MultiTech Lens™ Datasheet

Embedded Network Server & Key Management Toolset for LoRaWAN® Networks

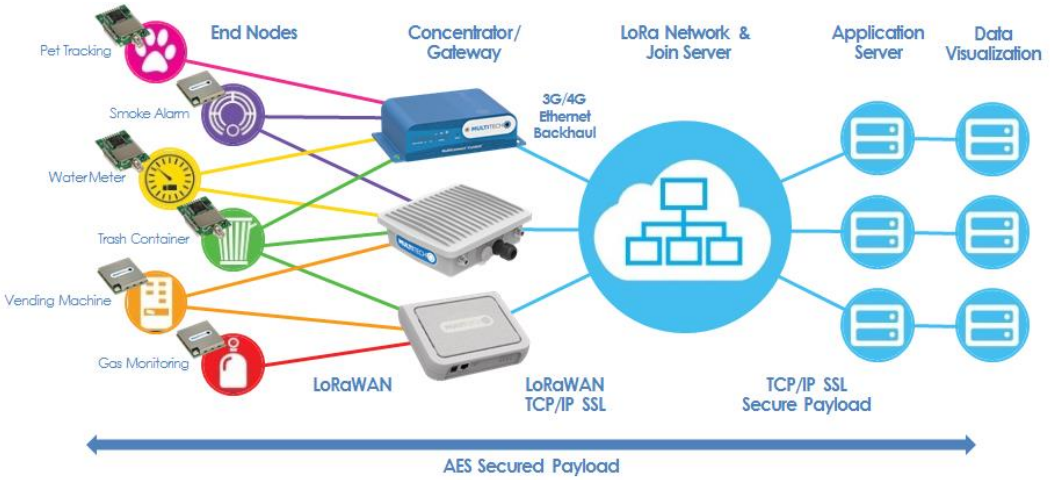
MultiTech introduces Lens™ – a hybrid LoRaWAN® network management platform that enables deployment and management of LoRaWAN networks at scale. Designed for private and enterprise networks, Lens provides a site-by-site user account and centralized management for LoRa® end devices, as well as configuration and control of Conduit® gateways. Lens has the capability to assign unique access rights to individual users, add gateways and LoRa end nodes in bulk, or create separate organizations and network segmentation to support different IoT use cases or applications.

Table of Contents

Lens Architecture

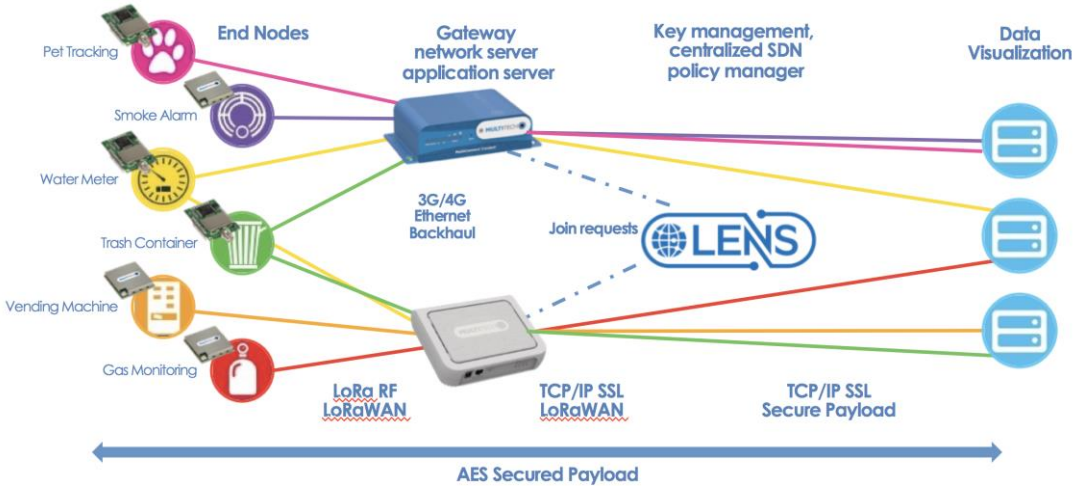
Traditional LoRaWAN Network Architecture

In traditional LoRaWAN networks, the network server, application server and join server are all located in the Cloud. The gateways are connected to this central network server, and applications subscribe or poll for messages from the server. All packets are sent to the gateways over the backhaul to the network server for authentication. Session information is not available at the gateway to allow filtering.



Lens LoRaWAN Network Architecture

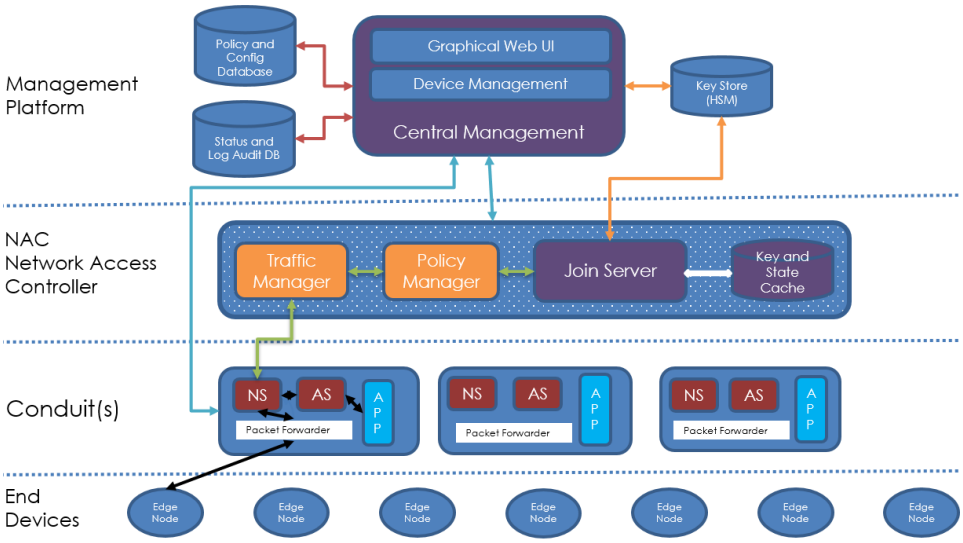
In a Lens LoRaWAN network, only the join server is located in the Cloud and each gateway is a network server. Having the network server on the gateway allows sensor data to be processed at the edge, without a round trip for packet filtering and decryption. You can configure a Conduit gateway to use Lens just for join requests, disabling packet data and statistics uploads to Lens to conserve backhaul data use.



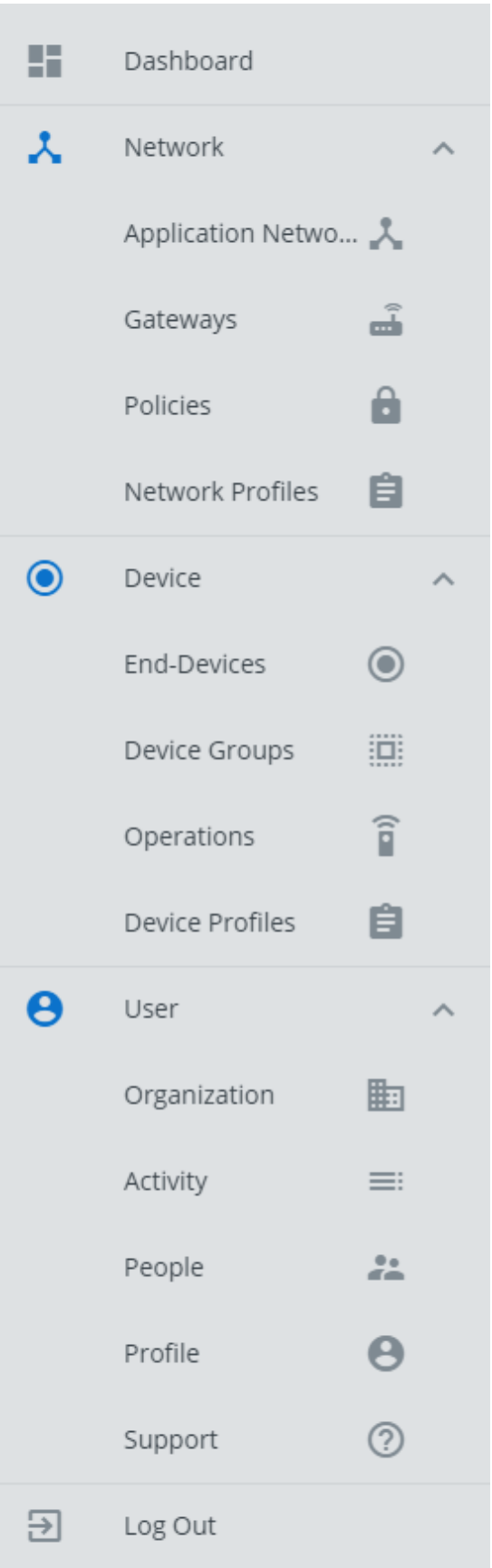
Lens Solution Architecture

Lens provides a gateway-hosted LoRaWAN network, join and application servers with the join server centralized in a private cloud instance, augmented with policy management, device management integration, and a web-based graphical user interface.

An end device can be joined to one gateway within an application network. Network signaling then happens between the end device and the gateway-hosted network server, and only pre-defined join requests are forwarded to the Cloud-hosted join server, thus minimizing backhaul traffic and managing network data at the network edge.



Lens Features & Functions



The Lens platform allows you to manage your LoRaWAN network components – **end devices**, **gateways** and **application networks** – and provides a variety of dashboard views at the network, organization, application, gateway or device. Network managers can see many different types of near real-time LoRaWAN network traffic information – packets, join requests, missed packets, and other information per hour/day/week by application network, gateway, or end point.

Main Features

- Lens supports segmenting multiple application use cases (e.g. mouse traps and cold storage monitoring) over your private LoRaWAN network
- Device Management provides the ability to remotely manage gateway configurations and applications
- White-listing capability provides complete control of traffic across your private LoRaWAN network
- Single point of control minimizes security risks
- Bulk uploading of gateways and end nodes allows rapid scale and easy management of your network
- Can be used worldwide with any LoRa-compatible end-device nodes

Change Audit System

The Change Audit system monitors the creation, updates, and deletions of the entities most closely related to the configuration and behavior of end devices and gateways. The audited changes capture which user performs the change and from what remote IP address. Each change will create a revision with a timestamp, version, action, user, and the changed fields. Certain fields are omitted from being audited, such as passwords and statistical information.

The following entities are audited:

- Organization profile
- User profile (including failed login attempts)
- Network profile
- Device profile
- End device
- Gateway
- Application network

Each of the entities will have a revision history. In addition, all entity changes can be viewed from the Organization – Update, Create, and Deletion tables. These are the entities associated with a given organization. Also, any user of an organization can view the actions of those users belonging to the same organization.

Health Check System

The Health Check system is a service on the Cloud that monitors the activity of joins and uplinks with respect to end devices, gateways, and application networks in order to give a high-level view of the state of the devices. Each application network will have an expected frequency of uplinks. When the Conduit gateway forwards uplinks for the joined end devices, then the end-device state becomes active and remains active as long as the uplinks come at an expected frequency. If the end-device state becomes active, but then the uplinks do not come as expected, then the state changes to inactive. The state of the end device is determined during the Health Check update.

The Health Check update is performed every four hours. The system first updates all end-device states, and then evaluates the gateway and application network states based on the updated end devices. The four hours provides an opportunity to evaluate the system; however, the Health Check fields that determine the status – such as the last join and last uplink – are updated as they occur.

Rules, Restrictions and Constraints

Single Tenant or Multi-Tenant

Single Tenant

Single tenancy means that a single instance of the software and all of the supporting infrastructure serves a single customer. With single tenancy, there is no sharing – each customer has their own independent database and instance of the software.

Multi-Tenant

Multi-tenancy means that a single instance of the software and all of the supporting infrastructure serves multiple customers. Each customer shares the software application and a single database. The data is tagged in the database as belonging to specific customers.

A Lens instance (or site) is either a single tenant or multi-tenant installation. It consists of a Lens back-end server, a configuration and system data database, a LoRa join server (Lens Network Admission Control join server) and a key database.

- The user interface (UI) browser URL domain is unique to a site
- Lens organizations do not have hierarchies. Multi-tenant sites simply have a list of organizations.
- A Lens user email address is unique to a site
- An end-device Extended Unique Identifier (EUI) is unique to a site
- A gateway EUI is unique to a site
- An end device belongs to one and only one application network
- A gateway may allow end devices from multiple application networks to join
- All Lens entities (end devices, gateways, application networks, users, device and network profiles and policies) belong to one and only one organization
- Users can only view the information associated with their one organization
- System Administrators can view the information associated with all the organizations in a multi-tenant site

Successful Lens Join Requirements

Lens Provisioning Requirements

- The end device must be provisioned in Lens
- The gateway must be provisioned in Lens
- The provisioned end device must be assigned to an application network
- The application network must belong to a provisioned gateway

Hardware / Firmware Settings and Requirements

- The end-device node must be in range of the Conduit gateway
- The Conduit gateway and end-device node must be able to communicate through a common frequency sub-band (FSB)
- The Conduit gateway LoRaWAN network setting and end-device node must have the same network mode (either "Public LoRaWAN" or "Private LoRaWAN")
- The Conduit gateway LoRaWAN network setting and end-device node must have the same join delay setting (e.g. 5 seconds)
- The Conduit gateway key management join server URL must be pointing to the Lens join server (Machine API path supporting LoRa backend interface)

Node Settings

- Set for OTA (Over-the-Air Activation – Note: Activation by Personalization (ABP) does not work with join server)
- Dev EUI must match provisioned end-device EUI (Otherwise the error Unknown DevEUI is generated for the join request)
- App key must match provisioned end-device app key (Otherwise the error MICFailed is generated for the join request)

Successful Lens Network, Statistics and Packets Requirements

- The Conduit gateway must be pointing to the Lens backend machine API path
- The "Enable Lens API" setting must be enabled
- The system time on the Conduit gateway must be within five minutes of the Lens backend server

Lens Timing Features

- The Conduit gateway polls the Lens database for configuration information, such as device and network profiles, through a gateway check-in. When a Lens user updates the configuration information, the Conduit gateway does not automatically get a push notification or update.
- A gateway check-in collects:
    - Traffic manager policies relevant to that gateway
    - Network profile settings relevant to that gateway
    - Device profile settings relevant to that gateway
    - Scheduled message and Firmware Over-The-Air (FUOTA) operations
- The Conduit gateway pushes network, statistics and packet data as they occur.
- Changing device and network profiles will not automatically update the Conduit gateway configuration – that will occur during the gateway check-in
- device and network profile information is obtained in two ways:

    - In a join response as VSExtension (Vendor Specific Extension) configuration information
    - During a Conduit gateway check-in
- Once the Conduit gateway network server has a valid join session, it is valid for the life of that session. Changing the Lens configuration (e.g. removing a provisioned end device) will not affect the Conduit gateway device session. Only subsequent re-joins from the Conduit gateway network server will rely on the current state of the Lens configuration.
- The Health Check system updates the status of each state entity every 4 hours.
- The Health Check state entity fields, used to determine the status, are updated as join requests and uplinks occur.

Gateway Map Viewing Requirements

Gateway maps may be viewed from the following UI locations:

1. Dashboard Map – shows all gateway locations with defined latitude/longitude for a given organization. At least one gateway must define a latitude/longitude for the dashboard to display the map.
2. Application Networks Dashboard – shows all gateway locations with defined latitude/longitude for a given application network.
3. Gateway Dashboard – shows a given gateway location with defined latitude/longitude.

In order for the gateway to appear in any map it must have a defined latitude/longitude.

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

Conduit Gateway Lens Compatibility

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
- Conduit AEP v5.0.x

System Administration

The System Administrator can optionally configure (or set):

- The **amount of time** to keep records for system records:
  - Join requests
  - Packets
  - Network statistics
- The **number of records** to keep for system records:
  - Join requests,
  - Packets
  - Network statistics
- The limit for number of provisioned end devices per organization (for evaluations)
- The limit for number of provisioned users per organization (for evaluations)
- The limit for number of provisioned gateways per organization (per contract or evaluation)

When end-device, user or gateway limits are reached, the Organization Administrator will get an email notification that a user of the organization has attempted to exceed the limit.

The System Administrator can send emails (or broadcasts) to all users of all organizations within the Lens instance.

The System Administrator is responsible for creating the organization(s) for single tenant or multi-tenant sites.

The System Administrator is responsible for inviting the Organization Administrators for each organization created in Lens. The Organization Administrators are able to extend invitations for their organization.

The System Administrator is responsible for enabling or disabling two-factor authentication per organization (the Organization Administrator may turn on/off this feature for their own organization – this setting will apply to all users when logging into the Lens system).

Security

LoRaWAN Security[1]

Mutual authentication

Mutual authentication is established between a LoRa end device and the LoRaWAN network as part of the network join procedure, proving that both have knowledge of the AppKey. This proof is made by computing an Advanced Encryption Standard – Cipher-based Message Authentication Code (AES-CMAC) using the AppKey on the device's join requests and by the backend receiver. Two session keys are derived, one for providing integrity protection and encryption of the LoRa Media Access Control (MAC) commands and application payload (the NwkSKey), and one for end-to-end encryption of application payload (the AppSKey). Keys are never shared over the air during onboarding - only the Effective User ID (EUID) and a random number are shared.

Integrity protection

Integrity protection is provided in two hops: one hop over the air through the integrity protection provided by the LoRaWAN network protocol and the other hop between the network and application server by using secure transport solutions such as Hypertext Transfer Protocol Secure (HTTPS) and virtual private networks.

Confidentiality

All LoRaWAN network traffic is protected using the two session keys. Each payload is encrypted by AES-Counter Mode (AES-CTR) and carries a frame counter (to avoid packet replay) and a Message Integrity Code (MIC) computed with AES-CMAC (to avoid packet tampering).

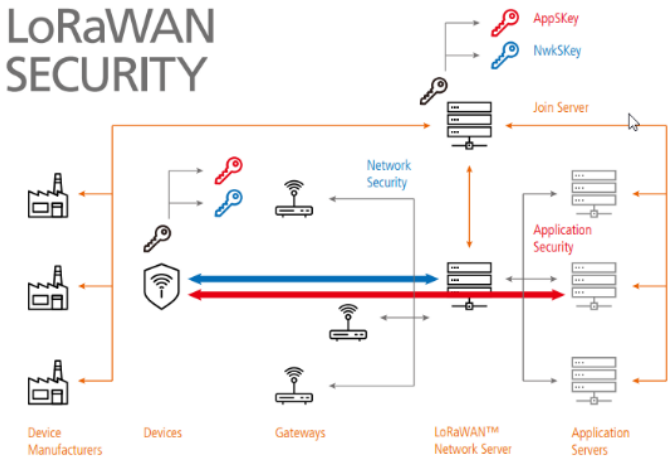
End-to-end encryption

End-to-end encryption is implemented for application payloads exchanged between the end devices and application servers. Lens encrypts all keys in flight and at rest.

AES cryptographic algorithms

Advanced Encryption Standard (AES) cryptographic algorithms are National Institute of Standards and Technology (NIST) approved and are used as a best security practice for constrained nodes and networks. Uses the AES cryptographic primitive combined with several modes of operation: CMAC for -bit AES key (called AppKey) and a globally integrity protection and CTR for encryption. Each LoRa device is personalized with a globally unique identifier (EUI-64-based DevEUI), both of which are used during the device authentication process.

[1] Excerpts from the LoRa Alliance website



Lens Additional Security

Traffic and Policy Management

Network managers can utilize features such as white-list management and set roaming parameters to obtain complete control over the amount, type and location of traffic running over their private network. This single point of control for join requests strengthens the security profile and reduces Wide Area Network backhaul costs.

User Login

Password complexity rules are enforced and password policies force password expiration and prevent re-use of passwords.

Two-Factor Authentication

Login requires two-factor authentication. The Transport Layer Security connections ensures that the link between the browser and the backend server is encrypted and has security. The password and two-factor authentication key can then be sent over this secure link.

Auditing Feature

The Change Audit system allows you to view user activity with regard to creating, updating, or deleting an organization profile, user profile (updates include failed login attempts), network profile, device profile, end device, gateway and application network. The Change Audit system captures what user performs the change, if performed from the UI, and from what remote IP address.

In-House Manufacturing

MultiTech has the ability to provision gateways and devices, which means the customer does not have to do their own key management.

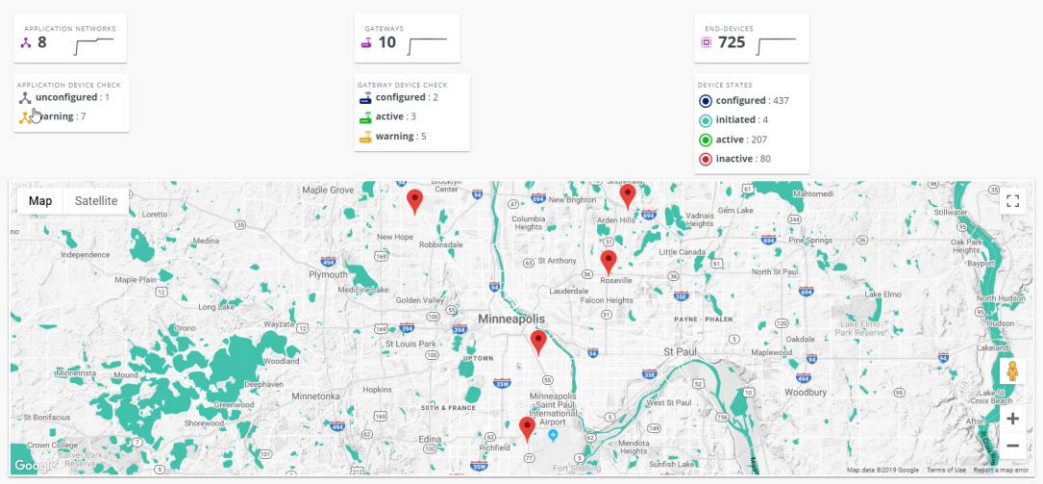
Dashboard – Lens Network Traffic Overview

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. The dashboard allows you to do the following:

- View LoRaWAN network traffic information – data packets, join requests, missed data packets, and cyclic redundancy check (CRC) error ratio per hour/day/week by application network, gateway, or end device
- Switch between multiple views: Organizational, application, gateway, end device

Gateway Map

This graph shows the location of each gateway that has latitude and longitude coordinates



Gateway Map Viewing Requirements

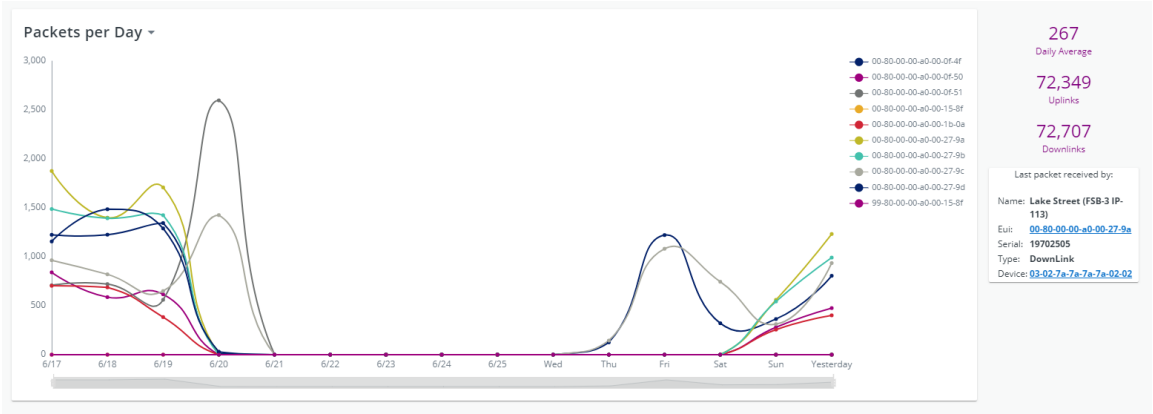
Gateway maps may be viewed from the following UI locations:

1. Dashboard Map – shows all gateway locations with defined latitude/longitude for a given organization. At least one gateway must define a latitude/longitude for the dashboard to display the map.
2. Application Networks Dashboard – shows all gateway locations with defined latitude/longitude for a given application network.
3. Gateway Dashboard – shows a given gateway location with defined latitude/longitude.

In order for the gateway to appear in any map it must have a defined latitude/longitude.

Packets per hour/day/week

This graph displays the number of packets received by each gateway over time. 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.

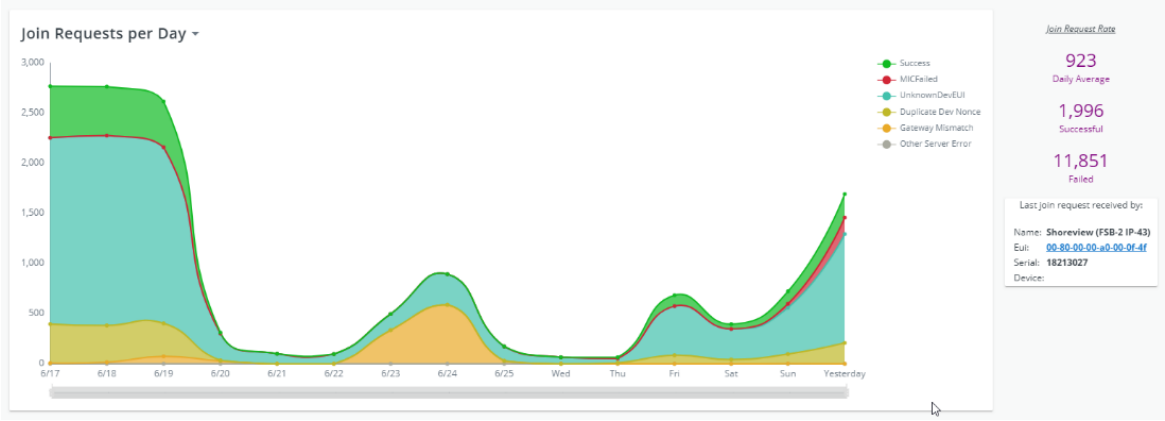


Successful Lens Network, Statistics, and Packets Requirements

- The Conduit gateway must be pointing to the Lens Backend Machine API path
- The "Enable Lens API" setting must be enabled
- The system time on the Conduit gateway must be within five minutes of the Lens backend server

Join Requests per hour/day/week

This graph displays the number of join requests received over time. 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.



Join Request Statuses

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 dev-nonce in LoRaWAN 1.0 end devices. Additionally, if an end device goes through two gateways with a common application network, only one gateway will get a successful join. The other gateway will receive a Duplicate Dev Nonce error.
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 requests.

Successful Lens Join Requirements

Lens Provisioning Requirements

- The end device must be provisioned in Lens
- The gateway must be provisioned in Lens
- The provisioned end device must be assigned to an application network
- The application network must belong to a provisioned gateway

Hardware / Firmware Settings and Requirements

- The end-device node must be in range of the Conduit gateway
- The Conduit gateway and end-device node must be able to communicate through a common FSB
- The Conduit gateway LoRaWAN Network Setting and end-device node must have the same network mode (either "Public LoRaWAN" or "Private LoRaWAN")

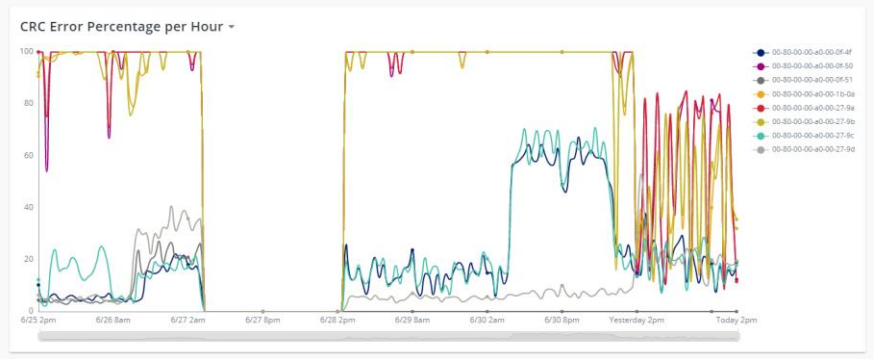
- The Conduit gateway LoRaWAN network setting and end-device node must have the same join delay setting (e.g. 5 seconds)
- The Conduit gateway key management join server URL must be pointing to the Lens join server (Machine API path supporting LoRa backend interface)

Node Settings

- Set for OTA (Over-the-Air activation – Note: Activation by Personalization (ABP) does not work with join server)
- Dev EUI must match provisioned end-device EUI (Otherwise the error Unknown DevEUI is generated for the join request)
- App key must match provisioned end-device app key (Otherwise the error MICFailed is generated for the join request)

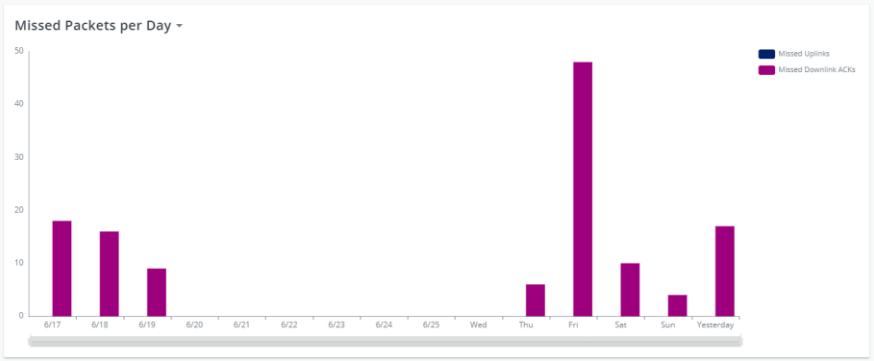
CRC Error Percentage per hour/day/week

This graph displays the number of packets received with failed CRCs 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 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 rates per hour, day or week. Data also includes the gateway with the highest CRC error percentage.



Missed Packets per hour/day/week

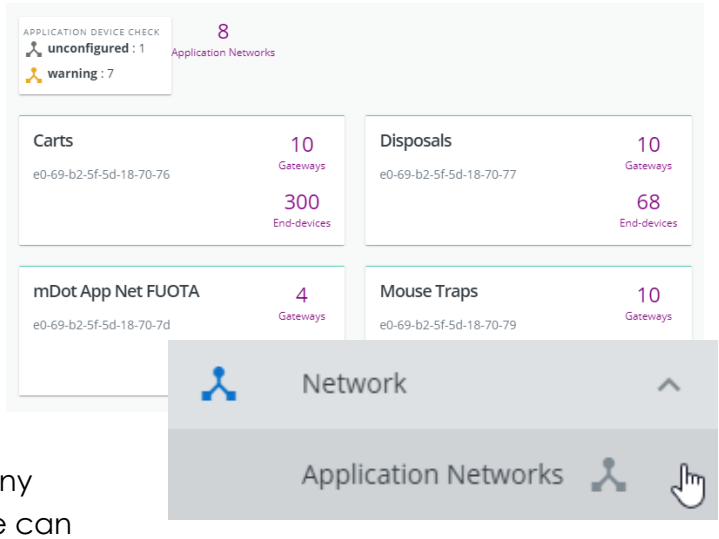
This graph includes missed uplinks (the number of uplink packets not received by the network server) and missed downlink acknowledgements (incremented for each confirmed uplink retry received by the network server, this indicates the number of downlink packets not received by the end device). Statistics accompanying the chart include packet uplink and downlink averages per hour, day or week and counts of missed uplinks and downlinks.


Missed Packets per Day
Missed Uplinks
Missed Downlink ACKs
50
40
30
20
10
0
6/17
6/18
6/19
6/20
6/21
6/22
6/23
6/24
6/25
Wed
Thu
Fri
Sat
Sun
Yesterday

Network

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. This allows segmentation of a set of gateways and end devices. User actions are recorded in a revisions table, which updates the Change Audit system.



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 the gateway. A gateway can belong to many application networks, but an end device can belong to only one application network.

Rules, Restrictions and Constraints

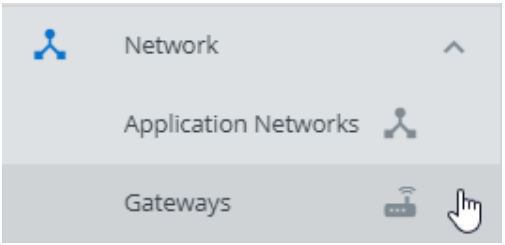
- An application network belongs to one and only one organization
- Join Requirements:
    - The application network must belong to a gateway that is in range of the end-device node
    - An end device must belong to the application network

Health Check States

The application network state indicates whether end devices have joined through the application network or not. If end devices have joined through the application network, then the application network state is derived from the end-device states.

- **Unconfigured –** The application network is provisioned, but no end devices belong to this application network, nor is the application network assigned to any gateway

- **Configured –** The application network has been assigned to at least one provisioned end device and belongs to at least one gateway, but no end devices have successfully joined through this application network



- **Initiated –** The application network had one or more end devices that joined through this application network that were set to initiated during the Health Check update
- **Active –** The application network had at least one active end device that joined through this application network during the Health Check update (there may be initiated end devices as well, but at least one active)
- **Warning –** The application network has at least one inactive end device

Health Check Fields

- **Application Network EUI –** The EUI for the provisioned application network
- **Status –** One of the application network Health Check states determined during a Health Check update
- **Last Status Update –** Timestamp for when the state changed
- **Expected Uplink Frequency –** The frequency (in hours) that the end devices for this application network are expected to send uplinks. This will determine if the end device is active or inactive during the Health Check update.

Gateways

A Conduit gateway reports received LoRa join requests to Lens. Any user actions are recorded in a revisions table, which updates the Change Audit system.

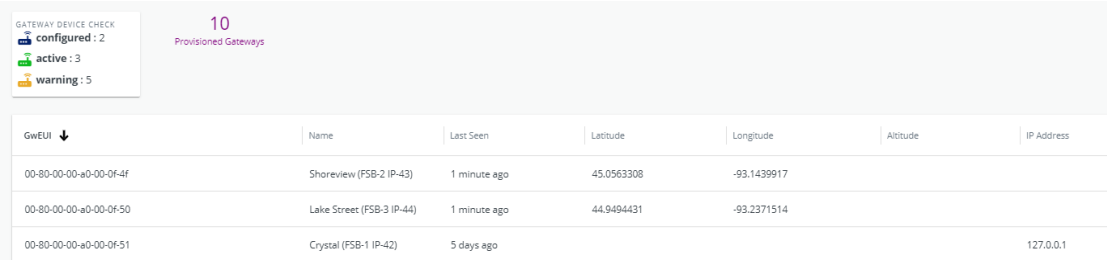
Gateway Check-Ins:

- Periodically collect traffic manager policies, network profiles, device profiles and operation requests (FUOTA and messages)

Rules, Restrictions and Constraints

- A gateway EUI is unique to a site
- A gateway may allow end devices from multiple application networks to join
- A gateway belongs to one and only one organization
- The Conduit gateway LoRaWAN network setting and end-device node must have the same network mode (either “Public LoRaWAN” or “Private LoRaWAN”)

- The Conduit gateway LoRaWAN network setting and end-device node must have the same join delay setting (e.g. 5 seconds)
- Defining the check-in interval requires Conduit AEP v1.6.2 or higher
- Join Requirements:
    - The gateway must be provisioned in Lens
    - The gateway and end device must be able to communicate through a common FSB



Health Check States

The gateway state indicates whether end devices have joined through the gateway or not. If end devices have joined, then the gateway state is derived from the end-device states.

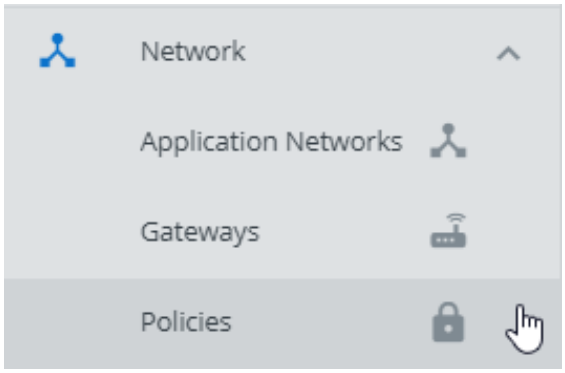
- **Unconfigured –** The gateway is provisioned, but does not belong to any application networks
- **Configured –** The gateway is provisioned and assigned to at least one application network, but no end devices have joined through this gateway
- **Initiated –** The gateway had one or more end devices that joined through this gateway that were set to initiated during the Health Check update
- **Active –** The gateway had at least one active end device that joined through this gateway during the Health Check update (there may be initiated end devices as well, but at least one active)
- **Warning –** The gateway has at least one inactive end device that joined through this gateway during the Health Check update (there may be initiated and active end devices as well, but at least one inactive)

Health Check Fields

- **Gateway EUI –** The EUI identifying the provisioned gateway
- **Status –** One of the gateway Health Check states determined during a Health Check update
- **Last Request –** Timestamp for last join request, regardless of status, coming through this gateway

- **Last Uplink –** Timestamp for last uplink packet coming through this gateway
- **Last Status Update –** Timestamp for when the state changed
- **Last Checkin –** Timestamp for when the last check-in occurred for this gateway
- **Next Checkin** – Timestamp for when the next check-in is expected. This field is based on Conduit gateway Lens server check-in API, if provided. If not provided, then 1 hour is assumed (requires Conduit AEP v1.7.4 or higher)

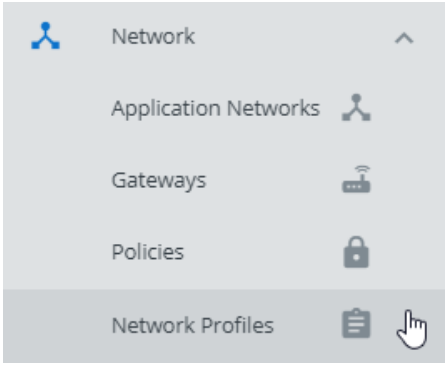
Policies



Gateways may receive join 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 enforced in the gateway-hosted network server, and are whitelists of end devices allowed to have their join requests forwarded to the Cloud-hosted join server. A policy manages associations between many end devices and an application network, an application network and many gateways, and many application networks and a gateway. A policy belongs to one and only one organization. Policies become available to the gateway when it checks in. Each gateway associated with a policy enforces the policy.

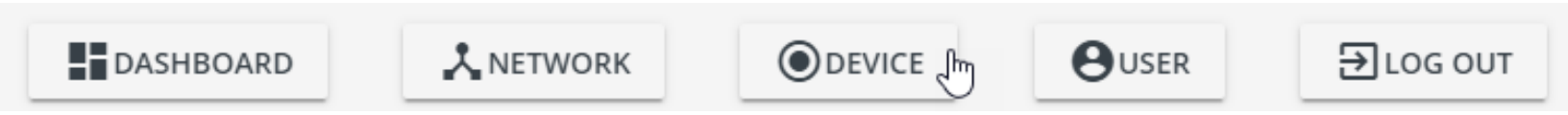
- Add end devices to the whitelist by selecting device groups and/or application networks
- Also add end devices to the whitelist by creating customer filters for specific device EUIs, device EUI ranges, join EUIs, or join EUI ranges
- When you set up a policy, you can apply the policy to selected individual gateways and/or to all the gateways associated with selected application networks
- The gateway does not forward join requests to the Cloud unless the filter criteria is met (if no policy for a gateway is defined, then all join requests are forwarded)
- Management of traffic manager policies requires Conduit AEP v1.6.2 or higher

Network Profiles



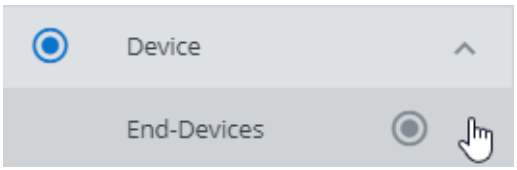
A network profile provides desired end-device settings (may apply to an application network or a specific end device) and support gateway deployment. When an end device first joins the network, it receives any default network profile settings via MAC commands. Any changes to the default settings are then sent to the end device in successive MAC commands until all settings have been relayed. Changes are also recorded in a revisions table, which updates the Change Audit system. Network profile settings override end-device profile and network settings. For example, the network profile is used to indicate an end device is operating in Class A, B, or C (the default is Class A). A network profile belongs to one and only one organization.

- Lens profiles do not overwrite profiles on the Conduit gateway; however, only the Lens profiles are used
- If there are conflicts between end-device profile settings and application network profile settings, the application network profile setting is applied
- Network profile settings are provided to the Conduit gateway in the join accept message and are collected during gateway check-ins
- Management of network profiles requires Conduit AEP v1.6.2 or higher



Device

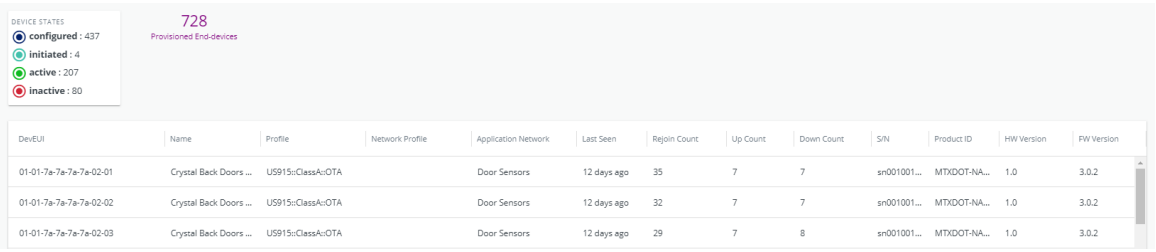
End-Devices



An end device is a sensor (also called an end-device node) 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, and may be assigned to a network profile or a device profile. Any user actions are recorded in a revisions table, which updates the Change Audit system.

Rules, Restrictions and Constraints

- An end-device EUI is unique to a site
- An end device belongs to one and only one application network
- An end device belongs to one and only one organization
- Join Requirements:
    - The end device must be provisioned in Lens
    - The end device must be assigned to an application network



Health Check States

- **Unconfigured –** The end device is provisioned, but is not assigned to an application network. In this case there is no way for the end device to join a network.
- **Configured –** The end device is provisioned and assigned to an application network, but has not joined a network.

- **Initiated –** The end device has joined the network, but there is no record of an uplink. If the end device becomes active/inactive and then rejoins, the state returns to initiated.
- **Active –** The end device becomes active when the first uplink for a join is received. The end device remains active as long as the uplinks occur at an expected frequency.
- **Inactive –** The end device becomes inactive when the uplink does not occur at an expected frequency.

Health Check Fields

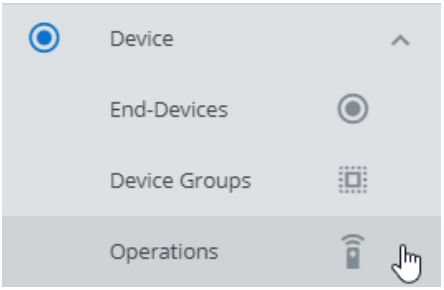
- **End-Device EUI –** The EUI identifying the provisioned end device
- **Status –** An end-device Health Check state determined during a Health Check update
- **Last Join –** Timestamp for when the last successful join occurred for this end device
- **Last Uplink –** Timestamp for when the last uplink for this join occurred. This field will be reset upon rejoins
- **Last Status Update –** Timestamp for when the state changed
- **Joined Application Network –** The application network that the end device joined through
- **Joined Gateway** – The gateway that the end device joined through
- **Join EUI –** The join EUI of the successful join request

Device Groups

Device groups help you manage multiple end devices. You can schedule firmware upgrades or messages for groups of devices instead of selecting individual devices.

- A collection of end devices with a channel ranging from 1-4
- May be used for traffic manager filtering, FUOTA firmware upgrades, or messages
- Requires Conduit AEP v1.6.2 or higher

Operations

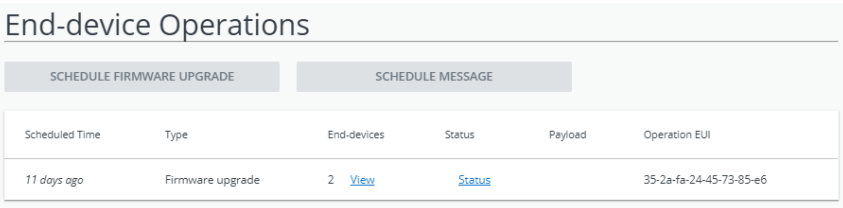


Operations allows you to schedule FUOTA firmware upgrades or messages for end devices or view information about currently scheduled messages and firmware upgrades. Both messages and upgrades can be scheduled for individual end devices or groups. You can also cancel scheduled upgrades and messages.

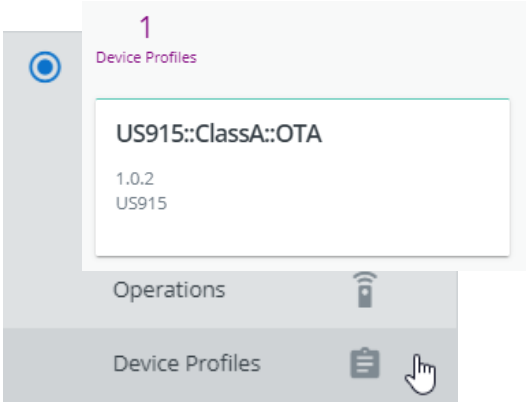
Conduit gateway check-ins enable this process. Every time a gateway checks in it collects scheduled operations and messages. Once the gateway has successfully gathered FUOTA and messaging operations, it performs these operations locally, according to a schedule. The status of the operation is reported periodically to Lens.

Rules, Restrictions and Constraints

- 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



Device Profiles



A device profile provides default settings the end device is expected to be using when it is joined to the network and supports end-device deployment. If the end device does not match these settings, communication with the end device may not be possible. Use end-device profiles to create and apply the same configuration to multiple end devices. A device profile belongs to one and only one organization. Any user actions are recorded in a revisions table, which updates the Change Audit system.

- Lens profiles do not overwrite profiles on the Conduit gateway; however, only the Lens profiles are used
- If there are conflicts between end-device profile settings and application network profile settings, the application network profile setting is applied
- Device profile settings are provided to the Conduit gateway in the join accept message and are collected during gateway check-ins
- Management of device profiles requires Conduit AEP v1.6.2 or higher

User

Lens is a **single user network**, as Lens has no mechanism for separating multiple users' datasets – thus suitable for private networks and enterprises but not for public operators.

Rules, Restrictions and Constraints

Every time a user logs into Lens, a session is created, which will expire after a certain amount of time. These login sessions can be seen from the Activity – Session screen. Any modification to an element monitored by the Change Audit system will be captured during the login sessions and can be viewed from the User Actions option (or from the Activity – Update/Create/Destroy screens, or from the Change Audit element revisions table). Users belong to one and only one organization.

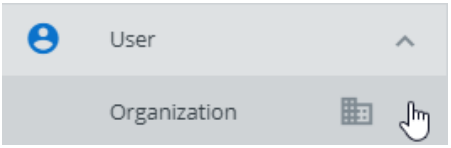
A successful login adheres to the following password constraints:

1. User passwords must be greater than or equal to 10 characters in length
2. User passwords must contain at least one special character, one digit and one capital letter
3. Users will be locked out of their account for 30 minutes, or until they respond to an unlock email sent to them, if they make more than five bad login attempts
4. Password expiration after 90 days
5. Prevents re-use of passwords

An email notification will be sent out to the user when:

- Password changes
- Email address changes
- Account (user) is locked out
- Password request is sent

Organization



Lens has multi-tenant features, which means that a Lens instance may be owned and maintained by a particular business that maintains their organization. Any actions are recorded in a revisions table, which updates the Change Audit system. Each entity belongs to one and only one organization, and all entities are visible only to the users of an organization (except system-related users). Each organization may have many of the following entities:

- End devices, gateways, and application networks
- Organization Admins, Organization Managers, and Organization Read-Only Users
- Policies, device profiles, network profiles

Organization Roles

Organizations have no hierarchies. When multiple organizations are created for a multi-tenant site, it is simply created as a list of organizations without additional organizational structure. There are no departments or sub-divisions within an organization.

Organization Administrator

- Invite additional users to the organization
- Change role of users for the organization
- Reset authentication for users
- Adjust Device Expected Uplink Frequency for a given application network state
- Enable or disable two-factor authentication for the organization (once allowed by System Admin for the organization)
- Receive email notifications if a user attempts to exceed set limits (if any) for end devices, gateways, or users. These settings will vary based on contracts and trial evaluations.
- Has all the capabilities of an Organization Manager

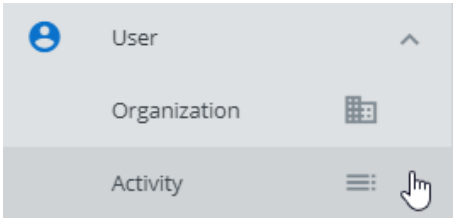
Organization Manager

- Create application networks
- Provision end devices
- Provision gateways
- Create device & network profiles
- Create traffic manager policies
- Create device groups
- Schedule FUOTA

Organization Basic User

- Can view, but not modify any entity created for the organization
- Cannot view traffic manager policies
- Can view session logins and Change Audit system changes

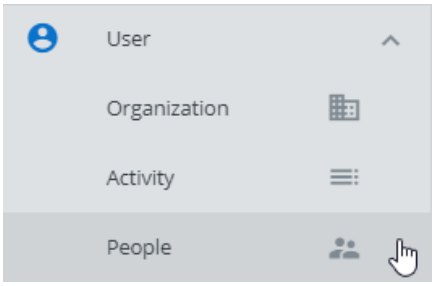
Activity



Every time a user logs into Lens they create a new user login session. This allows you to track the activities users perform during their login sessions. Different types of login information can be accessed based on the action the user has taken: Update, Create or Destroy, and the Change Audit system ensures that any activity is recorded. The following information is included in sessions:

- Created (the time at which the session was created – on the Create tab, also view the element, entity, user, remote address, and setup)
- Updated (the time at which the user last made an update – on the Update tab, also view the version, element, entity, user, remote address, and change)
- User (first and last names of the user)
- Expires (the time at which the session expires)
- Logout (when the user logs out – blank if they are still logged in)
- Login IP Address (IP address from which the user logged on)

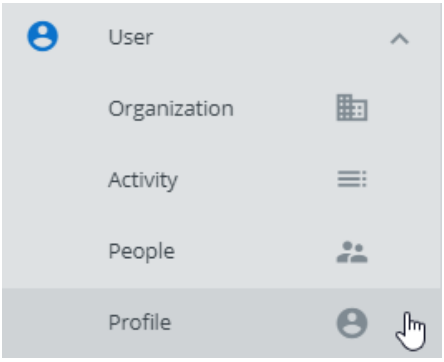
People



The people section displays users on the system; the range of users listed depends on the user's access. The following items are listed under People (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 (user roles include: Organization Admin, Organization Manager, User)
- Actions (depending on the user role):
    - **Profile Revisions** – provides Change Audit revisions of the user profile, including failed login attempts
    - **User Actions** – provides a list of user actions resulting in Change Audit revisions of end devices, gateways, application networks, etc.
    - **Edit** – modify the user name, email address, or password
    - **Delete** – remove the user account from the Lens system

User Profile

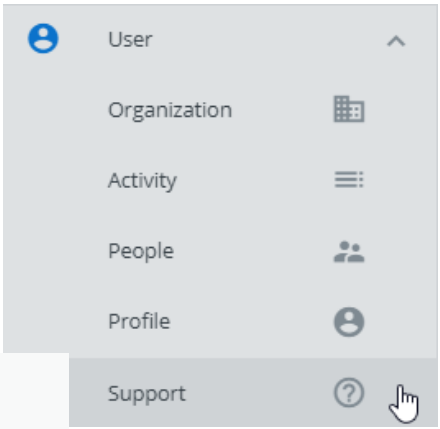


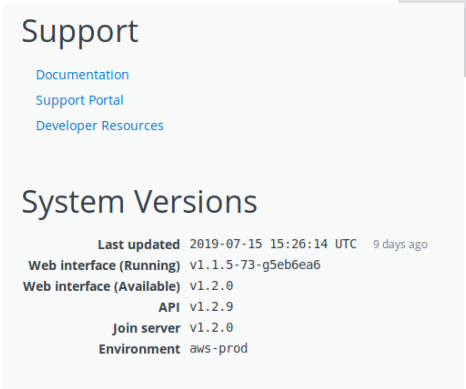
The Identity field includes the user email (unique to a site) and first and last name. The Permissions field lists the role as a user. User roles include: Organization Admin, Organization Manager, and User. Change Password field allows the user to modify their current password. A user belongs to one and only one organization. Changes are recorded in a revisions table, which updates the Change Audit system.

Support

Lens Support

Provides further resources for the user – including documentation (all Lens-related documents), a support portal (questions handled directly by the MultiTech team), and developer resources. System version information is also provided (when the program was last updated, the Web interface (Running), the Web interface (Available), API, the join server, and the environment).





MultiTech Support

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 www.multitech.com/warranty.go. 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

Produced in the U.S. of U.S. and non-U.S. components. Features and specifications are subject to change without notice.

2019-09 • 86002224 • © 2019 Multi-Tech Systems, Inc. All rights reserved.