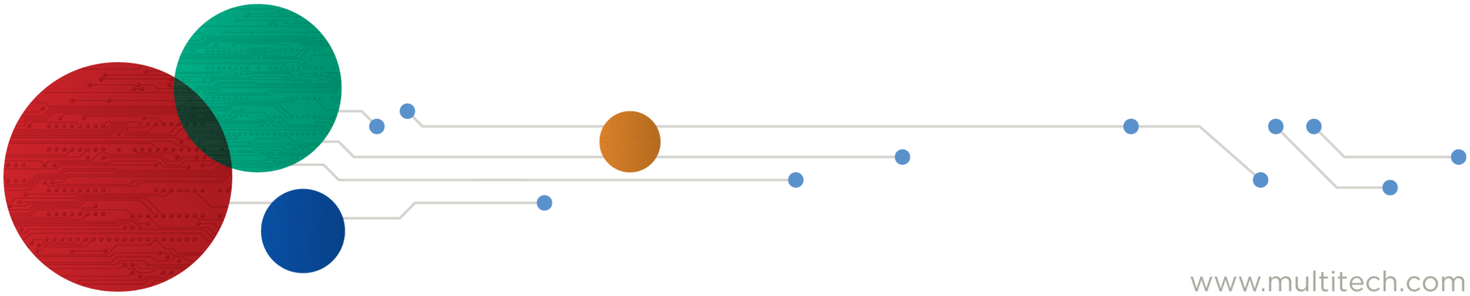
LENS® User Guide



www.multitech.com

LENS User Guide

Part Number: S000697, Version 1.5

Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2021 by Multi-Tech Systems, Inc.**

Multi-Tech Systems, Inc. makes no representations or warranties, whether express, implied or by estoppels, with respect to the content, information, material and recommendations herein and specifically disclaims any implied warranties of merchantability, fitness for any particular purpose and non-infringement.

Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc. to notify any person or organization of such revisions or changes.

Trademarks and Registered Trademarks

MultiTech, the MultiTech logo, LENS, DeviceHQ, Conduit, and xDot, are registered trademarks and mPower and mDot are trademarks of Multi-Tech Systems, Inc. All other products and technologies are the trademarks or registered trademarks of their respective holders.

Legal Notices

The MultiTech products are not designed, manufactured or intended for use, and should not be used, or sold or re-sold for use, in connection with applications requiring fail-safe performance or in applications where the failure of the products would reasonably be expected to result in personal injury or death, significant property damage, or serious physical or environmental damage. Examples of such use include life support machines or other life preserving medical devices or systems, air traffic control or aircraft navigation or communications systems, control equipment for nuclear facilities, or missile, nuclear, biological or chemical weapons or other military applications ("Restricted Applications"). Use of the products in such Restricted Applications is at the user's sole risk and liability.

Contacting MultiTech

Knowledge Base

The Knowledge Base provides immediate access to support information and resolutions for all MultiTech products. Visit http://www.multitech.com/kb.go.

Support Portal

To create an account and submit a support case directly to our technical support team, visit: https://support.multitech.com.

Support

Business Hours: M-F, 8am to 5pm CT

Country	By Email	By Phone
Europe, Middle East, Africa:	support@multitech.co.uk	+(44) 118 959 7774
U.S., Canada, all others:	support@multitech.com	(800) 972-2439 or (763) 717-5863

Warranty

To read the warranty statement for your product, visit https://www.multitech.com/legal/warranty. For other warranty options, visit www.multitech.com/es.go.

World Headquarters

Multi-Tech Systems, Inc.

2205 Woodale Drive, Mounds View, MN 55112

Phone: (800) 328-9717 or (763) 785-3500

Fax (763) 785-9874

Contents

Chapter 1 – Welcome

LENS® is a scalable LoRaWAN platform for deploying and managing LoRaWAN networks. LENS provides centralized key management for LoRaWAN end devices, and configuration and control of Conduit® gateways. LENS allows user to add gateways and end devices in bulk, create separate organizations, and segment networks to support different IoT applications.

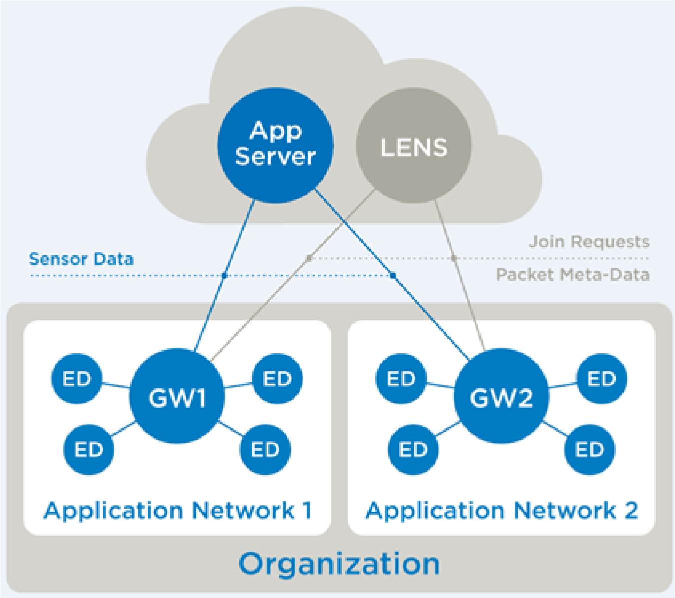
End devices have pre-shared keys installed and uploaded to the cloud join server. This allows an end device to securely join selected gateways without having foreknowledge of the application network.

In the join process, information is exchanged between the end device, the gateway, and the join server.

Highlights

- Central management tool for Network Access Control (NAC), Conduits, and end devices
- Easy deployment of Conduits, end devices, and use of central management
- Security and scalability

Architectural Overview



Compatible Gateways and Devices

Gateway Firmware Compatibility

Conduit, Conduit AP, Conduit IP67, and Conduit IP67 Series 200 gateways.

Availability of LENS Features on Conduit gateways:

- Conduit AEP v1.4.16

Key management must be configured to point to LENS

- Conduit AEP v1.6.2

Define check-in interval

Manage device groups

Manage traffic manager policies

Manage profiles

FUOTA operations

- Conduit AEP v1.6.4
- Conduit AEP v1.7.0
- Conduit AEP v1.7.2
- Conduit AEP v1.7.3

If the GPS is available and configured, then the Conduit gateway will report GPS locations to LENS and/or the user may manually define the latitude/longitude

Error: For non-GPS Conduit gateways with AEP v1.7.3 and v1.7.4, the Conduit gateway will overwrite any user-defined latitude/longitude pairs with zeros

- Conduit AEP v1.7.4

Next Check-In field provided in check-in API.

Error: For non-GPS Conduit gateways with AEP v1.7.3 and v1.7.4, the Conduit gateway will overwrite any user-defined latitude/longitude pairs with zeros

- mPower v5.0.0-AEP
- mPower v5.0.1-AEP
- mPower v5.1.2

RSSI Spectral Scan

Error: “Packet Data” option breaks Uplink / Downlink API to LENS (when “Packet Metadata” is selected)

- mPower v5.1.5
- mPower v5.1.6
- mPower v5.2.0
- mPower v5.2.1
- mPower v5.2.5
- mPower v5.3.0
- mPower v5.3.3
- mPower 5.3.4b

LoRaWAN 1.0.4 Devices

- Join Server for LENS v1.3 or greater
- mDot / xDot v3.3.5 or greater for Join Nonce enabled validation
- The LENS provisioned End-Device MUST be assigned to a Device Profile with MACVersion “1.0.4”

Note: The DevNonce and JoinNonce will both be reset to 0 when the Join EUI on the Node is updated. The Join Server v1.3 or greater will verify the Join EUI change based on last successful join.

FUOTA Requirements

- Requires minimum Conduit AEP v1.6.2
- Requires mDot v3.1.0 or v3.2.1
- Does NOT work on xDot v3.1.0 or v3.2.1

Chapter 2 – Getting Started

Logging in for the First Time

If a LENS account has been created for you, the system sends you an email to activate your account. To activate your LENS account:

1. Click the **Activate User Account** link in the email. This link is good for one hour.
2. Enter a new password for your account and click **Set Password.**

   Password must be at least 10 characters and must include at least 1 lowercase letter, 1 uppercase letter, one special character, and 1 digit.

   If multi-factor authorization is enabled for your account, the multi-factor authorization screen appears.
3. Install **Google Authenticator** on your smart phone or other device.
4. Open **Google Authenticator**.
5. Either scan the QR code on the Multi-Factor Authorization screen or enter the Issuer, Authorizer Name, and Google Secret code into Google Authenticator.
6. Click **OK.**
7. Enter your email and password.
8. Enter the code provided in Google Authenticator and click **Verify Code**.
   Note: You will need to enter an Google Authenticator code every time you login.

Logging in with Multi-Factor Authentication

If this is the first time you are logging in, refer to Logging in for the First Time.

To log in:

1. Go to https://lens.devicehq.com
2. Enter your **Email** and **Password.**
3. Enter your **Two-Factor Authorization Code** from the Google Authenticator app.
4. Click **Verify Code.**

Navigating the System

Page layout depends on the device used to access the tool. The program is designed to respond to your device's screen size. On a full-sized computer browser window, navigation runs along the left margin. On a smaller browser, such as a tablet or mobile device, navigation icons appear at the top.

To open a submenu:

- On a computer, click the menu name or ⌄.
- On a mobile device, touch the menu icon.

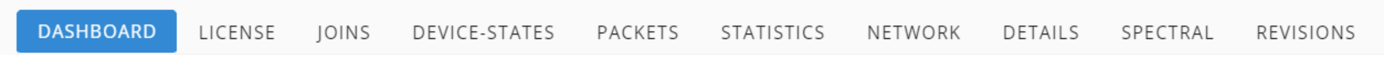
Also to scroll through a table on a mobile device, swipe left or right.

Note: If possible when using a smartphone to view for charts and tables, rotate the device horizontally for optimal viewing.

Icon	Function
▦	Dashboard
⅄	Network (submenu) and Application Network
📋	Network or Device Profiles
📶	Gateways
◉	Device (submenu) and End Devices
🔒	Policies
⬚	Device Groups
📡	Operations
👥	People
👤	User (submenu) and User's Account Profile
🏢	Organization
☰	Activity
✉	Broadcast
?	Support
⇥	Log Out

Tabs

To change the display on dashboard pages, click on the tabs above the map or table.



Filtering List Table Contents

Gateway, end device, joins, packets, and people lists can be filtered as needed.

To filter a list:

1. Click the column header for field you want the list to be filtered on.
2. Click ☰.
3. Enter a filter term, such as part of a name or number. The system filters the list to show only items that meet your filter criteria.

Note:

- You can filter on multiple fields. The Active Filter icon ▽ appears next to names of fields that are filtered.
- To remove a filter, click ☰ and clear the filter term.

Sorting List Table Contents

Gateway, end device, joins, packets, and people lists can be sorted with or without filtering as needed.

To sort a table:

1. Click the column header for field you want the listed to be sorted on.
2. Click ↑. The list is sorted in ascending order.

Note:

- For descending order, click the column header twice. The Sort icon flips, ↓.
- To remove sorting, click the column header a third time. The Sort icon clears.

Rearranging Columns

To rearrange the columns:

- Drag the column header to the location you want.

Searching LENS (Jump To...)

To search LENS for a specific application network, gateway, or end device:

1. Click in the **Jump To** field.
2. Enter the name or UI of the application network, gateway, or end device to be searched.

Any applications networks, gateways or end devices that match your search appear in a drop-down menu, with links to each one.

First Steps

This topic provides an overview of tasks for getting started with LENS Detailed steps are available in the linked topics.

After logging into LENS:

1. Create an Application Network.

   What is an Application Network?

2. Provision a Gateway.
   - What is a Gateway?
   - Adding multiple gateways? Upload a CSV
3. Provision an End Device.
   - What is an end device?
   - Adding multiple end devices? Upload a CSV

Chapter 3 – Dashboard

The LENS dashboard contains links and graphs pertaining to the application networks, gateways and end devices. Each graph provides specific data in increments of hours, days, or weeks.

Organization Snapshot

The top of the dashboard shows:

- **Application Networks:** Contains a count of application networks and a link to the Application Networks page.
- **Gateways:** Contains a count of gateways and a link to the Gateways page.
- **End Devices:** Contains a count of end devices and a link to the End Devices page.
- **Application Device Check:** Contains counts of application networks with health status alerts by alert type and a link to the Application Network Health Checklist page.
- **Gateway Device Check:** Contains counts of gateway health status alerts by alert type and a link to the Gateway Health Checklist page.
- **Device States:** Contains counts of end device health status alerts by alert type and a link to the End Device Health Checklist page.

Note: The line graphs adjacent to Application Networks, Gateways, and End Devices fields represent the number of entities over time. Where a line goes up indicates more entities added to the system. The end of the line is the current level noted by the number listed.

Graphs

- **Gateway Map:** Shows the location of each gateway that has latitude and longitude coordinates.
- **Packets per hour/day/week:** Number of packets received by each gateway over time. Gateways are listed by GwEUIs. Statistics accompanying the chart include average number of packets per hour, day, or week and counts of uplinks and downlinks. Data also includes details of the last packet received.
- **Join Requests per hour/day/week:** Number of join requests received over time. See join request status for more information. Statistics accompanying the chart include average number of join requests per hour, day, or week and counts of successful and failed join requests. Data also includes details of the last join request received.
- **CRC Error Percentage per hour/day/week:** Number of packets received with failed CRCs (cyclic redundancy checks) over time. A gateway typically receives some false packets (low SNR or signal-to-noise ratio) due to environmental noise. The CRC filters out packets without performing data look-ups on invalid input or data that is known to be incorrect. If a gateway receives few actual packets, this may indicate a high percentage of CRC error packets. Statistics accompanying the chart include average number of CRC error rate per hour, day, or week. Data also includes the gateway with the highest CRC error percentage.
- **Missed Packets per hour/day/week:**

  Missed Uplinks: Number of uplink packets not received by the network server.

  Missed Downlink ACKs: Incremented for each confirmed uplink retry received by the network server, this indicates the number of downlink packets not received by the end device.

Statistics accompanying the chart include packed uplink and downlink averages per hour, day or week and counts of missed uplinks and downlinks.

Join Request Status

The following table provides definitions of all possible join request outcomes.

Outcome	Definition
Success	End device EUI is in the key store and the end device has the correct AppKey.
MICFailed	End device EUI is in the key store, but the end device does not have the correct AppKey. This may indicate that a foreign device is trying to access the network using a spoofed DevEUI.
Unknown DevEUI	End device EUI is not in the key store. The end device may belong to another network in range of the gateway.
Duplicate Dev Nonce	End device EUI is in the key store, but the end device nonce value has recently been used. A foreign device may be trying to access the network using a replayed join request. This can occur naturally due to random selection of devnonce in LoRaWAN 1.0 and 1.0.4 end devices.
Gateway Mismatch	End device EUI is in the key store, but the end device is not allowed to join this gateway. The end device and gateway do not belong to the same application network. This can occur if two networks are deployed near each other and use the same frequency settings.
Other Server Error	An error occurred while processing the join request.

Health Check Overview

Health Check monitors joins and uplinks to give you a high-level view of the state of your devices. Every four hours, the system first updates end devices, and then evaluates gateway and application network states based on updated end devices.

Device checks for application networks, gateways, and end devices appear on the dashboard. Click on a health check tile for details.

- End devices become active when the server forwards uplinks for joined end devices. They remain active as long as uplinks come in at an expected frequency. If uplinks don’t come at as expected for an active end device, the state changes to inactive. For details, go to End Device Health Checklist.
- Gateway state shows whether end devices have joined through the gateway or not. If end devices have joined through the gateway, the gateway state is derived from the end device states. For details, go to Gateway Health Checklist.
- Application Network state shows whether or not end devices have joined through the application network. For details, go to Application Network Health Checklist.

Application Network Health Checklist

Application Device Check appears at the top of the dashboard, application networks page, and the application network health check list page. When you click on Application Device Check, the Gateway Health Checklist appears.

- **Configured:**Application networks that are assigned to at least one provisioned end device and belong to at least one gateway, but do not have successful joins.
- **Unconfigured:** Application networks that are provisioned, but do not have any gateways or end devices.

- **Initiated:**Application networks that have one or more end devices joined through the application network that were set to initiated during the health check update.
- **Active:** Application networks that had at least one active end device joined through the application network during the health check update. Other end devices joined through the application network may be at the initiated state.
- **Warning:** Application networks that had at least one inactive end device that joined through the application network during the health check update. Other ended devices joined through the application network may be at the initiated or active state.

Viewing the Application Network Health Checklist

When you click on Application Device Check, the Application Network Health Checklist appears. Application Networks are listed by order of concern; networks with a warning appear at the top of the list.

Application Network Health Check Fields

The bottom of the Application Network Health Checklist page lists end devices with issues sorted by order of concern.

Field	Description
Status	Application Network's health check status.
Name	End device name.
Application Network	EUI of the provisioned application network.
Last Status Update	Timestamp of the last state change.

Viewing Application Network End Device Details

To determine which end devices are causing a network status:

- Click on an application netork in the table.

Gateway Health Checklist

Gateway Device Check appears at the top of the dashboard, gateways page, and the gateway health check list page. When you click on Gateway Device Check, the Gateway Health Checklist appears.

- **Configured:** Gateways that are provisioned and assigned to at least one application network, but do not have successful joins. May include provisioned gateways not yet deployed in the field.
- **Unconfigured:** Gateways that are provisioned, but not assigned to any application networks.
- **Initiated:** Gateways that have one or more end devices joined through the gateway that were set to initiated during the health check update.
- **Active:** Gateways that had at least one active end device joined through the gateway during the health check update. Other end devices joined through the gateway may be at the initiated state.
- **Warning:** Gateways that had at least one inactive end device that joined through the gateway during the health check update. Other ended devices joined through the gateway may be at the initiated or active state.

Viewing the Gateway Health Checklist

When you click on Gateway Device Check, the Gateway Health Checklist appears. Gateways are listed by order of concern; gateways with a warning appear at the top of the list.

Gateway Health Check Fields

The bottom of the Gateway Health Checklist page lists gateways with issues sorted by order of concern.

Field	Description
Status	Gateway's health check status.
Last Request	Timestamp of last join request, regardless of status through this gateway.
Last Uplink	Timestamp of last uplink packet coming through this gateway.
Last Status Update	Timestamp of the last state change.
Name	Gateway name.
Gateway	EUI of the provisioned gateway.
Last Checkin	Timestamp of the last time the gateway checked in.
Next Checkin	Time when the next check-in is expected. This field is based on Conduit LENS Server Check-in API. If not provided, set to one hour after last check-in.

Viewing Details

To determine which end devices are causing a gateway status:

- Click on an gateway in the table.

End Device Health Checklist

Device States appear at the top of the dashboard, end devices page, and the end device health check list page. When you click on Device States, the End Device Health Checklist appears.

- **Configured:** End devices that are provisioned and assigned to an application network, but have not joined a network. May include provisioned end devices not yet deployed in the field.
- **Unconfigured:** End devices that are provisioned, but not assigned to an application network. End devices can't join a network until they are assigned to an application network.
- **Initiated:** End devices that have joined at network, but have no uplink record. If an end device becomes active and later rejoins, the state is set back to initiated to indicate that no uplink has occurred for this join. Initiated may also mean the gateway has not enabled the LENS API to send uplink packets.
- **Active:** End devices become active when the system receives the first uplink for a join. They remain active as long as uplinks occur at an expected frequency.
- **Inactive:** End devices become inactive when the uplink does not occur at the expected frequency.

End Devices Health Check Fields

The bottom of the End Device Health Checklist page lists end devices with issues sorted by order of concern.

Field	Description
Status	Device's health check status.
Last Request	Timestamp of last successful join.
Last Uplink	Timestamp of last uplink for the last join. Field is reset upon rejoins.
Last Status Update	Timestamp of the last state change.
Name	End device name.

Field	Description
End Device	End device EUI.
App Name	Application network the device joined through.
Joined App Network	EUI of the application network the device joined through.
Gateway Name	Gateway the end device joined through.
Joined Gateway	EUI of the gateway the device joined through.
Join EUI	Join EUI of the successful join request.

End Device Health Check Management

The Health Check Management watchlist shows end devices that have become inactive since the last (if any) reset. It also shows end devices that have had an inactive state, but have transitioned back to active. This helps users identify issues with an end device's reliability.

The watchlist includes a timestamp of the inactive timestamp.

Viewing the Watchlist

To view the watchlist:

1. Click the **Device States** legend on the dashboard or End Devices page.
2. Click **End Device Health Check Managemen**t.

Resetting an Inactive End Device

To reset an end device with an inactive status:

1. Click the check box for the inactive end device(s) you want to reset. To select all inactive end device currently displayed, click the checkbox for Status.
2. Click **CLEAR STATE**.

Removing an End Device from the Watchlist

To remove an end device from the Watchlist:

1. Click the check box for the inactive end device(s) you want to reset. To select all inactive end device currently displayed, click the checkbox for Status.
2. Click **REMOVE FROM WATCHLIST.**

Note: If the end device returns to an inactive state, it will reappear on the watchlist.

Generating a Watchlist Report PDF

To generate a watchlist report:

1. Click the **Device States** legend on the dashboard or End Devices page.
2. Click **End Device Health Check Management**.
3. Click **Report.**

LENS generates a PDF report, which opens in your PDF reader.

Purge Status of Deleted End Devices

Organization admin users can purge the end device state of deleted end devices. To do this:

1. Click the **Device States** legend on the dashboard or End Devices page.
2. Click **End Device Health Check Management**.
3. Select the check box for the deleted end device(s).

   (Deleted end devices show Deleted in the name field. Click Name to sort the list on this column.)
4. Click the check boxes for the inactive end devices states you want to purge.
5. Click **CLEAR STATE**.

Chapter 4 – Application Networks

An application network is a network of gateways and end devices that can be connected in order to report application data from deployed sensors. In application networks, you can:

- Associate end devices to gateways.
- Allow end devices to join a gateway and report data to an application.

If an end device and a gateway do not share an application network, then the end device cannot join to the gateway. A gateway can belong to many application networks, but an end device can belong to only one application network.

Application Networks Page

To access the Application Networks page, click **Network > Application Networks.**

This page lists the number of application networks in the top left appears, followed by a list of the application networks.

For each application network, this page shows the AppEUI, the number of end devices and gateways associated with that application network, and the application network health check status.

Use the **Application Networks** page to:

- Create new application networks.
- Edit existing application network settings.
- Delete an application network.

To view an application network's dashboard

- Click on that network.

Creating a New Application Network

1. Go to **Network > Application Networks** to view the list of application networks.
2. Click + to create a new application network.
3. Enter the AppEUI, a unique 64-bit EUI (8 hex digits), or leave blank to have an AppEUI automatically assigned.

   Note: The value will be sent to the Conduit in a join response to use in received uplink packets as the application identifier. For example, an AppEUI such as 16-ea-76-f6-ab-66-3d-80 can be created randomly, or use the mDot AT interface to generate one.

4. Enter the remaining application network information. For field descriptions, refer to Application Network Fields.
   - Application network name (required).
   - URL, if applicable.
   - Brief description of the application network.

5. Click **Provision** to save the new application network, or click **Cancel** to exit without saving.

   Note: The AppEUI and Name fields are required and defined by the user.

Application Network Fields

Field	Description
Name	Application network name. Up to 60 characters. Required.
AppEui	AppEUI, a unique 64-bit EUI (8 hex digits), or leave blank to have an AppEUI automatically assigned. **Note:** Note: The value is sent to the Conduit in a join response to use in received uplink packets as the application identifier. For example, an AppEUI such as 16-ea-76-f6-ab-66-3d-80 can be created randomly, or use the mDot AT interface to generate one.
Status	Shows the network's health check status. Options are configured, active, or warning. For status definitions, refer to Health Check Overview.
URL	If applicable, enter the application network's URL.
Container Name	Reserved for future use
Network Profile	Select a network profile from the drop-down list. For more information about network profiles, refer to Network Profiles.
Container ID	Reserved for future use
Description	Brief description of this network. Optional. To create a new line, press Shift + Enter.

Application Network Dashboard

The Application Network dashboard contains graphs for just the selected application network. Each graph provides specific data in increments of hours, days, or weeks.

Application Network Snapshot

The selected network's information appears the top of the page. This is pulled from setup information. For information about this content, refer to Application Network Fields.

Dashboard Graphs

- **Gateway Map:** Shows the location of each gateway that has latitude and longitude coordinates.
- **Packets per hour/day/week:** Number of packets received by each gateway over time. Gateways are listed by GwEUIs. Statistics accompanying the chart include average number of packets per hour, day, or week and counts of uplinks and downlinks. Data also includes details of the last packet received.
- **Join Requests per hour/day/week:** Number of join requests received over time. See join request status for more information. Statistics accompanying the chart include average number of join requests per hour, day, or week and counts of successful and failed join requests. Data also includes details of the last join request received.
- **CRC Error Percentage per hour/day/week:** Number of packets received with failed CRCs (cyclic redundancy checks) over time. A gateway typically receives some false packets (low SNR or signal-to-noise ratio) due to environmental noise. The CRC filters out packets without performing data look-ups on invalid input or data

that is known to be incorrect. If a gateway receives few actual packets, this may indicate a high percentage of CRC error packets. Statistics accompanying the chart include average number of CRC error rate per hour, day, or week. Data also includes the gateway with the highest CRC error percentage.

- **Missed Packets per hour/day/week:**

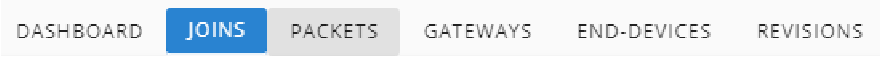
  Missed Uplinks: Number of uplink packets not received by the network server.

  Missed Downlink ACKs: Incremented for each confirmed uplink retry received by the network server, this indicates the number of downlink packets not received by the end device.

Statistics accompanying the chart include packed uplink and downlink averages per hour, day or week and counts of missed uplinks and downlinks.

Tabs

To change the display on dashboard pages, click on the tabs above the map or table.



The following information is available through the Application Network Dashboard:

- Joins Fields
- Packet Fields
- Gateway Fields
- End Device Fields
- Revisions

For more details, including the user's IP address, click the individual revision record.

Editing Application Networks

Follow these steps to edit or delete application networks.

1. Go to **Network > Application Networks** and click on the application network that you want to edit.
2. Click in any field to make edits.

   Note: You can not edit the AppEUI field.
3. Click 💾 to save or ↶ to revert changes.

Deleting an Application Network

To delete the application network:

1. Go to **Network > Application Networks** and click on the network you want to delete.
2. Click 🗑 .
3. Select whether to delete or preserve the associated join requests, packets, and statistics.
4. Click **DELETE** to permanently delete the application network, or click **CANCEL** to return to the application networks page without deleting.

Revisions

Revisions pages show the audit trail for an individual entity.

For an overall audit trail for your organization, refer to Activity.

Revision Fields

Field	Description
When	Revision timestamp
Type	*Gateway only.* Indicates if the change was to the gateway or an application network asset.
Version	Count of edits to the item.
Action	Create if the item is new. Update if the item was edited.
By User	User who made the change. Some revisions are system revisions.
Change	Description of change.

Network Profiles

Network profiles are settings for end devices to operate with. Use profiles to create and apply a standard configuration to multiple end devices.

When an end device first joins to the network, it receives any network profile settings via MAC commands. Any deviation between the network profile and the end device's default settings are sent to the end device in successive MAC commands until all settings have been relayed. Network profile settings override device profile and Conduit network settings.

Note:

- LENS profiles do not overwrite profiles on the Conduit; however, only the LENS profiles are used.
- The Conduit network settings and the device profile provides the default end device settings. Then the network profile settings are applied.

Creating a Network Profile

To create a network profile:

1. Go to **Network > Application Networks > Network Profiles** to view the list of application networks.
2. Click + to create a new network profile.
3. Enter a **Network Profile ID.** Must be unique for this organization. Required.
4. Select **RF Region** from the drop down list. Required.
5. Enter optional field settings as desired. Refer to field descriptions for details.
6. Click **CREATE.**

Application Network Profile Fields

Fields are listed in the order they appear on the Application Network Profile list rather than the New Network Profile Form.

Field	Description
Network Profile ID	ID of the network profile. The profile ID must be unique to your organization and cannot contain spaces.
RF Region	Region where the network is deployed. Select from the drop-down list. Option are: - US915 - AU915 - EU868 - IN865 - KR920 - AS923
RX Delay 1	Receive delay. Delay in seconds between the end of TX and the start of the first RX window. Set a number of seconds between 1 and 15.
RX DR Offset 1	Offset of TX data rate to RX1 data rate for the first RX window. Set an offset value between 0 and 7.
RX Data Rate 2	Data rate to be used for the RX2 window. Options are: - 0 - SF12 BW125 - 1 - SF11 BW125 - 2 - SF10 BW125 - 3 - SF9 BW125 - 4 - SF8 BW125 - 5 - SF7 BW125 - 6 - SF7 BW250 - 7 - FSK - 8 - SF12 BW500 - 9 - SF11 BW500 - 10 - SF10 BW500 - 11 - SF9 BW500 - 12 - SF8 BW500 - 13 - SF7 BW500

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>RX Freq 2</td><td>Frequency used for the RX2 window in MHz, for example 923.3 MHz. Values depend on the region of operation.
<table>
<tr><th>Region</th><th>Regional Limits</th></tr>
<tr><td>EU868</td><td>863-870 MHz</td></tr>
<tr><td>US915</td><td>902-928 MHz</td></tr>
<tr><td>AU915</td><td>915-928 MHz</td></tr>
<tr><td>AS923</td><td>915-928 MHz</td></tr>
<tr><td>KR920</td><td>920-923 MHz</td></tr>
<tr><td>IN865</td><td>865-867 MHz</td></tr>
</table>
</td></tr>
<tr><td>Max Duty Cycle</td><td>Maximum duty cycle supported by the end device. Options are:
■ 100%
■ 50.0%
■ 25.0%
■ 12.5%
■ 6.25%
■ 3.13%
■ 1.56%
■ 0.75%
■ 0.39%
■ 0.20%
■ 0.097%
■ 0.049%
■ 0.024%
■ 0.006%
■ 0.008%</td></tr>
</table>

Max EIRP	The maximum transmission allowed by end devices. This setting is transmitted to the end device in a downlink following OTAA join. Options are: ▪ 8 dBm ▪ 10 dBm ▪ 12 dBm ▪ 13 dBm ▪ 14 dBm ▪ 16 dBm ▪ 18 dBm ▪ 20 dBm ▪ 21 dBm ▪ 24 dBm ▪ 26 dBm ▪ 27 dBm ▪ 29 dBm ▪ 30 dBm ▪ 33 dBm ▪ 36 dBm
Ping Slot Period	Setting is informative, the end device controls the ping slot period setting. Optional if Class B mode supported. Options are: ▪ 1 second ▪ 2 seconds ▪ 4 seconds ▪ 8 seconds ▪ 16 seconds ▪ 32 seconds ▪ 64 seconds ▪ 128 seconds

<table>
<tr><td>Ping Slot DR</td><td>Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Options are:
■ 0 - SF12 BW125
■ 1 - SF11 BW125
■ 2 - SF10 BW125
■ 3 - SF9 BW125
■ 4 - SF8 BW125
■ 5 - SF7 BW125
■ 6 - SF7 BW250
■ 7 - FSK
■ 8 - SF12 BW500
■ 9 - SF11 BW500
■ 10 - SF10 BW500
■ 11 - SF9 BW500
■ 12 - SF8 BW500
■ 13 - SF7 BW500</td></tr>
<tr><td>Ping Slot Freq</td><td>Ping slot frequency value in MHz, for example 923.3 MHz. Values depend on the region of operation. Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default.
<table>
<tr><th>Region</th><th>Regional Limits</th></tr>
<tr><td>EU868</td><td>863-870 MHz</td></tr>
<tr><td>US915</td><td>902-928 MHz</td></tr>
<tr><td>AU915</td><td>915-928 MHz</td></tr>
<tr><td>AS923</td><td>915-928 MHz</td></tr>
<tr><td>KR920</td><td>920-923 MHz</td></tr>
<tr><td>IN865</td><td>865-867 MHz</td></tr>
</table></td></tr>
<tr><td>Class B Timeout</td><td>Maximum delay for the End Device to answer a MAC request or a confirmed DL frame. Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Set a number of seconds between 5 and 600.</td></tr>
<tr><td>Class C Timeout</td><td>Maximum delay for the End Device to answer a MAC request or a confirmed DL frame. Optional if Class C mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Set the number of seconds between 5 and 600.</td></tr>
<tr><td>Class Type</td><td>Enter A, B, or C.</td></tr>
</table>

Channel Mask	A bit-mask of channels enabled for the end device. Select the supported channels if multiple gateways are configured. If a channel mask is not specified in Network Settings, it is determined by frequency bands. **Note:** If you enable channels that the gateway is not configured to receive, uplink packets will be lost. ▪ Configured mask is sent using ADR commands in first downlink following an OTAA Join event. For ABPA devices, these commands are sent on first downlink or any time downlink and uplink counters are reset to 0. ▪ US915 and AU915 (64 – 125 KHz channels + 8 – 500 KHz channels) Start with 00 Channels 79-72 are not defined (1-byte), Channels 71-64 (1-byte), Channels 63-0 (8-bytes) FSB1 and FSB2 – 0003000000000000FFFF FSB1 and FSB8 – 0081FF000000000000FF ▪ EU868, IN865, AS923 and KR920 (up to 16 channels) ▪ Enable 8 channels - 00FF
Redundancy	The number of times to repeat an unconfirmed uplink. Repeating continues until this value is reached or a downlink is received in RX1 or RX2. Valid values are 1 to 15.
Uplink Dwell Time	Use with AS923 channel plan. Limits size of uplinks following OTAA join. Options are: ▪ GW Default (Uses the gateway's default setting.) ▪ 0 - No Limit ▪ 1 - 400 ms
Downlink Dwell Time	Use with AS923 channel plan. Limits size of downlinks following OTAA join. Options are: ▪ GW Default (Uses the gateway's default setting.) ▪ 0 - No Limit ▪ 1 - 400 ms
ADR ACK Limit	The number of uplinks with ADR enabled, after a downlink has been requested, before the TX data rate is reduced to ensure connectivity. Valid values are 0 to 128.
ADK ACK Delay	The number of uplinks with ADR enabled, before the network requests a downlink to ensure connectivity. Valid values are 0 to 128.

Uplink Channels	Channels used for uplink. Configure up to 16 channels to send to end devices. Not available for US915 and AU915 fixed channel plans. Click + to add a new channel plan and enter channel settings in the following format: Index | Frequency | Max DR | Min DR Index: Value 0-15 Frequency: Enter the uplink channel frequency band. Max/Min DR: One byte hex. Value 0-7
Downlink Channels	Channels used for downlinks for frequencies other than LoRaWAN defaults. Not available for US915 and AU915 fixed channel plans. Click + to add a new channel plan and enter channel settings in the following format: Index | Frequency Index: Value 0-15 Frequency: Enter the downlink channel frequency band.

Assigning a Profile to an Application Network

application network

To assign a profile to an application network:

1. Go to **Networks > Application Networks.**
2. Click on the application network you want to assign a profile to.
3. Select the desired profile from the **Network Profile** drop-down list.
4. Click 💾 to save changes or ↶ to restore changes.

The change saves automatically.

Application Network Profile Fields

Fields are listed in the order they appear on the Application Network Profile list rather than the New Network Profile Form.

Field	Description
Network Profile ID	ID of the network profile. The profile ID must be unique to your organization and cannot contain spaces.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>RF Region</td><td>Region where the network is deployed. Select from the drop-down list. Option are:
- US915
- AU915
- EU868
- IN865
- KR920
- AS923</td></tr>
<tr><td>RX Delay 1</td><td>Receive delay. Delay in seconds between the end of TX and the start of the first RX window. Set a number of seconds between 1 and 15.</td></tr>
<tr><td>RX DR Offset 1</td><td>Offset of TX data rate to RX1 data rate for the first RX window. Set an offset value between 0 and 7.</td></tr>
<tr><td>RX Data Rate 2</td><td>Data rate to be used for the RX2 window. Options are:
- 0 - SF12 BW125
- 1 - SF11 BW125
- 2 - SF10 BW125
- 3 - SF9 BW125
- 4 - SF8 BW125
- 5 - SF7 BW125
- 6 - SF7 BW250
- 7 - FSK
- 8 - SF12 BW500
- 9 - SF11 BW500
- 10 - SF10 BW500
- 11 - SF9 BW500
- 12 - SF8 BW500
- 13 - SF7 BW500</td></tr>
<tr><td>RX Freq 2</td><td>Frequency used for the RX2 window in MHz, for example 923.3 MHz. Values depend on the region of operation.
<table>
<tr><th>Region</th><th>Regional Limits</th></tr>
<tr><td>EU868</td><td>863-870 MHz</td></tr>
<tr><td>US915</td><td>902-928 MHz</td></tr>
<tr><td>AU915</td><td>915-928 MHz</td></tr>
<tr><td>AS923</td><td>915-928 MHz</td></tr>
<tr><td>KR920</td><td>920-923 MHz</td></tr>
<tr><td>IN865</td><td>865-867 MHz</td></tr>
</table></td></tr>
</table>

Max Duty Cycle	Maximum duty cycle supported by the end device. Options are: ▪ 100% ▪ 50.0% ▪ 25.0% ▪ 12.5% ▪ 6.25% ▪ 3.13% ▪ 1.56% ▪ 0.75% ▪ 0.39% ▪ 0.20% ▪ 0.097% ▪ 0.049% ▪ 0.024% ▪ 0.006% ▪ 0.008%
Max EIRP	The maximum transmission allowed by end devices. This setting is transmitted to the end device in a downlink following OTAA join. Options are: ▪ 8 dBm ▪ 10 dBm ▪ 12 dBm ▪ 13 dBm ▪ 14 dBm ▪ 16 dBm ▪ 18 dBm ▪ 20 dBm ▪ 21 dBm ▪ 24 dBm ▪ 26 dBm ▪ 27 dBm ▪ 29 dBm ▪ 30 dBm ▪ 33 dBm ▪ 36 dBm

<table>
<tr><td>Ping Slot Period</td><td>Setting is informative, the end device controls the ping slot period setting. Optional if Class B mode supported. Options are:<ul><li>1 second</li><li>2 seconds</li><li>4 seconds</li><li>8 seconds</li><li>16 seconds</li><li>32 seconds</li><li>64 seconds</li><li>128 seconds</li></ul></td></tr>
<tr><td>Ping Slot DR</td><td>Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Options are:<ul><li>0 - SF12 BW125</li><li>1 - SF11 BW125</li><li>2 - SF10 BW125</li><li>3 - SF9 BW125</li><li>4 - SF8 BW125</li><li>5 - SF7 BW125</li><li>6 - SF7 BW250</li><li>7 - FSK</li><li>8 - SF12 BW500</li><li>9 - SF11 BW500</li><li>10 - SF10 BW500</li><li>11 - SF9 BW500</li><li>12 - SF8 BW500</li><li>13 - SF7 BW500</li></ul></td></tr>
<tr><td>Ping Slot Freq</td><td>Ping slot frequency value in MHz, for example 923.3 MHz. Values depend on the region of operation. Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default.<table><tr><th>Region</th><th>Regional Limits</th></tr><tr><td>EU868</td><td>863-870 MHz</td></tr><tr><td>US915</td><td>902-928 MHz</td></tr><tr><td>AU915</td><td>915-928 MHz</td></tr><tr><td>AS923</td><td>915-928 MHz</td></tr><tr><td>KR920</td><td>920-923 MHz</td></tr><tr><td>IN865</td><td>865-867 MHz</td></tr></table></td></tr>
</table>

Class B Timeout	Maximum delay for the End Device to answer a MAC request or a confirmed DL frame. Optional if Class B mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Set a number of seconds between 5 and 600.
Class C Timeout	Maximum delay for the End Device to answer a MAC request or a confirmed DL frame. Optional if Class C mode supported. If you enter a setting in this field, it will override the gateway or channel plan default. Set the number of seconds between 5 and 600.
Class Type	Enter A, B, or C.
Channel Mask	A bit-mask of channels enabled for the end device. Select the supported channels if multiple gateways are configured. If a channel mask is not specified in Network Settings, it is determined by frequency bands. **Note:** If you enable channels that the gateway is not configured to receive, uplink packets will be lost. ■ Configured mask is sent using ADR commands in first downlink following an OTAA Join event. For ABPA devices, these commands are sent on first downlink or any time downlink and uplink counters are reset to 0. ■ US915 and AU915 (64 – 125 KHz channels + 8 – 500 KHz channels) Start with 00 Channels 79-72 are not defined (1-byte), Channels 71-64 (1-byte), Channels 63-0 (8-bytes) FSB1 and FSB2 – 0003000000000000FFFF FSB1 and FSB8 – 0081FF000000000000FF ■ EU868, IN865, AS923 and KR920 (up to 16 channels) ■ Enable 8 channels - 00FF
Redundancy	The number of times to repeat an unconfirmed uplink. Repeating continues until this value is reached or a downlink is received in RX1 or RX2. Valid values are 1 to 15.
Uplink Dwell Time	Use with AS923 channel plan. Limits size of uplinks following OTAA join. Options are: ■ GW Default (Uses the gateway's default setting.) ■ 0 - No Limit ■ 1 - 400 ms
Downlink Dwell Time	Use with AS923 channel plan. Limits size of downlinks following OTAA join. Options are: ■ GW Default (Uses the gateway's default setting.) ■ 0 - No Limit ■ 1 - 400 ms
ADR ACK Limit	The number of uplinks with ADR enabled, after a downlink has been requested, before the TX data rate is reduced to ensure connectivity. Valid values are 0 to 128.
ADK ACK Delay	The number of uplinks with ADR enabled, before the network requests a downlink to ensure connectivity. Valid values are 0 to 128.

Uplink Channels	Channels used for uplink. Configure up to 16 channels to send to end devices. Not available for US915 and AU915 fixed channel plans. Click + to add a new channel plan and enter channel settings in the following format: Index | Frequency | Max DR | Min DR Index: Value 0-15 Frequency: Enter the uplink channel frequency band. Max/Min DR: One byte hex. Value 0-7
Downlink Channels	Channels used for downlinks for frequencies other than LoRaWAN defaults. Not available for US915 and AU915 fixed channel plans. Click + to add a new channel plan and enter channel settings in the following format: Index | Frequency Index: Value 0-15 Frequency: Enter the downlink channel frequency band.

Editing a Network Profile

To edit a network profile:

1. Go to **Network > Network Profiles** and select **Groups**.
2. Make the desired changes. For profile field descriptions, go to Network Profile Fields

   Changes are saved automatically.

Deleting a Network Profile

To delete one or more network profiles:

1. Go to **Networks** > **Network Profiles.**
2. Click the check boxes for the profiles you want to delete.
3. Click 🗑.
4. To preserve associated join requests, packets, and statistics move the slide to the left. The default setting is to delete this data.
5. Confirm the deletion.

Chapter 5 – Gateways

Gateways are LoRaWAN gateways and access points that report received LoRaWAN join requests and packet metadata to the LENS Cloud.

Products supported include MultiTech's Conduit (MTCDT) with a LoRa accessory card (MTAC-LORA), Conduit IP67 Base Station (MTCDTIP), Conduit IP67 200 Series Base Station (MTCDTIP2) and Conduit AP (MTCAP and MTCAP2).

To access the Gateways page, click **Network > Gateways**.

Gateways Snapshot

The gateways page shows:

- Number of provisioned gateways
- Gateway Device Check: Counts of gateway health status alerts by alert type and a link to the Gateway Health Checklist page.
- A list of gateways. For more information about the data shown, refer to Data Fields in Gateway Fields.

Use the **Gateways** page to:

- Provision a new gateway
- View and edit gateway settings
- Upload CSV of gateways

Provisioning a New Gateway

Create a new gateway and assign it to one or multiple application networks.

Note: For information on importing gateway data, go to Uploading CSV Files.

You need the following information from the gateway, which is available from EEPROM through the API (https://<gatewayIP>/api/system)

- EUI from MTAC EEPROM

  Conduit

  MTAC Slot 1: https://192.168.2.1/api/system/accessoryCards/0/eui

  MTAC Slot 2: https://192.168.2.1/api/system/accessoryCards/1/eui

  Conduit AP: https://192.168.2.1/api/system/loraEui {"code" : 200, "result" : "00:00:00:00:00:00:20:30", "status" : "success"}
- UUID

  https://192.168.2.1/api/system/uid {"code" : 200, "result" : "2AB7F679AA6141609F1C5BF7E2CE3774", "status" : "success"}
- Serial Number/Device ID (also mPower Device information page)

  https://192.168.2.1/api/system/deviceId { "code" : 200, "result" : 11223344" "status" : "success" }

To provision a gateway:

1. In LENS, go to **Network > Gateways**.

2. Hover over ⋮.
3. Click +.
4. Enter the GwEUI, the UUID, and the serial number.

   Note: These fields are required.

5. Enter data in optional fields as desired. For field descriptions, go to Gateway Fields.
6. Select an application network from the drop-down list. A gateway can belong to multiple application networks.

   To select multiple networks, click on each network.

   To de-select a network, click on it again.

7. Click **Provision** or click **Cancel** to exit without saving.

Gateway Fields

Field	Definition
Setup Fields	
GwEUI	Registered gateway's ID. This is a hexadecimal string, 8 two-digit hexadecimal numbers. Valid characters are 0-9, A-F, a-f. Case does not matter. Required.
UUID	Universally unique identifier. Required.
Serial Number	Serial number assigned to the gateway. Required.
Name	Assigned name of the gateway. Optional.
Application Networks	Application network(s) associated with this gateway. Select one or more application networks from the drop-down list.
Data Fields	
Status	Shows the gateway's health check status. For status definitions, refer to Gateway Health Checklist.
API Error	If a gateway has a machine API error, the error code appears in this field. If a column displays an error, click the row to view the gateway's configuration screen.
Licensed	Indicates if the gateway is currently licensed.
Authorized	Indicates if a gateway is currently authorized. Gateways may be authorized, but not licensed during a short grace period after a license has expired. For enterprise organizations without individual gateway tokens, this fields indicated an authorized gateway.
Last Seen	Time of last report from the gateway.
Latitude	Location data of the gateway; can be reported by gateway if GPS is available.
Longitude	Location data of the gateway; can be reported by gateway if GPS is available.
Altitude	Location data of the gateway; can be reported by gateway if GPS is available.
IP Address	Address of the packet forwarder.

Field	Definition
Setup Fields	
IP Port	UDP port of the packet forwarder. Provided by the gateway when it checks in.
Protocol Version	Protocol version of the gateway. Provided by the gateway when it checks in.

Gateway Dashboard

The dashboard contains information and graphs pertaining to the specific gateway. Appears when you click on a gateway on the Gateways page.

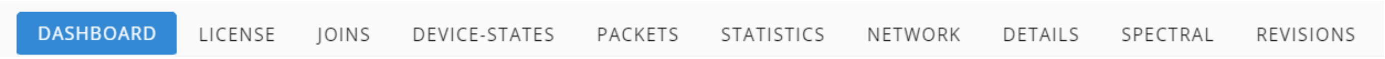
Gateway Snapshot

The selected gateway's information appears at the top of the page. This is information from gateway setup or that the gateway provides when it checks in. For information about this content, refer to Gateway Fields.

- **Gateway Map:** Shows the location of each gateway that has latitude and longitude coordinates.
- **Rx Signal Per Hour, Day, or Week:** Shows the gateway's minimum and maximum RSSI and SNR over time. Statistics accompanying the chart show RSSI and SNR average for the hour, day, or week, and the minimum and maximum RSSI and SNR values.
- **Packet Frequency Distribution:** Shows a gateway's uplinks and downlinks per frequency. Statistics accompanying the chart show the frequency used most often for uplinks and downlinks as well as the total uplinks and downlinks.
- **Packet Datarate Distribution:** Shows the number and percentage of uplinks and downlinks per datarate for the gateway.

Tabs

To change the display on dashboard pages, click on the tabs above the map or table.



License Tab Fields

Shows Gateway token information.

Field	Description
Token ID	Used for licensing renewals and uniquely identifies the MultiToken.
Activated	Date the token was activated.
Expiration Setting	Billing date plus the number license days. If there is a Expiration setting, the Expires On date is the same. If there is no expiration setting, the gateway has a trial token.
Expires On	Used by LENS to determine whether or not the gateway is licensed. A future date indicates a licensed gateway. No date or a date in the past indicates an unlicensed gateway. If the gateway is licensed, Expires On is Expiration Setting date. If the gateway has a trial token, this is the activation date plus 60. If this field is blank, the trial token has not been activated.
Days of Licensing	Shows the length of the token license, 60 represents an evaluation license. 365 is a full license.

Field	Description
Created On	Date the token was created.
Updated On	Most recent token update date.

Gateway Statistics

Statistics for single connected gateways.

Field	Definition
Timestamp	Date and time of this record.
Rx Count	Uplinks received by the gateway from end devices
Rx OK	Uplinks reported by gateway passing CRC
Rx Forwarded	Uplinks reported by the gateway
Uplinks	Uplinks received
OK Uplinks	Uplinks passing MIC validation
MIC Fail Uplinks	Uplinks failing MIC validation
Unknown Fail Uplinks	Uplinks from unknown devices. DevAddr does not match a device, or the device is from another network.
Tx Count	Downlinks transmitted by the gateway
Downlinks	Downlinks forwarded to the gateway
ACK Requested Downlinks	Downlinks sent requesting ACK
ACK Rate	ACK rate of uplink datagrams (measure of UDP connectivity)
MIC Fails	Uplinks failing MIC validation
CRC Errors	Uplinks failing CRC validation. CRC error can be a packet that has been interfered by other transmission, created by noise or a weak reflected signal.

Joins Fields

Field	Definition
Timestamp	Time received.
Join Server	One of the following: ▪ Shows Cloud if the join server handled the join request. ▪ Local if handled by the Conduit join server locally (local keys or NetworkID/NetworkKey).

Field	Definition
Result	One of the following: - **Success** - **MICFailed**: Key mismatch between the join server and the end device. Reconfigure the keys if this persists. - **JoinReqFailed**: Gateway mismatch. The device is known but can not join the gateway due to application network settings. - **UnknownDevEUI**: Device not found in the organization.
Description	Details of result.
End device	Device EUI from join request. Appears on application network and gateway join lists.
Gateway	Gateway EUI reporting join request. Appears on application networks and end device join lists.
Application Network	Application network name used for join request. Appears on gateway and end device join lists.
Join EUI	EUI of a successful join request.
RSSI	Signal strength of the received packet.
SNR	Signal to noise ratio of the received packet.
Freq	Frequency in MHz used for join requests.
Data rate	Data rate used for packet.
DevAddr	Network device address to be assigned to end device.
MAC Version	LoRaWAN protocol version implemented in end device firmware, for example 1.0.4 or 1.1.
HnetID	NetID configured in Conduit Network Server reporting packet.
RxDelay	Delay (measured in seconds) to be sent to the device in the join response. Used to time the opening of the Rx window.
DL Settings	Additional Rx Window settings of Rx1 data rate offset and Rx2 data rate.

Packet Fields

Fields	Definitions
Packet Time	Time that the packet was sent or received.
Link Direction	**Up** packets are transmitted by end device; **Down** packets are transmitted by gateways.
End device	EUI of device transmitting the uplink packet or destination of downlink packet. Appears on Gateway and Application Network Packets lists.
Gateway	EUI of gateway that received the uplink or transmitted the downlink packet. Appears on Application Network and End Device Packets lists.
Application Network	Application network used by the gateway or end device for this packet. Appears on Gateway and End Device Packets lists.
RSSI	Signal strength of the received packet, uplink packets only.

Fields	Definitions
SNR	Signal to noise ratio of received packet, uplink packets only.
Freq	Frequency in MHz that is used to transmit or receive the packet at the gateway.
Data rate	Data rate used for uplink or downlink packet.
Data Size	Size of application payload and MAC commands in packet; total packet size minus the header.
DevAddr	Address reported in the packet header.
Counter	32-bit counter maintained by the end device and network server. Only 16 bits are contained in the packet header sent over the air. Upper 16 bits are tracked at each side and used for encryption and MIC calculations.
Msg Type	Message type of packet, uplink or downlink, confirmed or unconfirmed. Confirmed packets may be present if ACK is not received.
Tx Power	Tx power used to transmit downlink packet from the gateway, downlinks only.
Rx Window	Rx window packet was scheduled for, downlinks only.
Port	Application port used in uplink or downlink packet. If port was not provided, 0 will display.
Control	FCtrl byte of packet header. Includes ADRACKReq, ADR bits, and length of FOpts (MAC Commands).
Commands	MAC commands included in the packet.

Editing a Gateway

To edit a gateway:

1. Go to **Network > Gateways**.
2. Click on the gateway you want to edit.
3. Click on the field you want to edit and make desired changes.
4. Click 💾 to save changes or ↶ to revert to the previous value.

Editing Multiple Gateways

Bulk editing allows you to set the application network for the selected gateways. To bulk edit:

1. Go to **Network > Gateways**.

   Note: Bulk editing is also available from the Application Network's Gateways tab.

2. Click the check boxes for the gateways you want to edit.
3. Click the **EDIT** button.
4. Select an application network from the drop-down list.
5. Click **SAVE** to save or **CANCEL** to revert changes.

Deleting a Gateway

To delete a gateway:

1. Go to **Network > Gateways**.
2. Click on the gateway you want to delete.
3. Click 🗑.
4. Confirm the deletion.

Alternatively, click the check box on the gateway list, click DELETE, and confirm the deletion.

Deleting Multiple Gateways

To delete multiple gateways:

1. Go to **Networks > Gateways**.
2. Click the check boxes for the gateways you want to delete.
3. Click the **DELETE** button.
4. To preserve associated join requests and packets, move the slider to the left.
5. Confirm the deletion by moving the **Are you sure?** slider to the right. The DELETE button is no longer grayed out.
6. Click **DELETE**.

Spectral Scan Overview

If your Conduit gateway is configured for RSSI/dBM spectral scan, this tab provides a 3D representation of spectral scan data. For details on configuring a Conduit product for spectral scan, refer to the Consult the mPower Conduit AEP Software Guide.

This illustrates sub-band usage before and after a gateway is deployed, which allows you to distinguish between busy and free channels in your channel plan. This helps you decide which sub-band frequencies you want to use for your LoRa gateways.

Setting Up the Spectral Scan Graph

To analyze spectral scan data, adjust the following settings as needed:

Time Series Traversal:

To show bandwidth usage at different times:

- Click a number in the sequence.

Selecting a Time Frame

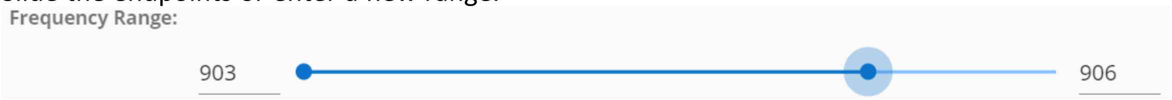
To select a time frame for the graph:

1. Slide the **Use Timeframe slider** to the right.
2. Select the **Beginning Data** and **Ending Date** range.

Setting the Frequency Range

To change the frequency range:

- Slide the endpoints or enter a new range.



Frequency Range:

903

906

RSSI Statistic Selection

Select a RSSI statistic from the drop-down list. Options are:

Option	Description
10%	10th percentile of RSSI, 10% of samples reported above this value
30%	30th percentile of RSSI, 30% of samples reported above this value
50%	50th percentile of RSSI, 50% of samples reported above this value, median
80%	80th percentile of RSSI, 80% of samples reported above this value
min	Minimum RSSI
avg	Average RSSI
max	Maximum RSSI

Graph Results

The graph shows frequency band usage over time.

RSSI Data

This section shows text values for the graph, including minimum and maximum values for RSSI, frequency, and time frame.

Fixed Min RSSI Range

To keep the minimum RSSI locked for the graph:

- Move the slider to the right (true).

To allow the minimum RSSI to adjust with changing data:

- Move the slider to the left (false).

To rotate the graph:

- Click on the graph and drag it.

Acceptable Signal Strengths

Signal Strength	Short Description	Detailed Description
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.

Revisions

Revisions pages show the audit trail for an individual entity.

For an overall audit trail for your organization, refer to Activity.

Revision Fields

Field	Description
When	Revision timestamp
Type	*Gateway only.* Indicates if the change was to the gateway or an application network asset.
Version	Count of edits to the item.
Action	Create if the item is new. Update if the item was edited.
By User	User who made the change. Some revisions are system revisions.
Change	Description of change.

Chapter 6 – Policies

Gateways may receive requests from end devices outside the network. To prevent these end devices from sending join requests to the join server, use policies to block unwanted traffic at the gateway. Policies are whitelists of end devices allowed to have their join requests forwarded to the join server.

Policies become available to the gateway when it checks in. Each gateway associated with a policy enforces the policy.

- Add end devices to the whitelist by selecting end device groups and/or application networks.
- Also add end devices the whitelist by creating custom filters for specific device EUIs, device EUI ranges, join EUIs, or join EUI ranges.
- When you set up a policy, you can apply the policy to selected individual gateways and/or to all the gateways associated with selected application networks.

Creating a New Policy

To create a new policy:

1. Go to **Network > Policies** and click ⊕.
2. Enter a policy **Name**, required, and **Description**, optional.
3. Move the slider to the right to enable the policy.
4. To apply this policy to one or more application networks or gateways, click the check boxes in the Applies To drop-down lists. For more information, refer to Policy Fields.
5. To set a filter for specific application networks or end device groups, click the check boxes in the Group Filter drop-down lists. For more information, refer to Policy Fields.
6. To enter custom filters, select the **Filter Type** from the drop-down list and click **ADD**.For more information, refer to Policy Fields.
7. Enter the **EUI** or EUI range for the filter.
8. Repeat Steps 5 and 6 for each custom filter you want to add.
9. Click **CREATE.**

Policy Fields

Fields	Descriptions
Identity	
Name	Policy name. Required.
Description	Policy description. Optional.
Enabled	Enable or disable the policy. Move the slider to the right to enable the policy.
Applies To	
Sends the policy to all the selected gateways and the gateways associated with the selected application networks. Selecting at least one application network or gateway is required.	

Fields	Descriptions
Application Networks	One or more application networks to which this policy applies. Click the check boxes to select application networks.
Gateways	One or more gateways to which this policy applies. Click the check boxes to select gateways.
Group Filters	
Specifies the end devices whitelisted for contacting the Join Server. Can be used with custom filters.	
Application Networks	Application networks whose devices are included in the whitelist. Click the check boxes the application networks.
End Device Groups	End devices groups included in the whitelist. Click the check boxes for the end device groups you want to include.
Custom Filters	
Specifies individual device or join EUIs or EUI ranges. For custom filters, select the type of filter from the drop-down list and click **ADD**. Then enter the filter value. You can add multiple filters.	
Filter Type	Options are: ■ Device EUI ■ Device EUI Range ■ Join EUI ■ Join EUI Range
(Filter value)	Enter the EUI or the EUI range for the selected filter type.

Editing Policies

To edit a policy

1. Go to **Network > Policies** and click on the policy you want to edit.
2. Make desired changes.
3. Click 💾 to save or ↶to revert changes.

Deleting Policies

To delete a policy:

1. Go to **Network > Policies.**
2. Click on the policy you want to delete.
3. Click 🗑.
4. Confirm the deletion.

Note: You can delete custom filters by clicking 🗑 for that filter.

Chapter 7 – End Devices

End devices are sensors with radios that report data via LoRa packets to a gateway. Before sending data, an end device must join a gateway. A transmit session lasts as long as the end device and gateway maintain the keys and counters associated with the sessions. If either side loses session information, a new join must be made. An end device can be joined to only one network server instance on a gateway.

To access the end devices page, go to **Device > End Devices**.

End Devices Snapshot

The End Device page shows:

- Number of provisioned end devices.
- Device Check: Counts of device health status alerts by alert type and a link to the End Device Health Checklist page.
- A list of end devices. For more information about the data shown, refer to End Device Fields.

Use the scroll bar at the bottom of the page to scroll through the end device table.

Use the **End Devices** page to:

- Provision a new end device
- View and edit end devices
- Upload a CSV of end devices

Provisioning an End Device

By default, all end devices are LoRaWAN Class A devices. Use Device Profiles to specify if the device is Class B or C.

To create and provision an end device:

1. Go to **Device > End Devices**. A list of end devices appears.
2. Hover over or tap ⋮.
3. Click +.
4. Enter the end device's unique identifier in the **DevEUI** field. For more information refer to End Device Fields.
    - Must contain 8 2-character hexidecimal numbers.
    - Valid characters are hex digits (0-9, A-F, a-f).
    - Hyphen separators (-) are automatically added.

   For examples and more information go to End Device Fields .
5. Enter the **AppKey.** For more information refer to End Device Fields.
    - Must containt 16 octets.
    - Valid characters are hex digits (0-9, A-F, a-f).
    - Period separators (.) are automatically added.
6. Enter optional field settings as desired. For details, go to End Device Fields.

7. Click **PROVISION** or **CANCEL** to exit without saving.

End Device Fields

Fields are listed in the order they appear on the End Device list rather than the New End Device Form.

Field	Description
Setup Fields	
DevEUI	End device's extended unique identifier. This is a hexadecimal string, 16 characters long. Valid characters are 0-9, A-F, a-f. Case does not matter. DevEUI is Required.
AppKey	Appears on End Device set up form only. Device specific AES-128 key used to create a secure encrypted and authenticated connection between the gateway and the end device over RF. Configured on the end device and the Cloud, AppKey is used to create session keys for each join session. These session keys are sent to the gateway. An end device creates the same session keys using nonce values in the join request/response messages. The response message is encrypted using the AppKey. To keep the AppKey secret and secure, it is not shared with the gateway. AppKeys are user-generated hexadecimal strings 32 characters long. Valid characters are 0-9, A-F, a-f. Case does not matter. For best practices, use a random value. Required.
Name	Assigned name. Optional.
Status	Shows the device's health check status. Options are configured, active, or warning. For status definitions, refer toHealth Check Overview.
Device Profile	Appears on End Device list as Profile. End device profile for this device. Optional. Select profile from the drop-down list. For more information, go to Device Profiles.
Network Profile	Appears on End Device list as Network. Network profile for this device. Optional. Select profile from the drop-down list. For more information, go to Network Profile Fields.
Application Network	Application Network for this device. Optional. Select from the drop-down list. For more information, go to Application Networks.
Serial Number (S/N)	End device's serial number. Optional.
Product ID	End device's product ID. Optional.
Hardware (HW) Version	End device's hardware version number. Optional.
Firmware (FW) Version	Version number of firmware installed on the end device. Optional.
Data Fields	
Last Seen	Time that a gateway last received an uplink packet from this end device. Appears on the End Device list only.
Rejoin Count	Number of times the end device has rejoined the network.
Uplink Count	Last reported 32-bit uplink counter value. Appears on the End Device list only.
Downlink Count	Last reported 32-bit downlink counter value. Appears on the End Device list only.

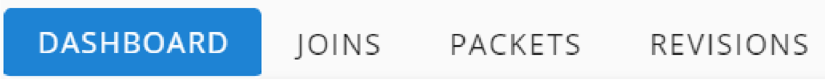
End-Device Dashboard

The dashboard contains graphs pertaining to the specific end device.

- **Rx Signal Per Hour, Day, or Week:** Shows the end device's minimum and maximum RSSI and SNR over time. Statistics accompanying the chart show RSSI and SNR average for the hour, day, or week, and the minimum and maximum RSSI and SNR values.
- **Packet Frequency Distribution:** Shows the end device's uplinks and downlinks per frequency. Statistics accompanying the chart show the frequency used most often for uplinks and downlinks as well as the total uplinks and downlinks.
- **Packet Datarate Distribution:** Shows the number and percentage of uplinks and downlinks per datarate for the end device.

Tabs

To change the display on dashboard pages, click on the tabs above the map or table.



The following information is available through the End-Device Dashboard:

- Joins Fields
- Packet Fields
- Revisions

Packet Fields

Fields	Definitions
Packet Time	Time that the packet was sent or received.
Link Direction	**Up** packets are transmitted by end device; **Down** packets are transmitted by gateways.
End device	EUI of device transmitting the uplink packet or destination of downlink packet. Appears on Gateway and Application Network Packets lists.
Gateway	EUI of gateway that received the uplink or transmitted the downlink packet. Appears on Application Network and End Device Packets lists.
Application Network	Application network used by the gateway or end device for this packet. Appears on Gateway and End Device Packets lists.
RSSI	Signal strength of the received packet, uplink packets only.
SNR	Signal to noise ratio of received packet, uplink packets only.
Freq	Frequency in MHz that is used to transmit or receive the packet at the gateway.
Data rate	Data rate used for uplink or downlink packet.
Data Size	Size of application payload and MAC commands in packet; total packet size minus the header.
DevAddr	Address reported in the packet header.

Fields	Definitions
Counter	32-bit counter maintained by the end device and network server. Only 16 bits are contained in the packet header sent over the air. Upper 16 bits are tracked at each side and used for encryption and MIC calculations.
Msg Type	Message type of packet, uplink or downlink, confirmed or unconfirmed. Confirmed packets may be present if ACK is not received.
Tx Power	Tx power used to transmit downlink packet from the gateway, downlinks only.
Rx Window	Rx window packet was scheduled for, downlinks only.
Port	Application port used in uplink or downlink packet. If port was not provided, 0 will display.
Control	FCtrl byte of packet header. Includes ADRACKReq, ADR bits, and length of FOpts (MAC Commands).
Commands	MAC commands included in the packet.

Joins Fields

Field	Definition
Timestamp	Time received.
Join Server	One of the following: ▪ Shows Cloud if the join server handled the join request. ▪ Local if handled by the Conduit join server locally (local keys or NetworkID/NetworkKey).
Result	One of the following: ▪ **Success** ▪ **MICFailed**: Key mismatch between the join server and the end device. Reconfigure the keys if this persists. ▪ **JoinReqFailed**: Gateway mismatch. The device is known but can not join the gateway due to application network settings. ▪ **UnknownDevEUI**: Device not found in the organization.
Description	Details of result.
End device	Device EUI from join request. Appears on application network and gateway join lists.
Gateway	Gateway EUI reporting join request. Appears on application networks and end device join lists.
Application Network	Application network name used for join request. Appears on gateway and end device join lists.
Join EUI	EUI of a successful join request.
RSSI	Signal strength of the received packet.
SNR	Signal to noise ratio of the received packet.
Freq	Frequency in MHz used for join requests.
Data rate	Data rate used for packet.

Field	Definition
DevAddr	Network device address to be assigned to end device.
MAC Version	LoRaWAN protocol version implemented in end device firmware, for example 1.0.4 or 1.1.
HnetID	NetID configured in Conduit Network Server reporting packet.
RxDelay	Delay (measured in seconds) to be sent to the device in the join response. Used to time the opening of the Rx window.
DL Settings	Additional Rx Window settings of Rx1 data rate offset and Rx2 data rate.

Viewing and Editing an End Device

Viewing an End Device's Information

To view or edit an end device:

- Go to **Device > End Devices** and click on a listed end device.

End Device Page

End Device name, DevEUI, and when the device was last seen by the gateway appear at the top of the End Device page. The rest of the top section shows the end device setting, which can be edited. For settings details, refer to End Device Fields.

The End Device dashboard appears below device configuration settings. For details go to End-Device Dashboard.

To view Joins or Packets information for this end device, click on JOINS or PACKETS. For details, refer to Joins Fields and Packets Fields.

Editing End Device Settings

To edit an end device:

1. Click on the device that you want to edit.
2. Make desired changes.
3. Click 💾.

To undo changes:

- Click ↶.

Editing Multiple End Devices

Bulk editing allows you to set the application network and device profile for the selected devices. To bulk edit:

1. Go to **Device > End Devices**.
   Note: Bulk editing is also available from the Application Network's End Devices tab.
2. Click the check boxes for the devices you want to edit.
3. Click the **EDIT** button.
4. Select an application network and/or device profile from the drop-down lists.
5. Click 💾 to save or ↶ to revert changes.

Delete an End Device

To delete an End Device:

1. Go to **Devices > End Devices**.
2. Click on the end device you want to delete.
3. Click 🗑.
4. Confirm the deletion.

Alternatively, click the check box on the end device list, click DELETE, and confirm the deletion.

Deleting Multiple End Devices

To delete multiple end devices:

1. Go to **Device > End Devices**.
2. Click the check boxes for the devices you want to delete.
3. Click the **DELETE** button.
4. To preserve associated join requests and packets, move the slider to the left.
5. Confirm the deletion by moving the **Are you sure?** slider to the right. The DELETE button is no longer grayed out.
6. Click **DELETE**.

Revisions

Revisions pages show the audit trail for an individual entity.

For an overall audit trail for your organization, refer to Activity.

Revision Fields

Field	Description
When	Revision timestamp
Type	*Gateway only.* Indicates if the change was to the gateway or an application network asset.
Version	Count of edits to the item.
Action	Create if the item is new. Update if the item was edited.
By User	User who made the change. Some revisions are system revisions.
Change	Description of change.

Chapter 8 – Device Profiles

Device Profiles

Device profiles provide default settings for end devices to use when joined to the network and support end-device deployment. Use device profiles to create and apply the same standard configuration to multiple end devices.

After a device profile has been created, it can be applied to new or existing end devices through the Device Profile drop-down list.

Note:

- LENS profiles do not overwrite profiles on the Conduit; however, when there are profiles for both LENS and the Conduit, only the LENS profiles are used.
- If there are conflicts between device profile settings and network profile settings, the network profile setting is applied.
- If the end device Rx window settings deviate from the device profile Rs window settings, lost downlinks may occur.
- Device profile settings are sent to the Conduit in the join accept message and are collected during gateway check-ins.

Creating a New Device Profile

To create a new profile:

1. Click **Device > Device Profiles.**
2. Click ⊕.
3. Enter a Device Profile ID. Required. By default this is based on profile settings. For more information, refer to Device Profile Fields.

   By default, the Device Profile form is enabled for Class A devices, joins, and 32 bit FCnt. If you enable support for other classes, fields for those options appear.
4. Move the sliders to the right to add support for Class B or Class C. Remove sliders to the left to remove support for join or 32 bit FCnt.
5. Enter settings for the options you selected. For field descriptions, refer to Device Profile Fields.
6. Click **SAVE.**

Device Profile Fields

Fields and steps depend on whether support for Class B, Class C, and Join is enabled.

Field	Description	Availability
Device Profile ID	ID of the device profile. By default this is based on profile settings. The profile ID must be unique to your organization and cannot contain spaces.	All

Field	Description	Availability
Supports Class B	Enables Yes to enable LoRaWAN operating Class B settings for this device profile. Move slider to the right to enable. Default is disabled.	All
Supports Class C	Enables LoRaWAN operating Class C settings for this device profile. Move slider to the right to enable. Default is disabled.	All
Supports Join	Enables Join. Move slider to the right to enable. Default is enabled.	All
Supports 32 bit FCnt	End device uses 32bit frame counter. Required for LoRaWAN 1.0 end device. Default is enabled.	All
RF Region	Set the RF region where the end device is located. Options are: ▪ US915 ▪ AU915 ▪ EU868 ▪ IN865 ▪ KR920 ▪ AS923	Class A
Reg Params Revision	Revision of the Regional Parameters document supported by the end device. Enter the revision letter.	Class A
MAC Version	LoRaWAN protocol version implemented in end-device firmware, for example 1.0.2 or 1.1. Enter 1.0.2 for LoRaWAN1.0.2 or 1.0.4 for LoRaWAN 1.0.4.	Class A
Max EIRP	Maximum EIRP supported by the end device. Options are: ▪ 8 dBm ▪ 10 dBm ▪ 12 dBm ▪ 13 dBm ▪ 14 dBm ▪ 16 dBm ▪ 18 dBm ▪ 20 dBm ▪ 21 dBm ▪ 24 dBm ▪ 26 dBm ▪ 27 dBm ▪ 29 dBm ▪ 30 dBm ▪ 33 dBm ▪ 36 dBm	Class A

Field	Description	Availability
Max Duty Cycle	Maximum duty cycle supported by the end device. Options are: - 100% - 50.0% - 25.0% - 12.5% - 6.25% - 3.13% - 1.56% - 0.75% - 0.39% - 0.20% - 0.097% - 0.049% - 0.024% - 0.006% - 0.008%	Class A
Class B Timeout	Maximum delay for the end device to answer a MAC request or a confirmed DL frame. Required if Class B mode supported. Set a number of seconds between 5 and 600.	Class B
Ping Slot Period	Required if class B mode supported. Options are: - 1 second - 2 seconds - 4 seconds - 8 seconds - 16 seconds - 32 seconds - 64 seconds - 128 seconds	Class B

<table>
<tr><th>Field</th><th>Description</th><th>Availability</th></tr>
<tr><td>Ping Slot DR</td><td>Required if class B mode supported. Options are:<ul><li>0 - SF12 BW125</li><li>1 - SF11 BW125</li><li>2 - SF10 BW125</li><li>3 - SF9 BW125</li><li>4 - SF8 BW125</li><li>5 - SF7 BW125</li><li>6 - SF7 BW250</li><li>7 - FSK</li><li>8 - SF12 BW500</li><li>9 - SF11 BW500</li><li>10 - SF10 BW500</li><li>11 - SF9 BW500</li><li>12 - SF8 BW500</li><li>13 - SF7 BW500</li></ul></td><td>Class B</td></tr>
<tr><td>Ping Slot Freq</td><td>Required if class B mode supported.<table>
<tr><th>Region</th><th>Regional Limits</th></tr>
<tr><td>EU868</td><td>863-870 MHz</td></tr>
<tr><td>US915</td><td>902-928 MHz</td></tr>
<tr><td>AU915</td><td>915-928 MHz</td></tr>
<tr><td>AS923</td><td>915-928 MHz</td></tr>
<tr><td>KR920</td><td>920-923 MHz</td></tr>
<tr><td>IN865</td><td>865-867 MHz</td></tr>
</table></td><td>Class B</td></tr>
<tr><td>Class C Timeout</td><td>Maximum delay for the end device to answer a MAC request or a confirmed DL frame. Required if Class C mode supported. Set the number of seconds.</td><td>Class C</td></tr>
<tr><td>RX Delay 1</td><td>Receive delay. Delay in seconds between the end of TX and the start of the first RX window. Set a number of seconds between 1 and 15.</td><td>ABP</td></tr>
<tr><td>RX DR Offset 1</td><td>Offset of TX data rate to RX1 data rate for the first RX window. Set an offset value between 0 and 7.</td><td>ABP</td></tr>
</table>

<table>
<tr><td>RX Data Rate 2</td><td>Data rate to be used for the RX2 window. Options are:
■ 0 - SF12 BW125
■ 1 - SF11 BW125
■ 2 - SF10 BW125
■ 3 - SF9 BW125
■ 4 - SF8 BW125
■ 5 - SF7 BW125
■ 6 - SF7 BW250
■ 7 - FSK
■ 8 - SF12 BW500
■ 9 - SF11 BW500
■ 10 - SF10 BW500
■ 11 - SF9 BW500
■ 12 - SF8 BW500
■ 13 - SF7 BW500</td><td>ABP</td></tr>
<tr><td>RX Freq</td><td>Frequency used for the RX2 window. Options are:
<table>
<tr><th>Region</th><th>Regional Limits</th></tr>
<tr><td>EU868</td><td>863-870 MHz</td></tr>
<tr><td>US915</td><td>902-928 MHz</td></tr>
<tr><td>AU915</td><td>915-928 MHz</td></tr>
<tr><td>AS923</td><td>915-928 MHz</td></tr>
<tr><td>KR920</td><td>920-923 MHz</td></tr>
<tr><td>IN865</td><td>865-867 MHz</td></tr>
</table></td><td>ABP</td></tr>
<tr><td>Factory Preset Freqs</td><td>List of factory-preset frequencies. Required for ABP.</td><td>ABP</td></tr>
</table>

Editing a Device Profile

To edit a device profile:

1. Go to **Device > Device Profiles.**
2. Click on the profile you want to edit.
3. Make desired changes.
4. Click the **Save** icon, 💾.

Delete Device Profile

To delete an end device profile

1. Go to **Device > Device Profile** and select the profile you want to delete.
2. Click 🗑.

3. Confirm the deletion.

Chapter 9 – Operations

Scheduling a message or FOTA update sets up a multicast session. In LENS, this creates a temporary device session for the multicast session. Except for cleanup at the end of a FOTA session, multicast sessions are the same for FOTA and multicast messages.

Use this page to schedule firmware upgrades FOTA and unicast or multicast messages for end devices. Both messages and upgrades can be scheduled for individual end devices or end device groups. This page allows you to view information about currently scheduled messages and firmware upgrades. You can also cancel scheduled upgrades and messages if the Conduit has not received the scheduled operation during check-in.

FOTA (FUOTA) Overview

This requires mDot firmware Version 3.1 or newer and a MTCDT, MTCDTIP, or MTCAP with AEP 1.6 or higher.

Firmware Over the Air (FOTA) also known as Firmware Upgrade Over the Air (FUOTA) is a way to upgrade end devices using multicast and file fragmentation packages defined in the LoRaWAN specification. FOTA allows the Conduit to update the firmware on many end devices at once using multicast and error correction packets. FOTA is still in its early stages of revision and does have potential problems, which are included in this topic.

FOTA Process

A FOTA session consists of three phases: session creation and setup, broadcast, and cleanup. LENS delivers the firmware to the gateway to distribute it to the end devices. When the operation is complete, the gateway reports the end device’s new firmware version back to LENS.

Session Creation and Setup (0 to 10% complete)

1. FOTA is scheduled in LENS.
2. The gateway checks in with LENS and receives the FOTA session.
3. When the gateway receives the session from LENS, it makes the session active. The gateway makes waits for the setup time to expire and makes the operation active.
4. The gateway contacts the selected end devices by queuing a session request.
5. When the end devices check in, they read the session request and negotiate a multicast session.

- Class A end devices read after an AT+SEND is processed.
- Class B and Class C end devices have a receive window.

6. End devices send session responses until the gateway acknowledges. AT+FOTA=3 is set to a countdown in seconds until the session launch time.
7. At launch time, (AT+FOTA=0) the end device switches to Class C mode.
8. The end device receives broadcast packets from the gateway

Broadcast (10 to 90% complete)

1. The gateway launch timer expires. At this point, the system assumes all devices have negotiated a Class C session.
2. The gateway broadcasts packets to the end devices.

- The gateway broadcasts parity fragments, which the end devices use to reconstruct missing packets.

Cleanup (90% to 100% complete)

1. The end device calculates CRC and sends a CRC message to the gateway.
2. The gateway verifies the CRC file and sends a reponse to the end device.
3. The end device reboots and flashes new firmware.
4. If the end device started as a Class A device, it returns to Class A mode.

FOTA Operation Timers

When the gateway checks into LENS, pending operations start the setup phase. The operation becomes active and the launch timer is started. Launch time is the scheduled time in LENS minus the gateway's check in time.

When the end device receives the setup request and response the launch time is set. LENS schedule time minus the end device setup time. (Viewed with AT+FOTA=3.)

Ensuring a Successful FOTA Update

- Schedule FOTA updates so that all the end devices can send data to the gateway and negotiate a multicast session. If an end device sends data once every four hours, the schedule time should be 8 hours.
- Setting the end device RX2 datarate to a higher value increases packet size, decreases the number of packets that need to be sent, and reduces the time on air. Note that higher RX2 datarates reduce the gateway's effective broadcast range. For example, RX2 data rate 13 –SF7 lower spread factor = shorter receive range and larger packet size.

Potential Problems

- If the mDot misses either setup message, the FOTA session will not be successful. The mDot attempts to receive both messages multiple times. If the mDot is unsuccessful, it resets the fragmentation sessions and multicast session.
- If the mDot does not receive a CRC response from the Conduit, it resets the fragmentation and multicast sessions and deletes the fragmentation file.
- The mDot can reset the multicast/fragmentation session at any time using AT+FOTA=2.
- When using AT+SLEEP, make sure to wake up the mDot before a scheduled FOTA session. Using AT+FOTA=3 will return the time in seconds before the FOTA session is scheduled to start.
- If AT+SLEEP is used during the FOTA session, the mDot will miss packets and the session will likely fail.
- The FOTA session sends down packets every 1.5 seconds (assuming no duty cycle) and parity packets every 3 seconds by default. For best results, Multitech recommends users suspend all normal mDot operations until the FOTA session is complete.

Operations Fields

Field	Description
Scheduled Time	Time the firmware upgrade or message is scheduled to occur.
Type	Either upgrade or message.
Description	Description of the upgrade or message, if one was entered with the upgrade or message was scheduled.
End Devices	Click **View** to see a list of end devices scheduled to receive the upgrade or message.

Field	Description
Status	Click a scheduled operation's Status for current status or completion percentage.
Payload	For a scheduled message, payload is the message. For a scheduled firmware upgrade, the payload is the firmware file.
Operation EUI	The EUI generated for the scheduled operation.

Scheduling a Firmware Upgrade

To schedule a firmware update for one or more end devices:

1. Click **Device > Operations** and click **SCHEDULE FIRMWARE UPGRADE.**
2. Select the firmware upgrade's binary file. For details, refer to Firmware Upgrade Fields.
3. Enter a description if desired.
4. Enter the date and time you want the firmware to be upgraded. For details, refer to Firmware Upgrade Fields
5. Select one or more groups from the End Device Groups drop-down list or one or more individual end devices. For details, refer to Firmware Upgrade Fields.
6. Click **SCHEDULE UPGRADE**.

Firmware Upgrade Fields

Field	Description
DROP FILE OR CLICK TO SELECT	Drag and drop the firmware upgrade binary file or click this field and select the upgrade file. Required.
Port	Enter a port number from 1 to 220.
Description	Firmware update description. Optional.
Date	Date to start the upgrade. Enter the date in YYY-MM-DD format or select a date on the calendar.
Time	Time to start the upgrade. Enter the time in HH:MM format, with the hours as a 24 hour clock or select the time from the clock. For example, to send a message at 10:30 pm, enter 22:30.
Target End Devices	
Send the message to an end device group or individually selected end devices.	
Group Selection	One or more groups of end devices scheduled to be upgraded. Click the End Device Groups field to open a drop down list. Click the check boxes for the groups you want to select. To make group changes, click **Manage groups**. Refer to End Device Groups
Select Individually	One or more end devices scheduled to be upgraded. Click the check boxes for the devices you want to select.

Scheduling a Multicast Message

To schedule a multicast message for end devices:

1. Go to **Device > Operations** and click **SCHEDULE MESSAGE.**
2. Enter the HEX string message. For details, refer to End Device Message Fields.
3. Enter a description if desired.
4. Enter the date and time you want the message to be sent. For details, refer to End Device Message Fields.
5. Select one or more groups from the End Device Groups drop-down list or one or more individual end devices. For details, refer to End Device Message Fields.
6. Click **SCHEDULE MESSAGE**.

End Device Message Fields

Field	Description
Message	Hex string message to be sent to the device. Required. Must contain an even number of characters, length from 0 to 484.
Port	Enter a port number, from 1 to 220.
Description	Message description. Optional.
Date	Date to send the message. Enter the date in YYY-MM-DD format or select a date on the calendar.
Time	Time to send the message. Enter the time in HH:MM format, with the hours as a 24 hour clock or select the time from the clock. For example, to send a message at 10:30 pm, enter 22:30.
Target End Devices	
Send the message to an end device group or individually selected end devices.	
Group Selection	One or more groups of end devices scheduled to receive the message. Click **End-Device Groups** field to open a drop-down list. Click the check boxes for the groups you want to select. To make group changes, click **Manage groups**. For details, go to Editing an End Device Group.
Selection Individually	One or more end devices scheduled to receive this message. Click the check boxes for the devices you want to select.

Canceling a Scheduled Operation

To delete a scheduled message:

1. Go to **Device > Operations**.
2. Highlight the message or firmware upgrade that you want to delete.
3. Click 🗑.
4. Confirm by clicking **DELETE**.

Chapter 10 – End Device Groups

Groups help you manage multiple end devices. You can schedule firmware upgrades or messages for groups of devices instead of selecting individual end devices. To access the groups page, go to **Device > Device Groups**.

The groups page shows existing groups including number of devices in the group.

Use this page to view or add groups.

Creating an End Device Group

To create an end device group:

1. Click **Device > Device Groups**.
2. Enter a group **Name**. Required.
3. Enter optional field settings as desired. The system automatically generates a multicast EUI if you do not enter one. Refer to Group Fields for details.
4. Click **CREATE.**

Group Fields

Field	Description
Name	Group name. Required
Multicast EUI	Group multicast EUI. Auto-generated if blank. This is a hexadecimal string, 16 characters long. Valid characters are 0-9, A-F, a-f. Case does not matter.
Channel	Group channel. Valid values are 1 through 4. Optional.

Adding End Devices to a Group

To add end devices to a group:

1. Go to **Device > Device Groups** and click the group you want to add end devices to.
2. Click **ADD END DEVICES**.
3. Click the check box for each end device you want included in the group.
4. Click **ADD TO GROUP**.

The devices appear on the **END DEVICES** tab.

Editing an End Device Group

To edit a group:

1. Go to **Device > Device Groups** and click the group you want to edit.
2. Click on a field to edit it and make desired changes.
3. To remove end devices from the group:
   a. Click the check boxes for each end device you want to remove from the group.

   b. Click **REMOVE FROM GROUP.**

4. To add a end devices to the group, refer to Adding End Devices to a Group

Changes are automatically saved.

Deleting an End Device Group

To delete a group:

1. Go to **Device** > **Device Groups** and click on the group you want to delete.
2. Click 🗑.
3. Confirm the deletion.

Chapter 11 – Importing Gateway and End Device Data

Uploading CSV Files

Follow these steps to upload CSV files to Gateways or End Devices.

1. Go to **Network > Gateways** or **Network > End Devices**, depending on where the CSV file must go.
2. Hover over ⋮ and then select ☁
3. To assign an application network to all the gateways or end devices in the CSV file, select an **Application Network** from the drop-down list.
4. *For end devices only.* To assign a device profile to all end devices in the CSV file, select a **Device Profile** from the drop-down list.
5. Click **DROP FILE OR CLICK TO SELECT.**
6. Select the CSV file to be uploaded, and click **Open**.
7. Review the results of the attempted upload.
   - Number of entries found in the file
   - Number of new entries created
   - Number of entries that failed to load
8. Review the additional information (if applicable) regarding the attempted upload.
   - If the file is formatted correctly, the new entries appear in the appropriate page along with the existing entries.
   - If the file is not in the correct format, an error message or messages appear below the file box.
   - If duplicate entries exist, the duplicate EUIs or GUIs appear below the file box.
9. Click **DONE** to exit.

Gateway CSV File Format

To import gateway information, use the following CSV format.

Note: Attribute fields, marked by brackets [ ], are optional.

```
GwEUI, UUID, SERIAL_NUMBER, [NAME], [LATITUDE], [LONGITUDE], [ALTITUDE]
```

End Device CSV File Format

To import end device information, use the following CSV format.

Note: Attribute fields, marked by brackets [ ], are optional.

```
DevEUI, APPKEY, SERIAL_NUMBER, PRODUCT_ID, HARDWARE_VERSION,
FIRMWARE_VERSION, [NAME],[APPLICATION NETWORK EUI]
```

Chapter 12 – Organization

The organization page allows users with Organization Administration rights to update their organization's information in the system.

Note: This page is visible only to those with access rights.

Organization Fields

Field	Description
Name	The organization's name.
Email	Email address for the organization's contact.
Address 1	Fields for entering the organization's address.
Address 2	
City	
State	
Postal Code	
URL	Organization's URL.
Device Management	When you enable Device Management, a Manage Devices link appears on the Organization page. To open DeviceHQ in a separate browser tab, click **Manage Devices**.
User Authentication	Move the slider right to enable two-factor authentication. When you enable user authentication, the system requires users to enter an authentication code from Google Authenticator.

MultiToken Licensing

To access the License page, click **User >License**.

This page is available to Organization Users.

About License Tokens

LENS has three types of tokens:

- **Host:** Licenses your Lens organization. Activated when the first user logs into LENS.
- **Service:** Licenses the user interface and API. Activated when the first user logs into LENS.
- **Gateway:** Licenses an individual gateway to store that gateway's data in LENS and join a node. Activated when the gateway checks into LENS. Each gateway requires a separate token.

Every LENS organization has one host token, one service token, and at least one gateway token. Tokens cannot be reassigned to another device or organization.

Note: When the Token License expires, it must be renewed; otherwise, you lose the abilities associated to the token type (host, service, gateway). LENS sends an email alert to remind users before a token expires.

Field	Description
Type	Indicates token type: host, service, or gateway.
API Code	Indicates a connection between LENS and the vault for syncing data. A value of 200 indicates a good connection. Other values indicate an error.
Enabled	Indicates if the token has been activated (true), expired (false) or license renewed again (true).
Entity Name	Describes the host name for host tokens, the organization name for service tokens, and the gateway name or serial number for gateway tokens.
Activation	Indicates if the token has been activated.
Days	Shows the length of the token license, 60 indicates an evaluation license. 365 indicates a full license.
Expiration	Date the token expires.
Expired On	If the token expired, shows the date the token expired.
Token ID	Used for licensing renewals and uniquely identifies the MultiToken.

Device Management

The Device Management feature allow you to launch DeviceHQ from the Organization page.

Enabling Device Management

To enable Device Management:

1. Go to **User > Organization.**
2. Slide the **Device Management** slider to the right.
3. Click 💾 or to undo the change, click ↶.

Launch DeviceHQ

When you enable Device Management, a Manage Devices link appears on the Organization page. To open DeviceHQ in a separate browser tab:

- Click **Manage Devices.**

To learn more about DeviceHQ, go to www.multitech.com/brands/devicehq/. For help using DeviceHQ, refer to that application's Help.

Revisions

Revisions pages show the audit trail for an individual entity.

For an overall audit trail for your organization, refer to Activity.

Revision Fields

Field	Description
When	Revision timestamp

Field	Description
Type	*Gateway only.* Indicates if the change was to the gateway or an application network asset.
Version	Count of edits to the item.
Action	Create if the item is new. Update if the item was edited.
By User	User who made the change. Some revisions are system revisions.
Change	Description of change.

Broadcast

Broadcast sends a message to all members of the organization.

1. Go to **User > Broadcast.**
2. Enter a Subject for the message.
3. To set the message as important, slide the Important slider to the right.
4. Enter the Message.
5. Click ➤

Broadcast Message History

Message history appear below the message form. This includes when the message was sent, the subject, level of importance, and message text. To expand the message, click the down arrow, ⌄.

Support

To access the Support page, click **User > Support.**

This page contains links for the help file, support portal, and developer resources. It also includes system version information.

Chapter 13 – User Accounts

Account Settings

To access your account settings, go to **User > Profile**.

The **Identity** field includes the user email and first and last name.

The **Permissions** field lists the role as a user. User roles include:

- **Admin:** Organization super-user, administrator who has full access within the organization
- **Manager:** User with access to manage application networks, gateways, and end devices within the organization
- **User:** User with read-only and restricted access to data within the organization

Editing User Account Settings

Follow these steps to edit your account settings.

1. Go to **User > Profile.**
2. Under Identity, click in the **First Name**, **Last Name**, or **Email** fields and make changes.

   Note: The **Permissions** field is view-only and cannot be edited.

3. To change your password:

   - Click in the **Current Password** field and enter the current password.
   - Click in the **New Password** field and enter the new password.

   Password Rules:

   - Must be 10 or more characters.
   - Must contain at least one lowercase letter (a-z), one uppercase letter (A-Z), one digit (0-9), and one special character.
   - If users make more than 5 bad login attempts, LENS locks them out for 30 minutes or until they respond to an unlock email sent to them.
   - Passwords expire after 90 days.
   - Passwords cannot be reused.

4. Click 💾 to save or ↶ to revert changes.

People

This page displays users on the system. The range of users listed depends on the user's access.

The following items are listed on the People page. Names, emails, and roles can be sorted in ascending or descending order.

- **First name:** User first name.
- **Last name:** User last name.
- **Email:** User email.

- **Role:** See Account Settings for a list of roles and their definitions.
- **Actions:** Includes the ability to edit ✎ or delete 🗑 the user.

Creating a User Account

Requires Organization Admin access rights. To add a user:

1. Go to **User > People** and click +
2. Enter the new user's email, first name, and last name.
3. Select the access rights level for this user from the Permission drop-down list. For details on access rights, refer to Account Settings.
4. Click **SAVE** to create the account or **CANCEL** to leave the form without creating the account.

Managing User Accounts

Only users with Organization Admin permission can edit or delete user accounts.

Edit a User Account

To edit a user's email, name, or permissions, or reset their password:

1. Click **User > People**.
2. Click ✎ for the account you want to edit. The icon appears when you highlight the account.
3. Make desired changes.
4. Click 💾 to save the changes, or click ↶ to discard the changes.

Delete a User Account

1. Click **User > People**.
2. Click 🗑 for the account you want to delete. The icon appears when you highlight the account.
3. Confirm the deletion.

Chapter 14 – Audit Activity

Organization Activity

The organization activity page shows the organization's change audit trail. The change audit system tracks login sessions and the creation, update, and deletion history for the following entities:

- Organization Profile
- User Profile
- Network Profile
- Device Profile
- Gateway
- Application Network

Each of these entities has its own audit record through **Revisions** tabs.

Sessions Audit Fields

Field	Description
Created	Timestamp when the user logged in, creating the session.
Updated	Timestamp of the user's most recent activity.
User	Name of the user who logged in.
Expires	When the user session will end due to inactivity. This is one hour after the most Updated timestamp.
Logout	Timestamp of user logout
Login IP Address	User's IP address

Create Audit Fields

Create shows the audit trail for newly created entities.

Field	Description
When	Timestamp of the creation.
Element	Type of entity that was created.
Entity	The specific entity that was created.
By User	User who added the entity.
Remote Address	The user's IP address.
Setup	Description of the addition.

Update Audit Fields

Update shows the audit trail for entities that were edited.

Fields	Description
When	Timestamp of the edit.
Element	Type of entity that was edited.
Entity	The specific entity that was edited.
By User	User who edited the entity. Some revisions are system revisions.
Remote Address	The user's IP address.
Change	Description of the change.

For more details, click the individual record.

Destroy Audit Fields

Destroy shows the deletion audit trail.

Field	Description
When	Timestamp of the deletion.
Version	Count of edits the item.
Element	Entity that was deleted.
By User	User who made the change.
Remote Address	The user's IP address.
Description	Description of change.

For more details, click the individual record.

15 – Glossary

Term	Definition
Application Client	Client instance running on a Conduit to forward end device data to the application server.
Application Network	A network of gateways and end devices that can be connected in order to report application data from deployed sensors. Gateways and end devices must be associated with the same application network.
Application Server	Resides on the Conduit.
Bandwidth	The difference between upper and lower frequencies in a continuous band of frequencies. Measured in hertz.
Change Audit System	Audit trail of user sessions and device additions, edits, and deletions.
Channel	Also communication channel. Here it refers to a logical connection over a multiplexed medium such as a radio channel in telecommunications and computer networking. A channel is used to convey an information signal, for example a digital bit stream, from one or several senders (or transmitters) to one or several receivers. A channel has a certain capacity for transmitting information, often measured by its bandwidth in Hz or its data rate in bits per second.
CRC	Cyclic redundancy check. Detects accidental changes to data.
dB	Decibel is a logarithmic unit used to measure ratios of power or intensity.
dBm	Sometimes dBmW (decibel-milliwatts), this is a measurement unit used to express the signal strength to power level ratio. Acceptable signal strengths.
End Devices	Sensors with radios reporting data via LoRa packets to a gateway. An end device must join a gateway before sending data. A session will last as long as the end device and gateway maintain the keys and counters associated with the session. If either side loses the session information, then a new join must be made. An end device can be joined to only one network server instance on a Conduit.
EUI	Extended Unique Identifier. All EUIs in this system consist of 16 hexadecimal characters.
FOTA	Firmware-Over-The-Air method of updating firmware on devices in the field. Also, FUOTA, firmware upgrade over the air.
Gateway	Conduit, Conduit AP, or Conduit IP67 hardware running network server and/or packet forwarder processes. Deployed in the network to receive packets from end devices.
Group	A collection of end devices.
Health Check	System that monitors join and uplink activity and reports device states.
Hexadecimal	A numbering system that uses 16 distinct symbols, using 0-9 to represent values up to 9 and a-f to represent 10-15.
Join Request	Transmission from an end device wanting to join a gateway before transmitting secure sensor data. Contains DevEUI, JoinEUI, Random Nonce, and MIC calculated using a pre-shared key known only to the end device and join server. On receipt, the gateway forwards packet contents to the join server for verification and valid response.

Term	Definition
Join Response	Transmission from the gateway in response to a validated join request. Contains DevAddr, NetID, Downlink settings and MIC. Packet is encrypted using the pre-shared key known only to the end device and join server. Only the intended end-device should be able to decrypt and use the join response.
Join Server (JS)	Authenticates join requests using the DevEUI and MIC from the join request and the pre-shared AppKey from the database.
MIC	Message Integrity Check.
multicast messages	Data package sent to multiple end devices at the same time.
NAC	Network Access Control. The center piece for enterprise integration. Integrates into enterprise authentication and user infrastructure. Provides policy control for managing all access points and edge nodes.
Network Server	Runs on a gateway and processes join requests directly or forwards requests to a remote join server. Responsible for maintaining session information for each joined end device. Authenticates packets received from joined end devices and forwards data to local applications.
Packet Forwarder	Process running on the gateway used to communicate with the LoRa radio card. A gateway can run a packet forwarder and send received packets to a remote or local network server.
Packet Metadata	Statistical information about received and sent packets such as: frequency, data rate, RSSI, SNR and various events occurring on Conduit network server instances.
Policy	Whitelist of end devices allowed to have their join request forwarded to the join server.
Profile	User-defined standard configurations that can be applied to multiple devices or application networks.
RSSI	Received Signal Strength Indicator is a measurement of how well your device receives a signal from an access point or router. It helps determine if the signal is strong enough for a good wireless connection.
SNR	Signal to Noise Ratio use to compare the desired signal level to the background noise level. A ratio higher than 1:1 (greater than 0 dB) indicates more signal than noise.
Spectral Imaging	Imaging the uses multiple bands across the electromagnetic spectrum. While an ordinary camera captures light across three wavelength bands in the visible spectrum, red, green, and blue (RGB), spectral imaging encompasses a wide variety of techniques that go beyond RGB. Spectral imaging may use the infrared, the visible spectrum, the ultraviolet, x-rays, or some combination of the above. It may include the acquisition of image data in visible and non-visible bands simultaneously, illumination from outside the visible range, or the use of optical filters to capture a specific spectral range. It is also possible to capture hundreds of wavelength bands for each pixel in an image.
UUID	Universal Unique Identifier.
unicast messages	Data package sent to a single end device.

Index