MULTITECH®

DeviceHQ®

User Guide

DeviceHQ User Guide

Part Number: S000755 Rev. 1.6

Copyright

This publication may not be reproduced, in whole or in part, without the specific and express prior written permission signed by an executive officer of Multi-Tech Systems, Inc. All rights reserved. **Copyright © 2026 by Multi-Tech Systems, Inc.**

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

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

Trademarks and Registered Trademarks

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

Disclaimers

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

Legal Notices

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

MULTITECH DOES NOT WARRANT THAT THE TRANSMISSION OF DATA BY A PRODUCT OVER A WIRELESS COMMUNICATIONS NETWORK WILL BE UNINTERRUPTED, TIMELY, SECURE, OR ERROR FREE, NOR DOES MULTITECH WARRANT ANY CONNECTION OR ACCESSIBILITY TO ANY WIRELESS COMMUNICATIONS NETWORK. MULTITECH WILL HAVE NO LIABILITY FOR ANY LOSSES, DAMAGES, OBLIGATIONS, PENALTIES, DEFICIENCIES, LIABILITIES, COSTS, OR EXPENSES (INCLUDING WITHOUT LIMITATION REASONABLE ATTORNEYS FEES) RELATED TO TEMPORARY INABILITY TO ACCESS A WIRELESS COMMUNICATIONS NETWORK USING THE PRODUCTS.

The MultiTech products and the final application of the MultiTech products should be thoroughly tested to ensure the functionality of the MultiTech products as used in the final application. The designer, manufacturer, and reseller has the sole responsibility of ensuring that any end-user product into which the MultiTech product is integrated operates as intended and meets its requirements or the requirements of its direct or indirect customers. MultiTech has no responsibility whatsoever for the integration, configuration, testing, validation, verification, installation, upgrade, support, or maintenance of such end-user product, or for any liabilities, damages, costs, or expenses associated therewith, except to the extent agreed upon in a signed written document. To the extent MultiTech provides any comments or suggested changes related to the application of its products, such comments or suggested changes is performed only as a courtesy and without any representation or warranty whatsoever.

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

Contact Information

General Information	info@multitech.com https://multitech.com/contact-us/
Sales	+1 (763) 785-3500 sales@multitech.com
Technical Support Portal	+1 (763) 717-5863 https://support.multitech.com
Website	www.multitech.com
World Headquarters	Multi-Tech Systems, Inc. 2205 Woodale Drive Mounds View, MN 55112 USA

Contents

1 Overview 7
About this Document 7
Architecture Overview 7
Supported Devices 7

Chapter 2 Getting Started 9
Creating a DeviceHQ Account 9
Creating Account and Device Keys 9
Activating a Login 11
Logging In 11
Logging in for the First Time 11
Logging in with Multi-Factor Authentication (MFA) 12

Chapter 3 Setting up an mPower Device for Use with DeviceHQ 14
Managing Your Device Remotely 14

Chapter 4 Setting up an MTR5, MTR6, MTE, or MTE2 for Use with DeviceHQ 16

Chapter 5 Working with Devices 18
Device Page 18
Filtering the Device List 18
Grouping Devices 19
Editing Device Information 19
Deleting a Device 20
Viewing Device Details 20
Upgrade Manager 20
Understanding Check-In Intervals 21
Deleting Multiple Devices 21

Chapter 6 Scheduling Tasks 22
Scheduling Device Actions 22
Abort Actions 22
Through the Device List 22
Through the Device Information Window 22
Updating Firmware 22
Scheduling Firmware Updates 23
Through the Device Information Window 23
Scheduling Radio Firmware Updates 24
Through the Device List 24

Through the Device Information Window 24
Upgrading Device Configuration File 24
Through the Device List 25
Through the Device Information Window 25
Partial Configuration Updates 25
Through the Device List 25
Through the Device Information Window 26
Settings 26
Rebooting Devices 26
Through the Device List 26
Through the Device Information Window 27
Managing Upgrades 27
Using an Upgrade Manager 28
Using the Upgrade Manager Status Page 28
Managing Upgrade Managers 29
Requesting and Downloading Device Logs 30
Through the Device List 30
Through the Device Information Window 30
Downloading Device Logs 30
Scheduling Regular Device Log File Uploads 31
Installing an App 31
Through the Device List 31
Through the Device Information Window 32
Uninstalling an App 32
Through the Device List 32
Through the Device Information Window 33
Uninstalling an App 33
Through the Device List 33
Through the Device Information Window 33
Verifying an Application on Your Conduit Device 34

Chapter 7 Files 35
Files 35
Firmware File Fields 35
Configuration File Fields 35
Updating Firmware 35
Scheduling Firmware Updates 36
Through the Device Information Window 36
Configuration Files 37
Uploading Configuration Files 37
Deleting a Configuration File 37

Deleting Configuration Files from the Files Page 37
To Delete a Configuration File from the Device Files Tab: 38
Editing a Configuration File 38
Download Configuration File 38
Downloading a Configuration File from the Files Page 38
Downloading a Configuration File from the Device Information Window 38
Using as a Template for a New Configuration File 39
Firewall 39
Firewall Configuration 39
Connection Tracker 40
Port Forwarding 40
Input Filter Rules 40
Output Filter Rules 41
Advanced Firewall Configuration 42
Prerouting Rule (DNAT) 42
Forward Filter Rules 43
Postrouting Rules (SNAT) 44
Setting up Static Routes 45
Trusted IP 45
Wireless Configuration 46
Wi-Fi Access Point 46
Wi-Fi as WAN 47
Bluetooth IP 47
Using IP Pipe in TCP/UDP Client mode 48
Using IP Pipe in TCP/UDP Client Mode 48
Configuring security settings 49
Bluetooth Low Energy 49
Deleting Firmware Files 49
Deleting a Firmware File from the Files Page 50
Deleting a Firmware File from the Device Information Window 50

Chapter 8 Admin 51
User Administration 51
Adding Users 51
Editing Existing User Information 51
Deleting User Accounts 52
Notifications 52
Notification Types 52
Notifications Page Fields 52
Creating Notifications 52
Setting Up Recipient Groups 53

Device Reboot Notification Settings 53
Failed Actions Notification Settings 53
High Data Use Notification Settings 54
Low Signal Notification Settings 54
Missed Check-in Notification Settings 55
Device Logs Page 55
Device Logs Requests 55
Device Logs 55

Chapter 9 Store 57

Chapter 10 Developer 58
Accessing the DeviceHQ Developer Page 58
Developer Page 58
Downloading the Custom App Template 58
Adding an Application to the App Store 58
Editing an App 59
Deleting an App 59

Revision History 61

1 Overview

DeviceHQ® is a cloud-based toolset for managing the latest generation of MultiTech devices. It allows users to remotely monitor, upgrade, and configure an entire device population. DeviceHQ takes remote device management and maintenance to a new level, by providing an application marketplace, allowing users to browse applications or build their own then easily deploy and customize them for remote devices.

About this Document

This user guide includes chapters on using the device's user interface to configure it for use with DeviceHQ as well as how to use the system.

Architecture Overview

Once a device is configured to communicate with DeviceHQ, it periodically sends device information and statistics to the cloud platform and checks for firmware and/or configuration updates to download. The frequency with which devices connect to the platform is configurable on a per-device basis.

Important: Devices do not maintain a persistent connection to the platform. Pending actions, such as firmware and configuration updates, are applied to the device only when it checks into the platform. A "live" connection does not exist and historical device statistics, such as signal level, are recorded at the time the device checks in.



Figure 1 shows a high level overview of the platform.

Supported Devices

Manage the following products with DeviceHQ:

- Conduit 300 Series (MTCDT3AC)
- Conduit (MTCDT)

- Conduit IP67 Base Station (MTCDTIP)
- Conduit IP67 Base Station 200 Series (MTCDTIP2)
- Conduit AP (MTCAP and MTCAP2)
- MultiConnect rCell 100 series (MTR)
- MultiConnect rCell 500 series (MTR5)
- MultiConnect rCell 600 Series (MTR6)
- MultiConnect eCell (MTE and MTE2)

Note: This document collectively refers to the MTCDT, MTCDTIP, MTCAP, and MTCAP2 as Conduit products.

To manage these devices in DeviceHQ, enable remote management on the device. For MTR, MTCDT, MTCDT3AC, MTCDTIP, MTCDTIP2, MTCAP, and MTCAP2, refer to Setting up an mPower Device for Use with DeviceHQ. For MTR5, MTR6, and MTE, refer to Setting up an MTR5, MTR6, MTE, or MTE2 for Use with DeviceHQ.

Chapter 2 Getting Started

Creating a DeviceHQ Account

To use DeviceHQ, create an account:

1. Go to **devicehq.com**
2. Click **Register Account**.
3. Complete the registration form.
4. Read the End User License Agreement (EULA) and then check **Accept EULA**.
5. Enter the CAPTCHA text into the text box.
6. Click **Create Account**.

   MultiTech sends an email to verify to confirm account creation.
7. In the verification email, click to activate your account.

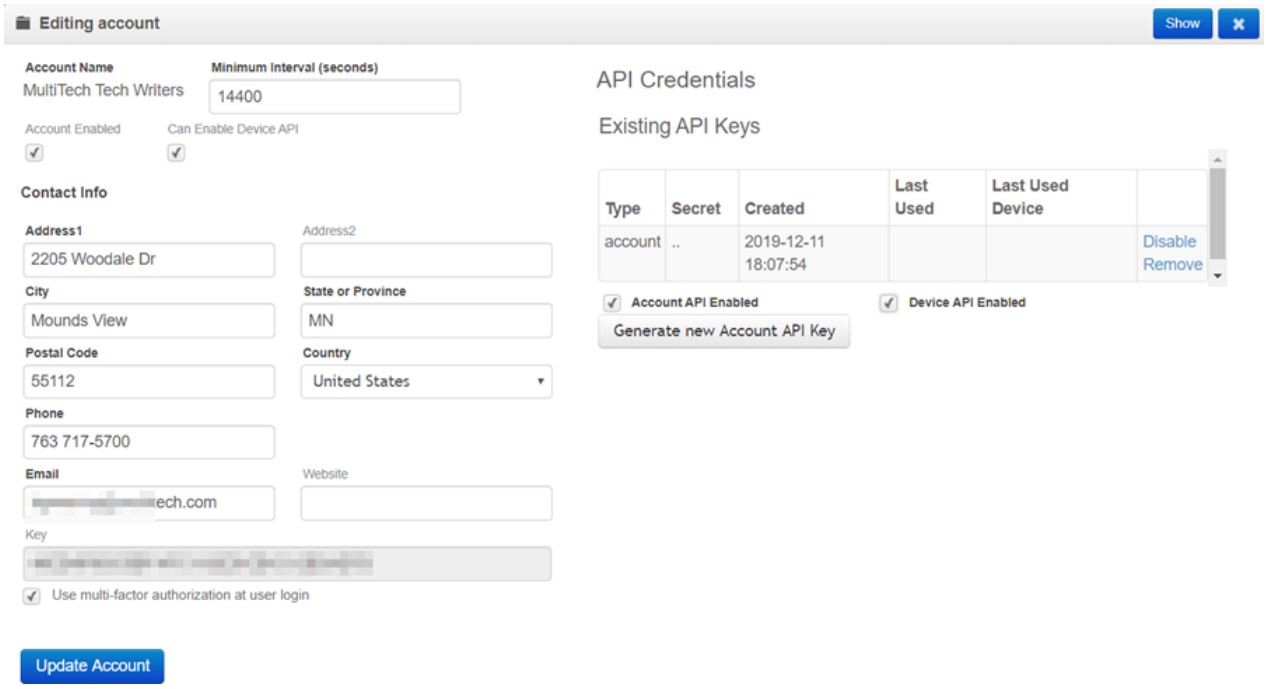
Creating Account and Device Keys

To create account and device keys:

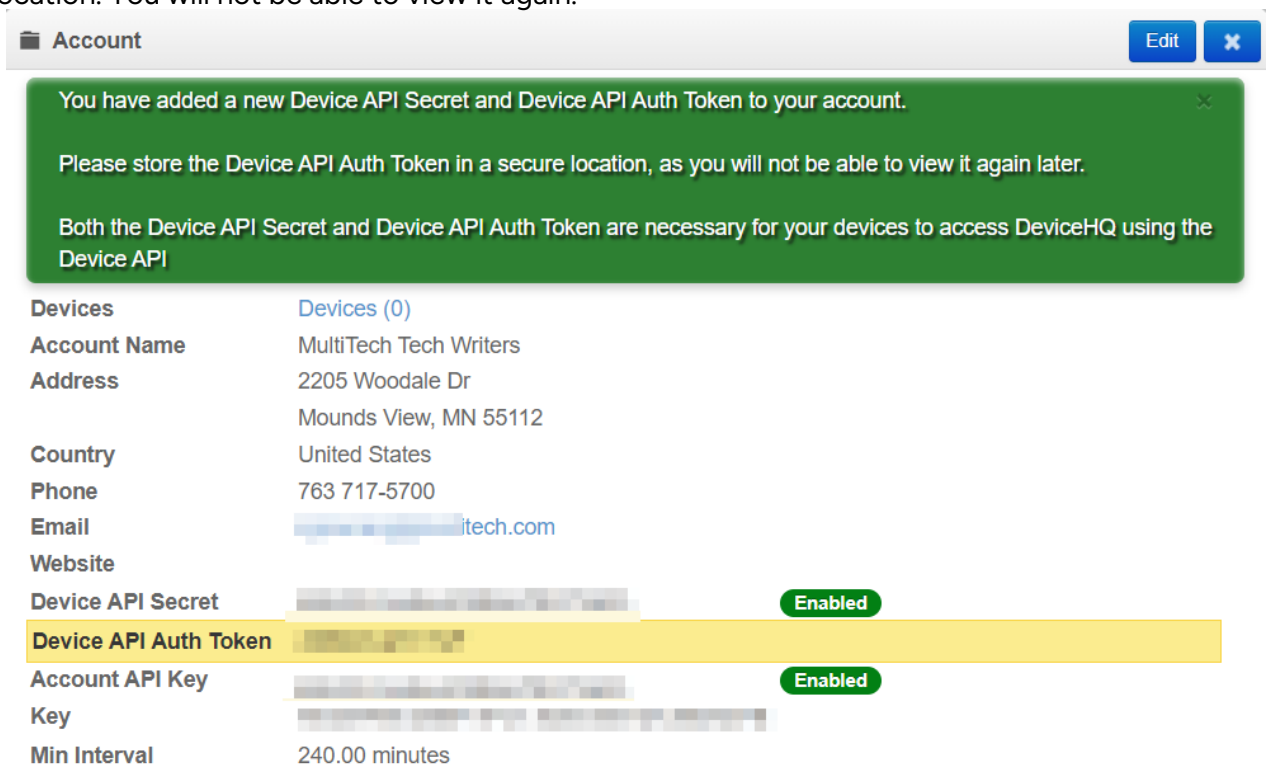
1. If you are not logged in, log in to DeviceHQ.
2. Click on your **email address** in the upper right hand corner.



3. Select **Account Info**.
4. Click **Edit**.



5. Check the boxes to for **Account API Enabled** and **Device API Enabled.**
6. Click **Update Account**.
7. Return to the Edit form.
8. Click **Generate new Account API Key** and confirm. Record the key and store it in a secure location. You will not be able to view it again.



9. Click **Generate new Device API Keys**, and confirm.
10. Record the **Device API Secret** and **Device API Auth Token** and store them in a secure location. You will not be able to view them again.

Activating a Login

This process is for new users who were registered by another user.

1. In the activation email, click the link.

   A User Activation window confirms your login has been activated.
2. Click **Set Password.**
3. Enter a new **Password** and confirm it.

   Password must:

   - Have a minimum of 10 characters
   - Contain at least 1 upper-case letter
   - Contain at least 1 lower-case letter
   - Contain at least 1 special character
   - Contain at least 1 digit
4. Click **Change Password**.
5. Log into DeviceHQ.
6. Review the End User License Agreement and check to **Accept EULA.**
7. Click **Submit.**

   If multifactor authentication is enable for your account, go to Logging in for the First Time for steps to setup multifactor authentication.

Logging In

If multi-factor authentication is enabled, skip to the next topic. To log in without multi-factor authentication:

1. Go to https://www.devicehq.com/sign_in
2. Enter the username and password used when you registered for an account.
3. Click **Sign In**.

Logging in for the First Time

If multi-factor authorization is enabled for your account, you need to set up an authenticator app, e.g. Microsoft Authenticator, Google Authenticator, etc.

1. Install an **authenticator app** on your smart phone or other device.
2. Open the **authenticator app**.

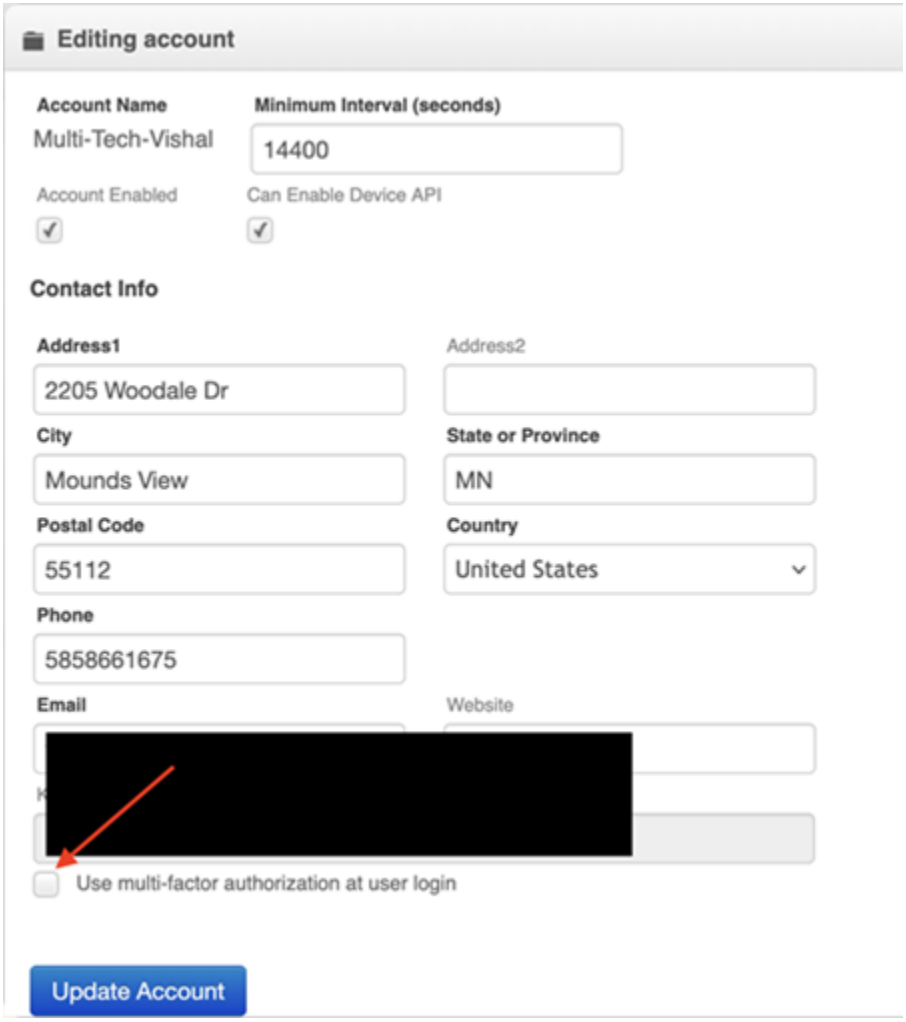
3. Scan the QR code on the Multi-Factor Authorization page or manually enter the account name (DeviceHQ) and secret presented in DeviceHQ into the authenticator app, e.g. Microsoft Authenticator, Google Authenticator, etc.
4. Click **OK.**
5. Enter your email and password.
6. Enter the code provided in the authenticator app and click **Verify Code**. If you have any issues, contact support@multitech.com.

Note: You need to enter an authenticator code every time you log in.

Logging in with Multi-Factor Authentication (MFA)

Want MFA enabled for your account? Email support@multitech.com to add MFA to your account. You can then enable or disable it anytime:

1. Select or clear the **Use multi-factor authorization at user login** check box.
2. Click **Update Account**.



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

To log in:

1. Go to https://www.devicehq.com/sign_in
2. Enter your **Email** and **Password.**
3. Enter your **Two-Factor Authorization Code** from the authenticator app.
4. Click **Verify Code.** If you have any issues, contact support@multitech.com.

Chapter 3 Setting up an mPower Device for Use with DeviceHQ

To use your device in DeviceHQ, enable remote management in the device's web management interface. Log into your device and complete the following task.

Managing Your Device Remotely

NOTE: Reboot the device before performing any firmware updates.

To configure your device to use DeviceHQ:

1. Go to **Administration > Remote Management** and check **Enabled**.
2. Go to options under **DeviceHQ Check-In Settings**.
3. Enable the **Intervals** check box to check in to DeviceHQ periodically at the specified interval.**If you do not select **Intervals**, certain DeviceHQ features will NOT be available. See note at the end for this topic for details.*
    a. To define how often the device connects to DeviceHQ to check in and request any pending updates, set the **Check-In Interval** field to the desired number of minutes between 240-10080 (240 minutes to 1 week). **Note:**The minimum check-in interval is 4 hours. If you set a device's check-in interval to less than 4 hours, the change is ignored.
    b. To define how often the device connects to DeviceHQ to send GPS data, set the **GPS Data Interval** field to the desired number of minutes, between 240-10080 (240 minutes to 1 week). **Note:** Some MTR models do not have GPS. Then this field does not display.
4. Enable **Single Check-In** to configure your device to check-in to DeviceHQ at the specific date and time. If you enable **Single Check-In**, click the **Date** field to select the date from the calendar picker, and then enter the **Time** (HH:MM) for your device to check-in.
5. Enable **Repeatable** to check-in to DeviceHQ periodically at the specified time daily or at the specific days of the week.
    a. Select **Daily** from the **Repeat** drop-down to check in to DeviceHQ every day, and enter the **Time** (HH:MM) for your device to check-in.
    b. Select **Custom** from the **Repeat** drop-down, then specify the days of the week, and enter the **Time** (HH:MM) for your device to check-in.
6. Go to options under **Update Settings**
7. If **Sync with Dial-On-Demand** is checked and cellular dial-on-demand is enabled, the connection is not dialed solely for the purpose of connecting to DeviceHQ. The device will connect to DeviceHQ only when other traffic brings up the link.
8. Check **Allow Firmware Upgrade** if you want DeviceHQ to make automatic updates of your firmware.
9. Check **Allow Configuration Upgrade** if you want DeviceHQ to make automatic updates of your configuration software.

10. Check **Allow Radio Firmware Upgrade** if you want DeviceHQ to make automatic updates of your cellular radio firmware.
11. Click **Submit**.
12. Click **Save and Apply** to save your changes.

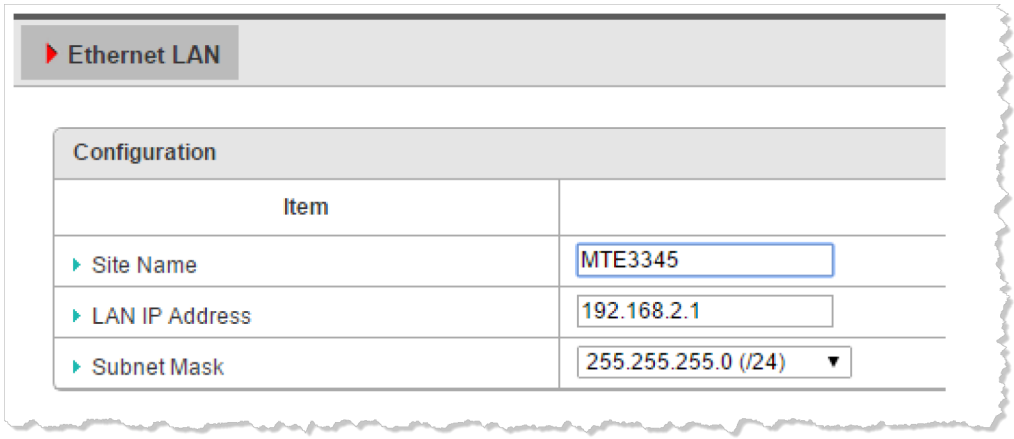
    ***NOTE**: If you do not select **Intervals**, certain DeviceHQ features will NOT be available including:

    - missed check-in alerts
    - device rebooted alerts
    - automatically scheduled device log uploads
    - home page notices for rebooted or missed check-in devices

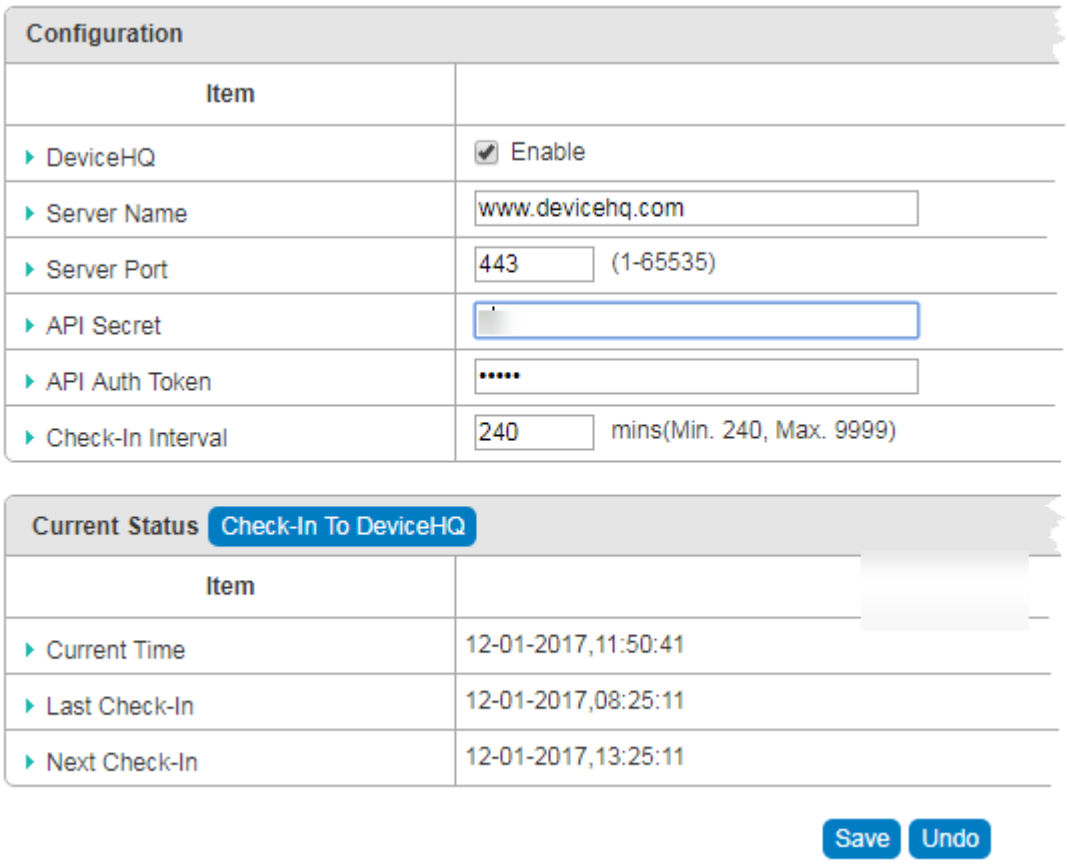
Chapter 4 Setting up an MTR5, MTR6, MTE, or MTE2 for Use with DeviceHQ

To setup your device to communicate with DeviceHQ:

1. Log into your device's user interface.
2. Enter and define the **Site Name** so it appears in the DeviceHQ description. Go to the Ethernet LAN tab for your device.
   - For an **MTR5**, go to **Basic Network > LAN/WAN**
   - For an **MTE** or **MTE2**, go to **Basic Network > LAN**
   - Fro an **MTR6**, go to **Configuration > LAN**



   Site Name can include upper and lowercase letters, numbers, and special characters.
3. Go to the **DeviceHQ** tab.
   - For an **MTR5**, go to **Advanced Network > System Management > DeviceHQ**,
   - For an **MTE**or **MTE2**, go to **Basic Network > System Management > DeviceHQ**.
   - For an **MTR6**, go to **Administration > Configure & Manage > DeviceHQ**



4. Check **Enable** for DeviceHQ.
5. Enter the DeviceHQ device API key in the **API Secret** field.
6. Enter the device **API Auth Token**.
7. Click **Save.**

Chapter 5 Working with Devices

Device Page

Shows the devices affiliated with your account.

To select which columns are shown, click **Columns** and check or uncheck columns as needed.

The **Filter** button displays additional filter options.

The **Tasks** button displays a list of available tasks for each device

Use the **Refresh** button to refresh the device list.

Field	Description
Description	Device description. The default description is product and serial number. This field is editable.
Product	Type of product. Not editable.
Serial Number	Product serial number. Not editable.
MAC	Product MAC address. This field is not editable.
Group	The group is user supplied.
Device Logs	Frequency of the upload of log files.
Actions	Shows the next pending action.
Firmware	Current firmware version on the device.
Hardware	Device hardware model.
Cell Provider	Cell service provider.
IMEI	Device International Mobile Equipment Identity number
IMSI	Device International Mobile Subscriber Identity number
RSSI	Signal strength.
Checked-In	Timestamp of the last check-in.
Location	GPS coordinates for the device, if available.
Interval	How often the device is set to check-in.
Uptime	How long the device has been running since last boot.

Filtering the Device List

To filter the device list:

1. Click **Devices.**
2. To show the filter tree, click **Filter.**

3. Select filter type and criteria:
   - **Action** - Devices with the selected action pending.
   - **Firmware** - Devices running the selected firmware version.
   - **Products** - Devices that are the selected product model.
   - **Groups** - Devices in the selected group.
   - **Upgrade Managers** - Devices in the selected Upgrade Manager. Further filter this list by upgrade status: Waiting, In Progress, Succeeded, Failed.

To clear the filter and show all devices, click **Filter** again.

Grouping Devices

To make devices easier to manage, assign them to groups and filter the list to show just a group's devices.

Note: A device may only belong to one group at a time. Assigning it to a new group removes it from the old group.

To group devices:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to group together. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Group Devices.**
4. Enter a new group Name or start entering the name of an existing group and select the group you want from the list.
5. Select the devices from the **Apply to** list, choose **Selected Devices** or F**iltered Devices.**
6. Click **OK** and then click **OK** again to confirm.

You can also drag and drop devices to group them:

1. Click **Devices** and then click **Filter**.

2. Click **Groups** and scroll to the group you want.

3. Drag devices to that group.

Editing Device Information

To change device information:

1. From the device's window, click **Edit.** From the device list, click the Edit icon, .
2. Make desired changes. Note that for devices with GPS capability, GPS coordinates are pulled from the device. For field descriptions, refer to Device Page.
3. Click **Update Device**.

Deleting a Device

To delete a device:

1. From the device list, click the **Delete** icon, ✖.
2. Confirm the deletion, click **OK** to delete or **Cancel** the deletion.

Viewing Device Details

To view an individual device's details, click the desired device. A window opens showing:

Note: Devices do not maintain a persistent connection to DeviceHQ. Device statistics, such as signal level, are recorded when the device checks in. Devices check in every 4 hours unless configured for a different interval. For information on check-in intervals, refer to Understanding Check-In Intervals.

The left panel includes:

- Identifying information (also listed on the Device page)
- Device status
- Active apps, including version and status
- Stats

The right panel consists of several tabs:

- **Map:** Device location (either supplied by GPS or user-defined)
- **Check-ins:** When the device checked into the platform
- **Signal:** Graph of signal strength, RSSI for all users. For Standard and Premium accounts the Cellular Signal Strength chart also shows RSRP and RSRQ values. Click on the acronym to change the chart display.
- **Network:** WAN and LoRaWAN addresses and network statistics
- **LoRa:** *(LoRa devices only)* Indicates LoRa status and stats.
- **Device Files:** Device logs and configuration files data.

Upgrade Manager

If the device has been included in an Upgrade Manager it is noted on the Task List below the map. If the Upgrade Manager has not yet assigned a task to the device, it appears as pending to indicate it is included in an upgrade.

When the Upgrade Manager creates a task for the device, the Upgrade Manager replaces the pending task with the actual task.

The task starts in a scheduled state, which means it does not run on the next device check-in. After it is added to the device's queue, it is given to the device for execution on the following check-in.

For more information, refer to Managing Upgrades

Understanding Check-In Intervals

Devices periodically send device information and statistics to DeviceHQ, where they also check for firmware and configuration updates. By default, devices check into DeviceHQ every 12 hours.

Use the device's web management interface to change how frequently any device checks in with DeviceHQ. The minimum time between check-ins is once every 4 hours (240 minutes). DeviceHQ ignores values less than 240 minutes. For example, if you indicate you want the device to check into DeviceHQ every 3 hours (180 minutes), the request is ignored.

Deleting Multiple Devices

To delete multiple devices and their history:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to delete. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Delete Devices.**
4. Click **OK** to confirm.

Chapter 6 Scheduling Tasks

Scheduling Device Actions

You can use a device's information window to schedule firmware and configuration updates, install or uninstall apps, install app configurations, or reboot the device.

- From the **Schedule** menu, select the desired action.

Any pending action for the device occurs when the device checks into MultiTech DeviceHQ.

Note: After 90 days, DeviceHQ deletes commands that have been executed or canceled

Abort Actions

Cancel scheduled actions through the device list or device information window.

Through the Device List

To abort actions through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) with scheduled actions you want to cancel. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Abort Actions.**
4. Click **OK** to confirm.

Through the Device Information Window

To abort actions through the Device information window:

1. Click **Devices**.
2. Click the device you want to update to open the Device information window.
3. From the **Schedule** menu, select **Abort Actions**.
4. Click **OK** to confirm.

Updating Firmware

MultiTech offers firmware updates you can download from our web site. You can download the firmware and evaluate it before updating devices.

Use DeviceHQ to update the firmware running on any supported device. When you schedule a device for a firmware update, it updates the next time the device checks in.

Note: Devices do not maintain a persistent connection. Pending actions, such as firmware updates, are applied to the device only when it checks in. There is no live connection

.

Scheduling Firmware Updates

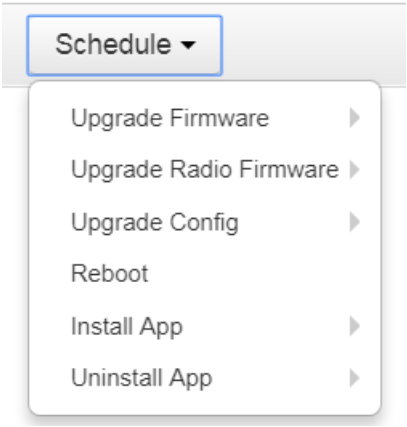
To schedule firmware updates through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to update. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Upgrade Firmware.**
4. Select the firmware version from the **File** list.
5. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
6. Click **Next**.
7. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time**.
8. Click **Next.** A message appears showing which selected devices are compatible with the selected firmware version and any that are not. Devices not compatible are not scheduled for update.
9. Click **Finish** to schedule the firmware update.

A confirmation message appears with details about the scheduled upgrade.

Through the Device Information Window

1. Click **Devices**.
2. Click the device you want to update to open the Device information window.
3. From the **Schedule** menu and select **Upgrade Firmware** and then select the firmware version.



4. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time**.
5. Click **Next.** A message appears showing which selected devices are compatible with the selected firmware version and any that are not. Devices not compatible are not scheduled for update.
6. Click **Finish** to schedule the firmware update.

A confirmation message appears with details about the scheduled upgrade.

Scheduling Radio Firmware Updates

You can update radio firmware for some products. This option is available only if a radio firmware file has been uploaded for this device.

Through the Device List

To schedule radio firmware updates through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to update. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Upgrade Radio Firmware**.
4. Select the radio firmware version from the **File** list.
5. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
6. Click **Next.**
7. Click **Next Check-in** or **Specified Time.** For Specified Time, enter the **Start Date** and **Start Time**.
8. Click **Next.** A message appears showing which selected devices are compatible with the selected radio firmware version and any that are not. Devices not compatible are not scheduled for update.
9. Click **Finish** to schedule the radio firmware update.

A confirmation message appears with details about the scheduled upgrade.

Through the Device Information Window

To schedule radio firmware updates through the Device information window:

1. Click **Devices**
2. Click the device you want to update to open the Device information window.
3. From the **Schedule** menu, select **Upgrade Radio Firmware** and then select the radio firmware version.
4. Click **Next Check-in** or **Specified Time.** For Specified Time, enter the **Start Date** and **Start Time**.
5. Click **Next.**
6. Click **Finish** to schedule the radio firmware update.

A confirmation message appears with details about the scheduled upgrade.

Upgrading Device Configuration File

Update the device configuration. This option is available only if a configuration file has been uploaded for this device.

Through the Device List

To schedule configuration updates through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to update. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Upgrade Config**.
4. Select a configuration file from the **File** list.
5. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
6. Click **Next.**
7. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time.**
8. Click **Next.** A message appears showing which selected devices are compatible with the selected configuration file and any that are not. Incompatible devices are not scheduled for update.
9. Click **Finish** to schedule the configuration update.

A confirmation message appears with details about the scheduled upgrade.

Through the Device Information Window

To schedule configuration updates through the Device information window:

1. Click **Devices** and filter the list if desired.
2. Click the device you want to update to open the Device Information window.
3. From the **Schedule** menu, select **Upgrade Config** then select the configuration file.
4. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time.**
5. Click **Next.**
6. Click **Finish** to schedule the configuration update.

A confirmation message appears with details about the scheduled upgrade.

Partial Configuration Updates

For supported devices, partial configuration update allows you to update just some sections of the device configuration file.

To remove a setting from the list click the corresponding minus sign.

Through the Device List

To schedule configuration updates through the device list:

1. Click **Devices** and filter the list if desired.
2. Select the devices you want to update from the Device List.

3. Click **Tasks** and select **Upgrade Config (Partial)**.
4. In the **Configuration Editor**, select the settings you want to update. Refer to *Settings* for information.
5. Click **Schedule.**
6. Click **OK** to schedule the partial configuration file upgrade.

Through the Device Information Window

To schedule radio firmware updates through the Device information window:

1. Click **Devices.**
2. Click the device you want to update to open the Device information window.
3. From the **Schedule** menu, select **Upgrade Config (Partial).**
4. In the **Configuration Editor**, select the settings you want to update. Refer to *Settings* for information.
5. Click **Schedule.**
6. Click **OK** to schedule the partial configuration file upgrade.

Settings

Configuration settings depend on the device. Consult your device documentation setting descriptions and details.

- Conduit (MTCDT, MTCDT3, MTCDIP, MTCAP and MTCAP2): https://multitech.com/wp-content/uploads/s000727-mPower-Edge-Intelligence-Conduit-AEP-software-guide.pdf
- MultiConnect rCell 100 Series (MTR): https://multitech.com/wp-content/uploads/s000720-mPower-Edge-Intelligence-MTR-Software-Guide.pdf
- MultiConnect rCell 500 Series (MTR5): https://multitech.com/wp-content/uploads/S000589-MTR5-LEU2-user-guide.pdf
- MultiConnect eCell (MTE-LAT6): https://multitech.com/wp-content/uploads/S000644.pdf
- MultiConnect eCell (MTE-LEU6): https://multitech.com/wp-content/uploads/S000644.pdf
- MultiConnect eCell (MTE-L12G2): https://multitech.com/wp-content/uploads/S000767_MTE2_User_Guide.pdf

Rebooting Devices

Schedules one or more devices to reboot on next check-in.

Through the Device List

To schedule a device reboot through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to reboot. To select all devices, click the check box in the device table's header row.

3. Click **Tasks** and select **Reboot Devices**.
4. Click **OK** to schedule or**Cancel**.

A confirmation message appears.

Through the Device Information Window

To schedule a device reboot through the Device information window:

1. Click **Devices.**
2. Click the device you want to reboot to open the Device information window.
3. From the **Schedule** menu, select **Reboot Devices**.
4. Click **OK** to schedule or **Cancel.**

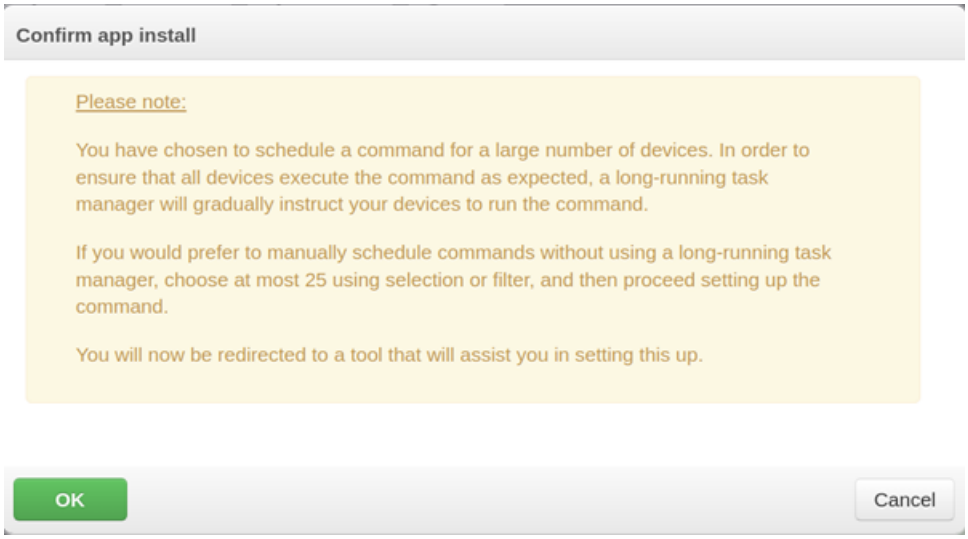
A confirmation message appears.

Managing Upgrades

Available for firmware upgrades, app installs, and full configuration updates only.

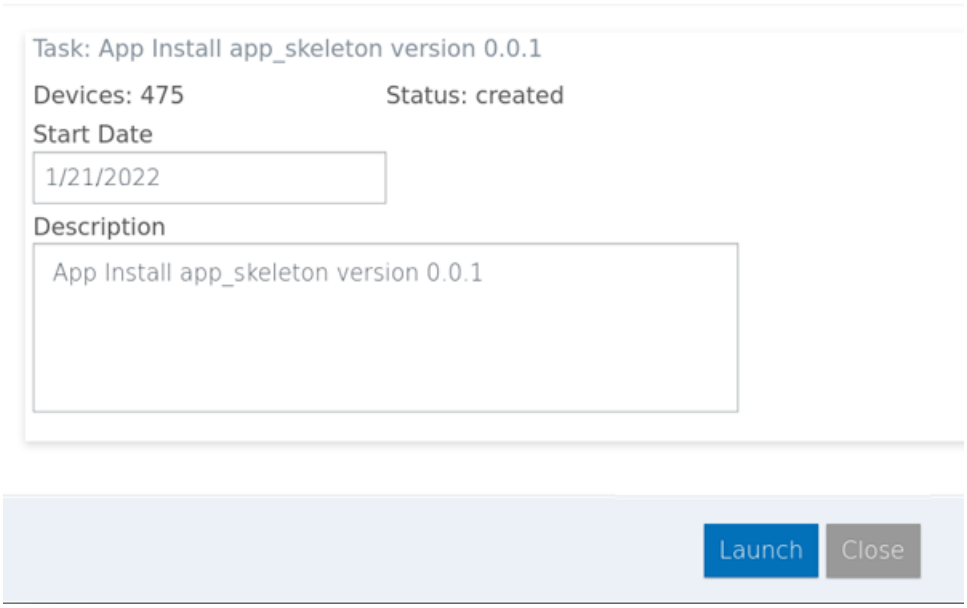
Upgrade Managers are long-running task managers that roll out upgrade tasks gradually on large groups of devices. DeviceHQ automatically creates an upgrade manager when a user creates an upgrade or install task for 25 or more devices. If you chose not to use the upgrade manager, you can still manually schedule upgrades for up to 25 devices at a time.

When you select a 25 or more devices for upgrades, DeviceHQ displays a pop-up window explaining an Upgrade Manager has been created.



- To use the Upgrade Manager, click **OK**. The Upgrade Manager page opens.
- To schedule upgrades manually, click **Cancel**.

Using an Upgrade Manager



To use an upgrade manager:

1. Enter a **Start Date**. Default date is today.

   Enter a **Description** (optional) and click Launch. If you click Close, the new UpgradeManager remains in a table and can be re-opened and launched later.

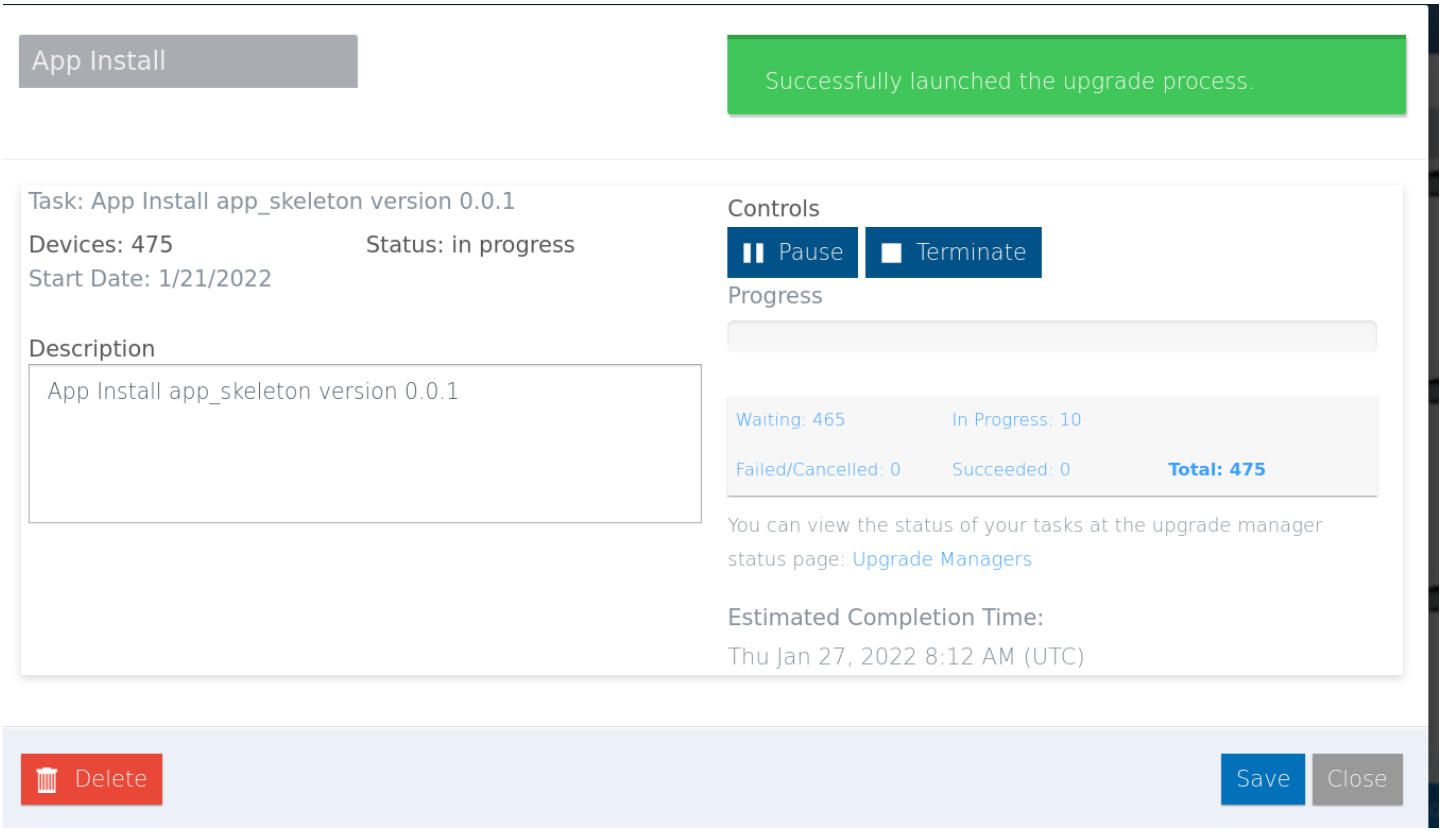
A status page appears, showing task status.

Note:

- After Launch, you can't add or remove devices from the Upgrade Manager, or change the task. The upgrade can be terminated on the status page.
- DeviceHQ activates the Upgrade Manager if the total number of devices scheduled is greater than the threshold. The default threshold is 25 devices, which is adjustable per account.
- When launched, the Upgrade Manager immediately schedules tasks for a few devices likely to check in within the next 15 minutes. After this, it updates periodically, each time scheduling new tasks for a few more devices.
- Once it has scheduled a task action for each device in the Upgrade Manager, the status changes to scheduling completed.

Using the Upgrade Manager Status Page

The Upgrade Manager status page shows the number of devices to be upgraded, upgrade status, and estimated completion time. If the page is left open, it updates current progress once per minute.



Progress links allow you to filter a device list to view devices based on upgrade status:

- **Waiting:** Upgrade task not yet issued to the device.
- **In Progress:** Upgrade task issued to the device.
- **Failed/Cancelled:** Upgrade task issued to the device and either failed or was cancelled.
- **Succeeded:** Upgrade task issued to the device and reported successfully completed.

Note: Once an upgrade task is scheduled and the Upgrade Manager status changes to complete, the launch time and description can't be changed and the Pause and Terminate buttons are no longer available.

To pause or restart an upgrade:

- Click **Pause.** The Upgrade Manager remains paused until you manually unpause it, by clicking Pause again.

To terminate an upgrade in progress:

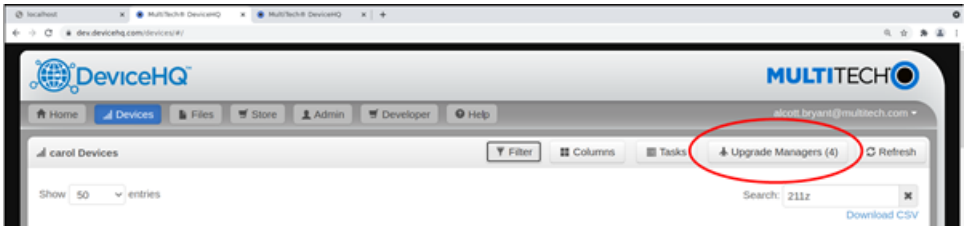
- Click **Terminate.** Any tasks in progress will complete. Additional tasks will not run.

To delete an upgrade manager:

- Click **Delete.**

Managing Upgrade Managers

After creating one or more upgrade managers, an Upgrade Managers button appears on the Devices pages.



To view a list of upgrade managers:

- Click **Upgrade Managers**.

The Upgrade Managers page shows the last 10 Upgrade Managers created, including the upgrade description, device count, status, and start date.

DeviceHQ deletes Upgrade Managers from the system 90 days after completion.

To view an Upgrade Manager's details:

- Click the **Edit** icon for that Upgrade Manager. This opens the Upgrade Manager Status Page.

To delete an Upgrade Manager:

- Click the **Delete** icon for that Upgrade Manager and then confirm the deletion.

Requesting and Downloading Device Logs

Through the Device List

To request device logs:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) from which you want device logs. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Request Device Logs**.
4. Click **OK**.

Through the Device Information Window

To request a device log through the Device information window:

1. Click **Devices**.
2. Click the device you want to open the Device information window.
3. From the **Schedule** menu, select **Request Device Logs**.
4. Click **OK**.

Pending device logs requests appear at the bottom of the window.

Downloading Device Logs

To download a device's logs:

1. Click **Devices**.

2. Click the device whose log you want download.
3. Click the **Device Files** tab.
4. Click **Download Logs.**

Scheduling Regular Device Log File Uploads

To schedule device logs uploads to DeviceHQ on a regular basis:

1. Click **Devices** and filter the list if desired
2. Select check boxes of the device(s) from which you want device logs. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Device Logs Settings**.
4. Select the **Request Device Logs interval**.
   - Never
   - Every Check-in
   - Custom Interval

   Set the custom interval length in hours. The minimum time allowed is 4 hours.
5. **Apply to** either **Selected Devices** or **Filtered Devices.**
6. Click **OK**.

   Pending device logs requests appear at the bottom of the window.

   Note: To request a device log without setting an interval, select **Request Device Logs** from the **Task** drop-down list.

Downloading Device Logs

To download a device's logs:

1. Click **Devices**.
2. Click the device whose log you want download.
3. Click the **Device Files** tab.
4. Click **Download Logs.**

Installing an App

DeviceHQ allows you to develop and install apps on Conduit products. For information about developing apps, refer to the https://multitech.com/wp-content/uploads/S000756_DeviceHQ_App_Developer_Guide.pdf.

Through the Device List

To install apps on a device through the device list:

1. Click **Devices** and filter the list if desired.

2. Select check boxes of the device(s) you want to update. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Install App.**
4. Select the app you want to install from the **Name** list.
5. Select an app **Version**.
6. Select an **App config** if applicable.
7. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
8. Click Schedule **App Install.**
9. Click **OK** to confirm.

DeviceHQ installs the app when the device checks in again.

Through the Device Information Window

To install apps on a device through the device information window:

1. Click **Devices**.
2. Click the device you want to update to open the Device information window.
3. From the Schedule menu, select **Install App.**
4. Select the app you want to install from the **Name** list.
5. Select an app **Version**.
6. Select an **App config** if applicable.
7. Click Schedule **App Install.**
8. Click **OK** to confirm.

DeviceHQ installs the app when the device checks in again.

Uninstalling an App

Through the Device List

To uninstall an app through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) with the app you want to uninstall. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Uninstall App**.
4. Select the app you want to remove from the **Name** list.
5. Select the app **Version.**
6. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
7. Click **Schedule Action.**

8. Click **OK** to confirm.

DeviceHQ uninstalls the app when the devices check in again.

Through the Device Information Window

To uninstall an app through the Device information window:

1. Click **Devices**.
2. Click the device you want to with the app you want to uninstall.
3. From the Schedule menu, select **Uninstall App**.
4. Select the app you want to remove from the **App** list.
5. Click **OK** to confirm.

DeviceHQ uninstalls the app when the devices check in again.

Uninstalling an App

Through the Device List

To uninstall an app through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) with the app you want to uninstall. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Uninstall App**.
4. Select the app you want to remove from the **Name** list.
5. Select the app **Version.**
6. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
7. Click **Schedule Action.**
8. Click **OK** to confirm.

DeviceHQ uninstalls the app when the devices check in again.

Through the Device Information Window

To uninstall an app through the Device information window:

1. Click **Devices**.
2. Click the device you want to with the app you want to uninstall.
3. From the Schedule menu, select **Uninstall App**.
4. Select the app you want to remove from the **App** list.
5. Click **OK** to confirm.

DeviceHQ uninstalls the app when the devices check in again.

Verifying an Application on Your Conduit Device

To verify if an app was installed on an a Conduit product:

1. Login to the device's user interface.
2. Select Apps from the menu bar.

The Apps section displays information for the currently running application. Only one application run at a time on the device. Consult the https://multitech.com/wp-content/uploads/s000727-mPower-Edge-Intelligence-Conduit-AEP-software-guide.pdf for more information about verifying apps.

Chapter 7 Files

Files

The Files page lists firmware and configuration files that have been uploaded to DeviceHQ.

Show at the top of the page controls the number of entries displayed per page.

Firmware File Fields

Field	Description
Show	Selected by default. Uncheck to remove the firmware file from the available firmware drop-down list.
Filename	Name of the uploaded file.
Model	Device model the firmware file applies to.
Version	File version.
Signed	Indicates if the firmware file is digitally signed.
Length	File size.
MD5	Checksum.
Uploaded	Date and time the file was uploaded

Configuration File Fields

Field	Description
Filename	Name of the uploaded file,
Model	Device modek the configuration file applies to.
Name	Descriptive file name. (Required)
Description	Explanation of the configuration file.
Length	File size.
MD5	Checksum.
Uploaded	Date and time the file was uploaded.

Updating Firmware

MultiTech offers firmware updates you can download from our web site. You can download the firmware and evaluate it before updating devices.

Use DeviceHQ to update the firmware running on any supported device. When you schedule a device for a firmware update, it updates the next time the device checks in.

Note: Devices do not maintain a persistent connection. Pending actions, such as firmware updates, are applied to the device only when it checks in. There is no live connection
.

Scheduling Firmware Updates

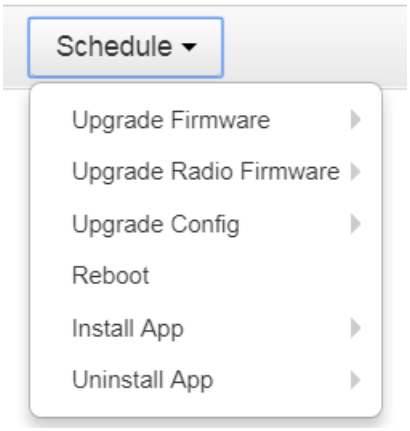
To schedule firmware updates through the device list:

1. Click **Devices** and filter the list if desired.
2. Select check boxes of the device(s) you want to update. To select all devices, click the check box in the device table's header row.
3. Click **Tasks** and select **Upgrade Firmware.**
4. Select the firmware version from the **File** list.
5. Select the devices from the **Apply to** list, choose **Selected Devices** or **Filtered Devices.**
6. Click **Next**.
7. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time**.
8. Click **Next.** A message appears showing which selected devices are compatible with the selected firmware version and any that are not. Devices not compatible are not scheduled for update.
9. Click **Finish** to schedule the firmware update.

A confirmation message appears with details about the scheduled upgrade.

Through the Device Information Window

1. Click **Devices**.
2. Click the device you want to update to open the Device information window.
3. From the **Schedule** menu and select **Upgrade Firmware** and then select the firmware version.



4. Click **Next Check-in** or **Specified Time**. For Specified Time, enter the **Start Date** and **Start Time**.

5. Click **Next.** A message appears showing which selected devices are compatible with the selected firmware version and any that are not. Devices not compatible are not scheduled for update.
6. Click **Finish** to schedule the firmware update.

A confirmation message appears with details about the scheduled upgrade.

Configuration Files

DeviceHQ allows users to apply a configuration file to other devices of the same type. After you create, save, and verify your desired configuration files, you can upload the files to DeviceHQ within the device's user interface or through DeviceHQ. For Conduit products and MTRs, DeviceHQ also allows you to save a device's configuration file as a template.

For help uploading through the device's user interface, refer to the device's documentation.

Uploading Configuration Files

Note: Use an external device to create and save configuration BIN files. The BIN file must be a .zip file when uploaded to DeviceHQ. Base the ZIP file name on the device description or serial number to identify it easily.

After you create, save, and verify your desired configuration files, upload the files to DeviceHQ to apply the configuration settings to other devices:

1. Click **Files**.
2. Click **New Configuration**. A dialog box appears.
3. In the **Name** and **Description** fields, type the name and description that you want to assign the configuration file.
4. Click **Choose File**. Go to the location where the configuration file is saved.
5. Select the file and click **Upload**.

The configuration file appears on the Files page. Select the file when you schedule a configuration update for a device or a group of devices.

Deleting a Configuration File

You can delete a configuration file from the available configuration files in DeviceHQ device or remove the configuration file from a specific device.

Deleting Configuration Files from the Files Page

To delete a configuration file from the Files page:

1. Click **Files.**
2. Find the file you want to delete from DeviceHQ, click the **Delete** icon,
   ✖

.

3. Click **OK** to confirm the deletion.

To Delete a Configuration File from the Device Files Tab:

To delete a configuration file uploaded from the device:

1. Click **Devices** and then click on a device to view the device details.
2. Click the **Device Files** tab.
3. Click **Delete Config**.
4. Click **OK** to confirm the deletion.

Editing a Configuration File

You can change configuration file name and description through the Files page.

1. Click **Files.**
2. Click the **Edit** icon, , for the configuration file.
3. Make desired changes.
4. Click **Save.**

Download Configuration File

You can download a configuration file for any device through DeviceHQ.

Downloading a Configuration File from the Files Page

To download a configuration file from the Files page:

1. Click **Files.**
2. Click the Download icon,

, for the configuration file you want to download. Depending on your browser, you may be prompted to open or save.

Downloading a Configuration File from the Device Information Window

To download a configuration file from the Device information window:

1. Click **Devices** and then click on a device to view the device details.
2. Click the **Device Files** tab.
3. Click **Download Config.** Depending on your browser, you may be prompted to open or save.

Using as a Template for a New Configuration File

For MTR and Conduit products, you can save an existing configuration file as a template for a new configuration file and adjust the settings.

Note: Configuration options vary between the MTR and Conduit product families. For detailed settings information, refer to the mPower Software guide for your device.

To use an existing configuration file as a template:

1. Click **Devices** and then click on a device to view the device details.
2. Click the **Device Files** tab.
3. Click **Use As a Template for New Config.** This opens the Configuration Editor.
4. Make desired changes for use as a template.
5. Click **Save As.**
6. Enter a **Name** and **Description** for the template.
7. Click **Save.**

Firewall

Firewall Configuration

This feature is available for full configuration with Standard and Premium accounts only.

The device's firewall enforces a set of rules that determine how incoming and outgoingpackets are handled. By default, all outbound traffic originating from the LAN is allowed to pass through the firewall, and all inbound traffic originating from externa networks is dropped. This effectively creates a protective barrier between the LAN and all other networks.

The firewall is built on top of iptables. The different rule groups correspond totheir respective chains in iptables.

Note: As a best security practice, the device employs minimum firewall rules by default. This means by default the device allows all outbound traffic from it in the Output Filter Rules. (Traffic through the device is handled by the Port/Inbound Forwarding Rules.) But all traffic to the device via WAN interfaces is blocked by default in the Input Filter Rules. Users may create their own specific and targeted input filter rules to allow certain traffic to the device based on their specific needs.

Use this page to view, add, or edit the rules for the device firewall configuration.

To configure the firewall:

1. On a device's **Device Files** tab, click Use As a Template for New Config and then click **Firewall** in the left navigation menu.
2. To use Prerouting (DNAT) or Post Routing (SNAT) rules, click Advanced in the upper right of the firewall section. See Advanced Firewall Configuration.
3. Click Add Rule for Port Forwarding, Input Filter Rules, or Output Filter Rules.
4. Enter settings and click **Save As**. See Related topics for details on each rule type.

Connection Tracker

At the bottom of the Firewall Settings page, there is a check box under Connection Tracker Helper. This feature is disabled by default due to its inherent security risks.

The **Connection Tracker Helper** enables connection tracking for multi-flow protocols that usually separate control and data traffic into different flows. Protocols supported include FTP, H323, and SIP. This feature enables and uses the kernel module, nf_conntrack_helper.

To enable this feature, check **Enabled**.

Port Forwarding

This feature is available for Standard and Premium accounts only.

Field	Description
Inbound Forwarding Rule	
Name	Enter a name for the rule.
Description	Enter a rule description. Optional.
External WAN Port(s)	Select a port.
Destination LAN Port(s)	Enter the destination LAN port that applies to this rule. If there is a range of ports, the ending port is automatically set.
Destination LAN IP	Enter the destination LAN IP address that applies to this rule.
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
Inbound Filter Rule	
External Source IP	Enter the source IP address that applies to this rule.
External Source Ports	Enter the source port range that applies to this rule.
Mask	Enter source subnet mask that applies to this rule.
Enable NAT Loopback	Check if you want to redirect LAN packets destined for the WAN's public IP address.

Input Filter Rules

This feature is available for Standard and Premium accounts only.

Field	Description
Name	Enter a name for the input filter rule.
Description	Enter a rule description. Optional.
Destination Settings	
Destination IP	Enter the destination IP address that applies to this rule.
Destination Port	Select the destination port that applies to this rule.
Destination Mask	Enter the subnet mask of the destination that applies to this rule.

Field	Description
Destination Interface	Select the destination interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
Source Settings	
Source IP	Enter the source IP address that applies to this rule.
Source Port	Select the source port range that applies to this rule.
Source Mask	Enter source subnet mask that applies to this rule.
Source MAC	Enter the source MAC address for the device that applies to this rule.
Source Interface	Select the source interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
General Configuration	
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
Chain	Select a grouping based on the traffic type affected by the rule. Options are: **INPUT, FORWARD, or OUTPUT.**
Target	Select a desired action for the firewall based on this rule. Options are: **ACCEPT, REJECT, DROP, or LOG.**

Output Filter Rules

This feature is available for Standard and Premium accounts only.

Field	Description
Name	Enter a name for the output filter rule.
Description	Enter a rule description. Optional.
Destination Settings	
Destination IP	Enter the destination IP address that applies to this rule.
Destination Port	Select the destination port that applies to this rule.
Destination Mask	Enter the subnet mask of the destination that applies to this rule.
Destination Interface	Select the destination interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
Source Settings	
Source IP	Enter the source IP address that applies to this rule.
Source Port	Select the source port range that applies to this rule.
Source Mask	Enter source subnet mask that applies to this rule.
Source MAC	Enter the source MAC address for the device that applies to this rule.

Field	Description
Source Interface	Select the source interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
General Configuration	
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
Chain	Select a grouping based on the traffic type affected by the rule. Options are: I**NPUT, FORWARD, or OUTPUT**.
Target	Select a desired action for the firewall based on this rule. Options are: **ACCEPT, REJECT, DROP, or LOG.**

Advanced Firewall Configuration

This feature is available for Standard and Premium accounts only.

The Firewall's Advanced Settings mode lets you manipulate DNAT, SNAT, and Filterrules directly. DNAT rules can manipulate the destination address and port of a packet; similarly SNAT rules can manipulate the source address and port of a packet.Filter rules apply an ACCEPT, REJECT, DROP, or LOG action to a packet. A DNAT or SNAT rule with the same name as a Forwarding rule will be associated under NormalSettings for Port Forwarding/NAT rules.

For advanced firewall configuration:

1. On a device's Device Files tab, click **Use As a Template for New Config** and then click **Firewall** in the left navigation menu.
2. Click **Advanced** in the upper right of the Firewall section.
3. To add a prerouting (DNAT) rule to your firewall, click **Add DNAT Rule**.
4. To add Forward Filter Rules, Input Filter Rules, or Output Filter Rules, click **Add rules** for that rule type.
5. To add postrouting (SNAT) rule to your firewall, click **Add SNAT Rule**.
6. Enter settings and click **Save As.**

Prerouting Rule (DNAT)

This feature is available for Standard and Premium accounts only.

Field	Description
Name	Enter a name for the filter rule.
Description	Enter a rule description. Optional.
Destination Settings	
Destination IP	Enter the destination IP address that applies to this rule.
Destination Port	Select the destination port that applies to this rule.
Destination Mask	Enter the subnet mask of the destination that applies to this rule.

Field	Description
Destination Interface	Select the destination interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
Source Settings	
Source IP	Enter the source IP address that applies to this rule.
Source Port	Select the source port that applies to this rule.
Source Mask	Enter source subnet mask that applies to this rule.
Source MAC	Enter the source MAC address for the device that applies to this rule.
Source Interface	Select the source interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
General Configuration	
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
NAT IP	Enter the local address for the Network Address Translation.
Enable NAT Loopback	Check Enable NAT Loopback if you want to redirect LAN packets destine for the WAN's public IP address.
NAT Port	Enter the port used to the Network Address Translation.

Forward Filter Rules

This feature is available for Standard and Premium accounts only.

Field	Description
Name	Enter a name for the rule.
Description	Enter a rule description. Optional.
Destination Settings	
Destination IP	Enter the destination IP address that applies to this rule.
Destination Port	Select the destination port that applies to this rule.
Destination Mask	Enter the subnet mask of the destination that applies to this rule.
Destination Interface	Select the destination interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
Source Settings	
Source IP	Enter the source IP address that applies to this rule.
Source Port	Select the source port range that applies to this rule.
Source Mask	Enter source subnet mask that applies to this rule.
Source MAC	Enter the source MAC address for the device that applies to this rule.

Field	Description
Source Interface	Select the source interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
General Configuration	
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
Chain	Select a grouping based on the traffic type affected by the rule. Options are: **INPUT, FORWARD, or OUTPUT.**
Target	Select a desired action for the firewall based on this rule. Options are: **ACCEPT, REJECT, DROP, or LOG.**

Postrouting Rules (SNAT)

This feature is available for Standard and Premium accounts only.

Field	Description
Name	Enter a name for the filter rule.
Description	Enter a rule description. Optional.
Destination Settings	
Destination IP	Enter the destination IP address that applies to this rule.
Destination Port	Select the destination port that applies to this rule.
Destination Mask	Enter the subnet mask of the destination that applies to this rule.
Destination Interface	Select the destination interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
Source Settings	
Source IP	Enter the source IP address that applies to this rule.
Source Port	Select the source port that applies to this rule.
Source Mask	Enter source subnet mask that applies to this rule.
Source MAC	Enter the source MAC address for the device that applies to this rule.
Source Interface	Select the source interface that applies to this rule. Depending on your device model, options may include: **ANY, LAN, WAN, Cellular, Wi-Fi WAN, WI-FI AP, ETHERNET, or OPENVPN.**
General Configuration	
Protocol	Select the protocol of the messages that apply to this rule. Options are: **TCP/UDP, TCP, UDP, or ANY.**
NAT IP	Enter the local address for the Network Address Translation.
NAT Port	Enter the port used to the Network Address Translation.

Field	Description
Target	Select a desired action for the firewall based on this rule. Options are: SNAT or MASQUERADE.

Setting up Static Routes

To set up a manually configured mapping of an IP address to a next-hop destination for data packets:

1. Go to **Firewall > Static Routes**.

   If you aren't in the Configuration Editor, on a device's **Device Files** tab, click Use As a Template for New Config and then click **Firewall** in the left navigation menu.
2. In the **Static Routes** window, click **Add Route**.
3. In the **Name** field of the **Add Route** dialog box, type the name of the route.
4. In the **IP Address** field, type the remote network IP address of the remote location.
5. In the **IP Mask** field, type the network mask that is assigned on the remote location.
6. In the **Gateway** field, type the IP address of the routing device that supports the remote IP Network.
7. Click **Finish**.
8. To save your changes, click **Save and Apply**.

Trusted IP

Trusted IP is a simplified interface to create iptables rules to allow or block specific IPs, IP ranges, or subnets. This feature allows users to create whitelists (which are allowed or trusted IPs) or black lists (which are blocked or unwanted IPs). You can add, edit, and delete IP addresses as needed.

If you select **White List** as **Trusted IP Mode** and you do not set any IP range, no traffic will be allowed. If you select **Black List** as **Trusted IP Mode** and you do not set any IP range, all traffic will be allowed.

To set up a Trusted IP range:

1. Go to **Firewall > Trusted IP**.

   If you aren't in the Configuration Editor, on a device's **Device Files** tab, click Use As a Template for New Config and then click **Firewall** in the left navigation menu.
2. Check the **Enabled** box to turn on Trusted IP.
3. Select the **Trusted IP Mode** from the drop-down, either **White List** or **Black List**. (**NOTE**: Be aware of the behavior of each list and its consequences based on your specific configuration. For example, if you select **White List** as **Trusted IP Mode**, you should include the device **IP Address Range** or **IP Address** and **Subnet Mask** to maintain your local device LAN access.)
4. To add IP addresses, click **Add IP Range** in the upper right corner.
5. Under the **Add IP Range**, enter or select the following parameters:
   a. **Name**
   b. Mode from drop-down, either **Subnet** or **IP Range**.
   c. For **Subnet**:

i. **IP Address**
ii. **Subnet Mask**

d. For **IP Range**:

i. **IP Address Start**
ii. **IP Address End**

e. **Destination Port** (default: **ANY**)
f. **Protocol** from drop-down including **ANY, TCP/UDP, TCP**, or **UDP**
g. Click **Finish**.

6. The system displays your recently added and existing IP ranges in a list. The list includes the relevant details. You may edit any IP ranges by clicking on the pencil icon under **Options**.
7. You may delete any IP ranges by clicking on the trash can icon under **Options**.
8. If you want to revert back to default settings (where **Trusted IP** is disabled and all IP ranges are removed), click the **Reset to Default** button in the lower right corner
9. Click **Submit**.
10. To save your changes, click **Save and Apply**.

Wireless Configuration

Wi-Fi Access Point

You can configure a device as a wireless access point (AP) to allow Wi-Fi enabled devices to connect to the device using Wi-Fi (limited to specific models-consult appropriate manual for details). The Wi-Fi access point can have up to 5 clients at a time.

To set up your device as an access point:

1. On a device's **Device Files** tab, click **Use As a Template for New Config** and then go to **Wireless > Wi-Fi Access Point**.
2. To enable Wi-Fi Access Point mode, check **Enabled**.
3. To set the **SSID** (service set identifier) for the access point supported by your device, in the SSID field, type the name. The Wi-Fi devices look for this ID in order to join the wireless network. All wireless devices on a WLAN must use the same SSID in order to communicate with the access point.
4. To specify the data rates supported, select a **Network Mode**. Options are: **B/G/N-Mixed, B/G-Mixed, B-Only**, and **N-Only**.
5. Select a **Network Band**. Options are: **2.4 GHz** and 5 **GHz.**
6. Select a **Channel** on which the device operates. Options are **1-11.**
7. In the **Beacon Interval** field, enter the period of time, in milliseconds, when the access point sends a beacon packet. Beacons help synchronize a wireless network. For most applications, the default value of 100 provides good performance.

8. In the **DTIM Interval** field, enter how often a beacon frame includes a Delivery Traffic Indication Message, and this number is included in each beacon frame. It is generated within the periodic beacon at a frequency specified by the DTIM Interval. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients about the presence of buffered multicast/broadcast data on the access point. The default value of 1 provides good performance for most applications. You might want to increase this value when using battery powered Wi-Fi devices, which can sleep (at reduced power consumption) during the longer DTIM interval period. You must balance the power savings from increasing the DTIM interval against possible reduced communication throughput.
9. In the **RTS Threshold** field, type the frame size at which the AP transmissions must use the RTS/CTS protocol. This is often used to solve hidden node problems. Using a small value causes RTS packets to be sent more often, consuming more of the available bandwidth. However, the more RTS packets that are sent, the quicker the system can recover from interference or collisions.

Wi-Fi as WAN

This feature is available for Standard and Premium accounts only.

To setup the device's Wi-Fi as WAN (limited to specific models-consult appropriate device manual for details):

1. On a device's **Device Files** tab, click **Use As a Template for New Config** and then goto **Wireless > Wi-Fi as WAN**.
2. To enable **Wi-Fi as WAN** mode, check **Enabled**.
3. In the **Available Wi-Fi Networks** group, click the **SSID** for the Wi-Fi access point you want to use. The **Add Saved Network** window opens. Here are the available fields to enter information:
   - **Network Name**
   - **Hidden Network** (only check if your target network is currently hidden)
   - **SSID**
   - **Security Mode:** None, WEP, WPA, WPA-PSK, WPA-2, or WPA2-PSK
   - **Username**
   - **Password**
   - **Unmask** (Check, Uncheck)
   - **WPA Algorithm:** TKIP+AES, TKIP, or AES
   - **Shared Key**
4. Review the information, enter any required security info, then click **Finish**. The Wi-Fi access point you just added appears under **Available Wi-Fi Networks**.

Bluetooth IP

This feature is available for Standard and Premium accounts only.

The Bluetooth-IP feature allows a data connection between a remote TCP/UDP client or server and a local Bluetooth device (limited to specific models-consult appropriate manual for details). To set up the Bluetooth connection:

1. On a device's **Device Files** tab, click **Use As a Template for New Config** and then go to **Wireless > Bluetooth IP**.
2. To enable the feature, check **Enabled**.
3. Confirm that the far-end Bluetooth device is powered on and waiting for a connection in the **Status** field.
4. Enter the **Name** of the Bluetooth device you want to use.
5. Enter the Bluetooth device's **MAC address**.
6. Set **IP Pipe** as either **Server** or **Client** mode. Refer to the following topics for details.
7. Configure security settings. Refer to *Configure security settings* for details.
8. Click **Submit.**

The device immediately connects to the local Bluetooth device.

- If successful the Status field displays Connected.
- If IP Pipe is configured for SERVER, the IP connection is initiated by the far-end TCP/UDP client.
- If Mode is set to CLIENT, the device initiates connections for the far-end TCP/UDP server based on the configured Connection Activation conditions are met.

At the bottom of the page is a list of Saved and Available Bluetooth Devices.

Using IP Pipe in TCP/UDP Client mode

In the IP Pipe group:

1. Set the Mode as **SERVER**.
2. Select the desired Protocol. Options are: TCP, UDP, or SSL/TLS.
3. In the Buffer Timeout field, enter the timeout after which data is sent to the network if the buffer is not full (in milliseconds).
4. In the **Server Port** field, type the desired port value in the range 1 to 65535.
5. In the Buffer Size field, enter the size of the buffer for reading data from the serial port and sending to the network (in bytes). Data is sent when the buffer is full.
6. Select a disconnect method for the IP pipe in the **Connection Termination**. Options are:

Using IP Pipe in TCP/UDP Client Mode

In the IP Pipe group:

1. Set the Mode as **CLIENT**.
2. Select the desired Protocol. Options are: **TCP, UDP,** or **SSL/TLS**.
3. In the **Server IP Address** field, type the address of the far-end TCP-UDP server.
4. In the **Server Port** field, type the port value used by the far-end TCP/UDP Server.
5. In case the primary server is unavailable, in the **Secondary IP Address** field and in the **Secondary Port** field, type the IP address and port number, respectively, of the alternate TCP/UDP server.

6. In Connection Activation, select a connection method. Options are:
   - **ALWAYS-ON**
   - **ON-DEMAND**
   - **CR:** Three carriage returns must be received from the Bluetooth side before TCP/UDP connection is established to the remote server.
7. In **Connection Termination,** select a disconnect method for the IP pipe. Options are:
   - **ALWAYS-ON:** Connected.
   - **SEQUENCE:** A sequence of characters received from the Bluetooth side used to disconnect the IP pipe.
   - **TIMEOUT:** The IP pipe connection disconnects if the configured timer expires with no data sent or received. Note: Timeout of zero disables the timeout. It is the equivalent of ALWAYS-ON.

Configuring security settings

To configure security settings:

1. Make sure you select **SSL/TLS** under **Protocol.**
2. If the Security Setting section is hidden,, click the **Show** link to the right.
3. Select any TLS version. Check **TLSv1.2** and/or **TLSv1.**1 Default: TLSv1.2 is enabled.
4. By default **Use default cipher suite** is selected. Uncheck to select a preferred Cipher Suite.

Bluetooth Low Energy

This feature is available for Standard and Premium accounts only.

Bluetooth Low Energy allows you to search and/or scan for BLE devices. You can connect with selected BLE device to obtain the list of UUIDs for services and characteristics that are supported on the device.

.

1. On a device's **Device Files** tab, click **Use As a Template for New Config** and then go to **Bluetooth Low Energy > Settings**, check the **Enabled** box.
2. Enter the Bluetooth device's **Name** and **MAC Address**.
3. Select a **Power Mode**, select from the drop-down including **Custom, High, Medium or Low**. If you select Custom, select the **RX Power Mode** and **TX Power Mode**. Options are **Low, Medium**, and **High**
4. Click **Submit**.

Deleting Firmware Files

You can delete a firmware file from the available firmware files in DeviceHQ device or remove the firmware file from a specific device.

Deleting a Firmware File from the Files Page

To delete a firmware file from the Files page:

1. Click **Files.**
2. Click the **Delete** icon,

. for the file you want to delete.
3. Click **OK** to confirm the deletion.

Deleting a Firmware File from the Device Information Window

To delete a firmware file from the Device information window:

1. Click **Devices** and then click on a device to view the device details.
2. Click the **Device Files** tab.
3. Click **Delete Config**.
4. Click **OK** to confirm the deletion.

Chapter 8 Admin

User Administration

The account registrant is the account manager by default. Once the account is created, additional users can be added.

The Users page lists all users that have access to the account. You can create, modify, or delete users from this page. User permission levels depend on the user account type, Manager or Basic

- A **Manager** has full read-write access to the system. This user can add/delete other users, edit/delete devices, and can perform firmware/configuration updates for devices.
- A **Basic** user has read-only access and cannot modify/delete any users or devices on the account.

Field	Description
Email	User's email address.
First Name	User's first name.
Last Name	User's last name.
Role	User's assigned role.

Adding Users

To add a new user account:

1. Click **Admin.**
2. Click **Users**.
3. Click **Invite User** in the upper right corner.
4. Select a user **Role.** Options are **Manager** or **Basic.**
5. Enter the user's **Email address**.
6. Enter the user's **First name** and **Last name**.
7. Click **Invite**.

DeviceHQ sends a login activation email to the provided email address.

Editing Existing User Information

To edit an existing user account:

1. Click **Admin.**
2. Click **Users.**
3. Click the **Edit** icon, , for the account you want to edit.
4. Make desired changes. Refer to User Administration for field descriptions.

5. Click **Update User**.

Deleting User Accounts

To delete a user account:

1. Click **Admin.**
2. Click **User.**
3. Click the **Delete** icon. ✖, for the user account you want to delete.
4. Click **OK** to confirm the deletion.

Notifications

Notifications provide users device status information. They can be displayed on the Home Page and sent as an email or text message. Users can define when the system triggers notifications.

Notification Types

- **Low Signal** - Signal strength is below the set threshold in dB.
- **Missed Check-in** - The device missed a check-in interval.
- **High data usage** - Data usage is above the threshold value.
- **Failed Actions** - A failed action occurred during the notification period.
- **Device Reboot** - The device rebooted during the notification period.

Notifications Page Fields

Field	Description
Device	Device name.
Event	Event that triggered the notification.
Sent At	Date and time notification was sent.
Recipients	Email address of user who received the notification.

Creating Notifications

To set up notifications for your devices:

1. Click **Admin.**
2. Click **Notifications.**
3. Click **Settings.**
4. Check **Enable notifications.**
5. To edit each notification, including enabling or disabling each event notification, click the Edit icon, , for the notification.

6. Add a **Recipient Group**. For more information, refer to Setting Up Recipient Groups.
7. Click **OK**.

Setting Up Recipient Groups

Recipient Groups are used when a Notification Event is triggered. To set up a Recipient Group:

1. On the **Admin Tools** page, click **Notifications**.
2. Click **Settings.**
3. Click **Add Group**.
4. Enter in a **Group Name**.
5. To add phone numbers for **SMS** notifications, click **Add**.
6. Enter in the **Name** and **Phone Number** of the person you want to add.
   - To enter another person, click **Add** again.
7. To add Email addresses for email notifications, click **Add.**
8. Enter in the **Name** and **Email** address of the person you want to add.
   - To enter another person, click **Add** again.
9. Click **OK.**

Device Reboot Notification Settings

Specify how often you want to be notified when a device reboots.

When you click the Edit icon, , for the Device Reboot notification settings, a dialog box appears where you can edit the notification criteria.

1. Check or uncheck the **Enabled** check box to enable or disable the notification.
2. Choose the **Recipient Group.**
3. Choose how often to send the notification:
   - Every Check-in
   - Daily
   - Monthly
4. Choose how you want the notification to be sent by checking the **Email** or **SMS** check boxes.
5. Click **OK**.

Failed Actions Notification Settings

Specify how often you want to be notified when a scheduled action fails.

When you click the Edit icon, , for the Failed Actions notification settings, a dialog box appears where you can edit the notification criteria.

1. Check or uncheck the **Enabled** check box to enable or disable the notification.
2. Choose the **Recipient Group.**
3. Choose how often to send the notification:
   - Every Check-in
   - Daily
   - Monthly
4. Choose how you want the notification to be sent by checking the **Email** or **SMS** check boxes.
5. Click **OK**.

High Data Use Notification Settings

Specify how often you want to be notified when a device reaches the data usage threshold set for that device.

Note: Data usage threshold settings must be set on each device individually. This can be accessed on the device edit screen.

When you click the Edit icon, , for the High Data Use notification settings, a dialog box appears where you can edit the notification criteria.

1. Check or uncheck the **Enabled** check box to enable or disable the notification.
2. Choose the **Recipient Group.**
3. Choose how often to send the notification:
   - Every Check-in
   - Daily
   - Monthly
4. Choose how you want the notification to be sent by checking the **Email** or **SMS** check boxes.
5. Click **OK**.

Low Signal Notification Settings

Specify how often you want to be notified when a device experiences low signals.

When you click the Edit icon, , for the Low Signal notification settings, a dialog box appears where you can edit the notification criteria.

1. Check or uncheck the **Enabled** check box to enable or disable the notification.
2. Choose the **Recipient Group.**
3. Choose how often to send the notification:
   - Every Check-in
   - Daily
   - Monthly

4. Choose how you want the notification to be sent by checking the **Email** or **SMS** check boxes.
5. Click **OK**.

Missed Check-in Notification Settings

Specify how often you want to be notified when devices miss scheduled check-ins.

When you click the Edit icon, , for the Missed Check-in notification settings, a dialog box appears where you can edit the notification criteria.

1. Check or uncheck the **Enabled** check box to enable or disable the notification.
2. Choose the **Recipient Group.**
3. Choose how often to send the notification:
   - Every Check-in
   - Daily
   - Monthly
4. Choose how you want the notification to be sent by checking the **Email** or **SMS** check boxes.
5. Click **OK**.

Device Logs Page

The **Admin > Device Logs Page** shows device log requests and device logs.

Device Logs Requests

Field	Description
Description	Product description.
Product	Type of device.
Serial	Device serial number.
Requested	How the device logs were requested.
Requested Time	Date and time the device logs were requested.
Expected Time	Time when device logs were uploaded to DeviceHQ.

To delete a device log request, click the Delete icon, ✖, for that request.

Device Logs

Field	Description
Description	Product description.
Product	Type of device.
Serial	Device serial number.

Field	Description
Filename	Name of the device log zip file.
Length	Size of file.
MD5	Checksum
Date	Date the device log was created.

To download a device log, click the Download icon, , for that log.

To delete a device log request, click the Delete icon, , for that request.

Chapter 9 Store

The Store is where you find custom apps you can install on your devices that support custom apps. For information on developing and uploading custom apps, refer to the Developer Page.

Note: Support for Node-RED/Node.js on MultiTech AT91SAM9G25-based products has been discontinued starting with mPower 5.3.

To view all apps:

- Click **All.**

To view just your apps:

- Click **My Apps.**

To view just public apps:

- Click the **Public** check box.

To view just your account's Private apps:

- Click the **Private** check box.

To add an app to My Apps:

- Click **Add to My Apps**. This makes the app available for installing on your device.

To remove an App from My Apps:

- Click **Remove from My Apps.**

Chapter 10 Developer

Accessing the DeviceHQ Developer Page

To gain access to the Developer page for uploading apps to the Store, your account needs a Developer Key. If Developer appears in the top navigation bar, you have already have a developer key.

To generate a Developer Key in Device:

1. If not logged in to DeviceHQ, log in.
2. Click your user name in the upper right corner of the page.
3. Click **My Profile.**
4. Click **Generate Developer Key.**

Developer is now an option in the top navigation bar.

Developer Page

Use the Developer Page to add, edit, and delete apps. Added apps are then available to users in the Store Page.

For information on developing apps for your Conduit product, refer to the DeviceHQ App Developer Guide available at https://multitech.com/wp-content/uploads/S000756_DeviceHQ_App_Developer_Guide.pdf.

Field	Description
App Name	Name of the app.
App Type	Node-RED or Custom. **Note:** Support for Node-RED/Node.js on MultiTech AT91SAM9G25-based products has been discontinued starting with mPower 5.3.
Description	App description. Also appears in the App Store.
Status	Indicates if device is private, public, or inactive.

Downloading the Custom App Template

The custom app template is a tar file template for a custom app. To download it, click **Download Custom App Template**.

Adding an Application to the App Store

To add an app to the Store:

1. If not logged into DeviceHQ, log in.
2. Click the **Developer** tab.

3. Click **Upload App.**
4. Click **Choose File** and select the app file you want to add to the store.
5. On the App list, find the newly uploaded app and click the **Edit** icon.
6. Select the app **Configuration** file to upload or select an application configuration file. For a new configuration file, click **Upload Configuration**, **Choose File**, enter a **Description**, and click **OK**.
7. Change the status to **Active** and enter a short version description,
8. Click **Save**.
9. On the **Description** tab:
    a. If desired, change the name of the app.
    b. Enter a description of the app. This appears in the App Store.
    c. Choose an icon for the app.
10. On the **Publish** tab, select the app Status. Options are Public, Private, and Inactive.
    - All DeviceHQ users will be able to see and use **Public** apps.
    - Only users of the same account will be able to use **Private** apps.
    - **Inactive** apps do not appear in the store.
11. Select the **License Agreement** you want for your app. Options are GNU General Public License, MIT License, and Custom. If you select custom, you'll be prompted to enter a TOS URL or TOS text.
12. Click **Save**.

The application appears in the store.

Editing an App

To edit an app:

1. Click **Developer.**
2. Find the app you want to edit, and click the **Edit** icon, .
3. Make desired changes.
4. Click **Save.**

Deleting an App

To delete an app from your account:

Note: If you delete a Public app that you created that other users have deployed, you will no longer have access. Other users who have deployed the app will continue to have access to this app.

1. Click Developer.
2. Find the app you want to delete, and click the Delete icon, ✖.

3. Click **OK** to confirm deletion.

Revision History

Revision Number	Description	Revision Date
1.6	Updated broken links and MTE references.	July 2024
1.5	Added Upgrade Manager.	February 2022
1.4	Added Setting up an MTR6 and MTE2.	July 2021
1.3	Added Firewall and Wireless Configuration.	March 2021
1.2	Deprecated NodeRED.	October 2020
1.1	Added additional help topics.	April 2020
1.0	Original publication.	February 2020