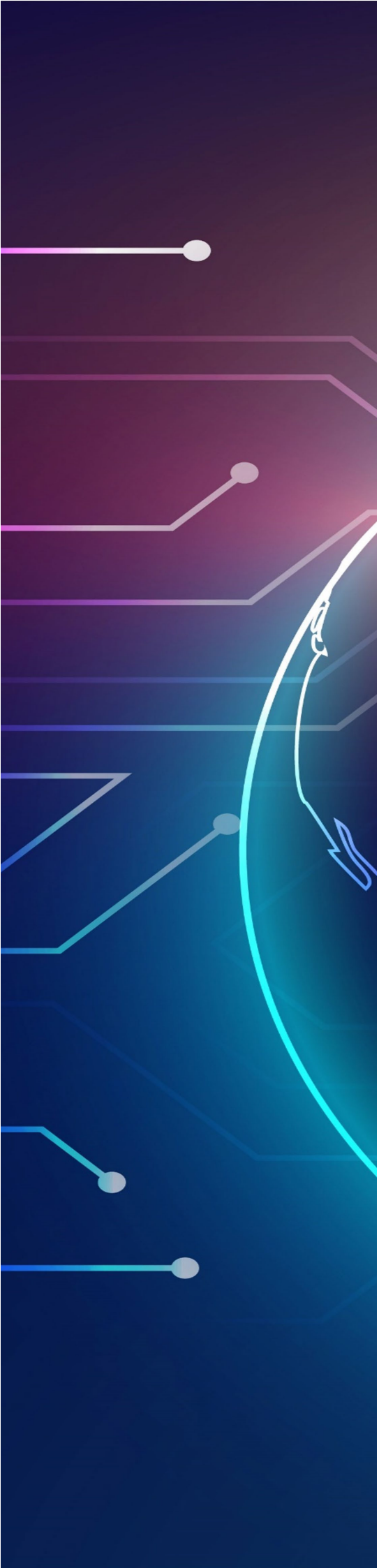


D-Link

Cloud Management Service

User Manual

D-ECS cloud

V1.60

Table of Contents

Introduction

D-ECS is a cloud management platform that removes the cost and complexity associated with owning and maintaining your corporate's network infrastructure. The platform is maintained by D-Link and access to D-ECS is through a web browser. D-ECS is a subscription-based service, and devices managed by the platform are individually licensed, allowing the system to scale with the requirements of an organization. Users can deploy, monitor, and configure their network devices imported to D-ECS. And for non-D-Link devices, you can obtain basic device information and monitor device status. Your organization's devices can also be grouped by their physical location into sites and can be configured for scheduled tasks. Users are granted privileges to access D-ECS based on roles, which restricts access to only functions that are permitted. D-ECS simplifies the management of your network and assets, reducing the workload of operation maintenance for network administrators by allowing large numbers of devices to be managed from a single interface. Devices can be pre-configured and delivered later to the designated organization, allowing network devices to be installed on site without requiring specialized IT knowledge. This streamlines installation and provisioning, which makes D-ECS an ideal solution for expanding and managing your new or existing network and further reducing management complexity of the network equipment in your organization. For example, when there are changes in device configuration or firmware, these changes can be pushed to the device via scheduled tasks. If a device is offline, it will try to connect to the D-ECS cloud continually until the connectivity is recovered. Once the device comes online, it automatically updates with the most recent configuration changes from D-ECS. Furthermore, administrators can rest assured that they will be notified instantly via email when a device's status changes.

Terms and Concepts

This section provides a brief introduction and description of the terms and concepts used in the system.

Organization Business Unit (OBU): An OBU is a separate division or a branch office of a corporate in other regions. It sells network devices such as LTE and 5G devices along with D-ECS to customers and is responsible for providing the initial administrative accounts (through invitation) and provisioning devices and licenses to the subscribed service providers.

Service Provider (SP): A service provider is an entity that sells network devices and D-ECS to customers and is responsible for providing the initial administrative accounts (through invitation) and provisioning devices and licenses to the subscribed organizations. Within the D-ECS structure, service providers are considered clients of an OBU. A service provider has the option to take over the task of maintenance of an organization along with its devices when creating an organization. Examples of service providers include telco companies and systems integrators (SI).

Organization (ORG): An organization is a business entity that subscribes to D-ECS through an SP. An organization cannot manage other organizations since all organizations belong to the same level of the D-ECS hierarchy. Within the D-ECS structure, organizations are considered clients of an SP. Examples of organizations include enterprises and business firms.

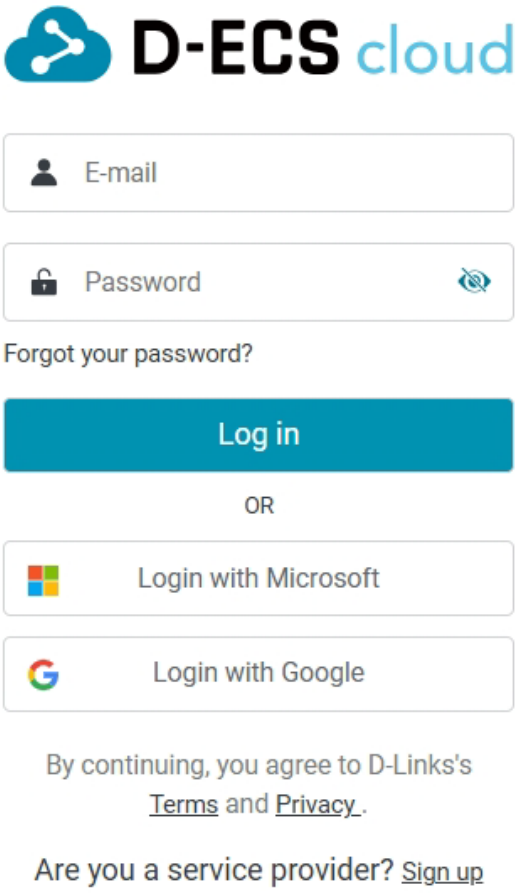
Site: A site is a label representing a physical location. Sites are used to group devices together for easier management. Sites should contain exact location information including countries, cities, districts, and street address. The D-ECS structure uses regions, sites, and groups for device management according to their physical placement with the hierarchical order of **regions** > **sites** > **groups**. (Refer to **Organization** for more information.)

The D-ECS Management Interface

The D-ECS management service is cloud based and can be accessed through a web interface with a valid username and password.

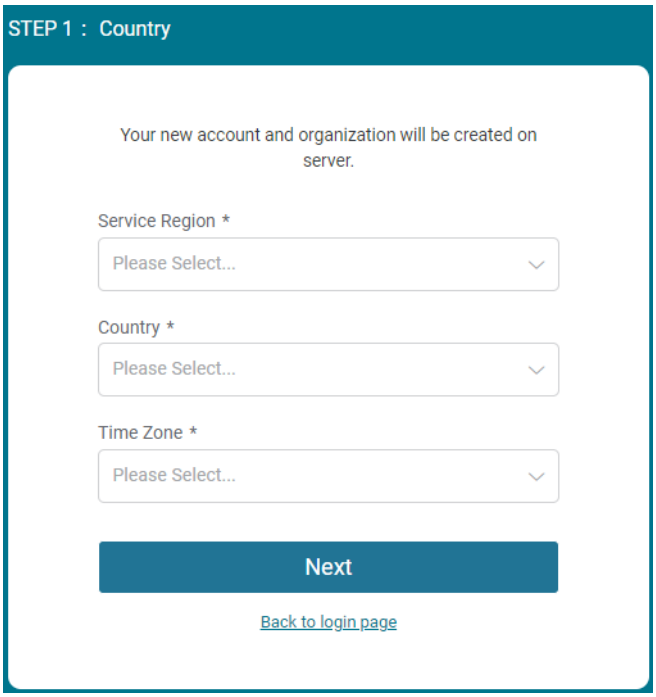
To log in to the D-ECS Management Interface:

1. Enter the URL: https://portal.decs.dlink.com/login

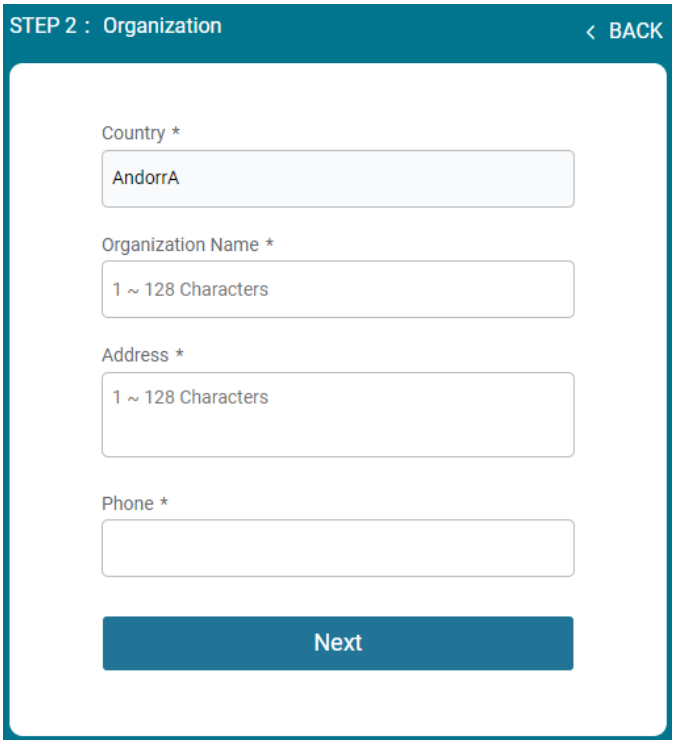


2. Enter a valid email and password at the login page. A valid account should be activated through email invitation. The activation process requires you to set a password with at least 8 characters and should contain at least one lower and upper case letter, one number, and one symbol such as !, @, #, $, %, ^, &, *, (,), _, +, -, =, [,], {, }, and |.
3. Alternatively, select **Login with Google** or **Login with Microsoft** to use your Google or Microsoft account if you have created an account with either of these services.
   The Login page also provides a Sign up page for service providers to sign up an account. Go through the sign-up process by filling in the following information:

- Service region information: Enter region, country, and time zone.

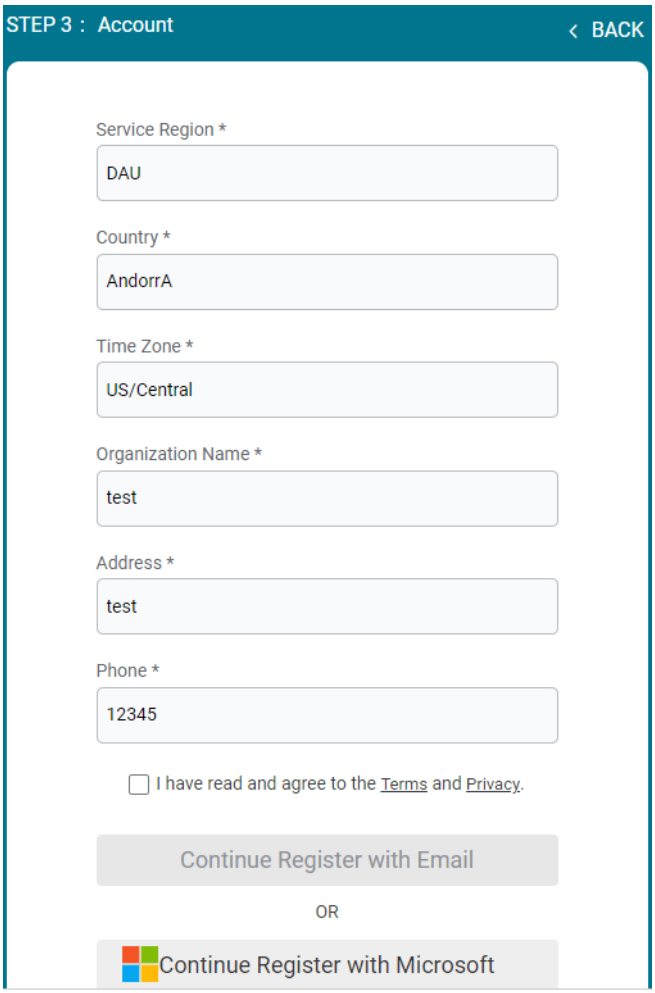


- Business organization information: Enter country, organization name, location address, and phone number.

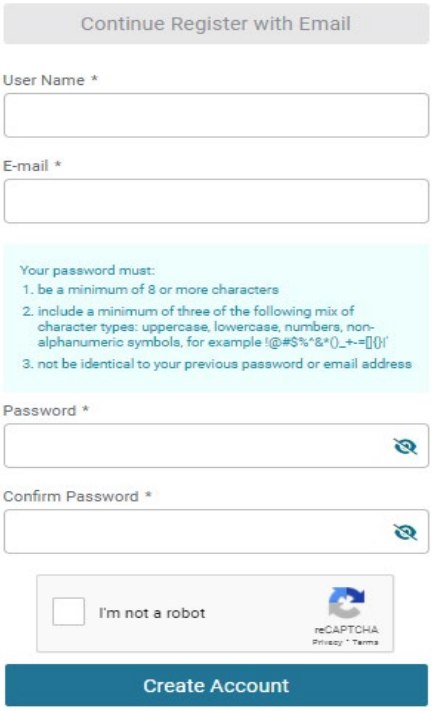


- Account information summary: Verify your account information and agree to the **Terms** and **Privacy.** Click one of the following registration methods to continue:

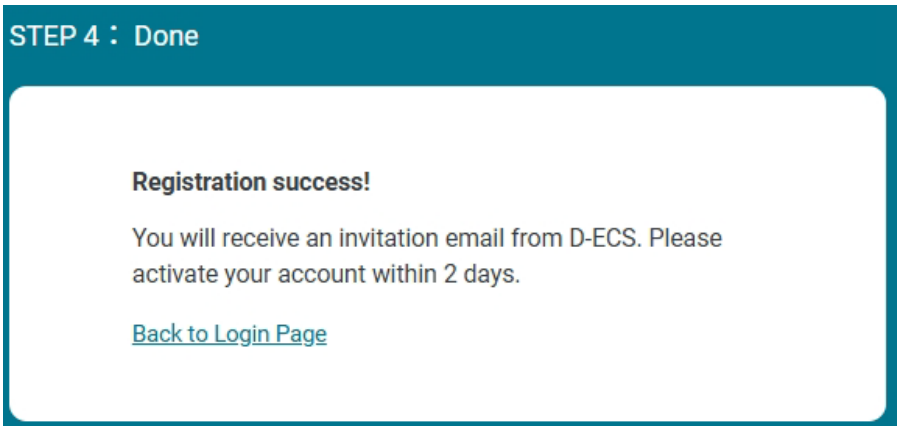
Continue Register with Email, **Continue Register with Microsoft**, or **Continue Register with Google**.



- If you choose **Continue Register with Email**, please create your account. Enter the username and email for the account. Also enter the password and confirm it.



- The Registration success screen will be displayed.



You will be notified by an invitation email. Please follow the instructions in the email to activate your account.

Dashboard

Devices continuously communicate status and network usage information back to the D-ECS cloud. Dashboard analytics are presented based on this information using graphs and charts and are updated regularly in the servers of the D-ECS cloud.

The Dashboard page is the first page after you log in to the management interface. This page provides a snapshot of device status and license information. The **Device Summary** displays the number of online and offline devices, inactive devices (i.e. service has been stopped, with expired licenses, or broken), and devices on the inventory. The **License Summary** (only available for an OBU and a service provider) displays the number of activated and expired licenses, as well as licenses that are available. The **Device Profile** gives the distribution of devices with respect to networking type or technology. The **My Staff Summary** (only available for a service provider) gives a summary of the registered users and their account types. The **Organization Account Summary** displays the names of organizations that are managed by the service provider (SP) (i.e. the service provider provides overall management service for the organization) along with the number of authorized users for management (refer to **List** of **Organization** for more information).

Note: The **Organization Account Summary** will not show any data if there are no organizations whose device and organization management tasks have been taken over by their service provider.

The table beneath the statistics provides the number of devices for each organization (or service provider depending on the user account) and links to the **Device Management**. You can click on an organization to go to the Device Management page to view detailed device information about devices belonging to the respective organization.

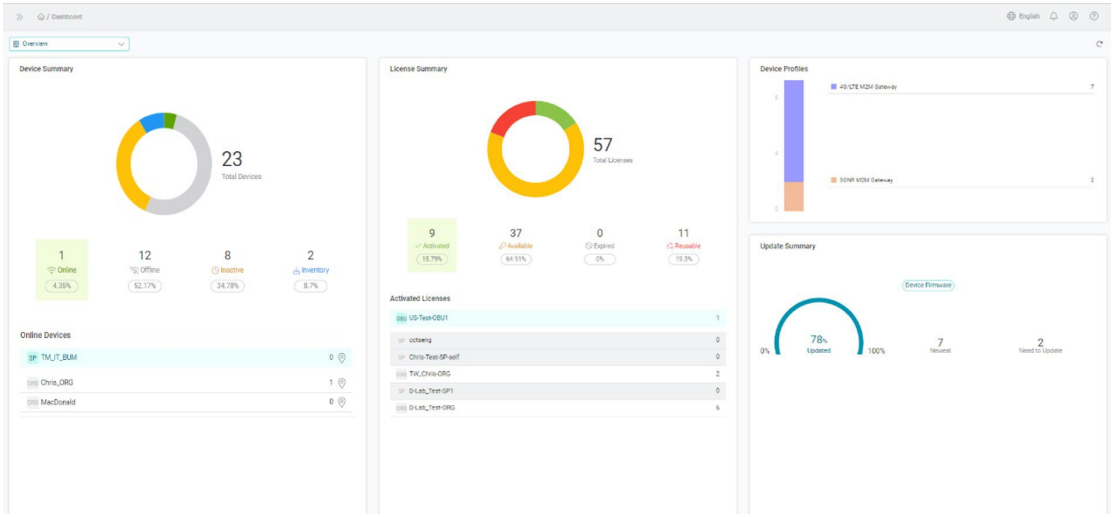
The **Update Summary** provides statistics on the number of devices with the latest firmware and those with older versions. The latest firmware version is based on the firmware file uploaded to the server (refer to **Upload OTA Files** for more information).

Note: The **My Staff Summary** as well as **License Summary,** which can be switched between by clicking  in the upper-right corner, is only available if your account is

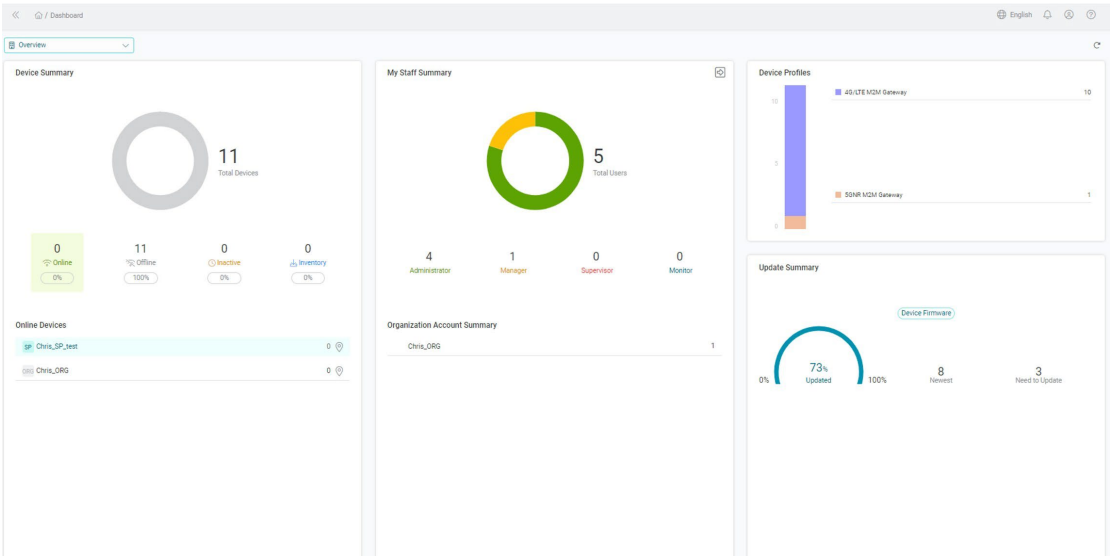
registered as an SP.

The **Google Map** (only available for an organization) at the lower left displays the location of devices that are currently online, offline, and inactive. You can switch to **Floor Plan** to display a visualization of the physical placement of the managed devices on a site map.

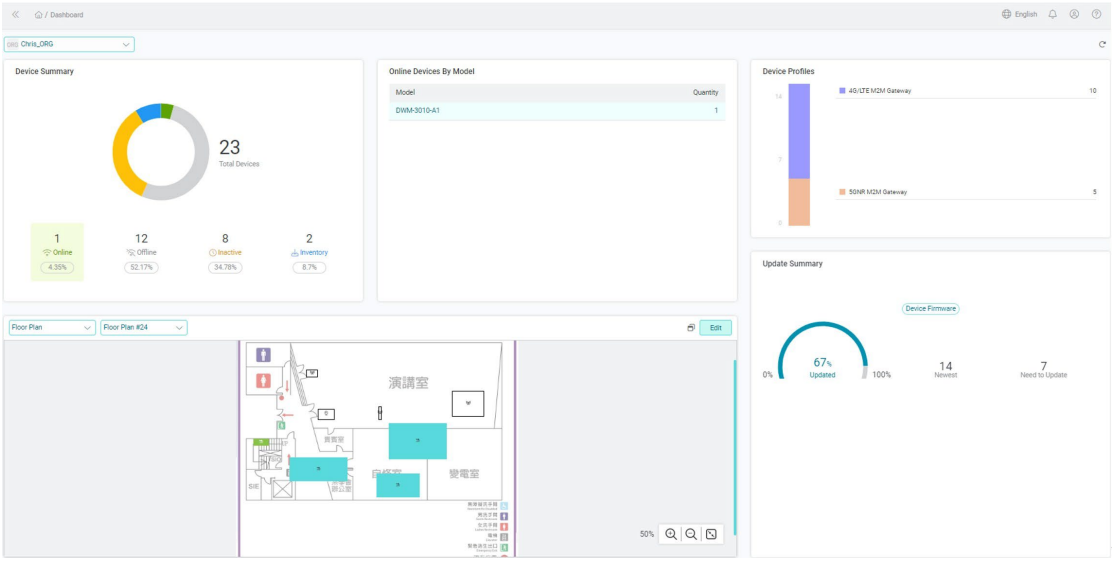
The dashboard layout is different for OBUs, service providers and organizations. This is the dashboard display for an OBU:



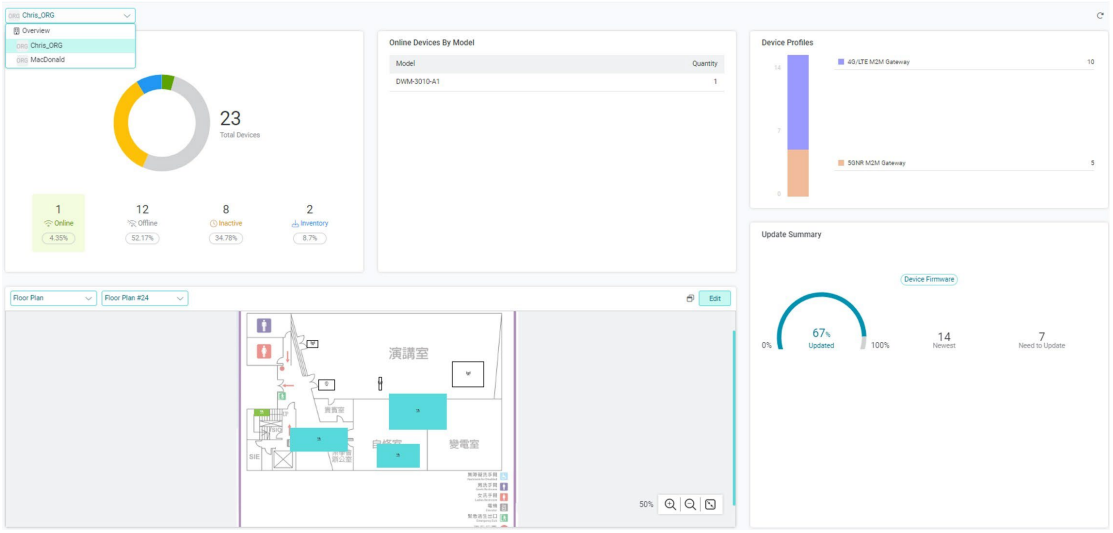
This is the dashboard display for a service provider:1



The following is a dashboard display for an organization:



A service provider can switch between the displays for an organization and a service provider by selecting among the entities at the top left (and likewise for an OBU to select among service providers and organizations):

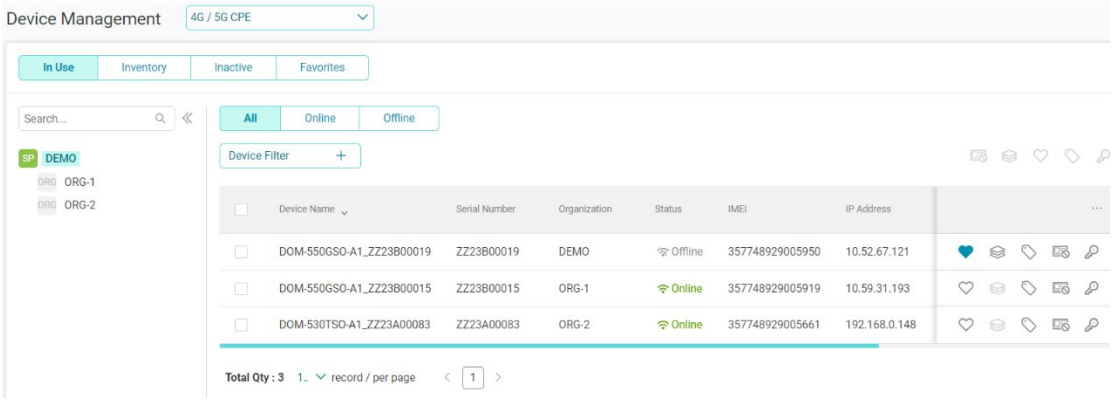


Devices

The Devices menu consists of the following submenus: **Device Management, Scheduled Tasks, Tag Management**, **Upload OTA Files, Alert Rules, Status Report Time**, and **Device Profile**.

Device Management

The Device Management is designed to make it easy to set up and centrally manage all your devices in one place in the cloud.



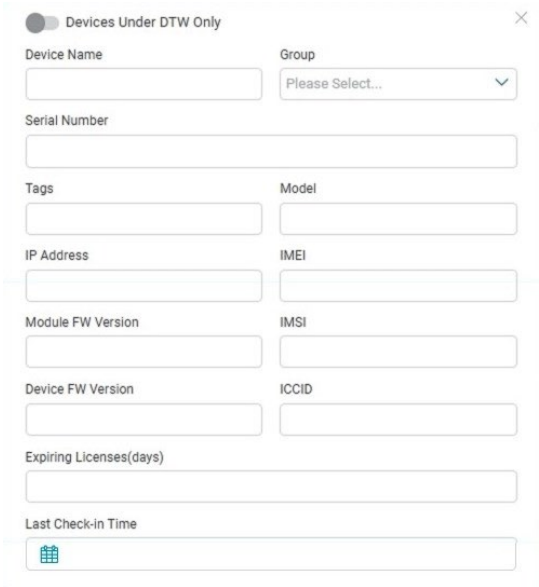
Note: Device registration is required for remote management through D-ECS. Refer to **Appendix** for device registration through D-ECS.

Navigate through the Device Management

A device can be listed in any of these tabs that represent its state of service: In Use, Inventory, and Inactive. Next to the title of the page (Device Management) is the product category drop-down list which distinguishes the major categories of the imported devices. The Favorites tab lists devices that have been added to the Favorites list for fast access. To list devices under an organization, click on the node of the organization in the left pane, which displays the hierarchy of the business entities. If you are a service provider, organizations shown in the left pane with green nodes allow you to manage their devices, whereas gray nodes prevent management from an SP. This section describes the functions for efficient inventory management and proper device maintenance and operation.

Search for a Device

You can create filters to filter the devices based on a number of properties.
To create a filter, click the **Device Filter+** button, enter the keyword(s) for the following parameters: **Device Name, Group, Serial Number, Model, Tags, IP Address, IMEI/IMSI/ICCID, Device/Module FW Version**, **Expiring Licenses(days)**, and **Last Check-in Time**.



Notes:

1. If you log in as an OBU or a service provider, the parent node lists all the devices under the parent entity as well as devices under its subordinates. If you would like to list devices only under this parent entity, enable the Devices Under *the parent entity name* toggle.
2. Users with the monitor role do not have the permission to perform the management functions instructed in this section by default.

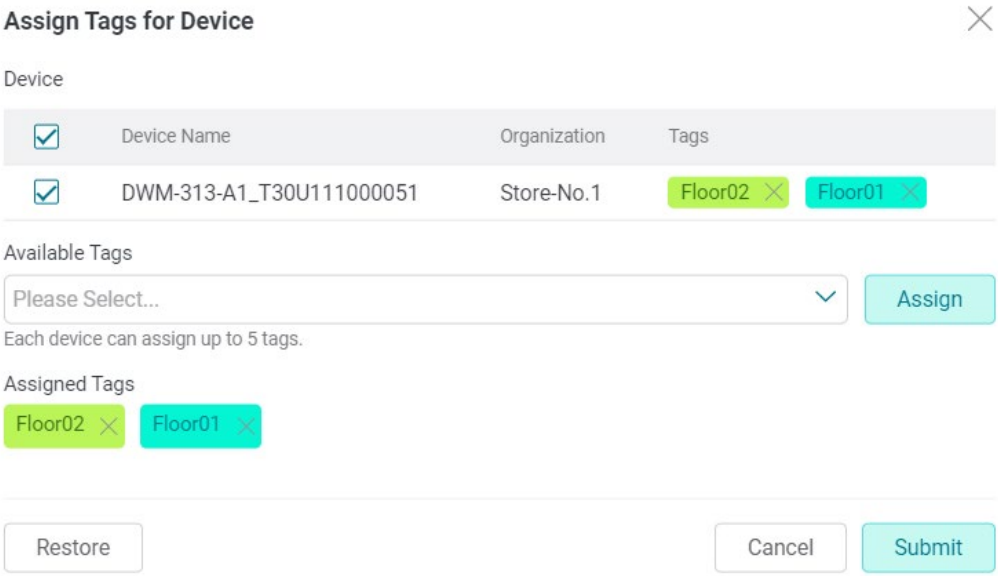
Tag a Device

This operation is only available for devices that are currently in use. Tags can be managed in the Tag Management page (refer to **Tag Management**).

Note: Tagging devices is not granted to users with the monitor role by default.

To tag a device:

1. Select device(s) in the list, then select in the upper-right corner for multiple devices or select at the end of the row for a single device.
2. Select the tag(s) from the **Available Tags** drop-down menu. Up to 5 tags can be selected for a device. Then click **Assign** to confirm your selection, which is listed under the **Assigned Tags** area.
3. Click **OK** when being asked for confirmation of device binding.
4. Click **Submit** to add the tag(s) to the device(s). If you want to retract your selection, click **Restore.**



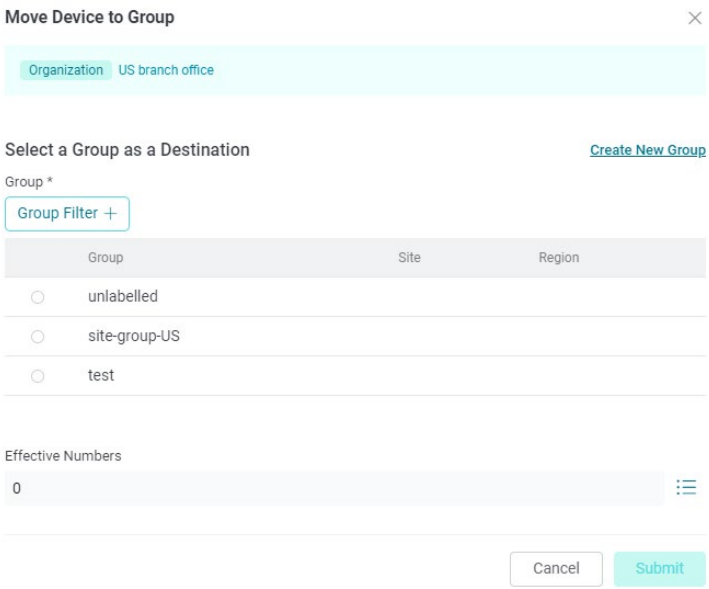
Move Devices to a Group

This operation is only available for devices that are currently in use. Groups can be managed in the **Group** page (refer to **Group** under **Organization**).

Note: Group assignment is not granted to users with the monitor role by default.
To move a device to a group:

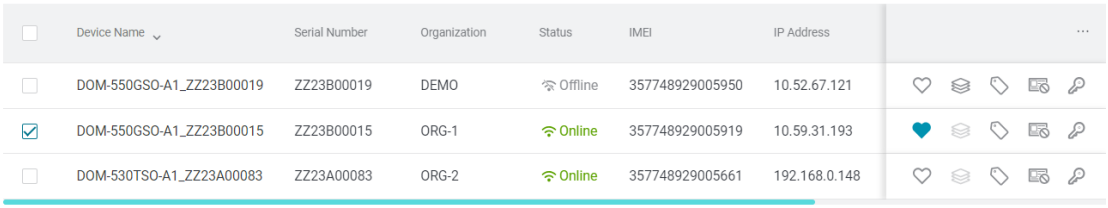
1. Select device(s) in the list, then select in the upper-right corner for multiple devices or select at the end of the row for a single device.
2. Use the **Group Filter** to filter groups. Select the region with the **All** option to list all groups under the parent region (or organization). Or select a particular region and then select the site to list available groups under this site.

3. Select the desired group for this device.
4. The **Effective Numbers** shows how many devices will be moved. To alter the list of effective devices, click details on the right.
5. Click **Submit**.



Add Devices to Favorites

This operation is only available for devices that are listed under **In Use**. To add device(s) to **Favorites**, select the device, then click . The device should also be also listed under the Favorites tab.

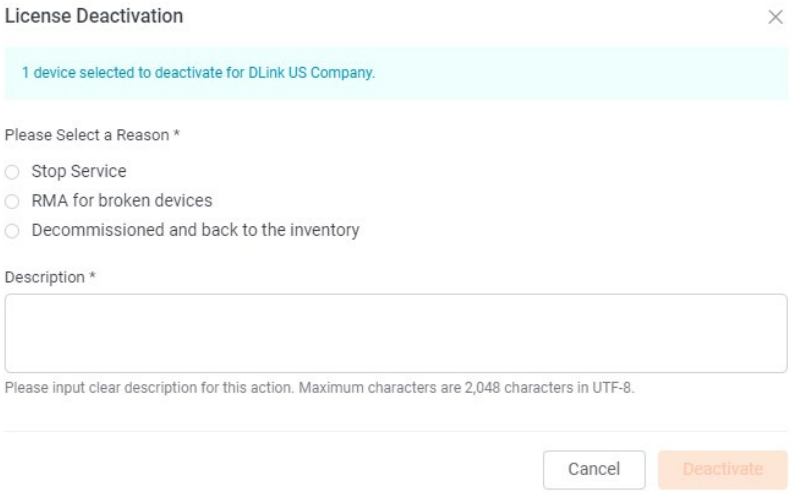


Deactivate a Device

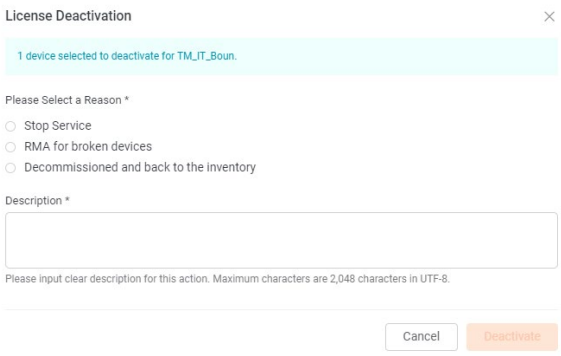
Product deactivation renders a device unusable.

Note: Product deactivation is not granted to users with the monitor role by default. To deactivate a product:

1. Select the device, then click  .
2. Select the cause of deactivation from one of the following categories:
   Stop Service
   RMA for broken devices
   Decommissioned and back to the inventory



3. State the reason in **Description**.
4. Click **Deactivate**.



The device will then be placed in the appropriate category of the **Inventory** or **Inactive** tab according to the specified reason. Moreover, the remaining duration of the subscription period will be listed under the **Reusable** tab of the **Licenses** menu.

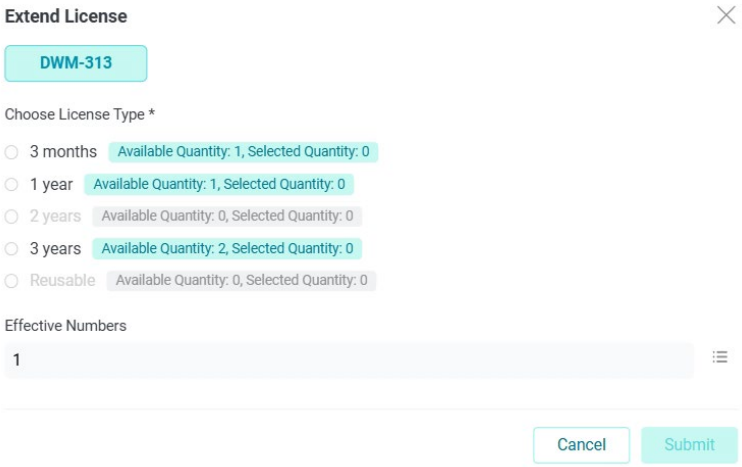
Extend License for a Device

This operation is only available for devices that are currently in use. Product license can be extended if there are available licenses.

Note: Product activation is not granted to users with the monitor role by default.

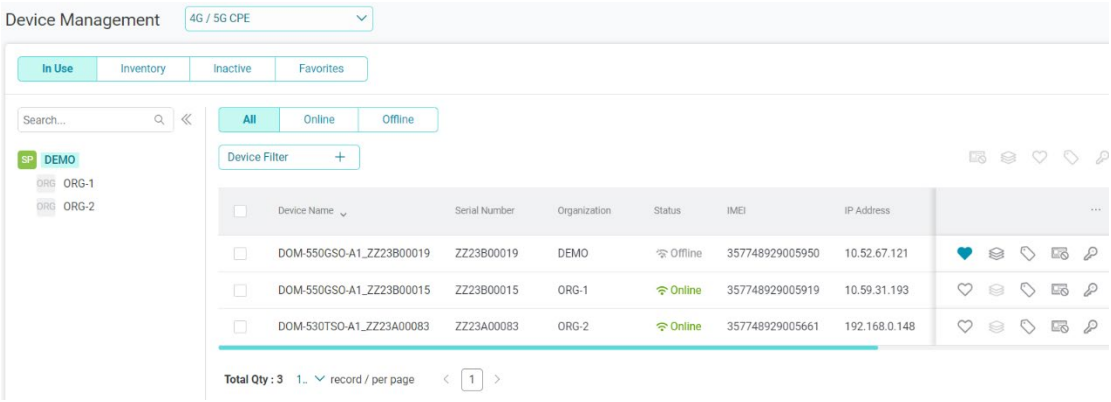
To extend a license for a product:

1. Select the device, then click .
2. Select the license term from the available licenses.
3. The **Effective Numbers** shows how many devices will be applied with the new license term. To alter the list of effective devices, click details on the right.
4. Click **Submit**.



In Use

The devices listed under the **In Use** tab are activated and operational. This section describes features for managing these devices (online or offline). To view the list of devices in use, click **Device Management > In Use.** Then select the product category from the drop-down list at the top: 4G/5G CPE



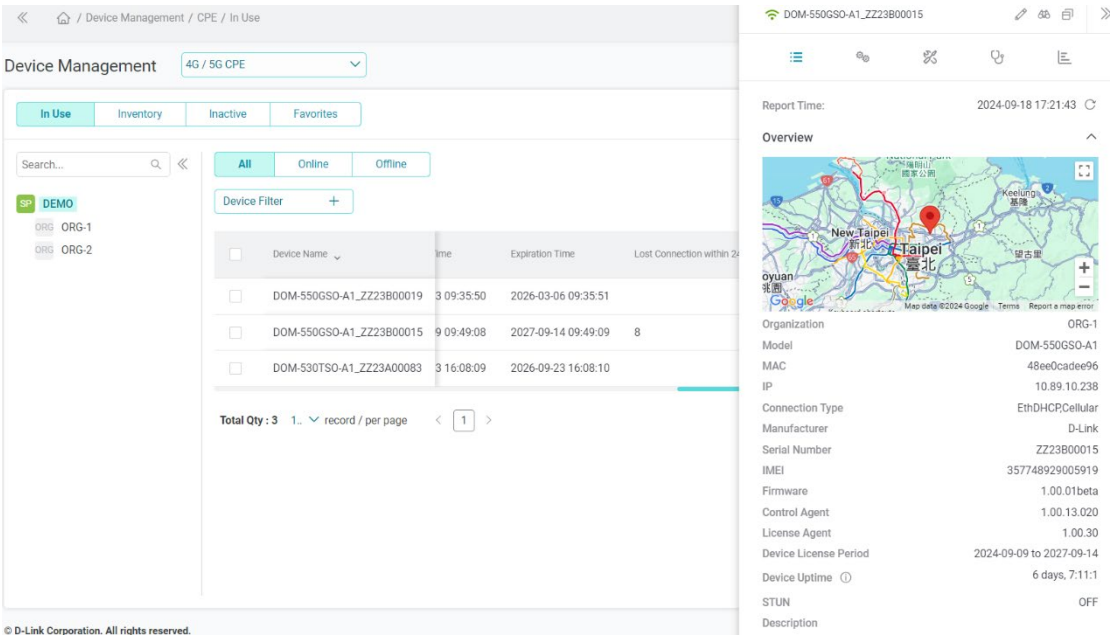
You can customize the displayed properties (hide or reveal the column) by clicking

 at the end of the table.

Device Name – Name of the device.
Serial Number – The serial number of the device.
Organization – The organization that this device belongs to.
Activation Time – The license activation time of the device.
Status – The online/offline status of the device.
Tags – The device tags for easy identification and search.
Group – The group where the device belongs.
IMEI – The International Mobile Equipment Identity is a unique number assigned to every mobile device.
IMSI – The SIM/USIM/UICC card has a unique number called an International Mobile Subscriber Identity (IMSI). This is used to identify and authenticate users on cellular devices.
ICCID – The Integrate circuit card identity is a unique number assigned to each SIM card.
RSRP – Reference Signal Received Power (RSRP), which measures the power level of the signal for the LTE and 5G network.
RSRQ – Reference Signal Received Quality (RSRQ), which measures the signal level and quality for the LTE and 5G network.
IP Address – The IP address of the device.
Model Name – The model name of the device.
Device FW Version – The firmware version of the device.
Module FW Version – The firmware version of the cellular module.
Cellular Signal – Signal strength indicator: the more lit bars, the better the signal.
Lost Connection within 24 hours – The total number of times the system did not receive status report from this device in 24 hours.
Last Check-in Time – The latest status report from this device that the system received.

Details

The **Details** tab provides a summary of the device information including interface settings and network statistics. It displays information on device settings, cellular interface, Ethernet WAN interface, LAN clients, and WLAN clients. To view this information, click **Device Management > In Use**, then click on the device to bring up the device information side menu.



Report Time – Shows the timestamp of the following information. You may click to refresh the information. You may also click to discover the device to obtain more in-depth data for device configurations. The Discovery operation takes longer than the Refresh operation.

Overview

The map at the top displays the current location of the device.
Device Name – Name of the device. It is unique and can be used to identify the device. You can modify it by clicking in the upper-right corner next to the displayed name.
Organization – The organization which the device belongs to.
Model – The model name of the device.
MAC – The MAC address of the device.
IP – IP address assigned to the interface.
Connection Type – The Internet connection method.
Manufacturer – Manufacturer of the device.
Serial Number – The serial number of the device.
IMEI – International Mobile Equipment Identity.
Firmware – The firmware version number installed.
License Agent – The current agent version for license management.

Control Agent – The current agent version for device management.
Device License Period – The period during which the device has been activated from YYYY-MM-DD to YYYY-MM-DD.
Device Uptime – The active length of time in days and hours:minutes:seconds that the device has been up. Click ⓘ to display device uptime history.
Description – A description for this device.

Cellular Interface 1

Network Name – The name of the mobile operator.
Current Use – The cellular technology used on this interface.
MNC – The Mobile Network Code.
MCC – The Mobile Country Code.
IMSI – The International Mobile Subscriber Identity.
Band – The LTE frequency band.
RSRP – Reference Signal Received Power(RSRP), which measures the power level in the LTE cell network.
SINR – Signal-to-interference-plus-noise ratio, which measures the quality of wireless signal by taking account of noise and other interfering factors.
RSRQ – Reference Signal Received Quality (RSRQ), which measures the signal level and quality in the cellular network.
Signal Level – The signal strength measured in dBm.
RSSI – Received Signal Strength Indication, which measures the power of a received radio signal.
TAC – The Type Allocation Code, which indicates the manufacturer and model of the device.
Cell ID – Indicates the cell tower or site.
Manufacturer – Manufacturer of the device.
Software Version – The software version information for the router.
APN Configuration – Access Point Name (APN), which sets up a network connection to enable Internet access through cellular communication.

Wireless

The following information identifies the available wireless networks:
SSID – The name of the Wi-Fi network.
BSSID – The MAC address of the Wi-Fi interface.

Channel – The channel assigned for this Wi-Fi network.
Transmit Power – The level of transmission power.
Total Bytes Sent – Number of bytes sent through this network.
Total Bytes Received – Number of bytes received through this network.
Total Packets Sent – Number of packets sent through this network.
Total Packets Received – Number of packets received through this network.
Total Associations – Number of connected clients.

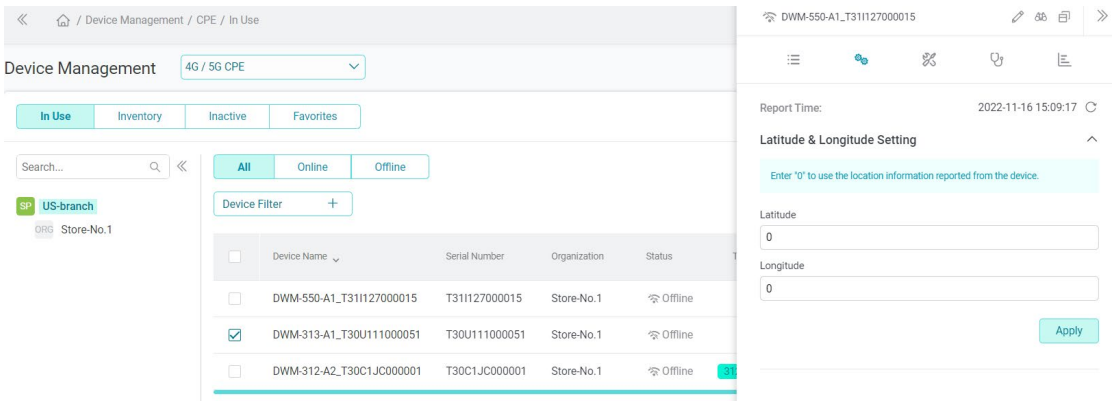
Connected Clients

The connected clients through both Ethernet cables and wireless radios are displayed with the following information:
Interface – The interface for connectivity with the network device.
Name – The host name of the client.
IP Address – The IP address of the client device.
MAC Address – The MAC address of the client device.

Note: The above information varies depending on the functionality of your model.

Config

The Config tab allows you to adjust the settings of your wireless network.



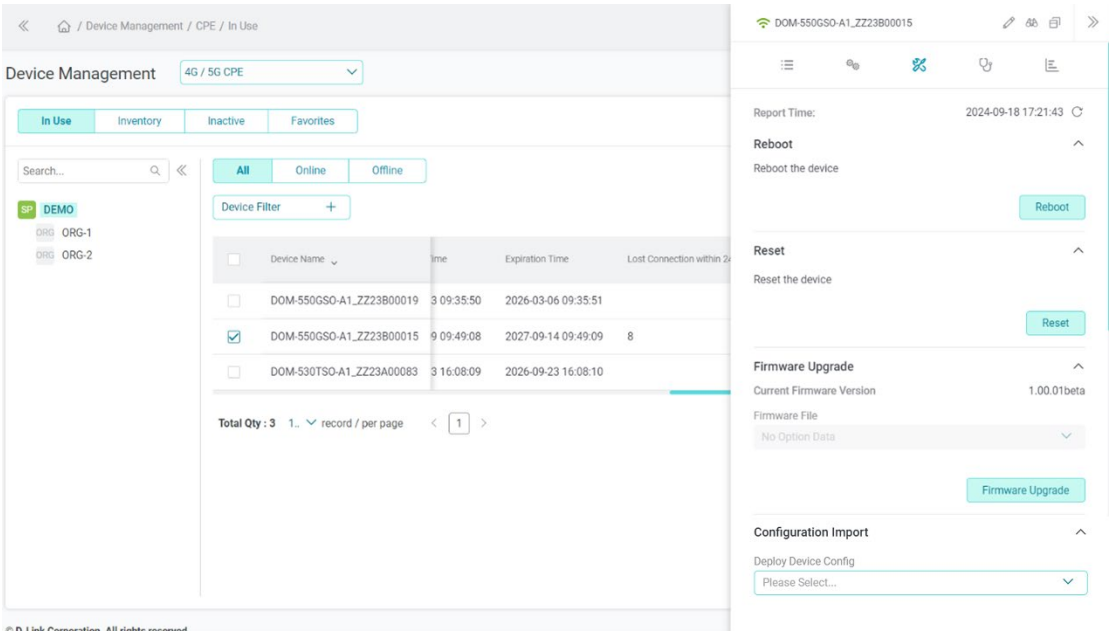
Note: Users with the monitor role do not have the permission to perform the configuration functions instructed in this section by default.

Manual Latitude & Longitude Settings

Enter the latitude and longitude settings for the device to be used for displaying location-related information. Enter "0" to use the location information reported from the device.

Operations

The **Operations** tab allows you to perform maintenance tasks such as firmware update and system configuration backup and restoration.



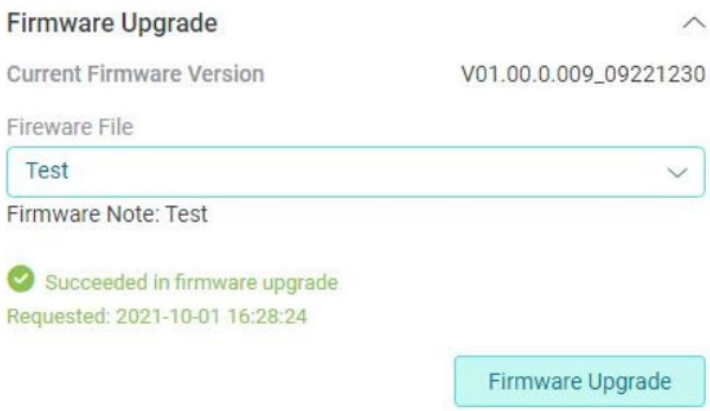
Notes:

1. Users with the monitor role do not have the permission to perform the operation functions instructed in this section by default.
2. The operations described in this section require the device status to be online.

Firmware Upgrade

The system allows you to upgrade firmware of both the device and cellular module. To upgrade the device firmware, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, scroll down to **Firmware Upgrade**, choose a firmware file from the list, then click the **Firmware Upgrade** button. Note that you will need to upload the firmware files to the server first

before performing firmware update (Refer to **Upload Firmware File to the Server**.

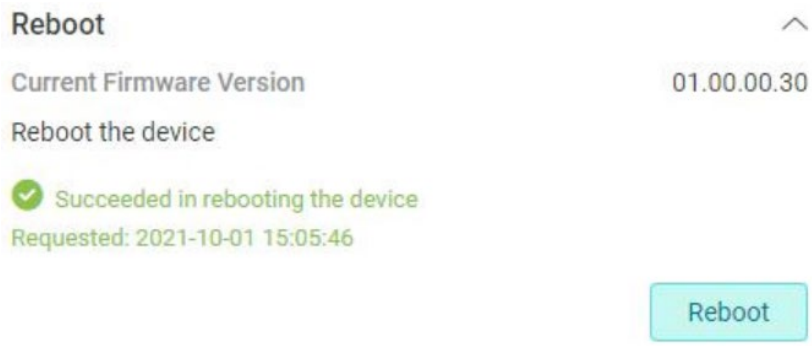


Reset

To reset a device, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, scroll down to **Reset**, then click Reset. Confirm your operation. You can cancel the reset process before it completes.

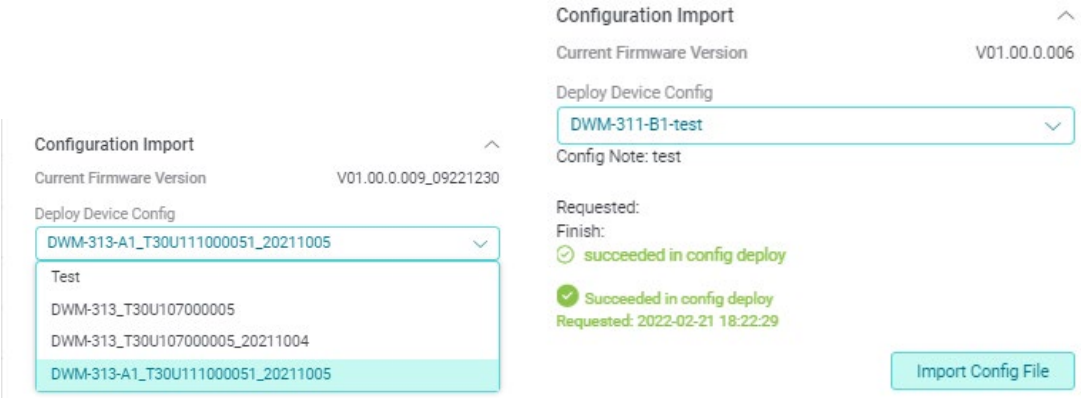
Reboot

To Reboot a device, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, find the **Reboot** option, then click **Reboot**. Confirm your operation. You can cancel the reboot process before it completes.



Configuration Import

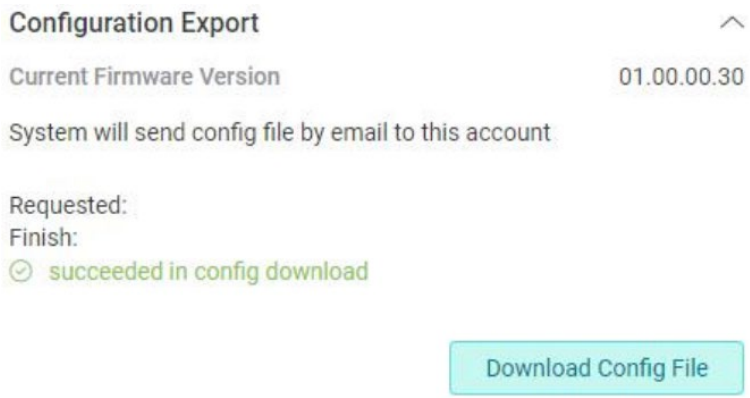
Configuration Import can be used to restore your device to an earlier configured state if the current configuration file is not operating as required or if you would like to revert changes to several settings. To import configurations, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, scroll down to **Configuration Import**, then click **Import Config File**. The available configuration files for import will be listed in **Upload OTA Files > Device Config File**. The system will show a warning sign stating that there are no configuration files on the system, and it will require you to upload a configuration file first. (Refer to **Upload Configuration File to the Server** for more information.)



Configuration Export

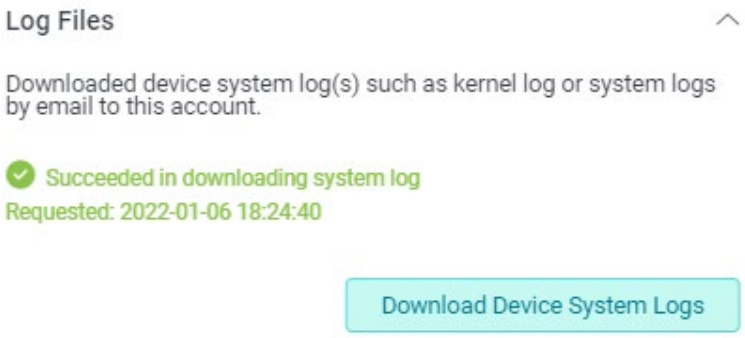
To export device configuration as a single file, click anywhere on the row of the device to bring up the device info side menu. Click **Operations** in the top pane, scroll down to **Configuration Export**, then click **Download Config File**. You can cancel the export process before the process is complete. Once the export is completed, it will

inform you whether it is a success or failure.
The configuration file will then be sent to the requester by email. Go to **Organization > Organization Users** for more information on users and email settings.



System Logs

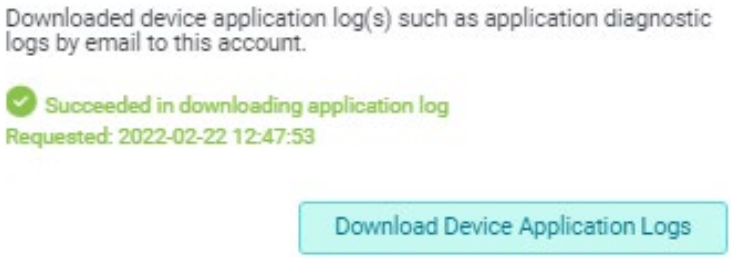
The Log File Download allows you to download system logs concerning kernel activities or system operation. You can cancel the operation before it is complete.
To download system logs, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, scroll down to **Log Files**, then click **Download Device System Logs**. You can cancel the download process before it is complete. Once the process is completed, it will display **System logs downloaded**.



The log file will be sent to the requester by email. (Refer to **Organization Users in Organization** for more information on users and email settings.)

Application Logs

The Log Files Download allows you to download application logs concerning management activities on the system. You can cancel the operation before it is complete. To download application logs, click anywhere on the row of the device to bring up the device information side menu. Click **Operations** in the top pane, scroll down to **Log Files**, then click **Download Device Application Logs**. You can cancel the download process before it is complete. Once the process is completed, it will inform you whether it is a success or failure.



The log file will be sent to the requester by email. (Refer to **Organization Users in Organization** for more information on users and email settings.)

Diagnostics

The Diagnostics tab provides tools to help you troubleshoot network issues. In addition, it allows you to monitor the health of your network.

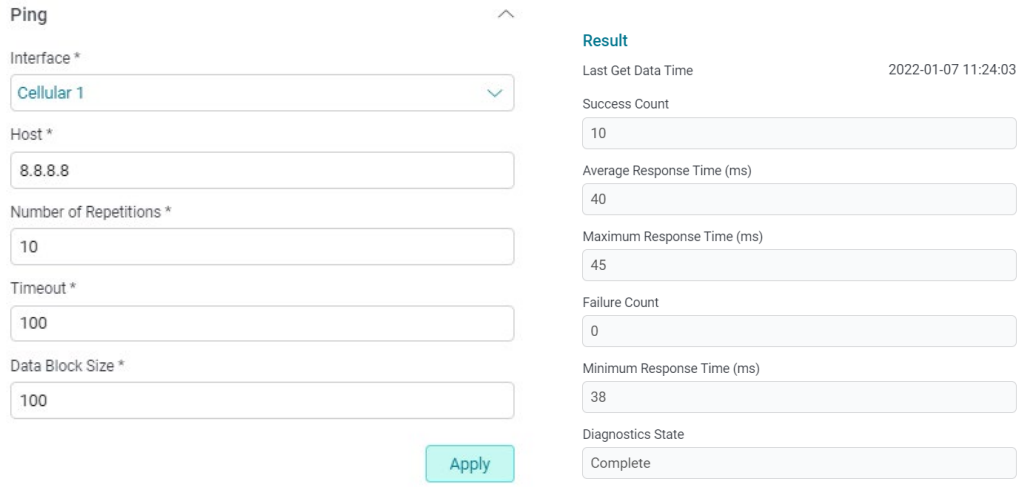
Notes:

1. Users with the monitor role do not have the permission to perform the diagnostic functions instructed in this section by default.
2. The functions described in this section require the device status to be online.

Ping

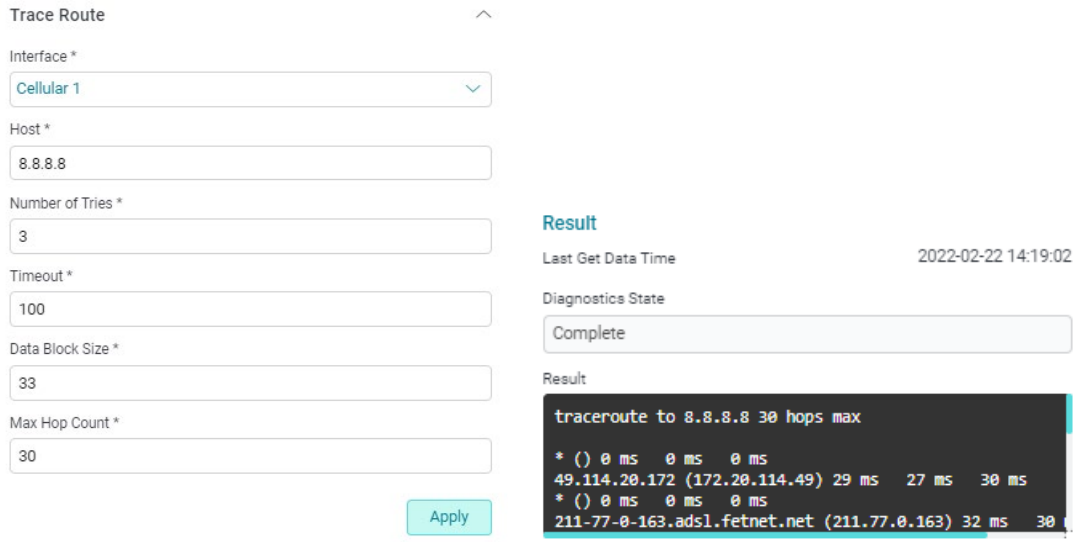
Use the Ping diagnostic tool to get the status of another device on the network.
To ping a device, select the **Interface** for the source interface of the command, enter the destination IP address for **Host**, enter the **Number of Repetitions** for the number of requests, and enter the **Timeout** value (milliseconds) and **Data Block Size** (bytes) to specify the packet size to be sent. Then click **Apply** to start the test. The ping results

will be displayed below.



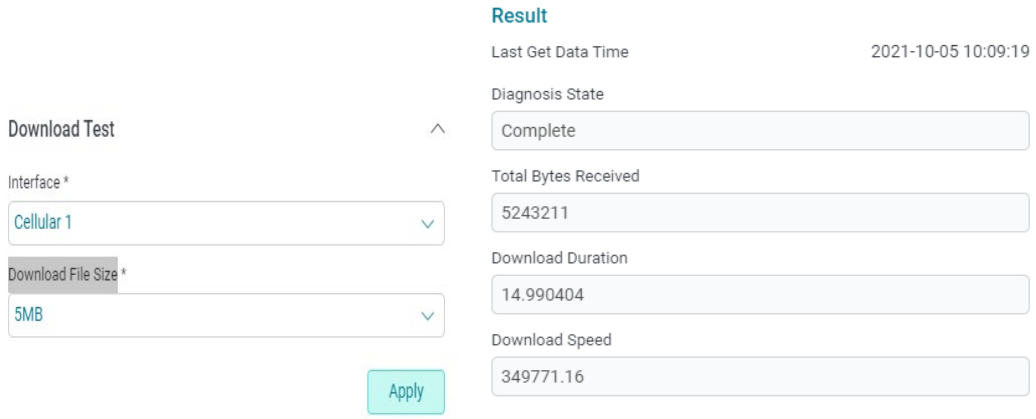
Trace Route

The Trace Route utility test the connectivity between the device and another one on the network. To trace route a device, select the **Interface** for the source interface of the command, enter the destination IP address for **Host**, enter the **Number of Tries** to specify the number of queries for each hop and the **Timeout** value (milliseconds) for each reply, and enter **Data Block Size** (bytes) as well as **Max Hop Count** for the maximum number of hops. Then click **Apply** to start the test. The trace route results will be displayed below.



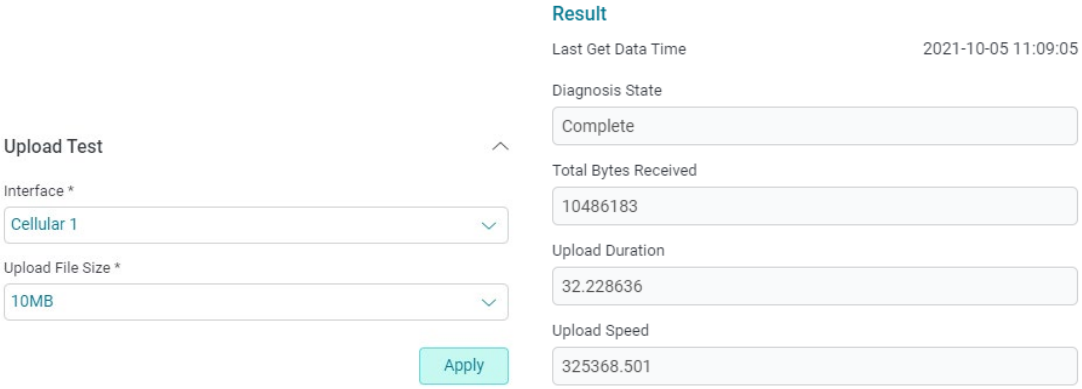
Download Test

The Download Test measures the rate at which the content is being transferred to the device from the server in the cloud.
To start the Download Test, select the interface for receiving the download file, select the file size for the download data, then click **Apply**. The results will be displayed below.



Upload Test

The Upload Test measures the rate at which the content is being transferred out of the device to the server in the cloud.
To start the Upload Test, select the interface for sending the upload file, select the file size for the upload data, then click **Apply**. The results will be displayed below.



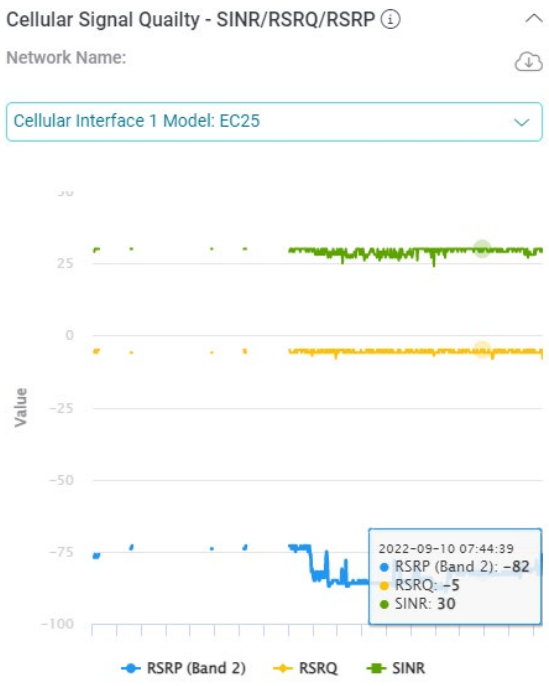
Stats

The Stats page displays statistics of cellular and Wi-Fi data relating to signal quality and data usage. For the following statistics, you can click  to send the

information to your account's registered email.

Cellular Signal Quality – SINR/RSRQ/RSRP

Signal to Interference plus Noise Ratio (SINR): The Signal-to-Interference-plus-Noise Ratio (SINR) indicates the signal quality with respect to interference in LTE and 5G network.
Reference Signal Received Power (RSRP): The Reference Signal Received Power (RSRP) indicates the estimated power level of signals in LTE and 5G network.
Reference Signal Received Quality (RSRQ): The Reference Signal Received Quality (RSRQ) indicates the signal quality of LTE and 5G network.
The RSRP, RSRQ, and SINR information is displayed graphically.



Mouse over ⓘ to obtain information about the classes in quality as shown in the following table:

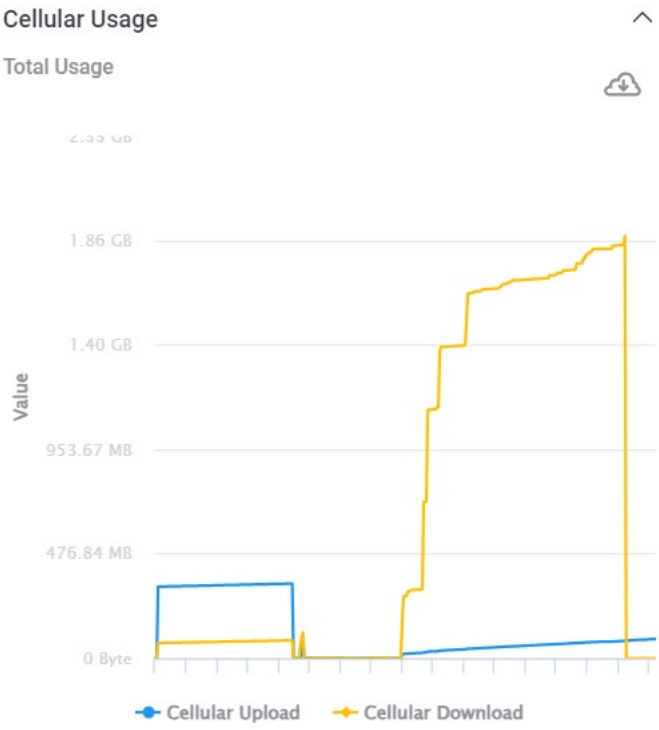
Cellular RF Signal Quality Reference

Quality	RSRP (dBm)	RSRQ	SINR (dBm)
Excellent	> -84	> -5	> -12.5
Good	-85 to -102	-5 to -9	12.5 to 10
Fair	-103 to -111	-9 to -12	10 to 7
Poor	< -111	< -12	< 7

You can then determine your signal quality by referencing this table.

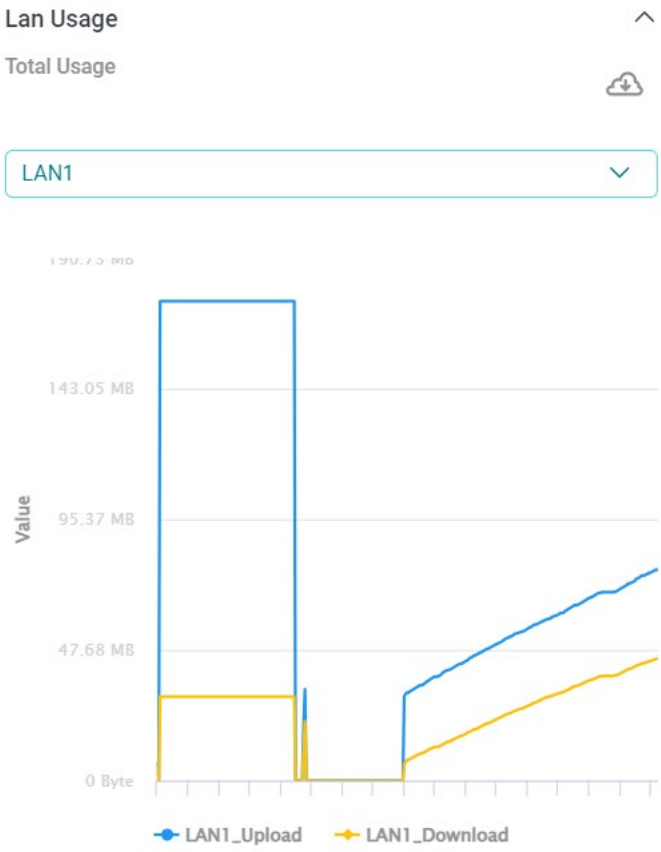
Cellular Usage

The cellular usage shows the amount of data being transferred through the selected cellular interface including the upload and download data.
Download data: The amount of data that is being transferred to the cellular interface.
Upload data: The amount of data that is being transferred to the Internet.
The following graph shows the usage data:



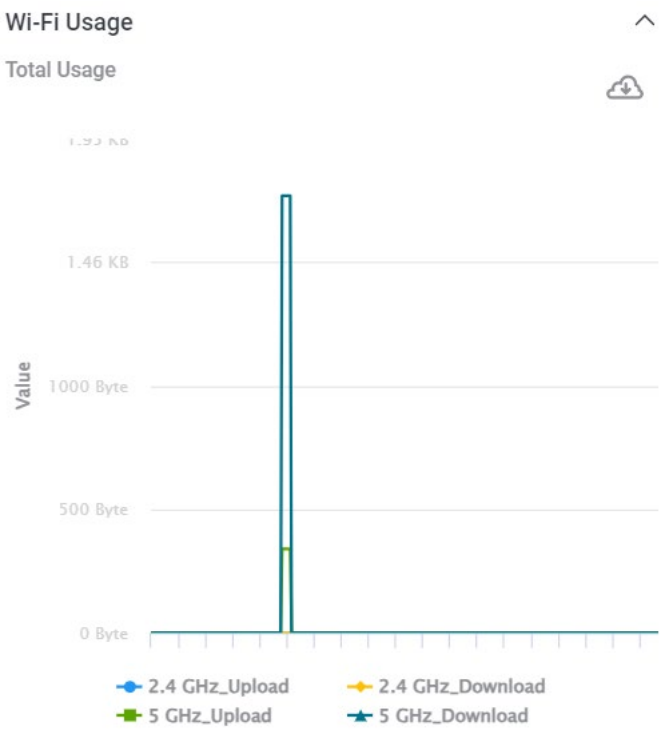
LAN Usage

The LAN usage shows the amount of data being transferred through the selected LAN interface including the upload and download data.
Download data: The amount of data that is being transferred to the LAN interface.
Upload data: The amount of data that is being transferred to the Internet.
The following graph shows the usage data:



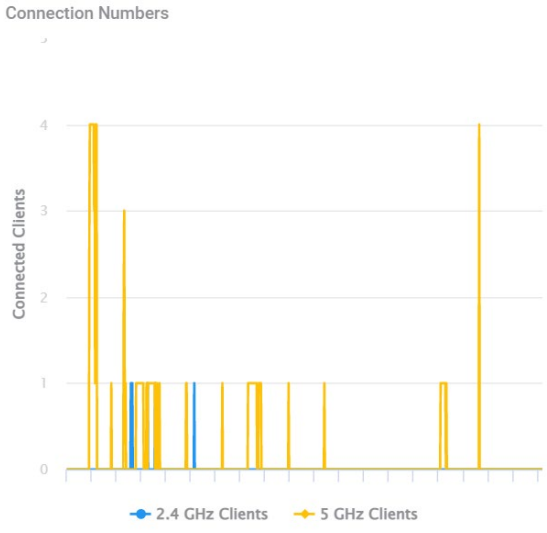
Wi-Fi Usage

The Wi-Fi usage shows the amount of data being transferred through the wireless Ethernet interface including the upload and download data.
Download data: The amount of data that is being transferred to the wireless interface.
Upload data: The amount of data that is being transferred to the Internet.
The following graph shows the usage data graphically:



Connected Clients

The Connected Clients information shows the number of clients connected to the wireless network with respect to time.



Inventory

The Inventory tab lists devices not being deployed to any organization. The **New Imported** tab lists devices that are imported to the system. The Inventory also contains the **Decommissioned** tab to list devices that are deactivated because of decommissioning. It provides essential inventory functions: device import, activation, deliver, and deletion on the Inventory.

Click **Device Management > Inventory** to see the following information:

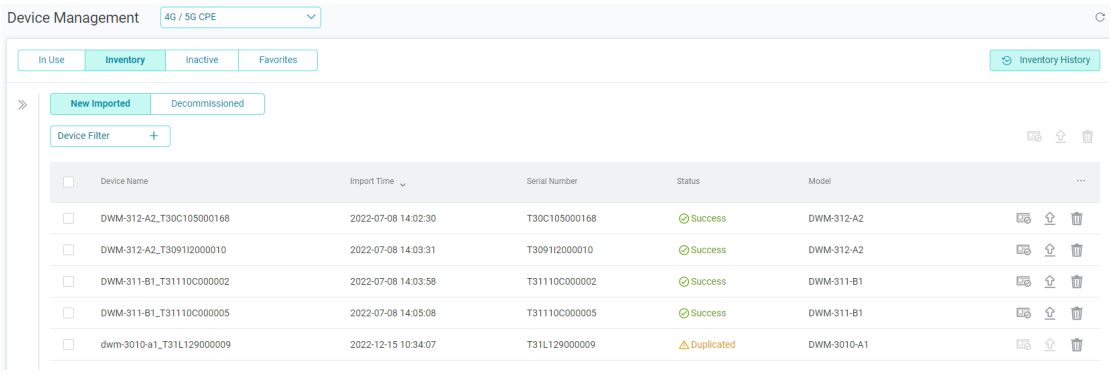
Device Name – Name of the device. It is unique and can be used to identify the device.

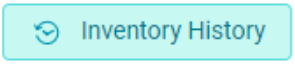
Import Time – The time that the device was imported to the server.

Serial Number – The serial number of the device.

Status – The import status of the device, i.e. Success, Duplicated (duplicated devices with the current inventory list), Error (unsuccessful import of the device).

Model – Model name of the device.



For every import, there is a record showing the import time, the account that performs device import, the number of devices that were successfully imported, duplicated, or failed to import. Click the **Import Devices** drop-down menu and select **Inventory History** 

to display records of import history.

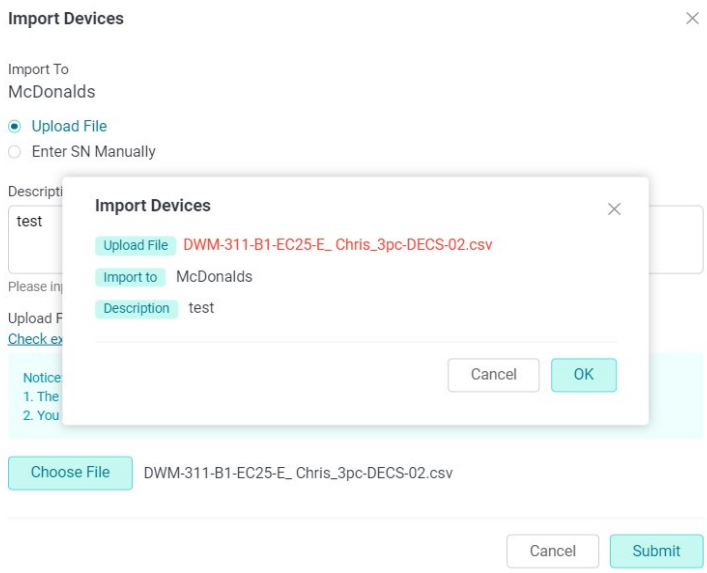
Import Devices to D-ECS

Importing devices to D-ECS requires a list of device serial numbers. The list can be saved in *.xls , .xlsx, or .csv format.

To import devices to D-ECS:

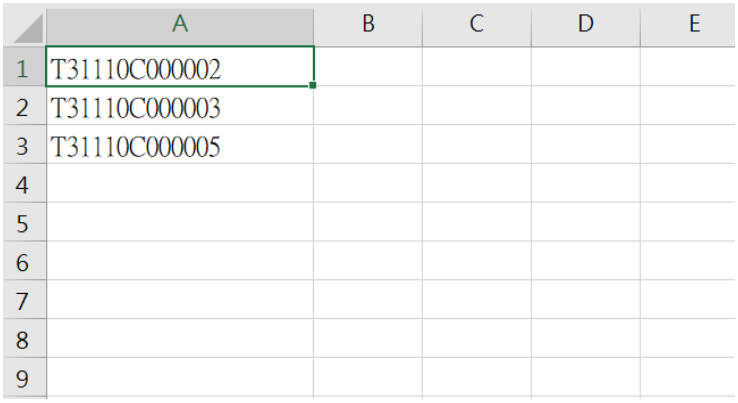
1. Go to **Device Management**, select **Inventory**, then select **Import Devices** at the top right, and then select **Import Devices** at the top right.

2. Choose **Upload File** to upload a file with a list of devices or **Enter SN Manually** to enter serial numbers manually.
3. Put a description for this import in the **Description** field.
4. Click **Choose File** to choose the file to be uploaded, then click **Submit** to start the import process.
5. Review the summary of the import, then confirm the import by clicking **OK**.



Note: Be sure to check the status of the inventory list to verify if the devices have been successfully imported to the system.

The following shows how the data should be recorded in a .xls file:



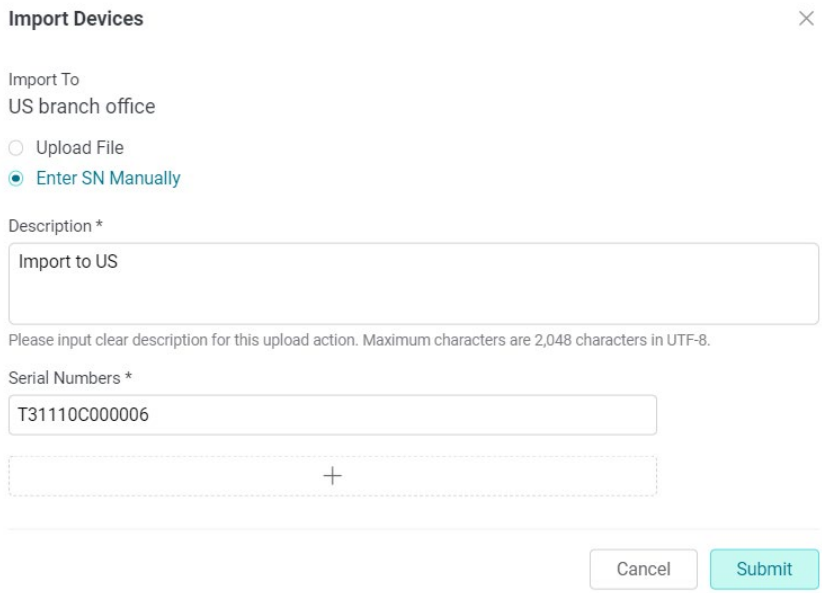
	A	B	C	D	E
1	T31110C000002				
2	T31110C000003				
3	T31110C000005				
4					
5					
6					
7					
8					
9					

The following shows how the data should be recorded in a .csv file:

T31110C000002
T31110C000003
T31110C000005

You can also add devices manually using the form provided on the web page shown

below:



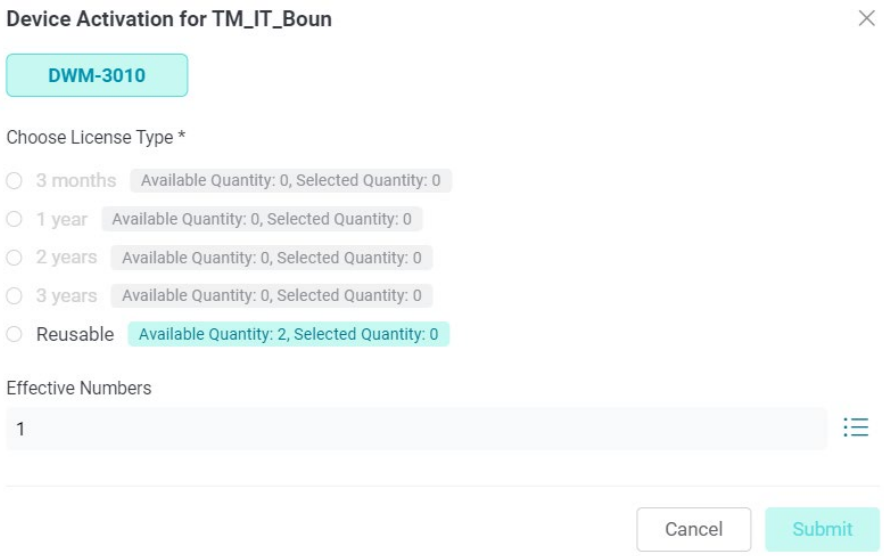
Click + to add serial numbers one after another.

If the import is successful, you will be able to view the list of imported devices under the **New Imported** tab.

For devices under the New Imported and Decommissioned list, you can perform the following actions: device activation, device delivery or retrieval (or return), and deletion.

To activate a device:

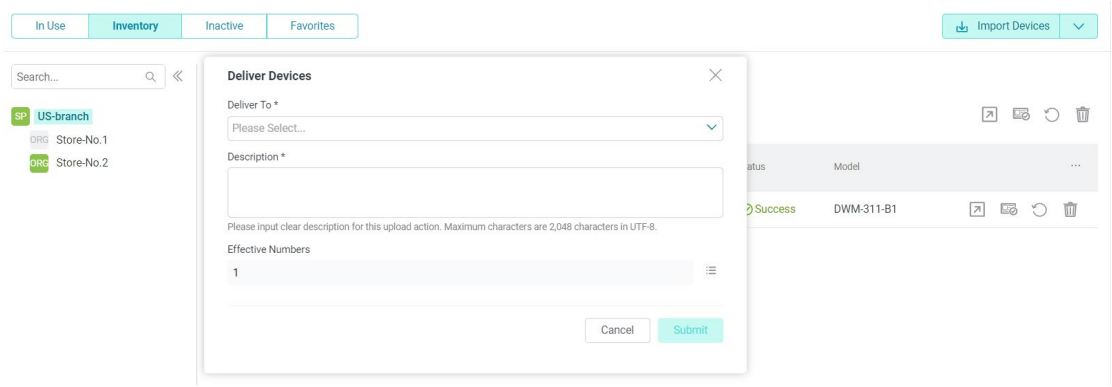
1. Select the device(s) and click Activate Device(s). For a single device, click at the end of the row. For multiple devices, click at the top of the table.
2. Select the license term: 3 months, 1 year, 2 years, 3 years or reusable license plans from the remaining term of device deactivation. The **Effective Numbers** shows how many devices will be activated under this license plan. To alter the list of effective devices, click details on the right.



Once a device is activated, it will be listed in the **In Use** tab instead. Note that devices that are activated can be deactivated later.

To deliver a device:

1. Select the device(s) and click Deliver Device(s) .
2. Select the client organization (i.e. a direct subordinate in the list) as the delivery destination.
3. Write a description for this displacement.
4. Click **Submit** to start the delivery process.



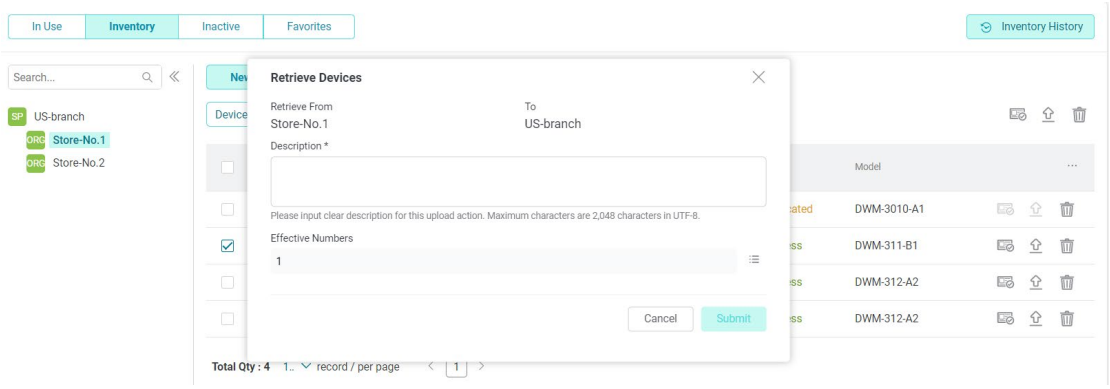
You can then view the device under the destination organization.

To retrieve a device:

This option is only available after a device has been delivered to a customer listed as a subordinate.

1. Select the device(s) and click Retrieve Device at the end of the row for a single device or click at the top right for multiple devices.
2. Write a description for this retrieval.

3. Click **Submit** to start the retrieval process.

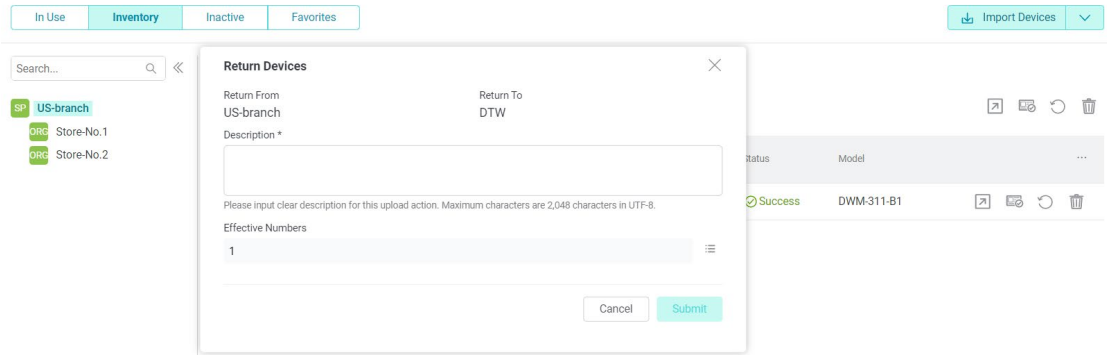


You can then view the device under the entity of your organization (or directory).

To return a device:

This option is only available for customers listed as subordinates after a device has been delivered.

1. Select the device(s) and click **Return Device** at the end of the row for a single device or click at the top right for multiple devices.
2. Write a description for the return.
3. Click **Submit** to start the return process.



The device will be returned to the parent organization (or directory).

To delete a device:

Select the device(s) and click Remove Device(s) .

Inactive

Devices listed under the Inactive tab are classified in 3 categories: **Stop Service**, **Expired**, and **Broken**. Stop Service are reported malfunction due to a variety of

reasons (e.g. hardware maintenance or software update) in which users may specify when they deactivate a device. Expired devices are due to license expiration. **Broken** are devices sent for Return Merchandise Authorization service as specified by users when they deactivate a device.

Click **Device Management > Inactive** to see the following information:

Device Name – Name of the device. It is unique and can be used to identify the device.

Import Time – The time that the device was imported to the server.

Serial Number – The serial number of the device.

Group – The group where the device belongs.

Model – Model name of the device.

Status – The current operating status of the device.

Event Description – Describes the cause of inactivity. The description is filled in by user as the reason for deactivating a device.

For devices in the **Inactive** category, you can reactivate it.

To reactivate a product with a valid license:

1. Select the device, then click  at the end of the row. Or select multiple devices, then click  at the top right.
2. Choose the License Type that are available for this product model.
3. The **Effective Number** displays the number of devices being selected. Click  to see device list and detailed information and alter your selection.
4. Click **Submit** to confirm your action.

Favorites

The Favorites tab lists devices that have been added to Favorites. To access devices under this category, click **Device Management > Favorites**. The following information is displayed for the devices in the list:

Device Name – Name of the device. It is unique and can be used to identify the device.

Serial Number – The serial number of the device.

Organization – The organization that this device belongs to.

Status – The status of the device.
Group – The group where the device belongs.
IMEI – The International Mobile Equipment Identity, which is a unique number assigned to every mobile device.
IMSI – The SIM/USIM/UICC card has a unique number called an International Mobile Subscriber Identity (IMSI). This is used to identify and authenticate users on cellular devices.
ICCID – The Integrate circuit card identity is a unique number assigned to each SIM card.
RSRP – Reference Signal Received Power (RSRP), which measures the power level for the LTE cell network.
RSRQ – Reference Signal Received Quality (RSRQ), which measures the signal level and quality for the LTE cell network.
IP Address – The IP address of the device.
Model Name – Model name of the device.
Device FW Version – The firmware version of the device.
Module FW Version – The firmware version of the cellular module.
Cellular Signal – The more lit bars, the better the signal.
Lost Connection within 24 hours – The total number of times the system did not receive status report from this device in 24 hours.
Last Check-in Time – The latest status report from this device that the system received.

To add a device to Favorites:

1. Go to **Device Management** and select the **In Use** tab.
2. Select the device, then click ♡ .
3. The device should also be listed under the **Favorites** tab.

Scheduled Tasks

The scheduled tasks are created to perform defined administrative tasks according to set schedules on selected devices. The tasks that can be set to perform automatically whenever the device comes online or periodically include reset, reboot, configuration deployment, firmware upgrade.

Notes:

1. Operations related to scheduled tasks are not granted to users with the monitor and supervisor role by default.
2. For configuration deployment and firmware, uploading the respective files will be required. (Refer to **Upload OTA Files** for more information.)

To view the configured tasks, click **Scheduled Tasks** under **Devices**, and select the **General** tab.

The following information will be displayed:

Task Name: Name of the task

Scheduled Task: Type of the task

Succeed: Number of devices completed the task and the Percentage of task completeness (number of devices completed the task/total number of devices selected)

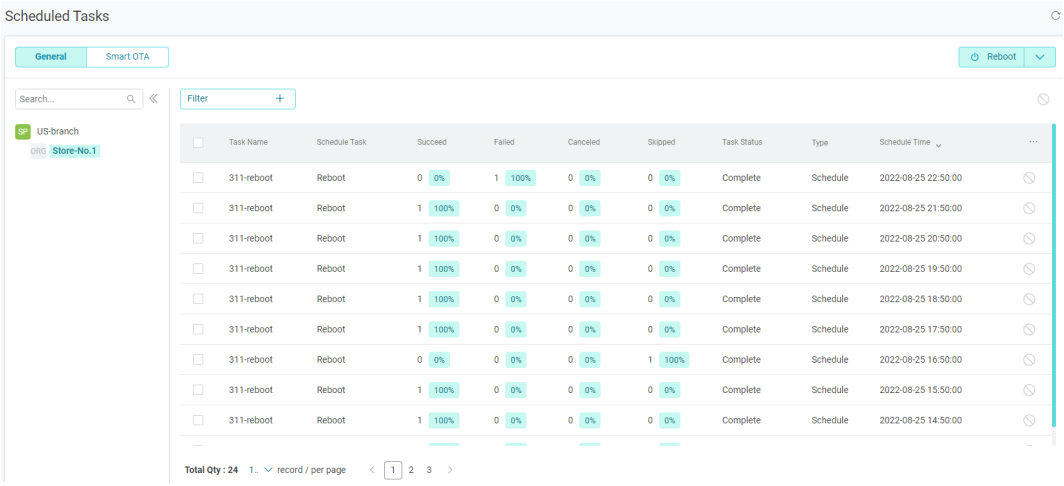
Failed: Number of devices failed the task and the Percentage of task failure (number of devices failed the task/total number of devices selected)

Canceled: Number of devices being canceled, and the Percentage of task canceled (number of devices being canceled while it is waiting to be executed/total number of devices selected)

Skipped: Number of devices being omitted and the Percentage of such omission (number of devices being omitted of the task/total number of devices selected). The reason for omission could be device offline or occupied with other tasks.

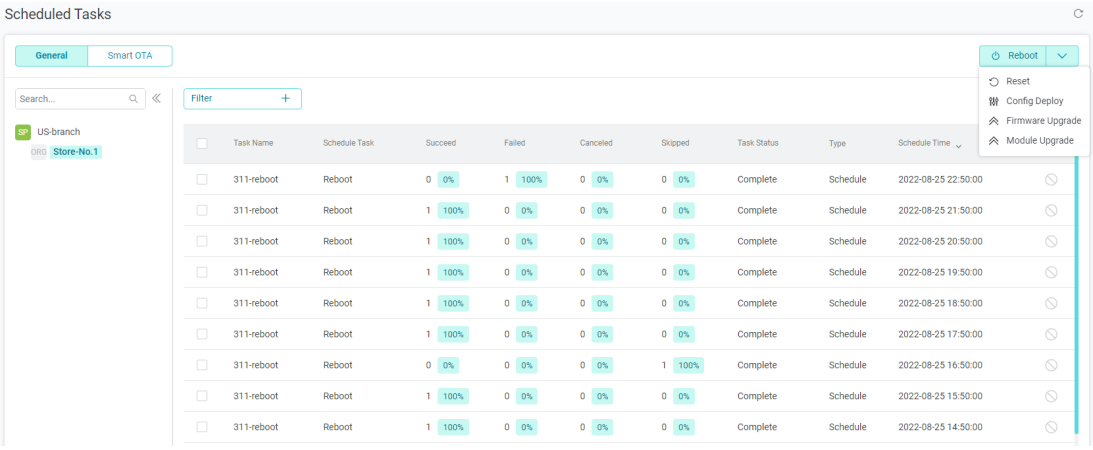
Task Status: The executing status of the task, i.e. **Queuing** (waiting to be executed based on the schedule), **Running** (executing now), **Complete** (task has already been done or the schedule has been successfully programmed on the device), or **Canceled** (task being canceled by user), or **Fail** (task failed)

Schedule Time: Scheduled time for the task.

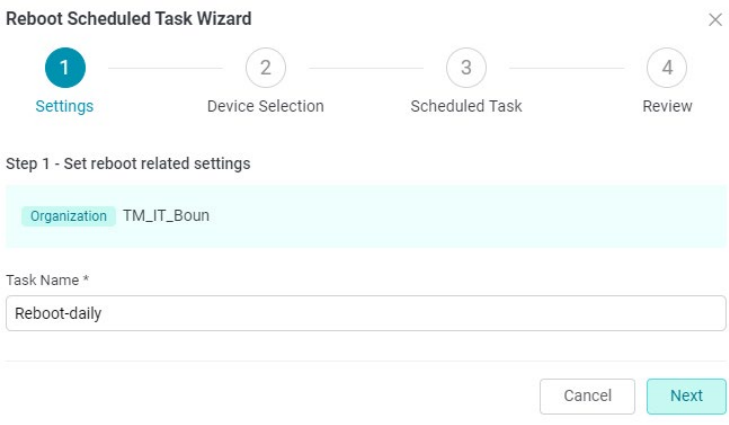


To create a scheduled task:

1. Select the task from the drop-down menu at the top right: **Reboot, Reset, Config Deploy,** and **Firmware Upgrade**.



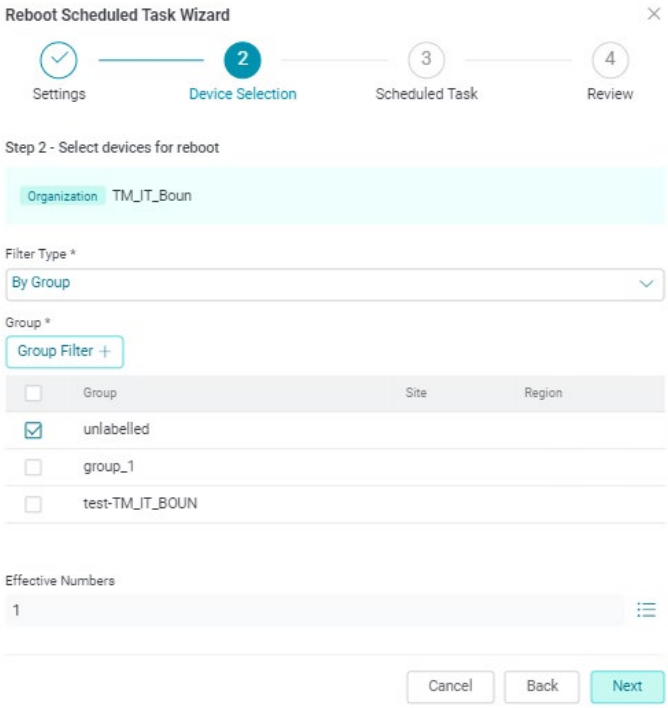
2. The respective task wizard appears.
3. Name your task then click **Next**. Special characters such as ^[~!@#$%^&*()+=:;,.<>\/?]*$ are not allowed.



4. For **Config Deploy** and **Firmware Upgrade**, select the device model first. Then For

Firmware Upgrade and **Config Deploy**, select the firmware file and configuration file respectively (note that the names of the firmware files or configuration files can be obtained from **Upload Firmware File to the Server** and **Upload Configuration File to the Server**).

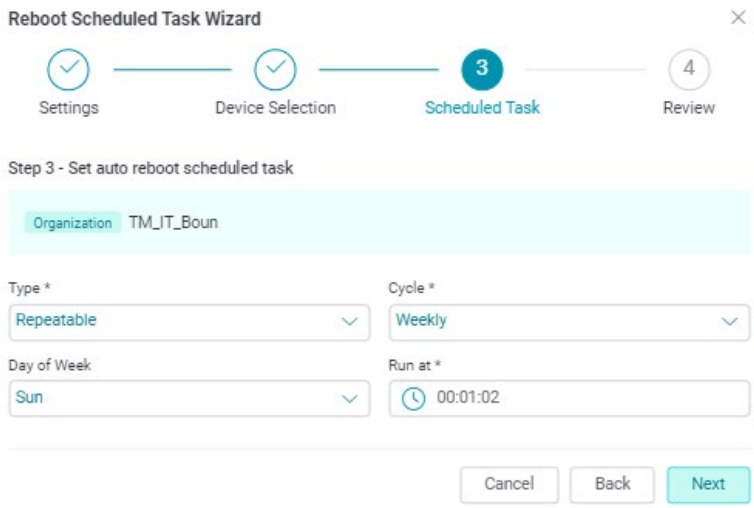
5. Select devices on which to perform the defined task. You can filter the devices using one or a combination of these properties: **Model** (only applicable with firmware upgrade and configuration deployment)**, Group, IMEI Range, MAC Address Range,** and **Tag**.
6. The number of selected devices will be displayed under **Effective Numbers.** You can click Details to show detailed device information. Then click **Next** to continue. Note that the effective number must be at least one or an error will be shown when submitting the task at the end of the configuration.



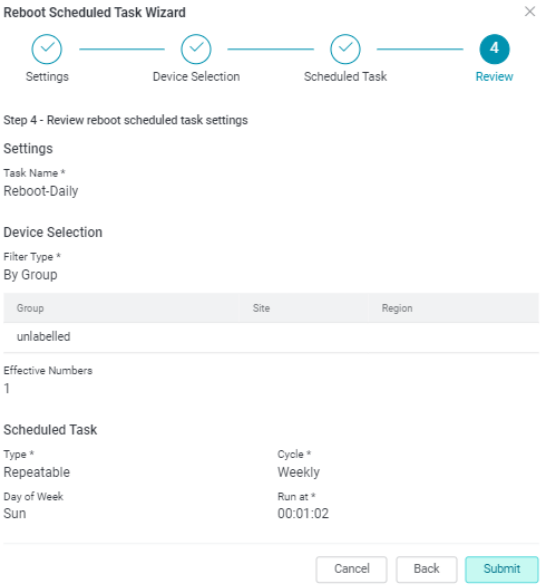
7. Select the timing for the task: **Now**, **Schedule**, or **Repeatable** (for Reboot only). Select **Now** to start the defined task immediately. Also select the number of times to execute this task (up to 10) with timed interval: 1 hour, 3 hours, or 6 hours. Select **Schedule** and define the **Start Time** (date and time) for this task. For multiple execute times, select the number of times (up to 10) to execute this task with the timed interval: 1 hour, 3 hours, or 6 hours. Note that if you select multiple times, you will see multiple entries for the same task. Select **Repeatable** and define the frequency of performing the automatic task from the **Cycle** drop-down menu: **Daily** or **Weekly**. For weekly, select the desired day of the week for the schedule. For both options, select the time to start the task with the 24-hour clock. Then click

Next to continue.

Note: The status of **Complete** refers to different configuration mechanism of scheduled tasks depending on the timing of the task. If the timing is **Now**, Complete status means that the task has been executed. If the timing is **Repeatable**, Complete status means the defined task has been programmed on the selected devices. (Please make sure that the repeatable task is what you intend before setting it.) For **Schedule** timing, Complete status means the defined task has been executed.



8. A Preview of the configured scheduled task will be displayed. Click **Submit** to finish the setting of scheduled task.



Tag Management

Tagging is useful in finding your devices as the number of your devices grows.
To view the configured tags, go to **Devices** > **Tag Management**.

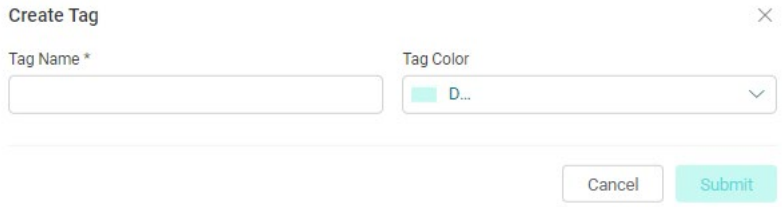
Note: Tag management is not granted to users with the monitor role by default.

The following information will be displayed:
Tag Name: Name of the tag.
Color: Color of the tag for better visibility.
Tagged Devices: Number of devices assigned with this tag.

You can edit a tag or delete it .

To create a tag:

Click Create Tag in the upper-right corner, enter a keyword in the **Tag Name** field, select the **Tag Color** for distinguishability, then click **Submit**.



To edit or delete a tag, select the tag, then click or respectively.

You can then use the pre-defined tag when adding tags to your devices (refer to **Tag a Device** in **Device Management**).

To list devices with a specific tag, click on the row of a tag name.

Upload OTA Files

The Upload OTA Files page allows you to upload and store firmware files for the system and device configuration files on the server in the cloud.

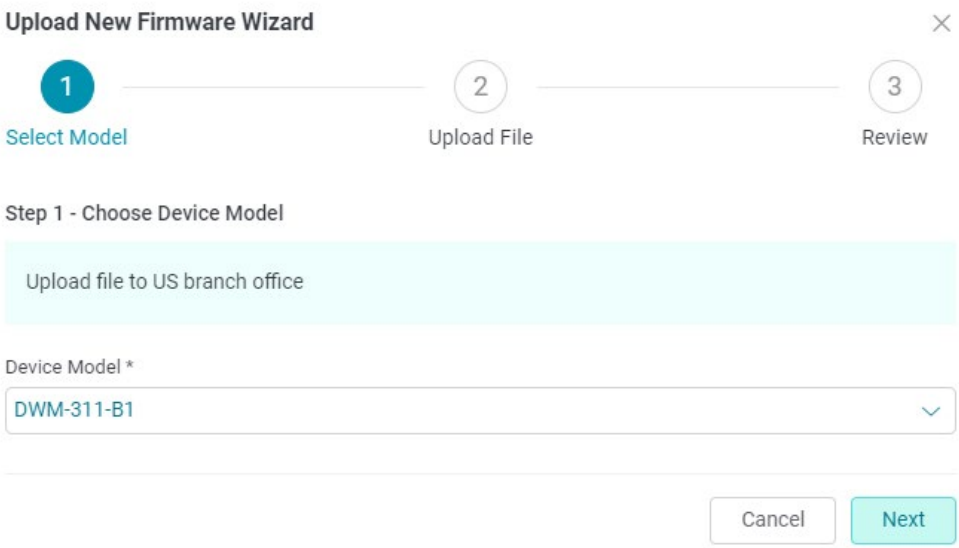
Upload Firmware File to the Server

Uploading firmware file to the server is required for subsequent firmware upgrade. (Go to **Device Management > Operations > Firmware Upgrade** and **Scheduled Tasks**.)

To upload firmware, go to **Devices > Upload OTA Files**:

1. From the **Upload OTA Files** at the left pane, click the **Device Firmware File** tab, choose the entity in the left pane to upload the file to, then click **Upload New Firmware**  button at the top right.

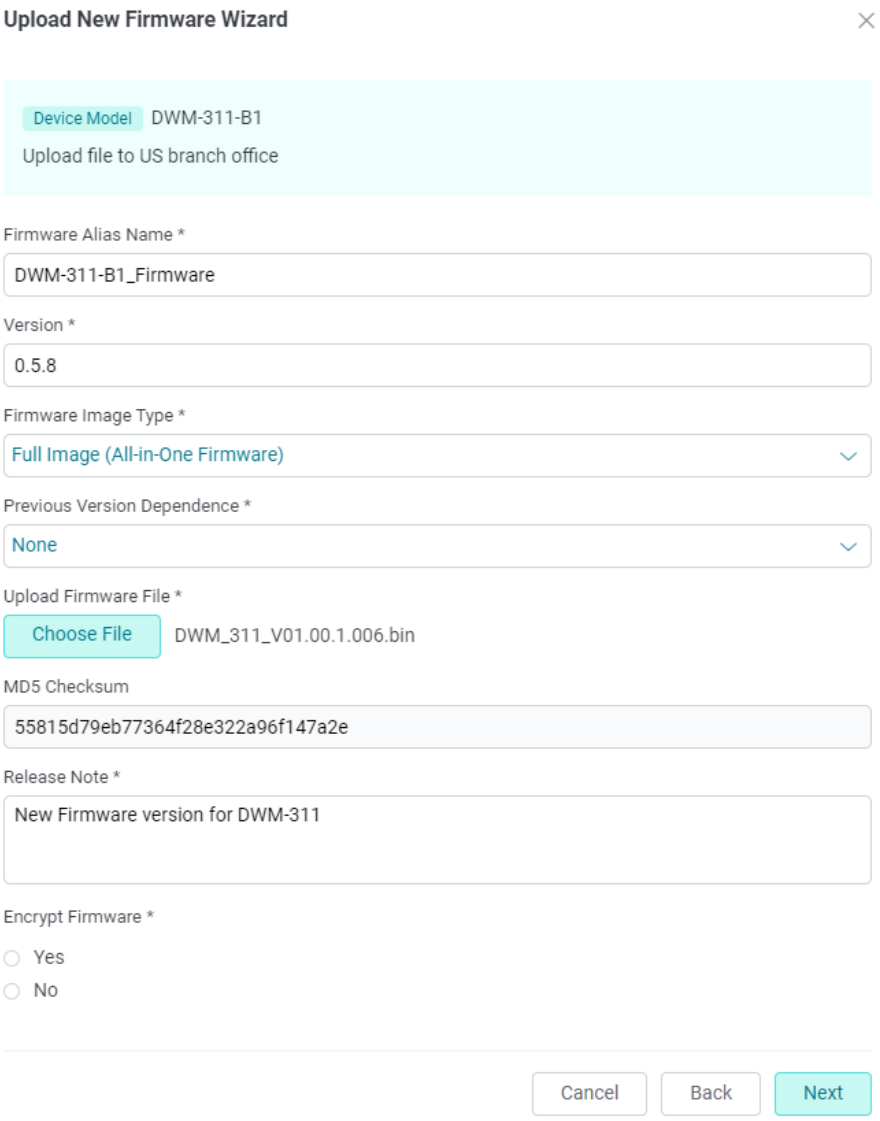
2. Choose the designated device model from the **Device Model** drop-down list. Click **Next** to continue.



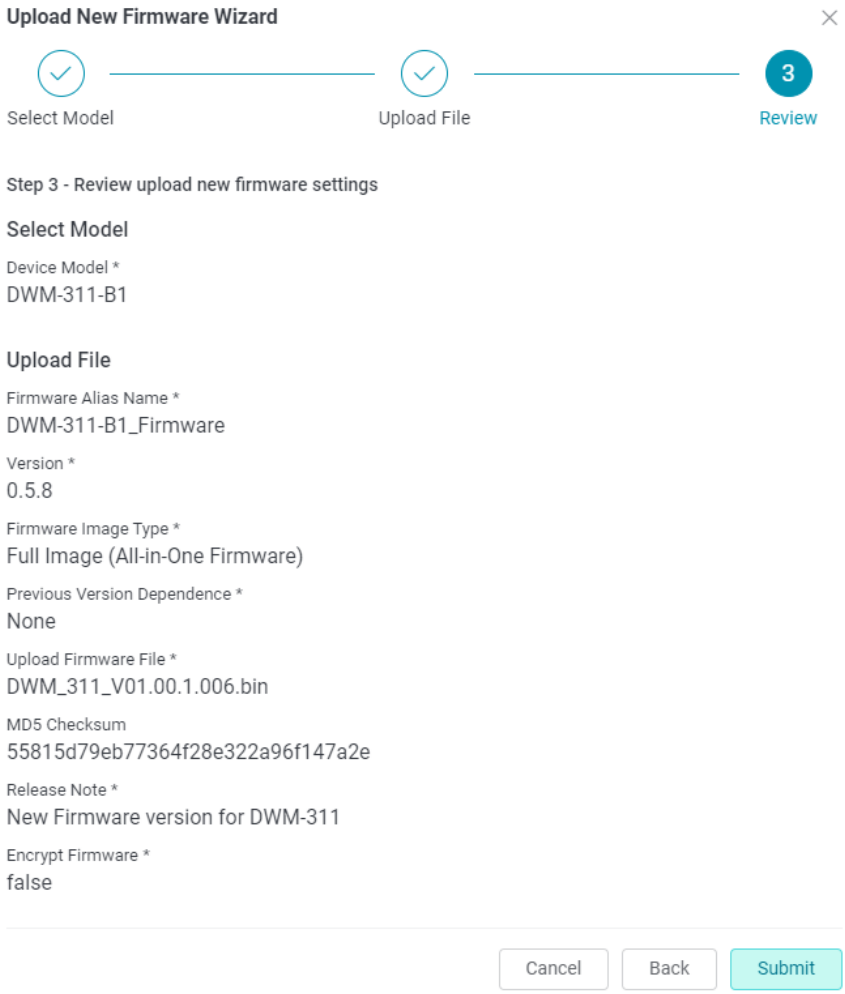
3. Enter a descriptive name for the firmware in the **Firmware Alias Name** field. The alias will be shown in the available firmware files for firmware upgrade (refer to **Firmware Upgrade** in **Device Management**) and Scheduled Tasks (refer to **Scheduled Tasks**).
4. State the **Version** number for the firmware. Select the **Firmware Image Type** from either one of the following: Full Image for complete image or Delta Image for incremental firmware image. Delta image reduces the size of the image file and therefore reduces network bandwidth requirement for faster

update delivery to accommodate frequent changes in firmware.

5. Select the **Previous Version Dependence** to specify the firmware dependency for the Delta Image firmware type.
6. Click **Choose File** to specify the firmware file to be uploaded.
7. The value for **MD5 Checksum**, calculated by system automatically, will be displayed. The MD5 checksum is used for verifying the integrity of the firmware file.
8. Write a note of the new firmware in the **Release Note** field.
9. Select whether the firmware file should be encrypted. (**Unless otherwise specified, do not encrypt the firmware**.)
10. Click **Next** to continue.



11. Review the information of the uploaded firmware image settings.
12. Click **Submit** to start uploading the firmware image.



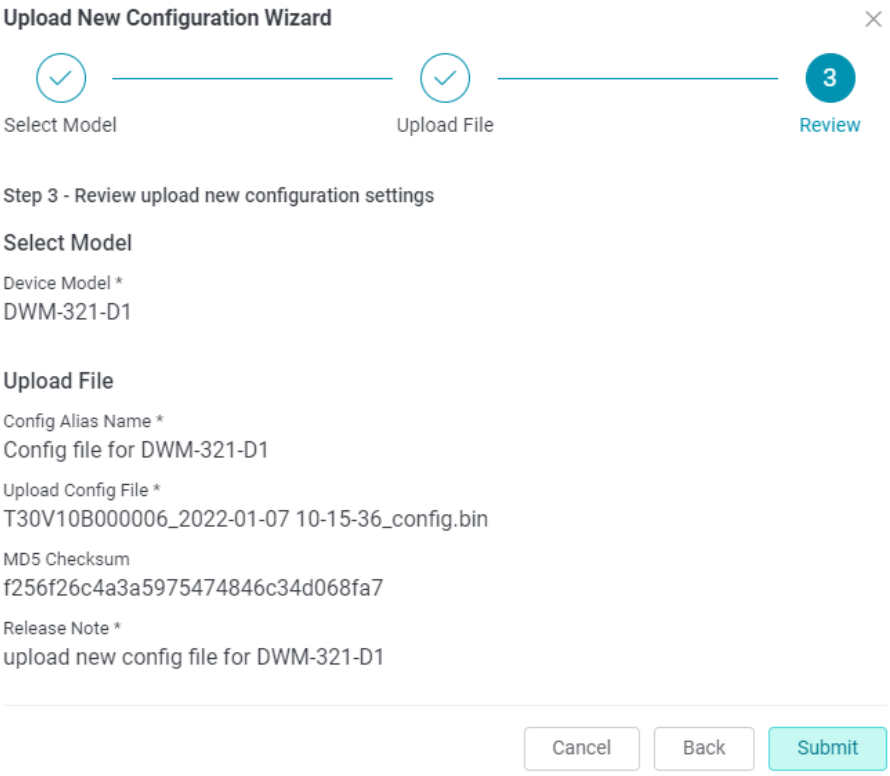
Upload Configuration File to the Server

Uploading configuration file to the server is required for subsequent import of system configuration.

1. At the **Upload OTA Files** tab from the left pane, click the **Device Config File** tab, then choose the entity in the left pane to upload the file to.
2. Click **Upload New Configuration** 

. The **Upload New Configuration Wizard** appears.
3. Select the model for configuration file upload from the **Device Model** drop-down menu, then click **Next**.
4. Fill in an alias from the configuration file. The alias will be shown in the available configuration files for Configuration Import (refer to **Configuration Import** in **Device Management**) and Scheduled Tasks (refer to **Scheduled Tasks**).
5. Upload the configuration file by clicking **Choose File** to locate and select the configuration file from your local directory.

6. The **MD5 Checksum** is displayed. The MD5 checksum is used for verifying the integrity of the configuration file.
7. Fill in the **Release Note** to describe this file.
8. Review the summary of the upload settings. Then click **Submit** to start the upload process.



Alert Rules

The **Alert Rules** page allows you to create rules to send email notifications automatically when devices' statuses change or when network traffic surpasses a certain level.

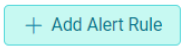
Note: Only administrators and managers can create alert rules by default.

The following information was displayed for alert rules created:
Rule Name: The name for the rule.
Rules: The condition of the rule.
Status: The status of the rule. **Complete** means the rule was effective in the past.
Running indicates the present time is within the duration of the effective time span.
Queuing indicates the alert rule is going to be effective in the future.
Period: The effective duration of the rule.

You can view detailed rule information by double-clicking on the rule.

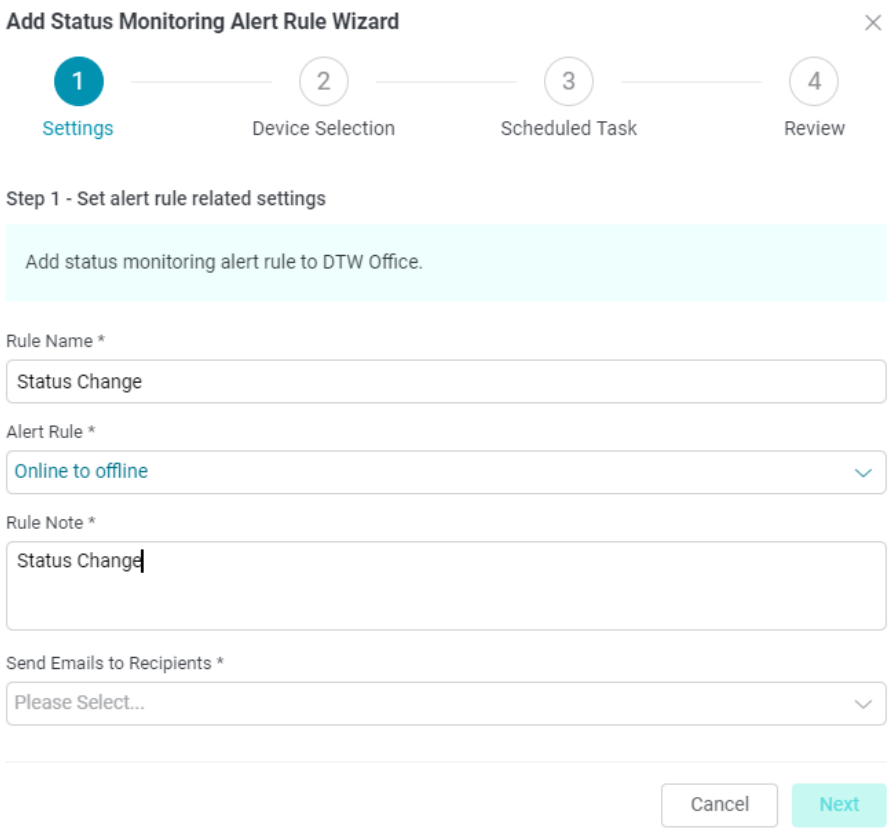
To create a rule, go to **Devices > Alert Rules**.

1. Choose the appropriate tab at the top: **Status Monitoring** or **Traffic Usage** to create alert rules for device status change or traffic growth.
2. Choose the appropriate organization from the left pane, then click **+Add Alert Rule**

   button at the top right. The **Add Status Monitoring Alert Rule Wizard** or **Add Traffic Usage Alert Rule Wizard** appears.
3. Fill in the following information for **Status Monitoring**:
   Rule Name: Give a name for this rule.
   Alert Rule: Select one of the following conditions for alert: **Online to offline**, **Offline to online**, or **Device status changed** for both states of status change.
   Rule Note: Write a brief description for this rule.
   Send Emails to Recipients: Select the available users which are the accounts of the respective organization from the drop-down list. You can select more than one user to be the recipients of the alert.
   Filter Type: Select the filtering criteria to filter the devices for the alert. You can select multiple criteria.
   The **Effective Numbers** shows the number of devices selected. To alter the list of

selected devices, click .



Or fill in the following information for **Traffic Usage**:

Rule Name: Give a name for this rule.

Interface Type: Select one of the available interfaces: **LAN**, **WAN**, **or WLAN**.

Channel: Select the available ports for the **LAN** interface and connection method for **WAN**. Or select the wireless frequency for WLAN.

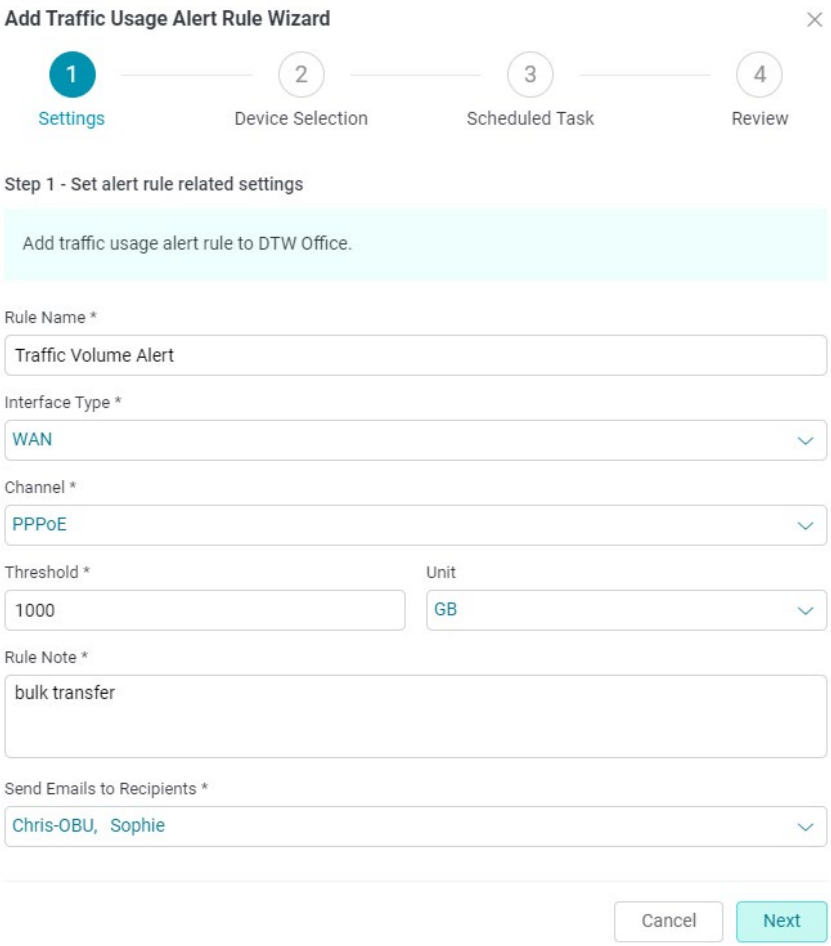
Threshold: Select the threshold value and the corresponding unit for triggering the alert.

Rule Note: Write a brief description for this rule.

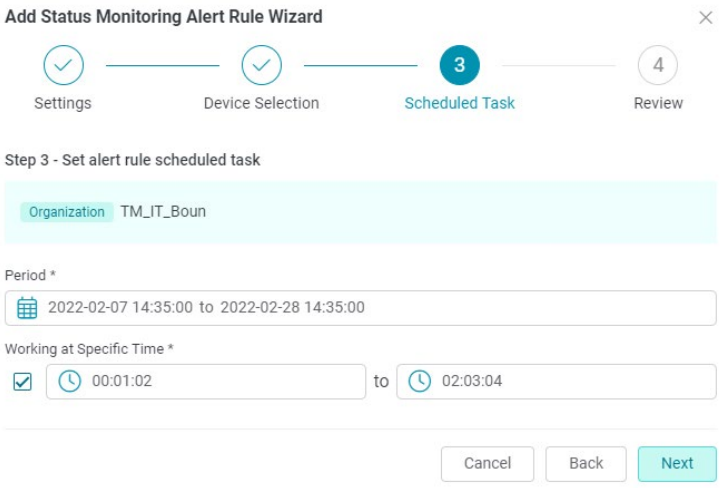
Send Emails to Recipients: Select the available users which are the accounts of the respective organization from the drop-down list. You can select more than one user to be the recipients of the alert.

Filter Type: Select the filtering criteria to filter the devices for the alert. You can select multiple criteria.

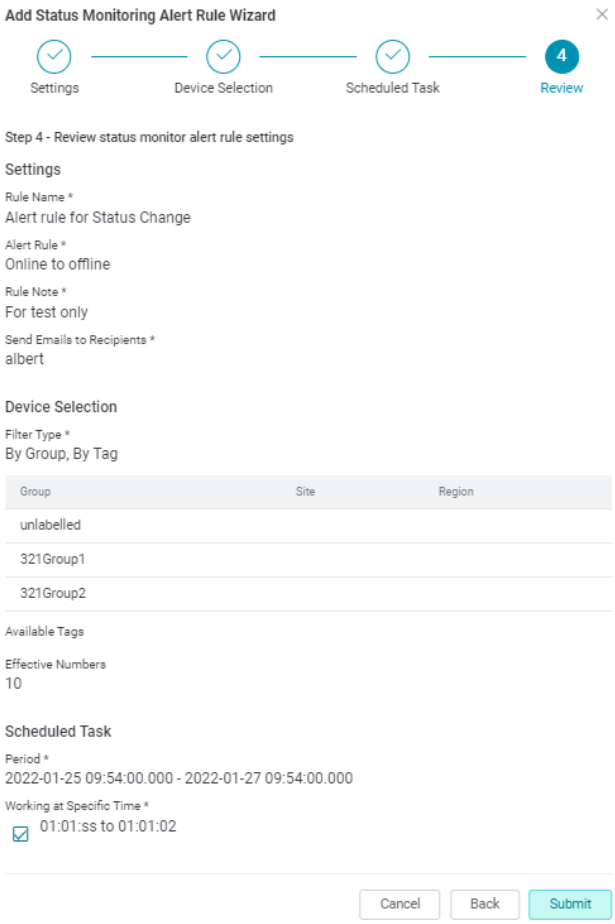
The **Effective Numbers** shows the number of devices selected. To alter the list of selected devices, click .



4. Select **Period** for the defined rule to be effective. Select **Working at Specific Time** to define the specific duration in 24-hour clock time that the alert rule will be applied every day in this defined time span. If you do not specify **Working at Specific Time**, you will receive alert notifications anytime during the day when the specified conditions are met.



5. A summary of the task will be displayed. Click **Submit** to finish the creation of the alert rule and close the wizard.


Add Status Monitoring Alert Rule Wizard
Settings
Device Selection
Scheduled Task
4
Review
Step 4 - Review status monitor alert rule settings
Settings
Rule Name *
Alert rule for Status Change
Alert Rule *
Online to offline
Rule Note *
For test only
Send Emails to Recipients *
albert
Device Selection
Filter Type *
By Group, By Tag
Group
Site
Region
unlabelled
321Group1
321Group2
Available Tags
Effective Numbers
10
Scheduled Task
Period *
2022-01-25 09:54:00.000 - 2022-01-27 09:54:00.000
Working at Specific Time *
01:01:ss to 01:01:02
Cancel
Back
Submit

Status Report Time

The Status Report Time page allows you to configure status report timing with the managed devices. There are 3 types of report timings that you can manage: **Periodic Report Time**, **Heartbeat Time**, and **Task Timeout Time**.

Periodic Report Time

Periodic Report Time sets the timing of the device status report for information about managed devices on the Device Management page, for instance, the connection parameters on the device details page (refer to **Details** in **Device Management**).

Model Name: The device model name.
Periodic Report Time: The time interval for sending the status report.
Last Applied Time: The time that the latest Periodic Report Time setting was applied. However, the value will be set on the device immediately only if the device is online. For offline devices, the value will be set once the devices become online.
Total Quantity: The number of devices that will be affected by the new timing.

You need first to add device model to the Periodic Report Time list:
Select the organization from the left pane and click **+Add Device to List** at the top right, then select the desired model from the available model list. This will add the periodic report timing of all the devices of the selected model to the designated organization. Note the **Total Quantity** column shows the number of affected devices.

To modify the periodic report time for a model:

1. Select the organization from the left pane and select desired model to be modified, click **Edit**  .
2. Select **Available Periodic Report Time** from the following options: Every 12 hours, Every 24 hours, Every 36 hours, and Customize (Minutes). For customized time, please enter a value larger than 1 minutes.
3. **Apply to All Online Devices:** Enable this option to overwrite the above report timing to all devices of this model when they become online. Disable this option to keep the default report timing of 24 hours.
4. Click **Submit** to apply the new settings.

Heartbeat Time

Heartbeat Time sets the timing of the heartbeat messages, which are used for communicating firmware version for firmware upgrade (refer to **Scheduled Tasks**).

The following information is displayed:
Model Name: The device model name.
Heartbeat Time: The time interval for sending the heartbeat message.
Last Applied Time: The time that the latest Heartbeat Time setting was applied. However, the value will be set on the device immediately only if the device is online. For offline devices, the value will be set once the devices become online.
Total Quantity: The number of devices that will be affected by the new timing.

To modify the heartbeat time for a model:

1. Select the desired model to be modified, then click **Edit**  **.**
2. Select **Available Heartbeat Time** from the following options: By 1 hour, By 3 hours, By 6 hours, By 12 hours, and Customize (Minutes). For customized time, please enter a value larger than 10 minutes.
3. Apply to All Online Devices: Enable this option to overwrite the above heartbeat timing to all devices of this model when they become online. Disable this option to keep the default heartbeat timing of 15 minutes.
4. Click **Submit** to apply the new settings.

Task Timeout Time

The Task Timeout Time sets the timeout value for scheduled tasks operation (refer to **Scheduled Tasks**).

The following information is displayed:
Model Name: The device model name.
Task Timeout Time: The timeout value for the scheduled task. The scheduled task will be aborted if it is not completed within this time.
Last Applied Time: The time that the latest Task Timeout Time setting was applied. However, the value will be set on the device immediately only if the device is online. For offline devices, the value will be set once the devices become online.
Total Quantity: The number of devices that will be affected by the new timing.

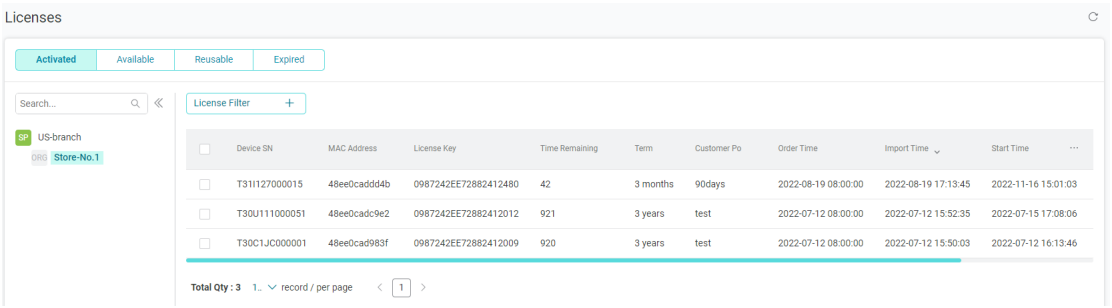
To modify the task timeout time for a model:

1. Select the desired model to be modified, then click **Edit**  **.**
2. Select **Available Task Timeout Time** from the following options: Within 15 minutes, Within 30 minutes, Within 45 minutes, Within 60 minutes, and Customize (Minutes). For customized time, please enter a value larger than 15 minutes. This timeout value applies to all scheduled tasks for the designated model.
3. **Apply to All Online Devices:** Enable this option to overwrite the above timeout timing to all devices of this model when they become online. Disable this option to keep the default timeout timing of 15 minutes.
4. Click **Submit** to apply the new settings.

Licenses

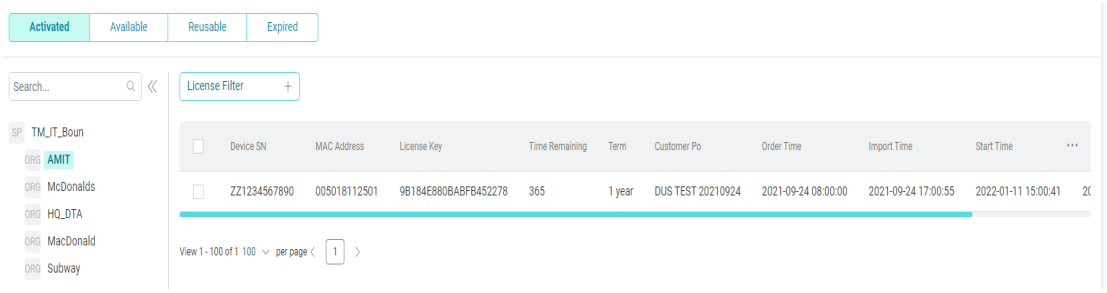
The **Licenses** page helps you track all licenses purchased for your devices. The devices managed by D-ECS are subscription-based products.

Note: Only administrators and managers have full access to license management by default.



Activated

To obtain devices that have a valid license, click the **Activated** tab. The following information is displayed:
Device SN: The serial number of the device.
MAC Address: The hardware address of the device.
License Key: The digital key for product subscription.
Time Remaining: The number of days left until the subscription expires.
Term: The period for the license.
Customer Po: Customer purchase order.
Order Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is purchased.
Import Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is imported to D-ECS.
Start Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the subscription starts.
Expiration Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the subscription ends.



Available

The Available licenses tab lists licenses that are purchased but have not been used by any device. The following information is displayed:

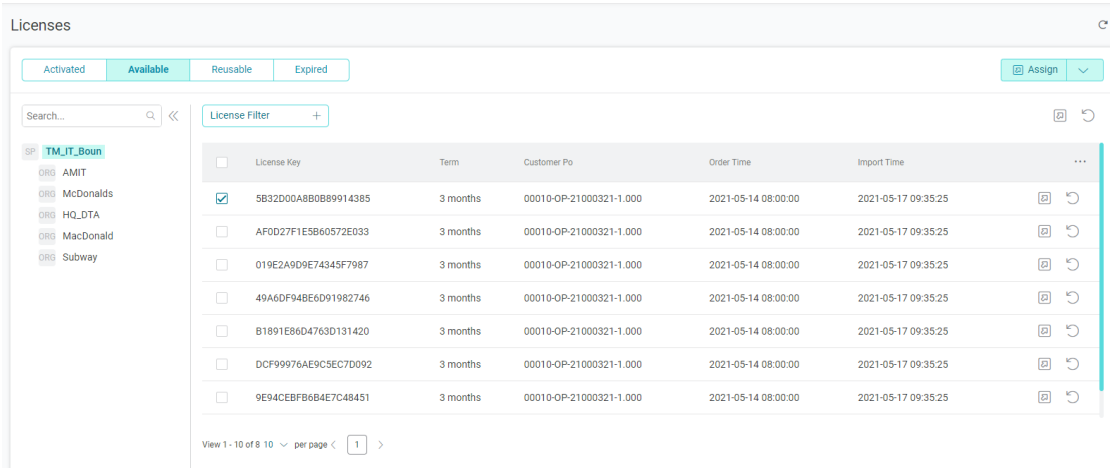
License Key: The digital key for product subscription.

Term: The period for the license.

Customer Po: Customer purchase order.

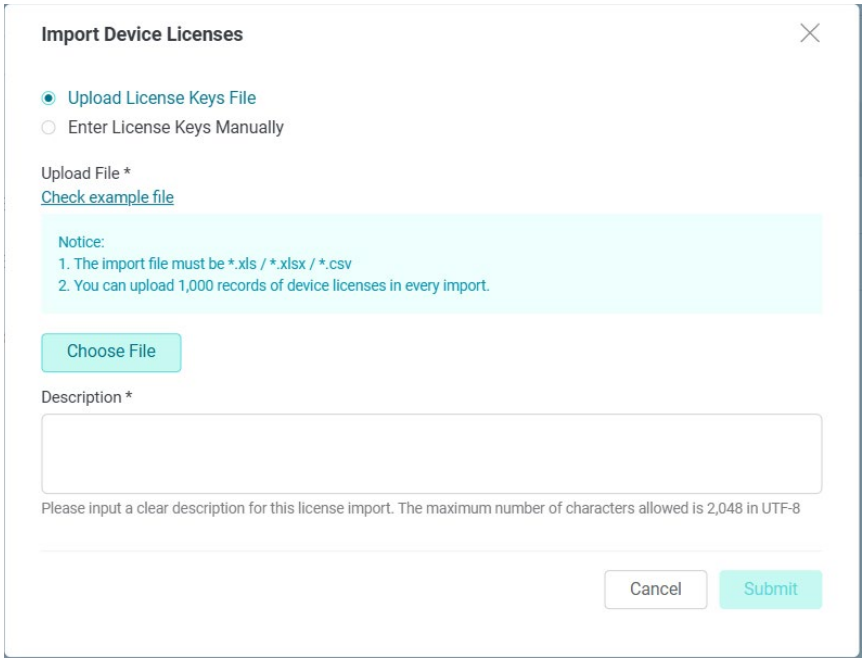
Order Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is purchased.

Import Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is imported to D-ECS. You can assign licenses to an organization to make them available for device activation for the assigned organization.

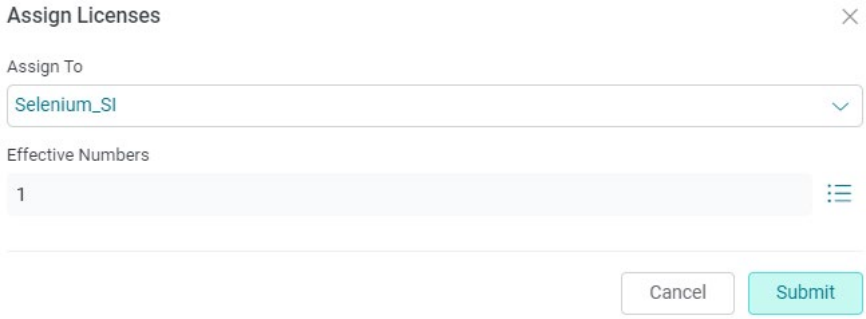


The system allows SP/ORG admins to import a device license. To import a license:

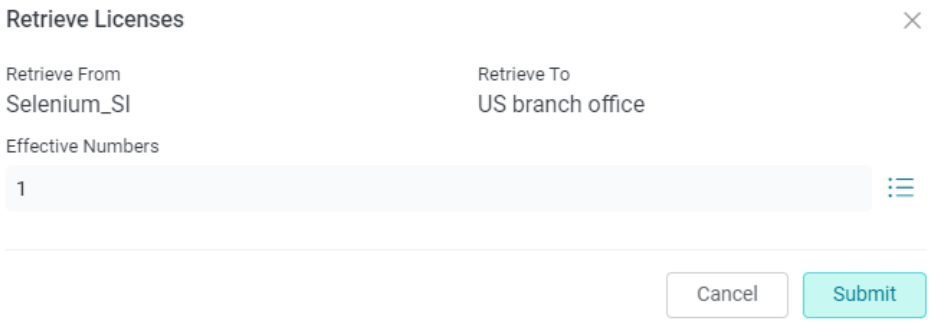
1. Click **Import Licenses** at the top right. The **Import Device Licenses** screen appears.
2. Chose **Upload Licenses Keys File** to upload a licenses keys file or **Enter Licenses Keys Manually** to enter licenses keys manually.
3. Enter a description for this import.
4. Click **Submit** to start the import process.



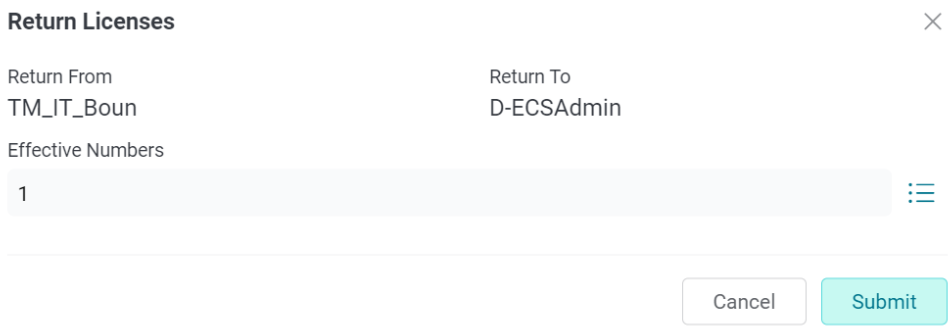
To assign a license, click the parent entity in the left pane, click on a license from the list and click **Assign to** . Then select a subordinate to dispatch the license to.



After a license has been assigned, you can revert the assignment by retrieving it. To retrieve a license, click on it and click **Retrieve License(s)** .



You can also return an assigned license to its original owner (i.e. a superior entity), To return a license, click **Return License(s)** :



Reusable

The Reusable tab lists licenses that are not currently activated but have remaining time from device deactivation (refer to **Deactivate a Device** in **Device Management**). Theses licenses can be used when you activate a device or reactivate a device. (Refer to **Inventory** and **Inactive** for more information.)

The following information is displayed:

License Key: The digital key for product subscription.

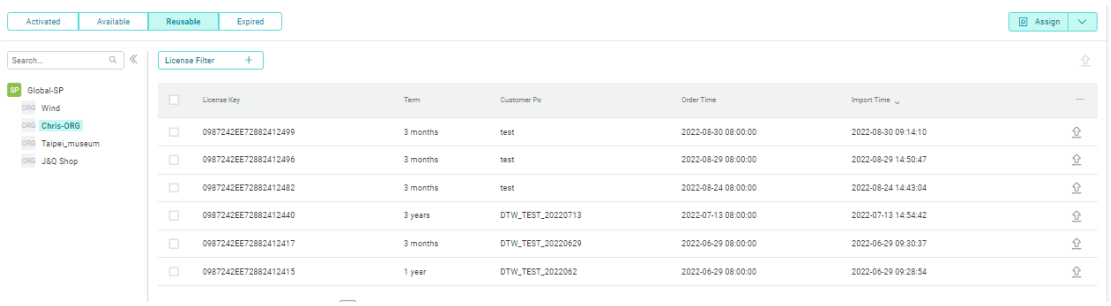
Term: The period for the license.

Customer Po: Customer purchase order.

Order Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is purchased.

Import Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is imported to D-ECS. You can assign licenses to an organization to make it available for device activation for the assigned organization.

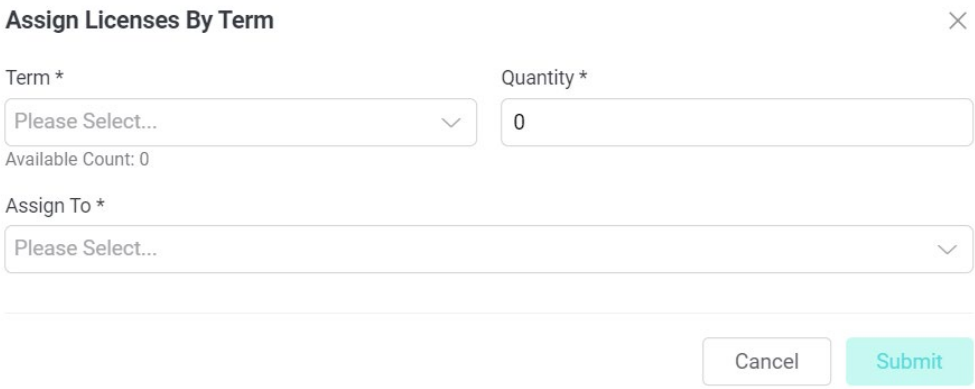
Time Remaining: The number of days left until the subscription expires.



Depending on the business entity that you have registered to, you can perform license retrieval, return, and assignment as instructed in the above topics for available licenses. In addition, you can perform group operation for licenses, for instance, to assign licenses by term, click **Assign** at the top of the table, the **Assign Licenses By Term** window appears:

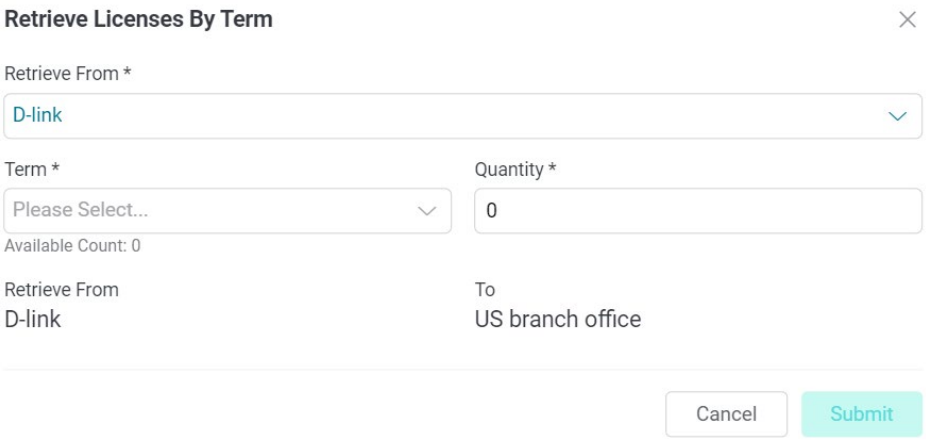
1. Select license term from the **Term** drop-down menu.

2. Select **Quantity**. Note that the available quantity depends on the available number of licenses with respect to the specified term.
3. Select a subordinate to dispatch the selected license(s).
4. Click **Submit.**



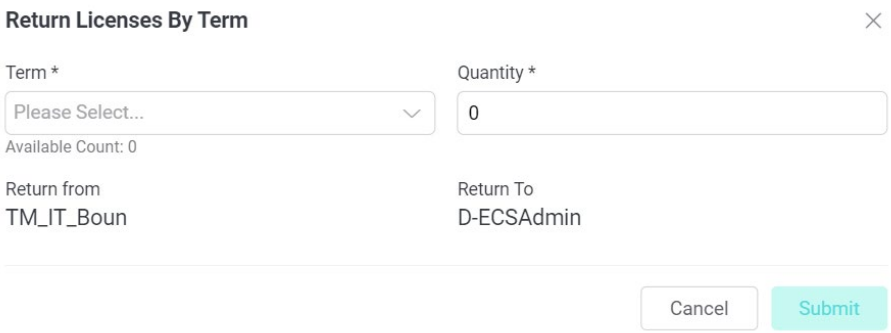
To retrieve licenses based on license terms, click **Retrieve** from the **Assign** button at the top of the table, the **Retrieve Licenses By Term** window appears:

1. Select a subordinate to retrieve the license from.
2. Select license term from the **Term** drop-down menu.
3. Select **Quantity**. Note that the available quantity depends on the available number of licenses with respect to the specified term.
4. Click **Submit**.



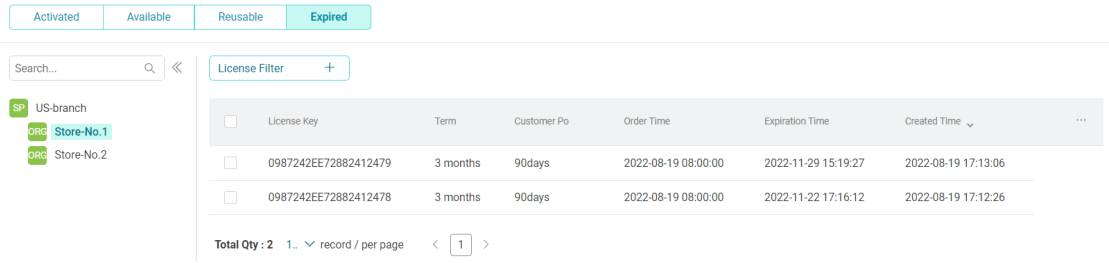
To return licenses based on license terms, click the **Return** from the **Assign** button at the top of the table, the **Return Licenses By Term** window appears:

1. Select license term from the **Term** drop-down menu.
2. Select **Quantity**. Note that the available quantity depends on the available number of licenses with respect to the specified term.
3. Click **Submit**.



Expired

The Expired tab lists licenses that are expired. The following information is displayed:
License Key: The digital key for product subscription.
Term: The period for the license.
Customer Po: Customer purchase order.
Order Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is purchased.
Created Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license is created.
Expiration Time: The date and time in yyyy-mm-dd, hours, minutes, and seconds when the license expires.

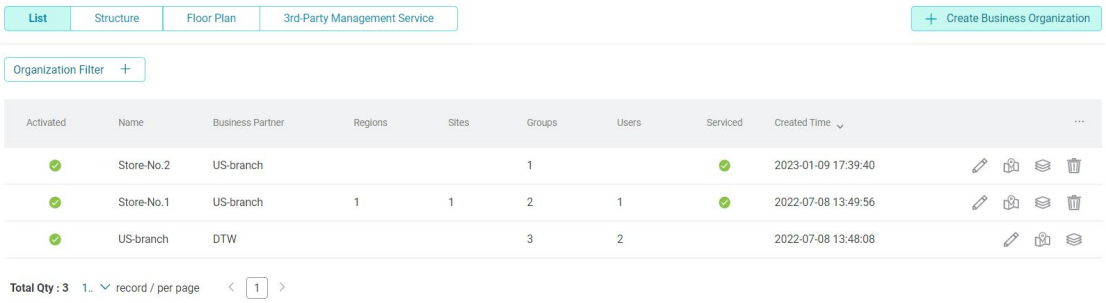


Organization

The Organization page displays the organizations composed of these entities: OBU, service providers, and organizations. The type of entities that you can view depending on the business entity that you have registered to. It allows you to create new entities as well as modify your existing ones.

Note: Only administrators and managers are allowed to create and maintain organizations on this page by default.

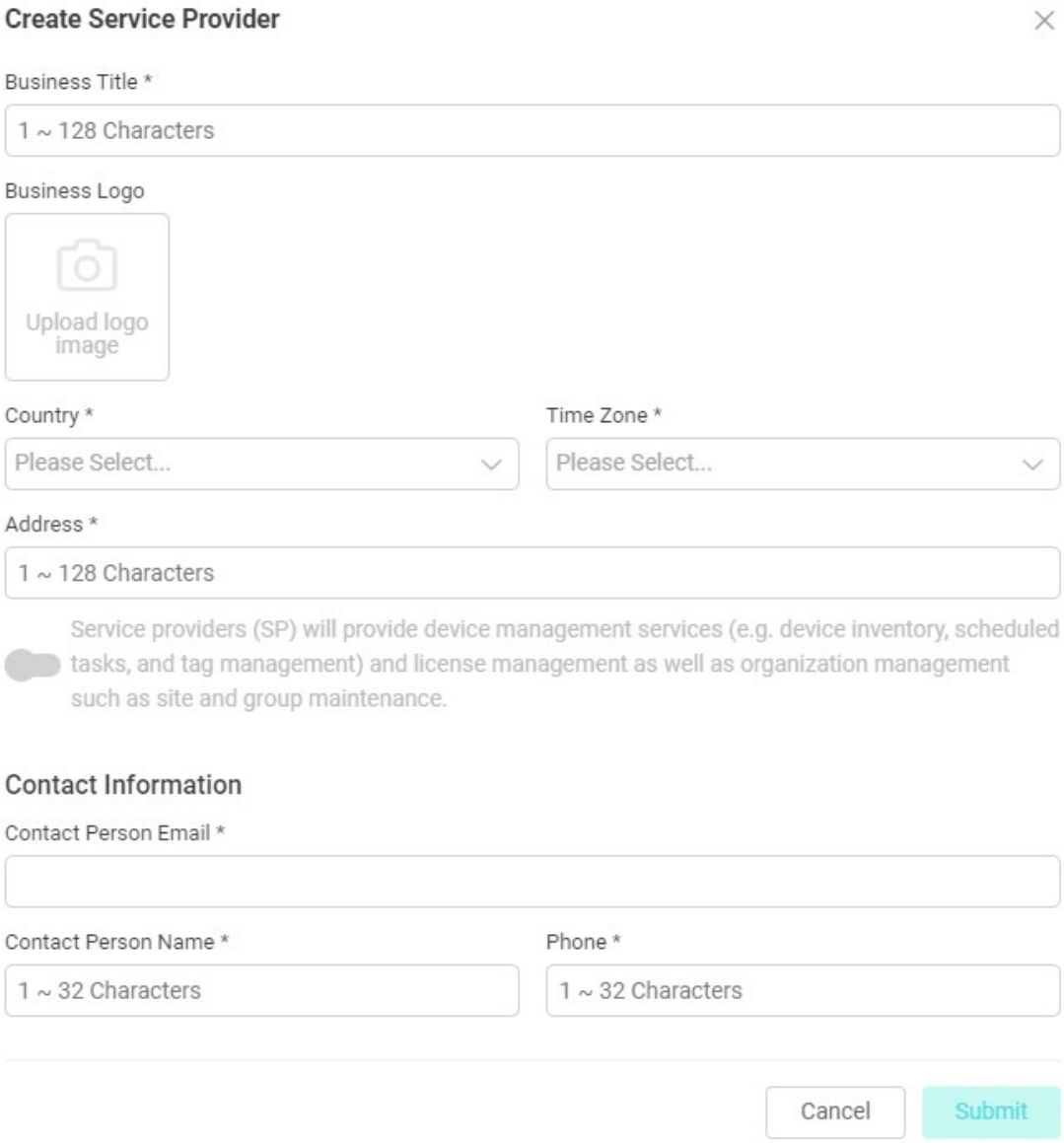
The following information is displayed:
Activated: Self-registered or invited D-ECS accounts must click on the verification link in the email to finish activation.
Name: The name of the organization.
Business Partner: The business entity that sold devices to the organization or the direct superior in the hierarchy.
Regions: The number of regions created under this business entity.
Sites: The number of sites created under this business entity.
Groups: The number of groups created under this business entity.
Users: The number of users that this business entity has.
Serviced: States whether a service provider (SP) will provide management services for its organizations encompassing device management services (e.g. device inventory, scheduled tasks, and tag management) and license management as well as organization management such as site and group maintenance.
Created Time: The time that the business entity was created.
You can customize the field by clicking …at the far right of the table.



Create Service Provider

Depending on your account and role (i.e. an OBU with the admin or manager role),

you can create a service provider (SP) by filling in the following information:



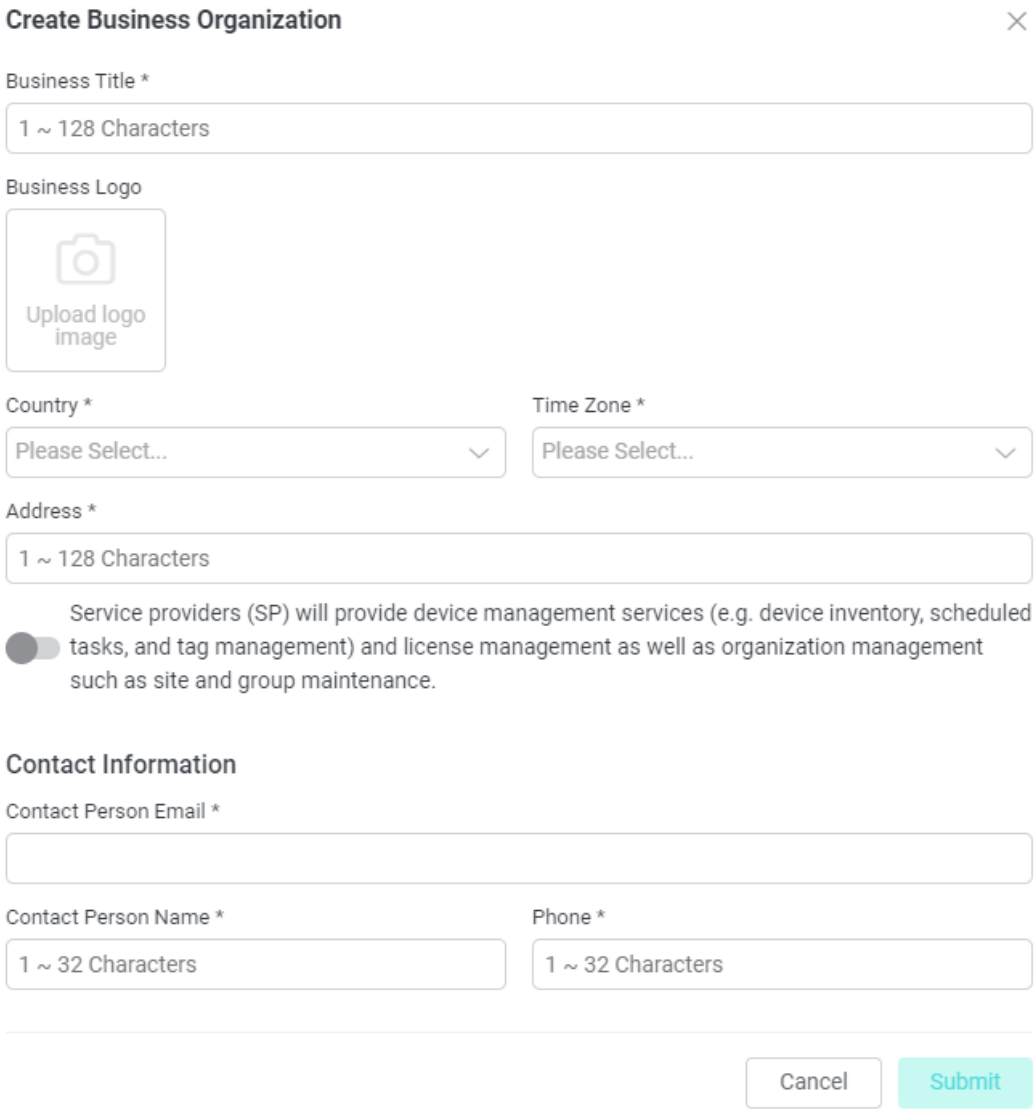
Business Title: Enter the name of the service provider, using a maximum of 128 alphanumeric characters.
Business Logo: Upload the company's logo with an image file of the PNG and JPG format with less than 2 megabytes in size.
Country: Select the country of the business organization.
Time Zone: Select the time zone of the business organization.
Address: Enter the address of the business site with street name, number, and state, using a maximum of 128 alphanumeric characters.

Enter the contact information which will be used to create an account in the system automatically with the admin role for managing the service provider:
Contact Information
Contact Person Email: Enter the email of the contact person.

Contact Person Name: Enter the name of the contact person.
Phone: Enter the phone number of the contact person.

Create Business Organization

Depending on your account and role (i.e. an SP with the admin or manager role), you can create a business organization (ORG) by filling in the following information:



Business Title: Enter the name of the business organization, using a maximum of 128 alphanumeric characters.
Business Logo: Upload the company's logo with an image file of the PNG and JPG format with less than 2 megabytes in size.
Country: Select the country of the organization.
Time Zone: Select the time zone of the business organization.
Address: Enter the address of the business site with street name, number, and state,

using a maximum of 128 alphanumeric characters.

Enable the following option to let the SP manage the organization and its assets: **Service providers (SP) will provide device management services (e.g. device inventory, scheduled tasks, and tag management) and license management as well as organization management such as site and group maintenance.** Once this option is enabled, it would be indicated in the organization list as **serviced** and the organization shown in the hierarchical representation of the left pane will be highlighted with a green node.

Contact Information
If you enable the above option, select contact person(s) that will be authorized to manage the organization. Furthermore, the contact person(s) account should be created and activated in advance under the respective service provider (SP). The number of contact people will be reflected in the **Organization Account Summary Organization Account Summary** of the dashboard.

If you *do not* enable the above option, enter the following contact information which will be used to create an account with the admin role automatically in the system to manage the business organization:

Contact Information
Contact Person Email: Enter the email of the contact person.
Contact Person Name: Enter the name of the contact person.
Phone: Enter the phone number of this contact person.

Note: If you later enable the above option to allow a service provider (SP) to manage an organization and its assets, the above account of a contact will be disabled from the system, which prevents its login to the system.

Organization Details

The **Organization Details** page provides both tabular and structural representation of the information on the organization. It consists of the following tabs: List, Structure, and Floor Plan.

List

The **List** tab displays business entities that are managed by the account user. It may contain entities such as service providers (SP), organizations (ORG) or operation

business unit (OBU) depending on the level of the hierarchy of the account user's registered entity. For example, if the account user is registered as an SP, the list may contain organizations that are managed by the parent SP. The table displays the following information:

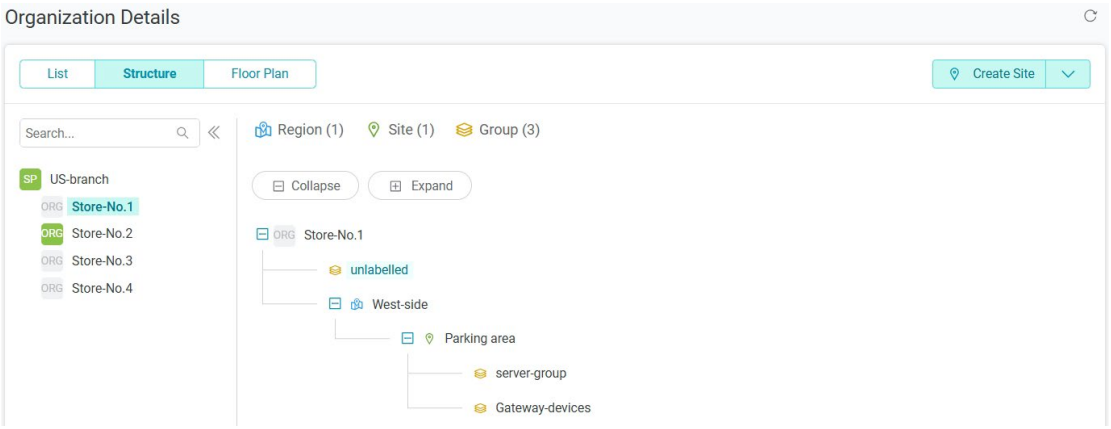
Activated: Self-registered or invited D-ECS accounts must click on the verification link in the email to finish activation.
Name: The name of the organization.
Business Partner: The business entity that sold devices to the organization or the direct superior in the hierarchy.
Regions: The number of regions created under this business entity.
Sites: The number of sites created under this business entity.
Groups: The number of groups created under this business entity.
Users: The number of users that this business entity has.
Serviced: States whether a service provider (SP) will provide management services for its organizations, including device management services (e.g. device inventory, scheduled tasks, and tag management) and license management as well as organization management such as site and group maintenance. This information will also be reflected in the **Organization Account Summary** of the dashboard.
Created Time: The time that the business entity was created.

You can customize the field by clicking …at the far right of the table. Depending on your permission role (i.e. Admin and Manager only by default), you can edit an entity or create regions or sites under this entity. To delete an entity, you need to be a superior in the hierarchy. (Refer to **Structure** below for site and region creation.)

Structure

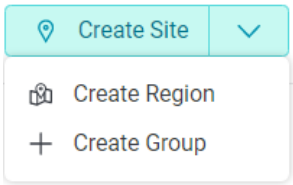
The **Structure** tab displays the hierarchical representation of physical locations. It uses regions, sites, and groups to give geographical visualization of devices under a business entity. If you are a service provider, organizations shown in the left pane with green nodes allow you to maintain their regions, sites and groups; on the other hand, organizations shown in the left pane with gray nodes prevent management from a service provider.

Note: Users with the monitor role cannot create or maintain regions or sites by default.



Region

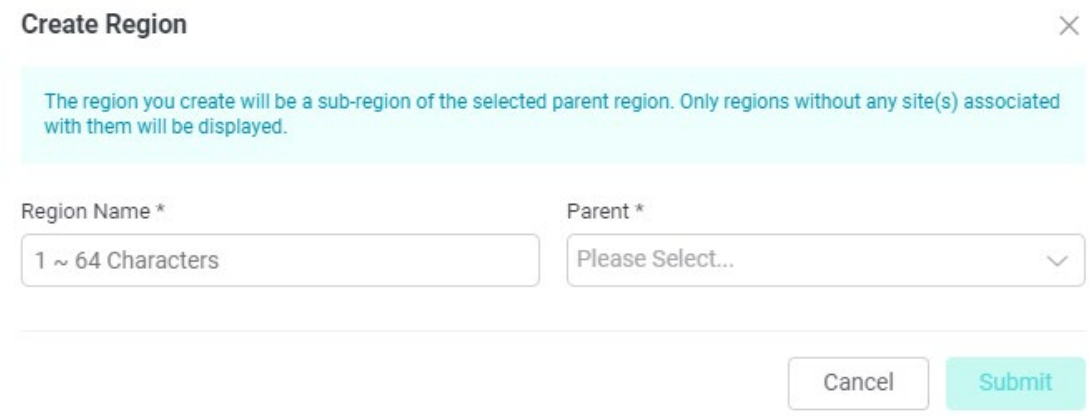
Regions denote geographic divisions of a business entity. They have a broader perspective than sites. An organization can have multiple regions and sites to represent its physical locations. For example, a company may have many branch offices (site) in different parts of the world (region).

To create a region, click **Create Region** 

in the upper-right corner. The **Create Region** screen appears, fill in the following information to create a new region:

Region Name: Name this region. Enter alphanumeric characters with a maximum of 64 characters.

Parent: Select the parent region for this region from available regions under this organization. You can create a region directly under the intended organization or under any region (but not a site) contained within this organization.



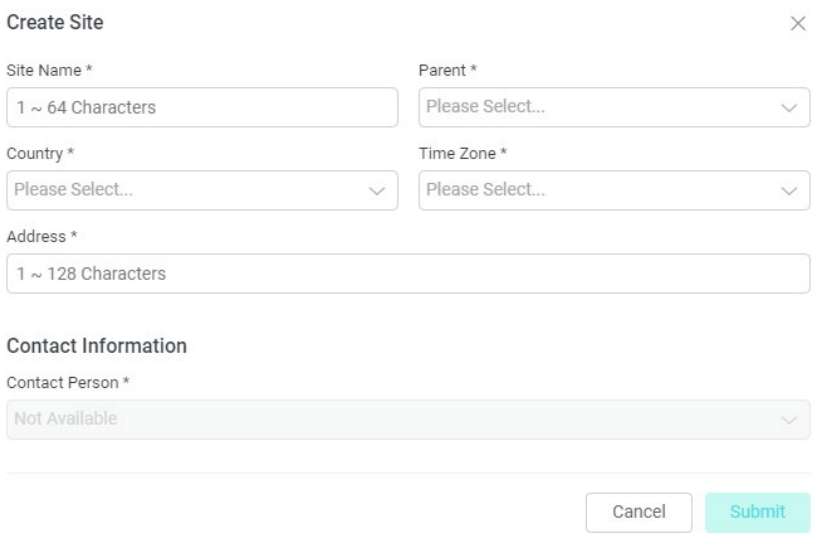
Site

Sites are placed under a region or directly under a business entity. Unlike a region, a site details location addresses of devices under an organization.

To create a site, click **Create Site** 

in the upper-right corner. The **Create Site** screen appears, fill in the information to create a new site.

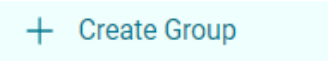
Site Name: Name this site. Enter alphanumeric characters with a maximum of 64 characters.
Parent: Select the region to which the site belongs.
Country: Select the country of the site.
Time Zone: Select the time zone of the site.
Address: Enter the address of the site with street name, number, and state, using a maximum of 128 characters.
Contact Person: Select one of the user accounts created for the organization to be the contact person.



Group

Group allows you to divide the devices in the organization into groups. You can organize your devices into groups based on physical placement (under a site) or functional perspective (under a business entity, i.e. service providers or organizations) according to your needs. After a group is created, you can then move a device to the group (refer to **Move Devices to a Group** in **Device Management**).

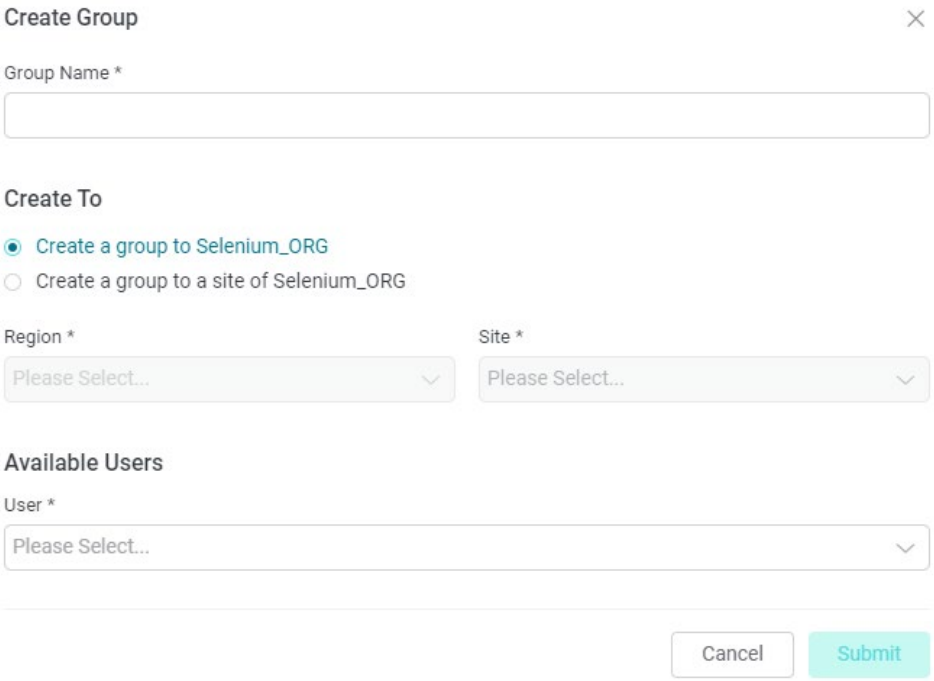
Note: Group management is not granted to users with the monitor role by default.

To create a group, click **Create Group**  in the upper-right corner. The **Create Group** screen appears, fill in the information to create a new group.

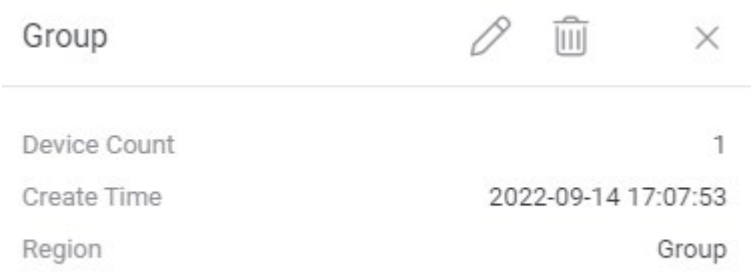
Group Name: Name the group.

Create to: Select either to place the group under the organization (parent entity) or a physical site of the organization. If you select **Create a group to a site**, select a region from the list of available regions under the organization and the designated site for the group.

Available Users: Select a user whose role does not inherently permit group management (i.e. monitor) from the list to allow management of the group and devices assigned to the group to this user.



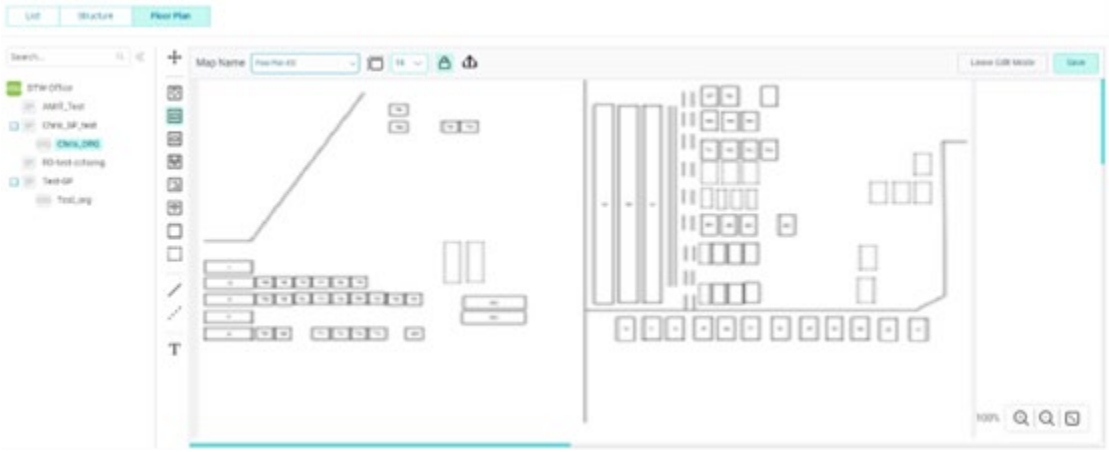
After a group is created, click on it to display options: Edit Group  and Delete Group  .



Note: A Group cannot be deleted if there are devices assigned to that group.

Floor Plan

The Floor Plan tab allows you to visualize the location of the managed devices on a site map. It helps visualize the geographic data of your devices to allow for quick identification of the location of the devices on the deployment site.

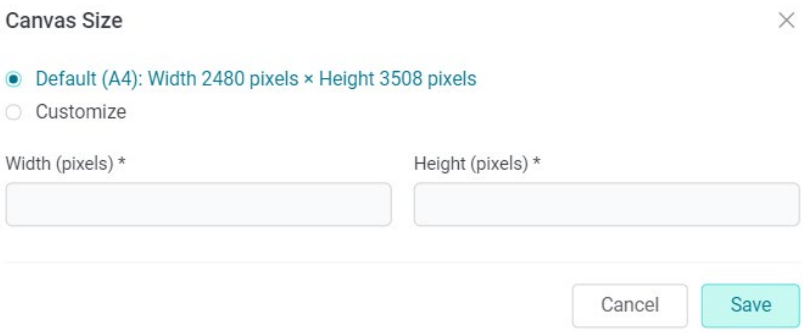


Note: Users with the monitor role cannot create or maintain regions or sites by default.

To create a floor plan:

1. Click **Start** in the middle of the screen or click **+ Add a new floor plan** at the top.

   The screen shows a blank canvas. To change the canvas size, click  and specify the width and height in pixels.

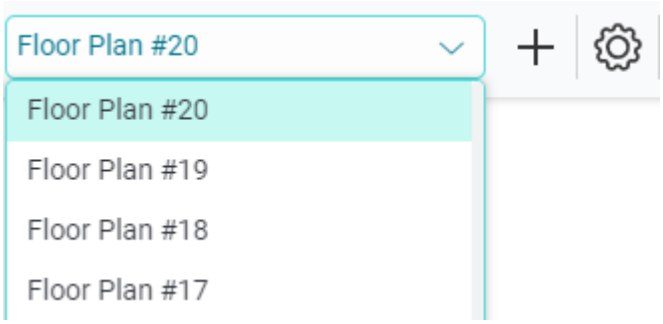


2. Click  to upload an image of the deployment site from your local drive.

   Note that it must be in JPG, JPEG, or PNG file format. Then click  to lock the background image from being reshaped and moved around on the canvas.

3. Click  or  to create an object on the canvas to identify your device (you may also use other provided device icons) and drag it around to reflect its position on the site. You may also use the available symbols for your devices.

   Then click  to enter a descriptive name for this device. Use Move  to move your objects on the canvas.
4. Right-click on the created object and click **Device Type** to select the device's type. Right-click on the created object and click **Link with** to select a device from the device list for the organization. Once a device is linked successfully, the object will be in different colors to inform you of its status, for example, green for online and gray for offline.
5. Click **Save** to save your drawing. Then click **Leave Edit Mode** to view your drawing.
6. In the View mode, you can create additional plans by clicking  and manage your existing plans by clicking  . To view and edit other plans for an organization, select the desired plan from the list of available plans.



Organization Users

This page allows you to manage all your users. You can create, edit, and delete users. You can use role-based access control to provide users with a subset of privileges to access the system instead of making them full local administrators.

To add a user on the server:

1. Click **Organization > Organization Users**, then select the **All Users** tab. Select the organization whose assets the user should have permission to access.
2. Click **Add User**  in the upper-right corner, and enter the following information:
   Name: Enter a username.
   Phone: Enter the contact phone number.
   Email: Enter the contact email.
   Role: Select the permission role. Refer to the following descriptions of different levels of access roles.
3. **Managed Site / Group:** Select the device group that can be managed by the user. This option is not available for creating an administrator.
4. Click **Submit**.

Note: You can only create users with the **Admin** role for a subordinate. Users with roles other than the **Admin** can only be created by an administrator within the same organization.

After users are created, they will receive invitation emails that will provide verification links for account activation.

You can also modify the information of a user by clicking  in the upper-right corner of the specific user. The options include View Profile, Edit, Resend Welcome Email and Delete User. The **Edit** option allows you to modify user information about the user as described in the above user creation settings. The **View Profile** option displays the information of the user including his organization, phone number, time that this user was created, his account email, and groups that he is allowed to manage. The **Resend Welcome Email** sends the invitation email again for the user to activate his account. The **Delete User** option removes this user.

The system supports the following roles:

Admin: This role can manage all members except administrators of its organization, including granting and revoking privileges. The admin account can only be created by a superior of the D-ECS hierarchy. For example, an administrator of an organization can only be created by an administrator or a manager from a service provider (SP). Likewise, an administrator of a service provider (SP) can only be created by an administrator or a manager from an operation business unit (OBU).

The following table describes the default set of privileges for the Admin role:

Privilege Category	**Privileges**	**Enabled by Default**
Device Diagnostic Test	Perform diagnostics on devices (refer to **Diagnostics** in **Device Management**).	Yes
Device Operations	Perform operations on devices including tasks in device management such as device tagging, group assignment, device activation and deactivation and license extension (refer to **Navigate through the Device Management** and **Operations** in **Device Management**).	Yes
Device Import	Perform device import to the inventory tab (refer to **Inventory** in **Device Management**).	Yes
License Management	License management functions such as license delivery, deletion, and retrieval (refer to **Licenses**).	Yes
User Management	User management functions such as adding, deleting, or modifying users (refer to **Organization Users** in **Organization**).	Yes
Organization	Organization management	Yes

Management	functions such as adding, deleting, modifying organizations as well as associated region/site/group management (refer to **Organization**).	
Scheduled Task Management	Create and cancel scheduled tasks (refer to **Scheduled Tasks** in **Devices**).	Yes
Alert Rules	Create and delete alert rules to monitor device status and traffic usage (refer to **Alert Rules** in **Devices**).	Yes
Status Report Time	Set up automatic status reporting (refer to **Status Report Time** in **Devices**).	Yes

Manager: A manager can also manage all members of its organization except the administrators and other managers. The following table describes the default set of privileges for the Manager role:

Privilege Category	Privileges	Enabled by Default
Device Diagnostic Test	Perform diagnostics on devices (refer to **Diagnostics** in **Device Management**).	Yes
Device Operations	Perform operations on devices including tasks in device management such as device tagging, group assignment, device activation and deactivation and license extension (refer to **Navigate through the Device Management** and **Operations** in **Device Management**).	Yes
Device Import	Perform device import to the inventory tab (refer to **Inventory** in **Device**	Yes

	Management).	
License Management	License management functions such as license delivery, deletion, and retrieval (refer to **Licenses**).	Yes
User Management	User management functions such as adding, deleting, or modifying users (refer to **Organization Users** in **Organization**).	Yes
Organization Management	Organization management functions such as adding, deleting, modifying organizations as well as associated region/site/group management (refer to **Organization**).	Yes
Scheduled Task Management	Create and cancel scheduled tasks (refer to **Scheduled Tasks** in **Devices**).	Yes
Alert Rules	Create and delete alert rules to monitor device status and traffic usage (refer to **Alert Rules** in **Devices**).	Yes
Status Report Time	Set up automatic status reporting (refer to **Status Report Time** in **Devices**).	Yes

Supervisor: A supervisor cannot manage any member of its own organization. The following table describes the default set of privileges for the Supervisor role:

Privilege Category	**Privileges**	**Enabled by Default**
Device Diagnostic Test	Perform diagnostics on devices (refer to **Diagnostics in Device Management**).	Yes
Device Operations	Perform operations on devices including tasks in device	Yes

	management such as device tagging, group assignment, device activation and deactivation and license extension (refer to **Navigate through the Device Management** and **Operations** in **Device Management**).	
Device Import	Perform device import to the inventory tab (refer to **Inventory** in **Device Management**).	No
License Management	License management functions such as license delivery, deletion, and retrieval (refer to **Licenses**).	No
User Management	User management functions such as adding, deleting, or modifying users (refer to **Organization Users** in **Organization**).	No
Organization Management	Organization management functions such as adding, deleting, modifying organizations as well as associated region/site/group management (refer to **Organization**).	Yes
Scheduled Task Management	Create and cancel scheduled tasks (refer to **Scheduled Tasks** in **Devices**).	Yes
Alert Rules	Create and delete alert rules to monitor device status and traffic usage (refer to **Alert Rules** in **Devices**).	No
Status Report Time	Set up automatic status reporting (refer to **Status Report Time** in **Devices**).	Yes

Monitor: A monitor cannot manage any member of its own organization. The following table describes the default set of privileges for the Monitor role:

Privilege Category	Privileges	Enabled by Default
Device Diagnostic Test	Perform diagnostics on devices (refer to **Diagnostics in Device Management**).	No
Device Operations	Perform operations on devices including tasks in device management such as device tagging, group assignment, device activation and deactivation and license extension (refer to **Navigate through the Device Management** and **Operations** in **Device Management**).	No
Device Import	Perform device import to the inventory tab (refer to **Inventory** in **Device Management**).	No
License Management	License management functions such as license delivery, deletion, and retrieval (refer to **Licenses**).	No
User Management	User management functions such as adding, deleting, or modifying users (refer to **Organization Users** in **Organization**).	No
Organization Management	Organization management functions such as adding, deleting, modifying organizations as well as associated region/site/group management (refer to **Organization**).	No
Scheduled Task	Create and cancel scheduled	No

Management	tasks (refer to **Scheduled Tasks** in **Devices**).	
Alert Rules	Create and delete alert rules to monitor device status and traffic usage (refer to **Alert Rules** in **Devices**).	No
Status Report Time	Set up automatic status reporting (refer to **Status Report Time** in **Devices**).	No

Permission

To display the permission of a user based on its role, go to **Organization > Organization Users**, then select the **Permission** tab. Function access rights are displayed in headings to show the corresponding privileges for each role.
The function access rights are explained below:

Device Diagnostic Test	Perform diagnostics on devices (refer to **Diagnostics** in **Device Management**).
Device Operations	Perform operations on devices including tasks in device management such as device tagging, group assignment, device activation and deactivation and license extension (refer to **Navigate through the Device Management** and **Operations** in **Device Management**).
Device Import	Perform device import to the inventory tab (refer to **Inventory** in **Device Management**).
License Management	License management functions such as license delivery, deletion, and retrieval (refer to **Licenses**).
User Management	User management functions such as adding, deleting, or modifying users (refer to **Organization Users** in **Organization**).
Organization Management	Organization management functions such as adding, deleting, modifying organizations as well as associated region/site/group management (refer to **Organization**).
Scheduled Task Management	Create and cancel scheduled tasks (refer to **Scheduled Tasks** in **Devices**).
Alert Rules	Create and delete alert rules to monitor device status and traffic usage (refer to **Alert Rules** in **Devices**).
Status Report Time	Set up automatic status reporting (refer to **Status Report Time** in **Devices**).

Activity Log

The Activity Log page displays all of devices' logs. The User Activity tab displays logs related to management operations and tasks performed by users. The Device Activity displays logs related to activities performed by system services and agents. Logs can be used to analyze device health and troubleshoot network connectivity as well as exam network security.

Note:
You can only view logs pertaining to the activities under your own organization. However, an account of a superior can view logs from its subordinates.

To view **User Activity** logs, click **Activity Log > User Activity**. The log entries contain the following information:
User – Username.
Email – Email of the user account.
Role – Privilege role of the user.
Activity – Operations performed by the user, e.g. device import, ping or trace route.
Info – Detailed descriptions of the activity.
Time – The timestamp of the user activity.

You can filter these logs based on username and time. To create a filter, click

at the top of the table.

To view **Device Activity** logs, click **Activity Log > Device Activity**. The log entries contain the following information:
Device Name – The name of the device.
Serial Number – Serial number of the device.
Model – Model name of the device.
IP Address – IP address assigned to the interface.
Severity – The degree of criticality.
Activity – Operations performed by the device, e.g. heartbeat received or reboot.
Time – The timestamp of the device activity.

You can filter these logs based on username and time. To create a filter, click

at the top of the table.

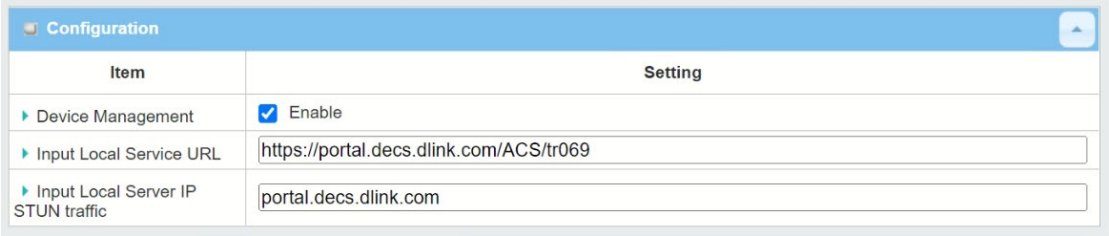
The following describes the log severity level from the highest to the lowest:

Critical	Indicates that the system is in critical condition when there are errors, failed operations, lost connections, etc.
Warning	Indicates conditions that may lead to errors, for example heartbeat timeout.
Normal	Indicates a normal condition when there are complete operations, heartbeat signal received, etc.

Appendix

Device registration allows D-ECS to manage the device and control some settings on the device. For supported devices, go to **Devices > Device Profile**.
To register devices to D-ECS, you need to configure the relevant settings in the device configuration page as shown below:

Item	**Setting**
Device Management	Select **Enable** to allow management by D-ECS
Input Local Service URL	Input the management service URL: https://portal.decs.dlink.com/ACS/tr069
Input Local Server IP STUN Traffic	Input the server address for processing STUN traffic: portal.decs.dlink.com
Note: The service URL and Server IP STUN Traffic should be modified accordingly depending on the deployment architecture of the D-ECS system.	



Revision Note

FW Version	Revision No.	Description	Date
V1.2.4.2.20230106	V1.50	● Modify menu icon ● Modify the minimum value for the periodic report time interval ● Delete Device Profile page	2023/01/09
V1.2.4.5.20230509	V1.51	● Take out the Wi-Fi AP and switch product category	2023/05/12
V1.3.0.0.20241203	V1.60	● Modify D-ECS cloud icon ● Remove obsolete features.	2024/12/05