# Digi Remote Manager®

## User Guide

## Revision history—90001436-13

| Version | Date | Description |
|---|---|---|
| H | May 2016 | Remote Manager platform release that includes the following features and enhancements:<br>■ Added expiration timeouts for health metric data. See Configure health metrics data expiration in Remote Manager.<br>■ Performance improvements and miscellaneous editorial corrections. |
| I | September 2016 | Remote Manager platform release that includes the following features and enhancements:<br>■ Added ability to link Remote Manager accounts together such that a parent account can access and manage subaccounts. See About subaccounts.<br>■ Performance improvements and miscellaneous editorial corrections. |
| J | February 2017 | Remote Manager platform release that includes the following new features and enhancements:<br>■ Added support for secure provisioning. See Add devices to Remote Manager for information on adding devices that require an installation code.<br>■ Performance improvements and miscellaneous editorial corrections. |
| K | May 2018 | ■ Added a Get Started section to the documentation.<br>■ Edited documentation. |
| L | September 2018 | Added information about the ping request user interface. See Ping a device. |

## Trademarks and copyright

Digi, Digi International, and the Digi logo are trademarks or registered trademarks in the United States and other countries worldwide. All other trademarks mentioned in this document are the property of their respective owners.

© 2018 Digi International Inc. All rights reserved.

## 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

## Send comments

**Documentation feedback**: To provide feedback on this document, send your comments to techcomm@digi.com.

## Customer support

**Digi Technical Support**: Digi offers multiple technical support plans and service packages to help our customers get the most out of their Digi product. For information on Technical Support plans and pricing, contact us at +1 952.912.3444 or visit us at www.digi.com/support.

# Contents

## Digi Remote Manager® User Guide



## Get Started



## Remote Manager dashboard

## Device management

## Messaging



## XBee networks



## Alarms



## Schedules and tasks

## Operations



## Carrier accounts



## Profiles



## Reports

## Data services



## Security set up and management



## Remote Manager Account administration

## Remote Manager views

# Digi Remote Manager® User Guide

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 Digi Remote Manager, you can efficiently interact with any device or group of devices in your Remote Manager inventory. This enables you to:

- Ensure that all of your devices are up to date with the latest security patches, firmware, and configurations.
- Set up health metrics that allow you to keep track of the state of your device inventory at a high level, and then drill down to assess issues.
- Set up alerts to inform you when there is an issue that requires your attention.
- Automate remediation if devices become out of compliance.
- Deploy application logic to your “edge” devices, such as routers and gateways.

This guide provides step-by-step instructions for using the Remote Manager user interface.

For information on using Remote Manager APIs, see *Remote Manager Programmer Guide*.

## Requirements

To use Remote Manager, make sure your system meets or exceeds the following requirements.

### Port requirements

| Port | Usage |
|---|---|
| TCP 3199 | Must be open for outbound traffic from devices to establish a secure connection to Remote Manager |
| TCP 3197 | Must be open for outbound traffic on devices configured to use raw TCP connection |

**Note** Outgoing ports may be blocked by firewalls.

### Communication protocols

Remote Manager uses various communication protocols.

- **EDP** (Easy Device Protocol): EDP is a Digi proprietary network protocol for communicating with Remote Manager.
- **RCI** (Remote Command Interface): RCI is a high-level communication protocol written in XML that is used for communications between end-user applications. Remote Manager uses RCI to remotely command and communicate with an embedded device, and with the Remote Manager server or with a client that resides in Remote Manager.

## Application types

Remote Manager recognizes two types of applications:

- **Device applications**: Device applications run on a device, and send data to and receive data from Remote Manager.
- **Client applications**: Client applications run on a PC or a device added to Remote Manager, and use Remote Manager services to communicate with the device application running on a device.

# Get Started

Remote Manager is a cloud-based device management platform that allows you to connect any device to any application, anywhere. To get started, you need a Remote Manager account. After you have created an account, you can add the devices that you want monitor to the Remote Manager inventory.

## Step 1: Create a Remote Manager account

You can download a free trial account that allows you to explore all the Remote Manager features and functionality. Before your trial account expires, you should upgrade your account to a paid account edition.

1. Create a free Remote Manager account and Determine the account owner
2. Log in to your Remote Manager account
3. Upgrade your account to a paid account

## Step 2: Add users to Remote Manager

You can add additional users to your Remote Manager account. These users can be assigned different roles to give them privileges to perform operations within Remote Manager.

- Add a user

## Step 3: Add and configure devices

You can add devices to your Remote Manager inventory, and then configure the devices so you can manage them remotely.

1. Add devices to Remote Manager
2. Configure and manage devices

## Step 4: View the dashboard and run reports

The dashboard appears automatically when you log into your account and shows device health and status information as a pie chart. For devices that support additional health metrics reporting, Remote Manager gathers device-level health metrics. You can create and run reports from this information.

1. View the dashboard
2. Generate device health reports

## Step 5: Set up security

Remote Manager allows users with certain roles and privileges to perform operations, such as making changes or setting up device operations. Each user must be assigned a role when a user account is created.

In addition to user roles, you can create security polices that control access to Remote Manager.

- Assign a user role
- Require two-factor authentication for log in
- Restrict access to only authorized IP addresses

## Step 6: Configure optional features

You can configure additional features in Remote Manager that help you manage your devices.

- Alarms: Create alarms to monitor various activities of the devices in Remote Manager.
- Schedules: Use Remote Manager schedules to perform common management tasks on one device or a group of devices.
- Profiles: Create device profile templates to control, monitor, and report on device firmware versions, configuration options, and file systems.
- Carriers: Configure various cellular service providers within Remote Manager so you can monitor your actual cellular data usage.
- Messaging: Configure messaging services that are useful for requesting connections to Remote Manager, sending data to and from devices, sending a command to a device, or sending a command line interface (CLI) command.

## Create a Remote Manager account

Before you can use Remote Manager, you must create a free trial Remote Manager account.

Part of creating the Remote Manager account is creating the first user account in Remote Manager. The first user becomes the account owner, who may not be a particular person, but a role within your organization. You may want to choose a user name that reflects a Remote Manager role rather than an actual person. See Determine the Account owner.

1. Go to www.digi.com/remotemanager.
2. Click **30-Day Free Trial**.
3. Complete the registration form, making note of your user name and password for future reference.
4. Review and accept the **Digi Remote Manager Terms of Service**.
5. Enter the image code in the text field.
6. Click **Start Free Trial**. An account confirmation screen appears.
7. Check your email inbox for your account activation link.
8. Click the account activation link in your email.
9. You can now log in to your Remote Manager account and begin adding devices to your device inventory. See Add devices to Remote Manager.

# Determine the Account owner

The account owner is the main system administrator for your Remote Manager customer account. When you create your trial customer account, the account owner is the first user record you create, and also the first user that can log in and add additional users to your Remote Manager account.

The account owner is assigned the administrator role by default, and can perform all functions and use all of the features in Remote Manager. In addition, only the account owner has billing authority for the account. The account owner can:

- Increase or decrease the device limit for an account
- Upgrade the account edition
- Add subscriptions
- Add or remove bundles and features for the account

When you enter the account owner information, you are required to enter a person's name and email address, as well as a user name for the account. Be aware that the account owner may not be a particular person, but a role within your organization. You may want to choose a user name that reflects a Remote Manager role rather than an actual person. Note that you cannot change the user name for a user after an account has been created. The name and email assigned to a user can be changed if needed.

To determine the account owner for your customer account, click **Security > Users** and then sort the users by the **Registered** column. Generally, the user with the oldest registration date and time is the account owner.

You cannot delete the user account that is designated as the account owner. If you try to delete the account owner, an error message appears and the deletion process is canceled.

The account owner is assigned the administrator role by default. You can change the user role assigned to the account owner; however, there must be at least one administrator for each customer account.

# Log in to your Remote Manager account

After you have created your Remote Manager account, you can log in.

**Note** See Create a Remote Manager account for instructions on how to create an account.

1. Log in to Remote Manager.
2. Type your login credentials in the **Username** and **Password** fields.

   **Note** If you have forgotten your credentials, click **Forgot Username or Password** and follow the online instructions. See Forgot user name or password.

3. Click **Log in**.

# Upgrade a trial account to a paid account

Remote Manager offers a free trial account that allows you to explore Remote Manager features. Before your trial account expires, you must upgrade your free account to a paid account edition in order to continue using Remote Manager.

The account edition you choose subscribes Remote Manager to a set of services appropriate for your device management requirements. You can add additional services and subscriptions if needed.

1. Determine which account edition you would like to purchase. Go to www.digi.com/remotemanager for details on current Remote Manager account editions and available features.
2. Call Digi International Inc. to purchase an account: **1-877-912-3444**.

# Remote Manager services

Remote Manager offers the following services.

| Service | Description |
|---|---|
| Device Management Service | Provides access and monitoring services for all devices in your inventory. |
| Device Messaging Service | Tracks messages between Remote Manager and Remote Manager-registered devices. |
| WebService Messaging Service | Tracks messages between Remote Manager and Remote Manager client applications. |
| XBee Smart Energy Management Service | Enables Smart Energy support within your Remote Manager account. Smart energy support allows for the aggregation of data within Remote Manager. The Smart Energy service allows data sent and received from the device to be interpreted using the Smart Energy Profile standards. |
| SMS Messaging Service | Enables you to send and receive SMS messages between Remote Manager and Remote Manager-registered devices. SMS can be used for basic device management tasks, as well as exchanging application data between Remote Manager and a connected device. Individual connected devices can subscribe to the SMS service and you can opt to activate SMS messaging on a per-device basis. |
| SM/UDP Messaging | This service comes auto-subscribed on all Remote Manager user accounts. This service provides the ability to send and receive SM/UDP messages between Remote Manager and Remote Manager-registered devices. SM/UDP may be used for very basic device management tasks as well as exchanging application data between Remote Manager and the connected device. You must enable SM/UDP support for a device before you can send any SM/UDP messages. |

| Service | Description |
|---|---|
| Embedded Device Customization | This service provides the option for a device manufacturer, utilizing Remote Manager embedded components, to enable access of their custom device(s) for management and data access via Remote Manager. This provides the ability for third party device vendors to register manufacturer IDs on Remote Manager and dynamically present appropriate configuration options specific to those devices. This is a global account-level service available at no charge.<br>For more information, see the *Remote Manager Programmer Guide*. |
| DIA API (Dia Data Management) | This resource interface is for creation of custom remote sampling solutions that report data through the DIA idigi_db presentation. Presentation data is stored in Remote Manager Data Streams. This allows Web Services client applications to directly query the DIA tables. Access to this API is available through a Web Services subscription. The DIA API is also called Dia Data Management within the user interface. |
| Web Services Monitor (Push Monitoring) | The Web Services Monitor API supports setting up, modifying, and deleting push notifications of special Web Services which will provide data and status reports based on user-defined conditions. For example, if you are monitoring DeviceCore and a new device was added to your Remote Manager account, then Remote Manager would push a DeviceCore CREATE message that included that information about the new device. The Web Services Monitor is also called Push Monitoring within the user interface.<br>For more information, see the *Remote Manager Programmer Guide*. |
| Data Streams | Data Streams is a RESTful API for storing and accessing time series data within Remote Manager. Your data is stored and replicated in multiple secure, commercial-grade storage systems to ensure complete protection of your data.<br>By provisioning this API, it will be possible to store and query time series data on Remote Manager. Additionally, any data previously accessible via the DIA or XBee APIs will be automatically replicated and available for historical query via the Data Streams API. |

# Remote Manager dashboard

The dashboard shows device health and status information as a pie chart. When you log into your account, the dashboard displays automatically. This section details the dashboards and explains how to configure device health metrics.

## View health metrics charts

The following charts appear in the dashboard screen:

- Device Health chart
- Connection Status chart
- Connection Status History chart
- Alarm Summary chart
- Monitor Status chart

## Configure health metrics on each device

For each device, you can configure health metrics, health metrics thresholds, data metrics expiration:

1. Configure each device in Remote Manager to enable health metrics reporting. See Configure health metrics for a device in Remote Manager.
2. Configure the metric thresholds for each device type. See Configure device health thresholds in Remote Manager.
3. Determine whether metrics data should be retained or allowed to expire. See Configure health metrics data expiration in Remote Manager.

## View device health for a subaccount

If you have created subaccounts, you can view device health for the devices in a subaccount. See View device health for a subaccount.

## Dashboard reference

The following reference sections include information about the dashboard pages:

- Dashboard view
- Device health configuration view

# Device Health chart

The Device Health chart in the dashboard shows a summary of the health of your devices. Device health 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.

For each health metric the device reports, you can configure the values for three thresholds: normal, warning, and error. See Configure device health thresholds in Remote Manager.

You can generate reports about the device health metrics that are represented by the chart in the dashboard. See Reports for more information.

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.

You can filter the data included in the chart using one or both of the following methods:

- Click a status label beneath the chart to include or exclude that status.
- From the **Filter by** options, select a group or device type that you want to display in the chart. See Filter the dashboard charts for more information.

# Connection Status chart

The Connection Status chart 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.

You can generate reports about the connection status information that is represented by the chart in the dashboard. See Reports for more information.

You can filter the data included in the chart using one or both of the following methods:

- Click a status label beneath the chart to include or exclude that status.
- From the **Filter by** options, select a group or device type that you want to display in the chart. See Filter the dashboard charts for more information.

# Connection Status History chart

The Connection Status History chart shows a history of the aggregate number of devices connected, disconnected, or never connected. Never connected denotes a registered device that has not yet connected to Remote Manager.

To display this chart, click the **History** link at the bottom of the screen, next to the Connection Status chart.

You can generate reports about the connection status history information that is represented by the chart in the dashboard. See Reports for more information.

You can filter the data included in the chart using one of the following methods:

- Click a status label beneath the chart to include or exclude that status.
- From the **Filter by** options, select a group or device type that you want to display in the chart. See Filter the dashboard charts for more information.
- Select a time range to display: 12 hours, 1 day, 1 week, or 1 month.

## Alarm Summary chart

The Alarm Summary chart shows a summary of all fired alarms by alarm type. You can filter the chart by clicking on the alarm type label beneath the chart to include or exclude one or more alarm types.

You can generate reports about the alarm summary represented by the chart in the dashboard. See Reports for more information.

## Monitor Status chart

The Monitor Status chart shows a summary of all system monitors by monitor status: Inactive, Active, Disabled, Suspended, Disconnecting, and Connecting. You can filter the chart by including and excluding monitor statuses.

You can generate reports about the monitor status information that is represented by the chart in the dashboard. See Reports for more information.

## Filter the dashboard charts

You can filter the Device Health, Connection Status, and Connection Status History charts by group or device type, or both.

1. Click **Dashboard**.
2. Select a filter option.
   - To filter by group, click **Group** and select a group to include in the charts. Only one group can be selected.
   - To filter by device type, click **Device Type** and select a device type to include in the charts. Only one device type can be selected.
3. You can remove a filter option.
   - Click **Group** and deselect the selected folder, or select or another group.
   - Click **Device Type** and deselect the selected device type, or select another device type.

## Configure health metrics for a device in Remote Manager

If a device supports health metrics reporting, you can configure general options for health metrics reporting for the device from Remote Manager. For mobile metrics reporting, you can also include metrics on latency and packet loss.

**Note** Enabling health metrics reporting for a device increases network traffic.

## Configure health metrics reporting

The following procedure gives general steps for configuring health metrics reporting on a device.

**Note** For detailed information on health metrics for your device, refer to the device product documentation.

1. Click **Device Management**.
2. In the device list, locate the device you want to configure and double-click the device.
3. Click **Configuration > Remote Management > Remote Manager > Health Metrics Reporting**.
4. Configure health metrics reporting options.
5. Click **Save** to save the configuration settings.

| Option | Description |
|---|---|
| **Global reporting interval (minutes)** | Select the time interval for reporting health metrics. The default interval is 60 minutes (every hour). |
| **Ethernet Metrics** | Turn on or turn off Ethernet metrics. The default is Off. |
| **Ethernet Sampling interval (seconds)** | ■ **Ethernet Sampling interval (seconds):** Select the time interval for collecting Ethernet metrics. The default interval is 3600 seconds (every hour).<br>■ **Mobile Metrics:** Turn on or turn off mobile metrics. The default is Off. |
| **Mobile Metrics** | Turn on or turn off mobile metrics. The default is Off. |
| **Mobile Sampling interval (seconds)** | Select the time interval for collecting mobile metrics. The default interval is 3600 seconds (every hour). |
| **System Metrics** | Turn on or turn off system metrics. The default is Off. |
| **System Sampling interval (seconds)** | Select the time interval for collecting system metrics. The default interval is 3600 seconds (every hour). |

## Configure mobile health metrics reporting

If you configured mobile metrics reporting for a device, you can opt to include metrics for latency and packet loss data. To do so, configure the PPP 1 interface to ping IP address 8.8.8.8 at 30-second intervals, turn on the firewall, and modify the firewall rules file (fw.txt).

**Note** Monitoring and reporting on latency and packet loss will result in increased charges with your mobile carrier.

To include latency and packet loss data with mobile health metrics reporting:

1. Click **Device Management**.
2. In the device list, locate the device you want to configure and double-click the device.

3. Click **Configuration > Network > Interfaces > Advanced > PPP > PPP 1**.
4. Configure the following options:
   - **Enable firewall on this interface:** Select **1** to enable the firewall on PPP 1.
   - **Send Ping packets to IP host:** Enter **8.8.8.8** as the IP address.
   - **Send Ping packets interval:** Select **30** to send packets every 30 seconds.
5. Click **Save** to save the configuration settings.
6. Include the following lines at the top of the firewall rules file (fw.txt):

```
pass out break end on ppp 1 proto icmp from addr-PPP 1 to 8.8.8.8
inspect-state oos 1 t=30 c=5 d=5 stat
pass break end
```

# Configure device health thresholds in Remote Manager

If a device supports health metrics reporting, you can configure the threshold metrics for all devices of the same type. You can configure three thresholds for each metric: normal, warning, and error.

You can also enable or disable whether the metric is used to determine overall device health.

**Note** Before you can edit a device health configuration, you must configure health metrics reporting for the device. See Configure health metrics reporting.

1. Click **Dashboard**.
2. Click **Device Type** to display a list of device types.
3. Click the gear icon to the right of the device type you want to configure. The **Device Health Configuration** screen appears.

   **Note** If no devices of the selected type are configured for health metrics reporting, a message displays on the page. Click the X icon to close the page and return to the dashboard.

4. For each health metric you want to configure:
   a. Click **Edit**.
   b. Enter threshold values for normal, warning, and error.
   c. If you want to reverse the threshold order, click  .
   d. Click the check box in the **Enabled** column.
   e. Click **Save**.
5. Click the **Close Profile Settings** icon (the X icon) to close the profile settings screen and return to the dashboard.

# Configure health metrics data expiration in Remote Manager

Devices in the Remote Manager inventory report health metrics and status information. The health metrics appear in the Device Health chart on the Remote Manager dashboard. This information is stored in Remote Manager by default.

You can determine whether you want to retain or expire the health metrics data:

- Disable health metric expiration: When you disable this feature, the health metrics data is retained indefinitely.
- Enable health metric expiration: When you enable this feature, the health metrics data expires after a specified time interval. You can choose to specify a time interval, or use the system-defined default.

### Enable health metric expiration

When a health metric expires, Remote Manager sets the metric back to normal, and the device continues to report health metric data. Subsequent data uploads can again set a metric to a warning or error state.

When you enable the health metric expiration feature, you must also determine whether the health metrics expire based on system-determined expiration timeouts or after a manually set expiration timeout.

1. Click **Admin > Account Settings > Preferences**.
2. Select **Enable Health Metric Expiration**.
3. Determine when the health metrics should expire:
   - **System-based expiration**: Select the **Automatically choose expiration timeout** option to expire the health metrics based on the system-determined expiration timeouts.
   - **Manually set expiration**: Deselect the **Automatically choose expiration timeout** option. The **Expiration Timeout** field becomes available. Enter the expiration timeout in the field. The time is measured in minutes, from 10 to 43,200 minutes (30 days).
4. Click **Save**.

### Disable health metric expiration

You can choose to disable health metric expiration. When this feature is disabled, the health metric information is stored indefinitely.

**Note** The health metric information can be viewed in the dashboard.

1. Click **Admin > Account Settings > Preferences**.
2. Deselect the **Enable Health Metric Expiration** option.
3. Click **Save**.

## View device health for a subaccount

If you are logged in to a Remote Manager account that has associated subaccounts, you can view device health charts for a selected subaccount.

See Customer accounts and subaccounts for more information about subaccounts.

1. Click **Admin > Customers**.
2. Double-click the subaccount you want to select. The subaccount is now the currently selected account.
3. Click **Dashboard**. All device health charts display device health for the selected subaccount.

# Device management

The Remote Manager **Device Management** view allows you to monitor and manage devices registered to your Remote Manager account. The options shown in your **Device Management** view depend on your Remote Manager edition and service bundles.

You can add and remove devices from the Remote Manager inventory, and refresh device information as needed. You can also remotely ping or reboot a device.

- Add devices to Remote Manager
- Remove a device from Remote Manager
- Device IDs
- Refresh device information
- Reboot devices
- Ping a device

After the devices have been added to Remote Manager, you can configure and manage the devices.

- Configure and manage devices
- Upload files to a device

You can use the search feature to find a device or a set of devices, or use the locate feature to locate a device on a map.

- Search for devices
- Locate a device on the map

You can remotely connect and disconnect devices from Remote Manager.

Connect and disconnect devices

You can use metadata, tags, device groups, and descriptors to describe and group devices.

- Organize devices: metadata, tags, and device groups
- Add a descriptor

## Add devices to Remote Manager

You must add all devices that you want to manage with Remote Manager to your Remote Manager inventory, and then configure the device to allow remote management.

Devices can be added individually, or you can add multiple devices using a CSV file.

- Add devices to your inventory individually
- Add multiple devices using a CSV file

## Add devices to your inventory individually

This topic explains how to add each device individually.

**Note** You can also add multiple devices using a CSV file. See Add multiple devices using a CSV file.

1. Click **Device Management > Devices**.
2. Click **Add Devices**. The **Add Devices** dialog appears.
3. For each device you want to add:
    a. From the drop-down menu, select the device identifier type to use for the device: **MAC address**, **IMEI #**, or **Device ID**. Typically, you can find the MAC address or IMEI number on the device label. See Device IDs.

    **Note** If a device has both a MAC address and an IMEI #, you must use the MAC address to add the device.

    a. Type in the device identifier.
    b. In the **Install Code** field, enter the installation code found on the device label. If you attempt to add a device that requires an installation code with a missing or incorrect code, you receive an error message. For devices that were not manufactured with an associated installation code, the installation code is optional.
    c. Click **Add**. The device is added to the device list box.
4. When you have finished entering devices, review the listed devices. If necessary, use **Remove** to remove any incorrect entries.
5. Click **OK** to add all the listed devices to your Remote Manager inventory.
6. After a few minutes, click the refresh icon in the toolbar to refresh the device list. The new devices appear in your device inventory.
7. Information about the added device is saved in the event log. Click **Admin > Event Log** to display the Admin > Event log view.

## Add multiple devices using a CSV file

You can add up to 1000 devices at one time to Remote Manager using a CSV file.

1. Create a CVS file that includes the list of devices you want to register with Remote Manager and save it on your local machine. See Create a CSV file to add multiple devices.
2. Click **Device Management > Devices**.
3. Click **More > Bulk Add Devices**. The **Bulk Add Devices** dialog appears.
4. In the **File** field, browse to and select the CSV file that contains the list of devices you want to add.
5. Click **OK**.
6. Click **Admin > Event log** to view the status of the Bulk Add Devices event in the Admin > Event log view.

### *Create a CSV file to add multiple devices*

You can add up to 1000 devices at one time using a CSV file that includes the devices you want to register with Remote Manager.

The format of the file is as follows:

- Specify one device per row in the file.
- Provide the device ID for each device. See Device IDs.
- If the device requires an installation code, provide the installation code after the device ID, separated by a comma.

The following shows a sample CSV file for adding multiple devices. The third device in the file includes a required installation code.

```
00000000-00000000-00000000-00000001
00000000-00000000-00000000-00000002
00000000-00000000-00000000-00000003,PS9MSPXQXM
```

## Remove a device from Remote Manager

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

1. Click **Device Management > Devices**.
2. Select one or more devices to remove.
3. Click **Remove Devices**. A confirmation dialog appears.
4. Click **Yes** to remove the selected devices.

## 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.

**Note** In resource web services, device IDs are listed as devConnectwareId elements. See the DeviceCore section in the *Digi Remote® Manager Programmer Guide*.

### 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<br>01234567-89ABCDEF |
| 01234567-89ABCDEF-01234567-89ABCDEF | No abbreviated form |
| 00000000-00000000-00000000-89ABCDEF | 00000000-00000000-89ABCDEF<br>00000000-89ABCDEF<br>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 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 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

## Refresh device information

Refresh the properties page to view the current information for a particular device.

1. Click **Device Management** > **Devices**.
2. Use one of the following methods to display the **Properties** page:
   - Select a device and then click **Properties** in the toolbar.
   - Right-click a device to display the short-cut menu and then click the **Properties** menu option.
3. Click **Refresh** in the toolbar.

## Reboot devices

You can reboot devices from your Remote Manager account on a one-time or scheduled basis.

1. Click **Device Management > Devices**.
2. Select a device. To select multiple devices, press **Control** and click additional devices.
3. Click **More > Reboot**. A dialog appears, requiring you to confirm that you want to reboot the device.
4. You can schedule when you want the reboot to occur. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
5. Click **Yes** to reboot the device immediately or at the scheduled time, or **No** to cancel.

# 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.

You can choose to ping a device once or on a scheduled date and time.

1. Click **Device Management > Devices**.
2. Select a device. To select multiple devices, press **Control** and click additional devices.
3. Click **More > Ping**. Click **Yes** to immediately ping the selected device(s).

   **Note** If desired, you can schedule the ping to occur on a date and time in future. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.

4. The **Progress** dialog appears, and shows the progress of the ping.
5. You can review information about the ping process.
   a. Click **Device Management > Operations**.
   b. In the list of operations, select the **Ping** operation you just submitted. You can check the date and time in the **Submitted** column.
   c. Click **Operation Details** in the toolbar. Information about the job appears in the **Operation Details** page. See Operations for more detailed information about this page.

# Configure and manage devices

After a device has been added to Remote Manager, you should configure it for use with Remote Manager. The topics in this section include general information on how to configure and manage a device in Remote Manager.

## Configure a device in Remote Manager

Most device types have unique options that you can configure to allow the device to be managed using Remote Manager.

**Note** Each device type has unique Remote Manager options that you can configure. For detailed information on remote management options for a device, refer to the specific device documentation or contact support services.

1. Click **Device Management > Devices**.
2. Double-click the device you want to configure. The device properties page appears.
3. Scan the configuration options to locate remote management options. Typically, the options are located under **Advanced Configuration > Remote Management**.
4. Enable remote management and set other remote management options, as needed.
5. Click **Save**.

## View device properties

You can view a device's properties to see the device type, MAC address, device ID, IP address, and description.

1. Click **Device Management > Devices**.
2. Select a device from the device list. The **Properties** button appears in the Devices toolbar.
3. Click **Properties**. The Properties page appears.

To return to your device inventory, click the **Devices** tab in the pane or click **Devices** in the upper left corner of the pane.

## Edit a device description

For most device types, you can add or change the device's description in Remote Manager. You may want to change the description for a device for a number of reasons. For example, you might want to edit the description to match its purpose or to better identify the device and its attributes.

1. Click **Device Management > Devices**.
2. Select a device in your device list. The **Properties** button appears in the toolbar.
3. Click **Properties**. If the device allows a description to be assigned, the **Advanced Configuration** menu appears in the left menu.
4. Click **Advanced Configuration > System**. The System pane appears.
5. Enter descriptive information in the **Contact**, **Location**, and **Description** fields.
6. Click **Save**.

## Update device firmware

You can update firmware for one or more devices. To update firmware for multiple devices at the same time, all devices must be the same type.

1. Download the updated firmware file for your device from the manufacturer's site.
2. In your Remote Manager account, click **Device Management > Devices**.
3. Select the first device you want to update. To select additional devices of the same type, press the Control key and select additional devices.
4. Click **More > Update Firmware**. The **Update Firmware** dialog appears.
5. Click **Browse** to select the appropriate firmware file for the device.
6. You can schedule when you want the update to occur. Click the gear icon to display the options. See Schedule an action for detailed information about the schedule options.
7. Click **Update Firmware** to update the firmware as specified. The updated devices will automatically reboot when the updates are complete.

## Customize device attributes

You can upload a customization file to change a device's attributes, if the device supports customization. This capability allows you to apply private labeling to supported devices by changing various attributes, including product name, company name, stylesheets, logos, and custom factory defaults.

**Note** Currently, only ConnectPort devices allow customization.

1. Click **Device Management > Devices**.
2. Select a device. To customize multiple devices, press the Control key and select additional devices.
3. Click **More > Customization**. The **Customization** dialog appears.
4. Click **Browse** and locate the customization file in your file system. The selected file name appears in the **File** field. You can click **Clear** to delete the selected file.
5. In the **Path** field, specify the location to which the file should be uploaded.
6. You can schedule when you want the customization to occur. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
7. Click **OK** to customize the selected device(s) immediately or at the scheduled time.

## Export device properties

You can export a device's XML configuration file to save the properties for future use, or to import them to another device.

1. Click **Device Management > Devices**.
2. Select a device.
3. Click **More > Export Properties**. The **Export Properties** dialog appears.
4. Click **OK**. The configuration file is downloaded and can be opened or saved.

## Import device properties

You can import a saved XML configuration file that was previously exported from a device.

1. Click **Device Management > Devices**.
2. Select a device.
3. Click **More > Import Properties**. The **Import Properties** dialog appears.
4. In the **File** field, browse for the previously exported and saved device XML configuration file.
5. You can schedule when you want the import to occur. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
6. Click **OK** to import the device properties as specified.

## Restrict and unrestrict a device

You can restrict a device to prevent it from connecting to Remote Manager. You can unrestrict a device when it should be allowed to connect to Remote Manager.

### *Restrict a device*

1. Click **Device Management > Devices**.
2. Select a device. To restrict multiple devices, press the Control key and select additional devices.

3. Click **More > Restrict**. A confirmation dialog appears.
4. In the drop-down box, select **Restrict**.
5. Click **Apply**.

**Note** When restricting a device that is currently connected to Remote Manager, you must disconnect the device after restricting.

### *Unrestrict a device*

You can unrestrict a device that has been restricted.

1. Click **Device Management > Devices**.
2. Select a device that has been restricted. To unrestrict multiple devices, press the Control key and select additional devices.
3. Click **More > Restrict**. A confirmation dialog appears
4. In the drop-down box, select **Unrestrict**
5. Click **Apply**.

## Untrust a device

You can untrust a device so that it can only perform a limited set of functions.

1. Click **Device Management > Devices**.
2. Select a device. To untrust multiple devices, press the **Control** key and select additional devices.
3. Click **More > Restrict**. A confirmation dialog appears.
4. In the drop-down box, select **Untrust**.
5. Click **Apply**.

## Schedule an action

You can schedule an action to occur at a specified date and time. Options are:

- **Immediate**: The action occurs when you click **OK**.
- **One-Time**: The action occurs once at a future date and time. You must specify the date and time in the associated fields. The schedule is saved when you click **OK**.
- **Recurring**: The action occurs at a future date and time, and with a specific frequency. You must specify the date range during which the action should occur and the action frequency, such as hourly, daily, weekly, or monthly. The schedule is saved when you click **OK**.
- **Schedule Off-line**: Queue the action to occur the next time this device connects to Remote Manager. The schedule is saved when you click **OK**.

# Upload files to a device

You can upload files to one or more devices in your device list if the device supports file uploads.

1. Click **Device Management > Devices**.
2. Select a device. To upload the same files to multiple devices, press the **Control** key and select additional devices.
3. Click **More** in the Devices toolbar and select one of the following:
   - **Upload Python Files** (Python files only): Uploads Python files to the root python directory of the specified device(s).
   - **Upload Files** (all other file types): Uploads files to the root directory of the device(s) selected.
4. In the **Upload Files** dialog, click **Browse** and select the file(s) to upload to the selected device (s).
5. You can schedule when you want the file upload to occur. For example, you may want to schedule an upload when anticipated network traffic is light. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
6. Click **OK** to upload the file(s) immediately or at the scheduled time.

# Search for devices

You can search for a device, or a set of devices, by using the search feature in Remote Manager. You can filter search results by device group, subaccount, or device attribute. To display the device attributes, click the down arrow in the **Search** field.

When you have completed a search, you can click the **x** in the search box to clear the search and reset search parameters to the defaults.

If you are logged in to a Remote Manager account that has associated subaccounts, you can locate devices within a selected subaccount.

1. Select a subaccount. Skip this step if you want to view a device map for the main customer account.
   a. Click **Admin > Customers**.
   b. Double-click the subaccount you want to select. The subaccount is now the currently selected account.
2. Click **Device Management > Devices**.
3. Select the device group you want to search within. For example, click the **Show/Hide Groups** icon to view your device groups, and select the root directory.
4. Click the down arrow inside the search window in the upper-right corner.
5. Select the search criteria.
6. Type a search string into the search window and then click the magnifying glass. Remote Manager returns a list of devices in your device list that match the search criteria.

# Locate a device on the map

Remote Manager's map component displays a geographical representation of the devices in your inventory containing GPS coordinates. Location information is pulled automatically based on a device's

longitude and latitude values.

In map view, pin markers indicate the locations of individual devices and circular markers indicate the locations of small, medium, and large device groups. Within the map's viewport, you can:

- Select a single device or a group of devices and view the properties of the selected device(s).
- Search for devices, for example, by tag name or device type. The map will automatically refresh and display only the devices matching the search criteria entered.
- Toggle between standard map view (with or without terrain displayed) and satellite map view (with or without labels displayed) using the buttons in the upper-right corner of the map's viewport.
- Zoom in or out with the + and - symbols in the upper-left corner of the map's viewport.

### View the device map

You can view the locations of devices with GPS coordinates on a map in your Remote Manager account. You can then access a summary of device properties and the more detailed Properties page for any device with GPS coordinates directly from map view.

If you are logged in to a Remote Manager account that has associated subaccounts, you can locate devices within a selected subaccount.

1. Select a subaccount. Skip this step if you want to view a device map for the main customer account.
    a. Click **Admin > Customers**.
    b. Double-click the subaccount you want to select. The subaccount is now the currently selected account.
2. Click **Device Management > Devices**.
3. Click the **Show/Hide Map** icon in the toolboar to display the device map. The pin markers indicate the locations of individual devices. The circular markers indicate the locations of small, medium, and large device groups. Click **Show/Hide Map** again to hide the device map.
4. Access device properties from the map.
    a. Zoom in until the individual device's pin is displayed within the map's viewport.
    b. Click the pin once. A summary dialog containing information pertaining to the device is displayed.
    c. Click **Open device properties** from within the summary dialog. Remote Manager displays the Properties page for this device.

## Connect and disconnect devices

A device can have two possible states when added to Remote Manager:

- Listed in Remote Manager and connected to Remote Manager.
- Listed in Remote Manager but not connected to Remote Manager.

If the device is plugged in, has an Ethernet or Wi-Fi connection, has carrier service and has a SIM card installed, it should automatically connect to Remote Manager when added to the Remote Manager inventory. However, if any of these requirements are not met, the device will not connect. In this case, try adding the device again once all requirements listed above have been met.

Devices in the device list display a red disconnect symbol if they are not connected, or a blue connected symbol if they are connected.

## Set up a connection strategy for a device

For most types of devices, you can determine the circumstances in which the device will disconnect from and reconnect to Remote Manager.

Some of the considerations for determining your device's connection strategy include the following:

- You may only want to connect a device to Remote Manager for one specific purpose at a scheduled time.
- You may want to set certain tasks or operations to occur, with device connection or disconnection as the trigger event.
- You may want to monitor and control cellular data usage.

**Note** Various connection options are available for different types of devices. Refer to the device documentation for more detailed connection information.

To set up the connection strategy for a device:

1. Click **Device Management > Devices**.
2. Select a device.
3. Click **Properties**. If the device is a type that can be configured with a connection strategy, the **Advanced Configuration** menu appears in the left navigation.
4. Click **Advanced Configuration > Remote management connection**.
5. Determine whether the connection is enabled.
    - Select **On** to enable the connection.
    - Select **Off** to disable the connection.
6. Determine the reconnect timeout preference for the device.
    - **Never reconnect**: Select this option if you do not want the device to reconnect following disconnect.
    - **Seconds**: Select a **Connection reconnect timeout** in seconds to set the device to reconnect after a certain period of time following disconnection.

## Connect a device via SMS request

You can send a connection request to a device via the SMS protocol. You must first configure the device for SMS messages and have cellular carrier service.

1. Click **Device Management > Devices**.
2. Select a device that you want to connect.
3. Click **More > Send Message** from the SMS section. The **Send Message** dialog appears.
4. Click **Request Connect** from the drop-down menu. The **SMS Request Connect** dialog appears.
5. Check **Request Response** if you want to receive a success or failure message from the device.

6. Click **Send**. The device will receive an SMS message instructing it to establish an EDP connection with Remote Manager.

To see the most updated status for your device, click the circular refresh button.

**Note** A device connected via SMS request may not disconnect automatically. In this case, manually disconnect the device.

## Connect a device via SM/UDP

You can send a connection request to a device via SM/UDP (Short Message/User Datagram Protocol). You must first configure the device for SM/UDP support.

1. Click **Device Management > Devices**.
2. Select a device that you want to connect.
3. Click **More > Send Message** from the SM/UDP category. The **Send Message** dialog appears.
4. Click **Request Connect** from the drop-down menu. The **SM/UDP Request Connect** dialog appears.
5. Check **Request Response** if you want to receive a success or failure message from the device.
6. Click **Send**. A dialog appears showing the progress of the connection request message. When complete, the device will receive an SM/UDP message instructing it to establish an EDP connection with Remote Manager.

To see the most updated status for your device, click the circular refresh button.

**Note** A device connected via SM/UDP may not disconnect automatically. In this case, manually disconnect the device.

## Disconnect a device

You can disconnect any currently connected device in your Remote Manager account. Note that the device may be set to auto-reconnect. A disconnected device remains in your device inventory, but its status will change from connected to disconnected.

You can also set a device to disconnect and reconnect on a schedule.

1. Click **Device Management > Devices**.
2. Select a device. To disconnect multiple devices, press the **Control** key and select additional devices.
3. Click **More > Disconnect**. A **Disconnect Devices** confirmation dialog appears.
4. You can schedule when you want the disconnect to occur. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
5. Click **Yes** to disconnect the selected device(s) immediately or at the scheduled time.

## View device connection history

Remote Manager tracks and displays a detailed connection history between a device and Remote Manager. You can view connection and disconnection times, connection methods, and disconnect reasons.

1. Click **Device Management > Devices**.
2. Select a device in your device inventory. The **Properties** button appears in the Devices toolbar.
3. Click **Properties**.
4. Click **Connection History** to view the recorded history of connects, disconnects and the reason for disconnects. See Device disconnect reasons.

## 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 by peer | The TCP connection was severed remotely from Remote Manager. Typically, a device or piece of networking equipment is causing disconnection. For example:<br>■ 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.<br>■ The device was reconfigured to a new server and a boot action=reset was executed. |
| 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. |
| 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. |
| 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. |

| Disconnect Reason | Description |
|---|---|
| Server reset | The 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. |

# Organize devices: metadata, tags, and device groups

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 your device inventory, and can assign devices to that group. You can also create a hierarchical structure of device groups to help organize your device inventory.

- Create device groups
- Add devices to a group
- Edit a device group
- Remove a device from a device group
- Show or hide device groups
- Remove a device group

## 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.

- Add device tags
- Edit device tags
- Remove a device tag

## Device metadata

Metadata is unstructured information associated with a device, such as an informational note. Metadata can help to identify a device, find a device, or simply provide additional information about a device. It is searchable from the Remote Manager user interface.

- Add or edit device metadata

## 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.

After you have created a device group, you can add devices to the group.

1. Click **Device Management > Devices**.
2. Click the **Groups** button and select **Add Group**. The **Add Group** dialog appears.
3. Type a group name.
4. Choose the folder where you want to place the new group. The default is the root level.
5. Click the **Add Group** button. The group name appears in the folder structure under the root directory in the left pane.
6. Add devices to the group. See Add devices to a group.

## 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.

1. Create a device group. See Create device groups.
2. Click **Device Management > Devices**.
3. Select the device(s) you want to add to a group:
   - Click any device list item to select that device.
   - Use **Control-click** or **Shift-click** to select multiple devices or a range of devices.
4. Click **More > Assign to Group** from the Organize category. The **Add to Group** dialog appears.
5. Choose a device group from the drop-down list.
6. Click **Assign to Group**. The devices are added to the selected device group.

## Edit a device group

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

1. Click **Device Management > Devices**.
2. Click a group name in your list of device groups.
3. Click **Groups** and select **Edit Group** from the drop-down.
4. Make changes to the group name and location as needed.
5. Click **Edit Group** to confirm your changes.

## 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.

1. Click **Device Management > Devices**.
2. Select the device(s) you want to remove from a device group.
3. Click **More > Assign to Group** from the Organize category. The **Add to Group** dialog appears.
4. Choose the root folder or a device group from the drop-down list.
5. Click **Assign to Group**. The device is removed from the original device list.

## Remove a device group

Removing a device group removes the group itself and moves all devices in that group to the parent level in your device list.

1. Click **Device Management > Devices**.
2. Click to select the device group you want to remove from the device hierarchy in the left panel under Groups.
3. Click **Groups** and select **Remove Group** from the drop-down. A confirmation dialog appears asking you to confirm that you want to remove that group.
4. Click **Yes** to confirm. The group is deleted and any devices in that group move to the parent level in your device hierarchy.

## Show or hide device groups

You can choose to show or hide the list of device groups.

1. Click **Device Management > Devices**.
2. Click the **Show/Hide Groups** button on the far left side of the **Devices** toolbar. The Groups display will toggle to hidden or visible.

## Add 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.

1. Click **Device Management > Devices**.
2. Select the device you want to update.
3. Click **More > Edit Tags**. The **Edit Tags** dialog appears.
4. Enter the name of a tag in the text box and click **Add Tag**.
5. Click **Save**. The new tag is associated with the device.

## Edit device tags

You can change the name of a device tag.

1. Click **Device Management > Devices**.
2. Select the device you want to update.
3. Click **More > Edit Tags**. The **Edit Tags** dialog appears.
4. Click the tag name you want to edit. The tag name appears in the text box.
5. Edit the tag name as needed.
6. Click **Change Tag**.
7. Click **Save**. The updated tag is associated with the device.

### Remove a device tag

Remote Manager uses tags to categorize devices. You can remove a tag that has been assigned to a device.

1. Click **Device Management > Devices**.
2. Select the device that has a tag you want to update.
3. Click **More > Edit Tags**. The **Edit Tags** dialog appears.
4. In the **Tag Name** list, select the tag that you want to remove.
5. Click the red X icon in the **Action** column.
6. Click **Save** to complete the removal process.

### Add or edit device metadata

Metadata is unstructured information associated with a device, such as an informational note.

1. Click **Device Management > Devices**.
2. Select the device you want to update.
3. Click **More > Edit Metadata** in the Organize category. The **Edit Metadata** dialog appears.
4. Add or change the information in the text box and click **Save**.

## Add a descriptor

You can use a descriptor to customize how a device's settings are represented in Remote Manager.

**Note** Descriptors are intended to be used with a non-Digi device.

1. Click **Device Management > Devices**.
2. Click **More > Edit Descriptors**. The **UI Descriptors** page appears.
3. Click **Add**. The **Add UI Descriptor** dialog appears.
4. Enter a unique descriptor for a device in the field.
5. Click **Add**. The new descriptor is added to the list.

# Messaging

Remote Manager supports a number of messaging services. These services are useful for requesting connections to Remote Manager, sending data to and from devices, sending a command to a device, or sending a command line interface (CLI) command.

Remote Manager offers four messaging services:

- SMS messaging
- SM/UDP messaging
- Device messaging over an EDP connection. See Web Services Monitor and Web services messaging.

SMS and SM/UDP messaging all use the SMS protocol for sending and receiving messages to and from Remote Manager and your devices, while the web service uses web services Remote Manager calls.

## 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

These topics explain how 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 messaging

These topics explain how to configure SMS messaging.

## *Enable global cellular SMS*

Enable global cellular SMS prior to configuring SMS messaging on a device. Refresh the device properties before configuring SMS for that device.

1. Click **Device Management** > **Devices**.
2. Select a device.
3. Click **Properties**.
4. Click **+** next to **Advanced Configuration**.
5. Click **Cellular SMS**.
6. In the **Enable** field, select **On** by clicking the radio button.
7. Delete the password if one is shown. You can add a password in this field after SMS service is established.
8. Click **Save**.
9. After you have enabled SMS messaging, you should configure SMS messaging on the device. See Configure SMS messaging.

## *Configure SMS messaging*

Once global cellular SMS support has been enabled on a Remote Manager account, or a device has been set to send and receive standard SMS messages, configure the device to enable Remote Manager SMS messaging.

1. Click **Device Management** > **Devices**.
2. Select a device.
3. Click **Properties**.
4. Click **+** next to **Advanced Configuration** and click **Product Manager SMS**.
5. Configure the following settings.
   - **SMS Enable**: On
   - **Server Phone Number**: no value
   - **Server Service Identifier**: no value
   - **Restrict Sender to only iDigi Server Phone Number**: Off

   **Note** For detailed information about these options, you should refer to the documentation for the device you are configuring.
6. Click **Save**.
7. Click **Refresh** to display the most recent device information.

## *Configure device phone number*

Typically, the device phone number is automatically configured when the device first connects to Remote Manager. If the device was automatically configured, all of the options within the SMS

category of the **More** menu are enabled. If only the **Configure** option within the SMS category of the **More** menu is available, you must manually configure the telephone number for the device.

1. Navigate to your device's local UI. Click **Configuration** > **Mobile** and ensure global SMS capabilities are enabled.
2. Within the **SMS Settings** section, ensure that the box next to **Enable cellular Short Message Service (SMS) capabilities** is checked.
3. Under **Built-In Command Settings**, verify the checkbox next to **#ping** is checked and the password field is blank.
4. Return to Remote Manager.
5. Click **Device Management** > **Devices**.
6. Select a device.
7. Click **Properties**.
8. Click **+** next to System Information and click **Mobile**.
9. Make note of the device ICCID and phone number.
10. Click the **Devices** tab.
11. Click **More** in the Device toolbar.
12. Select **SMS** > **Configure**. The **SMS Configuration** dialog appears.
13. Enter the device phone number and ICCID in the appropriate fields for **SIM 1**.
14. Click **Save**. The **SMS Configuration** dialog closes and the **Devices** page is refreshed.
15. Verify that the device is still selected in the Devices list and click **More**. Additional options within the SMS category of the **More** menu should now be available.
16. Click **Provision**. The **SMS Provision** dialog appears.
17. Click the **Request response** check box, and click **OK** to complete the device configuration. This populates all fields necessary for SMS communication that may have been left blank. It also overwrites incorrect data within all fields.
18. Click **OK** to confirm.
19. Confirm configuration settings by pinging the device using an SMS message from Remote Manager.

### *Request SMS provision response*

The Provision command sends a special **config** command to the device via SMS that sets the Remote Manager server phone number and service ID, and configures all options necessary for SMS communication. Prior to sending the command, use the device's local web UI or Remote Manager to enable global SMS and Remote Manager SMS.

If you select the **Request response** option, Remote Manager generates a success or failure response message.

**Note** If you configured your device to have "restrict sender" turned off, provisioning will not work because the device will not honor any requests except those coming from the configured Remote Manager phone number/service ID.

1. Click **Device Management** > **Devices.**
2. Select an SMS-capable device.
3. Click the **More** button, then click **Provision** in the SMS category. The **SMS Provision** dialog appears.
4. Verify that the **Request Response** box is checked.
5. Click **OK**.
6. If provisioning is successful, Remote Manager displays the **SMS provision complete** dialog.

### Send a message via SMS

If you have configured SMS support and cellular service for a device, you can send SMS messages between Remote Manager and the device.

1. Click **Device Management > Devices**.
2. Select the device to send the SMS message.
3. Click the **More** button, then select **Send Message** from the SMS category. The **Send Message** dialog appears.
4. Select a message to send. For each option, you can select the **Request Response** option if you want to receive a response from the device.
   - **Ping:** Pings the device via SMS to determine whether the device can receive SMS messages.
   - **Request Connect:** Request a Remote Manager data connection. If a connection has already been made, forces a reconnect.
   - **Reboot:** Reboots the device immediately.
   - **CLI:** Sends a command. The following options must be specified:
     - **Command**: Enter the CLI command.
     - **Max response length**: Specify the number of response messages that you want to receive from the list box.
5. Click the gear icon to schedule the message: **Immediate**, **One-time**, or **Recurring**.
6. Click **Send**.

## 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.

# SM/UDP messaging concepts

These topics explain how SM/UDP messaging uses various concepts and features.

## *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, 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 messaging

These topics explain how to configure SM/UDP messaging.

## *Enable SM/UDP*

You can use the SM/UDP feature to leverage the very small data footprint of Remote Manager SM protocol over UDP.

1. Click **Device Management > Devices**.
2. Select a device from the devices list. The **More** button appears in the toolbar.
3. Click **More**. The **More** menu appears.
4. Under SM/UDP, click **Configure**. The **SM/UDP** dialog appears.
5. Determine whether battery-operated mode should be enabled. Select **Battery Operated Mode** option to enable battery-operated mode.

   See Battery-operated mode with SM/UDP for more information.
6. Select **SM/UDP Service Enabled** to enable SM/UDP.
7. Click **Save**.

### *Disable SM/UDP*

You can disable the SM/UDP feature at any time.

1. Click **Device Management > Devices**.
2. Select your device.
3. Click **More**. The **More** menu appears.
4. Under SM/UDP, click **Configure**. The **SM/UDP** dialog appears.
5. Deselect **Battery Operated Mode** option to disable battery-operated mode.
6. Deselect **SM/UDP Service Enabled**.
7. Click **Save**.

### *Configure paged connections*

Before you can send a Request Connect message to a device, you must configure paged connections on that device.

1. Click **Device Management > Devices**.
2. Double-click your device to view its properties page.
3. Expand **Advanced Configuration > Remote management connection** in the navigation pane. The list of remote management connections appears.
4. Select a remote management connection. The profile appears in the main pane. Note that the connection type is different for each connection profile:
   - Remote management connection 1: Client initiated - Always connected
   - Remote management connection 2: Client initiated - Timed connection
   - Remote management connection 3: Server initiated
   - Remote management connection 4: Client initiated - Always connected
5. Complete all fields in the pane:
   - Select **On** or **Off** to enable or disable this connection profile.
   - Set the timed connection period.
   - Set the timed connection offset from its drop-down menu.
     - Immediate
     - onePeriod
     - randomTime
   - Select **On** or **Off** to enable or disable the last known address update.
   - Choose whether you want Remote Manager to reconnect if the connection times out. If enabled, set the time.
     - Select one of the server lists. The drop-down menu appears.
     - Under Server address, type the web address to which you want your device to connect (https://remotemanager.digi.com).
6. Click **Refresh**.

### *Connect a device via SM/UDP*

You can send a connection request to a device via SM/UDP (Short Message/User Datagram Protocol). You must first configure the device for SM/UDP support.

1. Click **Device Management > Devices**.
2. Select a device that you want to connect.
3. Click **More > Send Message** from the SM/UDP category. The **Send Message** dialog appears.
4. Click **Request Connect** from the drop-down menu. The **SM/UDP Request Connect** dialog appears.
5. Check **Request Response** if you want to receive a success or failure message from the device.
6. Click **Send**. A dialog appears showing the progress of the connection request message. When complete, the device will receive an SM/UDP message instructing it to establish an EDP connection with Remote Manager.

To see the most updated status for your device, click the circular refresh button.

**Note** A device connected via SM/UDP may not disconnect automatically. In this case, manually disconnect the device.

## Send CLI commands over SM/UDP

The **Command Line** command sends CLI commands via SM/UDP. These requests remain queued until an SM/UDP message is sent from the device to Remote Manager. Then Remote Manager sends the queued CLI command to the device. If the response to the command is close to 140 characters, Remote Manager will break it into multiple messages and reassemble them in proper order before displaying the data.

To send an SM/UDP CLI command:

1. Click **Device Management > Devices**.
2. Select the device you want to set up for SM/UDP.
3. Click **More**. The **More** menu appears.
4. Under the **SM/UDP** heading, click **Send Message**. The **Send Message** dialog appears.
5. Select **CLI**. The **SM/UDP CLI** dialog appears.
   - Type the command you want to send.
   - Select the maximum number of messages allowed.
   - If you don't want a reply, deselect the **Request Response** check box.
6. Click **Send**. The **SM/UDP CLI** complete dialog appears to confirm success.

## Send an SM/UDP Reboot message

The Reboot command reboots the device immediately.

1. Click **Device Management > Devices**.
2. Select the device you want to set up for SM/UDP. The **More** button appears in the toolbar.
3. Click **More**. The **More** menu appears.
4. Under the SM/UDP heading, click **Send Message**. The **Send Message** dialog appears.

5. Select **Reboot**. The **SM/UDP Reboot** dialog appears.
6. If you want to receive a reply from the device when it is rebooted, select the the **Request Response** check box. Deselect this option if you don't want to receive a reply.
7. Click **Send**.

# Web services messaging

Remote Manager web services messaging allows you to send messages between Remote Manager client applications and Remote Manager via web services Remote Manager calls.

To use web services messaging, you must have an account type that includes this service. Without this subscription, a web service message call will result in an authorization error.

For more information on web services messaging see the Web Services messaging section of the *Remote Manager Programmer Guide*.

# Web Services Monitor

The Web Services Monitor API allows you to set up, modify, and delete push notifications to your TCP or HTTP application in order to provide data and status reports based on user-defined conditions. For example, if you are monitoring DeviceCore and a new device was added to your Remote Manager account, Remote Manager would push a DeviceCore CREATE message with the new device information. The Web Services Monitor is also called Push Monitoring in the user interface.

For more information, see the Web Services Monitor section in the *Remote Manager Programmer Guide*.

# XBee networks

The XBee Networks tab under Device Management gives you access to all the XBee nodes in your device inventory. Click **Device Management > XBee Networks** to view the list of XBee nodes.

From the XBee Networks pane, you can perform the following tasks:

- Discover an XBee device
- Configure XBee node properties
- Export a list of XBee nodes to Excel
- Click the **Refresh** icon in the toolbar to refresh the list of devices on any XBee network

For detailed information about the XBee network views, see:

- Device management > XBee networks view
- Device management > XBee networks > XBee network properties view

## XBee Smart Energy management service

The XBee Smart Energy management service enables Smart Energy support in your Remote Manager account. The Smart Energy service allows data sent and received from the device to be interpreted using the Smart Energy Profile standards.

## Discover an XBee device

This command instructs an XBee device to search for all nodes on its network. If you select an XBee end node, the request is sent to the end node's gateway instead. By default, this button is hidden from view within the toolbar until an XBee device is selected within your XBee Node list.

1. Click **Device Management > XBee Networks**.
2. Select an XBee device from the devices list. The **Discover** button appears.
3. Click **Discover**. The **Discover** dialog appears.
4. Select the **Clear the cache on the device and perform a full rediscover** option to perform this action.
5. You can schedule when you want the discovery process to occur. Click the gear icon to display the schedule options. See Schedule an action for detailed information about the schedule options.
6. Click **Discover**. A progress dialog appears, and Remote Manager briefly displays a confirmation dialog when the process is complete.

# Configure XBee node properties

The XBee properties pane allows you to view and configure an XBee node's basic and advanced properties.

1. Click **Device Management > XBee Networks**.
2. Select an XBee device from the devices list. The **Properties** button appears.
3. Click **Properties**. The **Properties** pane appears in a separate tab labeled with the extended address and node identifier of the XBee device.
4. Edit any fields in the pane. For detailed information about each of the fields, refer to the documentation for the selected XBee module.
    - Click **Basic** to edit the basic properties of the device, such as the plain text node identifier.
    - Click **Advanced** to edit the advanced properties of the device, such as higher-level encryption.
5. Click **Refresh**.

# Export a list of XBee nodes to Excel

Remote Manager can export a list of the XBee nodes to an Excel file.

1. Click **Device Management > XBee Networks**.
2. Click **Export Networks**. An Excel spreadsheet is generated and the file is saved to your Downloads folder.
3. Click the downloaded spreadsheet to open it in Excel.

# Alarms

Within Remote Manager, you can create alarms to monitor various activities of the devices in Remote Manager. In the Alarms page, you can configure and manage alarms, and react to alarm conditions.

When the alarm fires, the alarm status will change to Fired in the alarm list. If you have set up email notification, you will receive an email.

From the Alarms pane, you can perform the following tasks:

- Create an alarm
- Manage alarm events
- Configure email notifications for an alarm

## Create an alarm

Alarms send notifications when certain events occur, such as when a device is disconnected.

1. Click **Device Management > Alarms**.
2. Click **Add**. The **Add Alarm** dialog appears.
3. From the **Alarm Type** drop-down, choose the alarm type from the options in the drop-down list. Note that this selection affects options available from this dialog. Options are:
    - DataPoint Condition
    - Device Excessive Disconnects
    - Device Offline
    - DIA channel DataPoint condition match
    - Missing DataPoint
    - Missing DIA channel DataPoint
    - Missing Smart Energy DataPoint
    - Smart Energy DataPoint Condition Match
    - Subscription Usage
    - XBee Node Excessive Deactivations
    - XBee Node Offline
4. From the **Severity** drop-down, select a severity rating for an alarm, based on the importance of that alarm.
5. In the **Name** field, enter a descriptive name for the alarm.

6. In the **Description** field, enter a detailed description of the alarm.
7. Set the conditions that must be met for the alarm to fire. The fields are related to the alarm type you selected.
8. Click **Create**.
9. You should configure the alarm notification to ensure that an alarm notification is received if it is fired. See Create an alarm notification.

## DataPoint condition alarm

This alarm 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.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **DataPoint Condition** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. |

The **Reset Condition** section contains the conditions that must be met for the alarm to reset.

| Field | Description |
|---|---|
| **Reset Condition** | Determines whether the alarm should be automatically reset after an alarm has been fired. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. |

In the **DataPoint** field, you must also 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, "dia/channel/*/lth/temp" matches the lth temperature reading for any device.

## Device excessive disconnects alarm

This alarm fires when a device disconnects from Remote Manager too often.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Device excessive disconnects** option for these fields to appear in the dialog.

| Field | Description |
|---|---|
| **Device disconnects more than <x> times in <x> minutes** | Enter the maximum number of disconnects allowed during the specified time period. The time is measured in minutes. The default is 5 minutes. |
| **Resets when device reconnects and stays connected for <x> minutes** | Specify whether the alarm should automatically reset if the device is connected and remains connected for the specified time period. The time is measured in minutes. Options are:<br>■ **Selected**: The alarm is automatically reset. This is the default.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset the alarm each time it fires. See Reset an alarm. |
| **Scope** | Specify the devices that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected. |

## Device offline alarm

This alarm fires when a device disconnects from Remote Manager and does not reconnect within a specified time.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Device offline alarm** option for these fields to appear in the dialog.

| Field | Description |
|---|---|
| **Fires when device does not reconnect within <x> minutes** | Enter the maximum length of time a device can remain unconnected. The time is measured in minutes. The default is 5 minutes. |
| **Resets when device reconnects** | Specify whether the alarm should automatically reset if the device reconnects. Options are:<br>■ **Selected**: The alarm is automatically reset. This is the default.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset the alarm each time it fires. See Reset an alarm. |
| **Scope** | Specify the devices that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected. |

## DIA channel data point condition match alarm

This alarm fires when a DIA channel condition matches a selected value.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **DIA channel data point condition match** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Dia instance** | Select the DIA instance from the options in the drop-down list. To set the alarm to fire on all DIA instances, select *. |
| **Channel** | Select the DIA channel from the options in the drop-down list. To set the alarm to fire on all DIA channels, select *. |
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. The default is 10 seconds. |

The **Reset Condition** section contains the conditions that must be met for the alarm to reset.

| Field | Description |
|---|---|
| **Reset Condition** | Determines whether the alarm should be automatically reset after an alarm has been fired. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |
| **Dia instance** | Select the DIA instance from the options in the drop-down list. To set the alarm to fire on all DIA instances, select *. |
| **Channel** | Select the DIA channel from the options in the drop-down list. To set the alarm to fire on all DIA channels, select *. |
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. |

Click **Next** to specify the scope for the alarm.

| Field | Description |
|---|---|
| **Scope** | Specify the devices that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected. |

## Missing datapoint alarm

This alarm fires when a data point is not reported within the specified time.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Missing DataPoint** option for these fields to appear in the dialog.

| Field | Description |
|---|---|
| **Fires when the time interval between datapoint uploads to the server exceeds <*time*> or when the time interval between reported datapoints exceeds <*time*>** | Enter the time threshold intervals to determine when an alarm should fire:<br>■ Time interval between datapoint uploads to the server exceeds the specified time limit. The default is 1 hour.<br>■ Time interval between reported datapoints from the device exceeds the specified time limit. The default is 10 minutes. |
| **Resets when data is reported** | Specify whether the alarm should automatically reset when the data is uploaded to the server. Options are:<br>■ **Selected**: The alarm is automatically reset. This is the default.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset the alarm each time it fires. See Reset an alarm. |
| **Scope** | In the **DataPoint** field, you must also 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, "dia/channel/*/lth/temp" matches the lth temperature reading for any device. |

## Missing DIA channel datapoint alarm

This alarm fires when devices have not reported DIA channel data within a specified time interval.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Missing DIA Channel DataPoint** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Dia instance** | Select the DIA instance from the options in the drop-down list. To set the alarm to fire on all DIA instances, select *. |
| **Channel** | Select the DIA channel from the options in the drop-down list. To set the alarm to fire on all DIA channels, select *. |
| **Upload interval** | Specify the time interval between datapoint uploads to the server. The default is 1 hour. |
| **Reading interval** | Specify the time interval between reported datapoints from the device. The default is 10 minutes. |

| Field | Description |
|---|---|
| **Reset Condition** | Determines whether the alarm should be automatically reset after data has been reported. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |

Click **Next** to specify the scope for the alarm.

| Field | Description |
|---|---|
| **Scope** | Specify the devices that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected. |

## Missing Smart Energy datapoint alarm

This alarm fires when devices have not reported Smart Energy data within a specified time interval.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Missing Smart Energy DataPoint** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Endpoint ID** | Select the endpoint ID from the options in the drop-down list. To set the alarm to fire on all endpoint ID, select *. |
| **Cluster Type** | Select the cluster type from the options in the drop-down list. To set the alarm to fire on all cluster type, select *. |
| **Cluster ID** | Select the cluster ID from the options in the drop-down list. To set the alarm to fire on all cluster IDs, select *. |
| **Attribute ID** | Select the attribute ID from the options in the drop-down list. To set the alarm to fire on all attribute IDs, select *. |
| **Upload interval** | Specify the time interval between datapoint uploads to the server. The default is 1 hour. |

| Field | Description |
|---|---|
| **Reading interval** | Specify the time interval between reported datapoints from the device. The default is 10 minutes. |
| **Reset Condition** | Determines whether the alarm should be automatically reset after data has been reported. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |

Click **Next** to specify the scope for the alarm.

| Field | Description |
|---|---|
| **Scope** | Specify the devices or node that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected.<br>■ **XBeeNode**: Select the **XBeeNode** option to display a list of the XBee nodes registered in Remote Manager. Click the node that you want to monitor. Only one node can be selected. |

## Smart Energy datapoint condition match alarm

This alarm fires when a Smart Energy datapoint condition matches a specific value or condition.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Missing Smart Energy DataPoint** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Endpoint ID** | Select the endpoint ID from the options in the drop-down list. To set the alarm to fire on all endpoint IDs, select *. |
| **Cluster Type** | Select the cluster type from the options in the drop-down list. To set the alarm to fire on all cluster types, select *. |

| Field | Description |
|---|---|
| **Cluster ID** | Select the cluster ID from the options in the drop-down list. To set the alarm to fire on all cluster IDs, select *. |
| **Attribute ID** | Select the attribute ID from the options in the drop-down list. To set the alarm to fire on all attribute IDs, select *. |
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. The default is 10 seconds. |

The **Reset Condition** section contains the conditions that must be met for the alarm to reset.

| Field | Description |
|---|---|
| **Reset Condition** | Determines whether the alarm should be automatically reset after an alarm has been fired. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |
| **Endpoint ID** | Select the endpoint ID from the options in the drop-down list. To set the alarm to fire on all endpoint IDs, select *. |
| **Cluster Type** | Select the cluster type from the options in the drop-down list. To set the alarm to fire on all cluster types, select *. |
| **Cluster ID** | Select the cluster ID from the options in the drop-down list. To set the alarm to fire on all cluster IDs, select *. |
| **Attribute ID** | Select the attribute ID from the options in the drop-down list. To set the alarm to fire on all attribute IDs, select *. |
| **Type** | Select the condition type. Options are NUMERIC or STRING. |
| **Condition** | Select the conditional operator, which is used to compare the data to the alarm value. |
| **Value** | Enter the threshold value that should be compared to the actual datapoint value from the device. |
| **Timeout** | Enter the length of time and the corresponding time unit that must be met before the alarm times out. |

Click **Next** to specify the scope for the alarm.

| Field | Description |
|---|---|
| **Scope** | Specify the devices or node that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected.<br>■ **XBeeNode**: Select the **XBeeNode** option to display a list of the XBee nodes registered in Remote Manager. Click the node that you want to monitor. Only one node can be selected. |

## Subscription usage alarm

This alarm fires when your subscription usage exceeds a specific threshold.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **Subscription Usage** option for these fields to appear in the dialog.

The **Fire Condition** section contains the conditions that must be met for the alarm to fire.

| Field | Description |
|---|---|
| **Service** | Select the service you are using. |
| **Metric** | Select the metric you want to use to measure subscription usage. Options are SIZE or MESSAGES. |
| **Exceeds** | Enter the threshold for the service usage. The value can be measured in KB, MB, or GB. |

The **Reset Condition** section contains the conditions that must be met for the alarm to reset.

| Field | Description |
|---|---|
| **Reset Condition** | Determines whether the alarm should be automatically reset when the usage value goes below the specified usage threshold. Options are:<br>■ **Selected**: The alarm is automatically reset.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset this alarm. See Reset an alarm. |

Click **Next** to specify the scope for the alarm.

| Field | Description |
|---|---|
| **Scope** | Specify the devices that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click on the device that you want to monitor. Only one device can be selected. |

## XBee node excessive deactivations alarm

This alarm fires when it detects an XBee node with an excessive number of deactivations.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **XBeeNode Excessive Deactivations** option for these fields to appear in the dialog.

| Field | Description |
|---|---|
| **XBee node goes inactive more than <x> times in <x> minutes** | Enter the maximum number of times the node can be inactive during the specified time period. The time is measured in minutes. The default is 60 minutes. |
| **Resets when XBee node activates and stays activated for <x> minutes** | Specify whether the alarm should automatically reset if the XBee node activates and remains activated for the specified time period. The time is measured in minutes. The default is 15 minutes. Options are:<br>■ **Selected**: The alarm is automatically reset. This is the default.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset the alarm each time it fires. See Reset an alarm. |

| Field | Description |
|---|---|
| **Scope** | Specify the devices or node that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected.<br>■ **XBeeNode**: Select the **XBeeNode** option to display a list of the XBee nodes registered in Remote Manager. Click the node that you want to monitor. Only one node can be selected. |

## XBee node offline alarm

This alarm fires when it detects that an XBee node has disconnected from Remote Manager and does not reconnect within a specific time interval.

From the **Alarm Type** drop-down in the **Add Alarm** dialog, select the **XBeeNode Offline** option for these fields to appear in the dialog.

| Field | Description |
|---|---|
| **Fires when XBee nodes to not reconnect within <x> minutes** | Enter the maximum length of time an XBee node can remain unconnected. The time is measured in minutes. The default is 5 minutes. |
| **Resets when node reconnects** | Specify whether the alarm should automatically reset if the XBee node reconnects. Options are:<br>■ **Selected**: The alarm is automatically reset. This is the default.<br>■ **Deselected**: The alarm is not automatically reset. You must manually reset the alarm each time it fires. See Reset an alarm. |

| Field | Description |
|---|---|
| **Scope** | Specify the devices or node that should be monitored for this alarm. Options are:<br>■ **Group**: Select the **Group** option and then select a device group. All of the devices in that group are monitored. Only one group can be selected.<br>■ **Device**: Select the **Device** option to display a list of all of the devices registered in Remote Manager. Click the device that you want to monitor. Only one device can be selected.<br>■ **XBeeNode**: Select the **XBeeNode** option to display a list of the XBee nodes registered in Remote Manager. Click the node that you want to monitor. Only one node can be selected. |

# Manage alarm events

This section describes how to manage alarm events and edit alarm configuration.

## Acknowledge an alarm

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

1. Click **Device Management > Alarms**.
2. Double-click an alarm in the list. The alarm status history tab opens.
3. Select an alarm event from the list. The **Acknowledge** button appears in the toolbar.
4. Click **Acknowledge**. Remote Manager briefly displays a confirmation of the acknowledgment.
5. Information about an alarm that you have acknowledged appears in the screen only if the alarm list has not been filtered.
    a. Click the **Filter** button to display the filter options.
    b. Deselect the **Hide acknowledged alarms** option to display the alarms that have been acknowledged.

## Reset an alarm

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

**Note** You can only reset the alarms that you have added. You cannot reset alarms that were added by another user.

1. Click **Device Management > Alarms**.
2. Double-click an alarm in the list. The alarm status history tab opens.
3. Select an alarm event from the list. The **Reset** button appears in the toolbar.
4. Click **Reset**. Remote Manager briefly displays a confirmation of the reset. The alarm is now actively monitoring its conditions and is ready to fire.
5. Information about an alarm that you have reset appears in the screen only if the alarm list has not been filtered.
    a. Click the **Filter** button to display the filter options.
    b. Deselect the **Hide reset alarms** option to display the alarms that have been reset.

## Edit an alarm configuration

You can update an alarm's configuration as needed.

**Note** You can only edit the alarms that you have added. You cannot edit alarms that were added by another user.

1. Click **Device Management > Alarms**.
2. Select the alarm you want to edit. The **Edit** button appears in the toolbar.
3. Click **Edit**. The **Edit Alarm** dialog displays the current configuration of the selected alarm.
4. In the alarm options portion of the dialog, modify the frequency settings.
5. In the alarm scope selection portion of the dialog, modify the scope.

    **Note** For some alarm types, you need to click **Next>>** to display alarm scope options.

6. Click **Update** to save your changes.

## View alarm status

The alarm status describes the current state of an alarm. Options are:

- **Normal**: No devices have met any of the conditions set in this alarm.
- **Fired**: One or more devices have been triggered by one or more conditions set in this alarm. The number next to the **Fired** status indicates the number of devices that have triggered the alarm.

For more information about the information on this page, see Device management > Alarms > Alarm status view.

1. Click **Device Management > Alarms**.
2. Select an alarm from the list, or shift-click to select multiple alarms.
3. Click **Alarm Status**. The **Alarm Status** page displays, and shows detailed information about the alarm.

4. You can use the filter icon  to show or hide the reset or acknowledged events.

   Both options are selected by default:
   - **Hide reset alarms:**: Hides reset alarms.
   - **Hide acknowledged alarms:**: Hides acknowledged alarms.
5. You can also view historical alarm status information. See View the status history of an alarm.

## View the status history of an alarm

You can create alarms to fire when certain events occur, such as when a device is disconnected. By default, only active alarm status information is displayed in the Alarm Status page. However, you can view historical alarm status events by selecting the **Show History** option.

1. Click **Device Management > Alarms**.
2. Select your alarm from the alarms list, or shift-click to select multiple alarms.
3. Click **Alarm Status**. The **Alarm Status** page appears.
4. Select the **Show History** option in the toolbar. Remote Manager displays detailed alarm status history for the selected alarm(s). Alarm status history is sorted from newest to oldest.

## Refresh alarms list

You can create alarms to send notifications when certain events occur. The list does not update automatically, so you may need to refresh the list to view changes.

1. Select **Device Management > Alarms**.
2. Click the **Refresh** icon.

## Enable or disable an alarm

You can disable an alarm if you no longer want Remote Manager to monitor a device or an XBee node. This feature is useful if you want to control when an alarm is in use instead of deleting it. After an alarm has been disabled, you can enable the alarm at any time.

The enabled or disabled status of the alarm displays in the **Enabled** column in the **Alarms** page.

If you want to delete an alarm permanently, see Delete an alarm.

**Note** You can only enable or disable the alarms that you have added. You cannot enable or disable alarms that were added by another user.

1. Click **Device Management > Alarms**.
2. Select the alarm you want to control. The **Enable/Disable Alarm** button appears in the toolbar.
3. Click **Enable/Disable Alarm**. A drop-down menu appears.
   - Select **Enable** to begin monitoring the conditions in that alarm. The status "Enabled" displays in the **Enabled** column.
   - Select **Disable** to stop monitoring the conditions in that alarm. The status "Disabled" displays in the **Enabled** column.

### Delete an alarm

You can delete an alarm that is no longer needed. Confirmation is not required to delete an alarm. When you click **Remove**, Remote Manager briefly displays an indicator at the top of the banner and then deletes the alarm.

**Note** You can only delete the alarms that you have added. You cannot delete alarms that were added by another user.

**Note** You can also disable an alarm and stop alarm monitoring without deleting the alarm. See Enable or disable an alarm.

1. Click **Device Management > Alarms**.
2. From the alarm list, select the alarm or alarms to delete. The **Remove** button appears in the toolbar.
3. Click **Remove**.

## Configure email notifications for an alarm

Remote Manager can send email notifications when an alarm is triggered. You can configure the name, email addresses for the notification recipients, frequency of notifications, and notification scope.

- Create an alarm notification

You can also edit and delete an alarm notification after it has been created.

- Edit an alarm notification
- Delete an alarm notification

**Note** You must have previously created an alarm before you can create an alarm notification for a user account. See Create an alarm.

### Create an alarm notification

You can create an alarm notification that sends an email to a specified email address when an alarm fires or is reset.

1. Click **Admin > Account Settings > Notifications**.
2. Click **Add**.
3. In the **Name** field, enter a descriptive name for the alarm.
4. In the **Description** field, enter a description of the alarm notification.
5. In the **Send Email to** field, enter the email address you want to receive the notification. More than one email address can be entered. The addresses must be separated by a comma.
6. Designate the notification frequency. Both options are enabled by default.
   - **Send daily summary reports at**: Send a daily summary at the time specified.
   - **Send notifications for each alarm event**: Send a notification for each alarm event when it occurs.

7. Specify whether you want to receive notifications for a set of alarms or for alarms scoped to a group. You can only select one option.
   - **Send notification for the following alarms**
     a. Select the **Send notification for the following alarms** option.
     b. Begin typing the name of the alarm. Remote Manager automatically searches and displays a list of matching alarms.
     c. Click the desired alarm in the list. The alarm is added to the field.
     d. Repeat the process to add additional alarms.
   - **Send notification for alarms scoped to the following groups**
     a. Select the **Send notification for alarms scoped to the following groups** option.
     b. Begin typing the name of the group. Remote Manager will begin searching automatically and will display a list of matching groups.
     c. Click a group in the list. The group is added to the field.
     d. Repeat the process to add additional group.
8. Click **Save**. The alarm is now enabled and active.

## Edit an alarm notification

You can change the frequency and scope of emails sent when an alarm fires or is reset.

1. Click **Admin > Account Settings > Notifications**.
2. Select a notification process from the list. The current configuration appears.
3. Edit the fields to change the configuration.
4. Click **Save**.

## Enable or disable an alarm notification

If you no longer want Remote Manager to send an alarm notification, you can disable it. This feature is useful if you want to control when an alarm notification is in use, rather than deleting it. You can enable a disabled alarm notification at any time.

The enabled or disabled status displays in the **Status** column in the Admin Notifications page.

If you want to delete an alarm notification permanently, see Delete an alarm notification.

1. Click **Admin > Account Settings > Notifications**.
2. Select the alarm notification you want to control. The **Enable/Disable Alarm** button appears in the toolbar.
3. Click **Enable/Disable Alarm**. A drop-down menu appears.
   - Select **Enable** to send an email alarm notification. A green icon with a white checkmark appears in the **Status** column.
   - Select **Disable** to stop sending an email alarm notification. A red icon appears in the **Status** column.

## Delete an alarm notification

If you want to stop receiving emails when an alarm fires or is reset, you can delete that notification process.

**Note** You can also disable an alarm and stop alarm notifications without deleting the alarm. See Enable or disable an alarm notification.

1. Click **Admin > Account Settings > Notifications**.
2. Select the notification process in the list. The **Remove** button appears in the toolbar.
3. Click **Remove**. The notification process disappears from the list, and notification emails associated with that alarm will no longer be sent.

# Schedules and tasks

You can use Remote Manager schedules to perform common management tasks on one device or a group of devices. These tasks include updating device firmware, rebooting a device, and uploading, retrieving, or deleting files. Schedules can be run once or configured to recur periodically. See About schedules and tasks.

From the Schedules pane, you can perform the following tasks:

- Create a schedule
- Edit a schedule
- Delete a schedule
- Disable a schedule
- Enable a schedule
- Schedule frequency
- Create a My Task option
- Run My Task device tasks

## About schedules and tasks

You can use Remote Manager schedules to perform common management tasks on one device or a group of devices. These tasks include updating device firmware, rebooting a device, and uploading, retrieving, or deleting files. Schedules can be run once or configured to recur periodically.

Multiple tasks can be added to a schedule, and you can remove tasks from a schedule if the task is no longer needed. If you schedule a series of tasks for the same device, one job does not start until the previous job in the series has been completed.

The My Task feature enables you to create and save a schedule with tasks that you can re-use. See Create a My Task option.

The Schedules feature consists of the following:

- **Task templates:** A task template is the framework of a schedule. The template specifies each management command associated with a particular schedule.
- **Schedules:** A schedule specifies when the chosen commands, as outlined in the task template, will be executed, and which device(s) will be targeted.

- **Tasks:** A task is the execution of one or more commands chained together in a task template. When Remote Manager executes a task, each command within the task is executed as a job and each job is assigned a system-generated ID. You can cite the task ID to query the overall status of the task, to cancel the task, or to delete the task. You can cite the job ID to find status for a specific command.

  Once a scheduled task has been created, you can:
  - Embed a task element as part of the request payload for the Schedules web service.
  - Upload an XML file that contains a task definition to the **my_tasks** folder within your Remote Manager account.

  A task spawned by scheduled operations automatically times out after four days.

# Create a schedule

Create a new schedule when you want to assign tasks to be performed on selected devices at a scheduled date and time.

For information about the **New Schedule** dialog and how to manage the tasks in the commands screen, see New Schedule dialog.

1. Click **Device Management > Schedules**.
2. Click **New Schedule**. The **New Schedule** dialog appears.
3. In the **Description** field, enter a descriptive name for the schedule.
4. Select the device type and the action on that device that you would like to perform. The links below lead to detailed information about the command information you need to enter.
   - Device: Select the **Device** option to a select task that can be performed on a device.
   - XBee: Select the **XBee** option to select the XBee device discovery task.
   - SMS: Select the **SMS** option to select a task that can be performed on a device that uses SMS messaging.
   - Satellite: Select the **Satellite** option to select a task that can be performed on a device that uses Satellite messaging.
   - SM/UDP: Select the **SM/UDP** option to select a task that can be performed on a device that uses SM/UDP messaging.
   - My Tasks: Select the **My Task** option to create a schedule with tasks that you can repeat for different devices.
   - **Public Tasks**: Select the **Public Tasks** option to create a schedule with tasks that have been supplied by Digi. You cannot add to or update the tasks in this list. However, you can update any Public Tasks that you add to a schedule.
5. Click the **On Error** drop-down list to specify the action that should be taken when the action ends in an error: **End Task**, **Continue**, or **Retry**.

6. Click the **On End** drop-down list to specify the action that should be taken when the task ends. Options are:
   - Nothing: Do not select the **Sleep** option. The device status is not changed.
   - **Sleep**: Select the **Sleep** option if the device should go to sleep after the action has been performed.
7. Select the **Allow Offline** option if the action should be taken even if the device is offline.

   **Note** This option is not available for all device type selections.

8. Repeat steps 4 through 7 to add additional tasks to the schedule.
9. Click **Schedule >>** to schedule the task(s) and select a device.
   a. Use the options in the **One Time** and **Recurring** tabs to schedule the tasks. See Schedule frequency for details about these options.
   b. Select a device from the list. Use the **SHIFT** and **CTRL** keyboard buttons to select additional devices.
10. Save or run the schedule.
    - Click **Schedule** to save the schedule.
    - If you chose the **Immediate** scheduling option, the **Schedule** button is not available. Click **Run Now** to run the schedule. The schedule is not saved.

## Add a device task

You can add device commands to schedule tasks to occur on a selected device.

For many of these options, you can specify the path and file name for the firmware file that you want to upload to the selected devices using one of the following options:

- **File field**: Manually enter a path and file name in the **File** field.
- **Browse**: Browse for the path and file name. The selected path displays in the **File** field.
- **Reference**: Select a file that is stored in Remote Manager. Click **Reference** to display a dialog. You can select a file from the list, or limit the list by entering a folder name in the search field. The selected path displays in the **File** field. The files in this list can be viewed in detail in the **Data Files** page. See Data services.

See Create a schedule for details about adding a task to a schedule.

### *Device > Reboot command*

This command reboots the selected devices.

| Option | Description |
|---|---|
| Wait for Reconnect | Associate completion status with device reconnection. |

### *Device > Gateway Firmware Update command*

This command updates the firmware on the selected devices.

| Option | Description |
|---|---|
| File | In the **File** field, enter the path and file name for the firmware file that you want to upload to the selected devices. |
| Browse | Click **Browse** to browse for and select the firmware file. |
| Reference | Click **Reference** to select a file that is stored in Remote Manager. |
| Wait for Reconnect | Associate completion status with device reconnection. |

### *Device > RCI Command*

This command sends an RCI request to the selected devices.

| Option | Description |
|---|---|
| Embed | Click **Embed** to enter RCI code. A code sample appears, and you can edit the code as needed. |
| File | Click **File** to enter or browse for a file containing RCI code. |
| File | In the **File** field, enter the path and file name for the RCI code request file. |
| Browse | Click **Browse** to browse for and select the RCI code request file. |
| Reference | Click **Reference** to select a file that is stored in Remote Manager. |
| Use Remote Manager Cache | Only applicable for cached data associated with a command, such as a query setting or query state. Uses the RM cached version of the settings. |

### *Device > Upload Python Files command*

This command uploads Python application and data files to the selected devices.

| Option | Description |
|---|---|
| File | In the **File** field, enter the path and file name for the Python file that you want to upload on the selected devices. |
| Browse | Click **Browse** to browse for and select the Python file. |
| Reference | Click **Reference** to select a file that is stored in Remote Manager. |

### *Device > Upload Files command*

This command uploads files to the selected devices.

| Option | Description |
|---|---|
| File | In the **File** field, enter the path and file name for the file that you want to upload on the selected devices. |

| Option | Description |
|---|---|
| Browse | Click **Browse** to browse for and select the file. |
| Reference | Click **Reference** to select a file that is stored in Remote Manager. |

### *Device > Retrieve Files command*

This command retrieves files from the file system of the selected devices.

| Option | Description |
|---|---|
| File | In the **File** field, enter the path and file name for the file that you want to retrieve from the selected devices. |
| **+** | Click the plus sign icon to add an additional path and file name. A new row appears. |
| **-** | Click the minus sign next to a path that you want to remove from the list of files. |

### *Device > Delete Files command*

This command removes files from the file system of the selected devices.

| Option | Description |
|---|---|
| File | In the **File** field, enter the path and file name for the file that you want to remove from the selected devices. |
| **+** | Click the plus sign icon to add an additional path and file name. A new row appears. |
| **-** | Click the minus sign next to a path that you want to remove from the list of files. |

### *Device > List Files command*

This command retrieves a list of files from the file system of the selected devices.

| Option | Description |
|---|---|
| Paths | In the **Paths** field, enter the path and file name for the file that you want to included in the list of files from the selected devices. |
| **+** | Click the plus sign icon to add an additional path and file name. A new row appears. |
| **-** | Click the minus sign next to a path that you want to remove from the list of files. |

### *Device > Disconnect command*

This command disconnects the selected devices. Any devices that are set to automatically reconnect will attempt reconnect to the server.

| Option | Description |
|---|---|
| Wait for Reconnect | Associate completion status with device reconnection. |

### *Device > Import Configuration command*

This command imports device property settings from a file to the selected devices.

**Note** Device identifiers (such as a MAC Address) and write-only fields (such as password fields) may not be imported.

| Option | Description |
|---|---|
| Import all | Select this option to import all device properties. |
| Import all except unique network and device identity properties. | Select this option to import all device properties except for unique network and device identity properties. |
| File | In the **File** field, enter the path and file name for the file that you want to import from the selected devices. |
| Browse | Click **Browse** to browse for and select the file. |
| Reference | Click **Reference** to select a file that is stored in Remote Manager. |
| Clear | Click **Clear** to remove the selected file name from the **File** field. |

### *Device > Command Line Interface command*

This command sends a CLI command to the selected devices.

| Option | Description |
|---|---|
| Command | Enter the CLI command. |

### *Device > Data Service Request command*

This command sends data service request to the selected devices.

| Option | Description |
|---|---|
| Edit Data Service Request | Edit the data service request code included in the task pane. |

## Add an XBee network discovery task

You can add an XBee network discovery task.

See Create a schedule for details about adding a task to a schedule.

### *XBee > XBee Network Discover command*

This task sends the XBee discover network command to the selected devices.

| Option | Description |
|---|---|
| Clear cache | Select the **Clear Cache** option to clear the cache on the XBee Gateway. This process updates the XBee Gateway network with any nodes that have been added or removed since the last XBee network discovery.<br><br>If you do not select the **Clear Cache** option, Remote Manager looks for XBee Gateway nodes that have been added since the last XBee network discovery, but does not clear out nodes that have been removed. |

## Add an SMS device task

You can schedule tasks to occur on selected devices that are configured for SMS messaging.

See Create a schedule for details about adding a task to a schedule.

### *SMS > SMS Request Connect command*

This command sends an SMS Request Connect message to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *SMS > SMS Reboot command*

This command sends an SMS reboot command to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *SMS > SMS Ping command*

This command sends an SMS ping request to the selected devices.

### *SMS > SMS Command Line command*

This command runs an SMS command on the selected devices.

| Option | Description |
|---|---|
| Command | Enter the CLI command that you want to run. |
| Max response length (number of messages) | Determines the number of response messages from the device that can be received. |
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *SMS > SMS Provision command*

This command sends an SMS message to the selected devices that will configure the return phone number to {0} to receive messages from the devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

## Add a Satellite device task

You can schedule tasks to occur on selected devices that are configured for Satellite messaging.

See Create a schedule for details about adding a task to a schedule.

### *Satellite > Satellite Request Connect command*

This command sends a Satellite Request Connect message to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *Satellite > Satellite Reboot command*

This command sends a Satellite reboot command to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *Satellite > Satellite Ping command*

This command sends a Satellite ping request to the selected devices.

### *Satellite > Satellite Command Line command*

This command runs a Satellite command on the selected devices.

| Option | Description |
|---|---|
| Command | Enter the CLI command that you want to run. |
| Max response length (number of messages) | Determines the number of response messages from the device that can be received. |
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

## Add an SM/UDP device task

You can schedule tasks to occur on selected devices that are configured for SM/UDP messaging. See Create a schedule for details about adding a task to a schedule.

### *SM/UDP > SM/UDP Request Connect command*

This command sends an SM/UDP Request Connect message to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *SM/UDP > SM/UDP Reboot command*

This command sends an SM/UDP reboot command to the selected devices.

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

### *SM/UDP > SM/UDP Ping command*

This command sends an SM/UDP ping request to the selected devices.

### *SM/UDP > SM/UDP Command Line command*

This command runs an SM/UDP command on the selected devices.

| Option | Description |
|---|---|
| Command | Enter the CLI command that you want to run. |
| Max response length (number of messages) | Determines the number of response messages from the device that can be received. |

| Option | Description |
|---|---|
| Response Required | Determines whether Remote Manager waits for a response from the device.<br>■ **Selected**: The operation is not complete unless Remote Manager receives a response from the device. If a response is not received, the operation has failed.<br>■ **Not selected**: The operation is complete when Remote Manager successfully sends a message. |

## Add a My Tasks task

You can schedule a task you have previously created and saved as a My Task option. See Create a My Task option for more information.

1. Select the **My Tasks** command. A list of the tasks you previously created and saved appears.
2. Select a task from the list. The task is added to the schedule. You can edit the task options as needed.

## New Schedule dialog

You can use the **New Schedule** dialog to create a new schedule. Each schedule must be assigned a name and consists of a set of tasks, a schedule to determine when the tasks should be run, and the device on which the tasks should be performed.

The **New Schedule** dialog consists of two screens:

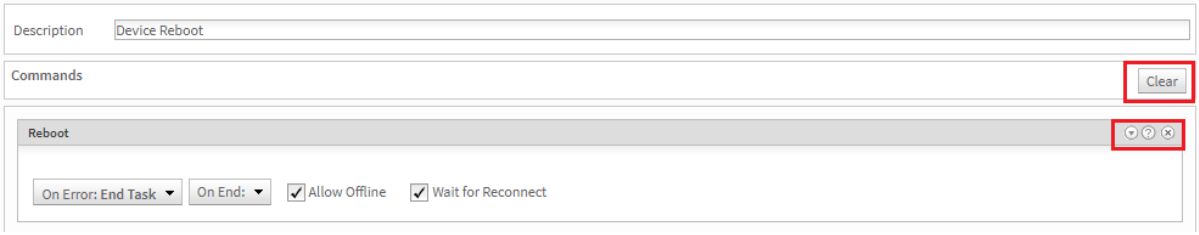
- **Commands screen**: This screen appears by default when you click the **New Schedule** button. In this screen, you enter the schedule name and select a command. After you have entered these items, the **Schedule >>** button becomes available.
- **Schedule screen**: Click **Schedule >>** in the commands screen to display the schedule screen. In this screen, you specify the schedule on which the tasks should be run and select the device on which the tasks should be performed. When you are in the schedule screen, click **Commands >>** to return to the commands screen.

### *Task dialog in the task pane*

Each command you add to the schedule appears in an individual dialog in the task pane. You can use the icons in the task dialog toolbar to collapse or expand the dialog, delete the task, or display a description of the task type.

| Button | Description |
|---|---|
|  | Click **Clear** to remove all of the tasks from the task pane. |

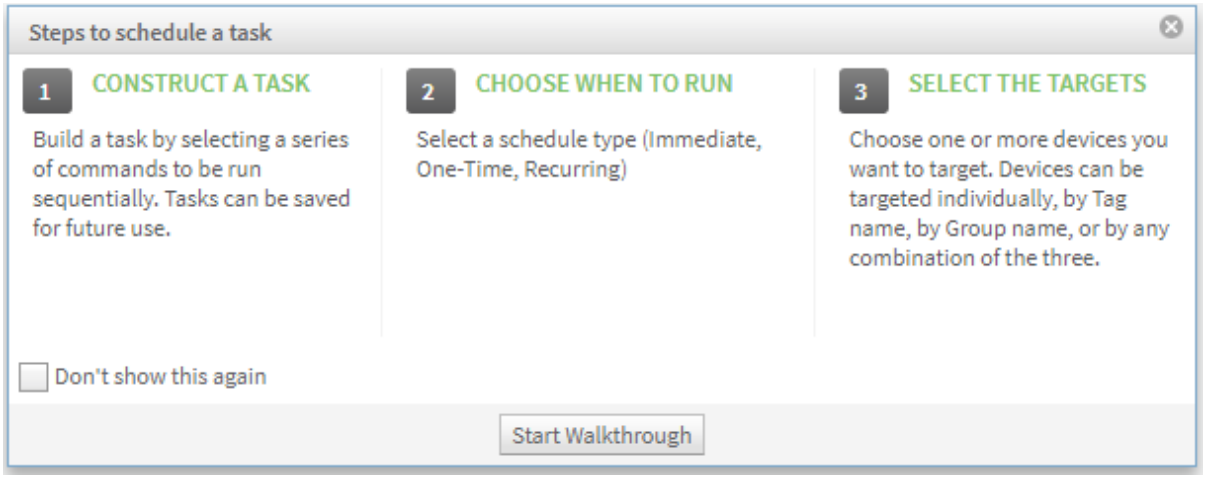
| Button | Description |
|---|---|
|  | Click this icon to hide or show the information in the task pane. |
|  | Click this icon to display a description of this task. |
|  | Click this icon to delete the task from the task pane. |




### *Schedule walk-through feature*

When you click **New Schedule** in the **Schedules** screen, the **Steps to schedule a task** dialog may appear, depending on whether the feature is enabled.

- Click **Start Walkthrough** to have direction about the steps you need to do to create a schedule.
- Select the **Don't show this again** option if you want to disable the walk-through feature.

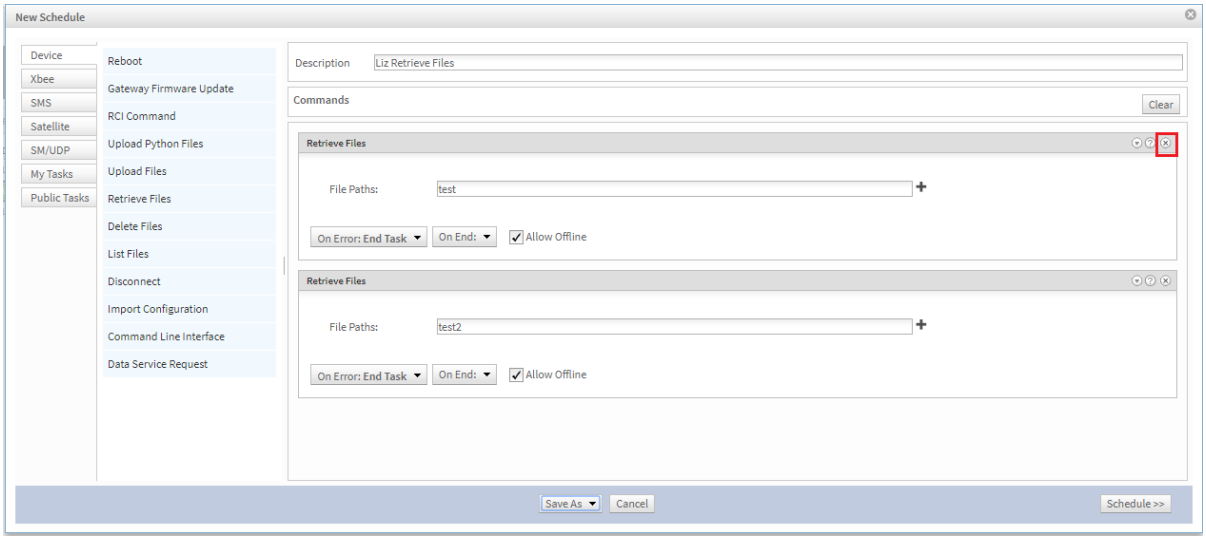



## Delete a task from a schedule

You can delete a task that is no longer needed from a schedule.

1. Click **Device Management > Schedules**.
2. Select the schedule that you want to change. The **Edit** button displays in the toolbar.

3. Click **Edit**. The **New Schedule** dialog appears, showing the schedule screen by default.
4. Click **Commands** to display the list of tasks assigned to the schedule.
5. Click the **X** icon in the upper right corner of the task to delete the task from the task pane.




6. Click **Save As**. The **Name** field appears.
    a. The current schedule name displays by default. If you want to update the schedule, do not enter a new name.
    b. Click **OK**. A confirmation dialog appears.
    c. Click **Yes**.

# Edit a schedule

You can change the schedule configuration and frequency of the scheduled tasks.

1. Click **Device Management > Schedules**.
2. Select the schedule that you want to change. The **Edit** button displays in the toolbar.
3. Click **Edit**. The **New Schedule** dialog appears, showing the schedule screen by default.
    a. Edit the fields in the schedule screen as needed.
    b. Click **<< Commands** to display the commands screen. Edit the fields in the commands screen as needed.
    c. In the commands screen, click **Schedule >>** to return to the schedule screen.
4. In the schedule screen, click **Update** to save the changes.

# Delete a schedule

You can delete a schedule that is no longer needed.

**Note** If you want to keep a schedule for future use, you can disable it, which suspends the scheduled activity without deleting the schedule. See Disable a schedule.

1. Click **Device Management > Schedules**.
2. From the schedule list, select the schedule that you want to delete. More than one schedule can be selected. The **Delete** button appears in the toolbar.
3. Click **Delete**. A confirmation dialog appears.
   - Click **Yes** to confirm the deletion.
   - Click **No** to cancel the process. The schedule is not deleted.

## Disable a schedule

You can disable a schedule if you don't want Remote Manager to perform the scheduled tasks until a future time. This feature is useful if you want to control when a schedule is in use. After a schedule has been disabled, the icon in the **Status** column changes to a gray circle.

You can enable a disabled schedule at any time. See Enable a schedule.

**Note** If you want to permanently delete a schedule, see Delete a schedule.

1. Click **Device Management > Schedules**.
2. Select the schedule you want to disable. The **Cancel** button appears in the toolbar.
3. Click **Cancel**. A confirmation dialog appears.
   - Click **Yes** to cancel the schedule.
   - Click **No** to cancel the process. The schedule will continue to perform tasks.

## Enable a schedule

You can enable a schedule that has been disabled. After a schedule has been disabled, the icon in the **Status** column changes to a gray circle.

1. Click **Device Management > Schedules**.
2. Select the schedule you want to enable.
3. Click **Edit**. The **New Schedule** dialog appears.
4. In the **Recurring** tab or in the **One Time** tab, change at least one existing date or time item to a new date or time.
5. Click **Update**.

## Schedule frequency

You can specify the frequency at which the scheduled tasks should occur.

**Immediate**: The schedule runs once when you click **Run Now**.

a. Click the **One Time** tab.

b. Select the **Immediate** option.

**Future**: The scheduled tasks run one time on a specified future date and time.

a. Click the **One Time** tab.

b. Select the **Future** option.

c. Select a date and time from the drop-down lists.

**Recurring**: The scheduled tasks are run on the frequency specified during the specified time range.

a. Click the **Recurring** tab.

b. From the **Start** and **End** drop-down list boxes, select the start and end date and time range for the schedule.

c. From the **Repeat** drop-down list box, select how often the task should be performed.

d. From the **Every** drop-down list box, select the frequency with which the task should be performed.

e. Select the **UTC** option if you want to use Coordinated Universal Time.

# Create a My Task option

The My Task feature enables you to create a schedule with tasks that you can repeat for different devices.

You can create a schedule and add tasks, and then save that personal schedule as a My Task option. These personal schedules are included in the **My Tasks** tab in the **New Schedule** dialog and are accessible only by the person who created the My Task.

After you have created a My Task option, you can select it when creating a new schedule. All of the tasks in the My Task, and any other tasks you add to the schedule, are performed on the selected device.

A My Task option can only be named and saved from the command screen in the **New Schedule** dialog. If you access the schedule screen, you must click **<< Commands** to return to the command screen to name and save the My Task option. Any configuration you made in the schedule screen is not saved.

**Note** You can also immediately run or schedule a My Task option for a selected device from the **More** menu. See Run My Task device tasks.

1. Click **Device Management > Schedules**.
2. Click **New Schedule**. The **New Schedule** dialog appears.
3. In the **Description** field, enter a descriptive name for the My Task schedule.
4. Select the device type and the action on that device that you would like to perform. The links below lead to detailed information about the command information you need to enter.
   - Device
   - XBee
   - SMS
   - Satellite
   - SM/UDP
5. Click the **On Error** drop-down list to specify the action that should be taken when the action ends in an error: **End Task**, **Continue**, or **Retry**.

6. Click the **On End** drop-down list to specify the action that should be taken when the task ends. Options are:
   - Nothing: Do not select the **Sleep** option. The device status is not changed.
   - **Sleep**: Select the **Sleep** option if the device should go to sleep after the action has been performed.
7. Select the **Allow Offline** option if the action should be taken even if the device is offline.

   **Note** This option is not available for all device type selections.

8. Repeat steps 4 through 7 to add additional tasks to the schedule.
9. Make sure you are on the commands screen of the **New Schedule** dialog. If you are on the schedule screen of the dialog, click **<< Commands** to return to the command screen. Any configuration you made in the schedule screen is ignored.
10. Click **Save As**. The **Name** field appears.
11. In the **Name** field, enter a descriptive name for the task. This name appears in the task list when you select the **My Tasks** option when creating a schedule.
12. Click **OK**.
13. Close the dialog.

# Run My Task device tasks

You can run the tasks in a My Task option that you have previously named and saved. See Create a My Task option for information about creating tasks for this feature.

1. Click **Device Management > Devices**.
2. Select a device.
3. Click **More** in the Devices toolbar and select **Show Tasks** from the Devices category of the **More** menu. The **Tasks** dialog appears.
4. Click the **Select a Task** drop-down and select a task from the task menu. The tasks you can choose from are My Task options that you previously created. See Create a My Task option for information about creating tasks for this feature in the **Schedule** tab.
5. Determine when you want the task to run.
   - **Immediately**: This is the default option. Click **Run Task** to start the task immediately.
   - **Future**: You can schedule when you want the task to run and then click **Run Task** to start the task at the scheduled time. Click the gear icon to display the schedule options. See Schedule frequency for detailed information about the schedule options.
   - **Cancel**: Click **No** to cancel the My Task.

# Operations

The Operations page shows all of the operations that have occurred in Remote Manager. The Operations list displays an entry for each Remote Manager operation performed within the last 24 hours. An individual operation is a job, and each job is assigned a unique Operation ID.

For each operation, Remote Manager displays the completion percentage. When an operation is performed on multiple devices, the completion percentage represents the number of devices that have completed the given task.

Operations include:

- All management tasks performed on multiple devices by Remote Manager
- Firmware downloads
- File transfers
- SMS jobs
- Any asynchronous SCI Web Service requests performed using your Remote Manager user credentials

Within this page you can:

- Click the **Refresh** icon to refresh the list of operations.
- Delete an operation.
- Cancel operations in progress.
- View a summary of operations over the last 24 hours. See View operations and operation details.
- View detailed information about a specific operation in the **Operation Details** page. The Operation Details page displays details about the job request, a list of devices the job was run against, and results on a per-device basis. If you select multiple jobs, multiple **Operation Details** pages are displayed in tabbed format. See View operations and operation details.

## View operations and operation details

The Operations page displays an entry for each of the Remote Manager operations performed within the last 24 hours.

1. Click **Device Management** > **Operations**. See Operations view for information about the fields on the **Operations** page.
2. Select an entry from the list of operations. Shift-click to select multiple entries.

3. Click the **Operation Details** button or double-click a selected entry. The **Operation Details** page appears. The **Operation Details** page displays details about the job request, a list of devices the job was run against, and results on a per-device basis. If you select multiple jobs, multiple **Operation Details** pages are displayed in tabbed format. See Operation Details view for information about the fields on the **Operation Details** page.

## Delete an operation

You can delete an entry on the **Operations** page.

**Note** Use the Delete function with care. You will not be asked to confirm deletion and the action cannot be reverted.

1. Click **Device Management** > **Operations**.
2. Select an entry from the list of operations. Shift-click to select multiple entries.
3. Click the **Delete** button.

# Carrier accounts

Remote Manager is integrated with various cellular service providers so you can monitor your cellular data usage directly within Remote Manager. To enable this functionality, Remote Manager creates a link between your Remote Manager-enabled device and its unique mobile identifier (ICCID for GSM and MEID, or ESN for CDMA).

To list the supported carriers, select **Admin > Account Settings > Carrier Account**.

Configuring a carrier account allows Remote Manager to interface with that carrier to gather and display your data usage information. Add carrier-integrated device(s) to your inventory to begin viewing carrier data usage information directly within Remote Manager.

Once you have configured a carrier account, the rate plans associated with that cellular service provider will be displayed within your list of subscriptions. Rate plans will correspond to cellular data or cellular SMS. If an SMS rate plan is not visible for your cellular service provider, either SMS usage is not available in your carrier's API or Remote Manager is not capable of sending or receiving SMS messages to mobile devices on your cellular plan.

When a carrier-integrated device is added to your Remote Manager inventory, the carrier subscription corresponding to that device will be assigned automatically. However, in the following cases, it may be necessary to manually assign a carrier subscription:

- More than one carrier account is configured within Remote Manager
- The Remote Manager account inventory contained carrier-integrated devices prior to carrier account configuration

**Note** Carrier data usage values available in Remote Manager are updated in accordance with the carrier's proprietary API, with frequency and timing of data refresh varying from carrier to carrier.

**Note** Carrier Subscription Management is provisioned by default with some Remote Manager editions, but not all. If you are unable to configure a carrier account, contact Customer Service to add this service to your account.

## Configure a carrier account

You can configure a carrier account for each carrier used by your organization.

If you configure only one carrier account, all devices in your inventory that support carrier integration are automatically assigned to the configured carrier. When you add a new device, Remote Manager automatically assigns those devices to your configured carrier account.

However, if you configure more than one carrier account, you must manually select a carrier for each device. See Manually assign a carrier subscription.

1. Click **Admin > Account settings > Carrier Account**. If you have not configured any carrier accounts, Remote Manager displays a blank **Credentials** dialog associated with each carrier.
2. Click **Enter Credentials** for your supported carrier. The **Enter credentials** dialog appears.
3. Enter the necessary credentials. Each carrier requires slightly different account information, so the dialog fields are carrier-dependent.
4. Read the Carrier Subscription Management Notice. When complete, select the **I acknowledge the above notice** option.
5. Click **Save**. The Carrier Account Management page refreshes, displaying the configured carrier account.
6. Click **Test Connection** to verify the credentials and connection.

## Remove carrier credentials

You can remove a carrier account's credentials from your Remote Manager account.

**Note** All carrier accounts can be removed. You are not required to have carrier accounts.

1. Click **Admin > Account settings > Carrier Account.**
2. Click **Remove** under the configured carrier account whose credentials you would like to remove. A confirmation dialog appears.
    a. Click **Yes** to confirm the deletion.
    b. Click **No** to cancel the process.

## Manually assign a carrier subscription

Remote Manager automatically assigns the configured carrier to each carrier-integrated device added to your inventory. However, if you configured more than one carrier for your account or if you configured the carrier after adding devices, you need to manually assign a carrier to each device.

1. Click **Device Management > Carrier.** Select the **Management** tab.
2. Select a device from the device list, or shift-click to select multiple devices.
3. Click **Assign Carrier Subscription**. The **Assign Carrier Subscription** dialog appears.
4. Using the drop-down box, designate the carrier you would like to assign to the selected device (s).
5. Click **Assign Carrier Subscription**. Remote Manager briefly displays a confirmation that the carrier subscription was assigned successfully.

## Update credentials for a carrier account

You can update the credentials for an existing carrier account.

1. Click **Admin > Account settings > Carrier Account**.
2. For the carrier you want to update, click **Change Credentials**. The **Edit credentials** dialog appears.

3. Update the necessary credentials. Each carrier requires slightly different account information, so the dialog fields are carrier-dependent.
4. Read the Carrier Subscription Management Notice. When complete, select the **I acknowledge the above notice** option.
5. Click **Save**. The Carrier Account Management page refreshes, displaying the configured carrier account.
6. Click **Test Connection** to verify the credentials and connection.

## Update carrier account usage

You can retrieve the latest usage information for the selected carrier.

1. Click **Device Management > Carrier**.
2. Select a carrier from the list.
3. Click the **Usage** tab.
4. Click **Update Usage**.

## Display carrier account usage information

You can display a chart that depicts usage information over time for the selected carrier. See Carrier usage details for more information.

1. Click **Device Management > Carrier**.
2. Select a carrier from the list.
3. Click the **Usage** tab.
4. Click **Details**. A set of charts appears.
5. Click the appropriate interval button in the tool bar to display the desired amount of usage.
6. From the rollup drop-down list, select the appropriate type.

## Activate or deactivate a carrier account

You can activate or deactivate carrier service for the selected device.

1. Click **Device Management > Carrier**.
2. Click the **Management** tab.
3. Select a device from the list.
4. Click **Activate/Deactivate** to display a sub-menu.
   - Click **Activate** to activate the carrier service for the device. When the carrier service is activated, a green icon appears in the status column.
   - Click **Deactivate** to deactivate the carrier service for the device. When the carrier service is deactivated, a red icon appears in the status column.

# Profiles

A device profile is a template you can use to control, monitor, and report on device firmware versions, configuration options, and file systems.

## Master device and device types

A master device is any device you select from your inventory to use as a model for a device profile. Once you have selected a master device for a profile, Remote Manager takes a snapshot of the device settings to use as the base for setting up the profile.

**Note** If you change or remove the master device upon which a profile is based, the profile is not changed. The snapshot of the selected master device is used only during the initial profile setup.

Once you have created a profile, you can apply that profile only to devices of the same device type. For example, if you create a profile using a TransPort WR21 as the master device, the profile can be applied only to other TransPort WR21 devices.

- Create a device profile
- Edit a device profile
- Delete a device profile
- Enable or disable a device profile

## Targets and scoping options

A profile can be applied to one or more specific devices and/or scoped to one or more groups or device tags.

**Note** Remote Manager applies the profile only to devices within the scoping options that match the profile device type. For example, if you create a profile using a TransPort WR21 as the master device and you specify a group named Western_Region as the profile target, Remote Manager applies the profile only to TransPort WR21 devices within the Western_Region group.

## Scan schedule and actions

For each profile, you can set up a recurring schedule that determines when Remote Manager scans your target devices for compliance with the profile settings. You can set up an hourly, daily, weekly, or monthly schedule for the profile scan.

You can also determine the actions you want Remote Manager to take when devices do not comply with profile settings. When a device does not match a profile setting, Remote Manager can trigger an alarm and/or modify the device so that it matches the profile settings.

- Manually scan a profile
- View the scan history for a profile

# Create a device profile

A device profile allows you to manage device firmware, configuration, and file system settings for one or more devices. When creating a device profile, you must select a master device from your inventory to use as a template for the profile.

**Note** A master device is used only during initial profile creation. If you modify a master device after creating a profile, the profile is not changed.

1. Set up the device you want to use as the master for the profile.
    a. Add the device to your Remote Manager inventory.
    b. Make sure the device is currently connected to Remote Manager.
    c. Modify device options as needed.
2. Go to **Device Management > Profiles**.
3. Click **Create Profile**. The Create Profile wizard appears.
4. Complete Step 1: Snapshot.
    - **Profile Name**: (Required) Enter a name for the profile.
    - **Profile Description**: (Optional) Enter a description of the profile.
    - **Master Device**: (Required) Select the device to use as the master for the profile.
5. Click **Save and Continue**.
6. Complete Step 2: Targets. Select the devices and/or scoping options for the profile.
    - **Devices**: Select one or more devices.
    - **Groups**: Select one or more groups.
    - **Tags**: Select one or more tags.
7. Click **Save and Continue**.

8. Complete Step 3: Settings. Select one or more settings to include in the profile.
   - **Firmware**: Enable **Firmware** and then browse to and upload a firmware file to include in the profile.
   - **Config**: Enable **Config** and then select the configuration options to include.

     **Note** Devices of the same device type can have different configuration options depending on hardware options. For example, a TransPort WR21 can have one or two Ethernet interfaces and a TransPort WR44 can include Wi-Fi. When selecting a master device for a profile, make sure the master device has the same configuration options as the devices to which you intend to apply the profile. Otherwise, you may get unexpected configuration mismatch errors when you apply the profile to a group of devices of the same type that have different configuration options.

   - **File System**: Enable **File System** and then select the files to include. Because configuration and file system settings are dependent on a specific firmware level, for best profile scan results, it is recommended that you include all profile settings—Firmware, Config, and File System—within a profile. If you attempt to match only one or two settings, you may get unexpected results.
9. Click **Save and Continue**.
10. Complete Step 4: Schedule. Set up a schedule and specify actions.
    - **Scan**: Select how often to run the profile scan: hourly, daily, weekly, or monthly.
    - **Time**: Specify the time to run the scan.
    - **Device Profile Alarm**: Enable this option to trigger an alarm when a scanned device does not match the profile. If you want to be notified via email when a Device Profile alarm is triggered, add the desired alarm type(s) to your account notifications. See Create an alarm notification.
    - **Bring Device into Compliance**: Enable this option if you want Remote Manager to modify non-matching devices to match the profile.
11. Exit the profile wizard.
    - Click **Save and Exit**. The profile is saved as an inactive draft.
    - Click **Activate Profile** to save and activate the profile.

# Edit a device profile

You can edit a profile whenever the profile is not in use. If a profile is currently in use, wait for the scan to complete before editing the profile. When you edit a profile, you can change any of the profile settings in any order.

**Note** You cannot select a different master device for an existing profile. If you need to base a profile on another device, create a new profile.

1. Go to **Device Management > Profiles**.
2. Browse the profile list and click the name of the profile you want to edit. You can also click the **Edit** icon for the profile. The **Edit Profile** wizard appears.
3. Complete Step 1: Snapshot.
   - **Profile Name:** (Required) Enter a name for the profile.
   - **Profile Description:** (Optional) Enter a description of the profile.
4. Click **Save and Continue**.
5. Complete Step 2: Targets. Select devices and/or scoping options for the profile:
   - **Devices:** Select one or more devices.
   - **Groups:** Select one or more groups.
   - **Tags:** Select one or more tags.
6. Click **Save and Continue**.
7. Complete Step 3: Settings. Select one or more settings to include in the profile.
   - **Firmware:** Enable Firmware and then browse to and upload a firmware file.
   - **Config:** Enable Config and then select the configuration options to include.
   - **File System:** Enable File System and then select the files to include.
8. Click **Save and Continue**.
9. Complete Step 4: Schedule. Set up a schedule and specify actions.
   - **Scan**: Select how often to run the profile scan: hourly, daily, weekly, or monthly.
   - **Time**: Specify the time to run the scan.
   - **Alam - Generate Device Profile Alarm**: Enable this option to trigger an alarm when a scanned device does not match the profile. If you want to be notified via email when a Device Profile alarm is triggered, add the desired alarm type(s) to your account notifications. See Create an alarm notification.
   - **Remediate - Bring Device into Compliance with Profile**: Enable this option if you want Remote Manager to modify non-matching devices to match the profile.
10. Exit the profile wizard.
    - Click **Save and Exit**. The profile is saved as an inactive draft.
    - Click **Activate Profile** to save and activate the profile

# Delete a device profile

You can delete a profile that is not in use. If a profile is currently in use, wait for the scan to complete before deleting the profile.

1. Go to **Device Management > Profiles**.
2. Select one or more device profiles from the list.

3. Click **Delete**.
    - Click **Yes** to confirm deletion.
    - Click **No** to cancel the process.

## Enable or disable a device profile

You can enable or disable a device profile whenever the profile is not in use. If a profile is currently in use, wait for the scan to complete before enabling/disabling the profile.

**Note** You cannot enable or disable a draft profile.

1. Go to **Device Management > Profiles**.
2. Select one or more device profiles from the list.
3. Click **Enable** or **Disable**.

## Manually scan a profile

You can manually scan a profile. This process scans your target devices for compliance with the profile settings. Each time a profile is scanned, a date- and time-stamped event log is created and saved.

1. Go to **Device Management > Profiles**.
2. Within the profile list, locate the profile you want to scan.
3. Click the **Scan Now** icon for the profile. Progress information appears in the screen. The information in the **Last Scan Time** column is updated.

## View the scan history for a profile

Each time a profile is scanned, a date- and time-stamped event log is created and saved. You can review the scan history in the event log.

1. Go to **Device Management > Profiles**.
2. Within the profile list, locate the profile for which you want to view the scan history.
3. Click the displayed **Last Scan Time** column or the **Scan History** icon. The Profile scan history appears.
4. Within the scan history view, click the displayed **Status** to see a detailed event log for the scan.

# Reports

You can create and generate account- and device-level reports using the health status information Remote Manager gathers for all devices within your inventory. You can immediately run a report and download the file to your local system, or you can schedule a report and automatically email the PDF report to one or more recipients. Reports are also automatically saved to the list of reports in the **Reports** view.

## Generate a health status report immediately

You can create and run a health status report at any time. Each report is also automatically saved to the list of reports in the **Reports** view.

**Note** If you want to create a report and run it at a future time, see Schedule a health status report.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Click **New Report**. The **Create new report** dialog appears.
3. Provide the following report information:
   - **Report name**: Enter a name for the report.
   - **Report description**: Enter a brief description for the report.
   - **Include the following reports**: Select account- and device-level report types. See Health status report types for information about the report types.
     - **Account**: Select one or more account-level report types to include in the report.
     - **Device**: Select one or more device-level report types to include in the report.
   - **Select a device:** For device reports, select the device for the reports. This section appears only if you have selected a device-level report.
4. Click **Run Now**.
5. Select the time range for the report data:
   - **Day:** Include the most recent day.
   - **Week:** Include the most recent week.
   - **Month:** Include the most recent month.
   - **Custom:** Include data within the specified date range.

6. Complete the report:
   - Click **Save Report** to save the report without running the report. The report is included in the list of reports in the **Reports** view, and can be run at any time.
   - Click **Save and Run Report** to run the report. The report PDF file is automatically downloaded to your local system, which you can open and view, and save. The report is included in the list of reports in the **Reports** view, and can be run at any time.

# Schedule a health status report

You can create and schedule a health status report to run at a future date and time. Each report is also automatically saved to the list of reports in the **Reports** view.

**Note** If you want to create a report and run it immediately, see Generate a health status report immediately.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Click **New Report**. The **Create new report** dialog appears.
3. Provide the following report information:
   - **Report name**: Enter a name for the report.
   - **Report description**: Enter a brief description for the report.
   - **Include the following reports**: Select account- and device-level report types. See Health status report types for information about the report types.
     - **Account**: Select one or more account-level report types to include in the report.
     - **Device**: Select one or more device-level report types to include in the report.
   - **Select a device:** For device reports, select the device for the reports.
4. Click **Run Later**.
5. Select a run interval. The time is on a 24-hour clock.
   - **Day:** Run the report daily at the specified time.
   - **Week:** Run the report weekly on the specified weekday and time.
   - **Month:** Run the report monthly on the specified day and time.
6. Select the time range for the report data. By default, the time range is the same as the selected run interval:
   - **Day:** Include the current day.
   - **Week:** Include the current week.
   - **Month:** Include the current month.

7. Specify send options for the report:
   - **Subject:** Enter a subject line for the emailed report. By default, the subject is the user-specified report name.
   - **Text:** Enter text to include on the report. By default, the text includes the user-specified report name and description, along with the specified date and time the report is generated.
   - **To:** Enter one or more recipients to whom you want to send the report:
     - To add a recipient, enter a valid email address and click **+** .
     - To remove a recipient, click **x** next the recipient you want to remove.
8. Complete the report:
   - Click **Save Report** to save the report without running the report. The report is included in the list of reports in the **Reports** view, and can be run at any time.
   - Click **Save and Schedule Report** to save the report, run the report per the specified schedule, and email a copy of the PDF report to all recipients. The report is included in the list of reports in the **Reports** view, and can be run at any time.

# Edit a health status report

You can make changes to the saved reports that appear in the **Reports** view.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Within the reports list, locate the report you want to edit and click on the report name or click the edit icon for the report. The **Edit** dialog appears.
3. Edit the report information as desired.
   - For information about the report fields and running a report immediately, see Generate a health status report immediately.
   - For information about the report fields and scheduling a report, see Schedule a health status report.
4. Determine if you want to save and/or run the report.
   - Click **Save Report** to save the changes without running the report. The report is included in the list of reports in the **Reports** view, and can be run at any time.
   - Click **Save and Run Report** to run the report. The report PDF file is automatically downloaded to your local system, which you can open and view, and save. The report is included in the list of reports in the **Reports** view, and can be run at any time.
   - Click **Save and Schedule Report** to save the report, run the report per the specified schedule, and email a copy of the PDF report to all recipients. The report is included in the list of reports in the **Reports** view, and can be run at any time.

# Run a health status report

You can run a report in the **Reports** view as needed. If you select a scheduled report, it is run immediately.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Within the reports list, locate the report you want to run and click  . The **Select a date range for report data** dialog appears.
3. Change the date range in the **From** and **Until** fields, as needed.
4. Click **Run report for selected dates**. Remote Manager runs the report and downloads a PDF file to your local system.

## Enable or disable a scheduled health status report

You can enable and disable a scheduled report. When the report is disabled, it does not run as scheduled.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Within the report list, locate a scheduled report that has a enabled/disabled toggle in the **Enabled** column.
   - Slide the toggle to the right to enable the report. The toggle is green.
   - Slide the toggle to the left to disable the report. The toggle is white.

## Delete a health status report

You can delete a report that is no longer valid.

**Note** Instead of deleting a scheduled report, you can disable it, to stop the report from generating on the scheduled date and time. See Enable or disable a scheduled health status report.

1. Click **Admin > Reports**. The **Reports** view appears.
2. Within the report list, locate the report you want to delete and click  . A confirmation dialog appears.
   - Click **Cancel** to cancel the deletion.
   - Click **Delete** to confirm the deletion.

# Health status report types

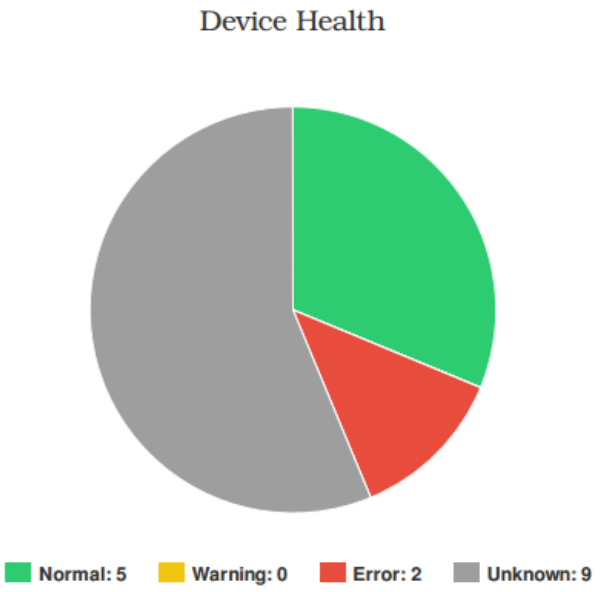
The following health status report types are available.

## Aggregate health status report

The account-level aggregate health chart shows aggregate health status for all devices in your Remote Manager account. 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.

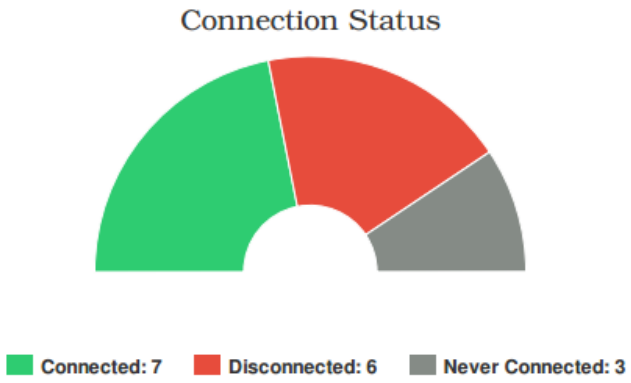
The following example shows a sample account-level aggregate health status report:




## Aggregate connection status report

The account-level aggregate connection status chart 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.

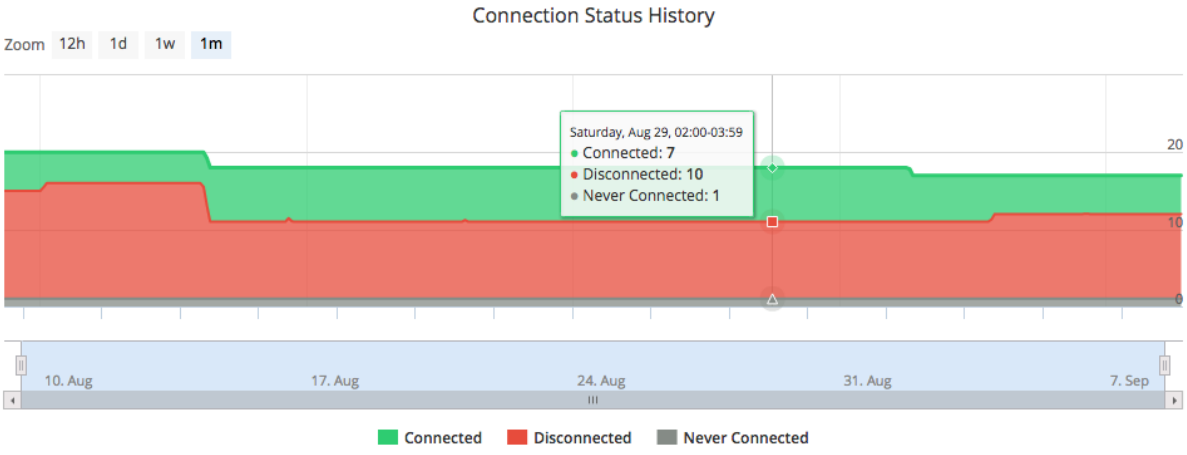
The following example shows a sample account-level connection status report:




## Aggregate connection status history report

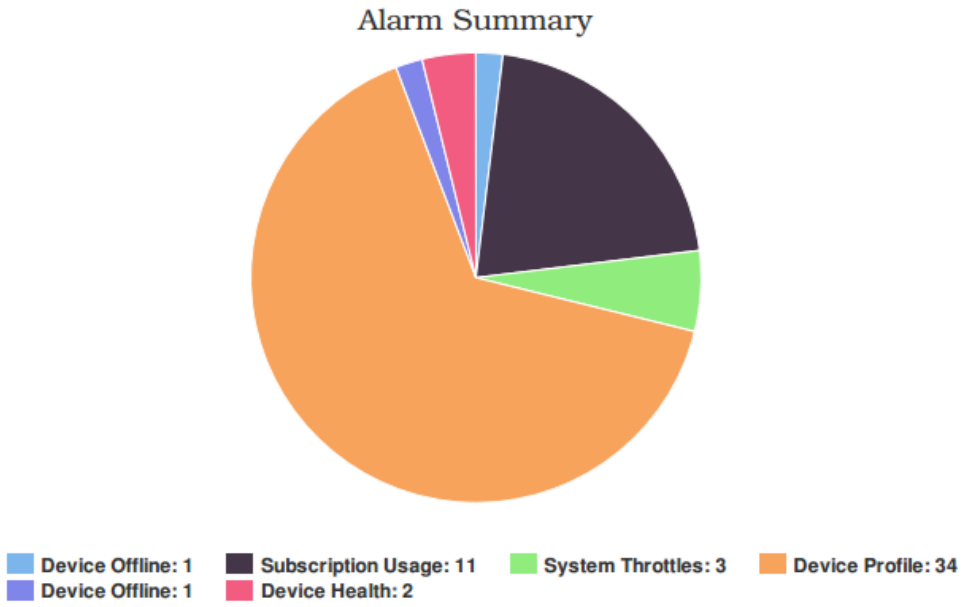
The account-level aggregate connection status history chart shows a history of the number of devices connected, disconnected, or never connected. Never connected denotes a registered device that has not yet connected to Remote Manager. You can opt to show data for a Day, Week, Month, or a custom date range.

The following example shows a sample account-level connection status history report:



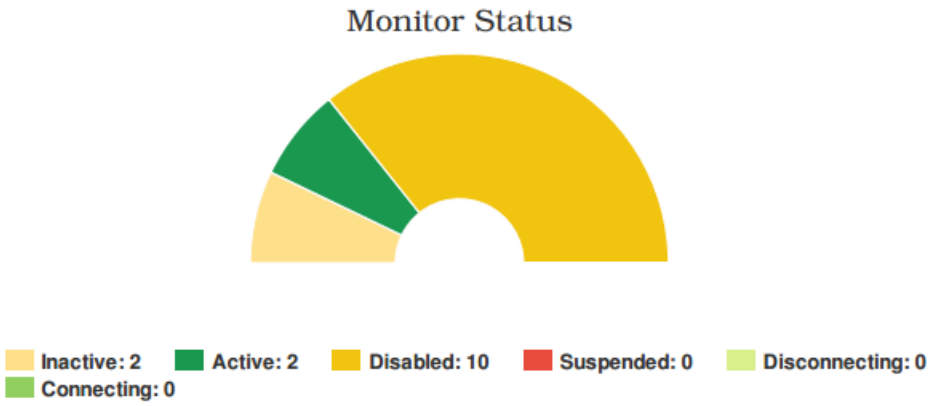

## Alarm status report

The account-level alarm status chart shows a summary of all fired alarms by alarm type. The following example shows a sample account-level alarm status report:




## Monitor status report

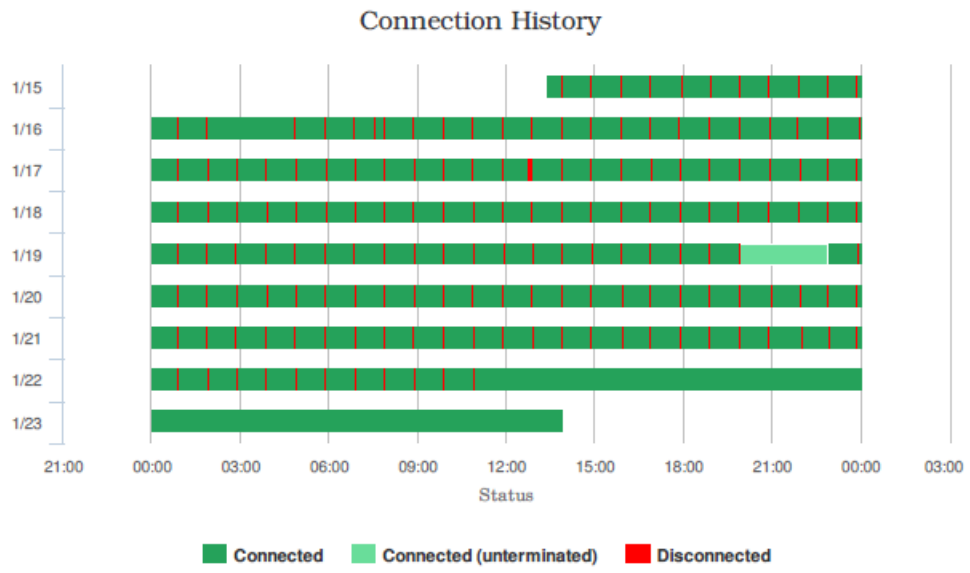
The account-level monitor status chart shows a summary of all system monitors by monitor status: Inactive, Active, Disabled, Suspended, Disconnecting, and Connecting. The following shows a sample account-level monitor status report:




## Connection history report

The device connection history report shows device connectivity over time. You must select a device when running this report.

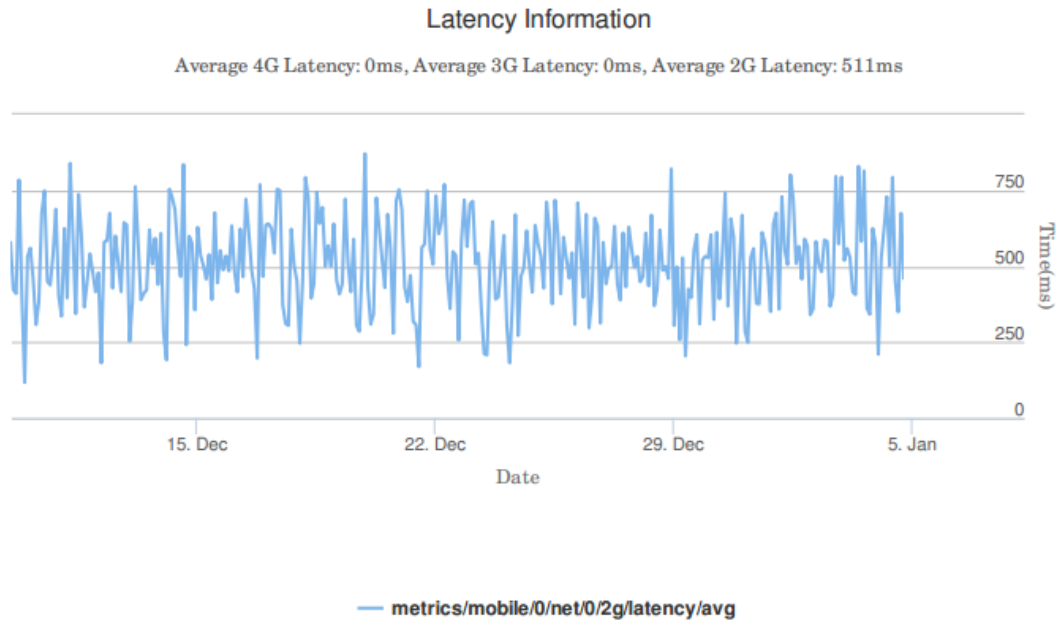
The following shows a sample device connection history report.




## Latency report

The device latency report shows average latency for 4G, 3G, and 2G connections. You must select a device when running this report.

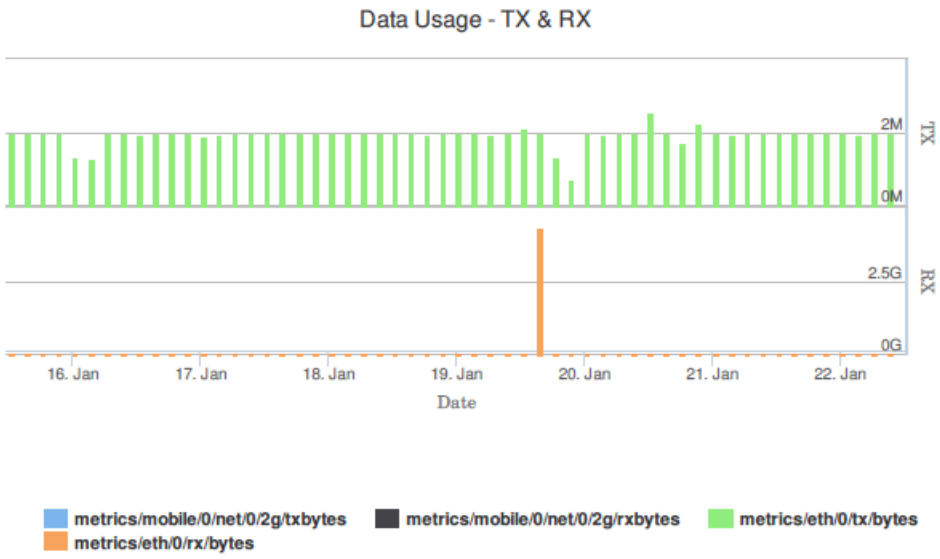
The following shows a sample device latency report.




## Data usage report

The device data usage report shows the amount of transmitted and received data for a device over time. You must select a device when running this report.

The following shows a sample device data usage report.




## Out-of-service report

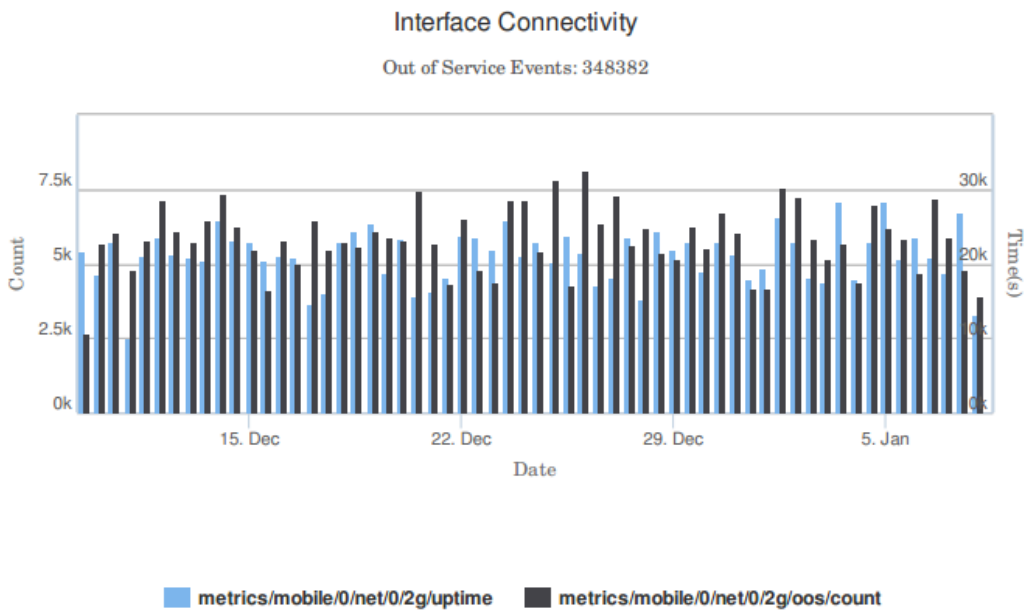
The device out-of-service report shows out-of-service events for a device over time. This report is available only for devices that report on out-of-service events.

You must select a device when running this report.

## Interface connectivity report

The device interface connectivity report shows the connection history for a device, along with out-of-service events. You must select a device when running this report.

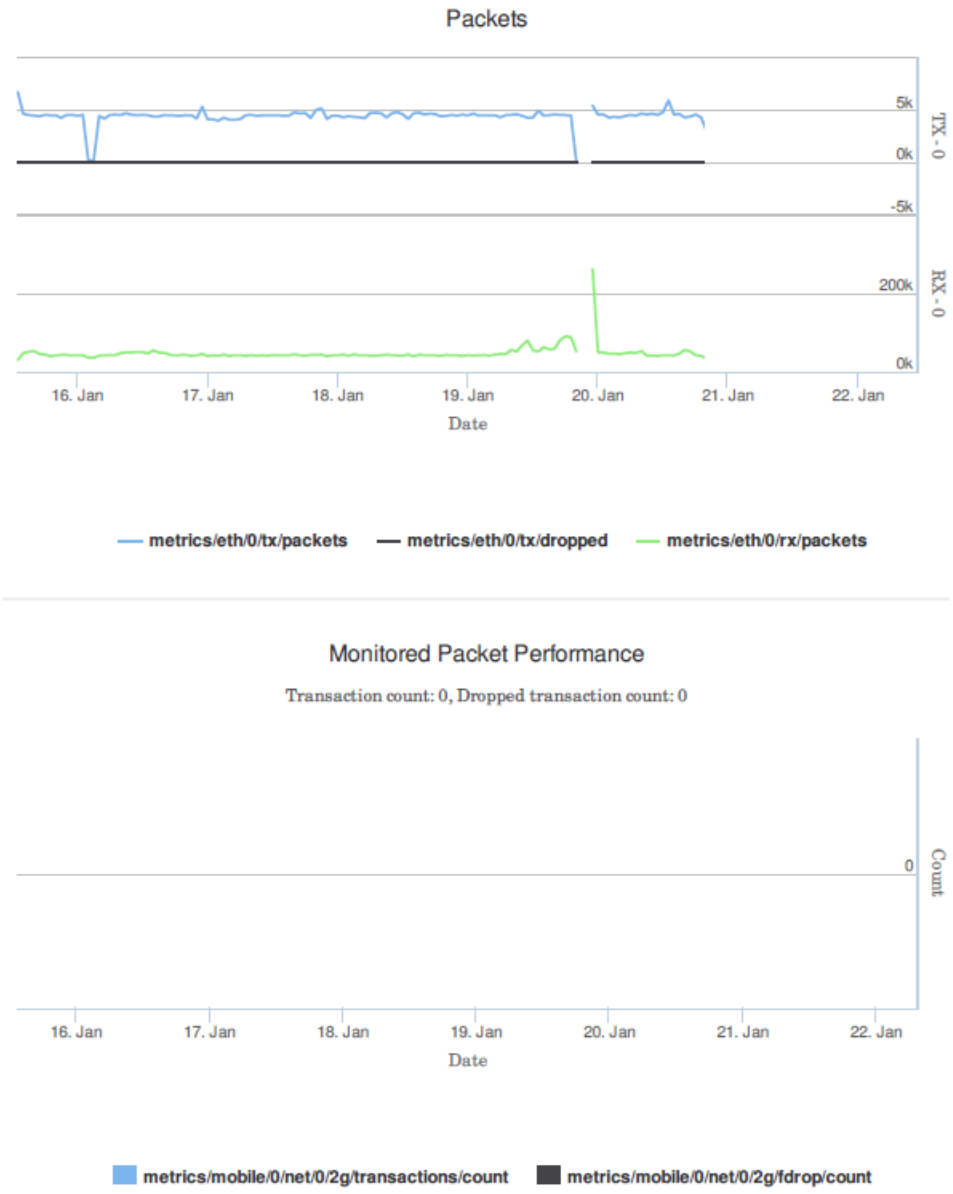
The following shows a sample device connectivity report.




## Packet report

The device packet report shows packets transmitted and received over time, as well as the total packets and dropped packets. You must select a device when running this report.

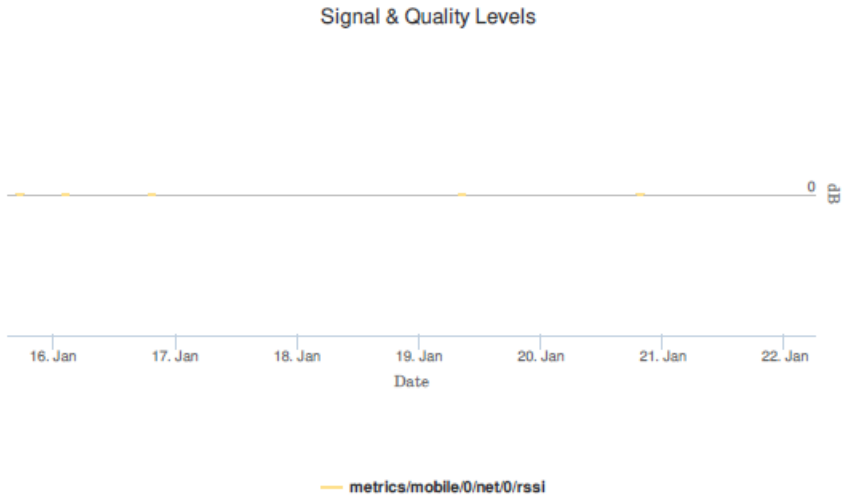
The following shows a sample device packet report.




## Signal report

The device signal report shows signal and quality levels for a device over time. You must select a device when running this report.

The following shows a sample device signal report.


Signal & Quality Levels
0
dB
16. Jan
17. Jan
18. Jan
19. Jan
20. Jan
21. Jan
22. Jan
Date
metrics/mobile/0/net/0/rssi

# Data services

Remote Manager data services allow you to collect and manage data from remote devices. For example, a device can send data files to the Remote Manager server, and Remote Manager temporarily caches the data files in a database. The files are stored by default for 24 days. Any files stored in the my_tasks folder are saved indefinitely.

## Data collections and files

Remote Manager stores the files in collections, which are similar to folders. You can access files and collections using the Remote Manager user interface and web services.

## Home collection tilde (~) character

For each user account, Remote Manager creates a home collection, which is represented by the tilde (~) character. All files for your user account are stored relative to your home directory. For example, if you created a collection named **mydata**, you can access the **mydata** collection as follows:

```
~/mydata
A collection for a device includes the Device ID.
~/00000000-00000000-00000000-12345678
```

## Data Stream

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 and data streams. Data points are the individual values which are stored at specific times, while data streams are containers of data points. 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.) Remote Manager's data streams service is a RESTful API for storing and accessing time series data in Remote Manager. By provisioning this API, you can query time series data in Remote Manager and store it there. Contact Remote Manager Technical Support for more information on data storage limits for your data streams subscription.

## 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 Data Streams API.

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. For more information, see Data Streams in the *Remote Manager Programmer Guide*.

## Add data stream

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

1. Click **Data Services > Data Streams**.
2. Click **Add**. The **Add Data Stream** dialog appears.
3. Fill in the following fields. See the Columns section in the Data streams view for more information about these fields.
    - **Stream ID**: The name for a container for data. You can manually enter a name. If data is uploaded from a device, information from the data stream is used by default to create the stream ID.
    - **Data type**: The type of data stored in the data stream. Select an option from the drop-down list.
    - **Description**: A user-defined description of the data.
    - **Units**: A user-defined description of the unit of measure for the reported data.
    - **Data expiration**: 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.
    - **Rollups expiration**: 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.
4. You can choose to enable the Data Forwarding feature for this data stream.
    a. Specify a stream or list of streams you want to receive the forwarded data. You can do this either by entering a data stream in the text box or selecting a stream from the drop-down menu.
    b. Click **Add Forward To**.

5. Click **OK**. The page refreshes and the new data stream is displayed within the data streams list.

## Delete data stream

You can delete a data stream and all data points that belong to the stream.

1. Click **Data Services > Data Streams**.
2. Select a data stream, or shift-click to select multiple streams.
3. Click **Delete**. A confirmation dialog appears.
   - Click **Yes** to delete.
   - Click **No** to cancel the deletion process.

## Edit data stream properties

Once a data stream has been created, you can edit any of the properties except the Stream ID.

1. Click **Data Services > Data Streams**.
2. Select the data stream you would like to modify.
3. Click **Properties**. The **Edit Data Stream** dialog appears.
4. Modify any field in the dialog. The **Stream ID** field cannot be changed. See Add data stream for information about the fields.
5. Click **OK**. The page refreshes and the edited data stream is displayed within the data streams list.

## Configure data stream preferences

You can configure the default preferences for new data streams in the **Data Streams Preferences** dialog.

1. Click **Data Services > Data Streams**.
2. Click **Preferences**. The **Data Stream Preferences** dialog appears.
3. Specify default time zones:
   - To add a time zone that is not displayed within the pane, click within the pane to access a scrollable list of all available time zones. Click a time zone from the list to add it to your list of preferred time zones.
   - To remove a time zone, click the **X** next to the name of the time zone you'd like to remove from your list of preferred time zones.
4. In the **Data Expiration Defaults** field, specify the default time length for data expiration. Type a new value into the text field or select a value from the drop-down list. The value is measured in seconds. The value can be between 0 and 16,070,400 seconds, which is 6 months.
5. In the **Rollups Expiration Defaults** field, specify the default time length for data rollups expiration. Type a new value into the text field or select a value from the drop-down menu.

6. Click **OK**. Remote Manager saves the new default preferences and displays a brief confirmation message at the top of the banner.

### View data streams

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.

1. Click **Data Services > Data Streams**.
2. Select a data stream from the list. Detailed information on that data stream appears below the data streams list.
3. Click the **Charts** tab to view a chart of the data points. Note that to display a chart, the data points must be numeric.
   - Use the **Show Last** tab options to select the time interval to display.
   - Use the drop-down menu to select which rollup method Remote Manager you want to use to display the data values. Note that this drop-down menu does not display if the **1 Hour** time interval option is selected.
4. Click the **Raw Data** tab to view raw data for the selected data stream. Remote Manager displays a table containing one entry for each data point within the selected data stream.

## DIA data management

The Remote Manager DIA (Device Integration Application) service allows you to create custom remote sampling solutions that report data through the DIA database (DIA idigi_db) presentation.

Presentation data is stored in Remote Manager data streams. This allows web services client applications to directly query the data streams. Access to DIA is available through web services and data streams subscriptions. To enable the DIA data management service, you first subscribe to the service.

# Security set up and management

Remote Manager allows users with certain roles and privileges to perform operations, such as making changes or setting up device operations. Each user must be assigned a role when a user account is created.

In addition to user roles, you can create security polices that assign security to devices, require that users log in from a specific IP address or a range of IP addresses, or require two-factor authentication.

- Add and manage users
- Security policies

## Add and manage users

You can add and manage user accounts in the Users page. Each user is assigned a user name and password, which is used to log in to Remote Manager.

To view all users and associated information in the **Users** page, click a column heading in the page to sort the users by that attribute. You cannot sort by role.

The topics in this section explain how to add new users and manage user accounts.

### Add a user

A Remote Manager Administrator can add a new user and set the appropriate privileges for the role of that user.

**Note** An Administrator can also add an application as a user to allow that application to programmatically work in Remote Manager. See Add an application as a user.

1. Click the **Security** tab.
2. Click **Add User**. The **Add User** dialog appears.
3. In the **User Name** field, enter a unique user name. This name cannot be changed once the user account is saved.
4. Fill in the required fields, which are marked with a red asterisk: **Password**, **Confirm Password**, **First Name**, **Last Name**, and **Email**.

5. From the **Role** drop-down list, select a user role: **Administrator**, **User**, or **Read-only User**. See User roles for information about the user role options.

   **Note** Do not select the **Application** or **Read-only Application** options. See Add an application as a user for more information about these options.

6. From the **Security Policy** drop-down list, select a web security policy option if desired. See Security policies for information about the web security policies.
7. Click **OK**.

## Add an application as a user

A Remote Manager Administrator can add an application as a user to allow that application to programmatically work in Remote Manager. This feature creates credentials for an application and allows that application to make web service calls to Remote Manager.

The user account for the application should include a user name that describes the application and the application password. The personal information for the user account could be the information for the application administrator.

1. Click the **Security** tab.
2. Click **Add User**. The **Add User** dialog appears.
3. In the **User Name** field, enter a unique user name that describes the application. This name cannot be changed once the user account is saved.
4. In the **Password** and **Confirm Password** fields, enter the password for the application.
5. Fill in the remaining required fields, which are marked with a red asterisk: **First Name**, **Last Name**, and **Email**.
6. From the **Role** drop-down list, select the **Application** or **Read-only Application** option. See User roles for information about the user role options.
7. From the **Security Policy** drop-down list, select a web security policy option if desired. See Security policies for information about the web security policies.
8. Click **OK**.

## Edit a user profile

You can edit the personal information for any Remote Manager user.

**Note** Your user account must be assigned the Administrator role to be allowed access to the **Security** tab.

1. Click **Security > Users**.
2. Select the user that you want to update.
3. Click **Edit User**. The **Edit User** dialog appears.
4. Fill in the required fields, which are marked with a red asterisk: **First Name**, **Last Name**, and **Email**.

5. From the **Role** drop-down list, select a user role. See User roles for information about the user role options.
6. From the **Security Policy** drop-down list, select a web security policy option if desired. See Security policies for information about the web security policies.
7. Click **OK**. The account profile is updated.

## User roles

Remote Manager allows users with certain roles and privileges to perform operations, such as making changes or setting up device operations. Each user must be assigned a role when a user account is created. Only users assigned an administrator role can create an unlimited number of additional role-based user accounts. See Add a user for information about adding new users.

**Note** The first user created for a customer account is designated by default as the account owner. The account owner also has privileges, even though the account owner is not a user role that can be assigned to a user. See Determine the Account owner for more information.

### *Summary of user roles*

The following table summarizes Remote Manager user roles.

| User Role | Permitted Actions |
|---|---|
| Administrator | Full read/write access to all administrator-only and user-based features within the account, either via web interface or REST APIs.<br>Only administrators can add or remove users, make changes to a user account, change the destination email for device notifications, or update carrier accounts.<br>There must be at least one administrator for each customer account.<br>The account owner is assigned the administrator role by default. |
| User | Read/write access to all resources except administrator-only features, either via web interface or REST APIs.<br>Only users with full user privileges (not read-only) may add or remove devices, or make changes to device alarms and schedules. |
| Read-only user | Read-only access to user-based features, either via web interface or REST APIs. |
| Application | Read/write access to user-based features and can run commands via REST APIs. Application credentials cannot be used to log in to the web interface. |
| Read-only Application | Read-only access to user-based features. Can perform operations but cannot run commands that require write privileges, such as uploading files. Application credentials cannot be used to log in to the web interface. |

## Change account password

A user assigned the Administrator role can change the password for any user account. A user assigned any other role can change only his or her own account.

### *Administrator: Change password for any user account*

1. Click **Security > Users**.
2. Select the user account for which you want to change the password. Only one user account can be selected.
3. Click **Change Password**. The **Change Password** dialog appears.
4. Type in the new password, and then confirm the new password.
5. Click **OK**. The password is updated.

### *User: Change password for own user account*

1. Click **Admin > Account Settings**.
2. Click **My Account**.
3. Click **Change Password**. The **Change Password** dialog appears.
4. Type in the old password and the new password, and then confirm the new password.
5. Click **OK**. The password is updated.

## Forgot user name or password

If you have forgotten your log in credentials, you can access the Remote Manager log in screen for help.

### *Forgot your password*

Follow these instructions to reset your password.

1. Access the Remote Manager log in screen.
2. Click **Forgot Username or Password?**. The **Forgot user name or password** screen appears.
3. Select the **I forgot my password** option.
4. Click **Next**.
5. In the **Username** field, enter the user name associated with the user account.

   **Note** Be sure to enter the correct user name. If the user name is invalid, Remote Manager will not find a user account, and won't send a password reset email.

6. Click **Next**. A message appears in the screen, notifying you that a Remote Manager password reset email has been sent to the email address associated with the user account.

   **Note** If you do not receive a password reset email, verify that the user name you entered is correct.

7. Open the email and follow the instructions. The Remote Manager **Change Password** screen appears.
   - In the **New Password** field, enter the new password.
   - In the **Confirm Password** field, re-enter the same password. The entries in these two fields must match exactly.
8. Click **OK**. The Remote Manager log in screen appears.
9. Log in to Remote Manager, using your new password.

### *Forgot your user name*

Follow these instructions to discover the user names associated with your email address.

1. Access the Remote Manager log in screen.
2. Click **Forgot Username or Password?**. The **Forgot user name or password** screen appears.
3. Select the **I forgot my user name** option.
4. Click **Next**.
5. In the **Email** field, enter the email address associated with the user account.

   **Note** Be sure to enter a valid email address that is associated with a user account. If the email address is invalid or not associated with a user account, Remote Manager will not find a user account, and won't send the informational email.

6. Click **Next**. A message appears in the screen, notifying you that a Remote Manager account information request email has been sent to the email address you entered.

   **Note** If you do not receive an email, verify that the email address you entered is valid and associated with a user account.

7. Open the email. All user names associated with the email address you provided appear in the email. Each user name represents a different user account.
8. Click the link in the email. The Remote Manager log in screen appears. The **Username** field is populated with the first user name in the list found in the email. You can change the user name if you want to access a different user account.
9. Log in to Remote Manager, using the password associated with the user name.

## Remove a user

A user account can be deleted as needed.

**Note** You cannot delete the user account that is designated as the account owner. If you try to delete the account owner user account, an error message appears and the deletion process is canceled.

**Note** Only a user assigned the administrator role can delete a user account.

1. Click the **Security** tab.
2. Select the user account(s) to be removed.

3. Click **Remove Users**. A confirmation dialog appears.
    a. Click **Yes** to confirm the deletion.
    b. Click **No** to cancel the deletion.

### Export a user list to a spreadsheet

You can export a user list from Remote Manager to an Excel spreadsheet file. This enables you to see all users along with their associated email addresses, registration dates, date and time of last login, and password permissions.

1. Click **Security > Users**.
2. Click **Export Users**. An Excel spreadsheet is generated and the file is saved to your Downloads folder.
3. Click the downloaded spreadsheet to open it in Excel.

## Security policies

You can set up different types of security policies that apply additional levels of security. A policy can restrict the users who are allowed to log in to Remote Manager and how they log in, or require that messages must be encrypted.

Click **Security > Polices** to access the Policies page.

**Note** Only users assigned the Administrator user role can access the **Security** tab and manage security policies.

- **Web policy**: A web policy requires users to log in from a specific IP address or range of IP addresses. You must first create a web security policy and then assign it to a user.
- **Duo policy**: Remote Manager integrates with Duo Security to provide two-factor authentication for account users. See Configure Duo two-factor authentication.
- **Device policy**: A device policy can require one or both of the following:
    - All device connections must use SSL (secure socket layer) protocol. See Enforce SSL connection for all device connections.
    - All devices must encrypt messages when communicating over transports such as SMS and SM/UDP. See Enforce encryption for SMS and SM/UDP communications.

### Create a web security policy

You can create a security policy that requires users to log in from a specific IP address or range of IP addresses. For example, to allow Remote Manager users to log in only from certain systems, use the CIDR (Classless Inter-Domain Routing) setting.

**Note** You can also Remove a web security policy after it has been created.

1. Click **Security > Policies**.
2. Click **Web**.
3. Click **Add** in the Policies panel. The **Add New Policy** dialog appears.

4. Type a name and description for the policy. For example, if the policy will apply to a site or office location, provide the name and description for that site.
5. Click **Add**.
6. Select the new policy from the Policies list.
7. Click **Add** in the **Rules** panel. The **Add New Rule** dialog appears.
8. Select **CIDR Block** from the drop-down menu.
9. Type the rule. You must provide an IP address with wildcards that specify the value for the 32-bit IP address. You can use a CIDR converter, if needed. Examples:
    - 192.0.0.0/8 (allow any IP address that starts with 192)
    - 192.168.0.0/16 (allow any IP address that starts with 192.168)
    - 192.168.1.0/24 (allow any IP address that starts with 192.168.1)
    - 192.168.1.27/32 (only allow IP address 192.168.1.27)
10. Provide a description of the rule. For example: "Log in allowed from IP address ranges from 192.168.1 to 255".
11. Click **Add**. The rule displays in the **Rules** pane.
12. You can remove a rule that is not needed.
    a. In the **Rules** pane, select the rule you want to remove. The **Remove** button appears in the toolbar.
    b. Click **Remove**.
13. Apply the new security policy to one or more users from the **Security > Users** tab. See Assign a web security policy to a user.

## Assign a web security policy to a user

A Remote Manager administrator can assign security policy to a user or users. You must have created at least one web security policy. See Create a web security policy.

**Note** You can Remove a web security policy from a user account if needed.

1. Click **Security > Users**.
2. Select a user account or shift-select multiple accounts.
3. Click **Assign Policy**.
4. Use the drop-down box to select a policy for the selected user(s).
5. Click **Set**. The security policy is applied to the selected users.

## Remove a web security policy

A Remote Manager administrator can remove a web security policy from a customer account in Remote Manager. If the policy has been assigned to a user account, the policy must be removed from the user account before it can be removed from the customer account.

### *Remove a web security policy from a customer account*

1. Click **Security > Policies > Web**.
2. Select a policy or shift-select multiple policies.
3. Click **Remove**. A confirmation dialog appears.
   - Click **Yes** to remove.
     - If the policy is not assigned to any user accounts, the policy is deleted.
     - If the policy is assigned to a user account, a confirmation dialog appears, and displays a list of the users assigned the policy. Make note of the list of users, and click **OK** to close the dialog. You must unassign the policy from these user accounts before you can delete the web security policy from your customer account. See Remove a web security policy from a user account.
   - Click **No** to cancel.

### *Remove a web security policy from a user account*

1. Click **Security** > **Users**.
2. Select the user to which the policy is assigned or shift-select multiple users.
3. Click **Edit User**. The **Edit User** dialog appears.
4. From the **Security Policy** list box, select the "none" option or select a different security policy.
5. Click **OK** to save the change.

## Configure Duo two-factor authentication

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 Remote Manager from one device must also authenticate his or her log in from a second device, such as a mobile phone.

Once 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 Remote Manager. Users with application or read-only application roles are not managed by the Duo Security application.

### *Before you begin*

To implement two-factor authentication, an administrator must first sign up for a Duo Security account and then add the Remote Manager application to the account. Contact your Remote Manager account representative for information on setting up and integrating Duo two-factor authentication.

### *Configure Duo two-factor authentication*

After the Duo Security account has been added, follow the steps below to configure your Remote Manager account to use the Duo two-factor authentication.

1. Make sure you have the Duo Security integration key and secret key, and your API host name.
2. Click **Security > Policies**.
3. Click **Duo**.

4. 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.
5. Click **Save**.

For information about the Duo Security policy view, see Security > Policies > Duo view.

## Enforce SSL connection for all device connections

You can require all device connections to use SSL (secure socket layer) protocol. This feature can be enabled only by a user with administrative privileges.

For information about the device policy view, see Security > Policies > Device view.

1. Click **Security > Policies**.
2. Click **Device**.
3. Select the **SSL Required** option to enable the feature.
4. Click **Save**.

## Enforce encryption for SMS and SM/UDP communications

You can require devices to encrypt messages when communicating over transports such as SMS and SM/UDP. This feature can be enabled only by a user with administrative privileges.

For information about the device policy view, see Security > Policies > Device view.

1. Click **Security > Policies**.
2. Click **Device**.
3. Select the **SM Encryption Required** option to enable the feature.
4. Click **Save**.

# Remote Manager Account administration

You can manage your Remote Manager account settings, subscriptions, and customer account information in the **Admin** page. You can also view the usage levels for services and view event information in the event log.

## Manage your Remote Manager account

If you are the account owner, you can use the Manage Services portal to request changes to your account. For example, you can add or cancel service subscriptions, increase device limits, or upgrade your account edition. This section describes how to use the Manage Services portal to manage your account.

### Increase the device limit for a customer account

If you have a Platform, Standard, or Premier Edition customer account, you can increase the device limit on your account using the Manage Services portal. Devices are added to your account inventory at your current contracted price. You will receive an email confirming your order, and an invoice for the additional devices is issued separately.

Only the customer account owner is able to access the **Manage Services** options.

1. Click **Manage Services** in the Remote Manager banner.
2. Select **Add Devices**.
3. Indicate the number of devices you would like to add to your account.
4. Click **Submit**.

### Upgrade account edition or add services

If you want to upgrade your edition or add bundles or features to your account, you can use the Manage Services portal to send your request to a Remote Manager representative.

Only the customer account owner is able to access the **Manage Services** options.

1. Click **Manage Services** in the Remote Manager banner.
2. Select **Upgrade edition or add bundles/features**.
3. Use the text field to describe the changes you want to make to your account.
4. Click **Submit**. A Remote Manager representative will contact you to process your request.

### Upgrade a trial or Developer Edition account

If you want to upgrade your trial or Developer Edition account to a full Remote Manager account, you can use the Manage Services portal to send your request to a Remote Manager representative.

Only the customer account owner is able to access the **Manage Services** options.

1. Click **Manage Services** in the Remote Manager banner.
2. Use the text field to describe the changes you want to make to your account.
3. Click **Submit**. A Remote Manager representative will contact you to process your request.

### Active user menu

The Remote Manager banner displays the user name of the user currently logged in. This indicator also functions as a drop-down menu allowing access to account information or to log out of Remote Manager.

| Menu option | Description |
|---|---|
| **My Account** | Select **My Account** to display an overview of available account information. Users can edit account information, change passwords, and request a vendor ID number (if applicable) from this page. This information can also be accessed by clicking **Admin > Account Settings > My Account**. See Account settings for detailed information. |
| **Getting Started** | Select **Getting Started** to display basic information about connecting a device to Remote Manager. |
| **Logout** | Select **Logout** to log out of Remote Manager. |

## Account settings

You can manage the settings for your account in the Account Settings views, available from the **Admin** tab.

### Manage your user profile

Click **Admin > Account Settings > My Account** to display your account settings.

- Edit your user profile
- Change account password
- Configure provisioning
- My Account view

### Manage alarm notifications

Click **Admin > Account Settings > Notifications** to manage any alarm notifications that should be sent to you.

**Note** You must have previously created an alarm before you can create an alarm notification for a user account. See Alarms.

- Configure email notifications for an alarm
- Notifications view

## Manage carrier information

Click **Admin > Account Settings > Carrier Account** to manage account information for the carriers you are using.

- Carrier accounts
- Carrier account view

## Manage account preferences

Click **Admin > Account Settings > Preferences** to manage your preferences for session timeout, storing device data, and health metrics.

- Configure session timeout
- Enable and disable device data storage
- Configure health metrics data expiration in Remote Manager
- Preferences view

## Edit your user profile

You can edit the personal information in your Remote Manager user profile. This information was entered when your user account was created.

1. Click **Admin > Account Settings > My Account**.
2. Click **Edit Profile**. The **Edit Profile** dialog appears.
3. Enter new or revised details. The required fields are marked by a red asterisk.
4. Click **OK**. The account profile is updated.

## Configure provisioning

You can configure the provisioning details for your vendor ID. This process specifies the default configuration that is applied to devices when a device is added to this customer account.

1. Click **Admin > Account Settings**.
2. Click **My Account**.
3. Click **Provisioning Configuration**. The **Configure Provisioning** dialog appears.
    a. From the **Restricted Status** list box, select the default restriction status for newly provisioned devices in your account. See My Account view for information about the options.
    b. From the **Group** list box, select the default group into which newly provisioned devices are placed. See My Account view for information about the options.
4. Click **OK**. The account profile is updated.

### Configure session timeout

You can configure how long a Remote Manager session should remain open and inactive. By default, Remote Manager times out after 30 minutes of inactivity.

1. Click **Admin > Account Settings > Preferences**.
2. Under **Security**, designate the session timeout duration as a value, in minutes, between 5 and 1440.
3. Click **Save**. Remote Manager briefly displays a confirmation message at the top of the banner.

### Enable and disable device data storage

The Device Data function controls whether Remote Manager stores data from your devices into persistent storage such as Data Streams or Data Files.

**Note** When device data storage is disabled, data is still published via Push Monitors.

1. Click **Admin > Account Settings > Preferences**.
2. Determine whether device data is stored in persistent storage.
   - **Enable**: Select the **Store Data Sent from Devices** option. The device data is stored in persistent storage.
   - **Disable**: Deselect the **Store Data Sent from Devices** option. The device data is not stored in persistent storage.
3. Click **Save**.

## Services

The Services view shows a summary of service usage information for the selected billing period. Click the arrow for each usage type to expand the section and display additional information.

**Note** If you are logged into a customer account that has subaccounts, service usage information is displayed only for the parent account. Subaccount information does not roll up into the parent account.

### Refresh service usage

You can retrieve updated information on your subscriptions and service usage for a selected month.

1. Click **Admin > Services**.
2. Select the month you want to view from the drop-down menu. Updated usage information is displayed for the selected month.
3. Click the **Refresh** icon to update the data.

# Remote Manager Account administration

You can manage your Remote Manager account settings, subscriptions, and customer account information in the **Admin** page. You can also view the usage levels for services and view event information in the event log.

### Export subscriptions to Excel

You can export the data describing your Remote Manager subscriptions for accounting or other purposes.

1. Click **Admin > Subscriptions**.
2. Click the **Export Subscriptions** button. An Excel spreadsheet is generated and the file is saved to your Downloads folder.
3. Click the downloaded spreadsheet to open it in Excel.

## Customer accounts and subaccounts

This section includes information about adding a subaccount to a customer account and how to export a customer list to an Excel spreadsheet.

### About subaccounts

Remote Manager customer accounts can have customer subaccounts assigned to it, so that one Remote Manager customer account can be the parent of associated subaccounts. Each parent account can have multiple subaccounts. Only a parent account can have subaccounts.

When you are logged in as an administrator of the parent account, you can:

- View all customer subaccounts associated with the parent account. See Admin > Customers view.
- View and work with devices from the perspective of a selected customer subaccount.

When you are logged in as an administrator of a subaccount, you can view all device data collected within the subaccount. You cannot view the data for the parent account or any other subaccounts associated with the parent account.

Contact your Remote Manager service representative to find out more about Remote Manager subaccounts.

### Select a customer subaccount

If you are logged in to a Remote Manager account that has associated subaccounts, you can view account information for a selected subaccount.

1. Click **Admin > Customers**.
2. Double-click the subaccount you want to select. The subaccount is now the currently selected account. You can view and manage Remote Manager devices as if you were a logged in user of the subaccount. A message appears indicating the current active customer, and the  icon is displayed next to the selected customer subaccount.

### Add a subaccount

If you are an administrator of an account for which the subaccount feature has been enabled, you can create additional Remote Manager accounts that function as subaccounts. When you create a subaccount, you also automatically create a user for the account that is an administrator for the account.

1. Log in to Remote Manager as an administrator of an account for which the subaccount feature has been enabled.
2. Click **Admin > Customers**.
3. Click **Add Subaccount**.
4. Provide the following information:

   **Company:** Enter the company name for the account.
   **Email:** Provide an email contact for the account.
   **User name:** Assign a username for the account.
   **Password:** Provide an initial password for the account user.

5. Click **OK**.

A new Remote Manager account is created as a subaccount of the current account.

### Export a customer list to Excel

Remote Manager can export a customer list to an Excel file. The spreadsheet includes information about the customer sub-accounts, such as customer ID, company name, phone number, and customer account number. See Admin > Customers view for more detailed information.

**Note** You must be assigned the Administrator role to be able to access the customer sub-account information.

1. Click **Admin > Customers**.
2. Click **Export Customer List**. An Excel spreadsheet is generated and the file is saved to your downloads folder.
3. Click the downloaded spreadsheet to open it in Excel.

## Event log

The event log includes information about devices that you have added or removed from Remote Manager.

By default, the event log shows events that have occurred in the previous 30 minutes. You can select different time view options from the time list box. You can also specify a time range. Events that occurred during this time range appear in the view.

## View the event log

1. Click **Admin > Event Log**. The Admin > Event log view appears.
2. Specify the time range for which you want to display events. The default is 30 minutes.
    a. Click the down arrow to select a different time range option. Select one of the following options:
        - Select the **Show events for the last** option and select a time range option from the list box.
        - Select the **Show events for the following time range** option, and use the calendars in the **From** and **To** fields to specify the beginning and end date and time of the time range.
    b. Click **OK**. The view is updated to display events that occurred during the selected time range.
3. To see details for an Event, double-click the Event. The Admin > Event log > Event log details view appears.

# Remote Manager views

# Dashboard view

The **Dashboard** view shows device health and status. The dashboard includes four charts: Device Health, Connection Status, Alarm Summary, and Monitor Status.

Click the **Dashboard** tab to display the **Dashboard** view.

## Charts

| Chart | Description |
|---|---|
| Device health | Shows a summary of the health for all devices in your Remote Manager account. Device health is determined by a set of health metrics reported by devices.<br>Sample health metrics include cellular signal strength and quality, CPU and memory usage, local network performance statistics, and so on.<br>For each health metric the device reports, you can configure three thresholds: normal, warning, and error. The overall health of a device is reported as an aggregate of all health metrics for the device:<br>■ **Normal:** All health metrics for the device are within configured normal thresholds.<br>■ **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.<br>■ **Error:** At least one health metric for the device is within a configured error threshold.<br>■ **Unknown:** Device health information is not found and the device health state is unknown.<br>You can filter the Device Health chart by group or device type. You can also filter the chart by including or excluding specific device health statuses. |
| Connection status | 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. You can filter the Connection Status chart by group or device type. You can also filter the chart by including or excluding the connection statuses. |
| Alarm summary | Shows a summary of all fired alarms by alarm type. You can filter the chart by including and excluding one or more alarm types. You can also filter the chart by including or excluding alarm by alarm type. |
| Monitor status | Shows a summary of all system monitors by monitor status: Inactive, Active, Disabled, Suspended, Disconnecting, and Connecting. You can filter the chart by including and excluding monitor statuses. You can also filter the chart by including or excluding monitor statuses. |

## Actions

| Action | Description |
|---|---|
| Filter by group | Selects the groups by which to filter the charts. More than one can be selected. |
| Filter by device type | Selects the device types by which to filter the charts. More than one can be selected.<br>Click (gear icon next to the device type) to define thresholds for a device type. See Configure device health thresholds in Remote Manager for more information. |
| History | Click the **History** link beneath the Connection Status chart to display the **Connection Status History** section. This section displays historical connection information for the devices being monitored.<br>See Connection Status History chart. |

# Device Management tab

Use the **Device Management** tab to manage devices registered to your Remote Manager account.

## Displays tabs

| Tab | Description |
|---|---|
| **Devices** | Monitor and manage devices in your inventory. See Add devices to Remote Manager. |
| **XBee Networks** | View the XBee gateways in your inventory. See XBee networks. |
| **Alarms** | Create and manage alarms. See Alarms. |
| **Operations** | View and manage Remote Manager jobs. See Operations. |
| **Schedules** | View and manage schedules. See Schedules and tasks. |
| **Carrier** | View and manage carrier subscriptions. See Carrier accounts. |
| **Profiles** | Create a default profile for a specific device type. This profile is applied when you add a device of the same type. See Profiles. |

## Buttons

| Button | Name | Action |
|---|---|---|
| Groups... | Groups | Displays the Groups menu for adding, removing, and editing groups. |
|  | Show/Hide Groups | Toggles the display to show or hide the Groups pane. |
|  | Toggle Flat View | Toggles the display to show or hide flat view. Flat view shows all the devices, regardless of subfolders. |
|  | Show/Hide Map | Toggles the display to show or hide the Map pane. |
|  | Refresh | Refreshes the display with current data from the server. |
| Add Devices | Add Devices | Adds one or more devices to your inventory. |
| Remove Devices | Remove Devices | Removes the selected device from you inventory.<br>This button displays when a device has been selected. |

| Button | Name | Action |
|---|---|---|
| Properties | Properties | Displays properties for the selected device.<br>This button displays when a device has been selected. |
| More... | More | Displays additional options for the selected device. Available options vary depending on the selected device. See More button options for more information. |

## Columns

| Column | Description |
|---|---|
| Active/Inactive | Displays an icon to show whether a device is active or not active. |
| MAC Address | Displays the MAC address of the device. |
| Device ID | Displays the device ID assigned to the device by Remote Manager when the device is added. |
| IP Address | Displays the IP address of the device. |
| Device Type | Displays the type of device. |
| Description | Displays an optional description of the device. |
| Firmware level | Displays the firmware version installed on the device. |
| Health Status | Displays the current health status for the device: Normal, Error, or Unknow. |
| Last Update Time | Displays the last time on which the device was updated. |
| User Meta Data | Displays the meta data assigned to the device. See Add or edit device metadata. |
| Tags | Displays the tags assigned to the device. See Add device tags. |
| Group Path | Displays the path of the group to which the device is assigned. See Add devices to a group. |

## More button options

| Menu option | For more information, see.... |
|---|---|
| Add devices | Add devices to your inventory individually |
| Bulk Add devices | Add multiple devices using a CSV file |
| Remove devices | Remove a device from Remote Manager |

| Menu option | For more information, see.... |
|---|---|
| Properties | View device properties |
| Upload files | Upload files to a device |
| Upload Python files | Upload files to a device |
| Customization | Customize device attributes |
| Reboot | Reboot devices |
| Disconnect | Disconnect a device |
| Restrict | Restrict and unrestrict a device |
| Show tasks | Run My Task device tasks |
| Export Properties | Export device properties |
| Import Properties | Import device properties |
| Update firmware | Update device firmware |
| Update Gateway Radio Firmware | Use this menu option to update the XBee radio firmware on the gateway(s). |
| Update XBee node firmware | Use this menu option to upload firmware files for each type of XBee node you would like updated. These files typically have .ebl extensions. The gateway must also be configured to enable over the air and auto updates. |
| Edit tags | Edit device tags |
| Edit MetaData | Add or edit device metadata |
| Assign to Group | Add devices to a group |
| Export Devices | Export device properties |
| Refresh descriptors | Click **More > Refresh Descriptors** to update the list of descriptors. |
| Edit Descriptors | Add a descriptor |
| Clear Descriptors | Click **More > Clear Descriptors** to remove the descriptors that you have added to the list. |
| Send Message (SM/UDP) | Connect a device via SM/UDP |
| Configure (SM/UDP) | Enable SM/UDP |
| Send message (SMS) | Send a message via SMS |
| Provision (SMS) | Request SMS provision response |
| Configure (SMS) | Configure device phone number |

# Device health configuration view

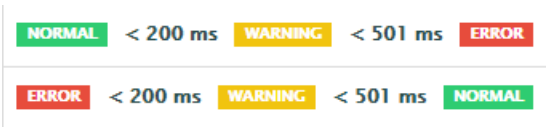
The **Device health configuration** view shows the health metrics and thresholds used to report device health.

See Configure device health thresholds in Remote Manager for information about accessing and editing the items in this view.

## Columns

| Column | Description |
|---|---|
| Metric | Shows the data stream that contains the health metric data. |
| Enabled | Shows whether the metric is included or excluded in determining the health status of the device. |
| Thresholds | Shows the threshold values for normal, warning, and error. |
| Actions | Displays available actions: Edit, Save, Cancel, and Sort. |

## Buttons

| Button | Description |
|---|---|
| Edit | Modifies threshold values for normal, warning, and error. |
|  | Reverses the ordered set of thresholds:<br>  |
| Save | Saves configuration settings. |
| Cancel | Cancels configuration settings. |

# Device management > Devices view

The **Device management > Devices** view lists all devices in your Remote Manager inventory. For each device, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| Connection status | Displays an icon for connection status:<br>  Connected: Indicates the device is connected to a network.<br>  Disconnected: Indicates the device is not currently connected to a network. |
| MAC address | Displays the MAC address associated with the device. |
| Device ID | Displays the device ID associated with the device. |
| IP address | Lists the IP address, if known. |
| Device type | Displays the configured device type. |
| Description | Displays a user-specified description for the device. |
| Firmware level | Displays the current firmware associated with the device. |
| Last update time | Displays the time in minutes, hours or days since the device was last updated. |
| User meta data | Displays user-specified data associated with the device. |
| Tags | Lists user-specified tags associated with the device. |
| Group path | Displays the location in the device group hierarchy under the root-level directory. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Show/hide groups | Shows or hides the Groups menu. |

| Button | Name | Description |
|---|---|---|
|  | Toggle flat view | Toggles all device and network views from flat to nested view.<br>■ Flat view displays all devices for the selected group and all subgroups. By default, the flat view is used.<br>■ Nested view displays the devices in the selected group only; that is, devices in subgroups of the selected group are not included.<br>Toggling this display affects all Remote Manager views that support flat and nested views. For example, if you switch from flat to nested view on the Devices view, the XBee Networks view also switches to nested view. |
|  | Show/hide map | Toggles the display of the map. By default, the map is hidden from view.<br>See View the device map. |
|  | Refresh | Refreshes the device list. |
| Add Devices | Add devices | Adds devices to your inventory. |
| Remove Devices | Remove devices | Removes the selected devices from your inventory. |
| Properties | Properties | Displays properties for the selected device. |
| More... | More | Displays additional options for the selected device. You can also right-click a device to display the same options available with the More menu. |

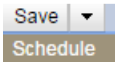
# Device management > Devices > Device properties view

The **Device management > Devices > Device properties** view displays device properties for the selected device in a two-pane display.

## Views

| Display | Description |
|---|---|
| Menu | Displays menu of configuration options. Options displayed are dependent on the selected device. |
| Device details display | Displays details for each device:<br>■ **Summary dash board:** If data is available for the device, displays a chart depicting connection history for the device.<br>■ **Configuration:** Settings for the selected menu option. |

## Buttons

| Button | Description |
|---|---|
|  | Immediately saves the current configuration settings, schedule a time for saving the configuration, or save the configuration settings to the device the next time the device is on line. |
|  | Exports the device configuration settings to a local XML file. The exported file can be imported back to another device of the same type. |
|  | Refreshes the display. |

# Device management > XBee networks view

The **Device management > XBee networks** view displays detailed information for all XBee network nodes in your inventory. For each XBee network node, Remote Manager displays the following details:

## Columns

| Column | Description |
|---|---|
| Extended address | Displays an icon that indicates the XBee device type. The extended address for the device displays next to the XBee device type icon.<br>  Coordinator node<br>  Router node<br>  End device<br>  New device that requires discovery |
| Gateway device ID | Shows the device ID of the device that contains the XBee gateway for the network to which the device belongs. |
| Node ID | Displays the user-specified descriptive name for the XBee node. |
| Model type | Displays the XBee module type. This is not supported on all XBee devices. |
| Product type | Describes the physical device that contains the XBee radio. This is not supported on all XBee devices. |
| Node type | Displays the device type identifier (AT DD setting). This is not supported on all XBee devices.<br>For more information on XBee node settings, see XBee product documentation available at www.digi.com/support. |
| Service | Displays the network service supporting the XBee gateway. |
| Role | Describes the type of XBee device:<br>Router<br>Coordinator<br>End node<br>Unknown |

| Column | Description |
|---|---|
| Network address | Displays the 16-bit network address (AT MY setting) of the XBee module.<br>A value of 0xFFFE means the module has not joined an XBee network. For more information on XBee node settings, see XBee product documentation available at www.digi.com/support. |
| Parent address | Displays the 16-bit network address of the XBee module parent (AT MP setting).<br>A value of 0xFFFE means the module does not have a parent. For more information on XBee node settings, see XBee product documentation available at www.digi.com/support. |
| Last synchronized | ■ For Smart Energy devices, displays the last time Remote Manager detected a status change for the node. Use this value to determine how long a node has been active or inactive.<br>■ For other device types, displays the last time Remote Manager discovered the node. |
| Status | Indicates whether the XBee node is currently connected to or disconnected from Remote Manager:<br>**Active:** Last reported node status indicated an active connection.<br>**Inactive:** Last reported node status indicated an inactive connection.<br>**blank**: No reported status for the node/device.<br>**Note** XBee node status is based on the node presence on the HAN, not the connectivity status of the gateway. Remote Manager displays the last reported node status in this column. Therefore, the gateway connection to Remote Manager can be inactive while the XBee node shows an **Active** status in this column. |
| Meta data | Displays user-specified data, such as location or keywords. |

## Buttons

| Button | Description |
|---|---|
|  | Shows or hides the **Groups** menu. |

| Button | Description |
|---|---|
|  | Toggles all device and network views from flat to nested view.<br>■ Flat view displays all devices for the selected group and all subgroups. By default, the flat view is used.<br>■ Nested view displays the devices in the selected group only; that is, devices in subgroups of the selected group are not included.<br>Toggling this display affects all Remote Manager views that support flat and nested views. For example, if you switch from flat to nested view on the Devices view, the XBee Networks view also switches to nested view. |
|  | Refreshes the device list. |
| Export Networks | Exports XBee network information to a local Microsoft Excel file. |
| Discover | Sends an XBee Discover command to the selected XBee coordinator or gateway. If you select an XBee end node, Discover is sent to the gateway of the XBee end node. Use the **Clear the cache on the device and perform a full rediscover** to clear the device cache before performing the discover. In addition, you can schedule when to perform the discovery.<br>See Discover an XBee device for more information. |
| Properties | Displays properties for the selected XBee device(s). |

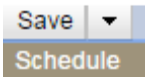
# Device management > XBee networks > XBee network properties view

The **Device management > XBee networks > XBee network properties** view displays network properties for the selected node in a two-pane display. To display this view, select an XBee network and click **Properties**.

## Views

| Display | Description |
|---|---|
| XBee menu | Displays a menu of configuration options. Options displayed are dependent on the device type. |
| Smart energy | Displays Smart Energy settings for Smart Energy devices.<br>For more information on XBee node configuration, see XBee product documentation available at www.digi.com/support; for information on Remote Manager web services, see the *Remote Manager Programmer Guide*. |

## Buttons

| Button | Description |
|---|---|
|  | Immediately saves the current configuration settings or allows you to schedule a time for saving the configuration to the device. |
|  | Exports the device configuration settings to a local XML file. The exported file can be imported back to another device of the same type. |
|  | Refreshes the display. |

# Device management > Alarms view

The **Device management > Alarms** view lists all alarms for your account. For each alarm, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| Alarm ID | Displays the unique ID assigned to the alarm. Individual operations are referred to as jobs. |
| Status | Displays the status of the alarm as well as the alarm's trigger count:<br>  <br>Fired and trigger count: Indicates the alarm has been triggered and shows the current trigger count. When an alarm is fired, the trigger count goes up. When an alarm is reset or acknowledged, the trigger count goes down.<br>  <br>Normal: Indicates that no alarm conditions exist for the specified alarm. |
| Name | Displays the name of the specific alarm. This is the name you give the alarm when you create it. |
| Description | Displays the description of the alarm. |
| Enabled | Specifies whether the alarm is enabled or disabled:<br>■ **Enabled**: Indicates that an alarm is enabled and Remote Manager is monitoring the conditions specified within the alarm.<br>■ **Disabled**: Indicates that an alarm is disabled. |
| Group path | Displays the name of the group or group pathway containing the device(s) targeted by the selected alarm. |
| Severity | Displays a severity rating for an alarm, based on the importance of that alarm. Severity ratings can be set to High, Medium or Low. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the alarm list. See Refresh alarms list. |
|  | Add | Adds a new alarm to your account. See Create an alarm. |

| Button | Name | Description |
|---|---|---|
| Alarm Status | Alarm Status | Displays detailed status information for the selected alarm. See View alarm status. |
| Edit | Edit | Updates an alarm configuration. See Edit an alarm configuration.<br>**Note** You can only edit the alarms that you have added. You cannot edit alarms that were added by another user. |
| Remove | Remove | Deletes an alarm that is no longer needed. Confirmation is not required to delete an alarm. See Delete an alarm.<br>**Note** You can only delete the alarms that you have added. You cannot delete alarms that were added by another user. |
| Enable/Disable Alarm ▾ | Enable/Disable Alarm | Disables an alarm that you do not want Remote Manager to monitor. This feature is useful if you want to control when an alarm is in use instead of deleting it. After an alarm has been disabled, you can enable the alarm at any time. See Enable or disable an alarm.<br>**Note** You can only enable or disable the alarms that you have added. You cannot enable or disable alarms that were added by another user. |

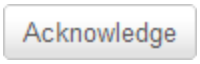
# Device management > Alarms > Alarm status view

The **Device management > Alarms > Alarm status** view lists the fired alarm events for the selected alarm. The events are sorted in reverse order of time, with the most recent alarm at the top of the page. You can view reset/acknowledged events for the alarm using the filter options in the upper-right corner of the page.

## Columns

| Column | Description |
|---|---|
| Source entity ID | Identifies the source entity that caused the alarm condition. A source entity can be a device ID, XBee node extended address, or any other entity depending upon the alarm type. |
| Details | Displays detailed information about the alarm event. |
| Timestamp | Indicates the date and time the event occurred. Events are sorted in reverse order of time, with the most recent alarm at the top of the page. |
| Status | Indicates the present condition of the alarm:<br>■ **Fired**: Alarm has fired.<br>■ **Reset**: Fired alarm has been reset.<br>■ **Acknowledged**: Fired alarm has been acknowledged. An acknowledged alarm indicates the alarm has been investigated but remains in alert status until the alarm is reset (automatically or manually). |

## Buttons and filter options

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the list of displayed events. |
|  | Acknowledge | Acknowledges the selected alarm event. An acknowledged alarm remains in alert status, but no longer commands attention within Remote Manager. Once the alarm is reset (automatically or manually), the alarm is a candidate for re-firing.<br>This button displays only when you select an event with the FIRED status.<br>See Acknowledge an alarm. |

| Button | Name | Description |
|---|---|---|
| Reset | Reset | Resets the selected triggered or acknowledged alarm condition. Remote Manager clears the alarm status and rearms the alarm for future triggering by the original alarm condition.<br>See Reset an alarm. |
| Show History | Show history | Displays or hides alarm history information. By default, alarm history information is not included in the display for an alarm.<br>See View the status history of an alarm. |
|  | Filter options | Includes/excludes reset and/or acknowledged alarms:<br>■ **Hide reset alarms**: Hides reset alarms. This option is selected by default.<br>■ **Hide acknowledged alarms**: Hides acknowledged alarms. This option is selected by default.<br>See View the status history of an alarm. |

# Device management > Operations view

The **Device management > Operations** view lists all operations for your Remote Manager account performed within the last 24 hours.

For each operation, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| Operation status | Displays an icon that shows the status of the operation:<br> In process: Operation is being executed.<br> Success: Operation completed successfully.<br> Disabled: Operation was canceled.<br> Disabled: Operation failed. |
| Operation type | Displays the type of operation being performed:<br>No icon: Standard Remote Manager job. Double-click to display job details.<br> Task icon: Remote Manager task. Double-click to view task details. |
| Operation ID | Displays system-assigned unique ID for the job. Individual operations are referred to as jobs. |
| Operation | Displays the name of the operation. |
| % | Displays the completion percentage for the operation or the number of devices that have completed the operation:<br>■ For an operation performed on a single device, displays the percentage of completion for the operation.<br>■ For an operation performed on multiple devices, displays the number of devices that have completed the operation or task. |
| Submitted | Displays the date and time the operation was submitted. |
| Completed | Displays the date and time the operation was completed. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the operations list. |
| Delete | Delete | Deletes the selected operation. |
| Operation Details | Operation details | Displays detailed information for the selected operation. The details view displays jobs details for the operation or task details for scheduled operations. |

# Device management > Operations > Operation details view

The **Device management > Operations > Operation details** view shows detailed information for the selected operation. An operation can be a job or a scheduled task. For each, Remote Manager displays the following details.

| Column | Description |
|---|---|
| Job or task detail | Shows detailed request for the job or task. |
| Job or task targets | Lists devices targeted by the job or task. |
| Target's response | Shows the detailed response for the job or task. |

# Device management > Schedules view

The **Device management > Schedules** view lists all scheduled tasks for your Remote Manager account. For each scheduled task, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| ID | Displays the unique system-assigned identifier for the scheduled task. Individual tasks run as jobs within the system. |
| Status | Displays the current status of the task:<br>Active: An active scheduled task is either currently running or scheduled to run at a specified date and time.<br>Inactive: An inactive scheduled task is either complete or canceled. See Disable a schedule. |
| Description | Displays the user-assigned name of the scheduled task. |
| Start time | Displays the date and time the task is scheduled to start. |
| Stop time | Displays the date and time the scheduled task ends for recurring scheduled tasks. |
| Previous run time | Displays the date and time the task last ran. |
| Next run time | Displays the date and time the task is next scheduled to run. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the current list of schedules. |
| New Schedule | New schedule | Creates a new scheduled task. |
| Edit | Edit | Edits the selected scheduled task.<br>See Edit a schedule. |

| Button | Name | Description |
|---|---|---|
| Cancel | Cancel | Cancels the selected scheduled task and sets the status to inactive. A canceled task does not execute.<br>See Disable a schedule and Enable a schedule. |
| Delete | Delete | Deletes the selected scheduled task.<br>See Delete a schedule. |

# Device management > Carrier > Usage view

The **Device management > Carrier > Usage** view displays cellular carriers, services, and plans for cellular-enabled devices in your inventory. For each device that is cellular-enabled, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| ICCID/MEID/ESN | Displays the device or SIM ICCID or MEID/ESN number associated with the rate plan.<br>■ **ICCID:** Unique identifier for a SIM. Typically the ICCID is printed on the SIM card. This number is similar to a serial number and cannot be changed.<br>■ **MEID/ESN:** Uniquely identifies a CDMA device. This number corresponds to the device rather than a SIM card. The use of ESN is being phased out in favor of MEID.<br>The usage list includes an entry for each rate plan corresponding to an ICCID/MEID/ESN number. |
| IMSI | Displays the IMSI code, a number that uniquely identifies the SIM on the carrier network. The codes include:<br>■ MCC: Mobile Country Code (for example, 310 for USA)<br>■ MNC: Mobile Network Code (for example, 410 for AT&T)<br>■ MSIN: Moble Sequential serial Identification Number |
| Device ID | Lists the device ID of the device integrated with a carrier. |
| Service | Displays the carrier-specific rate plan associated with your carrier account: cellular data or cellular SMS.<br>If your carrier account can use both cellular data and SMS, the usage list includes an entry for each.<br>If SMS is not available in your carrier API or Remote Manager cannot send or receive SMS message to mobile devices on your cellular plan, then an SMS rate plan is not displayed in the usage list. |
| Plan | Displays the carrier-specific rate plan associated with your carrier account: cellular data or cellular SMS.<br>If your carrier account can use both cellular data and SMS, the usage list includes an entry for each. |
| Usage #1 | Displays the total amount of cellular data used during the selected billing period.<br>For cellular SMS services, displays the total number of SMS messages sent and received during the selected billing period. |

| Column | Description |
|---|---|
| Usage #2 | Displays the number of data sessions for the selected billing period.<br>A data session includes receiving information (such as news, weather updates, and stock quotes), internet browsing, taking and sending pictures, as well as downloading applications and music.<br>Vodafone only: Displays the total number of SMS messages received during the selected billing period. |
| Usage #3 | Displays national and international usage during the selected billing period.<br>■ If your cellular provider does not track national and international usage separately, this column is blank.<br>■ If your cellular provides tracks national and international usage separately, displays the total amount of international cellular data used during the selected billing period.<br>■ Vodafone only: Displays the total number of SMS messages sent during the selected billing period. |
| Usage #4 | Displays the number of international data sessions during the selected billing period.<br>■ If your cellular provider does not track national and international usage separately, this column is blank.<br>■ If your cellular provider tracks national and international usage separately, displays the number of international data sessions during the selected billing period. |
| Billing period | Displays the month and year corresponding to the usage amounts displayed in this view.<br>**Note** This column specifies a calendar month. The calendar month does not represent a billing period for your carrier. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the carrier usage display. |
| Update Usage | Update usage | Retrieves the latest usage information for the selected carrier. |
| Details | Details | Displays a chart that depicts usage information over time for the selected carrier. |

# Device management > Carrier > Carrier > Carrier usage details view

The **Device management > Carrier > Carrier usage details** view displays data usage details in a two-pane display.

| Display area | Description |
|---|---|
| Chart | Shows a chart that depicts a rollup of usage information over time for the specified date range. Usage information corresponds to data usage transferred or SMS usage (measured by the number of messages), depending on the type of usage information displayed. |
| Raw data | Displays the raw data for the chart display.<br>■ **Time:** Displays the timestamp when the raw data was gathered.<br>■ **Data:** Displays the numerical data. Each data enty within the table corresponds to a data point within the chart. |

## Options

| Option | Description |
|---|---|
| Interval | Selects the time interval for the chart: 7 Days, 1 Month, 6 Months, or 1 Year. |
| Rollup type | Specifies the rollup type:<br>■ **Average:** Average of all values in each rollup interval.<br>■ **Sum:** Sum of all values in each rollup interval.<br>■ **Min:** Minimum value of each rollup interval.<br>■ **Max:** Maximum value in each rollup interval.<br>■ **Count:** Count of all data points in each rollup interval.<br>■ **Std. Deviation:** Standard deviation of all values in each rollup interval. |

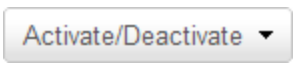
# Device management > Carrier > Management view

The **Device management > Carrier > Management** view manages carriers integrated with your Remote Manager devices.

## Columns

| Column | Description |
|---|---|
| Status | Displays the status of the carrier: active or inactive. |
| ICCID/MEID/ESN | Displays the ICCID or MEID/ESN number associated with the device or device SIM.<br>■ **ICCID:** Unique identifier for a SIM. Typically the ICCID is printed on the SIM card. This number is similar to a serial number and cannot be changed.<br>■ **MEID/ESN:** Uniquely identifies a CDMA device. This number corresponds to the device rather than a SIM card.<br>The usage list includes an entry for each rate plan corresponding to an ICCID/MEID/ESN number. |
| IMSI | Displays the IMSI code, a number that uniquely identifies the SIM on the carrier network. The codes include:<br>■ MCC: Mobile Country Code (for example, 310 for USA)<br>■ MNC: Mobile Network Code (for example, 410 for AT&T)<br>■ MSIN: Moble Sequential serial Identification Number |
| Type | Displays the carrier type. For example GSM or CDMA. |
| Device ID | Lists the device ID of the device integrated with a carrier. |
| Carrier subscription | Displays the name of the carrier subscription. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the carrier management display. |
|  | Activate/deactivate | Activates or deactivate carrier service for the selected device.<br>See Activate or deactivate a carrier account. |
|  | Assign carrier subscription | Manually assigns a carrier subscription to the selected SIM/device.<br>See Manually assign a carrier subscription. |

# Device management > Profiles view

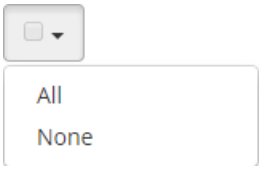
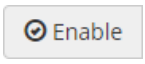
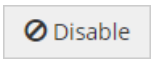
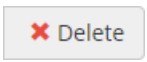
The **Device management > Profiles** view shows a list of all device profiles for your account. For each profile, Remote Manager displays the following information.

## Columns

| Column | Description |
|---|---|
| ☐ | Shows whether the profile is selected. |
| Enabled | Indicates whether the profile is currently enabled or disabled, activating, or in draft:<br>  Profile is enabled.<br> Profile is disabled.<br>  New profile is being activated.<br>Draft New profile has not yet been activated. |
| Profile ID | Displays the system-assigned ID for the profile. |
| Name | Displays the user-assigned name for the profile.<br>Click the displayed profile **Name** to view or edit the profile. |
| Device type | Shows the device type to which the profile applies. |
| Last modified | Shows the date and time the profile was last modified. |
| Last scan time | Shows the date and time the system last scanned devices to check for compliance with the profile. Click the displayed **Last Scan Time** to see the scan history.<br>See View the scan history for a profile. |
| Duration | Shows elapsed time of last scan. |

| Column | Description |
|---|---|
| Scan status | Shows the current status for the last scan:<br>■ **New:** Profile is new and no scan has occurred.<br>■ **Initiated:** Scan has been initiated by the scheduler but is not yet in progress.<br>■ **In Progress:** Scan is in progress.<br>■ **Terminated:** Scan was terminated while in progress (either by the user or Remote Manager).<br>■ **Completed:** Scan has completed. |
| Next scan time | Shows the date and time the profile is next scheduled to run. |
| Actions | Shows actions currently available for the profile:<br>  Show scan history for the selected profile.<br>  Edit the selected profile.<br>  Immediately scan the selected profile.<br>  Delete the selected profile.<br>**Note** Only actions available for the selected profile are displayed. |

## Buttons

| Button | Description |
|---|---|
|  | Quickly selects all or none of the profiles in the list. |
|  | Enables selected profiles.<br>See Enable or disable a device profile. |
|  | Disables selected profiles.<br>See Enable or disable a device profile. |
|  | Deletes selected profiles.<br>See Delete a device profile. |

| Button | Description |
|---|---|
| Refresh | Refreshes the list of profiles. |
| Create Profile | Creates a new profile.<br>See Create a device profile. |

# Device management > Profiles > Profile scan history view

The **Device management > Profiles > Profile scan history** view displays the history of scans for the selected profile. The scan history includes the following details for each scan:

| Column | Description |
|---|---|
| Scan start time | Displays the start time for the task. |
| Scan end time | Displays the end time for the task. |
| Status | Displays the result of the scan:<br>■ Success<br>■ Success with correction<br>■ Failed<br>■ Terminated<br>■ No devices scanned<br>Click the displayed **Status** to see a detailed log of the scan history. |
| Progress | Displays the current progress of a scan. |

# Device management > Profiles > Profile scan history > Profile scan history details view

The **Device management > Profiles > Profile scan history details** view shows step-by-step details for a selected scan.

| Column | Description |
|---|---|
| Device ID | Shows the device ID of the device included in the scan. |
| Details | Displays details for an individual scan task. |
| Start time | Displays the start time for the scan task. |
| End time | Displays the end time for the scan task. |
| Last modified | Displays the date and time the scan record was last updated. |
| Status | Displays the result of the scan task:<br>■ Failed<br>■ Success<br>■ Disconnected<br>■ In Progress<br>■ N/A |

# Data services > Data streams view

The **Data services > Data streams** view displays information on all data streams within your Remote Manager account in a two-pane display:

- **Data streams list:** The top portion of the display shows the list of data streams.
- **Charts/raw data:** The bottom portion of the display shows either a chart or the raw data for a selected data stream.

You can filter the display by selecting the category of data streams to display:

- All streams: The data stream includes all of the streams.
- Data streams
- Metric streams: The data stream includes a prefix for health metrics from the device.
- Management streams: The data stream includes a prefix for the JSON object used for connection history.
- Carrier streams: The data stream includes the device's carrier usage data.

**Note** In the data streams list, the columns are stationary. The display columns do not have the same capabilities as columns within other Remote Manager views. For example, you cannot right-click within a column heading to display a list of all the available columns, and you cannot hide or rearrange the columns. When sorting data streams, you can sort only by the stream, last updated, units, and data type fields.

## Columns

| Column | Description |
|---|---|
| Stream | Displays the user-assigned data stream name or the data stream path.<br>Examples:<br>Smart energy attributes:<br>se/attr/<Device Id>/<XBee Address>/<Endpoint Id>/<Cluster Type>/<Cluster Id>/<Attribute Id><br>Example:<br>se/attr/00000000-00000000-00409DFF-FF4584C9/00:13:A2:00:40:5C:0F:96/66/0/32785/13911399071804<br>Smart energy events:<br>se/event/<Device Id>/<XBee Address>/<Endpoint Id>/<Cluster Type>/<Cluster Id>/<Event Id><br>Example:<br>se/event/00000000-00000000-00409DFF-FF45ECC8/00:13:A2:00:40:5C:0F:96/94/1/1795/38<br>DIA channel data:<br>dia/channel/<Device Id>/<instance>/<channel><br>Example:<br>dia/channel/00000000-00000000-12300000-00000009/sensor0/temperature |
| Last updated | Displays the last time a data point was added to the data stream. |
| Current value | Displays the value of the last data point added to the data stream. |
| Current location | Displays the geo-location of the last data point added to the data stream. |
| Units | Displays the units for reported data. |
| Data type | Displays the type of data stored in the data stream. Valid data types include:<br>Integer<br>Long<br>Float<br>Double<br>String<br>Binary<br>Unknown |
| Description | Displays the user-assigned description for the data. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the list of data streams displayed and updates the graph. |
| Add | Add | Adds a new data stream. See Add data stream. |
| Delete | Delete | Deletes the selected data stream. See Delete data stream. |
| Properties | Properties | Edits properties for the selected data stream. See Edit data stream properties. |
| Preferences | Preferences | Configures preferences for new data streams. Preferences include data point and rollup TTLs (time to live in seconds) and time zones for rollups. See Configure data stream preferences. |
| All Streams | Category | Selects the category of streams to include in the display:<br>■ All streams<br>■ Data streams<br>■ Metrics streams<br>■ Management streams<br>■ Carrier streams |

## Chart options

| Option | Description |
|---|---|
| Show Last interval | Selects the time interval for the chart to show the last: 1 hour, 1 Day, 7 Days, 1 Month, 6 Months, or 1 Year. |
| Rollup type | Selects the rollup type:<br>■ **Average:** Average of all values in each rollup interval.<br>■ **Sum:** Sum of all values in each rollup interval.<br>■ **Min:** Minimum value of each rollup interval.<br>■ **Max:** Maximum value in each rollup interval.<br>■ **Count:** Count of all data points in each rollup interval.<br>■ **Std. Deviation:** Standard deviation of all values in each rollup interval. |

## Raw data options

| Option | Description |
|---|---|
| Time | Displays the date and time on which the data sample occurred on the device. |
| Updated | Displays the date and time on which Remote Manager received the data sample from the device. |
| Location | Displays the geo-location of the last data point added to the data stream. |
| Quality | Displays the quality level that is user-defined in the device configuration. |
| Data | Displays the value of the data point added to the data stream. |

# Data services > Data files view

The **Data services > Data files** view shows the file directory associated with your Remote Manager account.

When you add a device to your inventory, Remote Manager creates a root folder for the device using the fully-qualified device ID as the name. Each device folder is considered the root folder for the corresponding device. Data sent to Remote Manager from the device is stored in the device folder. You can create additional folders for your account and you can upload and download files from your account.

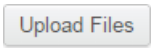
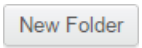
For each folder and file in your Remote Manager account, Remote Manager displays the following details.

## Columns

| Column | Description |
|---|---|
| Type | Displays an icon that indicates the object type:<br>  Folder<br>  File |
| Name | Displays the name of the folder or file. |
| Path | Shows the full path for the folder or file. |
| Last modified | For a folder, shows the date and time the folder was created.<br>For a file, shows the date and time the file was last modified. |
| Size | Displays the size of the folder or file (KBs or Bytes). |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Home | Navigates to the root (home) directory of your Remote Manager account. |
|  | Show/hide groups | Shows or hides the **Groups** menu. |

| Button | Name | Description |
|---|---|---|
|  | Toggle flat view | Toggles all device and network views from flat to nested view.<br>■ Flat view displays all devices for the selected group and all subgroups. By default, the flat view is used.<br>■ Nested view displays the devices in the selected group only; that is, devices in subgroups of the selected group are not included.<br>Toggling this display affects all Remote Manager views that support flat and nested views. For example, if you switch from flat to nested view on the Devices view, the XBee Networks view also switches to nested view. |
|  | Refresh | Refreshes the device list. |
|  | Upload files | Uploads one or more files to the current location within your Remote Manager account. |
|  | New folder | Creates a new folder at the current location within Remote Manager. |
|  | Open | For a folder, opens the selected folder.<br>For a file, immediately downloads the selected file to your local system. |
|  | Delete | Deletes the selected file or folder. |

# Security > Users view

The **Security > Users** view allows an administrator to view and manage users for a Remote Manager customer account. A customer account can include an unlimited number of users of any role, but a customer account must include at least one user assigned the administrator role.

For each user, Remote Manager displays the following information.

## Columns

| Column | Description |
|---|---|
| User name | Displays the user name for the registered user. |
| Role | Displays the role assigned to the user. Available user roles include:<br>■ Administrator<br>■ User<br>■ Read-only user<br>■ Application<br>■ Read-only application<br>See User roles for detailed descriptions of user roles. |
| Email | Displays the email address associated with the user. |
| First name | Displays the first name of the user. |
| Last name | Displays the last name of the user. |
| Registered | Displays the date and time the user registered with Remote Manager. |
| Last login | Displays the date and time the user last logged into Remote Manager. |
| Enabled | Displays whether the user account is enabled:<br>■ **True**: Account is enable.<br>■ **False**: Account is disabled. |
| Security policy | If assigned, displays the security policy assigned to the user. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refreshes the list of users. |
|  | Add User | Adds a user to the account. |

| Button | Name | Description |
|---|---|---|
| Remove Users | Remove User | Removes the selected user from your Remote Manager account. |
| Edit User | Edit User | Edits information for the selected user. |
| Change Password | Change Password | Assigns a new password to the selected user. |
| Assign Policy | Assign Policy | Assigns a security policy to the user. |
| Export Users | Export Users | Exports the list of users to a local Excel file. The exported file is named **User.xls**. |

# Security > Policies > Web view

The **Security > Policies > Web** view displays all user web policies defined for your Remote Manager account in a two-pane display:

- **Policies:** Displays the name and description for each policy defined for your Remote Manager account. Once defined, a user web policy can be assigned to one or more users.
- **Rules:** Displays the rules associated with the selected policy. Only one type of rule is supported: CIDR block rules.

| Button | Description |
|---|---|
| Add | ■ In the **Policies** pane, adds a new policy.<br>■ In the **Rules** pane, adds a new CIDR block rule to the selected policy. |
| Remove | ■ In the **Policies** pane, removes the selected policy.<br>■ In the **Rules** pane, removes the selected rule from the selected policy. |

# Security > Policies > Duo view

The **Security > Policies > Duo** view allows you to integrate a Duo Security account with Remote Manager to provide two-factor authentication.

## Fields

| Fields | Description |
|---|---|
| **Integration key** | Displays the Duo Security account integration key for Remote Manager. |
| **Secret key** | Displays the Duo Security account secret key for Remote Manager. |
| **API hostname** | Displays the API hostname for Remote Manager. |

## Buttons

| Buttons | Description |
|---|---|
| **Save** | Saves the current Duo Security account information. |
| **Clear** | Clears the current Duo Security account information. |

# Security > Policies > Device view

The **Security > Policies > Device** view displays all user device policies defined for your Remote Manager account.

| Policy/button | Description |
|---|---|
| SSL Required | Indicates whether all device connections are required to use SSL (Secure Sockets Layer):<br>■ **Enabled:** All device connections are required to use SSL.<br>■ **Disabled:** Device connection are note required to use SSL.<br>The default is disabled. |
| SM Encryption Required | Indicates whether devices must use encryption when communicating over transports such as SMS and SM/UDP.<br>■ **Enabled:** All device transport communications are required to use encryption.<br>■ **Disabled:** Device transport communications are not required to use encryption.<br>The default is disabled. |
| Save | Saves current device policy setting. |

# Admin > Account settings > My account view

The **Admin > Account settings > My account** view allows you to view and manage your account information, including the vendor ID associated with your customer account.

**Note** If you need to modify account subscriptions or services, contact the account owner.

## Account profile information

| Option | Description |
|---|---|
| Company | Displays the name of the company this user is associated with. |
| First name | Displays the first name of the account user. |
| Last name | Displays the last name of the account user. |
| Email | Displays the email address for the account user. |
| Title | Displays the title of the account user. |
| Phone | Displays the telephone number for the account user. |
| Description | Displays the description of the account user. |
| Role | Displays the user role for the account. |
| Address<br>City<br>State<br>Postal Code<br>Country | Displays the address of the physical location for the person or company associated with this account. |

## Vendor information

| Option | Description |
|---|---|
| Vendor ID | Displays the system-assigned vendor ID registered for your account. If you are using Cloud Connector and intend to manufacture devices, click **Register for new vendor id** to generate a unique vendor ID for your account. |
| Provisioning Configuration | Click **Provisioning Configuration**. The **Configure Provisioning** dialog appears, in which you can configure the provisioning details for your vendor ID. See Configure provisioning. |

| Option | Description |
|---|---|
| Restricted status | Specifies the default restriction status for newly provisioned devices in your account. It is recommended that you set the default restriction status for newly provisioned devices to either **Unrestricted** or **Untrusted**.<br>■ **Unrestricted:** Default status for newly provisioned devices is unrestricted. That is, there are no restrictions on newly provisioned devices.<br>■ **Restricted:** Default status for newly provisioned devices is restricted. A restricted device cannot be fully managed until the restriction status is changed to unrestricted.<br>■ **Untrusted:** Default status for newly provisioned devices is untrusted. New devices can be auto-provisioned, but the devices are not fully operational until validated. |
| Group | Specifies the default group into which newly provisioned devices are placed. Groups are created in the **Device Management** page. See Organize devices: metadata, tags, and device groups for information about device groups.<br>To disable provisioning, select the Group option **(Disable Provisioning)**. By default, provisioning is disabled. |

# Admin > Account settings > Notifications view

The **Admin > Account settings > Notifications** view allows you to manage alarm notifications for your account. For each defined alarm notification, Remote Manager displays the following details.

**Note** You must have previously created an alarm before you can create an alarm notification for a user account. See Alarms.

## Notification options

| Option | Description |
|---|---|
| Status | Shows an icon indicating the current status of the alarm notification:<br>Notification is enabled.<br>Notification is disabled. |
| Name | Specifies the name of the notification. |
| Description | Specifies a description for the notification. |
| Send Email to | Specifies one or more email addresses to send the notifications. Use a comma-delimited list to specify multiple email addresses. |
| Send daily summary reports at | Enables or disables daily summary reports. The daily summary report contains the current state of alarms and all alarm events that occurred in the last 24 hours.<br>If this option is enabled, you should specify the time at which to send daily summary reports. The default is enabled. The default time is 7:00 p.m. |
| Send notifications for each alarm event | Enables or disables notification for each alarm event. The default is enabled.<br>When enabled, an email notification is sent when an alarm event occurs. An alarm event includes both fired and reset alarm events. |
| Send notifications for the following alarms | If selected, specifies one or more alarms for which you want to send notifications. By default, notifications include all alarms. |
| Send notification for alarms scoped to the following groups | If selected, specifies one or more groups for which you want to send notifications. By default, groups are not used to scope notifications. |

## Buttons

| Button | Description |
|---|---|
| Add | Adds an alarm notification to your account.<br>See Create an alarm notification. |
| Remove | Removes the selected alarm notification from your account.<br>See Delete an alarm notification. |
| Enable/Disable | Enables or disables the selected alarm notification. Choose the desired option from the list box.<br>See Enable or disable an alarm notification. |

# Admin > Account settings > Carrier account view

The **Admin > Account settings > Carrier account** view shows carriers configured for your Remote Manager account.

- If you configure only one carrier for your account, Remote Manager automatically assigns the carrier to each new carrier-integrated device you add to your account.
- If you configure more than one carrier for your account, you need to manually assign a carrier to each carrier-integrated device you add to your inventory. See Manually assign a carrier subscription.

For each configured carrier, Remote Manager displays the following details.

## Carrier information

| Carrier information | Description |
|---|---|
| Name | Lists the names of a carrier supported by Remote Manager. |
| Last updated | Displays the date and time the carrier credentials were last updated. |
| Username | Displays the user name for the carrier. |
| Additional fields | Depending on your carrier, additional fields related to the carrier may appear, such as a administrator or monitor license key field. |

## Buttons

| Button | Description |
|---|---|
| Enter Credentials | Displays the credentials for a carrier account. The credentials are specific to each carrier.<br>You must read the carrier subscription management notice and select the **I acknowledge the above notice** option, and then click **Save** to save the carrier credentials.<br>See Configure a carrier account. |
| Change Credentials | Changes credentials for a configured carrier account.<br>See Update credentials for a carrier account. |
| Test Connection | Tests the connection for a configured carrier account. Remote Manager displays a message indicating whether the connection test succeeded or failed. If the connection test fails, click **Change Credentials** and verify that the credentials you have entered are correct. |
| Remove | Removes the corresponding carrier account configuration.<br>See Remove carrier credentials. |

# Admin > Account settings > Preferences view

The **Admin > Account settings > Preferences** view allows you to manage preferences for your account.

## Security

| Option | Description |
|---|---|
| Session timeout | Specifies the number of minutes of inactive use after which a Remote Manager session times out. You can specify from 5 to 1440 minutes. The default is 30 minutes. |

## Device Data

| Option | Description |
|---|---|
| Store data sent from devices | Specifies whether to store data sent from devices:<br>■ **Enabled**: Remote Manager stores data sent from devices to the appropriate storage (streams).<br>■ **Disabled**: Remote Manager does not store data sent from devices.<br>The default is **Enabled**, which means that Remote Manager stores data sent from devices.<br>**Note** This option does not affect data published via Push Monitors. |

## Health Metrics

| Option | Description |
|---|---|
| Enable health metric expiration | Specifies whether to expire health metrics.<br>■ **Enabled**: Remote Manager expires health metric error and warning states.<br>■ **Disabled**: Remote Manager does not expire health metrics. Once a health metric reports an error or warning status, the status does not expire.<br>The default is **Enabled**; that is, health metric error and warning states expire. |

| Option | Description |
|---|---|
| Automatically choose expiration timeout | Expires health metric data.<br>If you have enabled health metric expiration, you can either allow Remote Manager to automatically expire health metrics based on a system-chosen expiration timeout or set an expiration timeout.<br>■ **Enabled**: Remote Manager automatically expires health metrics based on a system-chosen expiration timeout.<br>■ **Disabled**: Health metrics expire based on **Expiration Timeout** setting.<br>The default is **Enabled**, which means that Remote Manager automatically expires health metrics based on a system-chosen expiration timeout. |
| Expiration timeout | Specifies the amount of time before a warning or error health metric is reset to normal. Timeout value can be from 10 to 43,200 minutes (30 days). |

## Buttons

| Button | Description |
|---|---|
| Save | Saves the current preference settings. |

# Admin > Services view

The **Admin > Services** view shows a summary of service usage information for the selected billing period. Click the arrow for each usage type to expand the section and display additional information.

**Note** If you are logged into a customer account that has subaccounts, service usage information is displayed only for the parent account. Subaccount information does not roll up into the parent account.

| Service | Description |
|---|---|
| Web Services (transactions) | Displays web services and messages recorded for your services. |
| Device Management (devices) | Displays the number of devices currently associated with your subscription. |
| SMS | Displays SMS usage information per billing period. |
| Data Streams | Displays data streams storage usage information. |

If you are the account owner, you can make changes to account services via the **Manage Services** button.

# Admin > Subscriptions view

The **Admin > Subscriptions** view shows detailed information about your account subscriptions and usage.

## Buttons

| Column | Description |
|---|---|
|  | Updates the information in the page. |
|  | Exports a list of subscriptions to an Excel spreadsheet. See Export subscriptions to Excel. |
| Billing period list box | Selects the billing period for usage. The billing period is a calendar month. |

## Subscriptions view fields

| Column | Description |
|---|---|
|  | Summarizes information about the state of the subscription:<br>■ Active (no icon)<br>■ Deactivated (red minus sign)<br>■ Expired (red X) |
|  | Shows whether the subscription is locked:<br>■ Locked (locked icon)<br>■ Unlocked (no icon) |
| ID | Displays the system-assigned ID for the subscription within Remote Manager. |
| MAC address | Displays the MAC address associated with the device. |
| Device ID | Displays the device ID associated with the device.<br>If no device ID is displayed, the service subscription is at the customer account level. |
| Service | Displays the service associated with the subscription. |

| Column | Description |
|---|---|
| Plan | Displays the name of the rate plan that for the subscription. Rate plans define costs and limits on the usage of Remote Manager resources, such as the amount of data, number of API calls, and so on. Rate plans can have a varied number of associated limits, referred to generically as 1 through 4. |
| Usage/Limit #1 | Depending on the rate plan, this column shows the current rate and the plan limit for item #1. A description of the usage limit is shown in parentheses. |
| Usage/Limit #2 | Depending on the rate plan, this column shows the current rate and the plan limit for item #2. A description of the usage limit is shown in parentheses. |
| Billing period | Specifies the billing period for usage. The billing period is a calendar month. |

# Admin > Reports view

The **Admin > Reports** view shows a list of all device reports for your account. For each report, Remote Manager displays the following details.

| Item | Description |
|---|---|
| New report | Creates a new report. See Generate a health status report immediately or Schedule a health status report. |
| Search | Searches for a report name or type of report. |
|  | Runs the selected report. |
| Enabled | Enables or disables a scheduled report. When the report is disabled, it does not run as scheduled. |
| Name | Displays the user-defined name for the report. |
| Includes | Lists all report types included in the report.<br>Account-level options include:<br>Aggregate health status report<br>Aggregate connection status report<br>Aggregate connection status history report<br>Alarm status report<br>Monitor status report<br>Device-level options include:<br>Connection history report<br>Latency report<br>Data usage report<br>Out-of-service report<br>Interface connectivity report<br>Packet report<br>Signal report |
|  | Edits the selected report.<br>See Edit a health status report. |
|  | Deletes the selected report.<br>See Delete a health status report. |

# Admin > Customers view

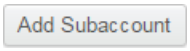
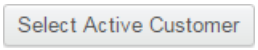
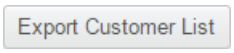
The **Admin > Customers** view shows a list of all customer accounts associated with the logged in user.

**Note** The **Customers** view is displayed only for a user of an account that has associated subaccounts.

## Columns

| Column | Description |
|---|---|
|  | Indicates the currently selected customer subaccount. All Remote Manager views show data for the selected customer subaccount only. This allows a parent account to view devices and data scoped to the selected customer subaccount. |
| Cust ID | Unique customer identification number used by Remote Manager APIs for parameters and identification. |
| Company | Company name of the customer. |
| Phone | Contact telephone number for the customer. |
| Customer # | Unique customer identification number used for billing and support calls. |

## Buttons

| Button | Name | Description |
|---|---|---|
|  | Refresh | Refresh the current list of customers. |
|  | Add subaccount | Add a new Remote Manager account as a subaccount of the current account. The **Add Subaccount** button is enabled only when the logged in user is licensed to create subaccounts. See Add a subaccount. |
|  | Select Active Customer | Select a customer subaccount as the active account. Once you have selected the active account, you can view and manage devices as if you were logged in to the selected account. |
|  | Export Customer List | Export the customer list to an Excel spreadsheet. See Export a customer list to Excel. |

# Admin > Event log view

The **Admin > Event log** view shows the status of completed events. For each event, Remote Manager displays the following information. To get details for an event, double-click an item to display the Admin > Event log > Event log details view.

| Event information | Description |
|---|---|
| Status | Shows the status of the event:<br>✓ Event was successful.<br>! Event failed. See details for more information. |
| Time | Shows the start time of the event. |
| User name | Displays the user that initiated the event. |
| Modification type | Shows the modification type: Create, Update, or Delete. |
| Source | Shows the event task. |
| Target | Shows the event target. |
| Details | Gives a detailed message for failed events. Double-click the event to show the Admin > Event log > Event log details view. |

# Admin > Event log > Event log details view

The **Admin > Event log > Event log details** view shows detailed information for an Event log item. For each event, Remote Manager displays the following information.

| Event detail | Description |
|---|---|
| completeTime | Shows the time the event completed. |
| completeTimeISO | Shows the event completed time in ISO format. |
| count | Shows the subscription usage for the event. |
| cstId | Shows the customer ID for the event. |
| duration | Shows the formatted duration of the event. |
| durationMS | Shows the amount of time in milliseconds the event required to complete. |
| facility | Shows the operation of the event. |
| hostname | Always blank. |
| ip | Shows the IP address from which the event was initiated. |
| jobs | Shows the jobs (if any) associated with the event. |
| modDetails | Shows details for failed event. |
| modType | Shows the modification type: Create, Update, or Delete. |
| protocol | Shows the protocol for the event: HTTP. |
| requestSize | Shows the size of the event request. |
| responseSize | Shows the size of the event response. |
| service | Shows the subscription service to which usage is charged for the event. |
| source | Shows the source that initiated the event. |
| success | Shows whether the task was successful: True for success and False for failure. |
| target | Shows the target for the event. |
| targetType | Shows the type for the target in the event. |
| timestamp | Shows the timestamp when the event was initiated. |
| timestampISO | Shows the timestamp in ISO format when the event was initiated. |
| user | Shows the user that initiated the event. |
| version | Shows the version of the event format. |