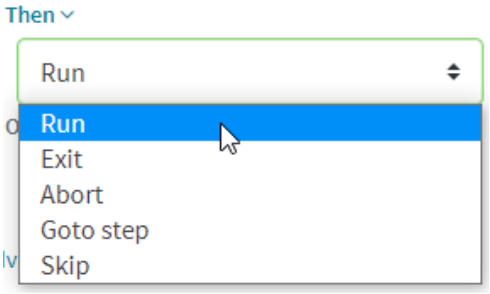
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

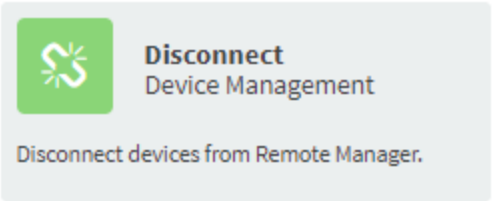
Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

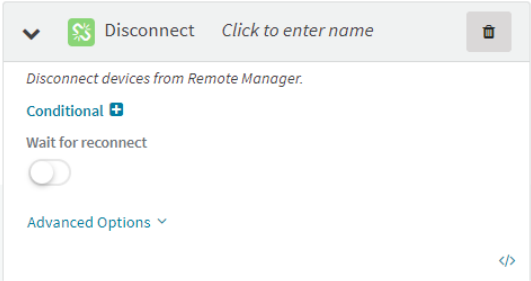
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

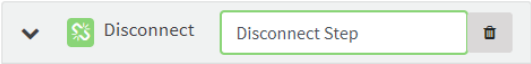
Disconnect step



1. Click **Disconnect** to add the Disconnect step to your automation.



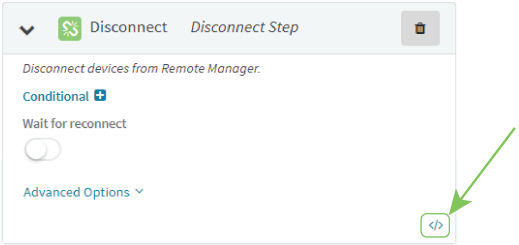
2. Click the header to enter a name for the step.



3. Enable **Wait for reconnect** if you want the automation to wait for the device to reconnect before proceeding..

You can also view the step in JSON format.

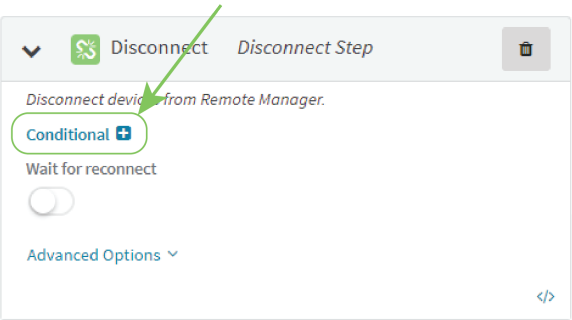
1. Click </>.



2. Click to return to edit mode.

Conditional processing

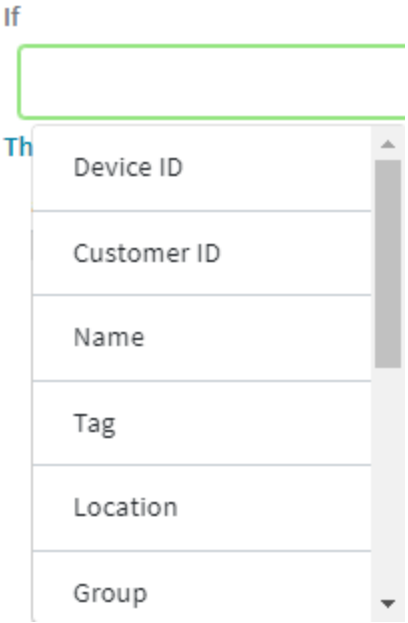
You can optionally set conditions that will determine whether this step should be executed.



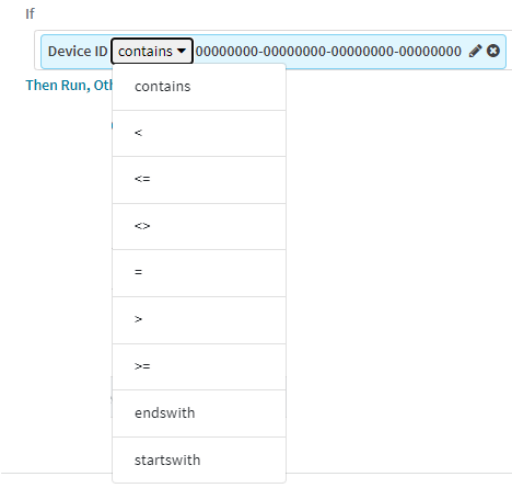
1. Click to expand Conditional.

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



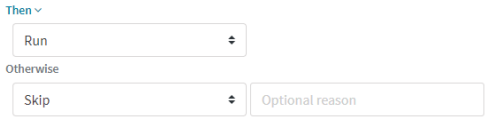
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



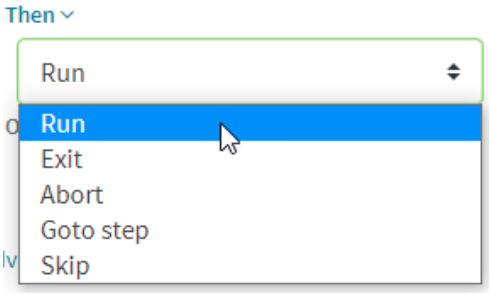
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

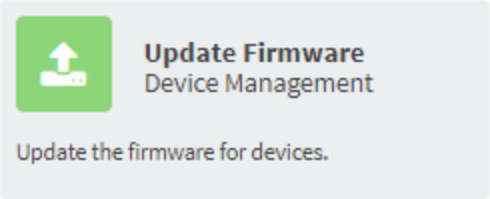
Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

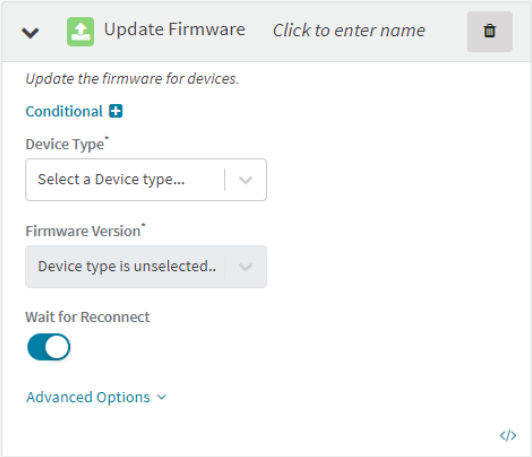
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

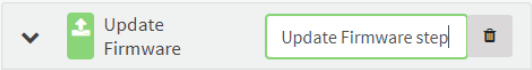
Update Firmware step



1. Click **Update Firmware** to add the Update Firmware step to your automation.



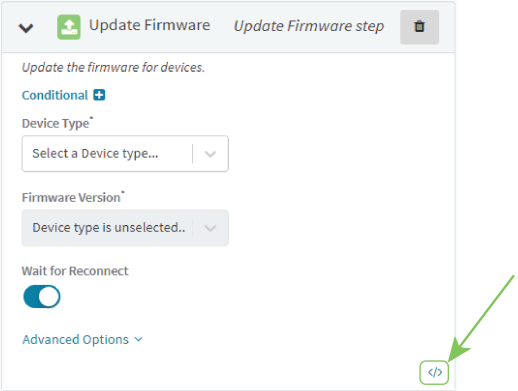
2. Click the header to enter a name for the step.



3. For **Device Type**, select the type of device to be updated.
4. For **Firmware Version**, select the version of firmware to be used.
5. Enable **Wait for reconnect** if you want the automation to wait for the device to reconnect before proceeding.

You can also view the step in JSON format.

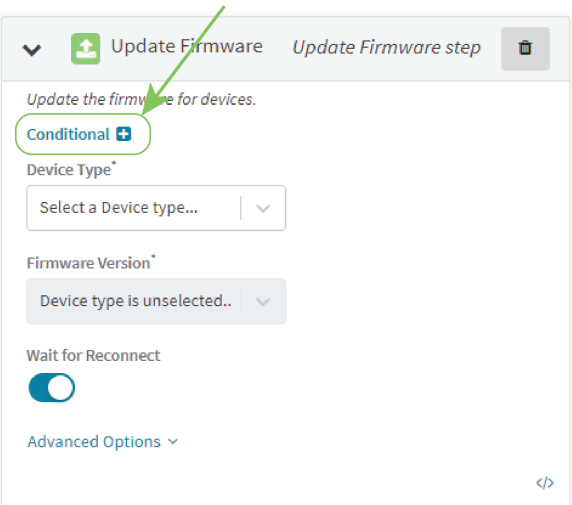
1. Click </>.



2. Click to return to edit mode.

Conditional processing

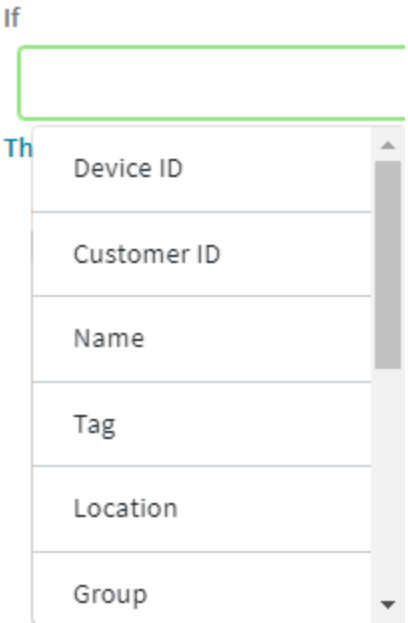
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

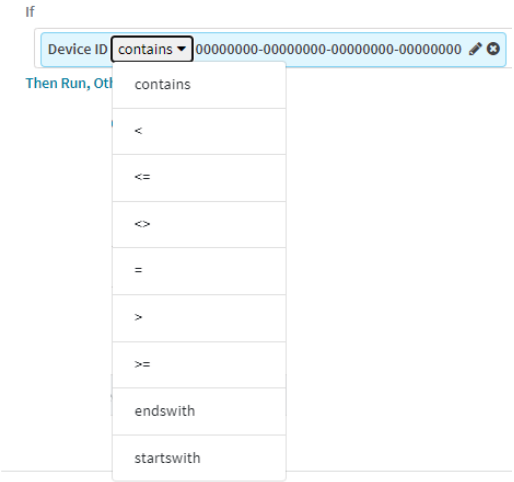
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

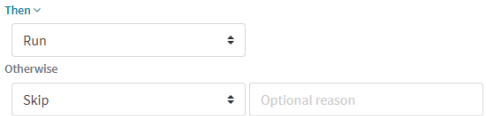
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



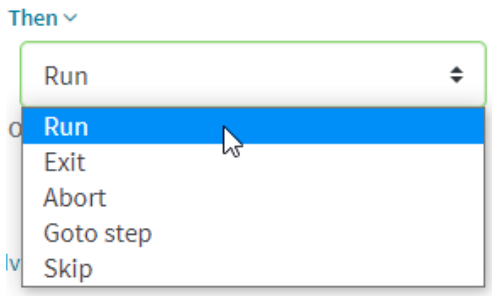
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

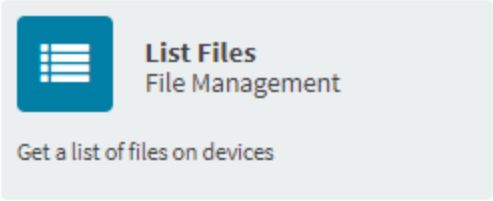
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

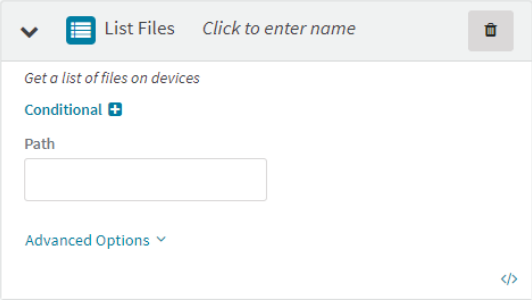
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

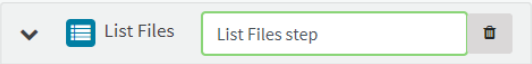
List Files step



1. Click **List Files** to add the List Files step to your automation.



2. Click the header to enter a name for the step.

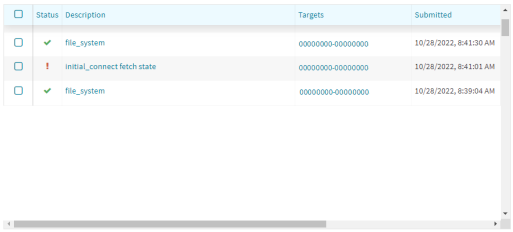


3. Type the **Path** to the files on the device.

   To view the output of the **List Files** step after a successful run:

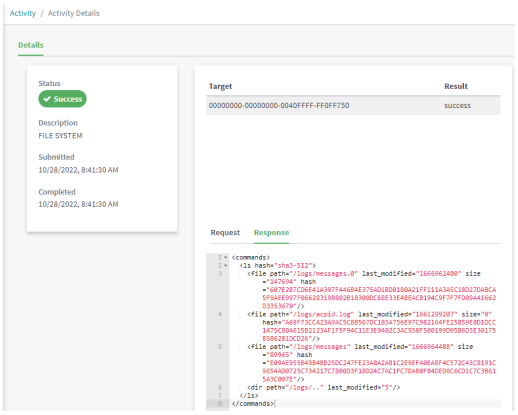
a. In the main menu, click **Activity**.

The output of the **List Files** step is listed as a **file_system** activity.



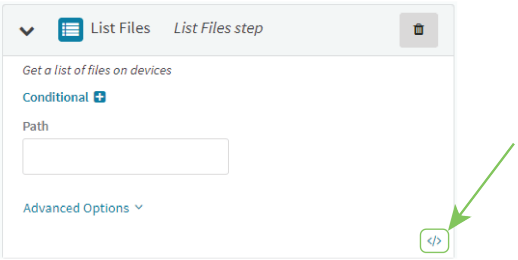
b. Click the Description to view **Activity Details**.

The activity details lists the filenames, modification date, size and hash.



You can also view the step in JSON format.

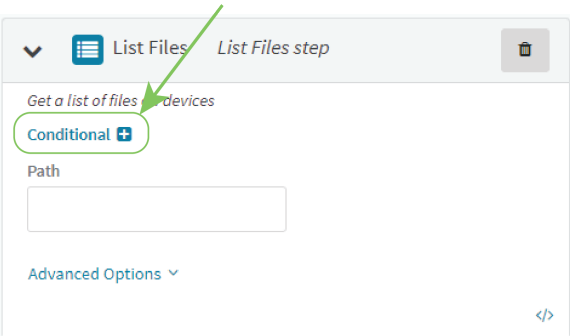
1. Click </>.



2. Click to return to edit mode.

Conditional processing

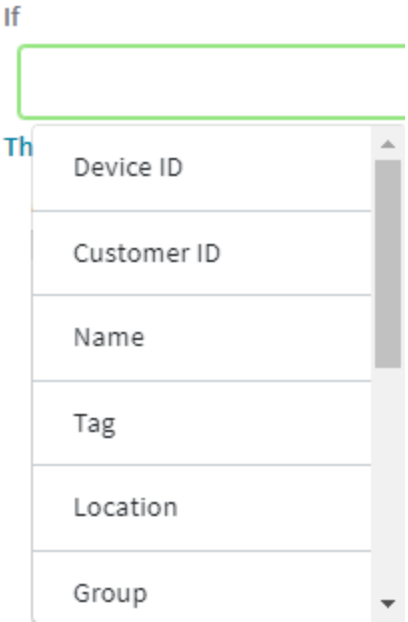
You can optionally set conditions that will determine whether this step should be executed.



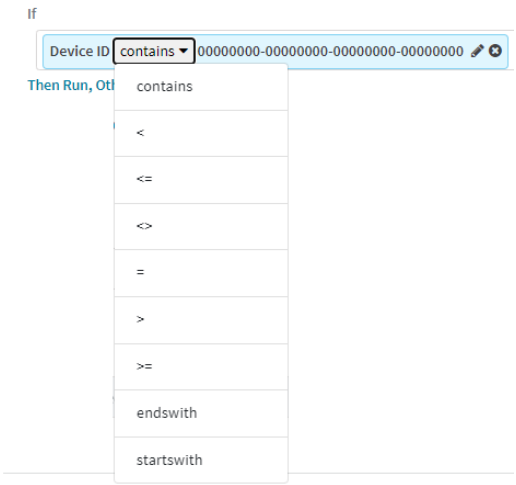
1. Click to expand Conditional.

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



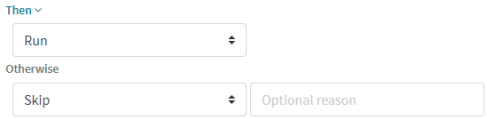
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



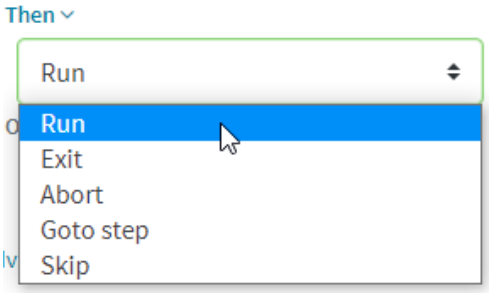
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

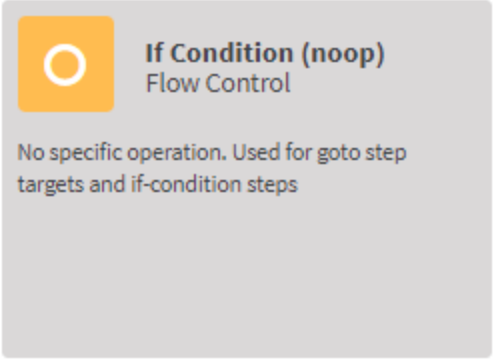
Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

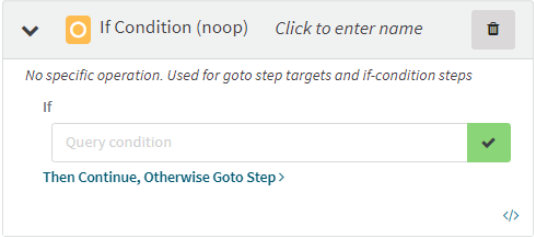
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

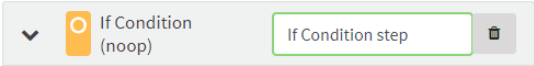
If Condition step



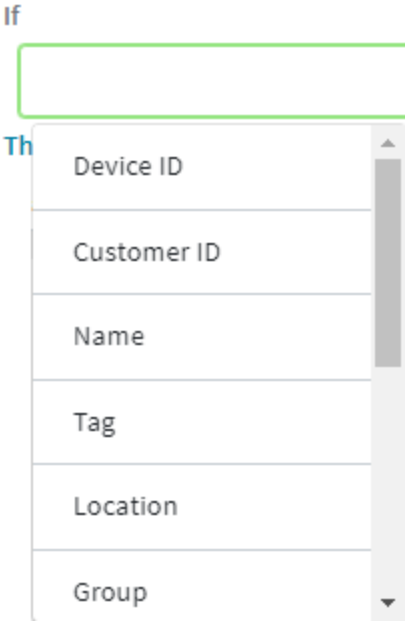
1. Click **If Condition (noop)** to add the If Condition (noop) step to your automation.



2. Click the header to enter a name for the step.

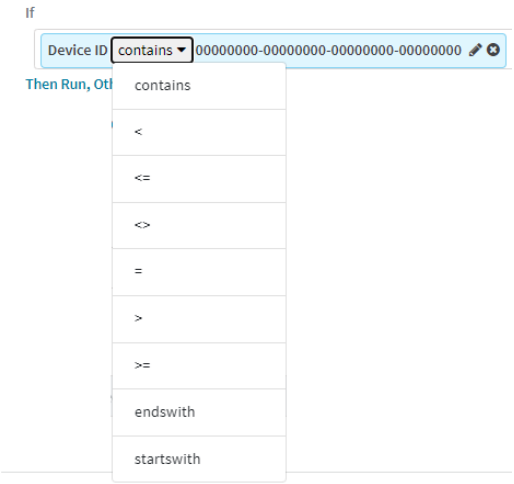


3. Click **Query condition**.
   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

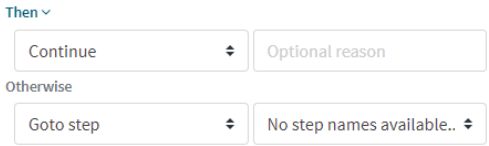
b. If Condition step control conditional matching. Click the comparison operator to open a menu to select a different operator.



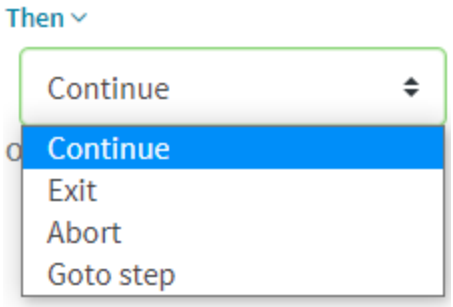
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

i. Click Then Continue, Otherwise Goto Step>.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

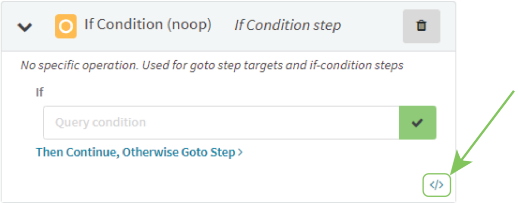
  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Continue**, **Exit**, or **Abort** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

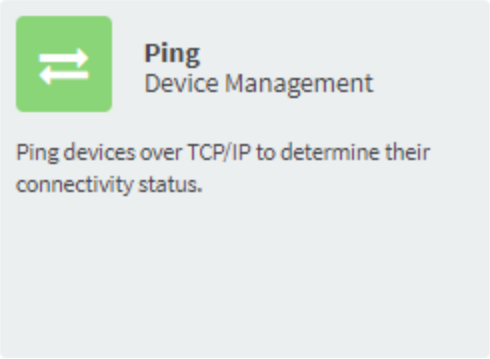
You can also view the step in JSON format.

1. Click </>.

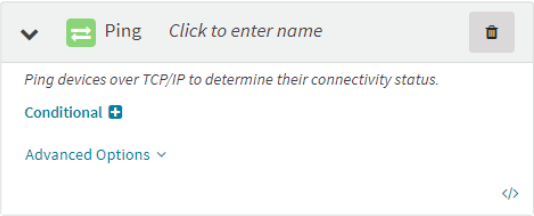


2. Click to return to edit mode.

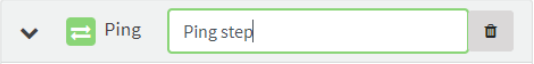
Ping step



1. Click **Ping** to add the Ping step to your automation.



2. Click the header to enter a name for the step.



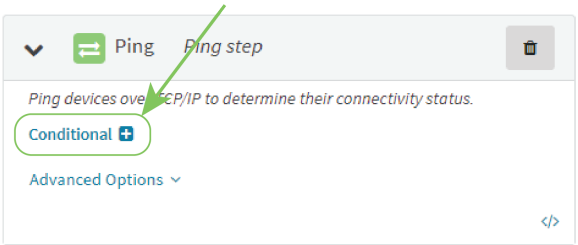
You can also view the step in JSON format.

1. Click </>.

2. Click to return to edit mode.

Conditional processing

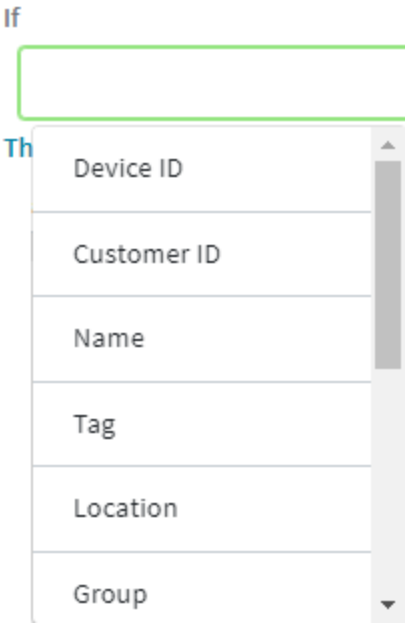
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

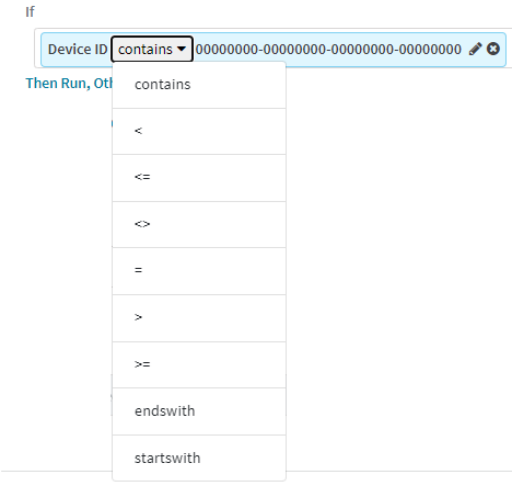
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

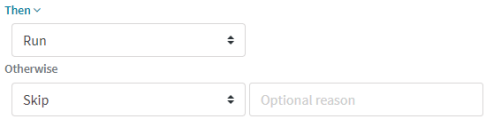
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



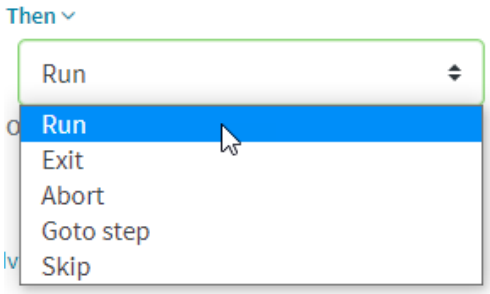
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

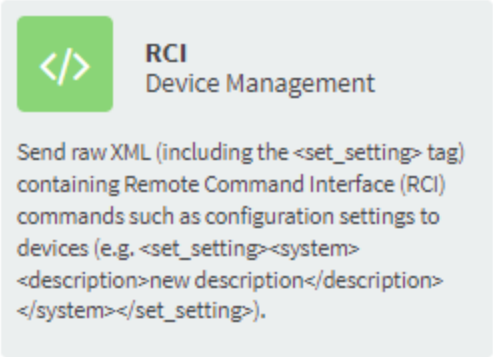
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

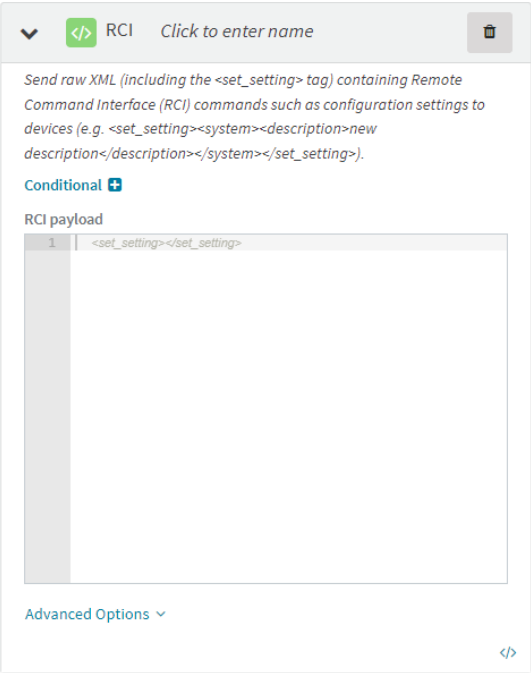
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

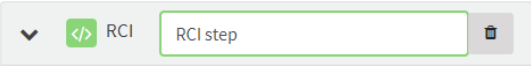
Remote Command Interface (RCI) step



1. Click **RCI** to add the RCI step to your automation.



2. Click the header to enter a name for the step.



3. Type an RCI command in XML format. The following commands are supported:
   - query_setting

     Retrieves the device's current settings. For example, to return all of the settings for a device, type:

     ```
     <query_setting/>
     ```

     You can also return a subset of the device settings. For example:

     ```
     <query_setting>
       <system/>
     <query_setting/>
     ```

     will return the device settings under the system node.
   - set_setting

     Sets the device's configuration settings. For example, to set the name of a device:

     ```
     <set_setting>
       <system>
         <name>Techpubs_device</name>
       </system>
     </set_setting>
     ```

- query_state

  Retrieves the state of the device. For example, to return the complete state of a device:

```
<query_state/>
```

  You can also return a subset of the state. For example:

```
<query_state>
  <metrics>
    <network>
      <device>
        <eth/>
      </device>
    </network>
  </metrics>
</query_state>
```

- set_state

  Sets the temporary running state of the device.
- query_descriptor

  Retrieves the RCI descriptor from a device.
- do_command

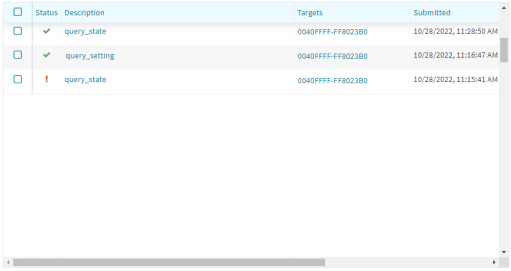
  Passes a command the specified target.

See the Remote Command Interface (RCI) Specification for further information about RCI commands.

To view the output of the RCI commands that retrieve information from the device:

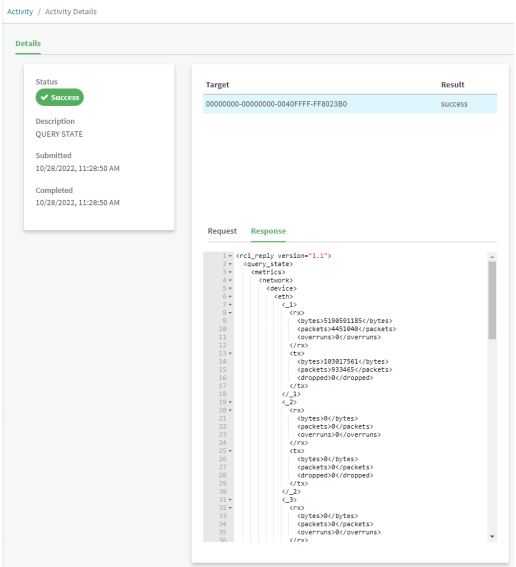
a. In the main menu, click **Activity**.

   The output of the RCI command step is listed by name.



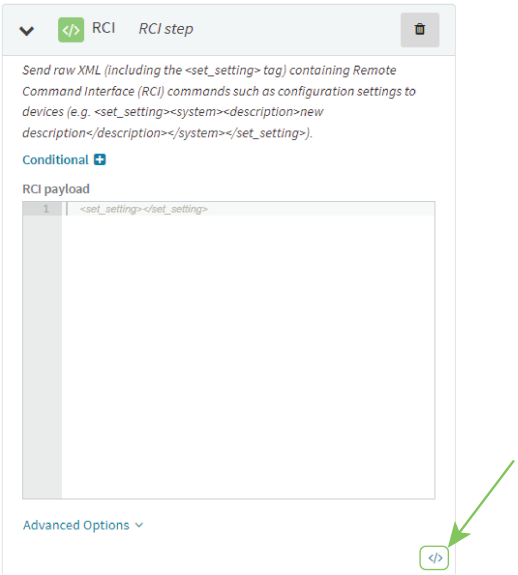
b. Click the Description to view **Activity Details**.

The activity details lists the filenames, modification date, size and hash.



You can also view the step in JSON format.

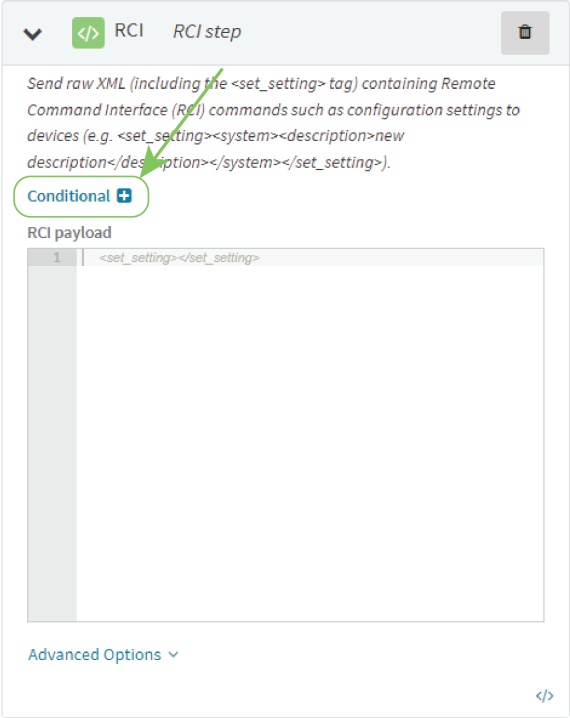
1. Click </>.



2. Click to return to edit mode.

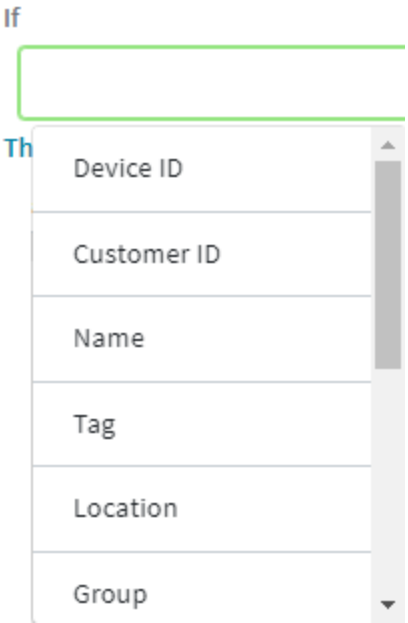
Conditional processing

You can optionally set conditions that will determine whether this step should be executed.



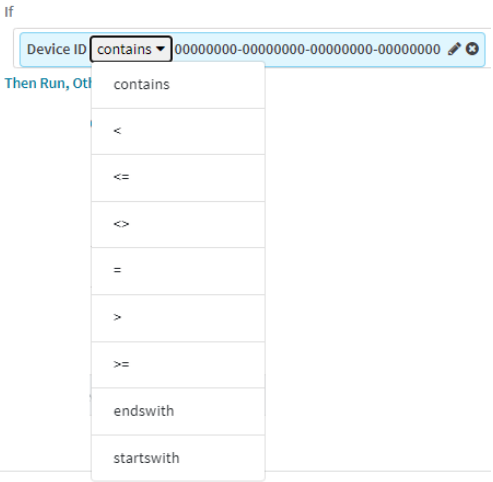
1. Click to expand Conditional.

2. Click **Query condition**.
   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

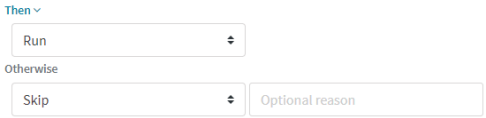
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



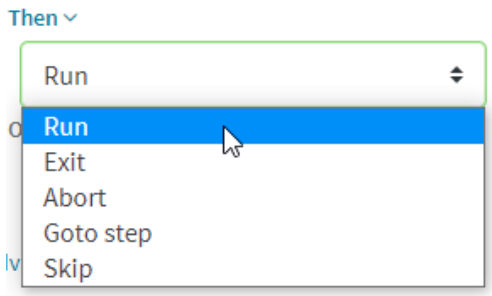
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

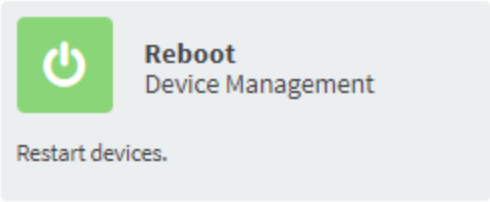
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

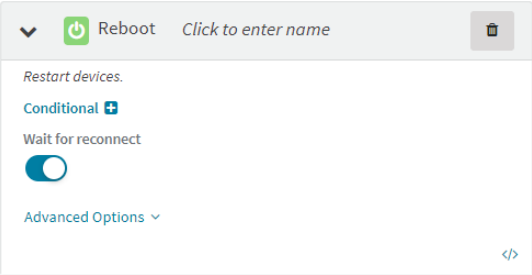
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

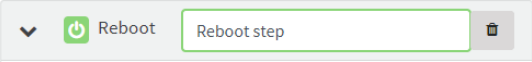
Reboot step



1. Click **Reboot** to add the Reboot step to your automation.

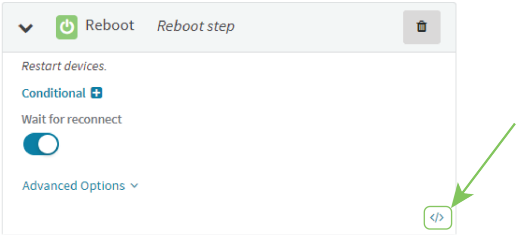


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

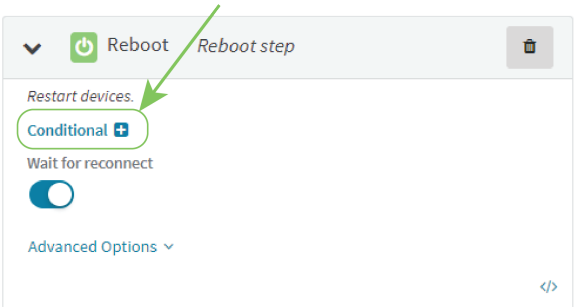
1. Click </>.



2. Click to return to edit mode.

Conditional processing

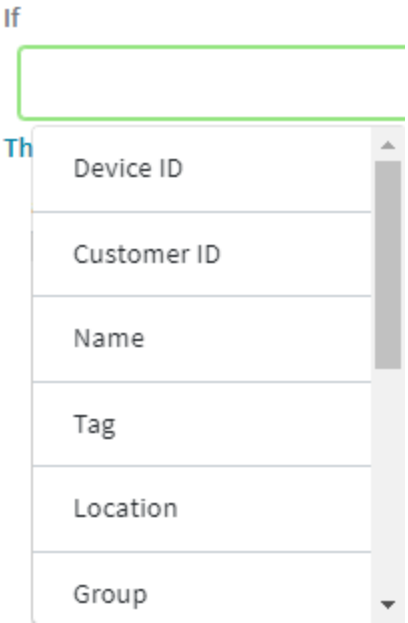
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional .

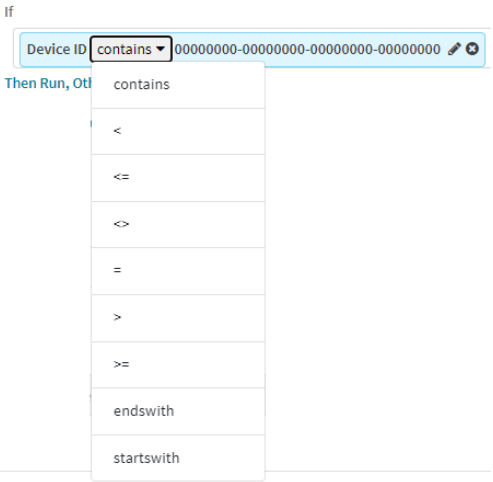
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

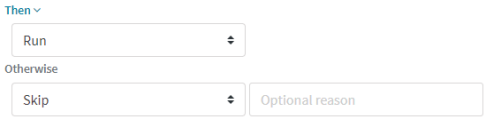
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



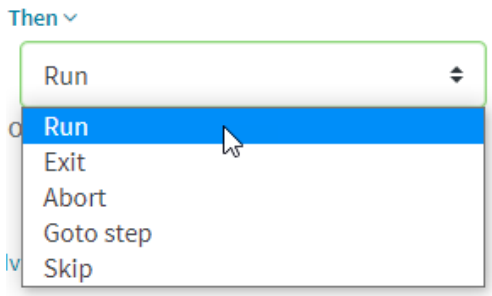
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

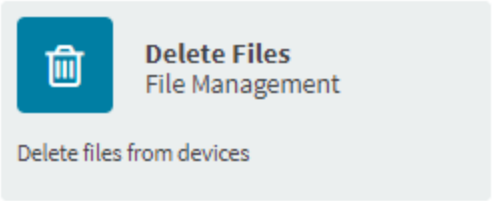
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

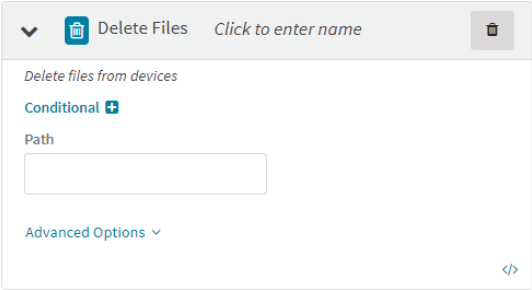
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

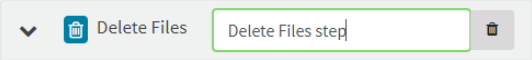
Delete Files step



1. Click **Delete Files** to add the Delete Files step to your automation.



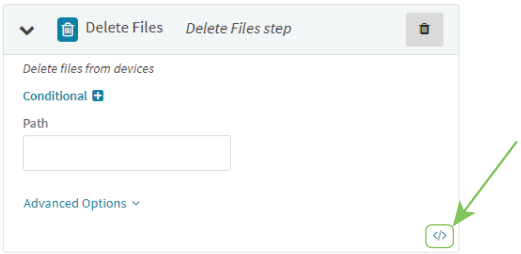
2. Click the header to enter a name for the step.



3. Type the **Path** and filename of the file to be deleted.

You can also view the step in JSON format.

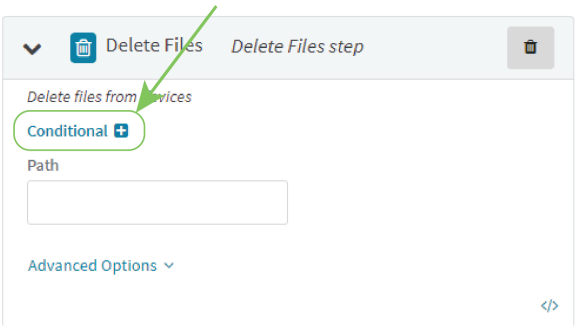
1. Click </>.



2. Click to return to edit mode.

Conditional processing

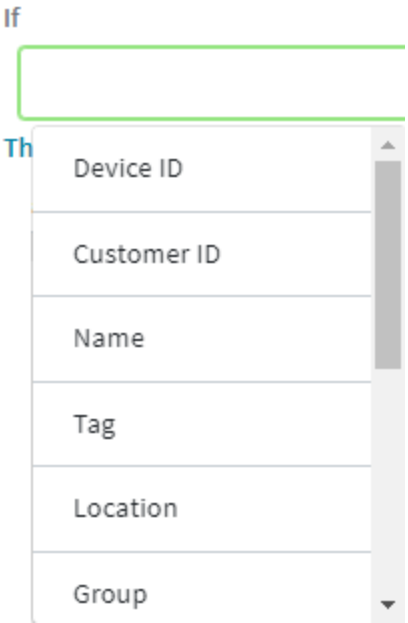
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

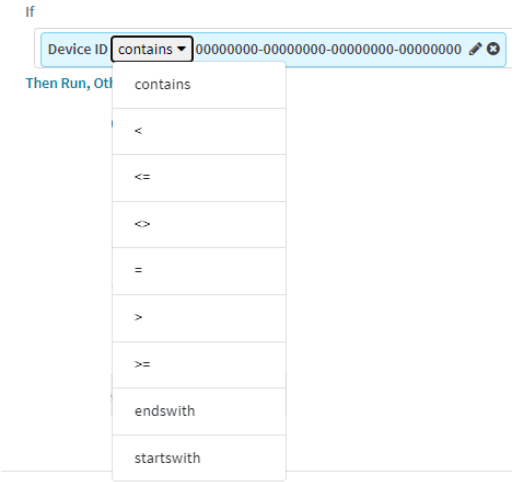
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

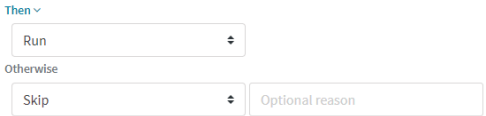
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



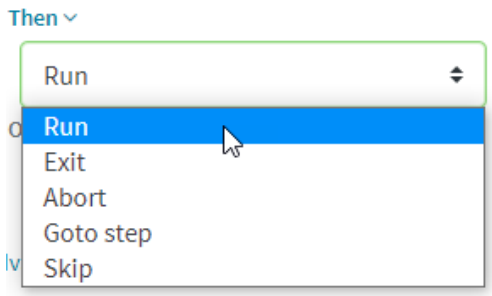
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

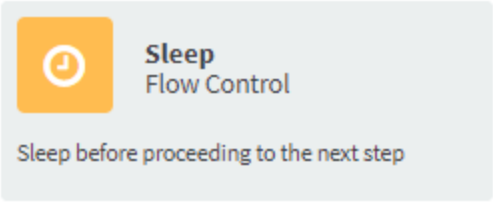
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

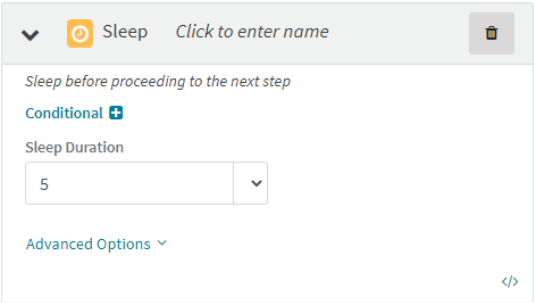
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

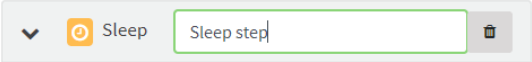
Sleep step



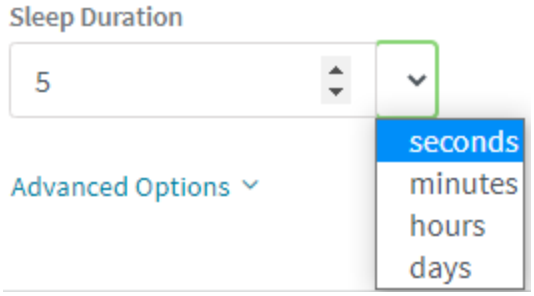
1. Click **Sleep** to add the Sleep step to your automation.



2. Click the header to enter a name for the step.

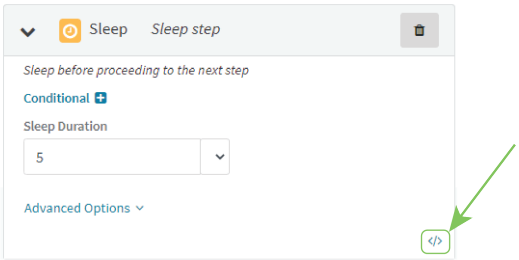


3. Type or select the **Sleep Duration**, and click ⊠to select the time period:



You can also view the step in JSON format.

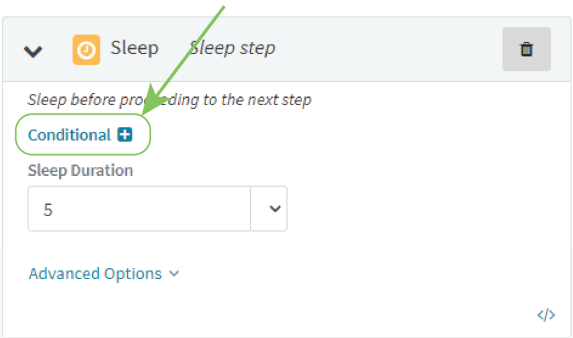
1. Click </>.



2. Click to return to edit mode.

Conditional processing

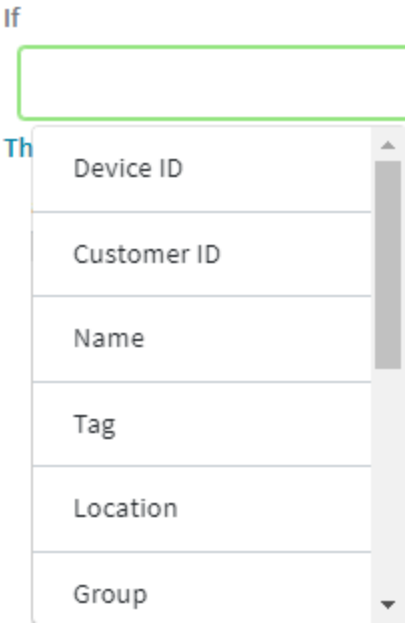
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

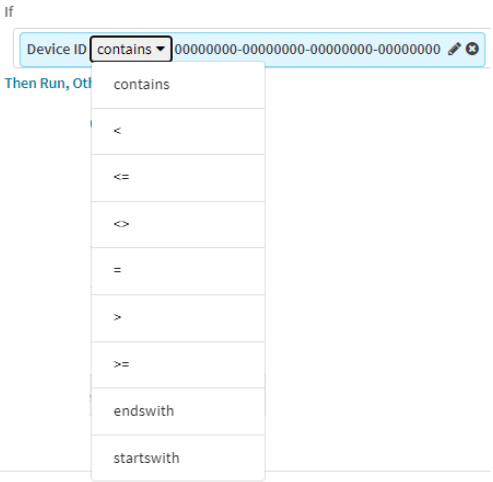
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

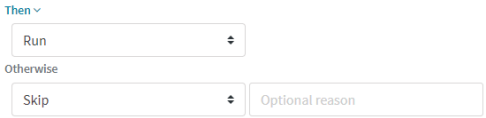
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



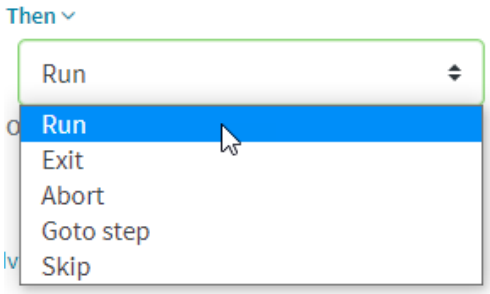
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

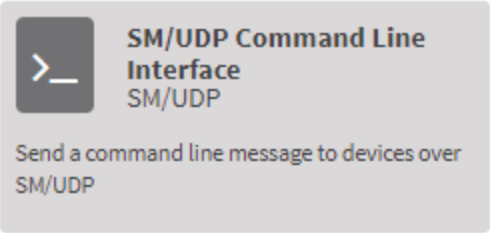
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

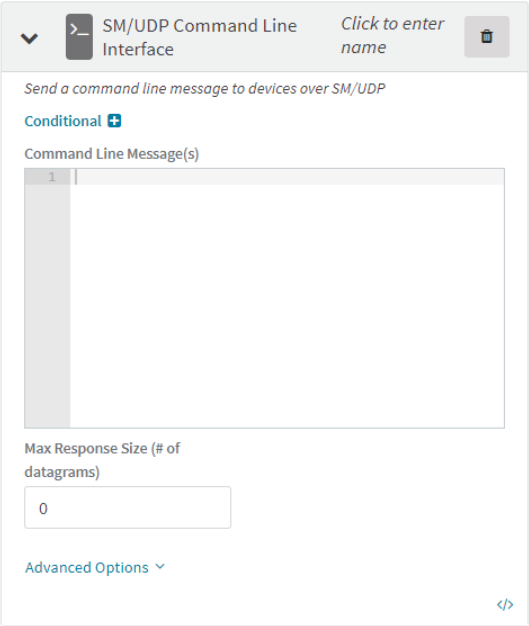
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

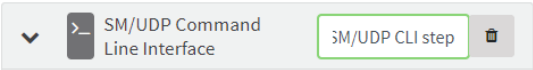
SM/UDP Command Line Interface step



1. Click **SM/UDP Command Line Interface** to add the SM/UDP Command Line Interface step to your automation.



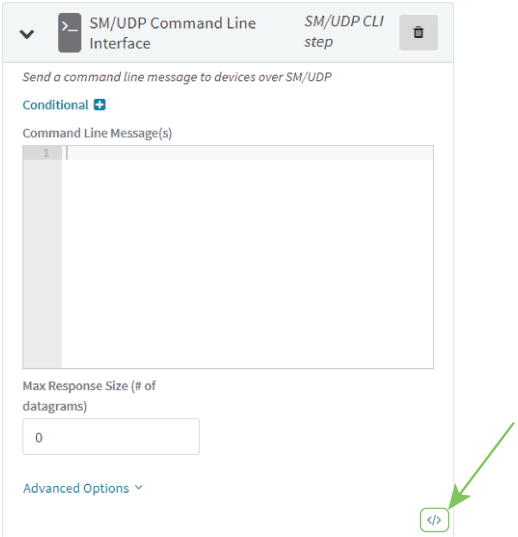
2. Click the header to enter a name for the step.



3. Type the **Command Line Message(s)** that should be executed at the command line as part of this automation.
4. For **Max Response Size**, type the maximum number of datagrams that the response can contain.

You can also view the step in JSON format.

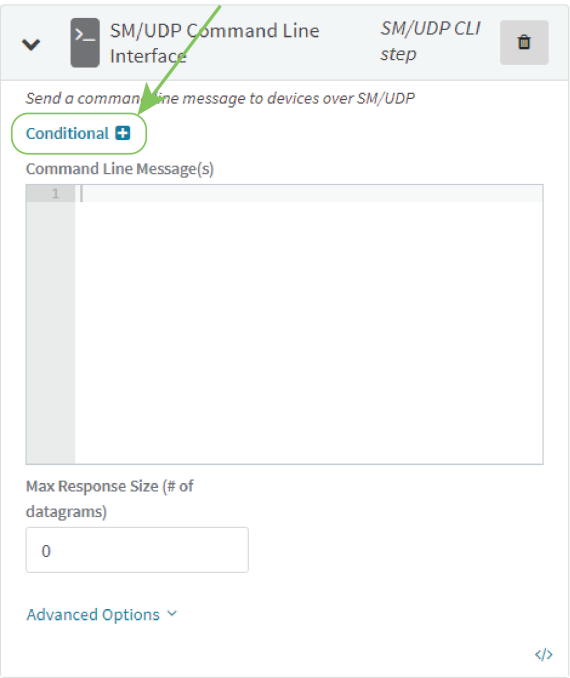
1. Click </>.



2. Click to return to edit mode.

Conditional processing

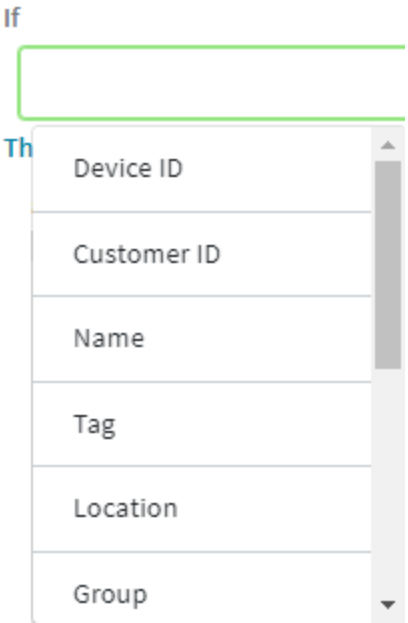
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional .

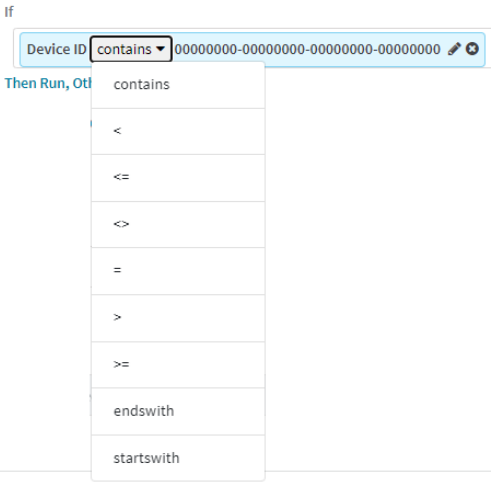
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

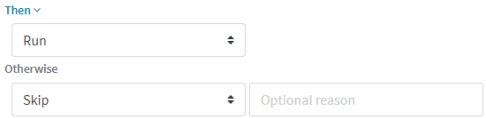
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



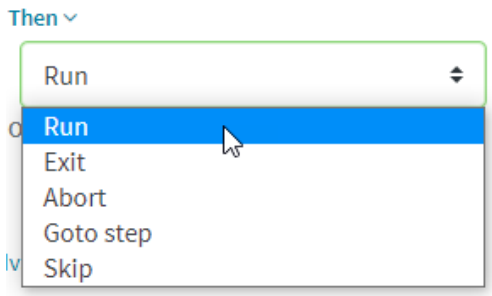
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

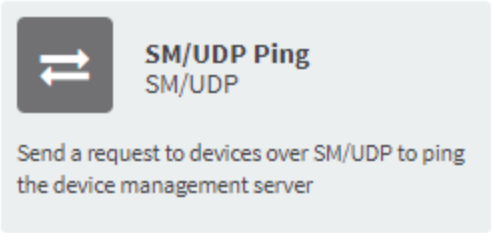
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

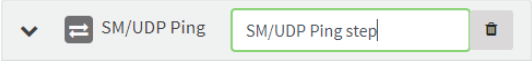
        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

SM/UDP Ping step



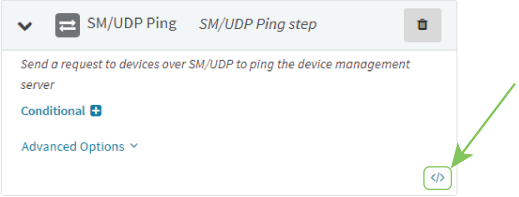
1. Click **SM/UDP Ping** to add the SM/UDP Ping step to your automation.

2. Click the header to enter a name for the step.



You can also view the step in JSON format.

1. Click </>.



2. Click to return to edit mode.

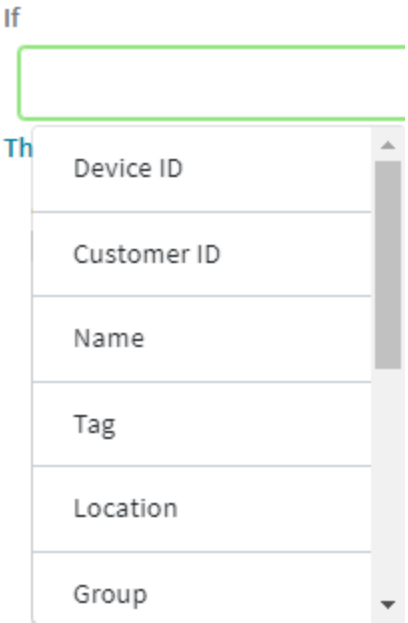
Conditional processing

You can optionally set conditions that will determine whether this step should be executed.

1. Click to expand Conditional.

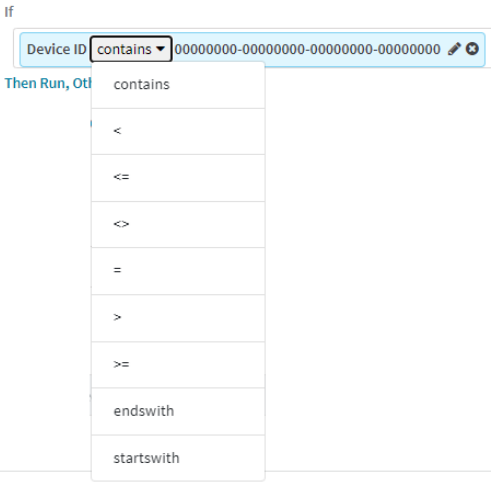
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

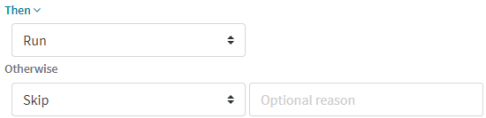
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



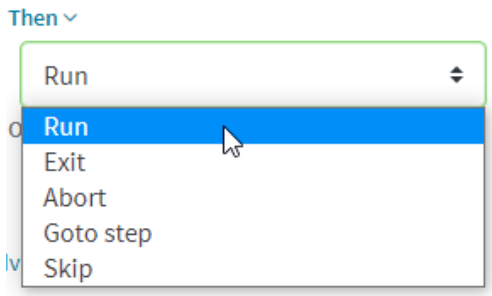
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

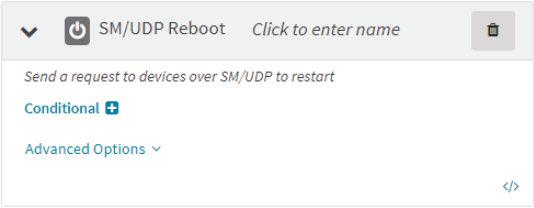
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

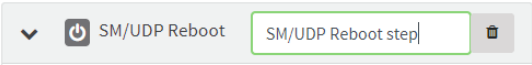
        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

SM/UDP Reboot step

1. Click **SM/UDP Reboot** to add the SM/UDP Reboot step to your automation.

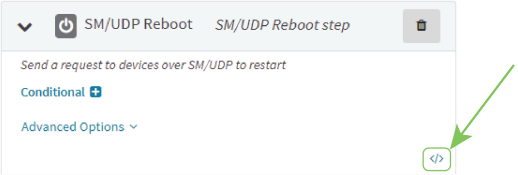


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

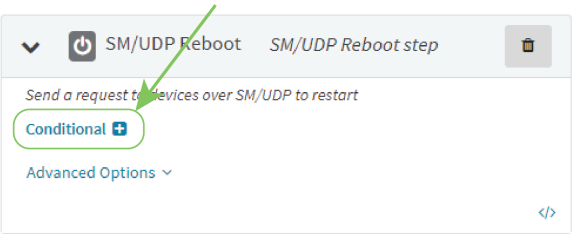
1. Click </>.



2. Click to return to edit mode.

Conditional processing

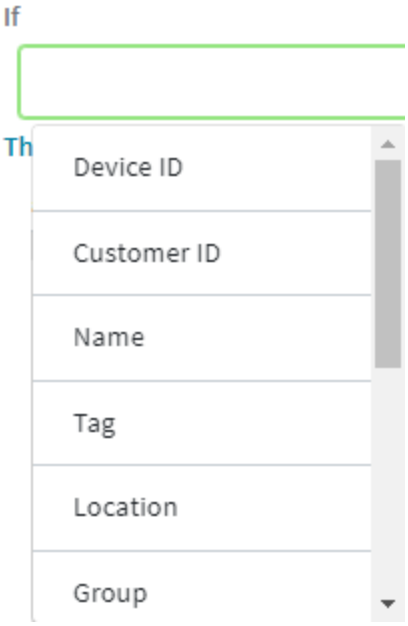
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

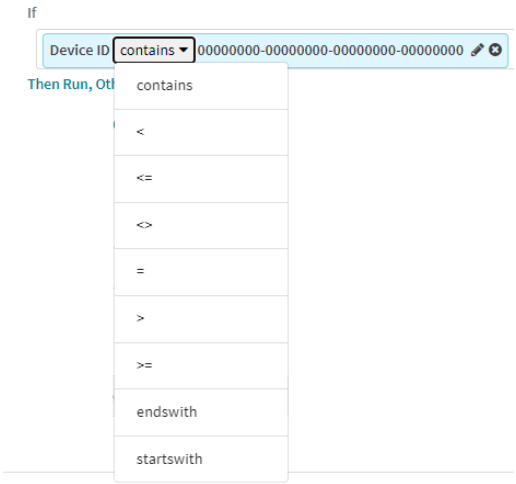
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click ▌.

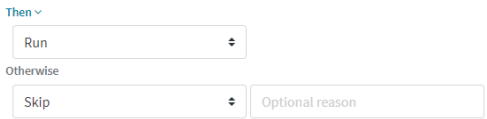
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



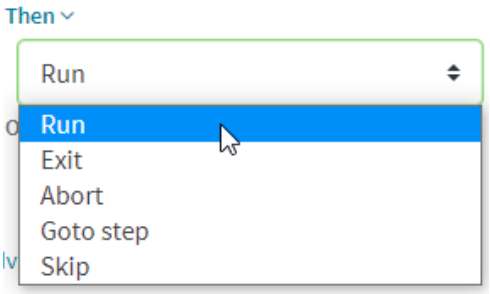
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

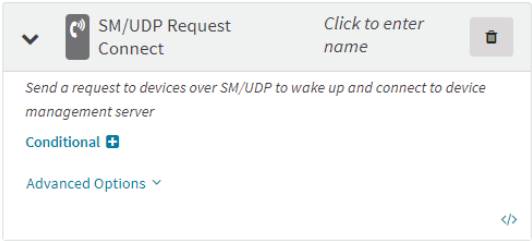
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

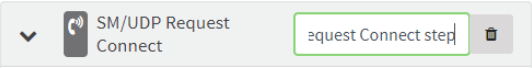
      - **Exit**
      - **Abort**

SM/UDP Request Connect step

1. Click **SM/UDP Request Connect** to add the SM/UDP Request Connect step to your automation.



2. Click the header to enter a name for the step.



You can also view the step in JSON format.

1. Click </>.

2. Click to return to edit mode.

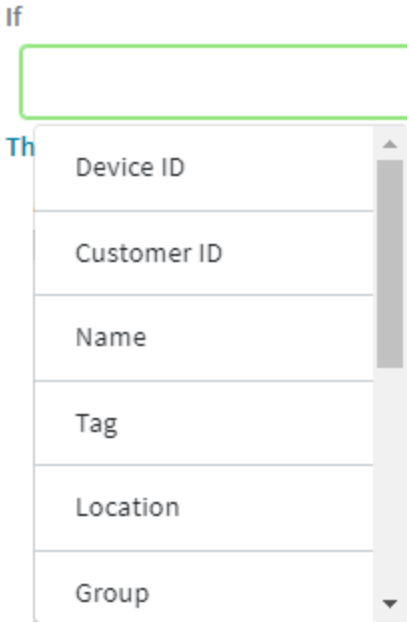
Conditional processing

You can optionally set conditions that will determine whether this step should be executed.

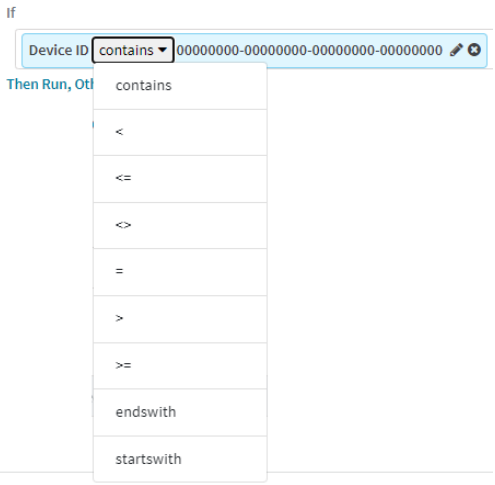
1. Click to expand Conditional .

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



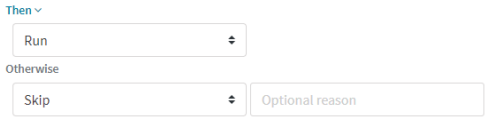
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



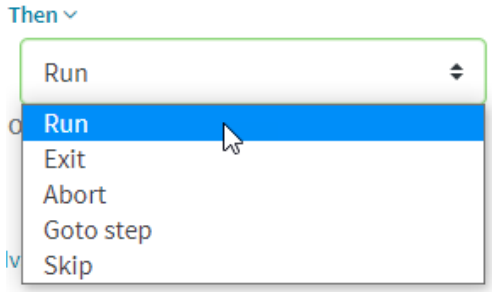
   c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

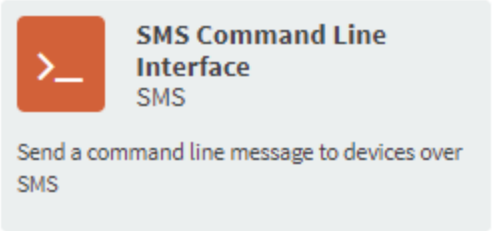
Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

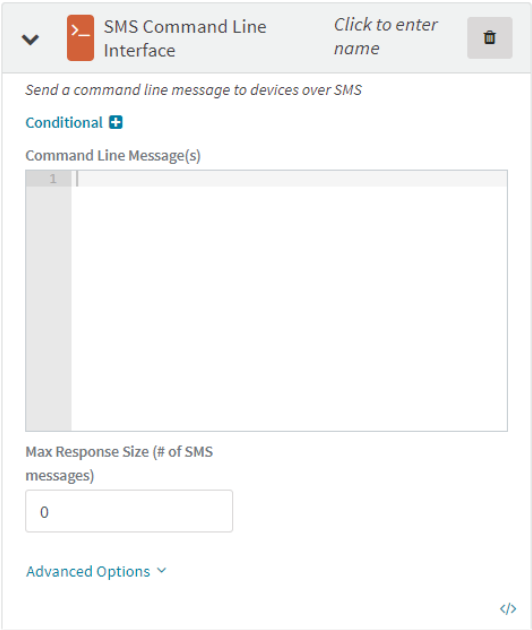
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

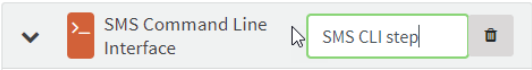
SMS Command Line Interface step



1. Click **SMS Command Line Interface** to add the SMS Command Line Interface step to your automation.



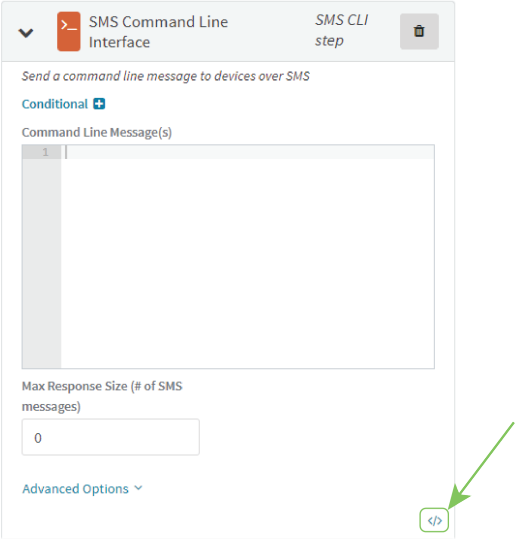
2. Click the header to enter a name for the step.



3. Type the **Command Line Message(s)** that should be executed at the command line as part of this automation.
4. For **Max Response Size**, type the maximum number of SMS messages that the response can contain.

You can also view the step in JSON format.

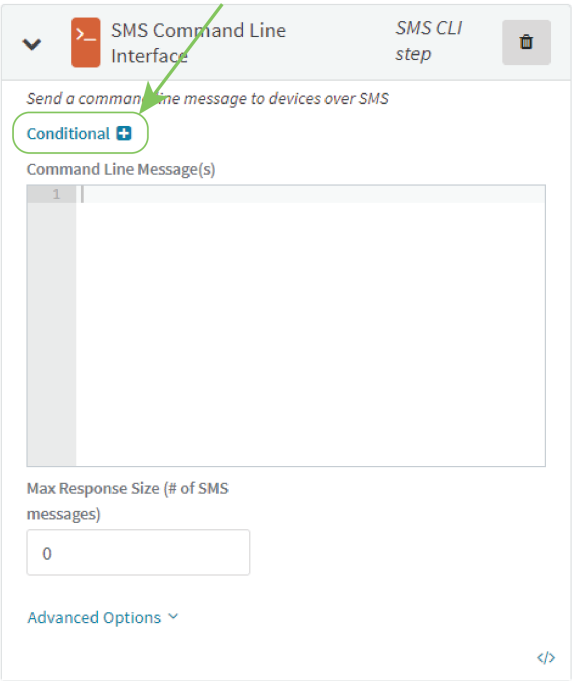
1. Click </>.



2. Click to return to edit mode.

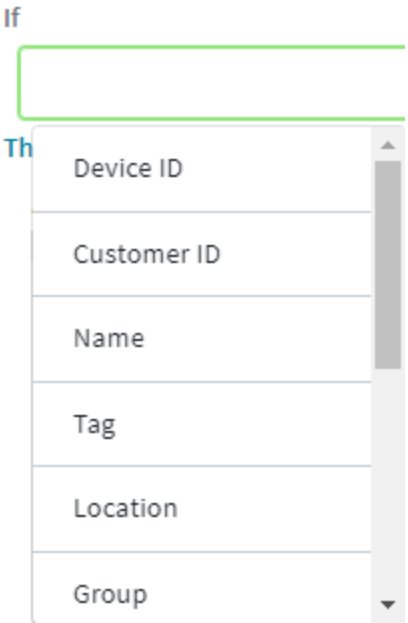
Conditional processing

You can optionally set conditions that will determine whether this step should be executed.



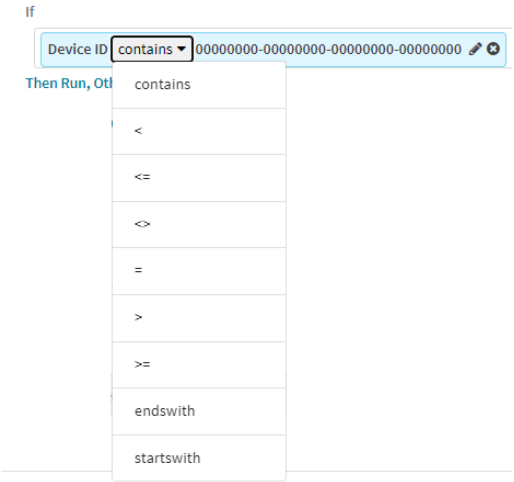
1. Click to expand Conditional.

2. Click **Query condition**.
   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

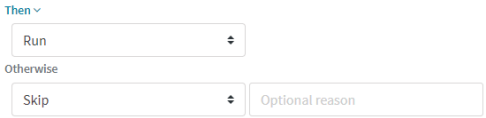
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



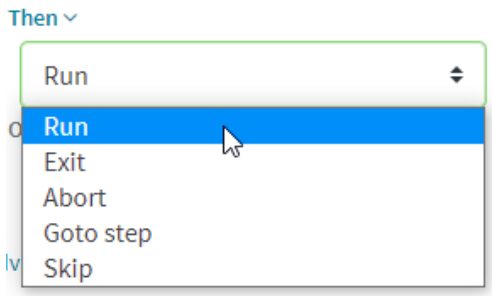
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

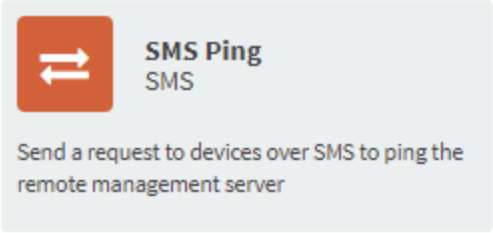
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

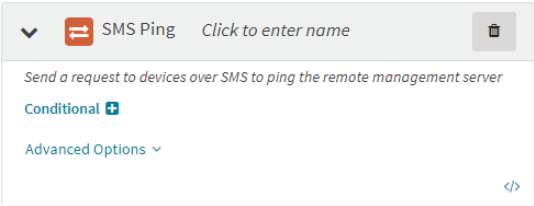
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

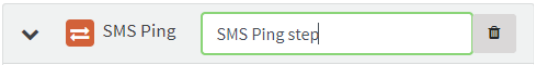
SMS Ping step



1. Click **SMS Ping** to add the SMS Ping step to your automation.

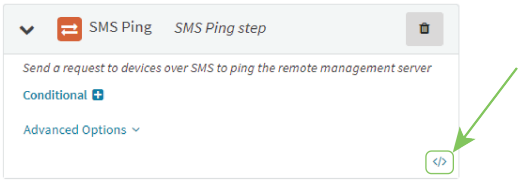


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

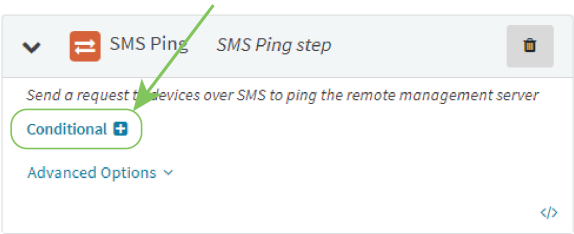
1. Click </>.



2. Click to return to edit mode.

Conditional processing

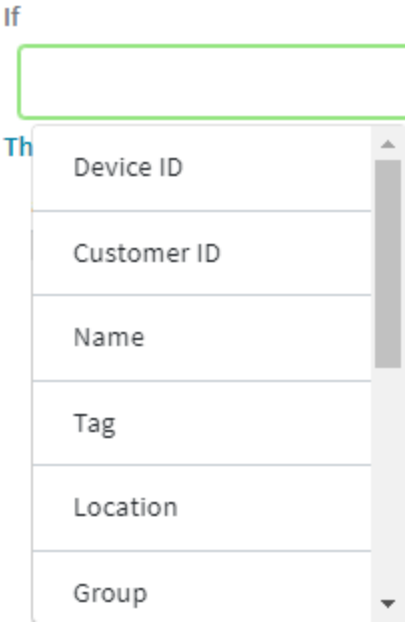
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

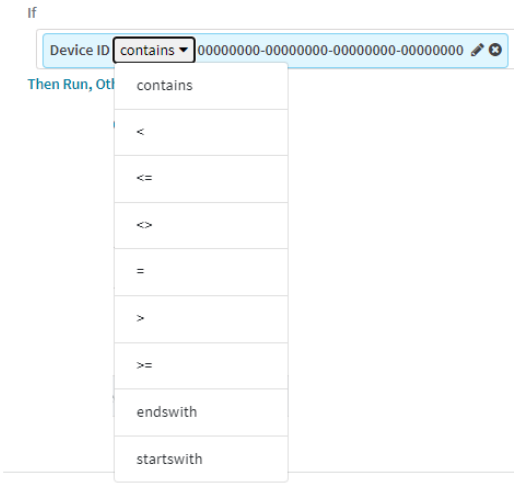
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

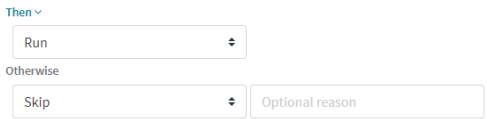
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



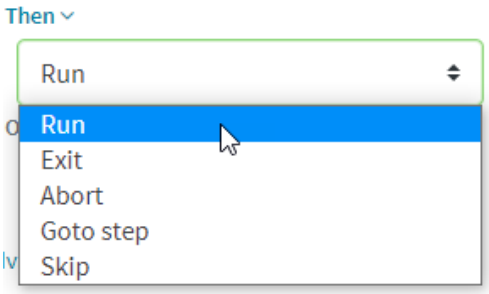
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

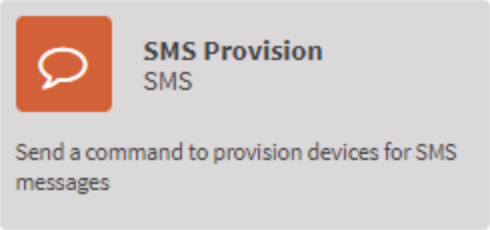
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

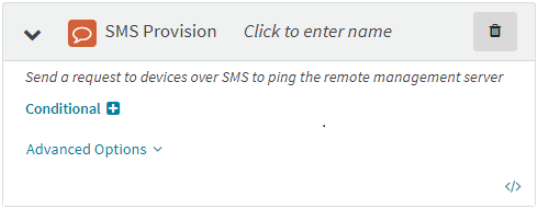
        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

      - **Exit**
      - **Abort**

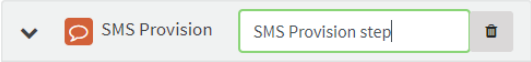
SMS Provision step



1. Click **SMS Provision** to add the SMS Provision step to your automation.

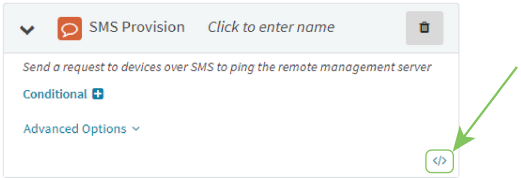


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

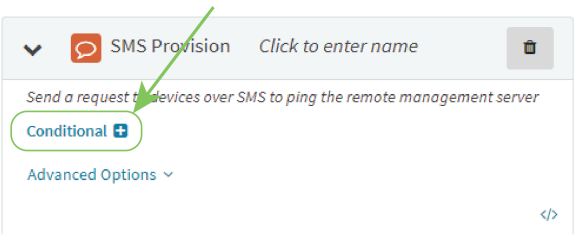
1. Click </>.



2. Click to return to edit mode.

Conditional processing

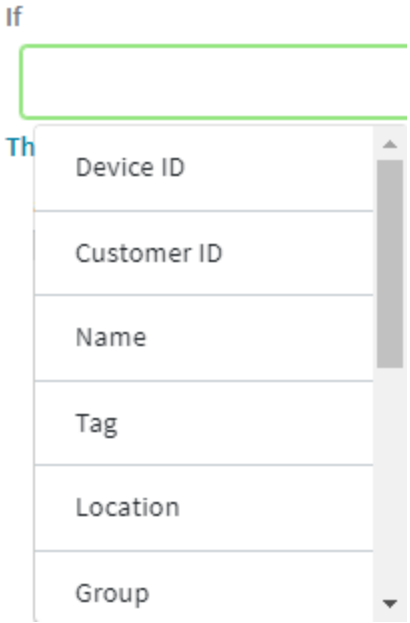
You can optionally set conditions that will determine whether this step should be executed.



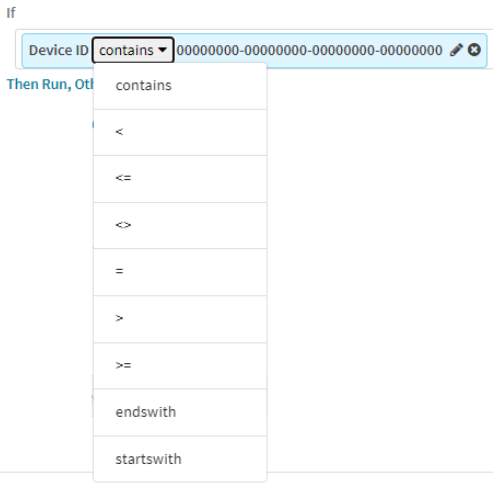
1. Click to expand Conditional .

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



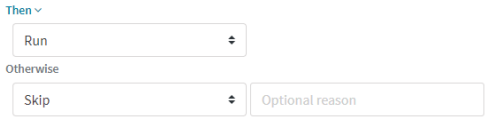
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



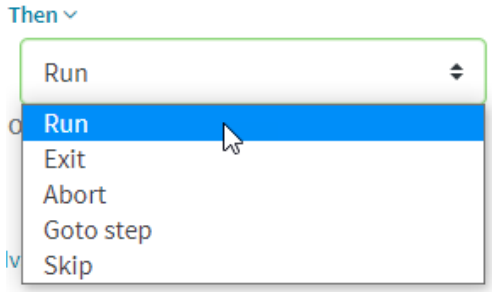
   c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

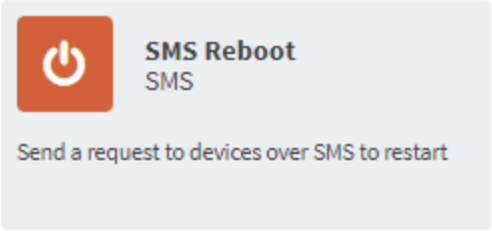
Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

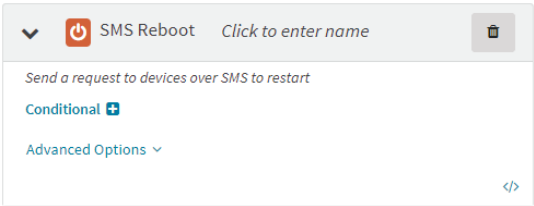
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

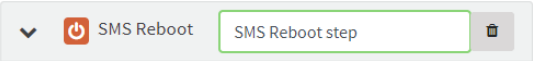
SMS Reboot step



1. Click **SMS Reboot** to add the SMS Reboot step to your automation.

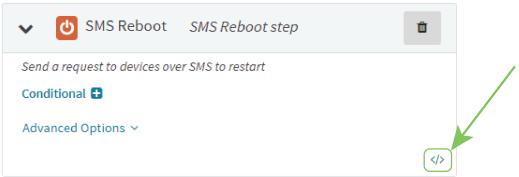


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

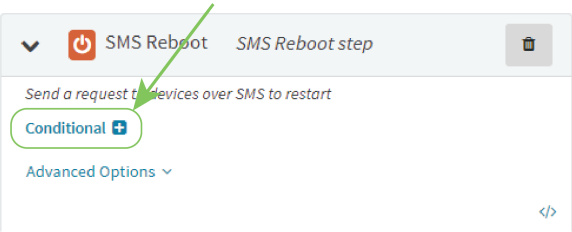
1. Click </>.



2. Click to return to edit mode.

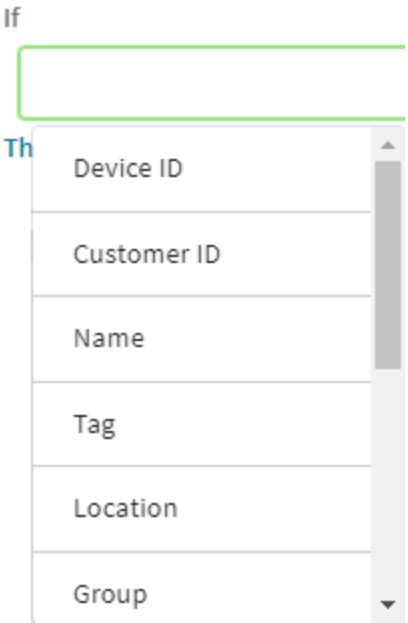
Conditional processing

You can optionally set conditions that will determine whether this step should be executed.



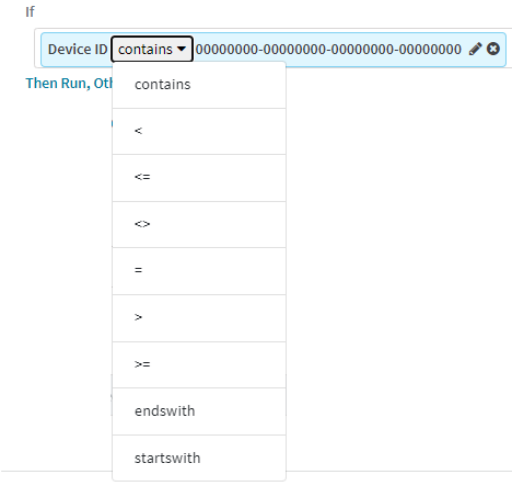
1. Click to expand Conditional.

2. Click **Query condition**.
   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

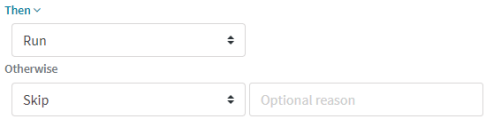
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



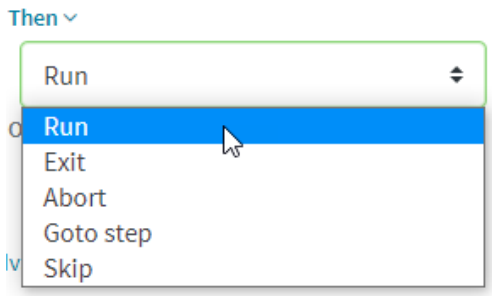
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

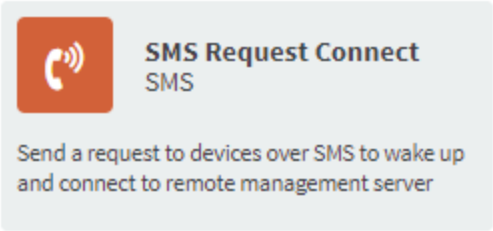
Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

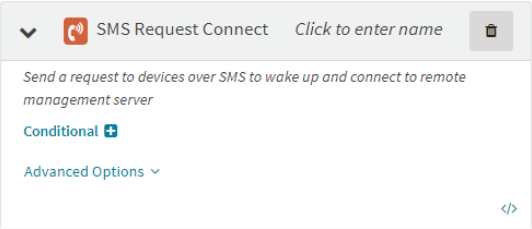
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

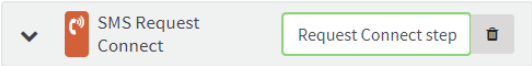
SMS Request Connect step



1. Click **SMS Request Connect** to add the SMS Request Connect step to your automation.

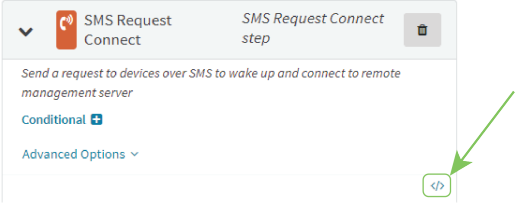


2. Click the header to enter a name for the step.



You can also view the step in JSON format.

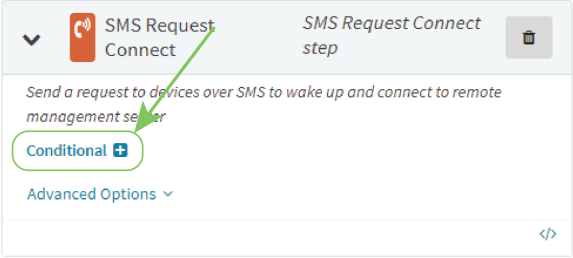
1. Click </>.



2. Click to return to edit mode.

Conditional processing

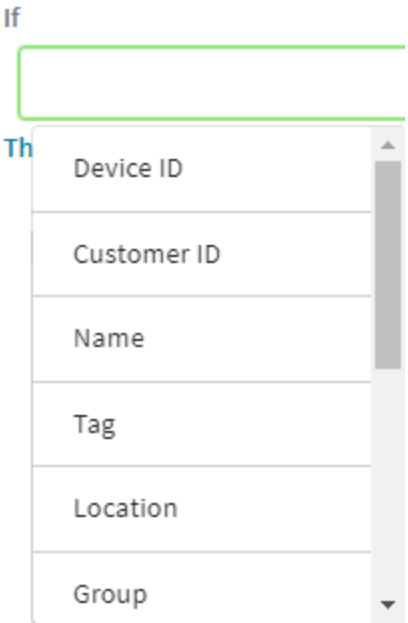
You can optionally set conditions that will determine whether this step should be executed.



1. Click to expand Conditional.

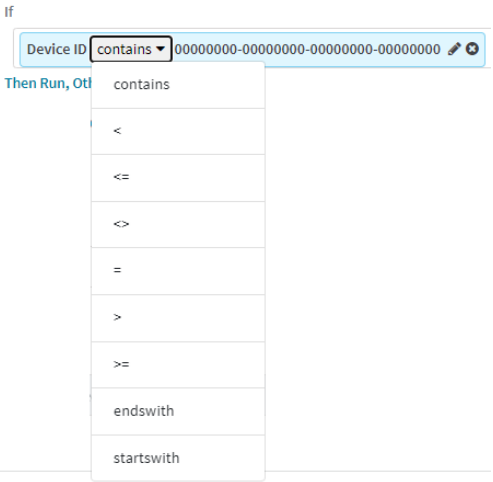
2. Click **Query condition**.

   A menu with a list available conditional query options displays.



a. Select an option, type a value, and click .

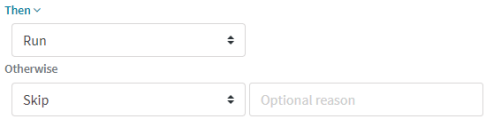
b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



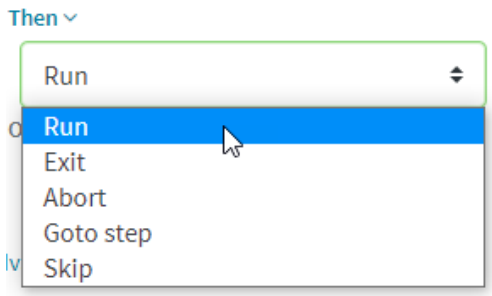
c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



ii. For **Then**, click to select an action to be performed when the query conditions are met:



- If **Goto step** is selected, click **Select a step name...** and select the name of the step.

  Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

- (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

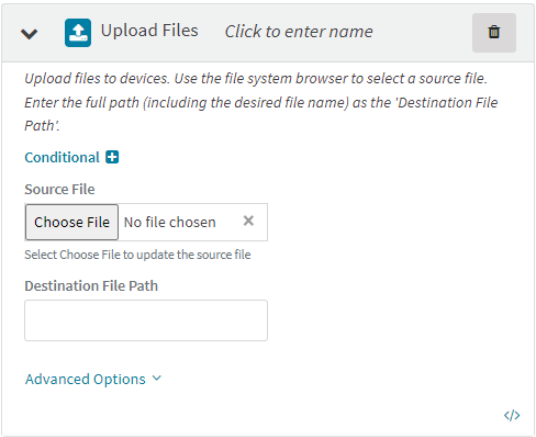
1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.

3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

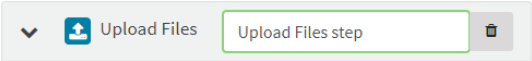
        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

Upload Files step

1. Click **Upload Files** to add the Upload Files step to your automation.



2. Click the header to enter a name for the step.



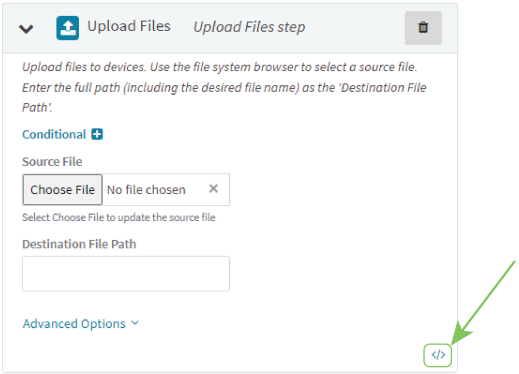
3. Click **Choose File** and select the file from your local filesystem.
4. For **Destination File Path**, type the path and filename on the device where the file should be uploaded to.

   For example, to upload a file named testfile.txt to the analyzer directory, type:

```
/analyzer/testfile.txt
```

You can also view the step in JSON format.

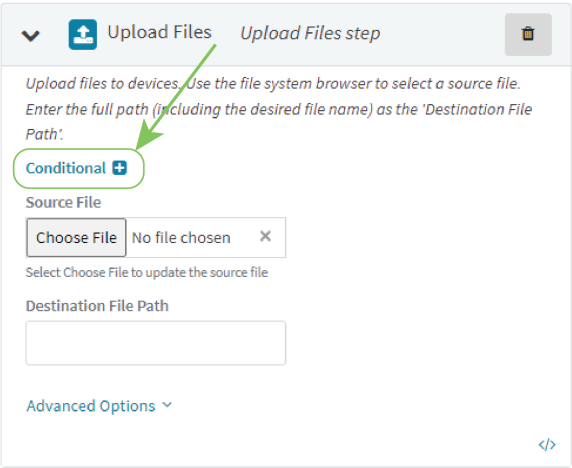
1. Click </>.



2. Click to return to edit mode.

Conditional processing

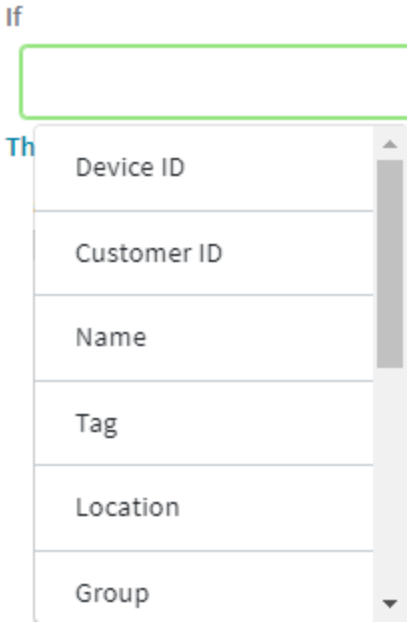
You can optionally set conditions that will determine whether this step should be executed.



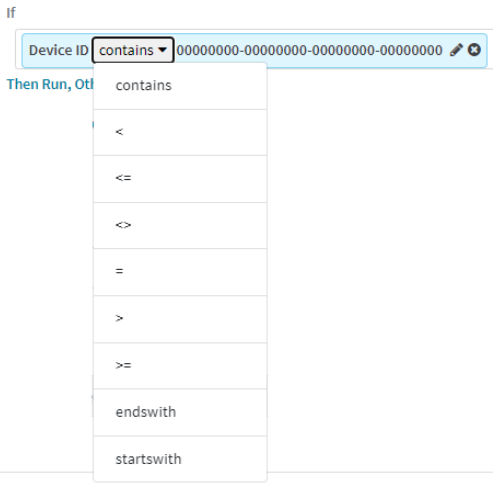
1. Click to expand Conditional .

2. Click **Query condition**.

   A menu with a list available conditional query options displays.



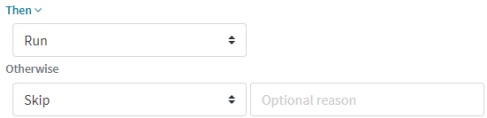
   a. Select an option, type a value, and click .
   b. Comparison operators control conditional matching. Click the comparison operator to open a menu to select a different operator.



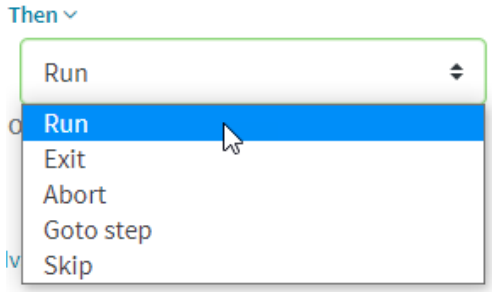
   c. Click in the **Query condition** text box again to add additional query options.

a. By default, the step will run if the query conditions are met, and will be skipped if the conditions are not met. To change the default behavior:

   i. Click Then Run, Otherwise Skip >.



   ii. For **Then**, click to select an action to be performed when the query conditions are met:



   - If **Goto step** is selected, click **Select a step name...** and select the name of the step.

     Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.

   - (Optional) If **Exit**, **Abort**, or **Skip** are selected, for **Optional reason**, type a message that will appear in the run details.

   iii. For **Otherwise**, click to select an action to be performed when the query conditions are not met.

Comparison operators

Operator	Matches if the current value of the query option...
contains	*Contains* the value entered in the **Query condition** text box.
<	Is *less than* the value entered in the **Query condition** text box.
<=	is *less than or equal to* the value entered in the **Query condition** text box.
<>	*Does not equal* the value entered in the **Query condition** text box.
=	*Equals* the value entered in the **Query condition** text box.
>	Is *greater than* the value entered in the **Query condition** text box.
>=	is *greater than or equal to* the value entered in the **Query condition** text box.
endswith	*Ends with* the value entered in the **Query condition** text box.
startswith	*Begins with* the value entered in the **Query condition** text box.

Error processing and post-processing

Advanced Options allow you to configure what actions to take when the step produces an error, and what actions to take when the step has completed successfully.

1. Click **Advanced Options**.
2. Enable **Wait if Offline** to allow this step to be queued while the device is offline and completed the next time it connects. Any actions that can be taken while the device is offline, will still be taken.
3. Click **On Error** to select what should happen when the step produces an error:
   - **End**: The automation will end when this step produces an error.
   - **Continue**: The automation will proceed to the next step when this step produces an error.
   - **Retry**: The automation will retry the step when it produces an error.
     - Select the number of times to retry the step. If the step does not succeed within the selected number of times, the automation will end.
4. Enable **On End** to select an action that should happen when the step ends:
   a. Select whether the on end action should take place **Always**, **When successful**, or **When errored**.
   b. Select an action, either:
      - **Goto step**: click **Select a step name...** and select the name of the step.

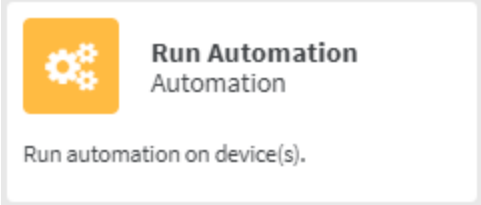
        Note To use the **Goto step** functionality, you must enter a name for steps during configuration of the step.
      - **Exit**
      - **Abort**

Manually run an automation

Automations can be also scheduled to run automatically, on the Triggers page of the automation details. See Create an automation.

Manually run an automation on a specific device

1. From the main menu, click **Management** > **Devices**.
2. Select one or more devices to run an automation against, or click a device **Name** or **Device ID** to open the **Device Details** view.
3. From the **Actions** menu, click **Run Automation**.



4. Select an automation and click **Run**.

Run an automation from the Automations page

1. From the main menu, click **Management** > **Automations**.
2. Select an automation.
3. Click **Actions** > **Run automation**.

You can also run an automations from the Automations details view

1. From the main menu, click **Management** > **Automations**.
2. Select an automation and click **Actions** > **Automation Details**, or click the **Automation ID** or **Name** of the automation.
3. Click **Run Automation**.

Set an automation to run as part of a configuration

You can also set an automation to run as part of a configuration:

- Prior to scanning devices.
- After remediation has been performed on a device.
- After a successful scan.

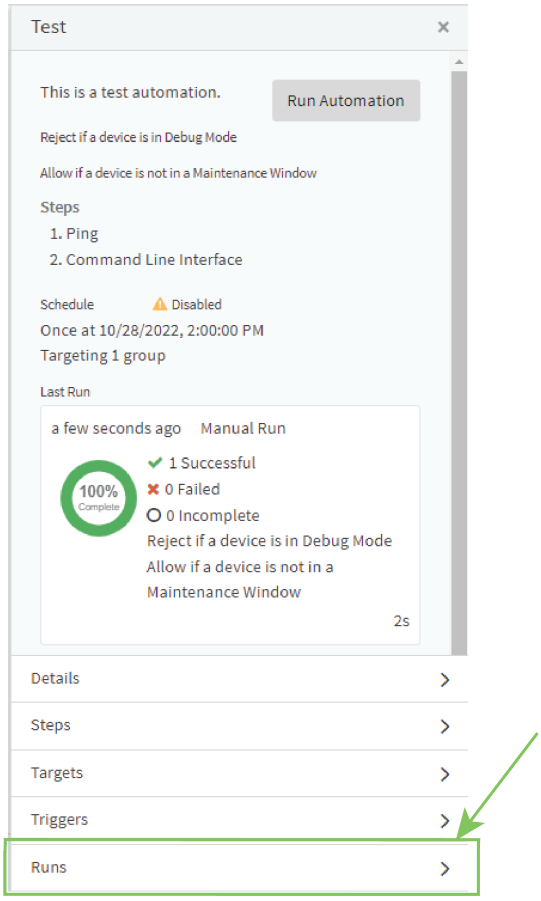
See Create a configuration for details.

Cancel an automation while it is running

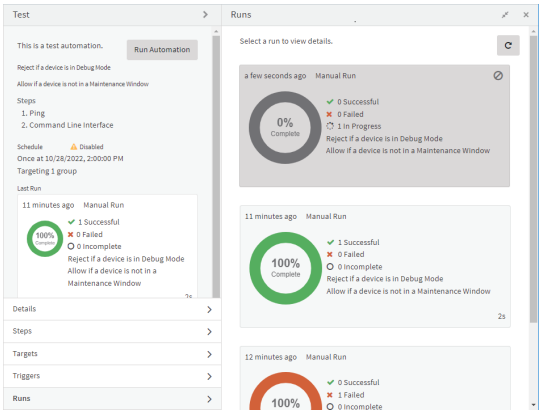
Automation runs can be canceled from the **Automation Runs** page:

1. From the main menu, click **Management** > **Automations**.
2. Select an automation.

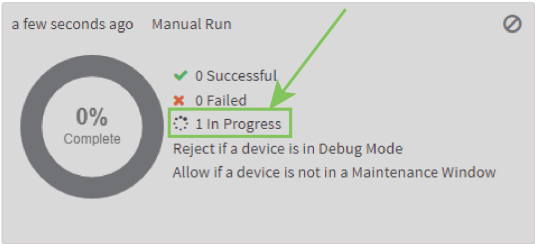
3. Click **Actions** > **Automation Details**.



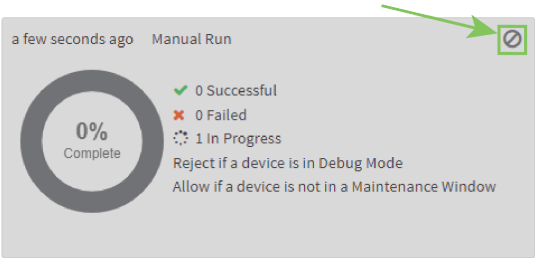
The **Runs** page is displayed.



4. Running automations are listed as **In Progress**.



5. Click to cancel.

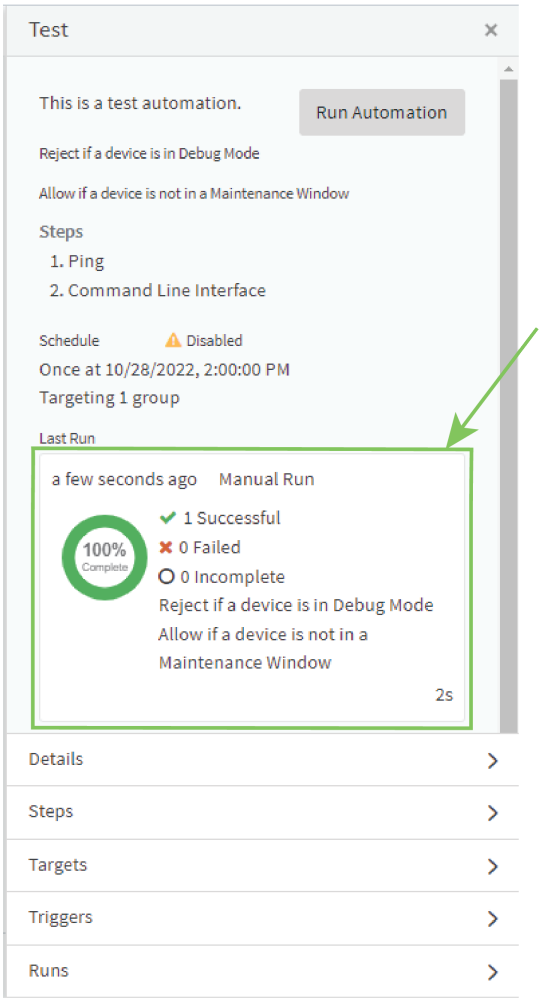


View the results of an automation run

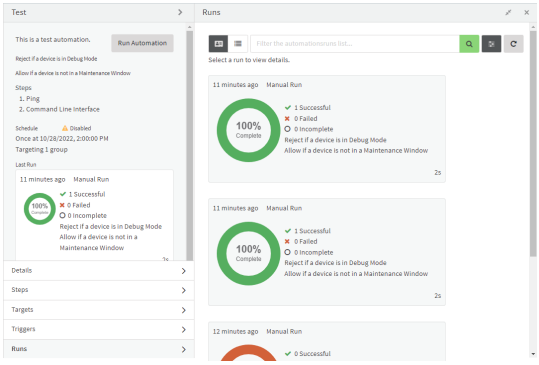
To view the results of an automation run:

1. From the main menu, click **Management** > **Automations**.
2. Select an automation.
3. Click **Actions** > **Automation Details**.

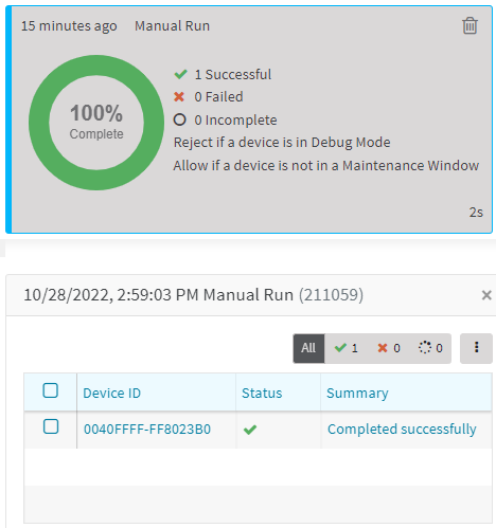
   The results of the most recent run are included with the details view.



4. For more details, and to view the results of previous runs, click the results card to open the **Automation Runs** page:



- Click a results card to display additional details about the run:



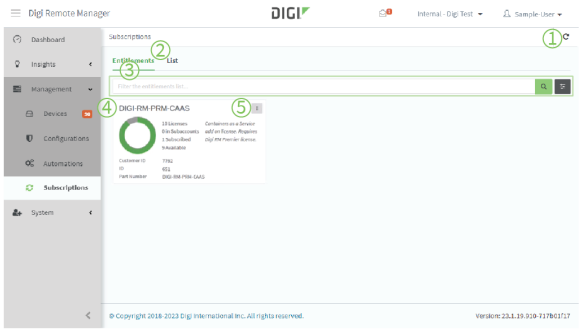
- Click to view the automations in list view. In list view, click the run **ID** to display additional details about the run.

Subscriptions

The **Subscriptions** page displays subscriptions for add-on subscriptions, and can be used to assign these subscriptions to devices and sub-accounts.

Note Subscriptions are enabled by Digi. Contact your Digi sales representative for information.

From the main menu, click **Management** > **Subscriptions**.



#	Component	Description
1	Refresh	Click to refresh the subscriptions list.
2	**Entitlements** or **List** view	▪ **Entitlements** displays subscriptions in card view.

#	Component	Description
		▪ **List** displays subscriptions in list view.
3	Subscriptions filter	▪ Click ▇ to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ▪ Click ▇ to filter the display. ▪ Click to clear the filter criteria.
4	Entitlement card	Provides the name, description, and further information about the entitlement. Depending on your user access level, you may be able to double-click to display sub-account entitlements.
5	Card menu	Depending on your user access level, you may have one or more of the following menu options: ▪ **View Subscriptions**: Opens a list view of the subscriptions. ▪ **Assign to a Device**: Allows you to an available entitlement to devices. ▪ **Use in Subaccount**: Allows you to assign available entitlements to a subaccount. ▪ **Edit**: Allows you to edit the entitlement.

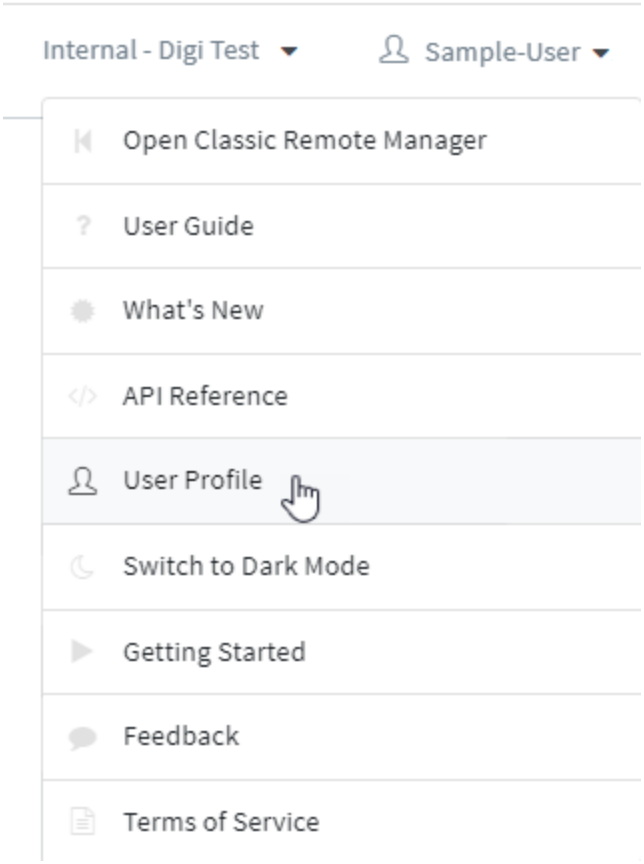
Users and accounts

This chapter contains the following topics:

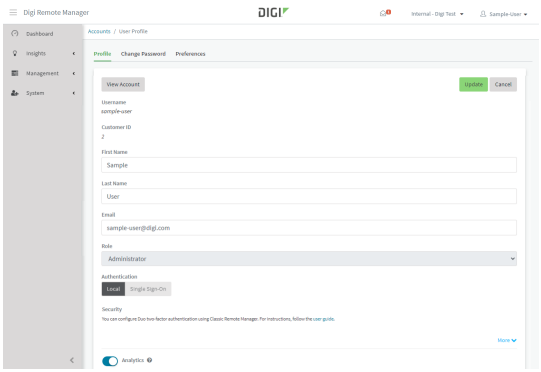
Your user profile

To view and edit your user profile:

1. Click your user name.
2. Click **User Profile**.

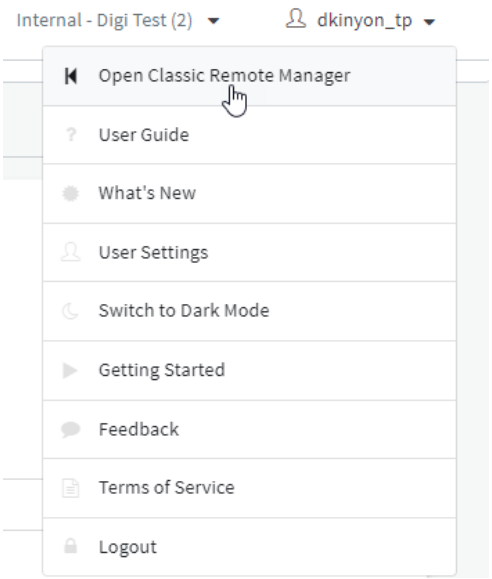


3. The User Profile page appears:



4. Edit your user information. Click More to access additional information.
5. For **Authentication**, you can configure users to use SAML Single Sign-On. See Enable Single Sign-On for a user for details.

6. For **Security**, you can configure users to use Duo two-factor authentication. To configure two-factor authentication, you must use the Classic Remote Manager user interface:
   a. Open the Classic Remote Manager user interface:
      i. Click your user name.
      ii. Select **Open Classic Remote Manager**.



   b. In the Classic Remote Manager interface, click the **Security** tab.
   c. Click the **Policies** tab.
   d. Click **Duo**.
   e. Provide the following information:
      - **Integration key**: Enter the Duo Security integration key.
      - **Secret key**: Enter the Duo Security secret key.
      - **API hostname**: Enter the API host name.
   f. Click **Save**.

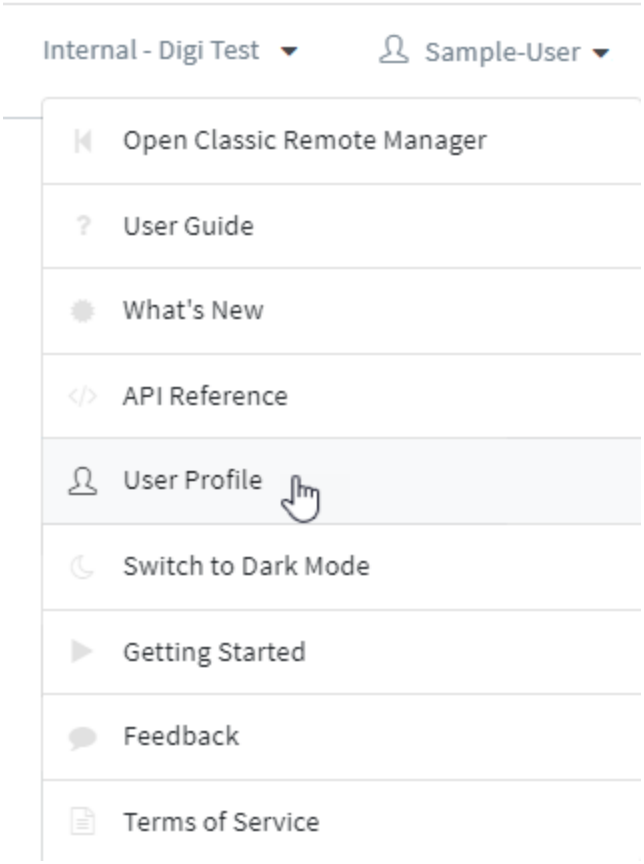
   See Configure Duo two-factor authentication in the *Classic Remote Manager User Guide* for more information.
7. Digi International Inc. uses analytics to better understand how users interact with Remote Manager. Toggle off **Analytics** to opt out.
8. Click **Update** to save changes.

Change your Remote Manager password

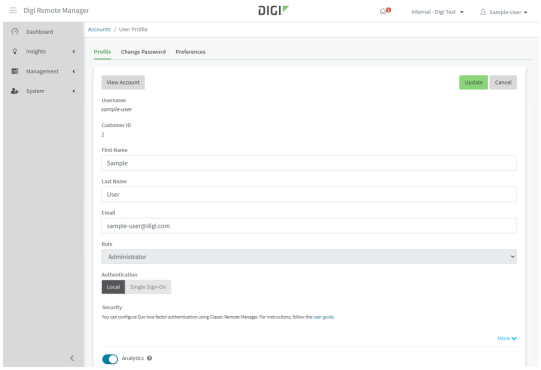
Note If SAML Single Sign-On is being used and your user has **Disabled Local Authentication** enabled, you cannot change the user password from within Digi Remote Manager.

To change your password:

1. Click your user name.
2. Click **User Profile**.



3. The User Profile page appears:



4. Click **Change password**.

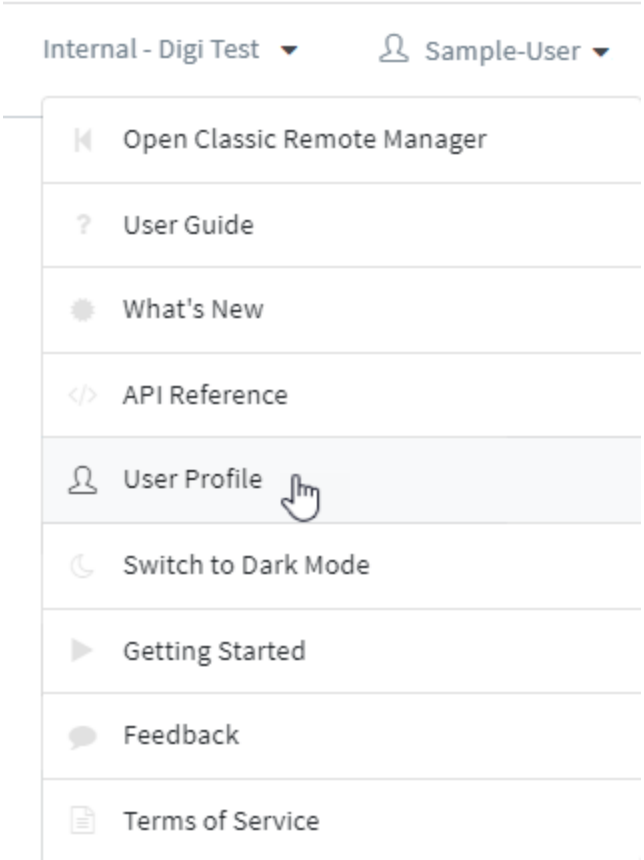
   The **Change Password** page appears.
5. For **Old Password**, type your current password.
6. For **Password**, type your new password.
7. **Confirm** your new password.

8. Click **Change Password** to save the changes.

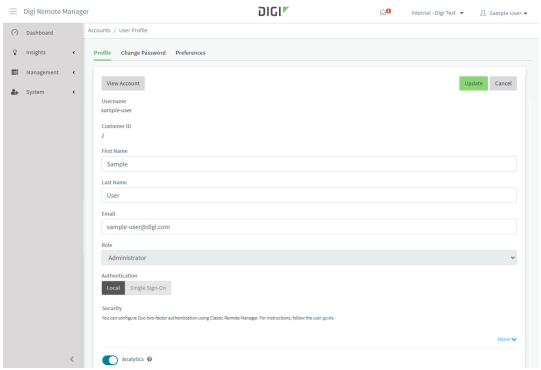
Set your user preferences

You can change the color mode for your Remote Manager interface to use daytime or nighttime mode, and you can set table preferences, set your preferred date and time format, and set other preferences.

1. Click your user name.
2. Click **User Profile**.



3. The User Profile page appears:



4. Click **Preferences**.

   The **Preferences** page appears.
5. Toggle **Color Theme Mode** to to use nighttime mode (dark background, lighter text) or to to use daytime mode (white background, darker text).
6. Select the amount of **Table Spacing** you prefer.
7. For Device ID, select either **Friendly** or **Full**:
   - **Friendly**: Displays Device IDs using the shorter format (for example: 12345678-90123456).
   - **Full**: Displays Device IDs using the longer format (for example: 00000000-00000000-12345678-90123456).
8. Toggle to enable **Lock Left Sidebar**.
9. Select your preferred **Date Format**.
10. Click More to set additional information.

User roles

All users are assigned a role within Digi Remote Manager, which dictates what they can see and do in the account.

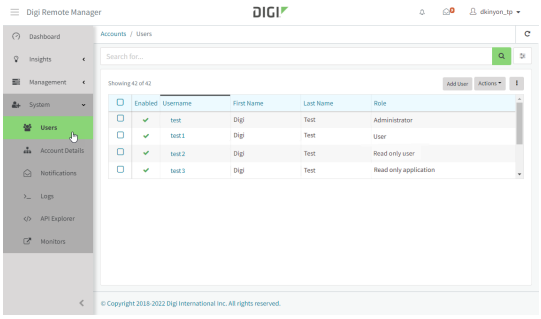
ROLE	PERMISSIONS
Administrator	User can add new users, change user passwords, set permissions, and enable single sign on.
User	User has full read and write permissions to the account, including adding or removing devices, and editing configurations.
Read only user	User has full read permissions to the account.
Application	User has full read and write permissions to the account via the Rest API. User has no read permission to the account via the web application.
Read only application	User has full read permissions to the account via the Rest API. User has no read permissions to the account via the web application.
Custom read only user	User has full read permissions to the account, with enhanced write permissions. ▪ Option to grant Reboot permission.
Custom user	User has full read permissions to the account, with limited write access. ▪ Option to limit Add Device, Remove Device, Edit Configs permissions.

Add a user

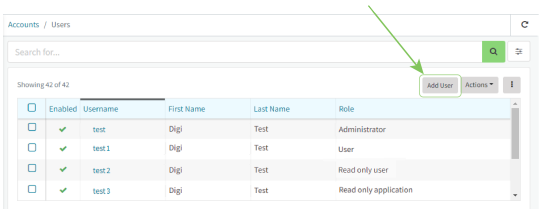
If you are an administrator, you can add, edit, or remove users from your account.

To add a user to your Digi Remote Manager account:

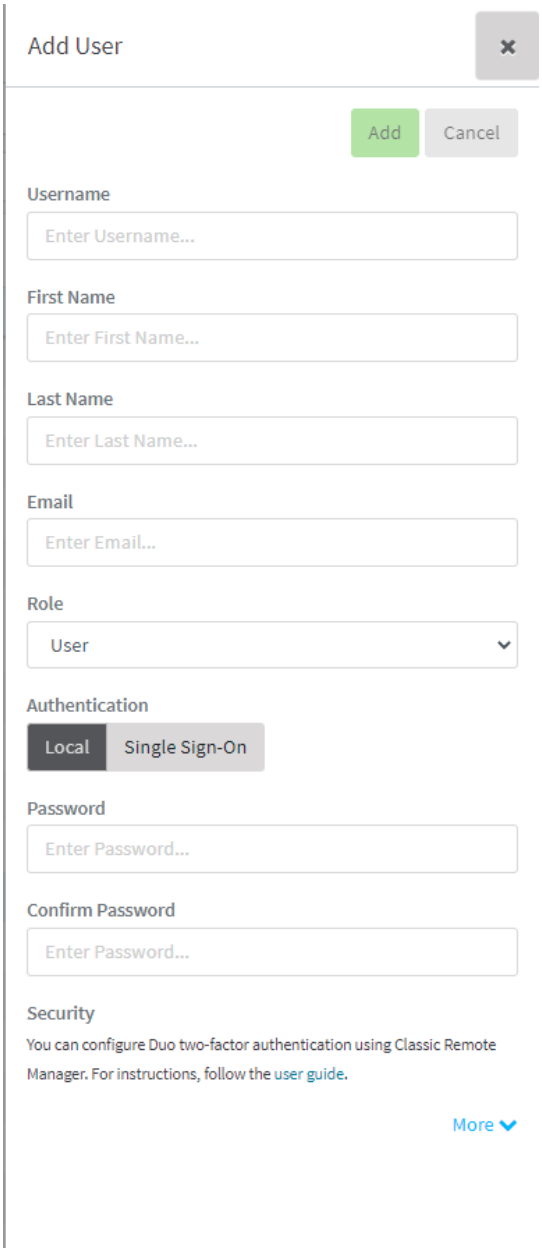
1. From the main menu, click **System** > **Users**.



2. Click **Add user**.



3. The **Add User** form displays:



Complete the form:

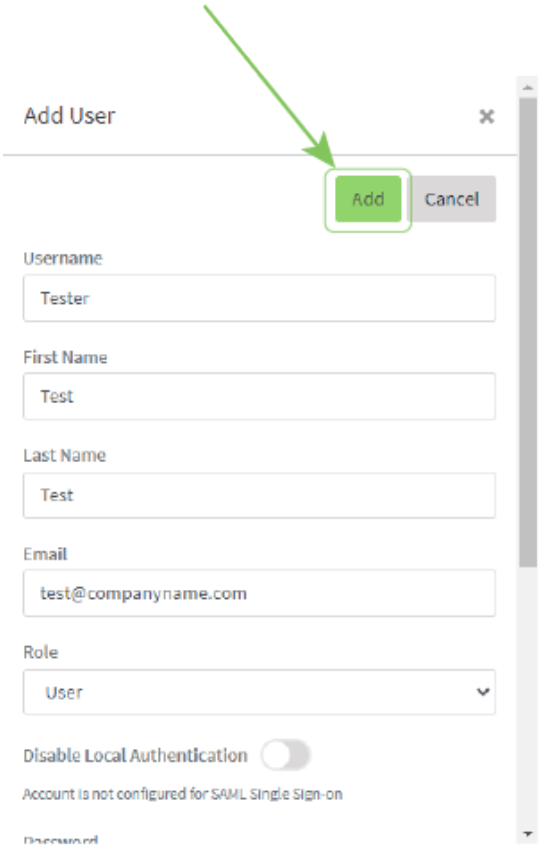
Item	Description
Username (required)	Unique username for the user.
First Name (required)	First name of the user.

Item	Description
Last Name (required)	Last name of the user.
Email (required)	Email address of the user.
Role	Role of the user. See User roles.
Authentication	If the user's customer account has been enabled for SAML Single Sign-On, click **Single Sign-On** to enable single sign-on for this user. See Configure Digi Remote Manager to use SAML Single Sign-On for more information.
Password (required for local authentication)	Password for the user name. If the user's customer account has been enabled for SAML Single Sign-On and local authentication has been disabled, this option is not available.
Confirm Password (required for local authentication)	Confirm the password for the user name.
Security	You can configure Duo two-factor authentication, use Classic Remote Manager. See for information about opening the Classic Remote Manager. See Configure Duo two-factor authentication in the Classic Remote Manager User Guide for information about configuring two factor authentication.

Click **More** to complete additional user information:

Item	Description
Job Title	The job title of the user.
Phone Number	Telephone number for the user.
Address	Street address of the user.
City	City of the user.
State	State of the user address.
Postal code	Postal code for the user address.
Country	Country of the user.

4. Click **Add**.



Edit a user

If you are an administrator, you can add, edit, or remove users from your account.

To edit a user in your Digi Remote Manager account:

1. From the main menu, click **System** > **Users**.
2. Select a user.
3. Select **Actions > Edit**.
4. Edit the user information as needed:

Item	Description
Username (required)	Unique username for the user.
First Name (required)	First name of the user.
Last Name (required)	Last name of the user.
Email (required)	Email address of the user.

Item	Description
Role	Role of the user. See User roles.
Authentication	If the user's customer account has been enabled for SAML Single Sign-On, click **Single Sign-On** to enable single sign-on for this user. See Configure Digi Remote Manager to use SAML Single Sign-On for more information.
Password (required for local authentication)	Password for the user name. If the user's customer account has been enabled for SAML Single Sign-On and local authentication has been disabled, this option is not available.
Confirm Password (required for local authentication)	Confirm the password for the user name.
Security	You can configure Duo two-factor authentication, use Classic Remote Manager. See for information about opening the Classic Remote Manager. See Configure Duo two-factor authentication in the Classic Remote Manager User Guide for information about configuring two factor authentication.

Click **More** to complete additional user information:

Item	Description
Job Title	The job title of the user.
Phone Number	Telephone number for the user.
Address	Street address of the user.
City	City of the user.
State	State of the user address.
Postal code	Postal code for the user address.
Country	Country of the user.

5. Click **Update User**.

Change password

If you are an administrator, you can add, edit, or remove users from your account. You can also reset the password for a user.

Note If SAML Single Sign-On is being used and the user has **Disabled Local Authentication** enabled, you cannot change the user password from within Digi Remote Manager.

To change the password for a user in your Digi Remote Manager account"

1. From the main menu, click **System** > **Users**.
2. Select a user.
3. Select **Action > Change password**.
4. Enter the new password in the **Password** and **Confirm Password** fields.
5. Click **Change Password**.

Remove a user

If you are an administrator, you can add, edit, or remove users from your account.

To remove a user from your Digi Remote Manager account:

1. From the main menu, click **System** > **Users**.
2. Select the user.
3. Select **Actions** > **Remove**.
4. Click **Remove**.

Configure Digi Remote Manager to use SAML Single Sign-On

SAML (Security Assertion Markup Language) is an authentication standard that allows for Digi Remote Manager users to be authenticated by an Identity Provider (for example, Okta). Digi Remote Manager can be configured to provide user identification through a SAML Identity Provider, rather than local user authentication.

Local Digi Remote Manager users

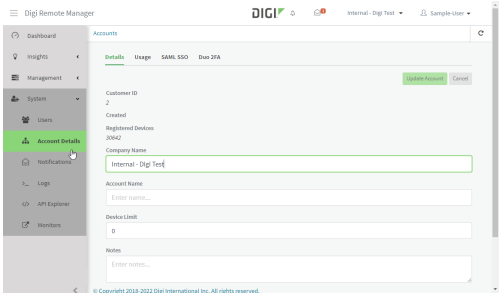
SAML Single Sign-On is configured at the account level, while local authentication is enabled or disabled for each individual user. See Enable Single Sign-On for a user for information about how to enable SAML Single Sign-On for a user.

To access Digi Remote Manager, users that are configured on your Identity Provider must have a corresponding local Remote Manager user. The username passed from the Identity provider must match the local Remote Manager username. See Add a user for information about creating local Remote Manager users.

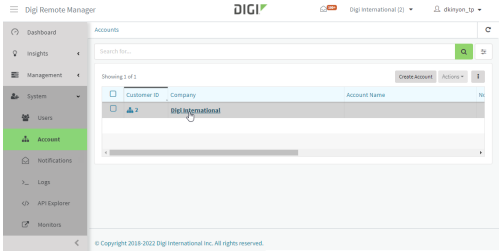
Note If your Identity Provider uses case sensitivity when authenticating usernames, you must make sure that the user's local Remote Manager username, and the username as configured on the Identity Provider, have identical case.

To configure Digi Remote Manager to use SAML Single Sign-On:

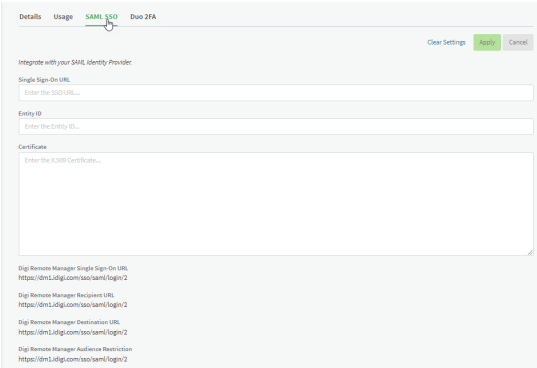
1. Click **Account** to expand the **Account** menu.
   - If there are no sub-accounts configured for the account, click **Account Details**.



   - If there are sub accounts configured, click **Accounts** and click the appropriate account.



2. Click **SAML SSO**.



   At the bottom of the SAML Single Sign-On page are several URLs that may be necessary when configuring your Identity Provider to integrate with Digi Remote Manager.

   For example, when configuring an SAML Integration on an Okta tenant for Digi Remote Manager, you will need the following Digi Remote Manager URLs:

   - **Digi Remote Manager Single Sign-On URL**
   - **Digi Remote Manager Audience Restriction** (in Okta, this is the **Audience URI**)

3. For **Single Sign-On URL**, type or paste the Single Sign-On URL provided by the Identity Provider.

   For example, with Okta, this is the **Identity Provider Single Sign-ON URL**. Other providers might refer to this as the **Assertion Consumer Service (ACS) URL**.

4. For **Entity ID**, type or paste the Identity Provider's Entity ID.

   For example, with Okta, this is the **Identity Provider Issuer**.

5. For **Certificate**, paste the X.509 certificate provided by your Identity Provider.
6. Click **Apply**.

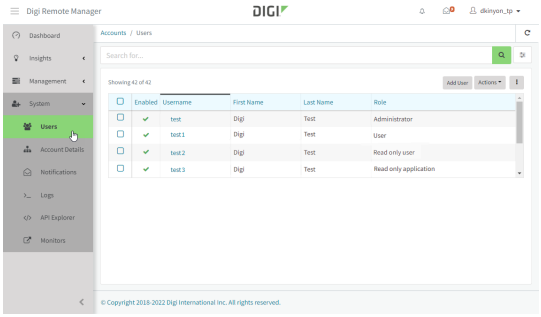
Enable Single Sign-On for a user

When SAML Single Sign-On has been configured for a Digi Remote Manager account, single sign-on functionality can been enabled for individual users. Users with single sign-on authentication enabled will be redirected to the single sign-on URL for login and password information. Local authentication will be disabled for these users.

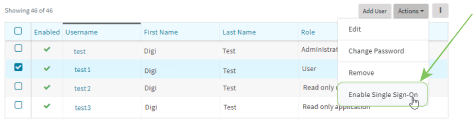
WARNING! To prevent the account administrator from being locked out of Digi Remote Manager, do not enable single sign-on functionality for the account administrator.

To disable local authentication for individual users:

1. From the main menu, click **System** > **Users**.



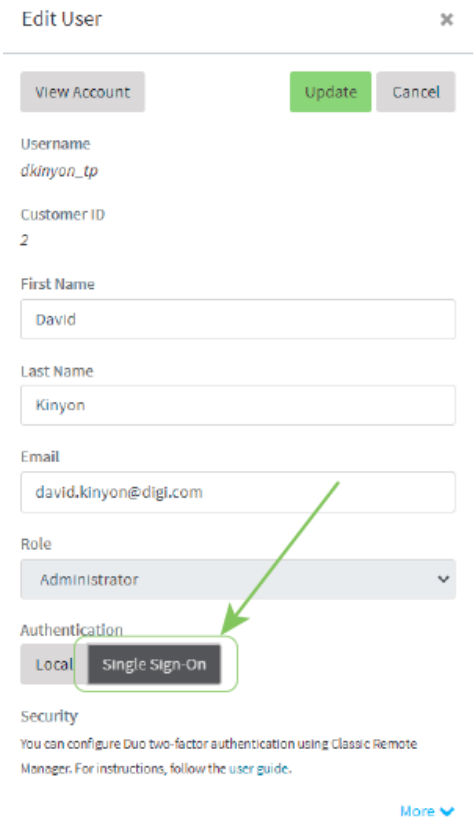
2. Either:
   - To use the **Actions** menu:
     a. Select the appropriate user.
     b. Click **Actions** > **Enable Single Sign-On**.



   - To use the **Edit User** pane:

a. Click the appropriate username or select the user and click **Actions** > **Edit**.

b. In the **Edit User** pane, click **Single Sign-On**.



c. Click **Update**.

Configure Digi Remote Manager to use Duo two-factor authentication

Digi Remote Manager integrates with Duo security to provide two-factor authentication for account users. When this feature is enabled, a user that logs in to Digi Remote Manager from one device must also authenticate his or her log in from a second device, such as a mobile phone.

Once Digi Remote Manager is configured to use Duo security, all users except those with application or read-only application roles must use two-factor authentication to log in to Digi Remote Manager. Users with application or read-only application roles are not managed by the Duo Security application.

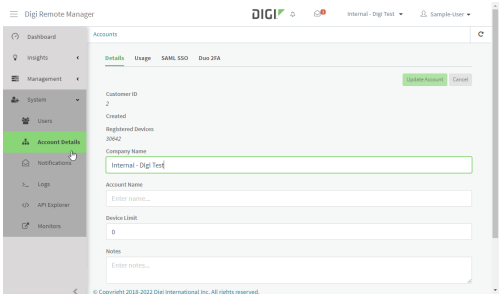
To use Duo two-factor authentication, you must separately have your own Duo account. See the Duo web site for details about setting up a Duo account. To configure Duo support in Digi Remote Manager, you just have:

- Your Duo integration key
- Your Duo secret key
- The API hostname.

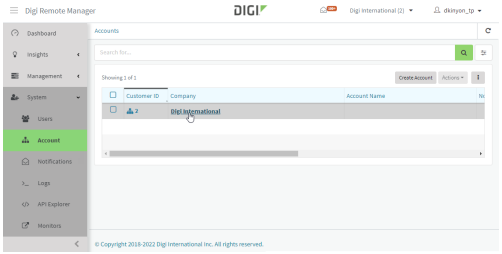
Note This configuration applies to the entire account. Within the Duo application, you can configure a Global Policy to **Allow access without 2FA**, so that users who are unknown to Duo can continue to log into Digi Remote Manager. We recommend that you use this option when initially configuring Digi Remote Manager to use Duo authentication, so that you don't accidentally lock yourself out of the account.

To configure Digi Remote Manager to use Duo two-factor authentication:

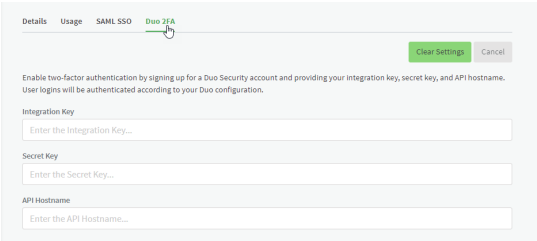
1. Click **Account** to expand the **Account** menu.
   - If there are no sub-accounts configured for the account, click **Account Details**.



   - If there are sub accounts configured, click **Accounts** and click the appropriate account.



2. Click **Duo 2FA**.

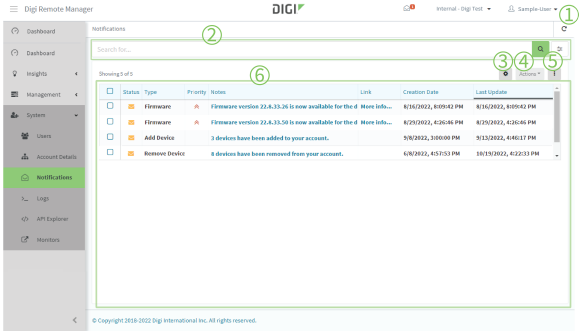


3. For **Integration Key**, type the Duo security integration key.
4. For **Secret Key**, type the Duo Security secret key.
5. For **API hostname**, type the API hostname.
6. Click **Apply**.

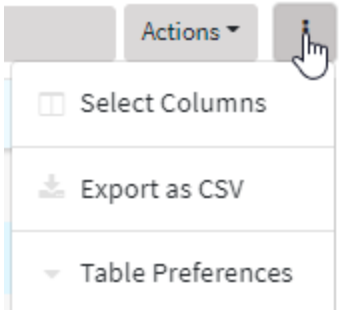
Notifications

The **Notifications** page displays notifications from the system.

From the main menu, click **Management System** > **Notifications**



#	Component	Description
1	Refresh	Click to refresh the notifications list.
2	Notifications filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ■ Click to filter the display. ■ Click to clear the filter criteria.
3	Notifications Preferences	Opens the **Notifications Preferences** dialog. Click to enable **Email daily summary of unread notifications**.
4	**Actions** menu	
5	Customize display menu	Click to customize the display.

#	Component	Description
		 ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click **Export as CSV** to export a list of the devices in CSV format. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly**

#	Component	Description
		(shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
6	Activities list	▪ Click to select an activity. ▪ Click a **Notes** message to view further information about the notification. Notifications list details: **Column** / **Description**: **Status** — Priority of the notification: Read, Unread **Priority** — Priority of the notification: Normal, Critical **Notes** — A message describing the notification. Click the message for further information. **Link** — If available, provides a link to more information. **Creation Date** — Date and time the notification was created. **Last Update** — Date and time the notification was last updated.

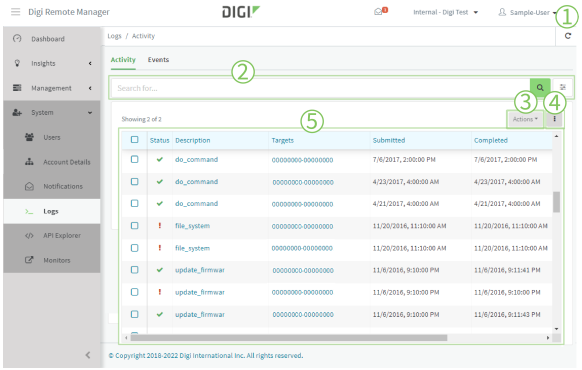
Logs

From the main menu, click **System** > **Logs**.

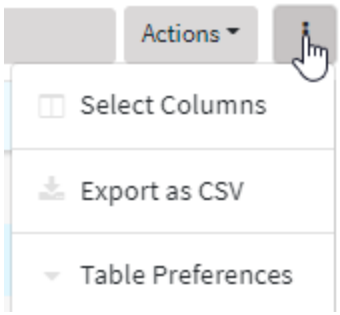
The **Log** page provides the following information:

Activity

The **Activity** page lists all jobs for your Digi Remote Manager account. For example, when you initiate a firmware update for one or more devices, the activity is listed in the **Activity** page.



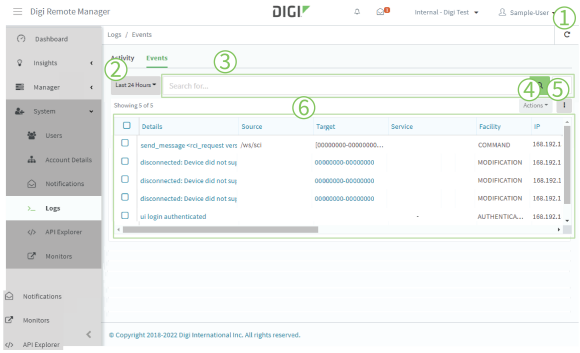
#	Component	Description
1	Refresh	Click to refresh the activities list.
2	Activities filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ■ Click to filter the display. ■ Click to clear the filter criteria.
3	**Actions** menu	■ **Activity Details**: Display further information about the selected activity. ■ **Cancel** Cancel the selected

#	Component	Description
		activity.
4	Customize display menu	Click to customize the display.  ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click **Export as CSV** to export a list of the devices in CSV format. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to

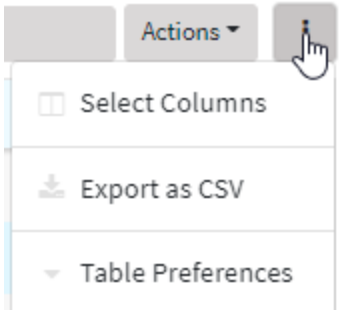
<table>
<tr><th>#</th><th>Component</th><th>Description</th></tr>
<tr><td></td><td></td><td>display the Device ID, either Friendly (shorter) or Full. (This table preference is not applicable for the Configurations table.)</td></tr>
<tr><td>5</td><td>Activities list</td><td>
Click to select an activity.
Click an ID to view further information about the activity.
Activity list display:
<table>
<tr><th>Column</th><th>Description</th></tr>
<tr><td>Status</td><td>Status of the job:
Success
Pending
! Failed</td></tr>
<tr><td>Description</td><td>Description of the job.</td></tr>
<tr><td>Targets</td><td>Device targets for the job.</td></tr>
<tr><td>Submitted</td><td>Date and time when the job was submitted.</td></tr>
<tr><td>Completed</td><td>Date and time the job completed.</td></tr>
<tr><td>Username</td><td>The account user who submitted the job.</td></tr>
<tr><td>ID</td><td>Unique identifier assigned to the job.</td></tr>
</table>
</td></tr>
</table>

Events

The **Events** page provides an audit record and information about activities that have taken place on the Remote Manager system.



#	Component	Description
1	Refresh	Click to refresh the events list.
2	Date and time selector	Select a relative time, such as within the **Last Hour**, **Last 30 Days**, or **Year to Date**. Or, enter a **Start** and **End** date.
3	Events filter	▪ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ▪ Click to filter the display. ▪ Click to clear the filter criteria.
4	**Actions** menu	When an event is selected, click **Actions** > **Event Details** to display event details.
5	Customize display menu	Click to customize the display.

#	Component	Description
		 ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click **Export as CSV** to export a list of the devices in CSV format. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing. • Click Device ID to determine how to display the Device ID, either **Friendly**

#	Component	Description
		(shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
6	Events list	▪ Click to select a events. ▪ Click a event's **Details** to display event details. See Events for further information.

Events list

The following table lists the default columns displayed in the Events list:

Column	Description
Details	A message describing the event. Click to display event details
Source	Shows the event task.
Target	Shows the event target.
Service	The service associated with the event, if any.
Facility	The Remote Manager facility that the operation is a part of. For example: AUTHENTICATION, COMMAND
IP	The IP address associated with the event.
Protocol	The protocol used by the event, for example, HTTP, EDP, KAFKA.
User	The user that initiated the event.
Start Time	The time that the event started.
End Time	The time that the event ended.
Success	Success status of the event: Success ! Failed
Request Size	The size of the request payload.
Response Size	The size of the response payload.
Jobs	The list of job IDs associated with the event.

Event details

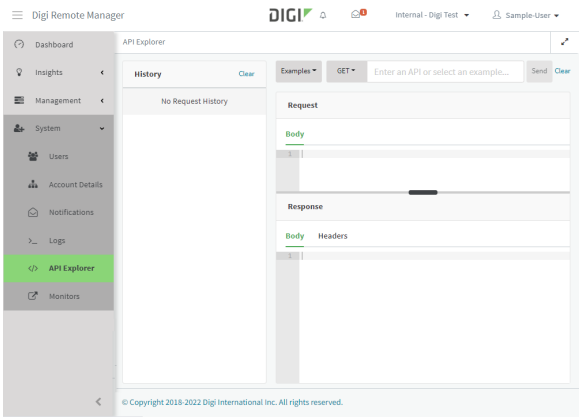
Additional information provided in the Events details pane:

Column	Description
ID	The ID of the event.
Duration	The number of milliseconds that the event took to complete.
Customer ID	The account in which the event occurred.
Modification Type	The type of change that occured: For example: CREATE, UPDATE, DELETE.
Count	The count associated with the event, if any.
Target Type	The type of object that was the target of the event. For example: DEVICE.
Sequence No	The sequence number associated with the event.

API explorer

Use the **API explorer** to request an API web service on behalf of your Remote Manager logon user account.

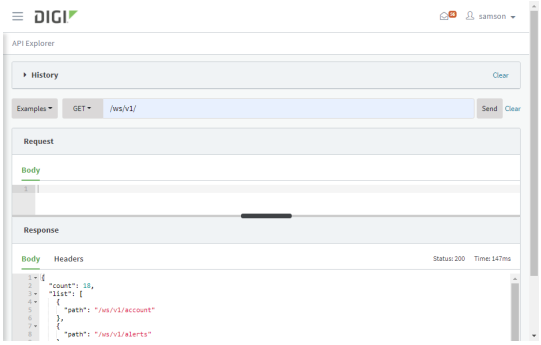
From the main menu, click **System** > **API Explorer**.



Get a list of available v1 APIs

To retrieve a list of all the v1 APIs available for your logged-in account:

1. From the main menu, click **System** > **API Explorer**.
2. Enter **/ws/v1/** and click **Send**.



A list of available v1 APIs is returned.

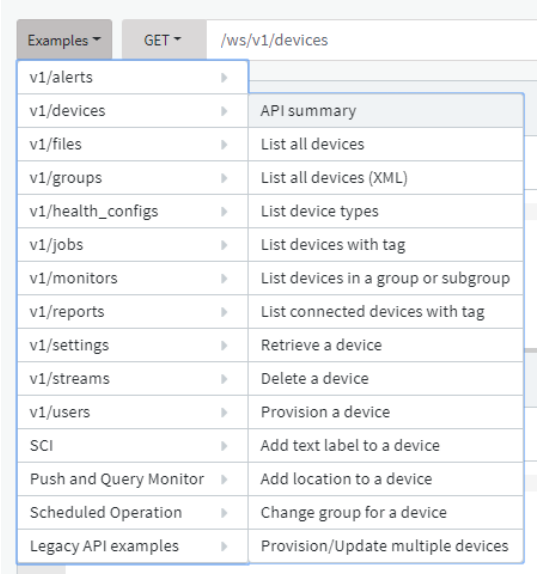
Get an API summary

Digi Remote Manager web services provide a summary of all the allowable forms for a web service.

To retrieve an API summary, issue a **GET** request on an API without any parameters or fields. The **Examples** drop-down offers a summary menu item for each API.

For example, to get a summary of the v1/devices APIs:

1. From the main menu, click **System** > **API Explorer**.
2. Click **Examples > v1/devices > API summary**.



3. Click **Send**. A summary of the v1/devices API is returned.

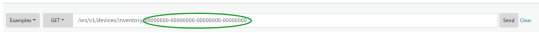
Copy and paste a device ID

You can copy and paste a device ID from the Devices display to use as a target in an API request.

To do so:

1. From the main menu, click **System** > **API Explorer**.
2. Locate the device you want to use as a target and click to copy the device ID to the clipboard.

3. From the menu, click **API Explorer**.
4. Click **Examples** and select the API you want to run.
   For example, to get information on a device, select **Examples > v1/devices > Retrieve a device**.
5. Paste the device ID in the clipboard into the API call:



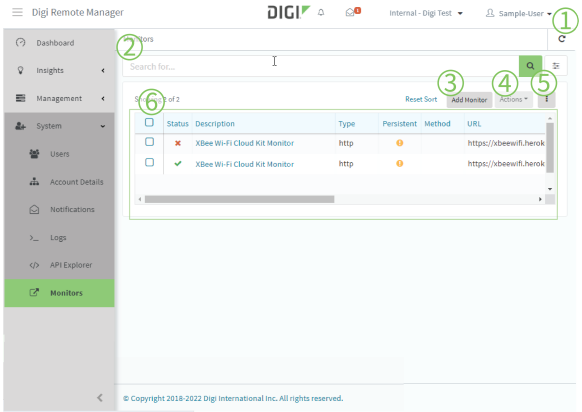
6. Click **Send**.

Get help

To get help creating scripts using Remote Manager web services, see the Digi Remote Manager Web Services Reference.

Monitors

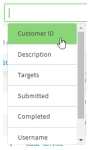
From the main menu, click **System** > **Monitors**.



The **Monitors** page lists all of monitors configured for your account.

The monitor feature is used to monitor Remote Manager activity and push notifications to a client application. For details about monitors, see:

- Tutorial: Experimenting with Monitors
- Tutorial: Monitors with Templated Payloads
- v1/monitors API

#	Component	Description
1	Refresh	Click to refresh the monitors list.
2	Monitors filter	■ Click to toggle between basic (keyword) search and advanced filtering. • Basic search: Type a word to search for. • Advanced filtering: click in the filter bar to select a filtering category:  ■ Click to filter the display. ■ Click to clear the filter criteria.
3	**Add Monitor**	For details about adding monitors, see the API Reference.
4	**Actions** menu	Select a monitor and click **Actions** to: ■ View and edit **Monitor Details**. ■ View **Recent Events**. ■ To restart the monitor, click **Force Restart**. ■ **Remove** the monitor.
5	Customize display menu	Click to customize the display. ■ Click **Select Columns** to open a list of columns. • Click to select the columns that will be displayed in the device list. • Click and select whether to send the column to the top or bottom of the list. • Click to reorder the listing by dragging and dropping a column. • Click **Use Defaults** to return to the default display. • Click **Close** when finished. ■ Click Table Preferences to set your table view preferences: • Click **Table Spacing** to select **Compact**, **Comfy**, or **Roomy** spacing.

#	Component	Description
		• Click Device ID to determine how to display the Device ID, either **Friendly** (shorter) or **Full**. (This table preference is not applicable for the Configurations table.)
6	Activities list	▪ Click to select an activity. ▪ Click **Description** to view further information about the activity. Activity list display: **Column** / **Description** **Status** — Status of the monitor: Success, Pending, ! Failed **Description** — Description of the monitor. **Type** — One of: ▪ Polling: Stores information in Remote Manager, which can be retrieved using the v1/monitors/history API. ▪ HTTP: Used to send push events to a client via HTTP PUT or POST. ▪ TCP: Used when the client application connects with TCP to fetch monitor events. **Persistent** — The monitor is persistent. The monitor is not persistent. **Method** — The method used (HTTP type monitors only). Either: ▪ POST ▪ PUT

#	Component	Description
		<table><tr><th>Column</th><th>Description</th></tr><tr><td>**URL**</td><td>HTTP monitors only. URL of the customer web server.</td></tr><tr><td>**Topics**</td><td>See the API Reference.</td></tr><tr><td>**Last Contact**</td><td>The date and time that Remote Manager was last connected to the client application.</td></tr><tr><td>**Last Sent**</td><td>The date and time that the last message was pushed to the client application.</td></tr></table>

Previous release notes

What's new in January 2024

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There were no security related changes.

Enhancements

For January 03, 2024

- Intersection of Automations Trigger
- Add a firmware history tab to device details
- A default account filter or retain between login sessions
- Add disclaimer to firmware update action & configuration templates for EX15s running 23.9 or older firmware
- Add warning to DAL PR products to notify of step-update to standard DAL firmware

Patches

For January 12, 2024

- Connection Duration should be 0 if there is no connect time.
- Configuration template not progressing user through creation process.
- Automation tab would not save for a configuration.

What's New in November 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Enhancements

Update for 11/27/2023

- Fixed an issue where device metric graphs did not display data.
- Fixed an issue where the **Alerts** list could not be exported.
- Added a **Scan Now** button the configurations aside.
- Fixed an issue where stream history charts displayed no data when scoped to a subaccount.
- Made the error messages for automation runs more readable.
- Fixed issue where a user is randomly logged out.
- Added a search bar to the groups aside.
- Added a toggle to hide pre-production firmware when updating a device.
- Added a device list and device details page action that can scan configurations for individual devices.

- Updated the navigation and header design.
- Added a message in the device settings tab if the device is being managed by a configuration.

Update for 11/06/2023

- Fixed an issue where the device connection history chart rendered incorrectly.
- Fixed an issue where stream history charts displayed no data when scoped to a sub account.
- Fixed issue that was preventing customers from copying configurations with uploaded files.
- Fixed corruption container image upload.

What's New in October 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Enhancements

- Updated CryptoJS (deprecated) to CryptoES.
- Fixed an issue where refreshing the reports page never completed.
- Added device connection status to the automations and api explorer target menus.
- Fixed an issue where IPSec data did not display on the device's Summary Dashboard.
- Fixed an issue where a device's configuration scan history was displayed out of order.
- Added error message to cell modem update screen when no modem was found in a device.
- Add UI for Configuration Audit logs.
- Fixed an issue where the left sidebar was stuck open on mobile.
- Updated 'deprecated' column on firmware tables to say 'supported'.
- Fixed messages and submit behavior on device details page.
- Improved the Add User aside so errors on submit does not cause the form to close.
- Updated the Summary Dashboard to display a signal quality chart for a second modem if one exists.
  - Updated the signal quality chart to display data for a second SIM if one exists.
- Added a "Reconnect" action to the Monitors page.
- Made the colors consistent in the device Summary Dashboard signal quality charts.

What's new in September 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 09/28/2023

Enhancements

- Added the Security Policies tab in account details for controlling IP-allow list rules.
- Increased the max length for data streams "unit" field.
- Added csv export function to the Activities table.
- Fixed an issue where new groups could not contain an underscore.
- Fixed an issue where the alert details page did not correctly link back to a device.
- Added a warning when creating a configuration that will not remediate devices.
- Fixed an issue where the device details page occasionally crashed after pinging the device.
- Added thousands separator to numbers in graph tooltips.
- Fixed an issue where the devices map would not update when the account filter changed.
- Added a "show password" toggle when logging in or changing a user's password.
- Improved removing multiple files from a device.
- The job ID column in the Activities table is now easily copied.
- Added "Move to Subaccount" action to the device list.

Update for 09/05/2023

Enhancements

- Represent payload better in automation data service request steps.
- Settings does not show errors.
- Improved experience creating scheduled reports.
- Implement SBOM generation for front-end code using Snyk.
- Add link to support in UI.

Resolved issues

- Flash message does not appear on the alerts list page.
- Ascending search doesn't appear to work for Automation ID in Automations list.
- Scan Now action for configuration remains disabled after enabling configuration until you re-select.
- Admin User using Edit to change User to Custom-User Role - unable to Apply change.
- Notifications table should be sorted with most recent update first.
- Clicking on 'Last Update' table header on notifications doesn't correctly sort.
- Last Modified date on a TX64 device files table is incorrect.
- TX64 Device/Settings/Status options crash web page.
- Please review the update button for changing account permissions for a potential bug.

What's new in August 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 8/14/2023

Enhancements

- Modem firmware is now displayed in order.

Resolved issues

- Fixed an issue where attempting to view the automation history of a device resulted in a crash.
- Fixed an issue where newly created configurations would not show as enabled.
- Fixed an issue where data points were sometimes connected out of order.
- Fixed an issue where clearing filters did not work on the some tables.
- Fixed an issue where the account usage tab was formatted incorrectly.

What's new in May 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 5/25/2023

Enhancements

- Enhanced password complexity requirements.

  By default, Remote Manager passwords must have:

  - A minimum of 12 characters.
  - At least one uppercase and one lowercase letter.
  - At least one digit.
  - At least one special character (punctuation mark or symbol).

  Additionally, passwords cannot be common English words and cannot be included in the National Institute of Standards and Technology (NIST) list of common passwords.

  Customers and system administrators can modify the password complexity requirements to meet their own security requirements through **System** > **Accounts**.
- In the API Explorer, RCI API examples were moved to the **SCI** section, from the **Legacy API examples** section.

Resolved issues

- Fixed an issue where the **Alerts** page would sometimes incorrectly display an unsaved changes warning.
- Fixed an issue where some table columns did not resize correctly.

- Fixed an issue where the alerts list did not display the count correctly.
- Fixed an issue where files did not sort by size correctly.
- Pressing the Enter key in fields for automations steps no longer applies the changes and advances to the next automation step.
- Fixed basic search functionality for scheduled reports list.
- Fixed an issue where deleting a file on a device showed an error message.
- Fixed an issue where searching the device status for a value caused the status name to no longer be displayed.
- Fixed an issue where configurations could not be copied to a sub-account.
- Fixed an issue where attempting to update a device's geolocation resulted in an error.
- Fixed an issue where the device console did not work when scoped to a subaccount.

Update for 5/02/2023

Enhancements

- **Cellular Modem ID** changed to Cellular Modem IMEI/ESN.
- Added a column for Customer ID to scheduled reports.
- Added the ability to create filters for scheduled reports.
- For Configuration templates, renamed **Overrides** to **Site Specific Settings**.
- The Device Availability report summary now shows the number of devices that were connected for each hour, which tracks the number of devices which were connected for at least some part of the hour.
- Removed the **Unterminated** connection status from the device **Summary Dashboard** graph.

Resolved issues

- Removed **Use default settings** from **Configurations** because of usability concerns.
- Fixed an issue where accepting the terms of service sometimes returned an error.
- Fixed an issue where the application would crash in certain circumstances after creating a new configuration and enabling it.
- Fixed an issue where the **Configurations Status** page was limited to viewing 100 devices.
- Fixed an issue where links inside an error message did not work.
- Fixed an issue where settings are sometimes unavailable in Configuration templates.
- Fixed an issue where, after deleting a container from a Configuration template, you could not continue.
- Fixed an issue where a container with spaces in its name could not be included in a Configuration template.

What's new in April 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 4/13/2023

Enhancements

- Added a **Run Report** action to the **Actions** menu on the **Scheduled Reports** page.
- Added a list view option for the **Automation Runs** page.
- Added new device properties to the **Alerts** summary and status APIs: **Name**, **Group**, **IP**, **Public IP**.
- Added the ability to upload one configuration overrides file for multiple configurations.
- Added a tooltip to disabled device actions to describe why the action is disabled.
- When an automation is triggered for a device that is already processing an automation, the newly triggered automation now goes into a pending state instead of failing.
- Added cellular phone numbers to the **Devices** list.

Resolved issues

- Improved the default sorting of the **Alerts** list.
- Fixed an issue where enabled alerts showed as disabled in the **Alerts** list.
- Fixed an issue where alerts could not be filtered by ID.
- **Automations Detail** view no longer closes due to the page performing an automated refresh.
- Fixed an issue where a scheduled report could not be renamed.
- Fixed an issue where the device availability report did not always reflect the correct amount of time that devices were connected.
- Fixed an issue with the company name being displayed from historical data.
- Fixed a timing issue when a **Configuration** was started on a newly-added device and the **Configuration** would sometimes fail with a "no device found" error.

What's new in March 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 3/28/2023

Enhancements

- Added new columns to the device list: **Cellular Modem 2 ID**, **ICCID**, **ICCID 2**, **APN**, **APN2**.
- Added the scheduling of reports to the user interface.
- Added support to retain console history when switching tabs, and the ability to pop out the console into a new tab from within the console interface.
- Added a filter bar to the **Configuration Status History**.
- Added a filter bar to the **Automation Run History**.
- Moved the RCI examples in the **API Explorer** to the legacy section.

Resolved issues

- Fixed an issue where the device actions menu was sometimes hidden by the page header.
- Fixed an issue where disabled users incorrectly displayed as enabled in the users list.

Update for 3/9/2023

Enhancements

- Added Duo 2-factor configuration to the Account page.
- Simplified the presentation of data in the **Details** column in the **Alerts** list view.
- Added support in the monitors data schema for the json, replace and slice helpers.

Resolved issues

- Opening the history table of a data stream with a **Type** of **JSON** that contains invalid JSON will no longer crash the UI.
- Fixed an issue where the main menu would open and close regardless of the setting for the **Lock Left Sidebar** preference.
- Fixed an issue where the health chart displayed too large on smaller screen sizes.
- When searching for devices, searches with "type contains unknown" or "type = unknown" now correctly return all devices that have their type listed as unknown. "type = empty" will display all devices with an empty type field.
- Provided firmware download capability for devices running Digi Accelerated Linux (DAL) firmware version 22.5 or earlier.
- writeOnly attributes are no longer returned as part of the GET /ws/v1/settings/inventory API method.
- Fixed a problem in the monitor schema language where a bad timestamp on DataPoint data would cause an error processing the data and prevent the monitor from receiving the data.

What's new in February 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 2/15/2023

Enhancements

- Added a **Health** page, linked in the **Insights** menu, that displays the health status view and allows users to view the definitions for health status metrics.
- Added a **Mark all as read** option for the **Notifications** menu.
- Added **Enabled** as a filter option on the **Users** page. Set to **true** to search for enabled users, or **false** to search for disabled users.

- Added the ability to edit entitlements that are in subaccounts.
- Added the ability to filter to the **Entitlements** page.
- Added the ability to subscribe devices to a service based on group or tag.
- Entitlements in subaccounts are now hidden by default and can be displayed by clicking on the subscription card.
- Added expiration as a default column in the Subscriptions table.
- Added ws/v1/reports/schedules API to the API explorer.
- Automations now include an **Offline Device Handling** setting that allows you to define how the automation will behave with regard to devices that are offline at the beginning of the automation run.

Resolved issues

- Fixed an issue where a firmware update would hang when a device disconnected during the file transfer.
- Fixed an issue where alarm monitors were created for new customers that do not have management alarm capabilities enabled.
- Fixed an issue in the Classic Remote Manager where the company name was displayed incorrectly.
- Fixed an issue where subscribing a device to a service did not always enable the service on the device.
- Fixed an issue in the user interface where updating a monitor removed the monitor's headers.

What's new in January 2023

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 1/19/2023

Enhancements

- Added a **Subscriptions** page and menu item to administer add-on subscriptions.
- Added an API to the Report service to schedule and send intelliFlow, Device Availability and Cellular Utilization reports.
- All Remote Manager users are now required to accept the Terms of Service when logging into Remote Manager. After having accepted the Terms of Service, users will not be required to accept them again unless there is a change to the Terms of Service.

  Previously, only account administrators were required to accept the Terms of Service.

Resolved issues

- Fixed an issue sorting and querying intelliFlow service domain names and port names.
- Fixed an issue where FileData resources retrieved via a query monitor were returned in a different format.
- Fixed an issue handling firmware uploads that referenced compressed files.

Update for 1/4/2023

Enhancements

- Added the serial number to the device details view.

Resolved issues

- Fixed an issue where the device map was not visible.
- Fixed an issue where the device map view was not filtered based on the sub-account selection.

What's new in December 2022

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Enhancements

- Renamed the **Uptime Percentage** column to **Connected Percentage** in the availability report.
- Removed **Year to Date** option from reports pages.
- Added the ability to export report tables and charts.
- Added examples in the API Explorer for v1/containers.
- Added the ability to refresh the configuration status table.

Resolved issues

- Fixed an issue in automations where the CLI step displayed the wrong value after the step was moved.
- Fixed an issue where a search pattern consisting of an asterisk (*) would crash the page.
- Fixed an issue where automation steps sometimes could not be saved.
- Added the ability to refresh the configuration status table.

What's new in November 2022

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 11/30/2022

Enhancements

- For some v1/reports/cellular_utilization and v1/reports/intelliflow APIs, added the fields bytes_sent/bytes_received. These are duplicates of the tx_bytes/rx_bytes fields.

  In the future, the tx_bytes/rx_bytes fields will be removed from these APIs, since the naming is inconsistent with other APIs.
- Added a server_domain field and report type to the ws/v1/reports/intelliflow APIs.

Resolved issues

- Updated the vi/reports cellular_utilization and device_availability APIs to correctly use the relative path for devices.
- **Maintenance mode** in the Automation device properties step now works correctly.
- **Wait for reconnect** option in the Automation firmware update step is more reliable when updating to a device running DAL firmware version 21.8 or newer.
- Fix issue where **Reason for Disconnect** message in the device **Summary Dashboard** (and in the /management/connections stream) was empty when the server received a TCP Reset message. The message used to be "Connection reset by peer." The new message is "Connection reset: connection ended unexpectedly."
- Reduced the verbosity of report service logging.

Update for 11/17/2022

Enhancements

- The main menu structure has been reorganized. There are now three top level menu headings with resources under each heading:
  - Insights
    - Map
    - Alerts
    - Reports
    - Data Streams
  - Management
    - Devices
    - Configurations
    - Automations
  - System
    - Users
    - Account Details
    - Notifications
    - Logs

    - API Explorer
    - Monitors
- Renamed the **Allow Offline** option in automation steps to **Wait if Offline** to make the behavior of the option more clear.

Resolved issues

- Fixed an issue where the default RCI payload for the Data Service Request automation step could not be edited.
- Fixed an issue where the events table listed filters that are not supported.
- Fixed an issue where the events table sometimes listed events out of order.

Update for 11/02/2022

Enhancements

- Accounts that have the containers enabled can now upload containers to Remote Manager as part of a configuration, and use the configuration to upload the containers and configure container support on devices managed by the configuration.
- Added additional details about automation steps in the automation summary.

Resolved issues

- Fixed a issue when copying a configuration that caused an error reporting that a vendor ID of 0 was invalid.

What's new in October 2022

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Enhancements

- **Speed Test** action added, with the following disclaimer: "This speed test will provide an estimate on the speed of your connection to the Internet. Many factors can influence this test, including but not limited to: load on the gate, load on the server, and Internet congestion. Digi does not guarantee the accuracy of this test.
- The **Feedback** dialog, accessed through the user menu, has been updated.
- Added the ability to export the events list in CSV format.

Resolved issues

- Fixed an issue where device health status sometimes showed the wrong icon.
- Fixed an issue where the **Actions** menu was not clickable when viewing the device connection history in table format.

- Fixed an issue where the device list filter sometimes could not be cleared.
- The **Cellular Utilization Report** table now displays bytes in a more readable format.

What's new in September 2022

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 9/28/2022

Enhancements

- Added group filter to the device availability report
- Added summary charts to the cellular utilization report page.

Resolved issues

- Fixed an issue where alerts could not be created when scoped to a sub-account
- Fixed an issue where the map in the device details page did not display correctly.

Update for 9/12/2022

Enhancements

- Added current connection status to header on connection status history table.
-

Resolved issues

- Fixed an issue where the DataPoint alert operator could not be set to "not equal to."
- Fixed a bug that was preventing settings from being applied to XBee Gateway devices.

What's new in August 2022

Welcome to the latest update of the Digi Remote Manager® This release provides features and general fixes. There are no security-related fixes in this release.

Update for 8/2/2022

New features

- Device geoposition can now be cleared in the UI.