mPower™ Edge Intelligence Conduit 300 Setup Guide

First-Time Setup

Setting Up Your Device using Setup Wizard (After Choosing Reset and Factory Default Settings)

Other than when you first power up the device, you must configure the device to factory default settings, reset it and then, access it through the default 192.168.2.1 IP address to see the first-time setup. To reset the device to factory default settings, go to **Administration > Save/Restore > Reset to Factory Default Configuration** and click the **Reset** button. This wizard helps you configure the main features of your device for initial setup.

Here are the steps for first-time setup:

1. Upon power up for the first time or after you set factory default settings, the device goes into commissioning mode. The system requires you to set up an admin user. Enter your desired username and click **OK**.
2. Enter a desired password for the admin user and click **OK**. This password must be of sufficient length and strength (with a mix of character classes such as letters, numbers, and symbols). Enter the password again to confirm. Click **OK**.
3. Log into your device using your new username and password.
4. Call Home Remote Management allows your device to receive configuration updates and firmware files from MultiTech's DeviceHQ platform. Ensure that your device is set up on DeviceHQ before calling home, or enabling this option.
5. Set the date, time, and time zone.
    a. Enter the desired **Date**.
    b. Enter the desired **Time**.
    c. Select the **Time Zone** in which the device operates.
    d. Click **Next**.
6. Configure LAN network interfaces Eth0 and Br0. Enter the device address and network information (Network Router mode only):
    a. In the **Network Interface Configuration** – **eth0** section, leave the **eth0** assigned to the bridge **br0**, or unassign **eth0** from bridge and enter network settings for the **eth0** interface - **IPv4 Address** and **Mask.**
    b. In the **Network Interface Configuration** – **br0** section, enter network settings for the **br0** interface **IPv4 Address** and **Mask**.
7. In the **Network Interface Configuration** – **eth1** section, leave the **eth1** assigned to the bridge **br0**, or unassign **eth1** from bridge and enter network settings for the **eth1** interface - **IPv4 Address** and **Mask.**

8. Configure your device's **PPP**. (NOTE: This is not available, if your device has no radio.)
    a. Enter the **APN** (Access Point Name). The APN is assigned by your wireless service provider. (This field is not available on all models.)
    b. Click **Next**.

9. Set up **PPP Authentication**:
    a. Select the authentication protocol **Type** used to negotiate with the remote peer: **PAP, CHAP, or PAPCHAP**. The default value is **NONE**.
    b. Enter the **Username** with which the remote peer authenticates. Optional. Username is limited to 60 characters.
    c. Enter the **Password** with which the remote peer authenticates. Optional. Password is limited to 60 characters.

10. Configure **Remote Management**

    Remote management enables the device to connect to MultiTech's DeviceHQ device management platform. To configure DeviceHQ, it is recommended that you leave the default settings in place, and:
    a. Enter account key and click **Enable.**

11. Configure **HTTP/HTTPS Access**.
    a. In the **HTTP Redirect to HTTPS** panel define how the device handles HTTP traffic. Check **Enabled** to enable HTTP and redirect to HTTPS.
    b. Configure HTTP **Port**. By default, 80.
    c. Check **Via LAN** (enabled by default) to allow traffic from local area network.
    d. Check **Via WAN** (disabled by default) to allow traffic from the wide area network.
    e. In the **HTTPS** panel, define how the device handles secure HTTP traffic.
    f. Check **Via WAN** to allow traffic from the wide area network. Note: HTTPS traffic via LAN is enabled by default and cannot be changed.
    g. Configure HTTPS **Port**. By default, 443.

12. Set up **Bootloader Protection** by setting a u-boot password.
    a. Enter a password and click **Enable**. The password will be set immediately.
    b. To change the password, enter a new password and click **Change Password**.
    c. To disable the password, click **Disable**.

13. Click **Finish**.
14. To save your changes, click **Save and Restart**.

Note: **SSH** on LAN and WAN will be disabled by default. To enable SSH, go to Administration->Access Configuration on the WebUI and select **Enabled**, and **Via LAN**, click **Submit**, and then **Save And Restart**. The **Bootloader Protection** settings depend on the previous u-boot configuration and are preserved when device is reset to factory defaults.