UBIQUITI
NETWORKS

UniFi®

Enterprise System Controller

Release Version: 5.6.2

User Guide

Table of Contents

Chapter 1: Software Installation

Introduction

Thank you for purchasing the Ubiquiti Networks® UniFi® Enterprise System. The UniFi devices are bundled with the UniFi Controller software, which allows you to manage your UniFi network using a web browser.

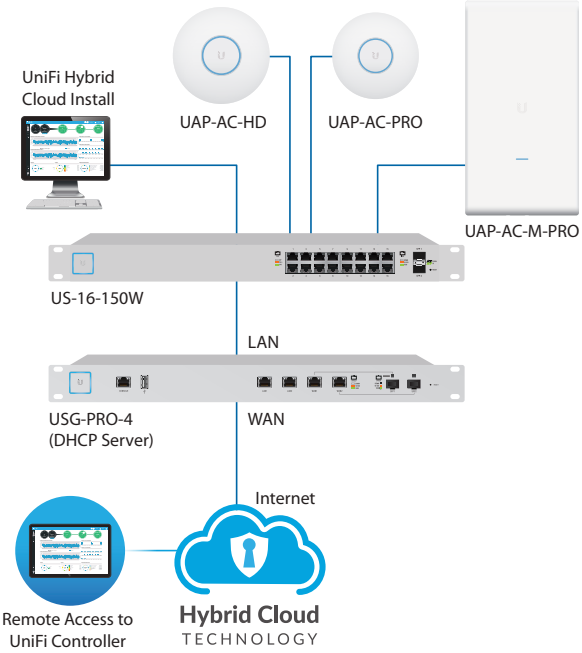
This User Guide is for use with version 5.6.2 or above of the UniFi Controller software.

System Requirements

- Linux, Mac OS X 10.11 (or above), or Microsoft Windows 7/8/10
- Java Runtime Environment 1.8 or above recommended
- Web Browser: Google Chrome (Other browsers may have limited functionality.)

Network Topology Requirements

- A DHCP-enabled network (so any device can obtain an IP address)
- One of the following:
  - UniFi Cloud Key
  - A management station running the UniFi Controller software, located either on-site and connected to the same Layer-2 network, or off-site* in a cloud or NOC
- For the public address system capability of the UAP-AC-EDU: A compatible Android™ or iOS device located on the same Layer-2 network as the UniFi Controller and UniFi APs



Sample Network Diagram

* Requires Layer-3 adoption. For details, refer to: http://ubnt.link/UniFi-Layer3-Adoption

All UniFi devices support off-site management controllers.

Follow the instructions in this chapter after you install the hardware, which is described in the Quick Start Guide.

Software Installation

Download the latest version of the UniFi Controller software at downloads.ubnt.com/unifi

Follow the instructions for your specific computer or device type.

UniFi Cloud Key Users

If you have the UniFi Cloud Key, please refer to **"UniFi Cloud Key" on page 5** for more information.

UniFi Cloud Users

If you have a UniFi cloud account, please refer to **"UniFi Cloud Account" on page 13** for more information.

Linux Users

Please refer to the UniFi blog on our community site at: http://ubnt.link/UniFi-Blog

Mac Users

1. Launch **UniFi.pkg**.

2. Click **Continue** and follow the on-screen instructions to install the software.

3. Go to **Go** > **Applications** and double-click the *UniFi* icon.

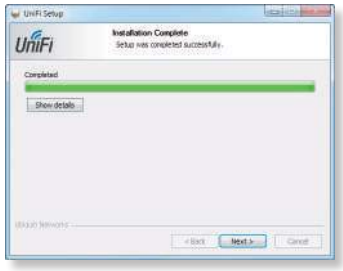
Proceed to **"Configuring the UniFi Controller Software" on page 2**.

PC Users

1. Launch **UniFi-installer.exe**.
2. Click **Install**.

3. If your computer doesn't have Java 1.6 or above installed, you will be prompted to install it. Click **Install** to continue.

4. Click **Next**.



5. Ensure that the *Start UniFi Controller after installation* option is checked and click **Finish**.

Note: The UniFi Controller software can also be launched from **Start** > **All Programs**.

Configuring the UniFi Controller Software

1. The UniFi Controller software startup will begin. Click **Launch a Browser to Manage Wireless Network**.

Note: The above applies to Windows and OS X only. On Linux, open a browser and go to the following URL: **https://<IP_address_of_controller>:8443**

2. Select your country and time zone. Alternatively, you can click **restore from a previous backup** to use a file that contains your backup settings. Click **Next**.

Note: **Enable Auto Backup** is on by default. Toggle off if you wish to disable.

Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

3. Select the devices that you want to configure and click **Next**.

Note: If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

4. The UniFi Setup Wizard will create a secure primary wireless network for your devices.

Perform the following steps:

a. Enter the wireless network name (SSID) in the *Secure SSID* field.

b. Enter a passphrase to be used for your primary network in the *Security Key* field.

c. To enable guest access, select **Enable Guest Access**, and enter a guest network name in the *Guest SSID* field.

d. Click **Next**.

5. Create the superadmin for your UniFi Controller.

Perform the following steps:

a. Enter an admin name in the *Admin Name* field.

b. Enter an email address in the *Admin Email* field.

c. Enter a password in the *Password* field to use when accessing the management interface as a superadmin.

d. Confirm your password in the *Confirm Password* field.

e. To use the same login for SSH access, select **Use the same name and password for SSH access**.

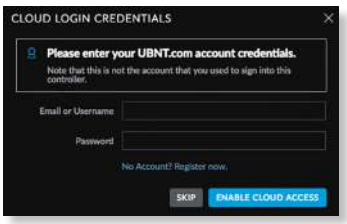
f. To set up a separate login for SSH access, enter an admin name and password for the *Device Authentication* fields.

g. Click **Next**.

Note: Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller. Ensure that you save the superadmin login information for future use.

6. Review your settings. Click **Finish** to save your settings or click *Back* to make changes. Once the wizard is finished, the browser will be redirected to the *Cloud Login Credentials* screen.

7. Enter your Ubiquiti account email/username and password to enable cloud access. Alternatively, you can click **Register now** to create a Ubiquiti account. Click **Enable Cloud Access**.



8. A login screen will appear for the UniFi Controller management interface. Enter the admin name and password that you created and click **Sign In**.

Proceed to **"Using the UniFi Controller Software" on page 17** for information on using the UniFi Controller software.

Chapter 2: UniFi Cloud

Introduction

You can access the UniFi Controller via the UniFi Cloud Key and/or the UniFi cloud account. This chapter describes the following:

- UniFi Cloud Key
- **"UniFi Cloud Account" on page 13**

UniFi Cloud Key

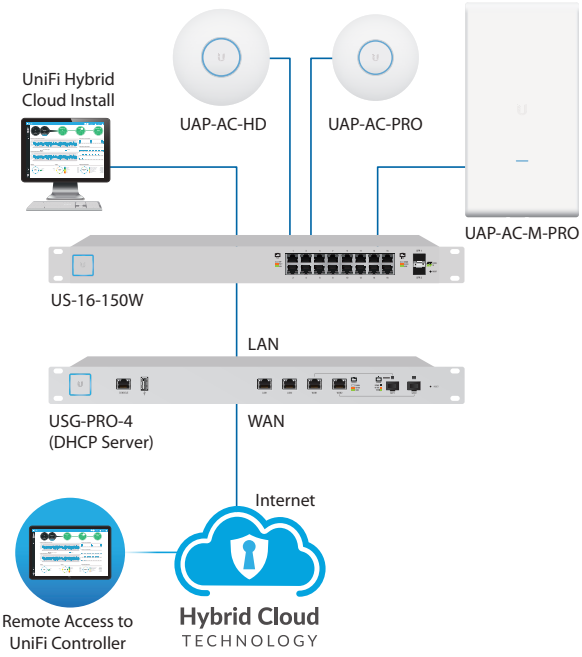
The UniFi Cloud Key includes the pre-installed UniFi Controller software.

System Requirement

Web Browser: Google Chrome (Other browsers may have limited functionality.)

Network Topology Requirement

A DHCP-enabled network (for the UniFi Cloud Key to obtain an IP address)



Sample Network Diagram

Software Installation

After you follow the hardware installation instructions in the UniFi Cloud Key Quick Start Guide, use one of the following methods to launch the software:

- If you are using Chrome, go to the *Chrome Instructions* section (recommended).
- If you are using a different web browser, go to **"Instructions for Other Web Browsers" on page 7**.

Chrome Instructions

1. Ensure that your host system is on the same Layer-2 network as the UniFi Cloud Key.
2. Launch the Chrome web browser and type **https://unifi.ubnt.com** in the address field. Press **enter** (PC) or **return** (Mac).

3. Enter the username and password for your UBNT account. Click **Sign In**.

4. Click **Discover Cloud Key**.

Note: The default fallback IP address of the UniFi Cloud Key is *192.168.1.30*.

5. If the Ubiquiti® Device Discovery Tool is already installed, proceed to step 7.

   If the tool is not installed, you will be prompted to add it. Proceed to step 6.

6. To install the tool:
   a. Click **Install**.

   b. Click **Add app** to confirm.

7. The Ubiquiti Device Discovery Tool will search for the UniFi Cloud Key. Click **Adopt** in the Cloud Key's *Actions* column to continue.

8. If the Cloud Key firmware is not the latest version, click **Upgrade Firmware** to upgrade the firmware.

9. Click **Open Controller Wizard** to set up the Controller on the Cloud Key.

10. The *UniFi Setup Wizard* screen appears. Select your country and time zone. Alternatively, you can click **restore from a previous backup** to use a file that contains your backup settings. Click **Next**.

Note: **Enable Auto Backup** is on by default. Toggle off if you wish to disable.

Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

11. Select the devices that you want to configure and click **Next**.

Note: If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

12. The UniFi Setup Wizard will create a secure primary wireless network for your devices.

Perform the following steps:

   a. Enter the wireless network name (SSID) in the *Secure SSID* field.
   b. Enter a passphrase to be used for your primary network in the *Security Key* field.
   c. To enable guest access, select **Enable Guest Access**, and enter a guest network name in the *Guest SSID* field.
   d. Click **Next**.

13. Create the superadmin for your UniFi Controller.

Perform the following steps:

a. Enter an admin name in the *Admin Name* field.

b. Enter an email address in the *Admin Email* field.

c. Enter a password in the *Password* field to use when accessing the management interface as a superadmin.

d. Confirm your password in the *Confirm Password* field.

e. To use the same login for SSH access, select **Use the same name and password for SSH access**.

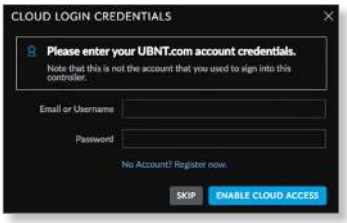
f. To set up a separate login for SSH access, enter an admin name and password for the *Device Authentication* fields.

g. Click **Next**.

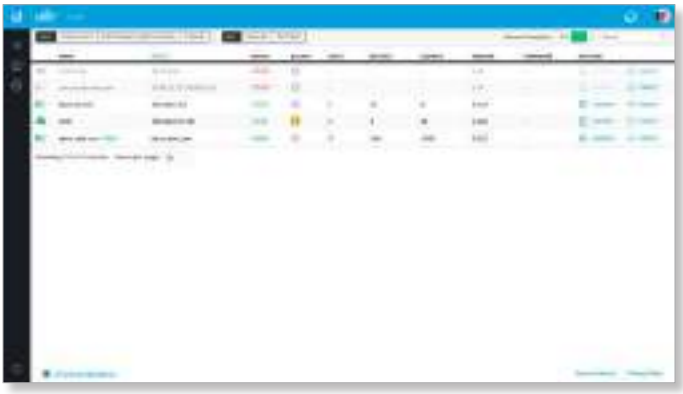
Note: Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller. Ensure that you save the superadmin login information for future use.

14. Review your settings. Click **Finish** to save your settings or click *Back* to make changes. Once the wizard is finished, the browser will be redirected to the *Cloud Login Credentials* screen.

15. Enter your Ubiquiti account email/username and password to enable cloud access. Alternatively, you can click **Register now** to create a Ubiquiti account. Click **Enable Cloud Access**.



16. Wait for the UniFi Controller to be adopted, and then click **Launch**.



Proceed to **"Using the UniFi Controller Software" on page 17** for information on using the UniFi Controller software.

Note: A future feature will enable backup of the UniFi Controller database and configuration on the included microSD card.

Instructions for Other Web Browsers

1. Ensure that your host system is on the same Layer-2 network as the UniFi Cloud Key.
2. The UniFi Cloud Key is set to *DHCP* by default, so it will try to automatically obtain an IP address. Assign a specific IP address to the UniFi Cloud Key, or check the DHCP server for its IP address.

   Note: The default fallback IP address of the UniFi Cloud Key is *192.168.1.30*.

3. Launch the web browser. In the address field, type **https://** followed by the appropriate IP address. Press **enter** (PC) or **return** (Mac).

4. Click **Manage** to run the UniFi Setup Wizard.

Note: You can click *Configure* to change the settings of the UniFi Cloud Key (refer to **"UniFi Cloud Key Configuration" on page 9** for more information). The default login is *ubnt/ubnt* or *root/ubnt*.

5. The *UniFi Setup Wizard* screen appears. Select your country and time zone. Alternatively, you can click **restore from a previous backup** to use a file that contains your backup settings. Click **Next**.

Note: **Enable Auto Backup** is on by default. Toggle off if you wish to disable.

Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

6. Select the devices that you want to configure and click **Next**.

Note: If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

7. The UniFi Setup Wizard will create a secure primary wireless network for your devices.

Perform the following steps:

a. Enter the wireless network name (SSID) in the *Secure SSID* field.

b. Enter a passphrase to be used for your primary network in the *Security Key* field.

c. To enable guest access, select **Enable Guest Access**, and enter a guest network name in the *Guest SSID* field.

d. Click **Next**.

8. Create the superadmin for your UniFi Controller.

Perform the following steps:

a. Enter an admin name in the *Admin Name* field.

b. Enter an email address in the *Admin Email* field.

c. Enter a password in the *Password* field to use when accessing the management interface as a superadmin.

d. Confirm your password in the *Confirm Password* field.

e. To use the same login for SSH access, select **Use the same name and password for SSH access**.

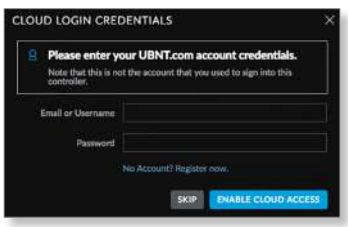
f. To set up a separate login for SSH access, enter an admin name and password for the *Device Authentication* fields.

g. Click **Next**.

Note: Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller. Ensure that you save the superadmin login information for future use.

9. Review your settings. Click **Finish** to save your settings or click *Back* to make changes. Once the wizard is finished, the browser will be redirected to the *Cloud Login Credentials* screen.

10. Enter your Ubiquiti account email/username and password to enable cloud access. Alternatively, you can click **Register now** to create a Ubiquiti account. Click **Enable Cloud Access**.



A login screen will appear for the UniFi Controller management interface. Enter the admin name and password that you created and click **Login**.

Proceed to **"Using the UniFi Controller Software" on page 17** for information on using the UniFi Controller software.

Note: You can back up the UniFi Controller database and configuration on the included microSD card.

UniFi Cloud Key Configuration

Login Instructions

1. Ensure that your host system is on the same Layer-2 network as the UniFi Cloud Key.
2. The UniFi Cloud Key is set to *DHCP* by default, so it will try to automatically obtain an IP address. Assign a specific IP address to the UniFi Cloud Key, or check the DHCP server for its IP address.

   Note: The default fallback IP address of the UniFi Cloud Key is *192.168.1.30*.

3. Launch the web browser. In the address field, type **https://** followed by the appropriate IP address. Press **enter** (PC) or **return** (Mac).

4. You have two options:
   - **Manage** Click **Manage** to access the UniFi Controller. Proceed to **"Using the UniFi Controller Software" on page 17** for more information.
   - **Configure** Click **Configure** to change the settings of the UniFi Cloud Key.

5. After you click *Configure*, enter the *Username* and *Password* (the default login is *ubnt*/*ubnt*). Then click **Login**.

The *Main* screen will appear.

Navigation Bar

The UniFi Cloud Key configuration consists of three primary pages:

- **"Main" on page 10**
- **"Configuration" on page 11**
- **"Maintenance" on page 12**

Username

At the top right of each screen, click the *Username* to display the *Change Password, Change Username,* and *Logout* options:

Change password To change the password, click Change password . The *Change Password* screen will appear:

- **Old password** Enter the current password (the default is *ubnt*).
- **New password** Enter the new password.
- **Confirm password** Enter the new password again.
- **Submit** Click **Submit** to apply changes.
- **Cancel** Click *Cancel* to discard changes.

Change username To change the username, click Change username . The *Change Username* screen will appear:

- **New password** Enter the new username.
- **Submit** Click **Submit** to apply changes.
- **Cancel** Click *Cancel* to discard changes.

Logout To manually sign out of the UniFi Cloud Key configuration, click Logout .

Main

The *Main* screen displays basic status information about the UniFi Cloud Key.

Status

Device Name Displays the hostname or alias of the UniFi Cloud Key.

Uptime Displays the duration of time the UniFi Cloud Key has been running.

Version Displays the version number of the UniFi Cloud Key firmware.

MAC Address Displays the MAC address or hardware identifier of the UniFi Cloud Key.

Date Displays the current date and time.

UniFi

Version Displays the version number of the UniFi Controller software.

Status Displays the status of the UniFi Controller software.

Disk Space

Available Displays the percentage of available disk space.

Used Displays the amount of used disk space.

Free Displays the amount of available disk space.

Total Displays the total amount of disk space.

SD Card

Available Displays the percentage of available space on the SD card.

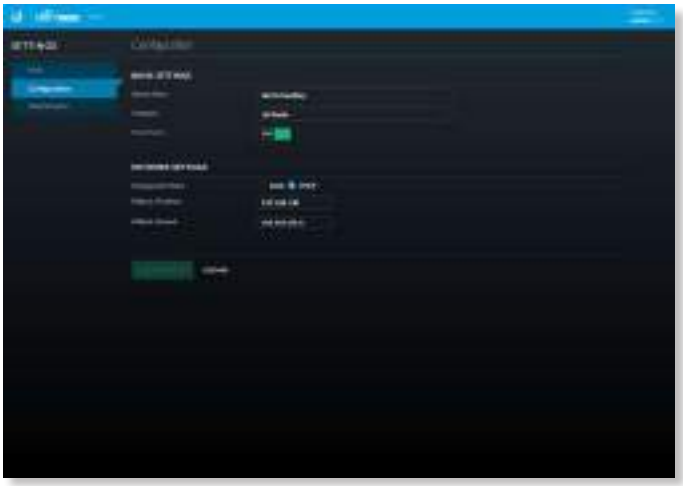
Used Displays the amount of used space on the SD card.

Free Displays the amount of available space on the SD card.

Total Displays the total amount of space on the SD card.

Configuration

The *Configuration* screen allows you to configure the basic and network settings of the UniFi Cloud Key.



Basic Settings

Device Name Enter a descriptive name or identifier for the UniFi Cloud Key. Also known as a host name.

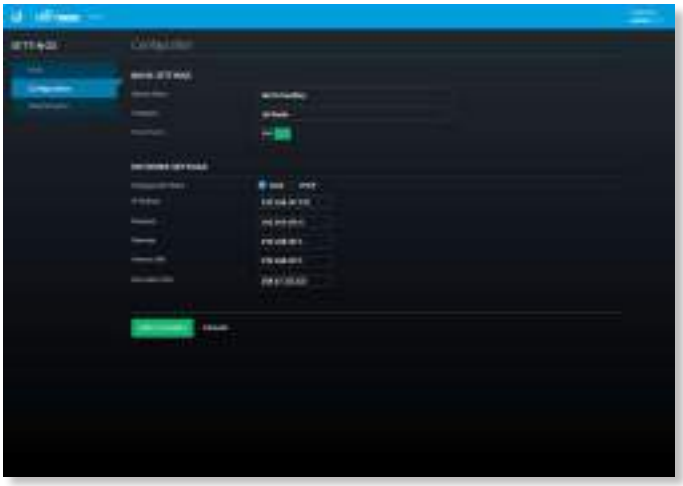
Time Zone Select the appropriate time zone.

Reset Button Use of the hardware *Reset* button on the UniFi Cloud Key is enabled by default. To prevent an accidental reset to default settings, click to toggle *Off*.

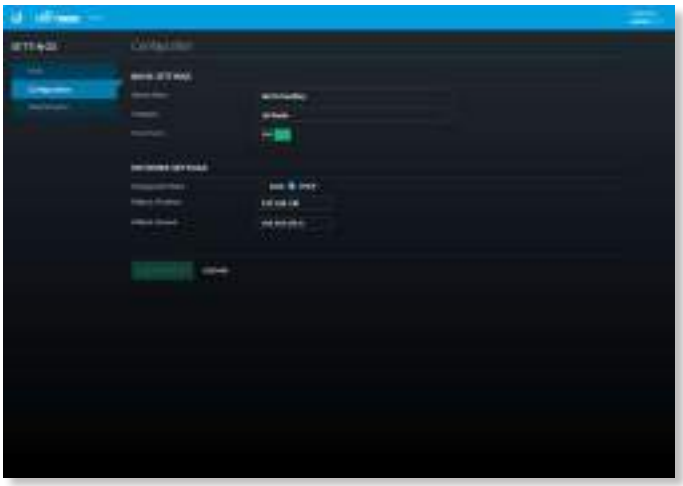
Network Settings

Configuration Mode Select the appropriate mode: **Static** for fixed settings or **DHCP** for automatic configuration by your DHCP server.

- **Static** Enter the following information:
  - **IP Address** Enter the local IP address of the UniFi Cloud Key.
  - **Netmask** Enter the subnet mask of the UniFi Cloud Key.
  - **Gateway** Enter the IP address of the network's gateway router.
  - **Primary DNS** Enter the IP address of the network's primary DNS server.
  - **Secondary DNS** Enter the IP address of the network's secondary DNS server.



- **DHCP** The use of the Dynamic Host Configuration Protocol (DHCP) is the default. The UniFi Cloud Key automatically acquires network settings from the network's DHCP server.
  - **Fallback IP Address** Enter the IP address for the UniFi Cloud Key to use if an external DHCP server is not found.
  - **Fallback Netmask** Enter the netmask for the UniFi Cloud Key to use if an external DHCP server is not found.

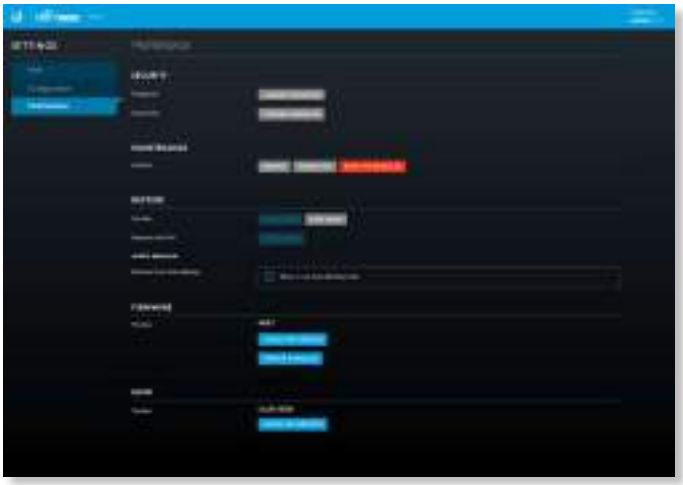


Apply Changes Click **Apply Changes** to save changes.

Discard Click *Discard* to cancel changes.

Maintenance

The *Maintenance* screen contains administrative options, so you can change the password, reboot the UniFi Cloud Key, power it off, reset it to factory defaults, restore the UniFi Controller software, upgrade the UniFi Cloud Key firmware, or upgrade the UniFi Controller software.



Security

Password To change the password, click **Change Password**. The *Change Password* screen will appear:

- **Old password** Enter the current password (the default is *ubnt*).
- **New password** Enter the new password.
- **Confirm Password** Enter the new password again.
- **Submit** Click **Submit** to apply changes.
- **Cancel** Click *Cancel* to discard changes.

Username To change the username, click **Change Username**. The *Change Username* screen will appear:

- **New username** Enter the new username.
- **Submit** Click **Submit** to apply changes.
- **Cancel** Click *Cancel* to discard changes.

Maintenance

Reboot Click **Reboot** to powercycle the UniFi Cloud Key.

Power Off Click **Power Off** to turn off the UniFi Cloud Key.

Reset to Defaults Click **Reset to Defaults** to reset the UniFi Cloud Key to its factory default settings. This option will reboot the UniFi Cloud Key, and all factory default settings will be restored.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before resetting the UniFi Cloud Key to its defaults.

Restore

Service While the UniFi Controller software is running, click **Stop UniFi** to stop it. To restart the software, click **Start UniFi** to restart it.

Restore from file Click **Choose File** to restore the UniFi Controller from a file you specify. Follow the on-screen instructions.

Auto Backup

Restore from Auto Backup Click to restore from the automatic backup file. Follow the on-screen instructions.

Firmware

Version Displays the version number of the UniFi Cloud Key firmware.

Check for Updates Click **Check for Updates** to see if there is a newer firmware version. If there is, then you can follow the on-screen instructions to upgrade now.

Update Manually Click **Update Manually** to update the firmware. The *Please Confirm Update* screen will appear.

You have two options:

- **upload file** If you have the firmware saved in a specific location, then click **Select File** to browse for the file.

- **get file from URL** If you know the URL of the firmware's location, then enter it in the *URL* field.

- **Update** Click **Update** to proceed with the update.
- **Cancel** Click *Cancel* to skip the update.

Note: Updating the UniFi Cloud Key firmware will also update the UniFi Controller software. We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before updating the UniFi Cloud Key firmware.

UniFi

Version Displays the version number of the UniFi Controller software.

Check for Updates Click **Check for Updates** to see if there is a newer software version. If there is, then you can follow the on-screen instructions to upgrade now.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before upgrading the UniFi Controller software.

UniFi Cloud Account

You must be a superadmin for initial cloud management. Once cloud access is enabled by the superadmin, then any other admin can also enable cloud access.

Note: The cloud account is also known as the Single Sign-On (SSO) account.

Login Instructions

1. Launch the Chrome web browser and type **https://** followed by the appropriate *Controller Hostname/IP* address as specified in **"Settings > Controller" on page 56**. Press **enter** (PC) or **return** (Mac).

2. Enter the username and password for your UBNT account. Click **Sign In**.

A list of UniFi Controllers will appear.

You can apply one of the following primary filters:

- **All** Displays all UniFi Controllers.
- **Cloud Key** Only displays UniFi Cloud Keys.
- **Software Installation** Only displays instances of software installations.
- **Cloud** Only displays UniFi Controllers with cloud access.

A secondary filter is available:

- **All** Displays all UniFi Controllers.
- **Online** Only displays online UniFi Controllers.
- **Offline** Only displays offline UniFi Controllers.

Discover Cloud Key Click to discover a UniFi Cloud Key on your local network.

Search Search Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

You can click any of the column headers to change the list order.

(icon) Displays the icon corresponding to the device running the UniFi Controller. Green indicates an active UniFi Controller. Gray indicates an inactive UniFi Controller.

UniFi Cloud Key

Computer

Name Displays the hostname, alias, or MAC address of the device running the UniFi Controller. You can click the name to get additional details at the bottom of the screen. (Go to **"Additional Details" on page 15** for more information.)

Host Displays the IP address of the device running the UniFi Controller.

Status Displays the status of the UniFi Controller:

- **Online** ONLINE The UniFi Controller is available for access.
- **Offline** OFFLINE The UniFi Controller is not available.
- **Manage By Other** MANAGE BY OTHER The UniFi Controller is not available because it is managed by another admin.

Alerts Displays the number of alerts for the UniFi Controller.

Sites Displays the total number of sites managed by the UniFi Controller.

Devices Displays the total number of devices managed by the UniFi Controller.

Clients Displays the total number of clients on the sites managed by the UniFi Controller.

Version Displays the software version number of your UniFi Controller.

Firmware Displays the firmware version number, if available.

Actions Click a button to perform the desired action:

- **Launch** Click LAUNCH to access the UniFi Controller. Proceed to **"Using the UniFi Controller Software" on page 17** for more information.
- **Forget** Click FORGET to remove the UniFi Controller from your cloud account.

Chat At the lower left of the screen, click to open a window for online chat support.

Admin

At the top right of the screen, click the account icon (by default or the user-specified icon) to display the *Preferences*, *My Account* and *Sign Out* options:

Store Click Store to access the store site for UniFi products.

Preferences To change your account preferences, click Preferences. The *Preferences* screen will appear:

The available settings are:

- **Condensed view** Enabled by default. The table padding is condensed and the font size is minimized to fit as much data on the screen as possible.
- **Dark settings** Enabled by default. A dark theme is used on the *Settings* screens.
- **Wide panel** Disabled by default. If enabled, the *Details* panel is displayed with maximum width.
- **Show device adopt requirements** Enabled by default.
- **Confirm before device restart** Enabled by default.
- **Confirm before device reset** Enabled by default.
- **Find Cloud Key automatically** Disabled by default.
- **Find Device automatically** Disabled by default.
- **Show Demo Controller** Enabled by default.
- **Show connection requirements** Enabled by default.
- **Language** The default is *English*.

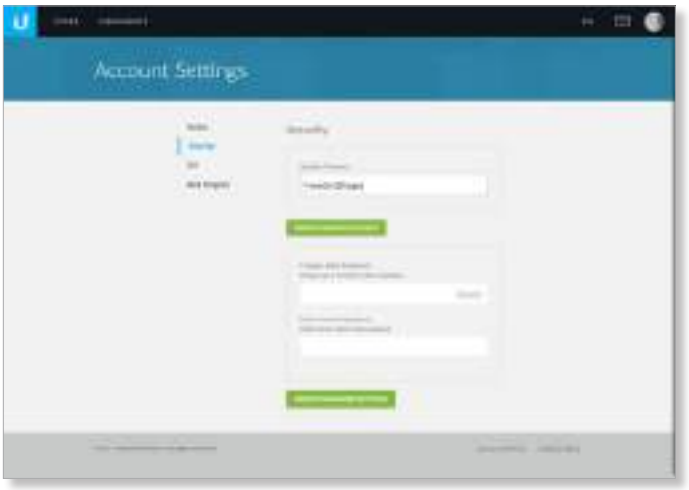
Your changes are automatically saved. To cancel changes, click **Cancel**. To reset to factory default settings, click **Reset to Defaults**.

My Account To change your account settings and/or password, click My Account. The *Account Settings* screen will appear:

There are four pages available:

- **Profile** Access your account settings:
  - **First Name** Enter your first name.
  - **Last Name** Enter your last name.
  - **Username** Enter your login username.
  - **Email** Enter the email address of your cloud account.
  - **Current Password** Enter your current account password.
  - **Update Settings** Click to apply your changes.
- **Security** Change the duration of your session and/or your account password:
  - **Session Timeout** Select the appropriate duration of your session. You will be automatically logged out for security purposes.
  - **Update Session Settings** Click to apply your changes.

- **Create a New Password** Enter a new password with at least eight characters.
- **Enter Current Password** Enter your current account password.
- **Update Password Settings** Click to apply your changes.



- **2FA** Follow the on-screen instructions if you want to use the Google Authenticator app for two-factor authentication (2FA).
  - **Insert 2FA token** Enter the 6-digit code after you have scanned the on-screen QR code.
  - **Enable 2FA** Click to apply the code.

- **Beta Program** Follow the on-screen instructions if you want to join the beta program.
  - **I agree to the Terms of Service & Beta Program Guidelines** Select to agree to the terms and guidelines for joining the beta program.
  - **Join Now** Click to join the beta program.

Sign Out To manually sign out of the cloud account, click Sign Out.

Additional Details

Select a UniFi Controller to display more information on the right side of the screen.

- **(icon)** A green circle icon ● indicates an active UniFi Controller. Gray indicates an inactive UniFi Controller.
- **(controller_name)** Displays the *Controller Hostname/IP* address as specified in **"Settings > Controller" on page 56**.
- **IP Address** Displays the IP address of the device running the UniFi Controller.

Sites Overview

- **Search** Search Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.
- **Launch Using Cloud** If cloud access is available, then you can use it to access the UniFi Controller. Click the appropriate option: **Launch using Cloud**, **Launch using hostname of your Controller**, or **Launch using IP of your Controller**.

  For cloud access, these are the requirements:

  - Ports 443 (TCP), 3478 (UDP), and 443 (UDP) must be open.
  - If you access this Controller using unifi.ubnt.com, there will be some outbound UDP traffic if remote access is ongoing (via WebRTC), and the port numbers are dynamic.

- **Name** Displays the name of the site. You can click the name to get additional details on the right.
- **Status** Indicates the number of alerts and status of each dashboard node.
  - **(Unread Alerts)** 6 Displays the number of unread alerts.
  - **(WAN/LAN/WLAN)** The status of each dashboard node: UniFi Security Gateway, UniFi wired network, or UniFi wireless network is indicated by color:
    - **Green** Indicates an active node.
    - **Red** Indicates that the node or some of its devices are offline.
    - **Gray** Gray indicates that there is no connection or there are no devices available for that node.
- **Actions** Click a button to perform the desired action:
  - **Launch** Click LAUNCH to access the UniFi Controller. Proceed to **"Using the UniFi Controller Software" on page 17** for more information.

Details

- **Software Version** Displays the software version number of the UniFi Controller.
- **Devices** Displays the total number of devices managed by the UniFi Controller.
- **Clients** Displays the total number of clients on the sites managed by the UniFi Controller.
- **Sites** Displays the total number of sites managed by the UniFi Controller.
- **Inform URL** Displays the URL, port, and path to the UniFi Controller. This tells UniFi APs where to look for the UniFi Controller.

Chapter 3: Using the UniFi Controller Software

The UniFi Controller software has a browser-based interface for easy configuration and management.

To access the interface, perform the following steps:

1. Launch the UniFi Controller application if it hasn't already been started.
   - Mac users: **Go > Applications > UniFi**
   - Windows users: **Start > All Programs > Ubiquiti UniFi**
2. The UniFi login screen will appear. Enter the username and password in the appropriate fields and click **Log In**.

Navigation Bar

The UniFi software consists of six primary pages. This User Guide covers each page with a chapter. For details on a specific page, refer to the appropriate chapter.

"Dashboard" on page 63

"Statistics" on page 71

"Map" on page 81

"Devices" on page 89

"Clients" on page 99

"Insights" on page 105

Common Interface Options

The common interface options are accessible from all tabs in the UniFi interface.

Current Site

The UniFi Controller can manage multiple UniFi networks, which are called sites. Each site has its own configurations, maps, statistics, guest portals, and site administrator accounts. The multiple sites are logically separated, and the initial site is named *Default*.

Current Site To view available sites or create a new site, click the *arrow* icon.

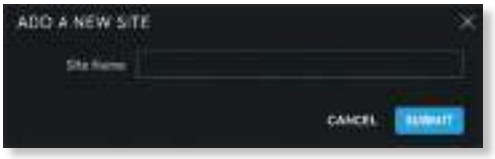
- **Sites overview** To display a list of available sites, click Sites overview. The *Sites Overview* screen will appear.

Each site is displayed with the following:

- **Name** Displays the name of the site.
- **Alerts** Displays the number of pending alerts.
- **WAN** The icon is color-coded to display the WAN connection status. Green indicates active; red indicates inactive.
- **LAN** The icon is color-coded to display the wired network connection status. Green indicates active; red indicates inactive.
- **Active** Displays the number of active wired devices.
- **Inactive** Displays the number of inactive wired devices.
- **Pending** Displays the number of wired devices pending adoption.
- **WLAN** The icon is color-coded to display the wireless network connection status. Green indicates active; red indicates inactive.

- **Active** Displays the number of active wireless devices.
- **Inactive** Displays the number of inactive wireless devices.
- **Pending** Displays the number of wireless devices pending adoption.
- **Users** Displays the number of wireless users and wired users.
- **Guests** Displays the number of wireless guests and wired guests.

- **Add new site** To create a new site, click + Add new site, and the *Add a New Site* screen will appear:



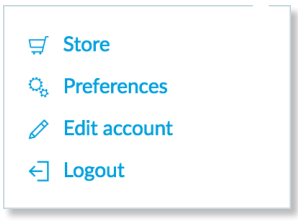
  - **Site Name** Enter a name that describes the site. It will be used in the *Current Site* drop-down menu.
  - **Cancel** Click to discard changes.
  - **Submit** Click to save changes.

- **Import Site** Click to import a new site. The *Import Site* screen will appear.

  - **Site Name** Enter a name that describes the site. It will be used in the *Current Site* drop-down menu.
  - **Choose File** Browse for the appropriate file.
  - **Cancel** Click to discard changes.

Username

At the top right of the screen, click the **Username** to display the *Store*, *Preferences*, *Edit Account,* and *Logout* options:



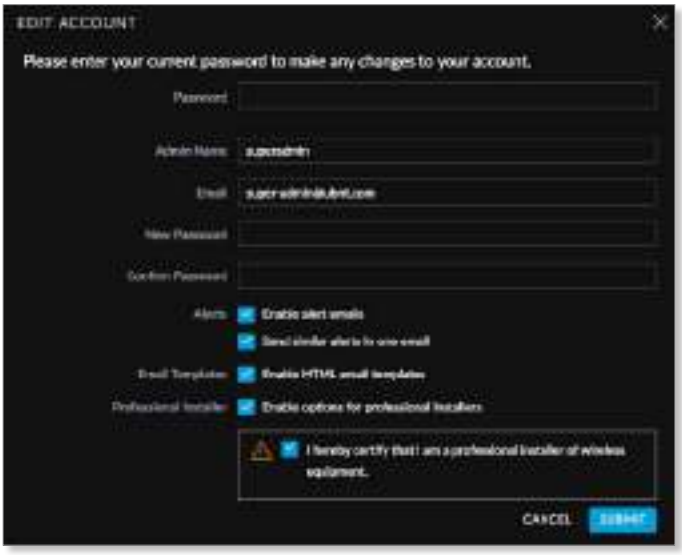
Store If enabled by the admin, there is a direct link to: **store.ubnt.com**

Preferences To change the UI settings, click Preferences.

- **Rows per panel** Displays the number of rows per page for tables in the property panels. The default is *10*.
- **Dark settings** Enabled by default. A dark theme is used on the *Settings* screens.
- **Condensed view** Enabled by default. The table padding is condensed and the font size is minimized to fit as much data on the screen as possible.
- **Responsive tables** Disabled by default. If enabled, the *Responsive tables* option removes columns on smaller-sized browsers to prevent excessive scrolling when the table columns are not customized.
- **Inline property panel** Enabled by default. When the property panel is inline, it compresses the main content when it is open. When the property panel is not inline, it opens on top of the content, as a popup.
- **Undocked panels** Disabled by default. Properties appear as overlays instead of in the property panel.
- **Confirm before blocking client** Enabled by default.
- **Confirm before device upgrade** Enabled by default.
- **Confirm before device restart** Enabled by default.
- **Enable dynamic dashboard** Disabled by default. If you enable it, then you can customize the Dashboard display. For more information, go to **"Dynamic Dashboard (beta)" on page 69**.
- **Auto discover devices** Enabled by default. Devices are automatically discovered.
- **Remember all refresh rates** Disabled by default. Quick refresh rates are not recommended for permanent use or large installations.
- **Enable refresh button** Disabled by default. If enabled, the refresh button is displayed.
- **Enable WebSocket connection** Enabled by default. WebSocket allows cloud access.
- **Use 24-hour time** Disabled by default.
- **Date format** Enter the format you want to use. The default is *MM/DD/YYYY*.
- **Language** Select the appropriate language.
- **Alerts position** Select the position you want alerts to appear: **Top left**, **Top center**, **Top right**, **Bottom left**, **Bottom center**, or **Bottom right**.

- **Statistics timezone** Select the appropriate time zone for logging the statistical data: **Browser's**, **Site's**, or **UTC**. The default is *UTC*.
- **Refresh rate** The default is *2 minutes*.
- **Cancel** Click to discard changes.
- **Save and Close** Click to save changes.
- **Reset to Defaults** Click to reset to factory defaults.

Edit Account To change the login name and/or password, click Edit account. The *Edit Account* screen will appear:



- **Password** Enter your current password.
- **Admin Name** Enter the admin name.
- **Email** Enter the email address of the admin account.
- **New Password** Enter the new password.
- **Confirm Password** Enter the new password again.
- **Alerts** Select this option to enable email notifications.
  - **Send similar alerts in one email** Select this option to group similar alerts in a single email notification.
- **Email Templates** Select this option to enable the use of HTML email templates.
- **Professional Installer** Select this option to enable options for professional installers. Then select **I hereby certify that I am a professional installer of wireless equipment**. (This allows you to set the antenna gain for the UAP-AC-M device, which has a detachable antenna.)
- **Submit** Click to apply changes.
- **Cancel** Click to discard changes.

Logout To manually sign out of the UniFi Configuration Interface, click Logout.

Properties

The *Properties* panel is hidden by default. To display it, select a device.

Information about each selected device appears as a popup within this panel. The information varies depending on the device type. For more information, see the appropriate chapter:

- **"UniFi Security Gateway Details" on page 115**
- **"UniFi Switch Details" on page 121**
- **"UniFi Access Point Details" on page 131**
- **"Client Details" on page 147**

Note: For management of the UniFi VoIP Phones, please download the UniFi VoIP Controller: **www.ubnt.com/download/unifi**

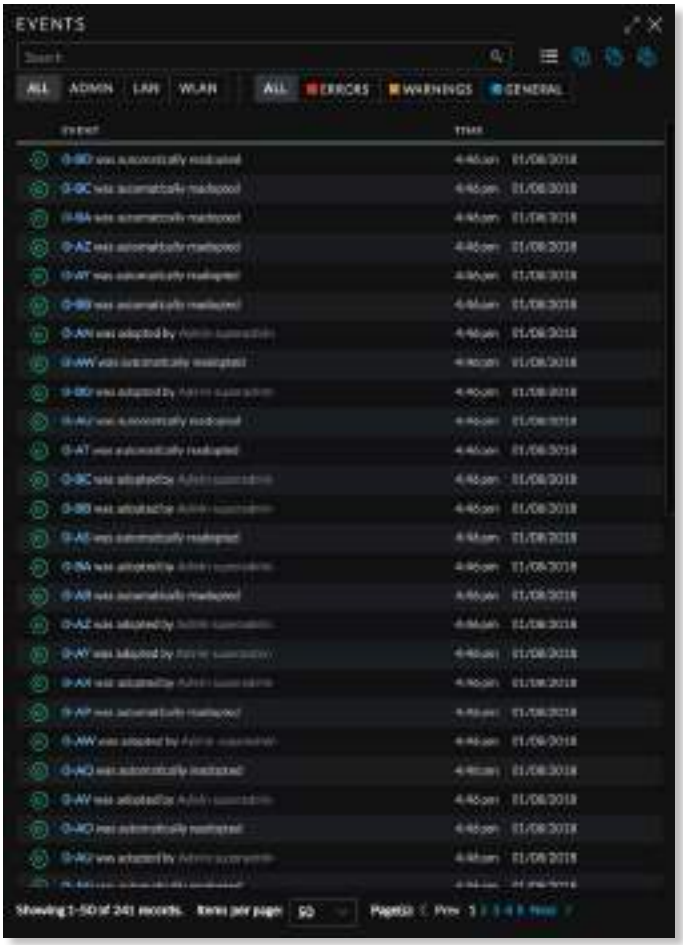
Controls and Live Chat

At the bottom left of the screen, there are four controls:

- *Events*
- *Alerts* (see **"Alerts" on page 20**)
- *Settings* (see **"Settings" on page 21**)
- *Chat with Us* (see **"Chat with Us" on page 62**)

Events

The *Events* tab displays a list of recent events, along with the corresponding device icon, device name, message, date, and time.



Maximize/Minimize Click to maximize the screen size. Click again to minimize the screen size.

Close Click to close the screen.

Search Search You can enter text that you want to search for. Simply begin typing; there is no need to press *Enter*.

You can apply one of the following filters to filter recent events based on the time period you specify:

- **(All)** Display all of the recent events.
- **(1 day)** Filter recent events for a one-day duration.
- **(7 days)** Filter recent events to display a week's duration.
- **(31 days)** Filter recent events to display a month's duration.

You can apply one of the following filters:

- **All** Display all of the recent events.
- **Admin** Only display recent events for the administrator.
- **LAN** Only display recent events for the wired network.
- **WLAN** Only display recent events for the wireless networks.

You can apply one of the following filters:

- **All** Display all of the recent events.
- **Error** Only display error-level events.
- **Warnings** Only display warning-level events.
- **General** Only display general-level events.

Icons

The messages use the following icons (not all are shown here):

	Scheduled for upgrade
	UniFi Security Gateway
	UniFi Switch
	UniFi Access Point

Clicking an Event Device Link

The messages have clickable links for client and UniFi devices:

- **"UniFi Security Gateway Details" on page 115**
- **"UniFi Switch Details" on page 121**
- **"UniFi Access Point Details" on page 131**
- **"Client Details" on page 147**

Alerts

When there is a new alert, an orange icon displaying the number of new alerts appears.

The *Alerts* tab displays a list of important events, along with the corresponding device icon, device name, message, date, and time.

Maximize/Minimize Click to maximize the screen size. Click again to minimize the screen size.

Close Click to close the screen.

Search Search You can enter text that you want to search for. Simply begin typing; there is no need to press *Enter*.

You can apply one of the following filters to filter recent alerts based on the time period you specify:

- **(All)** Display all of the recent alerts.
- **(1 day)** Filter recent alerts for a one-day duration.
- **(7 days)** Filter recent alerts to display a week's duration.
- **(31 days)** Filter recent alerts to display a month's duration.

Show archived alerts Select this option to display all of the archived alert messages.

You can apply one of the following filters:

- **All** Display all of the recent events.
- **Error** Only display error-level events.
- **Warnings** Only display warning-level events.

Archive All Click **Archive All** to archive all of the alert messages.

Archive Click to archive the selected alert message.

Icons

The messages use the following icons (not all are shown here):

	UniFi Security Gateway
	UniFi Switch
	UniFi Access Point

Clicking an Alert Device Link

The messages have clickable links for client and UniFi devices:

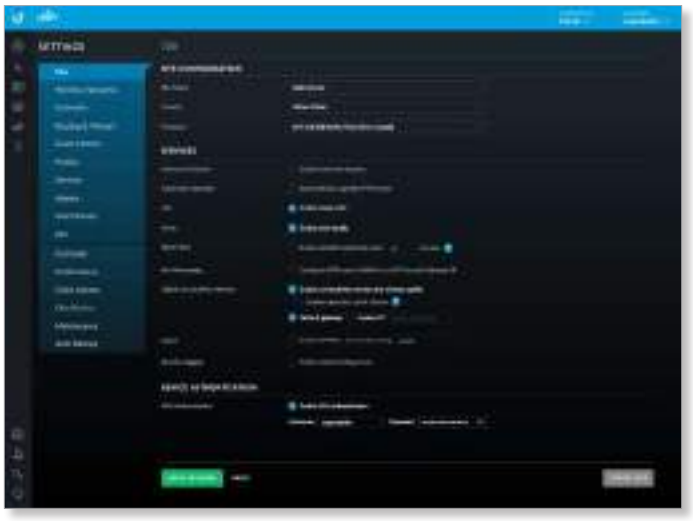
- **"UniFi Security Gateway Details" on page 115**
- **"UniFi Switch Details" on page 121**
- **"UniFi Access Point Details" on page 131**
- **"Client Details" on page 147**

Settings

The *Settings* tab displays a list of available sub-tabs:

Settings > Site

Configure the site-specific settings. To switch sites, select a different site from the *Current Site* drop-down menu at the top of any screen.



Site Configuration

Site Name Change the name of the site.

Country Select the appropriate country.

Time Zone Select the appropriate time zone.

Services

Advanced Features When enabled, airtime fairness, bandsteering, minimum RSSI, and load balancing features become available.

Automatic Upgrade When enabled, the UniFi Controller will automatically upgrade your APs' firmware when an update is available.

LED When enabled, the status LEDs on the UniFi devices will light up. When disabled, the LEDs will turn off.

Alerts Select this option to enable alert emails, which will be sent to the email addresses of the administrators.

Speed Test When enabled, you can run a periodic speed test. Enter the interval in minutes.

Port Remapping When enabled, the VOIP port on the UniFi Security Gateway, model USG, will be remapped as a WAN2 port.

Uplink Connectivity Monitor It monitors the uplinks of the managed APs, either wired or wireless, by checking to see if the gateway/custom IP can be reached.

- **Enable connectivity monitor and wireless uplink** The monitor and wireless uplink capability are enabled by default.
  - **Enable automatic uplink failover** Enable this option to have the UniFi Controller automatically select a new wireless uplink if the original uplink fails. This allows the UniFi APs to switch to alternative uplinks/mesh configurations if a node fails.
- **Default Gateway** Enabled by default. All managed APs will use the gateway of the AP that is providing IP information, either by *DHCP* or *Static* designation.
- **Custom IP** Click to specify an IP address.
  - **Uplink IP Address** All managed APs will use the IP address you enter.

SNMP Select this option to activate the SNMP (Simple Network Monitor Protocol) agent. SNMP is an application layer protocol that facilitates the exchange of management information between network devices. Network administrators use SNMP to monitor network-attached devices for issues that warrant attention.

- **Community String** Specify the SNMP community string. It is required to authenticate access to MIB (Management Information Base) objects and functions as an embedded password. The device supports a read-only community string; authorized management stations have read access to all the objects in the MIB except the community strings, but do not have write access. The device supports SNMP v1. The default is *public*.

Remote Logging Enable to define a remote syslog server.

- **Enable debug logging** Select this option to create debug logs.
- **Remote IP or Hostname** Enter the IP address or hostname of the syslog server.
- **Port** Enter the port number of the syslog server. The default is *514*.

Device Authentication

SSH Authentication This option protects SSH access to the UniFi devices. All devices in the same site share the same SSH username and password. You can also make changes:

- **Username** Enter the new username.
- **Password** Enter the new password.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Export Site Click to export the site to another controller of the same or higher version number. Then follow the on-screen instructions.

- **Download Backup File** Click to download a backup configuration file.
- **Cancel** Click to cancel the export.

Settings > Wireless Networks

Configure the wireless networks for each site. You can have up to four wireless network names or SSIDs per WLAN group.

WLAN Group The *Default* WLAN group is automatically created.

Add a New WLAN Group To add a new WLAN group, click the + button. Go to the *Add or Edit a WLAN Group* section.

Add or Edit a WLAN Group

- **Name** Enter or edit a descriptive name for the WLAN group.
- **Mobility** To enable seamless roaming (Zero Handoff), select the checkbox.

Note: Not all UniFi APs support Zero Handoff Roaming.

When you enable this option, multiple Access Points (APs) act as an AP cluster, appearing as a single AP. The wireless client detects only one AP, so it seamlessly roams from AP to AP – there is no need to re-negotiate. The APs determine which AP has the best connection and should serve the client. They use multicasting to communicate so they must be wired in the same Layer 2 domain.

Zero Handoff Roaming does not support wireless uplinks and can only be used on a secured network. It is also not meant for all scenarios. For example, if there is too much load or interference, then Zero Handoff Roaming may not be appropriate for your scenario.

Configure the following options:

- **Radio** Select the appropriate radio, **2G** or **5G**.
- **Channel** Select the channel that all of the APs will use for Zero Handoff Roaming.

- **Legacy Support** (Not available if you enabled the *Mobility* option.) By default, legacy devices, such as 802.11b devices, are excluded. Select this option if you want to support legacy devices.

Advanced Options Click to display more options.

- **PMF** Enabling PMF (Protected Management Frames) may cause a drop in performance. Select the appropriate option:
  - **Disabled** The UniFi APs will not use PMF for any stations.
  - **Optional** The UniFi APs will use PMF for all PMF-capable stations while allowing non-PMF-capable stations to join the wireless network.
  - **Required** The UniFi APs will use PMF for all stations. Stations that are not capable of PMF will not be allowed to join the wireless network.

Save Click to apply changes.

Cancel Click to discard changes.

For each WLAN group, you have the following:

- **Remove a WLAN Group** To remove a WLAN group (except for the *Default*, which cannot be removed), select it from the drop-down menu, and then click the *delete* button.

- **Options** To make changes, select the WLAN group from the drop-down menu, and then click the *edit* button. Go to **"Add or Edit a WLAN Group" on page 22**.

Wireless Networks

Name Displays the wireless network name or SSID.

Security Displays the type of security being used on your wireless network.

Guest Network Indicates whether or not the network is a guest network.

VLAN Indicates its VLAN ID.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the wireless network settings. Go to the *Create or Edit a Wireless Network* section.
- **Delete** Click DELETE to remove the wireless network.

Create Wireless Network Click + CREATE NEW WIRELESS NETWORK to add a wireless network. Go to the *Create or Edit a Wireless Network* section.

Create or Edit a Wireless Network

- **Name/SSID** Enter or edit the wireless network name or SSID.
- **Enabled** Select this option to make the network active.
- **Security** Select the type of security to use on your wireless network.
  - **Open** This option is typically only used on the guest network. When enabled, wireless network access is open to anyone without requiring a password.
  - **WEP** WEP (Wired Equivalent Privacy) is the oldest and least secure security algorithm. WPA™ security methods should be used when possible.

- **WEP Key** Enter a WEP encryption key in hexadecimal format. You can enter a 64-bit or 128-bit key:

Type	Hex
64-bit	10 Hexadecimal Characters (0-9, A-F, or a-f) Example: **00112233AA** Note: You can use 5 printable characters, which will be translated to the corresponding HEX code.
128-bit	26 Hexadecimal Characters (0-9, A-F, or a-f) Example: **00112233445566778899AABBCC** Note: You can use 13 printable characters, which will be translated to the corresponding HEX code.

- **Key Index** Specify which Index of the WEP Key to use. Four different WEP keys can be configured at the same time, but only one is used. Select the effective key: **1**, **2**, **3**, or **4**.

- **WPA-Personal** WPA or Wi-Fi Protected Access was developed as an encryption method stronger than WEP. WPA-Personal requires a passphrase to connect to the wireless network.

- **Security Key** Enter the passphrase that users will use to connect to the wireless network.

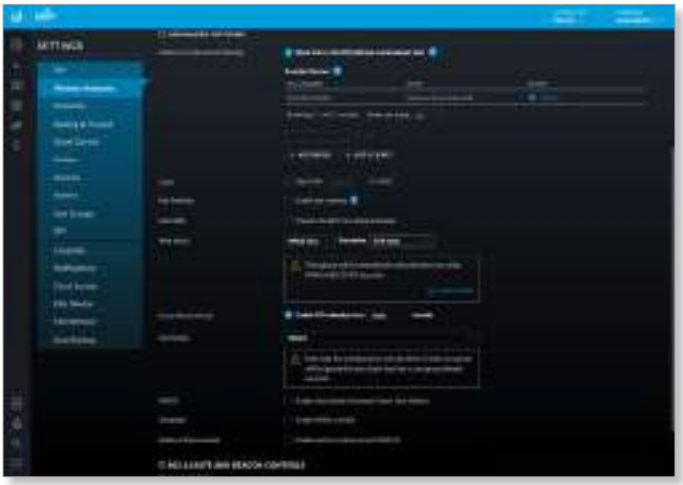
- **WPA-Enterprise** WPA Enterprise uses a RADIUS server to authenticate users on the wireless network.

  - **RADIUS Profile** Specify a RADIUS profile:
    - Select a RADIUS profile from the drop-down list, or
    - Click **Create New RADIUS Profile** to create a new RADIUS profile. Refer to **"Create or Edit a RADIUS Profile" on page 45** for detailed information.
  - **Hotspot 2.0** Select this option to enable Hotspot 2.0. Then select a Hotspot profile from the drop-down list. Go to **"Hotspot 2.0" on page 49** for more information.

- **Guest Policy** Select this option to enable guest access policies on this wireless network. By default, guest policies will drop broadcast traffic from wireless stations and also block LAN => WAN broadcast and multicast data from all except the default gateway. See *Advanced Options* for custom whitelisting.

Advanced Options

Click to display options for advanced users.

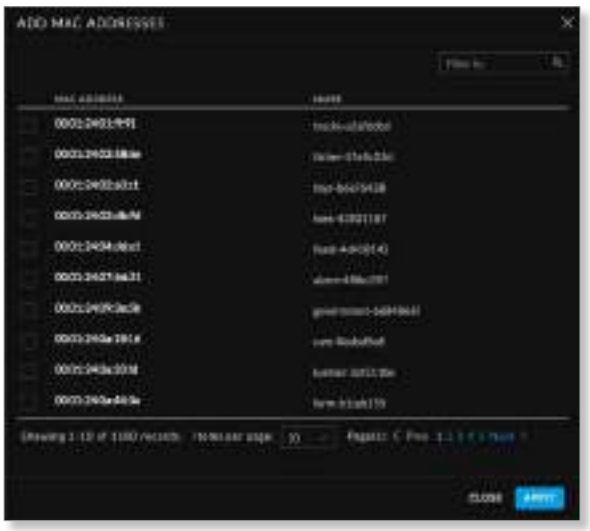


- **Multicast and Broadcast Filtering** Disabled by default. We recommend to enable it if there are more than 100 wireless clients on a single Layer-2 network. When Multicast and Broadcast Filtering is enabled, devices such as Chromecasts and Apple TVs will not be discovered unless the USG MDNS service is enabled. Multicast/broadcast data is sent out at the lowest modulation rate, so we recommend that you block this traffic unless it is absolutely essential. Disable this option if proper multicast/broadcast controls are already implemented on the LAN infrastructure.

- **Excepted Devices** You can specify devices that need to send multicast/broadcast data to Wi-Fi stations. In most cases, only the default gateway needs to send multicast data to Wi-Fi stations and is automatically added by the UniFi Controller. You can add any other devices, such as Bonjour printers or Chromecast devices.
  - **MAC Address** Displays the MAC address of the device.
  - **Name** Displays the name or hostname of the device.
  - **Action** Click REMOVE to remove this device.
  - **(MAC_address)** To add an excepted device, enter the MAC address and click + ADD .
  - **Add Batch** Click to add a group of devices.

    - **(MAC_addresses)** Enter the MAC addresses in the field provided.
    - **Override current MAC Access Control List** Select this option to override this list. Disabled by default.
    - **Import** Click + IMPORT to import a list of MAC addresses.
    - **Apply** Click to save changes.
    - **Close** Click to exit the screen without saving any changes.

- **Add Clients** Click to add a group of wireless clients.



  - **Filter by** Enter keywords to search for specific devices.
  - **MAC Address** Displays the MAC address of the client device.
  - **Name** Displays the name or hostname of the client device.
  - **Apply** Select the client devices and then click to save changes.
  - **Close** Click to exit the screen without saving any changes.

- **VLAN** To use a VLAN, select **Use VLAN ID** and enter the VLAN ID number.
- **Fast Roaming** Fast Roaming allows certain devices with 802.11r capabilities to potentially roam more quickly. However, older devices may experience connectivity issues due to their lack of 802.11r client-side support or compatibility. Select this option with caution.
- **Hide SSID** Select this option if you don't want the wireless network name or SSID to be broadcast.
- **WPA Mode** (Available if WPA security is enabled.) Select the appropriate WPA method: **Both**, **WPA1 Only**, or **WPA2 Only** (default).
  - **Encryption** (Available if WPA security is enabled.) Select the appropriate encryption method: **Auto**, **TKIP Only**, or **AES/CCMP Only** (default).
- **Group Rekey Interval** (Available if WPA security is enabled.) Select this option to rekey the GTK (Group Temporal Key) after an interval specified in seconds. The default is *3600* seconds.
- **User Group** Assign wireless users to a specific user group. For more information about user groups, see **"Settings > User Groups" on page 54**.
- **UAPSD** Disabled by default. Select **UAPSD** (Unscheduled Automatic Power Save Delivery) to enable the power save mode of Wi-Fi devices.
- **Scheduled** Select **Enable WLAN Schedule** to restrict wireless access to the schedule you set.
  - **Monday-Sunday** Select the days you want to schedule.
  - **(hours)** Use the slider bars to adjust the start and end times of the day's wireless access.
- **Multicast Enhancement** Disabled by default. Enabling *Multicast Enhancement* is useful for applications such as IPTV installations.

  If clients do not send IGMP (Internet Group Management Protocol) messages, then they are not registered as receivers of your multicast traffic. Using IGMP snooping, *Multicast Enhancement* isolates multicast traffic from unregistered clients and allows the device to send multicast traffic to registered clients using higher data rates. This may lessen the risk of traffic overload and increase the reliability of multicast traffic since packets are transmitted again if the first transmission fails.

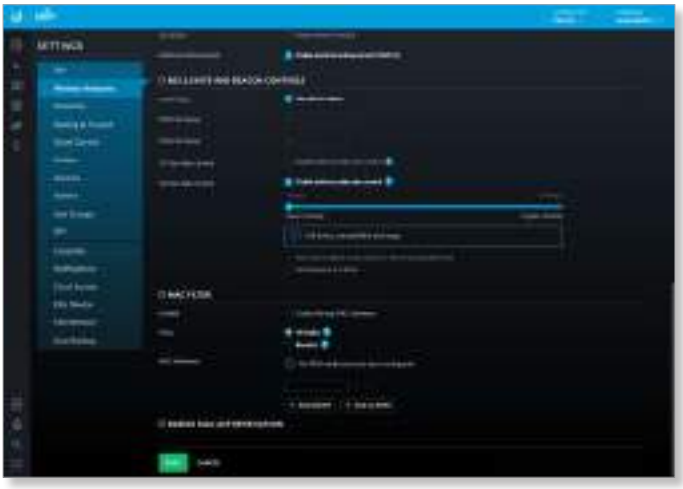
  If clients do not send IGMP messages but should receive multicast traffic, then you may need to keep *Multicast Enhancement* disabled.

Note: IGMPv3 is supported by the UniFi APs.

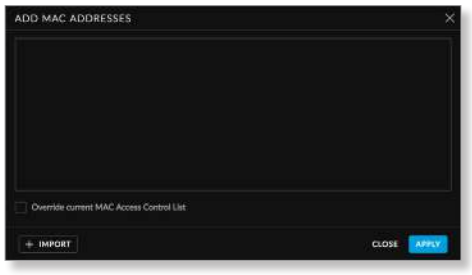
802.11 Rate and Beacon Controls

- **DTIM Mode** Select this option to use the default DTIM (Delivery Traffic Indication Message) values. Increasing the DTIM values allows devices to conserve power, at a slight latency penalty. Deselect it to configure the values below.
- **DTIM 2G Period** Enter the number of beacons between the 2.4 GHz DTIM beacons. The default is *1*.
- **DTIM 5G Period** Enter the number of beacons between the 5 GHz DTIM beacons. The default is *1*.
- **2G Data Rate Control** Select this option to determine what bit rates your 2.4 GHz network will allow. Disabling lower bit rates can improve performance for higher-density networks but will make some older devices incompatible with your network and limit the range of your wireless network.
  - **Also require clients to use rates at or above the specified value** Select this option to set minimum rates for clients.
  - **Send beacons at 1 Mbps** Select this option to set the beacon speed at 1 Mbps.
- **5G Data Rate Control** Select this option to determine what bit rates your network will allow. Disabling lower bit rates can improve performance for higher-density networks but will make some older devices incompatible with your network and limit the range of your wireless network.
  - **Also require clients to use rates at or above the specified value** Select this option to set minimum rates for clients.
  - **Send beacons at 6 Mbps** Select this option to set the beacon speed at 6 Mbps.

MAC Filter



- **Enabled** Select this option to filter MAC addresses.
- **Policy** Select **Whitelist** to allow connections from the following MAC addresses; all others will be blocked. Select **Blacklist** to block connections from the following MAC addresses; all others will be allowed.
- **MAC Addresses** To add a MAC address, enter it and click + ADD .
  - **Add Batch** Click to add a group of devices.



  - **(MAC_addresses)** Enter the MAC addresses in the field provided.
  - **Override current MAC Access Control List** Select this option to override this list. Disabled by default.
  - **Import** Click + IMPORT to import a list of MAC addresses.
  - **Apply** Click to save changes.
  - **Close** Click to cancel changes.

- **Add Clients** Click to add a group of wireless clients.

- **Filter by** Enter keywords to search for specific devices.
- **MAC Address** Displays the MAC address of the client device.
- **Name** Displays the name or hostname of the client device.
- **Apply** Select the client devices and then click to save changes.
- **Close** Click to cancel changes.

RADIUS MAC Authentication

- **Enabled** Select this option to enable RADIUS MAC authentication.
- **RADIUS Profile** Select the appropriate RADIUS profile or create a new one; go to **"Create or Edit a RADIUS Profile" on page 45** for more information.
- **MAC Address Format** Select the format used to convert a client's MAC address to the RADIUS username.
- **Empty Password** Select this option to allow a blank password.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Settings > Networks

Configure the networks for each site.

Networks

Name Displays the network name.

Purpose Displays the purpose of this network: *Corporate*, *Guest*, *VLAN Only*, *Remote User VPN*, *Site-to-Site VPN*, or *VPN Client*.

Subnet Displays the IP address and prefix size.

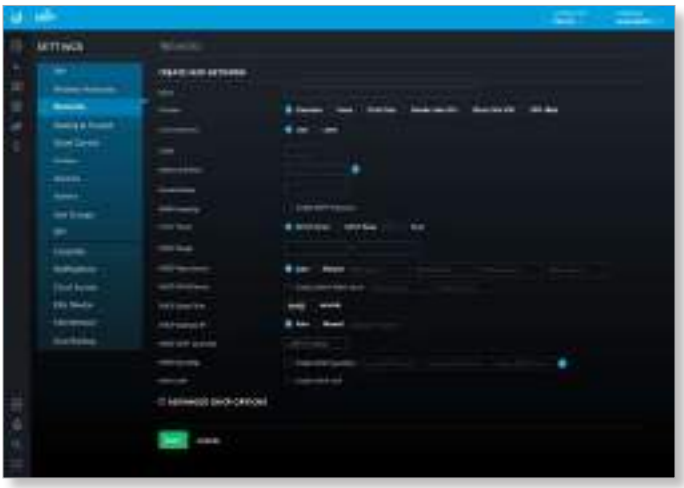
VLAN Displays the VLAN ID, if applicable.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the network settings. Go to the *Create or Edit a Network* section.
- **Delete** (Not available for the default network.) Click DELETE to remove the network.

Create New Network Click + CREATE NEW NETWORK to add a network. Go to the *Create or Edit a Network* section.

Create or Edit a Network



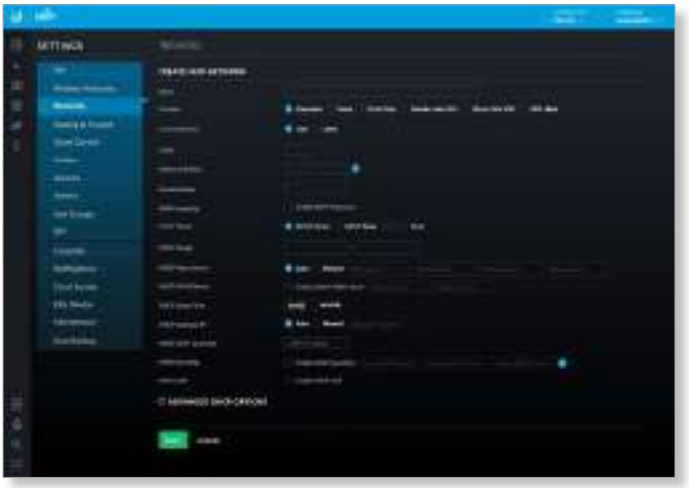
- **Name** Enter or edit the network name.
- **Purpose** Select the most appropriate description:
  - **Corporate** Corporate networks are appropriate for networks containing trusted systems. Corporate networks have no restrictions between them, or from them to the internet, by default.

- **Guest** Guest networks are often used in combination with the *Guest Control* feature (refer to **"Settings > Guest Control" on page 37**) for limiting access. The default *Guest Control* restrictions block authenticated guests from reaching any private IP subnet (RFC 1918).
- **VLAN Only** Deploys the configured VLAN ID and associated configuration to the UniFi Switch(es).
- **Remote User VPN** Allows configuration of a UniFi Security Gateway as a remote access PPTP or L2TP VPN server to connect mobile VPN clients.
- **Site-to-Site VPN** Site-to-site VPNs connect different networks with an always-on connection and routing between. Auto, IPsec, and OpenVPN options are available.
- **VPN Client** Configures a VPN client on the UniFi Security Gateway to connect to a remote PPTP VPN server, acting like a mobile client would. Traffic leaving VPN client interfaces is source NATed to the IP assigned to the VPN client, so return routing from the server side isn't needed.

Note: The *Corporate*, *Guest*, *Remote User VPN*, *Site-to-Site VPN*, and *VPN Client* settings apply to the UniFi Security Gateway only. The *VLAN Only* setting applies only to UniFi Switches.

After making your selection, follow the instructions for your selection:

Corporate or Guest Network



- **Parent Interface** Select the physical interface of the USG that this network will be associated with: **LAN1** or **LAN2**.
- **VLAN** (Not available for the default *Corporate* network, *LAN*.) Enter the VLAN ID.
- **Gateway/Subnet** Enter the IP address and subnet mask.
- **Domain Name** Enter the domain name.
- **IGMP Snooping** Select this option to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
- **DHCP Mode** Select the appropriate option: **DHCP Server**, **DHCP Relay**, or **None**.
  - **DHCP Server** Enabled by default. The local DHCP server assigns IP addresses to DHCP clients on the network.
    - **DHCP Range** Enter the starting and ending IP addresses of the range in the fields provided.
    - **DHCP Name Server** Configure the name or DNS (Domain Name System) server setting:
      - **Auto** Enabled by default. When this option is selected, all clients on the network are assigned the UniFi Security Gateway's IP address as their DNS server. The clients will then use the UniFi Security Gateway's caching DNS resolver as their DNS server.
      - **Manual** Select this option to specify name servers. Then enter the IP address of a server in each *DNS server* field.
    - **DHCP WINS Server** Select this option to designate WINS (Windows Internet Naming Service) server(s). Then enter the IP address of a server in each *WINS server* field.
    - **DHCP Lease Time** Enter the DHCP lease time in seconds. The IP addresses assigned by the DHCP server are valid only for the duration specified by the lease time. Increasing the lease time will extend the time clients retain their IP address in absence of the DHCP server. However, any network changes will take just over half the lease length to apply to all clients. In networks with high rates of device churn, much shorter lease lengths should be used to prevent exhausting the DHCP IP address pool.
    - **DHCP UniFi Controller** Enter the IP address of the UniFi Controller.
  - **DHCP Relay** Select this option to enable DHCP relay, which forwards DHCP packets to a DHCP server when DHCP clients are not on the same local network or subnet as their DHCP server. Go to **"DHCP Relay" on page 51** for configuration instructions.
  - **None** Select this option to disable DHCP.
- **DHCP Guarding** Disabled by default. Select this option to detect and block unauthorized DHCP servers. DHCP guarding configures UniFi Switches to restrict DHCP servers on this network to the IP address(es) specified here. All other IP addresses attempting to serve DHCP will have the DHCP responses blocked, and the UniFi Controller will generate an alert.
  - **Trusted DHCP Server** Enter the IP address of a trusted DHCP server in each field.
- **UPnP LAN** Disabled by default. Select this option to allow UPnP (Universal Plug and Play) on the local network.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

VLAN Only

The UniFi Switch is required for this option.

- **VLAN** Enter the ID number of the VLAN. Devices belonging to the same VLAN communicate as if they were attached to the same wire. Every VLAN ID represents a different VLAN. The VLAN ID range is 2 to 4009.
- **IGMP Snooping** Select this option to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
- **DHCP Guarding** Disabled by default. Select this option to detect and block unauthorized DHCP servers. DHCP guarding configures UniFi Switches to restrict DHCP servers on this network to the IP address(es) specified here. All other IP addresses attempting to serve DHCP will have the DHCP responses blocked, and the UniFi Controller will generate an alert.
  - **Trusted DHCP Server** Enter the IP address of a trusted DHCP server in each field.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Remote User VPN

The UniFi Security Gateway is required for this option.

- **VPN Type** To connect mobile VPN clients, configure the UniFi Security Gateway as a remote access VPN server. Select the appropriate server type, **PPTP Server** or **L2TP Server.**
- **Gateway/Subnet** Enter the IP address and subnet mask.
- **IP Pool** The starting and ending IP addresses of the pool automatically appear after you complete the *Gateway/Subnet* field. These are the IP addresses that will be assigned to connected VPN clients.
- **Name Server** Configure the name or DNS (Domain Name System) server setting.
  - **Auto** Enabled by default. Name servers are automatically assigned by the DHCP server.
  - **Manual** Select this option to specify name servers. Then enter the IP address of a server in each *DNS server* field.
- **WINS Server** Select this option to designate WINS (Windows Internet Naming Service) server(s). Then enter the IP address of a server in each *WINS server* field.
- **Site-to-Site VPN** Enabled by default. The remote user can access the site's resources as well as the resources of any other VPNs connected to the site. If you disable this option, then the remote user can only access the site's resources.
- **RADIUS Profile** Select a RADIUS profile from the drop-down list, or click **Create New RADIUS Profile** to create a new RADIUS profile. Refer to **"Create or Edit a RADIUS Profile" on page 45** for information.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Site-to-Site VPN

The UniFi Security Gateway is required for this option.

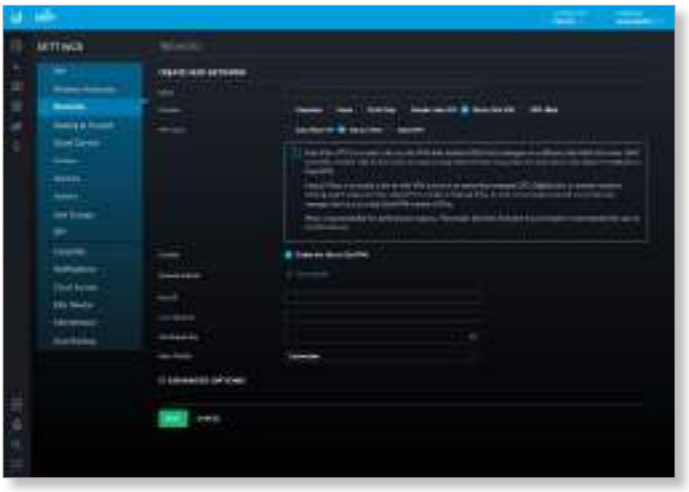
- **VPN Type** Select the type of VPN being configured: **Auto IPsec VTI**, **Manual IPsec**, or **OpenVPN**.
  - **Auto IPsec VTI** *Auto IPsec VTI* is the default. This option lets you connect two sites on the same controller by simply picking the other site. The other end of the VPN tunnel uses a UniFi Security Gateway managed on a different site within the same UniFi Controller. If either side of the tunnel is using USG firmware 4.2.x, then the Auto IPsec VTI option will fall back to OpenVPN.

    No further configuration is necessary; UniFi automatically creates a secure IPsec VPN and configures routing between the sites. Also, the VPN connection is bidirectional: creating an auto VPN from site A to site B also provides connectivity from site B to site A (nothing is configured on site B).

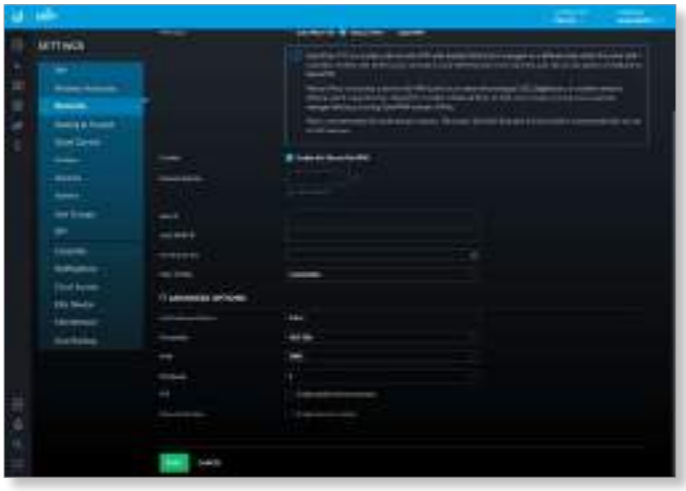
- **Remote Site** Select the appropriate site from the drop-down list.

Note: You must have admin privileges for the local and remote sites to view and select sites.

- **IPsec VPN** Select this option to create a VPN that uses IPsec (IP security protocol).



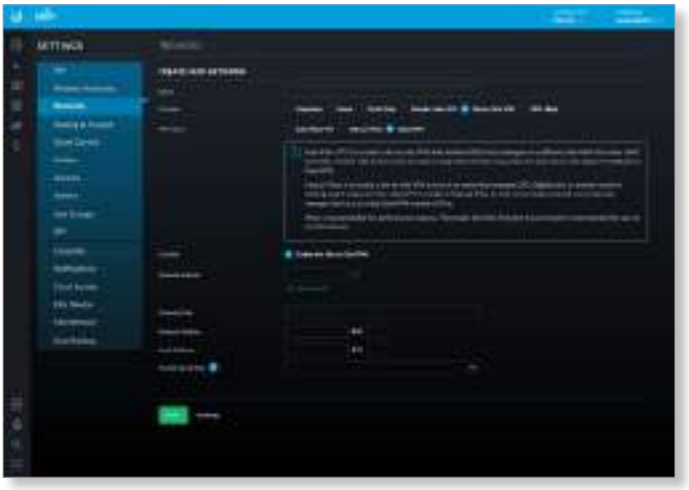
- **Enabled** Select this option to create an IPsec VPN tunnel between two peer routers over the internet, from a local device to an externally managed device, such as an externally managed UniFi Security Gateway, EdgeRouter™, or third-party device that supports IPsec. (The UniFi Security Gateway is the local peer router.)
- **Remote Subnets** Click **Add Subnet** to add an address for a remote network.
- **Peer IP** Enter the internet IP address of the remote peer router.
- **Local WAN IP** Enter the internet IP address of the local UniFi Security Gateway.
- **Pre-Shared Key** Enter the pre-shared secret key. Both peer routers must use the same pre-shared secret key for authentication.
- **IPsec Profile** Select the appropriate option:
  - **Customized** Select this option to customize your settings.
  - **Azure dynamic routing** Select this option if you are using Microsoft Azure with dynamic routing for a route-based VPN.
  - **Azure static routing** Select this option if you are using Microsoft Azure with static routing for a policy-based VPN.
- **Advanced Options** Click to access the advanced configuration.



- **Key Exchange Version** Both peer routers must use the same Internet Key Exchange (IKE) version. Select the appropriate version: **IKEv1** or **IKEv2**.
- **Encryption** Both peer routers must use the same encryption method. Select the appropriate encryption method: **AES-128**, **AES-256**, or **3DES**.
- **Hash** Both peer routers must use the same hash algorithm. Select the appropriate hash algorithm: **SHA1** or **MD5**.
- **DH Group** The DH (Diffie-Hellman) group specifies the strength of the DH encryption key for the key exchange. Both peer routers must use the same DH group. Select the appropriate DH group: **2**, **5**, **14**, **15**, **16**, **19**, **20**, **21**, **25**, or **26**. The default is *14*.
- **PFS** Select this option to enable PFS (Perfect Forward Secrecy), which protects your past sessions from decryption should your key be compromised in the future.
- **Dynamic Routing** Select this option to use VTI-based IPsec (otherwise tunnel mode will be used).

Note: If you selected *Azure dynamic routing* or *Azure static routing*, then the defaults of the *Advanced Options* will also change accordingly.

- **OpenVPN** Select this option to create a VPN that uses the OpenSSL (Secure Sockets Layer) library and SSL/TLS (Transport Layer Security) protocols.



  - **Enabled** Select this option to create an OpenVPN tunnel between two peer routers over the internet, from a local device to an externally managed device. (The UniFi Security Gateway is the local peer router.)
  - **Remote Subnets** Click **Add Subnet** to add an address for a remote network.
  - **Remote Host** Enter the hostname of the remote router.
  - **Remote Address** Enter the internet IP address and port number of the remote router.
  - **Local Address** Enter the internet IP address and port number of the UniFi Security Gateway.
  - **Shared Secret Key** Enter the pre-shared secret key. (Include only the text below "BEGIN" and above "END" and remove the new lines.) Both peer routers must use the same pre-shared secret key for authentication.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

VPN Client

The UniFi Security Gateway is required for this option.

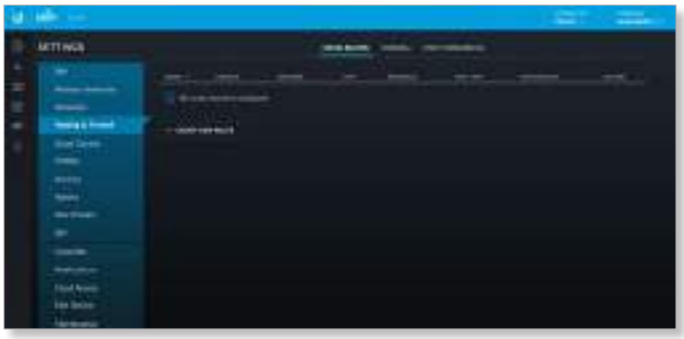
- **VPN Client** **PPTP Client** is automatically selected.
- **Enabled** Select this option to enable the VPN client.
- **Default Route** Select this option to route internet traffic via the VPN tunnel.
- **Route Distance** Enter the administrative distance. (The default of PPTP client routes is 50.)
- **Remote Subnets** (Available if *Default Route* is disabled.) Enter the network address of the remote network. This VPN client will be used to reach the specified remote network(s).
  - **Add Subnet** If you have another remote subnet, click this option and enter its network address.
- **DNS** Select this option to use the DNS servers specified by the VPN server.
- **Server** Enter the IP address of the VPN server.
- **Username** Enter the VPN username.
- **Password** Enter the VPN password.
- **MPPE** Select this option to require MPPE (Microsoft Point-to-Point Encryption).
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Settings > Routing & Firewall

The *Routing & Firewall* screen displays the following tabs:

- *Static Routes* tab
- **"Firewall" on page 32**
- **"Port Forwarding" on page 36**

Static Routes



The *Static Routes* tab displays a list of user-defined static routes:

Name Displays the name of the static route.

Enabled Displays a check mark if the static route is enabled.

Network Displays the IP subnet of the network in Classless Inter-Domain Routing (CIDR) or slash notation (example: 192.0.2.0/24).

Type Displays the static route's type: *Next Hop*, *Interface*, or *Black Hole*.

Interface Displays the interface associated with the static route.

Next Hop Displays the IP address of the next hop for the static route.

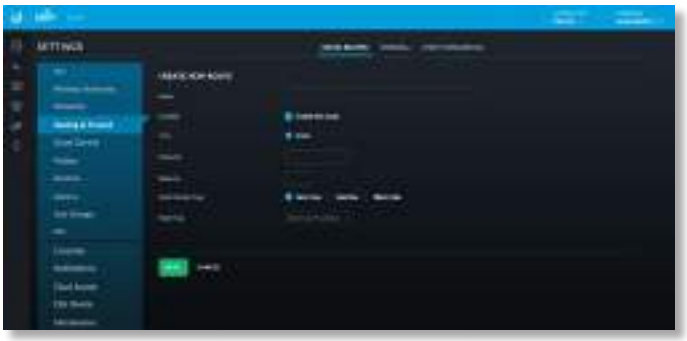
Hop Distance Displays the status route's administrative distance.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the static route entry. Go to **"Create or Edit a Static Route" on page 32**.
- **Delete** Click DELETE to remove the static route.

To create a static route, click CREATE NEW ROUTE and go to **"Create or Edit a Static Route" on page 32** .

Create or Edit a Static Route



Name Enter a name for the static route.

Enabled Keep this option selected to enable the route. The route is enabled by default.

Type This read-only field displays the route type: *Static*.

Network Enter the IP address and subnet mask using CIDR or slash notation:
<network_IP_address>/<subnet_mask_number>
(example: 192.0.2.0/24).

Distance Enter the static route's administrative distance. This is a number between *1* and *255*. This number is often set to 1 (or a similarly low value) to create a route with a shorter distance than dynamic routes.

Static Route Type Select the static route's type: **Next Hop**, **Interface**, or **Black Hole**.

- **Next Hop** The IP address of the next hop gateway for the desired routing path. This is the default.
  - **Next Hop** Enter the next hop IP address.
- **Interface** Interface routes are used with point-to-point connections, where there need not be a gateway IP. They are most often used with VPNs.
  - **Interface** Select the appropriate interface.
- **Black Hole** Select this option to forward unwanted traffic into a black hole, or to drop it.

Save Click to apply changes.

Cancel Click to discard changes.

Firewall

Firewall rules are used to allow or block packets on an interface. There are predefined rules that cannot be edited or deleted, and you can create your own rules. When you create a rule, you specify matching criteria, such as the protocol (any, TCP, UDP, etc.) and whether the rule will be evaluated before or after the predefined rules. Rules are evaluated in order; as soon as one rule results in a match, that rule is applied, and rule evaluation stops.

The *Firewall* tab displays user-defined firewall information, organized into three sub-tabs: *Rules*, *Groups,* and *Settings*.

Rules

The *Rules* sub-tab displays existing firewall rules. There are three network types:

WAN This is your internet connection.

LAN This is in reference to all corporate networks.

Guest This is in reference to any guest subnets.

There are three instances per network type: *In*, *Out*, and *Local*:

In Filters packets that enter the interface and traverse the router.

Out Filters packets that leave the interface. This applies to traffic that traverses the system or from the router itself.

Local Filters packets that are destined for the router.

Note: There are predefined firewall rules for most interfaces. For detailed information on these predefined rules, refer to **"Predefined Firewall Rules" on page 33**.

The interfaces are *WAN In, WAN Out, WAN Local, LAN In, LAN Out, LAN Local, Guest In, Guest Out,* and *GUEST Local*.

The following information is displayed for each rule:

(order) Click to change the order of the rules (except for the predefined rules).

Rule Index Displays an automatically generated index number associated with the rule.

Enabled Displays a check mark if the rule is enabled.

Name Displays the descriptive name of the rule.

Action Displays the action to take if the rule criteria are satisfied: *Drop*, *Reject*, or *Accept*.

Protocol Displays the protocol(s) that apply to the rule. If *Except:* precedes the listed protocol(s), all protocols except those listed are applicable.

Source Displays the source to which the rule applies.

Destination Displays the destination to which the rule applies.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the firewall rule. Go to **"Create or Edit a Firewall Rule" on page 33**.
- **Delete** Click DELETE to remove the firewall rule.

To create a firewall rule, click CREATE NEW RULE and go to **"Create or Edit a Firewall Rule" on page 33**.

Create or Edit a Firewall Rule

Predefined Firewall Rules

The following firewall rules are predefined (cannot be edited or deleted):

Interface	Rule Name	Action	Protocol
WAN IN	Allow established/related sessions	Accept	All
	Drop invalid state	Drop	All
WAN OUT	None*	-	-
WAN LOCAL	Allow established/related sessions	Accept	All
	Drop invalid state	Drop	All
	Allow ICMP	Accept	ICMP
LAN IN	Packets from UniFi to VoIP	Accept	All
	Packets from Intranet to VoIP	Drop	All
	Accounting defined network 192.168.1.0/24	Accept	All
LAN OUT	Accounting defined network 192.168.1.0/24	Accept	All
LAN LOCAL	None	-	-
GUEST IN	Allow DNS packets to external name servers	Accept	UDP
	Allow packets to captive portal	Accept	TCP
	Allow packets to allow subnets	Accept	All
	Drop packets to restricted subnets	Drop	All
	Drop packets to intranet	Drop	All
	Drop packets to voip	Drop	All
	Drop packets to remote user	Drop	All
	Authorized guests white list	Drop	All
GUEST OUT	None	-	-
GUEST LOCAL	Allow DNS	Accept	UDP
	Allow ICMP	Accept	ICMP

* The WAN_OUT ruleset is not deployed by default until controller version 5.5.2 and newer. To deploy WAN_OUT in earlier versions, set config.ugw.deploy_firewall_wan_out=true in config.properties.

Create New Rule

Name Enter a descriptive name for the rule.

Enabled Enables or disables the rule (enabled by default).

Rule Applied Specify when the rule will be applied: **Before Predefined Rules** (default) or **After Predefined Rules**.

Action Select the action to take if the rule criteria are satisfied:

- **Drop** Packets are blocked with no message. This is the default action.
- **Reject** Packets are blocked, and an ICMP (Internet Control Message Protocol) message is sent saying that the destination is unreachable.
- **Accept** Packets are allowed through the firewall.

Protocol Specify the protocol(s) to which the rule applies. Select one of the following:

- **All** Match packets of all protocols (default).
- **TCP** Match TCP packets.
- **UDP** Match UDP packets.
- **TCP and UDP** Match TCP and UDP packets.
- **ICMP** Match ICMP packets.
- **Choose a protocol by name** Select a protocol from the drop-down list to match packets of that protocol.
- **Enter a protocol number** Enter the port number of the protocol to match packets of that protocol.
- **Match all protocols except for this** Match all protocols *except* for the selected protocol(s). (At least one protocol must be selected; *All* is not a valid selection with this option.)
- **ICMP Type Name** (Available if ICMP is selected.) Select the appropriate type from the drop-down list.

Advanced

Logging Check the box to enable logging (disabled by default).

States Select each state that will apply to the rule (none are selected by default).

- **New** The packet is the first packet seen in a new connection.
- **Established** The packet is part of an existing connection which has seen packets in both directions.
- **Invalid** The packet cannot be identified or its state cannot be determined.
- **Related** The packet is part of a new connection that is related to an existing connection.

IPsec Select the criteria for IPsec packet filtering: **Don't match on IPsec packets** (default), **Match inbound IPsec packets**, or **Match inbound non-IPsec packets**.

Source

Source Type Select **Address/Port Group** or **Network**.

- **Address/Port Group** The source is an address/port group. Specify the following:
  - **Address Group** Select an address group from the drop-down list. To create a new address group, click **Create Address Group**.
    - **Name** Enter a descriptive name.
    - **Address** Enter an IP address.
    - **Add** To add another address to the group, click **Add**.
    - **Save** Click to apply changes.
    - **Cancel** Click to discard changes.

  - **Port Group** Select a port group from the drop-down list. To create a new address group, click **Create Port Group**.
    - **Name** Enter a descriptive name.
    - **Port** Enter a port number.
    - **Add** To add another port number to the group, click **Add**.
    - **Save** Click to apply changes.
    - **Cancel** Click to discard changes.

- **Network** The source is a network. Specify the following:
  - **Network** Select the network from the drop-down list. Then select **IPv4 Subnet** or **USG IP Address** from the drop-down list.

MAC Address Enter the MAC address of the source.

Destination

Destination Type Select the type of destination:

- **Address/Port Group** The destination is an address/port group. Specify the following:
  - **Address Group** Select an address group from the drop-down list. To create a new address group, click **Create Address Group**.
    - **Name** Enter a descriptive name.
    - **Address** Add an IP address.
    - **Add** To add another address to the group, click **Add**.
    - **Save** Click to apply changes.
  - **Port Group** Select a port group from the drop-down list. To create a new address group, click **Create Port Group**.
    - **Name** Enter a descriptive name.
    - **Port** Enter a port number.
    - **Add** To add another port number to the group, click **Add**.
    - **Save** Click to apply changes.
- **Network** The destination is a network. Specify the following:
  - **Network** Select the network from the drop-down list. Then select **IPv4 Subnet** or **USG IP Address** from the drop-down list.

Save Click to apply changes.

Cancel Click to discard changes.

Groups

The *Groups* sub-tab displays the following information:

Name Displays the name of the group.

Type Displays the group type: *Address* or *Port*.

Count Displays the total addresses or ports in the group.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the group. Go to the *Create or Edit a Firewall Group* section.
- **Delete** Click DELETE to remove the group.

To create a group, click + CREATE NEW GROUP and go to the *Create or Edit a Firewall Group* section.

Create or Edit a Firewall Group

Name Enter a name for the group.

Type Select the type of group to create: **Address** or **Port**.

Address (Available if *Type* is set to *Address*.) Enter the IP address.

Port (Available if *Type* is set to *Port*.) Enter the port number.

Add Click **Add** to add another address or port to the group.

Save Click to apply changes.

Cancel Click to discard changes.

Settings

The *Settings* sub-tab displays the following options:

Conntrack Modules

FTP Tracks FTP connections. Enabled by default.

GRE Tracks GRE connections. Enabled by default.

H.323 Tracks H.323 connections. Enabled by default.

PPTP Tracks PPTP connections. Enabled by default.

SIP Tracks SIP connections. Disabled by default.

TFTP Tracks TFTP connections. Enabled by default.

State Timeouts

ICMP Enter the ICMP state timeout in seconds. The default is *30*.

Other Enter the state timeout for protocols excluding TCP, UDP, and ICMP in seconds. The default is *600*.

TCP Close Enter the ICMP state timeout in seconds. The default is *10*.

TCP Close Wait Enter the state timeout in seconds for connections in TCP Close Wait status. The default is *60*.

TCP Established Enter the state timeout in seconds for connections in TCP Established status. The default is *7440*.

TCP FIN Wait Enter the state timeout in seconds for connections in TCP FIN Wait status. The default is *120*.

TCP Last ACK Enter the state timeout in seconds for connections in TCP Last ACK status. The default is *30*.

TCP SYN Recv Enter the state timeout in seconds for connections in TCP SYN (Synchronize) Recv status. The default is *60*.

TCP SYN Sent Enter the state timeout in seconds for connections in TCP SYN Sent status. The default is *120*.

TCP Time Wait Enter the state timeout in seconds for connections in TCP Time Wait status. The default is *120*.

UDP Other Enter the state timeout in seconds for UDP connections with traffic in only one direction. The default is *30*.

UDP Stream Enter the state timeout in seconds for UDP connections with bidirectional traffic. The default is *180*.

Firewall Options

Broadcast Ping Controls whether the UniFi Security Gateway replies to broadcast pings. Disabled by default.

Receive Redirects Controls whether the UniFi Security Gateway accepts ICMP redirects. Disabled by default.

Send Redirects Controls whether the UniFi Security Gateway sends ICMP redirects. Enabled by default.

SYN Cookies Controls usage of SYN cookies, a technique to resist SYN flood attacks that want to open ports on the UniFi Security Gateway. Enabled by default.

Apply Changes Click to save changes.

Reset Click to discard changes.

Port Forwarding

The *Port Forwarding* tab displays a list of port forwarding entries.

Name Displays the name of the port forwarding entry.

From Displays the source IP address, if specified.

Port Displays the port or ports that will be forwarded to the LAN. Also known as the external port(s).

Dest IP/Port Displays the destination IP address and port(s) that will receive the forwarded port traffic. Also known as the internal port(s).

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the port forwarding entry. Go to the *Create or Edit a Port Forwarding Entry* section.
- **Delete** Click DELETE to remove the port forwarding entry.

To create a port forwarding rule, click + CREATE NEW PORT FORWARD RULE and go to the *Create or Edit a Port Forwarding Entry* section.

Create or Edit a Port Forwarding Entry

Name Enter a name to identify this port forwarding entry.

From The default is *Anywhere*, which accepts traffic from any source IP address. To specify a source IP address, select **Limited** and enter the source IP address in the field provided.

Port Enter the port or ports that will be forwarded to the LAN (also known as the external port or ports). You can identify the port or ports by name, number, and/or range. To specify multiple ports, use a comma-separated list (example: *20-23,554*).

Forward IP Enter the LAN IP address that will receive the forwarded port traffic.

Forward Port Enter the port or ports that will receive the forwarded port traffic (also known as the internal port). You can identify the port or ports by name, number, and/or range. If you do not specify this port, then the original destination port of the traffic will be used.

Protocol Select the protocol that will be forwarded: **Both**, **TCP**, or **UDP**.

Logs Select this option to create port forward logs.

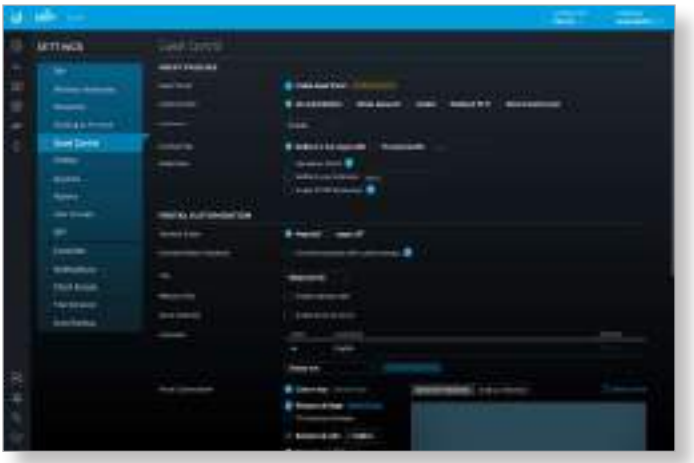
Save Click to apply changes.

Cancel Click to discard changes.

Settings > Guest Control

The *Guest Control* screen displays the following sections:

- *Guest Policies* (see below)
- **"Portal Customization" on page 40**
- **"Hotspot" on page 41** (for *Hotspot* authentication)
- **"Access Control" on page 45**



Guest Policies

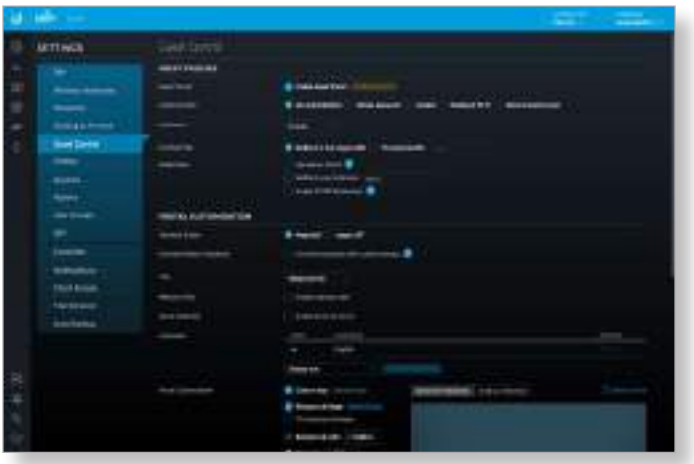
Enable Guest Portal Disabled by default. When disabled, guests can access the internet without entering a password or accepting the terms of service. When this option is enabled, you can control the *Guest Portal*.

Authentication When the *Guest Portal* is enabled, the authentication options will appear:

- *Authentication > No Authentication*
- **"Authentication > Simple Password" on page 38**
- **"Authentication > Hotspot" on page 38**
- **"Authentication > Facebook Wi-Fi" on page 39**
- **"Authentication > External Portal Server" on page 39**

Authentication > No Authentication

Select this option if guests are not required to log in (you can choose to require the terms of service).



Expiration Specify the guest login expiration after a designated period of time: **8 hours**, **24 hours**, **2 days**, **3 days**, **4 days**, **7 days**, or **User-defined**, which can be designated in *minutes*, *hours*, or *days*.

Landing Page After connecting, guests are redirected to the landing page. Select one of the following options:

- **Redirect to the original URL** After connecting, guests are directed to the URL they requested.
- **Promotional URL** After connecting, guests are redirected to the URL that you specify. Ensure that the URL begins with **http://**. Example: http://www.ubnt.com

Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal.

Redirect Using Hostname Select this option to enter and use a hostname for the portal URL in place of the default IP address. Paired with an SSL certificate, this ensures that site certificates are displayed as trusted in the guest browser. Example: www.ubnt.com

When logging in with *No authentication*, guests can click **Connect** for immediate access.

If you enable the terms of service, then guests will be required to accept the terms of use before gaining access to the internet.

You can select **Enable terms of service** under *Settings > Guest Control > Portal Customization* to enforce selection of the terms of service by the guest. See **"Access Control" on page 45** for more information.

Enable HTTPS Redirection When selected, unauthorized guests will be redirected to the guest portal when they are HTTPS browsing.

Authentication > Simple Password

Select this option if guests are required to enter a simple password (you can choose to require the terms of service). See **"Guest Policy" on page 24** for more information.

Guest Password Enter a password that guests must enter before connecting to the internet.

Expiration Specify the guest login expiration after a designated period of time: **8 hours**, **24 hours**, **2 days**, **3 days**, **4 days**, **7 days**, or **User-defined**, which can be designated in *minutes*, *hours*, or *days*.

Landing Page After connecting, guests are redirected to the landing page. Select one of the following options:

- **Redirect to the original URL** After connecting, guests are directed to the URL they requested.
- **Promotional URL** After connecting, guests are redirected to the URL that you specify. Ensure that the URL begins with **http://**. Example: http://www.ubnt.com

Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal. If you don't have a valid certificate installed on the UniFi Controller, then guests will see a certificate error and the Captive Network Assistant on OS X may not appear.

Redirect Using Hostname Select this option to enter and use a hostname for the portal URL in place of the default IP address. Paired with an SSL certificate, this ensures that site certificates are displayed as trusted in the guest browser. Example: www.ubnt.com

When logging in with *Simple Password* authentication, guests will be required to enter the *Guest Password* before gaining access to the internet.

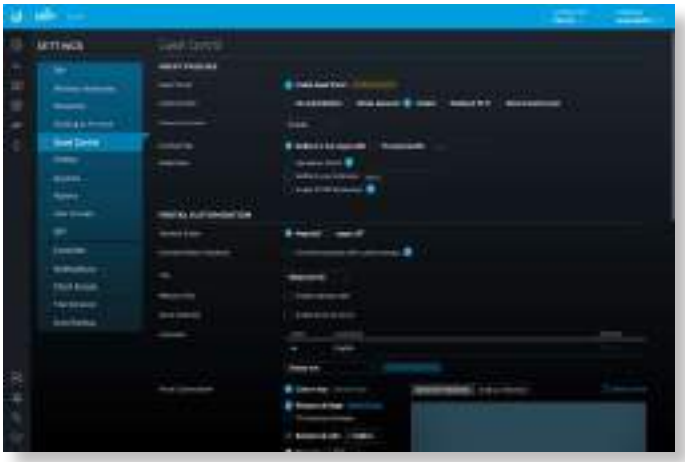
If you enable the terms of service, then guests will be required to accept the terms of use before gaining access to the internet.

You can select **Enable terms of service** under *Settings* > *Guest Control* > *Portal Customization* to enforce selection of the terms of service by the guest. See **"Access Control" on page 45** for more information.

Enable HTTPS Redirection When selected, unauthorized guests will be redirected to the guest portal when they are HTTPS browsing. They may see an invalid certificate error if they are HTTPS browsing before authentication.

Authentication > Hotspot

Select this option to enable *Hotspot* functionality, including the ability to customize portal login pages and bill customers using major credit cards or other supported methods. You must also select **Enable Guest Portal** under *Settings* > *Guest Control* to enforce voucher entry, payment, and selection of the terms of service by the guest. See **"Guest Policy" on page 24** for more information.



Default Expiration Specify the guest login expiration after a designated period of time: **8 hours**, **24 hours**, **2 days**, **3 days**, **4 days**, **7 days**, or **User-defined**, which can be designated in *minutes*, *hours*, or *days*.

Landing Page After connecting, guests are redirected to the landing page. Select one of the following options:

- **Redirect to the original URL** After connecting, guests are directed to the URL they requested.
- **Promotional URL** After connecting, guests are redirected to the URL that you specify. Ensure that the URL begins with **http://**. Example: http://www.ubnt.com

Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal. If you don't have a valid certificate installed on the UniFi Controller, then guests will see a certificate error and the Captive Network Assistant on OS X may not appear.

Redirect Using Hostname Select this option to enter and use a hostname for the portal URL in place of the default IP address. Paired with an SSL certificate, this ensures that site certificates are displayed as trusted in the guest browser. Example: www.ubnt.com

Enable HTTPS Redirection When selected, unauthorized guests will be redirected to the guest portal when they are HTTPS browsing. They may see an invalid certificate error if they are HTTPS browsing before authentication.

Authentication > Facebook Wi-Fi

Select this option to enable free Wi-Fi via Facebook, so businesses can offer free Wi-Fi via Facebook check-in for their customers. For more information, go to: **https://www.facebook.com/help/facebookwifi**

Expiration Specify the guest login expiration after a designated period of time: **8 hours**, **24 hours**, **2 days**, **3 days**, **4 days**, **7 days**, or **User-defined**, which can be designated in *minutes*, *hours*, or *days*.

Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal. If you don't have a valid certificate installed on the UniFi Controller, then guests will see a certificate error and the Captive Network Assistant on OS X may not appear.

Redirect Using Hostname Select this option to enter and use a hostname for the portal URL in place of the default IP address. Paired with an SSL certificate, this ensures that site certificates are displayed as trusted in the guest browser. Example: www.ubnt.com

Enable HTTPS Redirection When selected, unauthorized guests will be redirected to the guest portal when they are HTTPS browsing. They may see an invalid certificate error if they are HTTPS browsing before authentication.

Facebook Wi-Fi

Gateway Name Enter the name of your Facebook Wi-Fi gateway.

Gateway Configuration You can configure the gateway after you register it with Facebook. The registration will happen automatically after applying the changes with the Facebook Wi-Fi feature enabled for the first time. Once you select the name, you cannot change it without registering the gateway again.

For more information, go to: **https://www.facebook.com/help/facebookwifi**

Authentication > External Portal Server

Select this option if you are using an external server to host a custom guest portal.

Custom Portal Enter the IP address in the *IP Address* field.

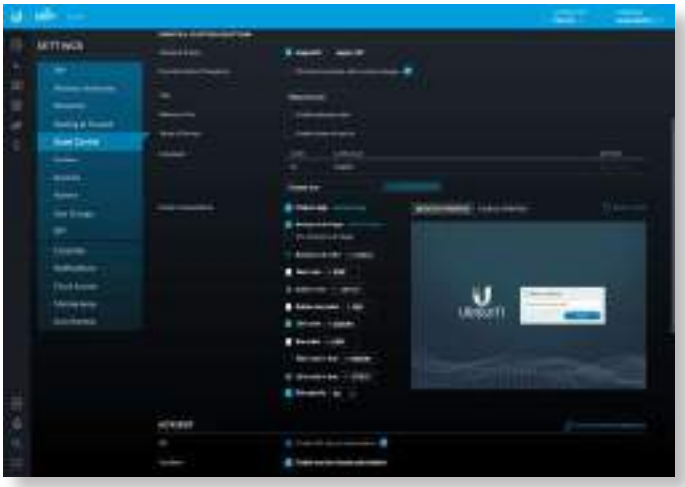
Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal. If you don't have a valid certificate installed on the UniFi Controller, then guests will see a certificate error and the Captive Network Assistant on OS X may not appear.

Redirect Using Hostname Select this option to enter and use a hostname for the portal URL in place of the default IP address. Paired with an SSL certificate, this ensures that site certificates are displayed as trusted in the guest browser. Example: www.ubnt.com

Enable HTTPS Redirection When selected, unauthorized guests will be redirected to the guest portal when they are HTTPS browsing. They may see an invalid certificate error if they are HTTPS browsing before authentication.

Portal Customization

Select this option to have customized portal pages appear in place of the default login pages. (This option is not available if you are using Facebook Wi-Fi or an external portal server.)



Template Engine Select **AngularJS** for client-side rendering or **Legacy JSP** for server-side rendering. We recommend AngularJS unless you are using old templates.

Note: AngularJS is not compatible with old templates because the old templates were designed to work with JSP (Java Server Pages).

The UniFi Controller offers a built-in editor to customize AngularJS; however, it is not fully customizable at this time.

AngularJS is a single-page app, so it should work more quickly. However, AngularJS uses JS (JavaScript), which may not work with some really old web browsers or newer browsers with JS support disabled.

AngularJS uses responsive design, so it will adapt to the size of a mobile device, such as a tablet or smartphone.

Legacy JSP is fully customizable and uses old HTML, so it should work with any web browser. You can customize Legacy JSP only by overriding files. Legacy JSP works more slowly and is not responsive by default.

AngularJS

Select **AngularJS** for client-side rendering.

- **Override Default Templates** Select this option if you want to manually edit the styles or templates. Please note that changing the templates may mean that some of the fields available in the UI will no longer apply to the portal.
- **Title** Enter the title of your portal. The default is *Hotspot portal*.
- **Welcome Text** Select **Enable welcome text** to add a welcome message.

After you have added your welcome text, click **Submit** to save your changes or click *Cancel*.

Once you have welcome text, then you can click EDIT to make changes.

  - **Text position** Select the appropriate location for the welcome text, **Under the logo** or **Above boxes**.

- **Terms of Service** Select **Enable terms of service** to add any terms of service you want hotspot users to accept.

Click **Submit** to save your changes or click *Cancel*.

Once you have the terms of service, then you can click EDIT to make changes.

- **Languages** Displays the languages you have added. English is the default and cannot be deleted.
  - **Code** Displays the language code.
  - **Language** Displays the name of the language.
  - **Actions** Click DELETE to remove the language.
  - **Add Language** To add a language, select it and click + ADD LANGUAGE.

  Note: Some languages are not supported by default, so you will need to create a *locales/<code>/* directory in your overrides path and translate the appropriate language files.

- **Portal Customization** You can make the following formatting changes:
  - **Customize logo** Click **Upload image** and select the logo you want to use. (We recommend the use of the .png format.) Then click **Open**.
  - **Background image** Click **Upload image** and select the image you want to use. (We recommend the use of the .jpg format.) Then click **Open**.
    - **Tile background image** Select this option if you want to repeat the background image in a tile pattern.

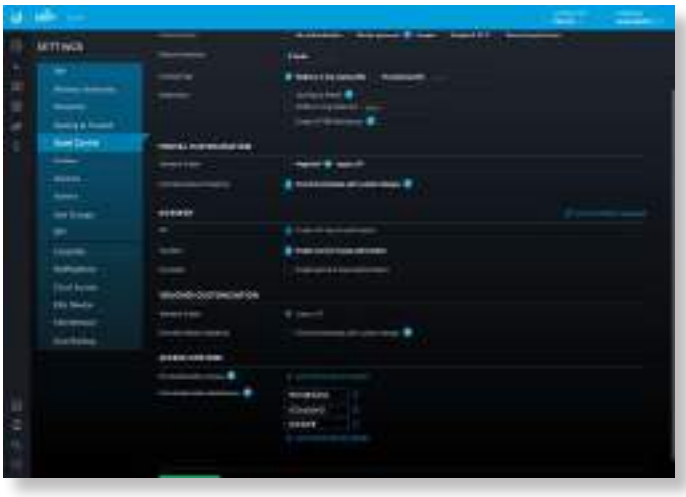
- **Background color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#233041*.
- **Text color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#ffffff*.
- **Button color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#1379b7*.
- **Button text color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#ffffff*.
- **Link color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#00db9e*.
- **Box color** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#ffffff*.
- **Text color in box** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#000000*.
- **Link color in box** Click to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#1379b7*.
- **Box opacity** You can change the opacity of the box background color. The default is *90*.

- **Desktop Preview** Enabled by default. The **Desktop Preview** previews the portal in the desktop view.
- **Mobile Preview** Click **Mobile Preview** to preview the portal in the mobile view.
- **Reset Style** Reset *Portal Customization* changes to the factory defaults.

Note: At this time AngularJS does not support voucher customization; however, you can customize vouchers using the voucher.html and voucher.css files. Refer to **"Customizable Default Files" on page 160** for more information.

Legacy JSP

Select this option to enable server-side rendering.



- **Override Default Templates** Select this option if you want to manually edit the styles or templates. Please note that changing the templates may mean that some of the fields available in the UI will no longer apply to the portal. See **"Portal Customization with Legacy JSP" on page 157** for more information.

Hotspot

When *Hotspot* authentication is selected, the *Hotspot* section is displayed.

API API-based authorization is enabled by default.

Select the methods of authorization:

Vouchers Use Hotspot Manager to create vouchers (including distributable code, duration values, and use restrictions). See **"Payments" on page 42** and **"Hotspot Manager" on page 151**.

Payments Set up payment-based authentication. Go to the *Payments* section.

RADIUS Available if AngularJS is enabled. Go to **"RADIUS" on page 48**.

Facebook Available if AngularJS is enabled. This authentication method requires *Redirect using hostname* to be enabled. Go to **"Facebook" on page 45**.

Google+ Available if AngularJS is enabled. This authentication method requires *Redirect using hostname* to be enabled. Go to **"Google+" on page 45**.

Go to Hotspot Manager Click **Go to Hotspot Manager** to manage *Analytics*, *Wireless Guests, Payments/Transactions, Vouchers,* and *Operator Accounts*. See **"Hotspot Manager" on page 151**.

When logging in with voucher-based *Hotspot* authentication, guests will be required to enter the voucher number before gaining access to the internet.

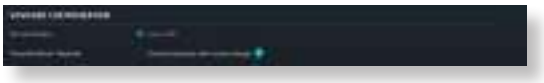
If you enable the terms of service, then guests will be required to accept the terms of use before gaining access to the internet.

When logging in with payment-based *Hotspot* authentication, guests will be required to select the package type and click the payment choice before gaining access to the internet.

If you enable the terms of service, then guests will be required to accept the terms of use before gaining access to the internet.

You can select **Enable terms of service** under *Settings > Guest Control > Portal Customization* to enforce selection of the terms of service by the guest. See **"Portal Customization with Legacy JSP" on page 157** for more information.

Voucher Customization



Template Engine Legacy JSP is enabled by default.

Override Default Templates Select this option if you want to manually edit the styles or templates. Please note that changing the templates may mean that some of the fields available in the UI will no longer apply to the portal. See **"Portal Customization with Legacy JSP" on page 157** for more information.

Payments

Payment Packages (Available only for payment-based authentication.) There are three packages by default: *Basic 8HR ($5.99)*, *Premium Daypass ($8.99)*, and *Free Trial*.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the package settings. Go to **"Add or Edit a Package" on page 43**.
- **Delete** Click DELETE to delete the package.

Add Another Package Click + ADD ANOTHER PACKAGE to create a new package. Go to **"Add or Edit a Package" on page 43**.

Add or Edit a Package

- **Name** Enter or edit the name of the package.
- **Payment** Select **Free package** if appropriate. (Only one free package is allowed. There is a free package by default, so unless you delete it, this option is not available.)
- **Price** Select the appropriate currency from the drop-down menu, and then enter the price.
- **Charged as** Enter the text that will be shown on the credit card statement.
- **Overwrite Limit** Select this option if you want to overwrite the user group policy per WLAN/user.
- **Hours** Enter the number of access hours the package allows.
- **Limit Download** Enter the maximum download bandwidth in Kbps.
- **Limit Upload** Enter the maximum upload bandwidth in Kbps.
- **Limit Quota** Enter the maximum amount (in megabytes) of data transfer allowed per session.
- **Customize payment fields** Select to customize form fields.
  - **Enable first name field** Select this option to create a field for a first name.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable last name field** Select this option to create a field for a last name.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable address field** Select this option to create a field for an address.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable city field** Select this option to create a field for a city.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable state field** Select this option to create a field for a state.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable Zip/Postal Code field** Select this option to create a field for a zip or postal code.
    - **Required** Select this option if you want to make this field mandatory.
  - **Enable country field** Select this option to create a field for a country.
    - **Required** Select this option if you want to make this field mandatory.
    - **Default value** Select the appropriate default country from the drop-down menu.
  - **Enable email field** Select this option to create a field for an email address.
    - **Required** Select this option if you want to make this field mandatory.
  - **Submit** Click to apply changes.
  - **Cancel** Click to discard changes.

Payment Field Options Certain fields may be required by some payment gateways; please check with your payment gateway for specific requirements. Refer to the *Add or Edit a Package* section in the previous column for information about the *Payment Field Options*.

Payment Gateway You have multiple options:

- **PayPal™ Website Payment Pro (US, Canada, UK)** Use your **PayPal Website Payments Pro** account. To manage payments and transactions, click GO TO HOTSPOT MANAGER, and see **"Hotspot Manager" on page 151**.

Enter the PayPal account details:

- **API Username** Enter the corresponding *Username*.
- **API Password** Enter the corresponding *Password*.

- **API Signature** Enter the corresponding *Signature* for the PayPal account that will receive payments.
- **Use sandbox account** For PayPal testing purposes, select this option. Then click **Apply Sandbox Account** to set up or access your **PayPal Sandbox Test Environment**.

- **Stripe (US, Canada, UK)** Use your **Stripe** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 151**.

Enter the Stripe account detail:

- **API Key** Enter the live secret API key.

Note: We recommend that you perform a test transaction with the test secret API key first before using the live secret API key.

- **Quickpay (Europe)** Use your **Quickpay** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 151**.

Enter the Quickpay account details:

- **Merchant ID** Enter the ID for your merchant account.
- **API User API Key** Enter the API key.
- **Agreement ID** Enter the agreement ID.
- **Enable test mode** Select this option to use the test mode.

- **Authorize.Net® (US, Canada)** Use your **Authorize.Net** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 151**.

Enter the Authorize.Net account details:

- **API Login ID** Enter the API login ID used to identify yourself as an authorized user.
- **Transaction Key** Enter the key used to authenticate transactions.
- **Use test account** For Authorize.Net testing purposes, select this option. Then click **Apply Test Account** to set up or access your **Authorize.Net test account**.

- **Merchant Warrior (Australia, New Zealand)** Use your **Merchant Warrior** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 151**.

Enter the Merchant Warrior account details:

- **Merchant UUID** Enter the ID for your merchant account.
- **API Key** Enter the API key.
- **API Passphrase** Enter the API passphrase.
- **Use test account** For Merchant Warrior testing purposes, select this option. Then click **Apply Test Account** to set up or access your **Merchant Warrior test account**.

- **IPpay™ (US, Canada)** Use your **IPpay** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 151**.

Enter the IPpay account details:

- **Terminal ID** Enter the terminal number for your merchant account.
- **Use test account** For IPpay testing purposes, select this option. Then click **Apply Test Account** to set up or access your **IPpay test account**.

RADIUS

Profile Select the appropriate RADIUS profile or create a new one; go to **"Create or Edit a RADIUS Profile" on page 45** for more information.

Authentication type Select **MS-CHAPv2** or **CHAP**.

Disconnect Requests Select this option to accept incoming disconnect requests.

- **Receiver Port** Enter the appropriate port number. The default is *3799*.

Facebook

App ID Enter the ID for the Facebook app. For more information, go to: **https://developers.facebook.com/docs/apps/register**

App Secret Enter the secret key.

Scope Select this option to request the user's email address.

For more information, go to: **ubnt.link/UniFi-Social-Media-Authentication**

Google+

Client ID Enter the ID for the Google API. For more information, go to: **https://developers.google.com/identity/protocols/OAuth2**

Client Secret Enter the secret key.

Scope Select this option to request the user's email address.

Domain Enter a domain to limit the connection to users of a specific Google Apps domain.

For more information, go to: **ubnt.link/UniFi-Social-Media-Authentication**

Access Control

Pre-Authorization Access Enter any hostnames or subnets (internal or external) that you want guests to be able to access, even if they have not been authenticated. Click the *delete* icon to remove a subnet from this list.

- **Add Hostname or Subnet** Click **Add Hostname or Subnet** to add more allowed hostnames or subnets.

Post-Authorization Restrictions Enter any hostnames or subnets that you don't want guests to be able to access. Click the *delete* icon to remove a subnet from this list.

- **Add Hostname or Subnet** Click **Add Hostname or Subnet** to add more restricted hostnames or subnets.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Settings > Profiles

You can use this option to create profiles for RADIUS authentication. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service.

RADIUS

Name Displays the name of the RADIUS authentication profile.

 # Servers Displays the number of servers associated with this profile.

Accounting Enabled Displays a check mark if RADIUS accounting is enabled.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete the profile.

Add New RADIUS Profile Click + CREATE NEW RADIUS PROFILE to create a new RADIUS profile. The *Create New RADIUS Profile* screen appears.

Create or Edit a RADIUS Profile

Profile Name Enter a name for the RADIUS profile.

VLAN Support Use these options to configure VLAN support:

- **Enable RADIUS assigned VLAN for Wired Network** Disabled by default. Select this option to allow the RADIUS server to dynamically assign a VLAN to a wired client.
- **Enable RADIUS assigned VLAN for Wireless Network** Disabled by default. Select this option to allow the RADIUS server to dynamically assign a VLAN to a wireless client.

  If you set a VLAN ID as a static value for another SSID on the same AP, then you cannot re-use the same VLAN ID for the RADIUS-assigned (dynamic) VLAN. For example, if you have a VLAN set to VLAN 10, then you cannot use VLAN ID 10 for RADIUS-controlled VLAN users as those users will not be assigned an IP address.

RADIUS Auth Server Enter information used to identify the RADIUS server(s):

- **IP Address** Enter the IP address of the RADIUS authentication server.
- **Port** Enter the port number of the RADIUS authentication server. The default is *1812*.
- **Password/Shared Secret** Enter the password or shared secret (a case-sensitive text string) that will be used to validate communication with the RADIUS authentication server.
- **Add Auth Server** Click to add another RADIUS authentication server to the profile.

Accounting This option is disabled by default. If you are using an accounting server, click **Enable Accounting** and then configure the *Interim Update* and *RADIUS Accounting Server* settings:

Interim Update To specify the duration between accounting information updates, select **Enable Interim Update**.

- **Interim Update Interval** Enter the appropriate duration between updates for UniFi APs; the default is *3600* seconds.

RADIUS Accounting Server Configure the following settings:

- **IP Address** Enter the IP address of the RADIUS accounting server.
- **Port** Enter the port number of the RADIUS accounting server. The default is *1813*.
- **Password/Shared Secret** Enter the password or shared secret (a case-sensitive text string) that will be used to validate communication with the RADIUS accounting server.
- **Add Accounting Server** Click to add another RADIUS authentication server to the profile.

Save Click to apply changes.

Cancel Click to discard changes.

Switch Ports

You can define switch port profiles that specify VLAN groupings for easy configuration. VLAN groupings allow you to create a combination of native networks (untagged) and tagged networks (tagged VLANs) for switch ports. The groupings configured here are then available for assignment to switch ports on the Switch's *Port Configuration* tab.

Name Displays the name of the profile.

PoE Displays the selected PoE option.

Native Network Displays the selected native network.

Link Neg. Displays the selected link negotiation option.

Isolation Displays the selected isolation option.

Storm Ctrl. Displays the selected storm control option.

Actions Click a button to perform the desired action:

- **View** Click VIEW to display more details. Go to the *Create or View Switch Port Profile* section.
- **Delete** Click DELETE to delete the entry.

Add New Port Profile Click to create a new profile.

Create or View Switch Port Profile

- **Profile Name** Enter a name to identify this profile.
- **PoE** Select the appropriate option: **Do not modify**, **Off**, **24V Passive**, **PoE/PoE+**, or **Passthrough**.
- **Native Network** The *Native Network* specifies the default VLAN, or Port VLAN Identifier (PVID), for the switch port. This determines the VLAN to be used for untagged traffic on that port. Most client devices do not VLAN-tag traffic; they will therefore only use the *Native Network* on their port.

The Switch accepts tagged and untagged packets in the ingress direction, and the untagged packets are assigned to the VLAN of the native network. For example, if the PVID is *VLAN 30*, then all untagged packets are assigned to *VLAN 30*. In the egress direction, the native network packets are stripped of the VLAN 30 header and exit as untagged packets.

This table lists how the packets are handled:

Packet Type	Ingress	Action	Egress
Tagged	Accepted	Remains tagged	Sent out as tagged
Untagged	Accepted	Assigned to VLAN of native network	VLAN header removed and sent out as untagged

Each physical port can have multiple networks attached; however, only one of them can be native (untagged). Select the appropriate native network. (Additional networks may be created in **"Settings > Controller" on page 56**.)

- **Tagged Networks** The VLANs chosen here will be permitted as tagged on switch ports configured with this grouping. This permits ingress and egress traffic with the applicable VLAN tag. Any VLAN tags other than those chosen here will be dropped.

  As an example, the following illustrates how an access point's switch port functions with one native network and two tagged VLANs used for additional wireless SSIDs. The AP's switch port uses a VLAN grouping with *LAN* (*VLAN 1*) as the native network, and has VLANs 20 and 30 defined as tagged networks.

  - VLAN 20: corporate
  - VLAN 30: guest

  This table lists how the packets are handled:

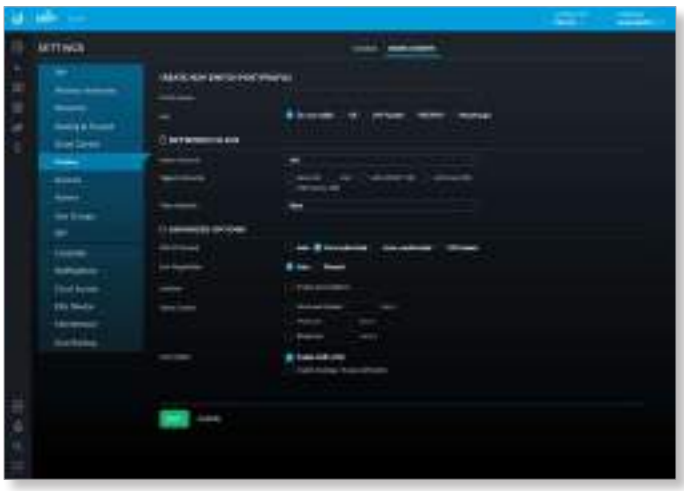
Packet Type	Ingress	Action	Egress
Untagged	Accepted	Assigned to VLAN 1	VLAN header removed and sent out as untagged
Tagged as VLAN 20	Accepted	Remains tagged	Sent out tagged as VLAN 20
Tagged as VLAN 30	Accepted	Remains tagged	Sent out tagged as VLAN 30

  The proper use of VLANs isolates the traffic of each VLAN. The guest traffic on VLAN 30 will be kept separate from the traffic on the corporate network.

  Select the appropriate tagged network. (Use **"Settings > Controller" on page 56** to create more networks.)

- **Voice Network** Select the appropriate voice network, if applicable.

- **Advanced Options** Click to access advanced options.



  - **802.1x Control** Select **Auto**, **Force authorized**, **Force unauthorized**, or **MAC-based** to use a RADIUS server for user authentication on the Switch's ports.
  - **Link Negotiation** The default is *Auto*, enabling Ethernet autonegotiation, which is appropriate for almost all cases. Do NOT use *Manual* unless the device being connected to the port has also been set manually; if so, then switch to **Manual** to disable autonegotiation and enable manual configuration of duplex and speed:
    - **Full Duplex** (Available for RJ45 ports only.) Full-duplex transmission is enabled by default. If disabled, it will be set to half duplex.
    - **Link Speed** Set the link speed of the interface as needed to match the device plugged into the port. For RJ45 ports, select **10 Gbps**, **1000 Mbps**, **100 Mbps**, or **10 Mbps**. For SFP+ ports, select **10 Gbps** or **1000 Mbps**. SFP ports must be set to **1000 Mbps**.
  - **Isolation** Select to mark this port as an isolated port. An isolated port cannot communicate directly with any other isolated port.
  - **Storm Control** Monitor the unicast, multicast, and/or broadcast traffic for this port. If the specified type of traffic on this port exceeds the threshold rate you specify, then the UniFi Switch drops the excess traffic.
    - **Unknown Unicast** Select to monitor unknown unicast traffic. Enter the threshold value in packets per second.

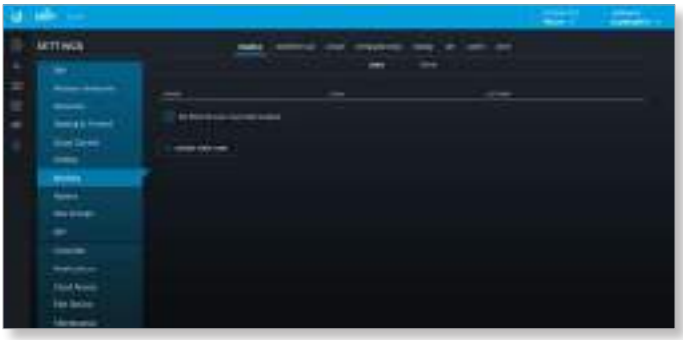
      Note: Unlike *Broadcast* and *Multicast* storm control, *Unicast* storm control does not apply to all unicast traffic. It applies only to traffic destined for a MAC address not found in the switch's MAC address table. Most devices should have a very low rate of such traffic. High rates of such traffic indicate malicious activity, or a broken device. Blocking excessive rates of such traffic may prevent problems on other devices on the network.

  - **Multicast** Select this option to control unicast traffic destined to unknown MAC addresses. Enter the threshold in packets per second.
  - **Broadcast** Select this option to monitor broadcast traffic. Enter the threshold in packets per second.
- **LLDP-MED** You can use LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and configuration of IP phones.
  - **Enable LLDP-MED** Enabled by default.
  - **Enable topology change notification** Disabled by default. This allows the Switch to receive notifications about any IP phone topology changes.

- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Settings > Services

You can configure a variety of services: RADIUS, Hotspot 2.0, DHCP, Dynamic DNS, MDNS, SIP, UPnP, and NTP.



RADIUS

Add RADIUS users and configure a RADIUS server.

Users

A list of RADIUS users is displayed.

Name Displays the name of the user.

VLAN Displays the assigned VLAN.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes. Go to the *Create or Edit a User* section.
- **Delete** Click DELETE to delete the profile.
- **Create New User** Click to add a new user.

Create or Edit a User

Create a new user or make changes.

- **Name** Enter the name of the user.
- **Password** Enter a password.
- **VLAN** Enter the appropriate VLAN number.
- **Tunnel Type** Select the appropriate type: *1 - Point-to-Point Tunneling Protocol (PPTP)*, *2 - Layer Two Forwarding (L2F)*, *3 - Layer Two Tunneling Protocol (L2TP)*, *4 - Ascent Tunnel Management Protocol (ATMP)*, *5 - Virtual Tunneling Protocol (VTP)*, *6 - IP Authentication Header in the Tunnel-mode (AH)*, *7 - IP-in-IP Encapsulation (IP-IP)*, *8 - Minimal IP-in-IP Encapsulation (MIN-IP-IP)*, *9 - IP Encapsulating Security Payload in the Tunnel-mode (ESP)*, *10 - Generic Route Encapsulation (GRE)*, *11 - Bay Dial Virtual Services (DVS)*, *12 - IP-in-IP Tunneling*, or *13 - Virtual LANs (VLAN)*.
- **Tunnel Medium Type** Select the appropriate tunnel medium type: *1 - IPv4 (IP version 4)*, *2 - IPv6 (IP version 6)*, *3 - NSAP*, *4 - HDLC (8-bit multidrop)*, *5 - BBN 1822*, *6 - 802 (includes all 802 media plus Ethernet "canonical format")*, *7 - E.163 (POTS)*, *8 - E.164 (SMDS, Frame Relay, ATM)*, *9 - F.69 (Telex)*, *10 - X.121 (X.25, Frame Relay)*, *11 - IPX*, *12 - AppleTalk*, *13 - Decnet IV*, *14 - Banyan Vines*, or *15 - E.164 with NSAP format subaddress*.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Server

Configure a RADIUS server.

Enable RADIUS Server Click to configure a RADIUS server.

Secret Enter the key shared with the RADIUS server.

Clients Clients are configured for the entire network.

Authentication Port Enter the appropriate port number to use for authentication; the default is *1812*.

Accounting Port Enter the appropriate port number to use for accounting; the default is *1813*.

Accounting Interim Interval Enter the appropriate duration between updates; the default is *3600* seconds.

Tunnelled Reply Enabled by default.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Hotspot 2.0

Use this option to create Hotspot 2.0 profiles for each site. Hotspot 2.0 is a standard for Wi-Fi roaming between Wi-Fi and cellular networks with automatic authentication.

Note: The Hotspot 2.0 feature is supported by generation 2 and 3 APs.

Hotspot 2.0 Profile Name Displays the name of the Hotspot 2.0 profile.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the profile. Go to the *Create or Edit a Hotspot 2.0 Profile* section.
- **Delete** Click DELETE to delete the profile.

Create or Edit a Hotspot 2.0 Profile

- **Hotspot 2.0 Profile Name** Enter a name for the Hotspot 2.0 profile.

Internetworking Information

- **Network Type** Select the network type: **Private network**, **Private network with guest access**, **Chargeable public network**, **Free public network**, **Personal device network**, **Emergency services only network**, **Test or experimental**, or **Wildcard**.
- **Network Access** Configure these settings as required:
  - **Internet** Disabled by default.
  - **Additional step required for access** Disabled by default.
  - **Emergency services reachable** Disabled by default.
  - **Unauthenticated emergency services accessible** Disabled by default.
- **HESSID** Specify the Homogeneous External Service Set Identifier (HESSID). This should be the MAC address of one of the APs in the network.
- **Venue Info** Specify the *Venue Group* and *Venue Type*. The available venue types vary depending on which venue group is selected, as shown in the following table:

Venue Group	Available Venue Types
Unspecified	*Unspecified*
Assembly	*Unspecified, Arena, Stadium, Passenger terminal, Amphitheater, Amusement Park, Place of worship, Convention center, Library, Museum, Restaurant, Theater, Bar, Coffee shop, Zoo or Aquarium, Emergency coordination center*
Business	*Unspecified, Doctor or Dentist office, Bank, Fire station, Police station, Post office, Professional office, Research and development facility, Attorney office*
Educational	*Unspecified, Primary school, Secondary school, University or College*
Factory or Industrial	*Unspecified, Factory*
Institutional	*Unspecified, Hospital, Long-Term Care Facility (e.g., nursing home, hospice, etc.), Alcohol and Drug Rehabilitation Center, Group home, Prison orJail*
Mercantile	*Unspecified, Retail store, Grocery market, Automotive service station, Shopping mall, Gas station*
Residential	*Unspecified, Private residence, Hotel or Motel, Dormitory, Boarding house*
Storage	*Unspecified*
Utility and Miscellaneous	*Unspecified*
Vehicular	*Unspecified, Automobile or Truck, Airplane, Bus, Ferry, Ship or Boat, Train, Motor Bike*
Outdoor	*Unspecified, Muni-mesh Network, City park, Rest area, Traffic control, Bus stop, Kiosk*

- **Venue Name** Displays a list of Hotspot 2.0 venues that have been created for the site:
  - **Language** Displays the language used by the venue.
  - **Name** Displays the name of the venue.
  - **Actions** Click DELETE to delete the venue.

To add a venue name:

- **Language** Select the appropriate language.
- **Name** Enter a descriptive name.
- **Add Venue Name** Click to save the venue name.

NAI Realm List

- **Name** Displays the name of the NAI realm.
- **EAP Method** Displays the name of the EAP method that is being used by the NAI realm.
- **Realm Enabled** Displays *Yes* if the realm is enabled or *No* if the realm is not enabled.
- **Actions** Click a button to perform the desired action:
- **Edit** Click EDIT to make changes to the NAI realm. Go to the *Add or Edit a NAI Realm* section.
- **Delete** Click DELETE to delete the NAI realm.
- **Add NAI Realm List** To add an NAI realm to the list, click + ADD NAI REALM. Go to the *Add or Edit a NAI Realm* section.

Add or Edit a NAI Realm

- **Name** Enter the name of the NAI realm.
- **Realm Enabled** Check the box to enable the NAI realm. This option is disabled by default.
- **EAP Method** Select the Extensible Authentication Profile (EAP) method: **EAP-TLS**, **EAP-SIM**, **EAP-TTLS**, **EAP-AKA**, or **EAP-AKA'**.
- **(List of authentication types)** Displays a list of authentication types that have been defined for this NAI realm list entry:
- **Auth Type** Displays the authentication type.
- **Auth Subtype** Displays the authentication subtype.
- **Actions** Click DELETE to delete the authentication type from the list.

To add an authentication type to the list, select the *Auth Type* and *Auth Subtype*, and then click + ADD AUTH.

The available authentication subtypes vary depending on the value of *Auth Type*, as shown in the following table:

Auth Type	Auth Subtype
Non-EAP Inner Authentication	*PAP, CHAP, MSCHAP, MSCHAPv2*
Inner Authentication EAP Method	*None*
Credential	*SM, USIM, NFC Secure Element, Hardware Token, Softoken, Certificate, Username/Password, Anonymous, Vendor Specific*

- **Submit** Click to save your changes to the NAI realm list entry.
- **Cancel** Click to discard changes.

Domain Name List

- **Name** Displays the domain name.
- **Actions** Click DELETE to delete the domain name from the list.
- **Add Domain Name** To add a domain name to the list, fill out the *Name* field, and then click + ADD DOMAIN NAME.

Roaming Consortium List

- **Name** Displays the name of the roaming consortium.
- **Organization ID** Displays the roaming consortium's IEEE-assigned organization ID.
- **Actions** Click DELETE to delete the roaming consortium from the list.

To add a roaming consortium to the list, fill out the *Name* and *Organization ID* fields, and then click + ADD ROAMING CONSORTIUM.

3GPP Cellular Network List

- **Name** Displays the name of the 3GPP cellular network.
- **MCC** Displays the Mobile Country Code (MCC). The default is *001*.
- **MNC** Displays the Mobile Network Code (MNC). The default is *001*.
- **Actions** Click DELETE to delete the 3GPP cellular network from the list.

To add a 3GPP cellular network to the list, fill out the *Name*, *MCC*, and *MNC* fields, and then click + ADD 3GPP CELLULAR NETWORK.

Save Click to apply changes made to the profile.

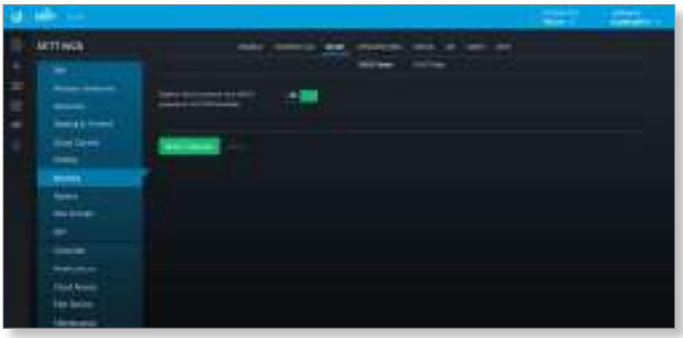
Cancel Click to discard changes.

DHCP

A DHCP (Dynamic Host Configuration Protocol) server assigns IP addresses to DHCP clients. You can add DHCP servers and configure DHCP relay.

DHCP Server

The UniFi Security Gateway forwards DNS queries from local clients to DNS servers.



Register client hostname from DHCP requests in USG DNS forwarder Enabled by default.

Apply Changes Click to save changes.

Reset Click to cancel changes.

DHCP Relay

You can add additional DHCP servers and configure DHCP relay settings. DHCP relay forwards DHCP packets to a DHCP server when DHCP clients are not on the same local network or subnet as their DHCP server.

DHCP Servers Click **Add Server**. Then enter the IP address of the new DHCP server in the field provided.

Hop Count Enter the maximum number of hops allowed (range: 1-255).

Maximum Packet Size Enter the maximum number of packets allowed (range: 64-1400).

Listen and Transmit Port Enter the port number (range: 1-65535).

Relay Agent Options Handling Specify what action should be taken if the DHCP request already includes relay information:

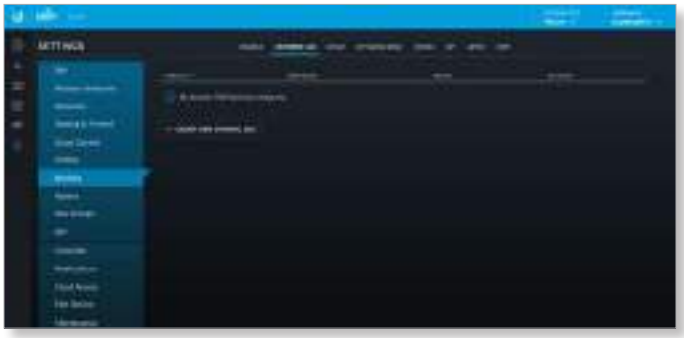
- **Default** Discards the DHCP packet.
- **Append** Adds to the existing DHCP packet.
- **Discard** Drops the DHCP packet.
- **Forward** Forwards the DHCP packet unchanged.
- **Replace** Replaces the existing DHCP packet.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Dynamic DNS

Domain Name System (DNS) translates domain names to IP addresses. Each DNS server on the internet holds these mappings in its respective DNS database. Dynamic Domain Name System (DDNS) is a network service that notifies the DNS server in real time of any changes in the device's IP settings. Even if the device's IP address changes, you can still access the device through its domain name. The list of DDNS entries is displayed:



Service Displays the name of the DDNS service.

Hostname Displays the hostname registered with the DDNS service.

Server Displays the IP address or hostname of the DDNS server that should receive DDNS updates.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete a DDNS entry.

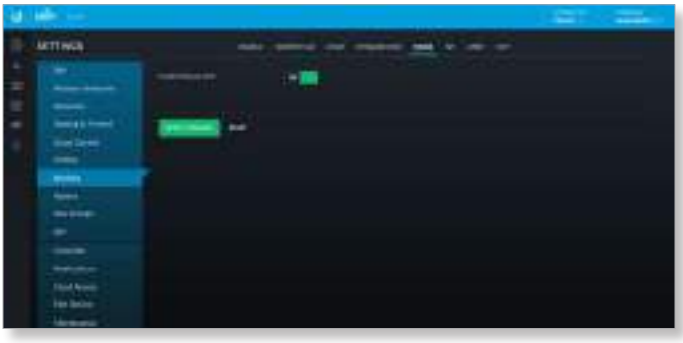
Create New Dynamic DNS Click to create a DDNS entry.

Create New Dynamic DNS

- **Interface** Select the appropriate interface, **WAN 1** or **WAN 2**.
- **Service** Select the appropriate DDNS service: **afraid**, **dnspark**, **dslreports**, **dyndns**, **easydns**, **namecheap**, **sitelutions**, or **zoneedit**.
- **Hostname** Enter the host name of the device.
- **Username** Enter the user name of the DDNS account.
- **Password** Enter the password of the DDNS account.
- **Server** Enter the address of your DDNS server.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

MDNS

mDNS (Multicast DNS) creates an identifier for a device to use as a hostname with a multicast service on a local network. This helps simplify network configuration because no unicast DNS server is needed.



Enable Multicast DNS Click to enable this option.

Apply Changes Click to save changes.

Reset Click to cancel changes.

SIP

You can configure the UAP-AC-EDU as a SIP client to use it as an extension of a SIP phone system.

Note: The UAP-AC-EDU can be used either as part of a SIP system or through the EDU app – not both. For example, if the UAP-AC-EDU is configured as a SIP client, then you cannot use the EDU app to make broadcasts through it.

Configuration

Primary SIP settings are configured. Use the *Endpoint* tab to add each UAP-AC-EDU as an endpoint (SIP client).

Enable EDU SIP Client Click to use the UAP-AC-EDU as a SIP client.

SIP Server For your SIP server, enter the IP address, IP address with port number (IP:port), FQDN, or FQDN with port number (FQDN:port). The default port is *5060*.

Outbound Proxy Optional: For your outbound proxy server, enter the IP address, IP address with port number (IP:port), FQDN, or FQDN with port number (FQDN:port).

Apply Changes Click to save changes.

Reset Click to cancel changes.

Endpoint

Add each UAP-AC-EDU as an endpoint. The list of existing endpoints is displayed.

Device Name Displays the MAC address or hostname.

Extension/Username Displays the extension number or username.

Auth User Displays the name of the authorized user.

Volume Displays the volume level.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete an endpoint.

Create New Endpoint Click to add a UAP-AC-EDU as an endpoint.

Create or Edit an Endpoint

- **Device** Select or search for the appropriate UAP-AC-EDU.
- **Extension/Username** Enter the extension number or username.
- **Auth User** Enter the name of the authorized user.
- **Password** Enter the SIP password.
- **Volume** Specify the volume level.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

UPnP

Instead of manually configuring port forwarding rules, you can use UPnP for automatic port forwarding when you have hardware that supports UPnP.

Configuration

Enable UPnP Disabled by default. Click to use this option; additional settings will appear.

WAN Interface Select the appropriate interface, **WAN 1** or **WAN 2**.

Enable NAT Port Mapping Protocol Enabled by default. This protocol is typically used by Apple devices.

Enable Secure Mode Enabled by default. This restricts port mappings to the clients' own IP addresses.

Networks

LAN Click to use UPnP for your primary local network.

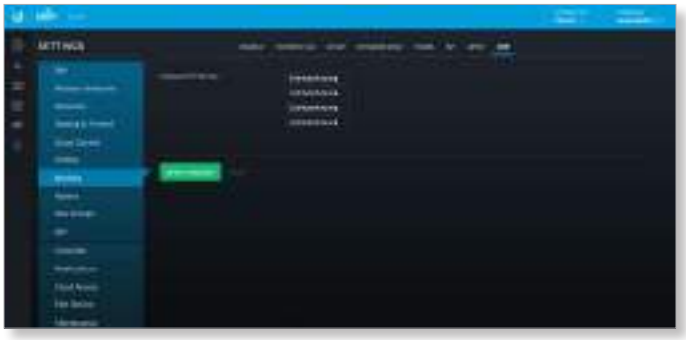
LAN__ Click to use UPnP for your local networks.

Apply Changes Click to save changes.

Reset Click to cancel changes.

NTP

NTP (Network Time Protocol) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. UniFi can obtain the system time from NTP servers on the internet.



Configure NTP Servers The default server IP addresses are displayed. You can designate different NTP servers.

Apply Changes Click to save changes.

Reset Click to discard changes.

Settings > Admins

You can create administrator accounts that are site-specific; these site administrators can only see the sites they manage and cannot see any devices that are *Pending Approval*.

The superadmin account is created during the Setup Wizard and has global admin (read/write) access; this superadmin account cannot be revoked or re-invited. Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: Ensure that you save the superadmin login information for future use.

To create operator accounts for the Hotspot Manager, see **"Operator Accounts" on page 155**.

Username Displays the name of the administrator.

Email Displays the email address of the administrator.

Verified Displays a checkmark to indicate that an admin is verified after he or she responds to an email invitation.

Role Displays the permissions level: *Admin* (read/write access) or *Read Only*.

Permissions Displays whether the admin can adopt devices, see pending devices, and/or have read-only access to all sites.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete the user group. (The *Default* user group cannot be deleted.)

Add New Admin Click + CREATE NEW ADMIN to add a new admin. Go to the *Create or Edit an Admin* section.

To create operator accounts for the Hotspot Manager, see **"Operator Accounts" on page 155**.

Create or Edit an Admin

- **Invite to Controller** Select this option to allow the new administrator access. The admin who issued the invitation can select which role the new administrator will have with respect to the UniFi Controller. You have three options:
  - **Send an invitation via email** Send an email to the new administrator.
    - **Name** Enter the name of the new administrator.
    - **Email** Enter the email address of the new administrator.
    - **Cloud Access** For remote access, select this option. The new administrator must use his or her own cloud account (linked to the same email address) to manage the UniFi Controller.
  - **Manually set and share the password** Set up the password and share it with the new administrator.
    - **Name** Enter the name of the new administrator.
    - **Password** Enter the password for the new administrator. Select **Require the user to change their password** if you want the password changed after the initial login.
    - **Email** Enter the email address of the new administrator.
  - **Invite existing admin** Add an administrator from another site.
    - **Select Admin** Search for an existing administrator from the drop-down list.
- **Role** Select **Administrator** (read/write access) or **Read Only**.
- **Site Permissions** Select this option to allow the new administrator to adopt pending devices.
- **Global Permissions** There are two options:
  - **Show pending devices** Select this option to allow the new administrator to view pending devices.
  - **Allow read only access to all sites** Select this option to restrict the new administrator to read-only access for all sites.
- **Invite** Click to invite the new administrator.
- **Cancel** Click to discard changes.

Settings > User Groups

Configure user groups on this screen. The default user group is named *Default* and has no bandwidth limits.

User Group Settings

Name Displays the name of the user group.

Bandwidth Limit (Download) Displays the download limit.

Bandwidth Limit (Upload) Displays the upload limit.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the user group settings. Go to the *Create or Edit a User Group* section.
- **Delete** Click DELETE to delete the user group. (The *Default* user group cannot be deleted.)

Create New User Group Click + CREATE NEW USER GROUP to create a new user group. Go to the *Create or Edit a User Group* section.

Create or Edit a User Group

- **Name** Enter or edit the name of the user group.

- **Bandwidth Limit (Download)** Select to limit the download bandwidth. Enter the maximum in Kbps.
- **Bandwidth Limit (Upload)** Select to limit the upload bandwidth. Enter the maximum in Kbps.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

See **"Wireless Client – Configuration" on page 148** or **"Wired Client – Configuration" on page 150** for information on how to assign a user or guest to a user group.

Settings > DPI

Configure the Deep Packet Inspection (DPI) settings of the UniFi Controller.

Enable DPI When enabled, this option turns on the DPI feature of the UniFi Security Gateway. The data will accumulate until you either click **Clear DPI Counters** (described below) or reboot/upgrade the Gateway. This feature will not work for any WAN connection when Smart Queue is enabled on it.

Clear DPI Counters Click this button to clear the DPI counters.

Apply Changes Click to save changes.

Reset Click to cancel changes.

DPI Restriction Groups

Add Group Click + ADD GROUP to add a group. Go to the *Add Group* section.

One group is created by default. Click + to expand the section for any group.

The following information is listed for each restriction:

Category/App Displays the traffic category or application.

Enabled Displays the status of the restriction.

Blocked Displays whether matching traffic is blocked.

Log Traffic Displays whether matching traffic is logged.

Actions Click the appropriate button:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete the DPI restriction group. (The *Default* group cannot be deleted.)

Add Restriction Click + ADD RESTRICTION to add a restriction. Go to the *Add Restriction* section.

Add Group

- **Group Name** Enter a descriptive name.
- **Create** Click to apply changes.
- **Cancel** Click to discard changes.

Add Restriction

- **Select Category** Select the appropriate traffic category from the drop-down list, and then click + ADD .
- **Enabled** Select to apply this restriction to the selected group.
- **Block** Select to block all traffic that matches this restriction.
- **Log Traffic** Select to log all traffic that matches this restriction.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

DPI Restriction Assignments

Click NETWORKS to expand the section for networks.

The following information is listed for each wired network:

Network Displays the name of the network.

Group Name Displays the name of the DPI restriction group.

Purpose Displays the purpose of the restriction.

Subnet Displays the subnet mask.

VLAN Displays the assigned VLANs, if any.

Actions Click the appropriate button:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to delete the restriction.

The following information is listed for each wireless network:

Network Displays the name of the network.

Group Name Displays the name of the DPI restriction group.

Security Displays the security description.

Guest Network Displays the name of the guest network.

VLAN Displays the assigned VLANs, if any.

Actions Click the appropriate button:

- **Edit** Click EDIT to make changes.
- **Delete** Click DELETE to remove this assignment.

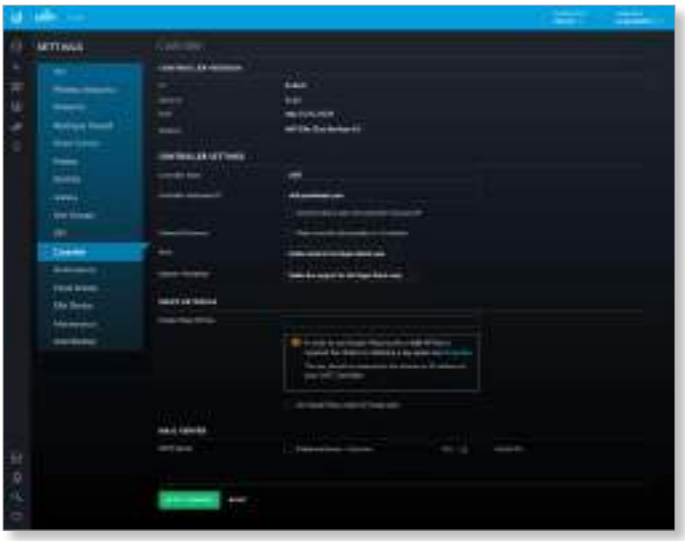
Assign Network Click + ASSIGN NETWORK to assign a restriction. Go to the *Assign Restriction* section.

Assign Restriction

- **Network** Select the appropriate wired or wireless network from the drop-down list.
- **Restriction Group** Select the appropriate DPI restriction group from the drop-down list.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Settings > Controller

(Available for the superadmin only.) Configure the system settings of the UniFi Controller.



Controller Version

UI Displays the version number of the user interface.

Backend Displays the version number of the server-side application and database.

Build Displays the version number of the software build.

Platform Displays the version number of the cloud service.

Controller Settings

Controller Name Enter a descriptive name for your UniFi Controller instance.

Controller Hostname/IP (For advanced users only.) Enter the hostname or IP address of the UniFi Controller.

Note: When alert emails are sent out, the *Controller Hostname/IP* will be specified in the *Controller URL* at the bottom of every message.

- **Override inform host with controller hostname/IP** An inform host URL is used for Layer-3 device adoption using the UniFi Discovery Utility. Select this option to override the inform host URL. Then enter the appropriate hostname or IP address.

  Note: The default inform port is *8080*. (You can customize this in system.properties.)

Network Discovery When enabled, this option allows UniFi to be discoverable via UPnP on the Layer-2 network. This option is disabled by default.

Store Users can have a link to **store.ubnt.com**. Select the appropriate option: **Enable store for the Super Admin only**, **Enable store for all users**, or **Disable store for all users**.

Support Messaging Select the appropriate option: **Enable Live Chat for the Super Admin only**, **Enable Live Chat for all users**, or **Disable Live Chat for all users**.

Maps Setting

If you want to use Google Maps on the *Map* screen, you need a Google API key. Follow the instructions in the following article to obtain a Google API key:

https://developers.google.com/maps/documentation/javascript/get-api-key#get-an-api-key

Google Maps API Key Enter a valid API key.

Use Google Maps engine for image maps Select this option to enable the use of Google Maps.

Mail Server

When enabled, UniFi will send email alerts triggered by disconnected UniFi devices. Specify the administrator email address when you create an account under **"Settings > Admins" on page 53**.

SMTP Server Select this option to enable emails.

- **Hostname** Enter the outgoing (SMTP) mail server name.
- **Port** The default is *25*. If Secure Sockets Layer (SSL) is enabled, then the port number will automatically change to *465*.
- **Enable SSL** You can enable SSL to enhance secure communications over the internet.
- **Enable authentication** Select this option to enable authentication.
  - **Username** Enter the username required by the mail server.
  - **Password** Enter the password required by the mail server.
- **Specify sender address** Select this option to specify the sender email address. Enter the email address that will appear as the sender of the email alert.
- **Test SMTP Server** Enter an email address and click **Send** to test the mail server setup.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Settings > Notifications

Customize the types of notifications you receive from the UniFi Controller for a variety of events.

(show/hide disabled events) Click to show or hide disabled events on the *Notifications* screen.

(collapse/expand all) Click to collapse all events to their section headings or expand to display all events on the *Notifications* screen.

AP Events Click to access *AP Events* notifications.

Select the appropriate notification type for the following event types involving APs: *AP adopted, AP automatically readopted, AP changed channel, AP configured, AP connected, AP deleted, Rogue AP detected, Pending AP discovered, AP elite license assigned, Elite AP offline, AP elite license revoked, AP upgrade failed (firmware check), AP upgrade failed (download), AP failed host key verification, AP isolated, AP license changed, AP disconnected, AP event, AP channel interference, AP detected radar, Pending AP rediscovered, AP restarted by admin, AP restarted by unknown, Rolling upgrade triggered, AP upgrade scheduled, AP upgraded, AP wireless event, Wireless uplink configured,* and *Wireless uplink disconnected.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

Gateway Events Click to access *Gateway Events* notifications.

Select the appropriate notification type for the following event types involving Gateways: *Gateway adopted, Gateway automatically readopted, Gateway commit error, Gateway connected, Gateway deleted, Pending gateway discovered, Gateway elite license assigned, Elite gateway offline, Gateway elite license revoked, Gateway upgrade failed (firmware check), Gateway upgrade failed (download), Gateway failed host key verification, Gateway license changed, Gateway disconnected, Gateway event, Gateway restarted by admin, Gateway restarted by unknown, Gateway upgrade scheduled,* and *Gateway upgraded.*

Event Select this option to receive a notification on the *Events* screen.

Alert Select this option to receive a notification on the *Alerts* screen.

Email Select this option to receive a notification email.

Switch Events Click to access *Switch Events* notifications.

Select the appropriate notification type for the following event types involving Switches: *Switch adopted, Switch automatically readopted, Switch connected, Switch deleted, Switch detected rogue DHCP server, Pending switch discovered, Switch elite license assigned, Elite switch offline, Switch elite license revoked, Switch upgrade failed (firmware check), Switch upgrade failed (download), Switch failed host key verification, Switch license changed, Switch loop detected, Switch disconnected, Switch event, Switch overheating, Switch restarted by admin, Switch restarted by unknown, Switch upgrade scheduled,* and *Switch upgraded.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

Client Events Click to access *Client Events* notifications.

Select the appropriate notification type for the following event types involving clients: *Client blocked (wired), Client unblocked (wired), Guest connected (wired), Guest disconnected (wired), User connected (wired), User disconnected (wired), Client blocked (wireless), Client unblocked (wireless), Guest unauthorized, Guest unauthorized by quota, Guest connected (wireless), Guest disconnected (wireless), Guest AP roaming, Guest channel roaming, User connected (wireless), User disconnected (wireless), User AP roaming,* and *User channel roaming.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

Hotspot Events Click to access *Hotspot Events* notifications.

Select the appropriate notification type for the following event types involving hotspots: *Guest authorized w/o authentication, Guest authorized by password, Guest payment processed,* and *Voucher used.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

Stream Events Click to access *Stream Events* notifications.

Select the appropriate notification type for the following event types involving streaming: *Stream config incorrect, Scheduled stream failed,* and *Stream skipped devices.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

Admin Events Click to access *Admin Events* notifications.

Select the appropriate notification type for the following event types involving administrators: *Auto backup failed, Guest authorized, Guest authorization extended, Guest unauthorized, Hotspot operator login, Admin login, Admin login failed, Payment refunded, Controller update available, Voucher(s) created,* and *Voucher deleted.*

- **Event** Select this option to receive a notification on the *Events* screen.
- **Alert** Select this option to receive a notification on the *Alerts* screen.
- **Email** Select this option to receive a notification email.

When you are done with customizing the notifications, you have the following options:

Apply Changes Click to save changes.

Reset Click to cancel changes.

Reset to Defaults Click to reset to the factory default settings.

Settings > Cloud Access

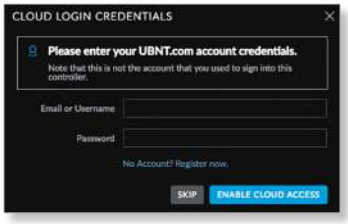
Set up the login for cloud access.

Cloud Access

Enable Cloud Access Disabled by default. Click to configure the login.

Note: Enabling or disabling cloud access will affect cloud access for all admins on that UniFi Controller.

The *Cloud Login Credentials* screen will appear.



- **Email or Username** Enter the email address or username of your UBNT account.
- **Password** Enter the password of your UBNT account.
- **No account? Register now.** If you do not have a UBNT account, click here to visit this link: **https://account.ubnt.com/register**

  Follow the on-screen instructions to set up an account.
- **Enable Cloud Access** Click to save changes.
- **Skip** Click to skip the login.

Controller

Status Displays "Connected" if cloud access is active.

User Cloud Access

Dashboard Click **unifi.ubnt.com** to access the dashboard for your cloud account.

Configured for Displays the username or email address of your UBNT account.

Advanced Options

Click to display the advanced option:

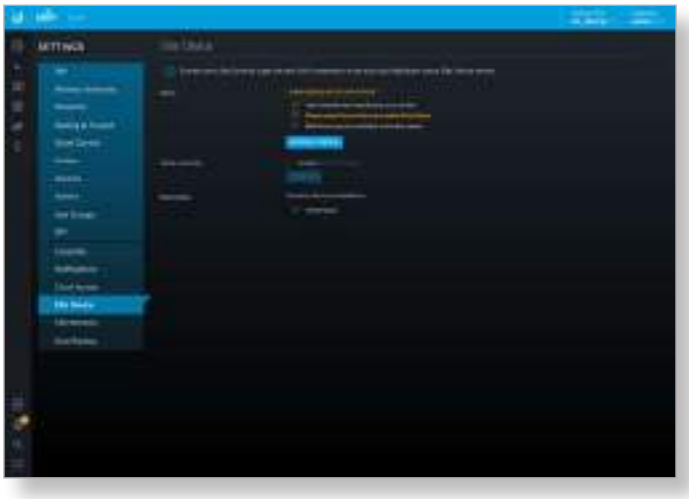
Report Errors to Ubiquiti Disabled by default. To enable connection errors to be reported to Ubiquiti, select this option. This allows us to acquire technical information to help troubleshoot any issues with connecting to our cloud services.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Settings > Elite

For information about the UniFi Elite service, go to: www.ubnt.com



Status

This section describes the status of the UniFi Elite service requirements, which includes, cloud access, online availability, acceptance of the Terms of Service, and Elite service availability in the applicable country.

Refresh Status Click to update the status information.

Terms of Service

I accept Terms of Service You can click Terms of Service to review the terms. To use the service, select **I accept Terms of Service**.

Confirm Click to confirm acceptance of these terms.

Restrictions

UniFi Elite service is currently available in the countries listed.

Settings > Maintenance

(Available for the superadmin only.) The *Maintenance* screen contains administrative options, so you can customize logs, manage system backups, and download configuration information to assist in support issues.

If your UniFi Controller is running on a UniFi Cloud Key, you can use the *Maintenance* tab to upgrade the UniFi Cloud Key firmware, upgrade the UniFi Controller software located on the UniFi Cloud Key, reboot the UniFi Cloud Key, power it off, or reset it to factory defaults.

Server Information

Current Version Displays the software version.

Services

Log Level You can customize the support information that is collected:

- **Device** Select the level of severity required to trigger device log entries: **Normal**, **More**, or **Debug**. The default is *Normal*.
- **Mgmt** Select the level of severity required to trigger management log entries: **Normal**, **More**, or **Debug**. The default is *Normal*.
- **System** Select the level of severity required to trigger system log entries: **Normal**, **More**, or **Debug**. The default is *Normal*.
- **Cloud Access** Select the level of severity required to trigger system log entries: **Normal**, **More**, or **Debug**. The default is *Normal*.
- **Apply** Click to save changes.

Compact Database Click to optimize disk usage by freeing up pre-allocated disk space. There may be service interruptions during the process. Click **Confirm** to continue.

Device Firmware Update Click to check for available firmware updates.

Data Retention

Time Series with 5 Minutes Granularity Select the appropriate interval: **1 hour**, **2 hours**, **6 hours**, **12 hours**, **1 day**, **7 days**, or **30 days**. The default is 1 *day*.

Time Series with Hourly Granularity Select the appropriate interval: **1 day**, **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, or **No limit**. The default is *30 days*.

Time Series with Daily Granularity Select the appropriate interval: **31 days**, **90 days**, **180 days**, **365 days**, or **No limit**. The default is *90 days*.

Time Series with Monthly Granularity Select the appropriate interval: **31 days**, **90 days**, **180 days**, **365 days**, or **No limit**. The default is *365 days*.

Non time series (Users, Devices, Events...) Select the appropriate interval: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **No limit**. The default is *365 days*.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Backup

Backup Data Retention Select the time duration of the backup data retention: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **No limit**. The default is *7 days*.

Download Backup Click this option to download a file that contains all of your settings and data retained for the duration you specify, so you can restore them later if you choose.

Restore

Browse Click **Choose File** to select a backup file that you've already downloaded. Follow the on-screen instructions to restore settings from the selected file.

Support Info

Download Click **Download Support Info** to download a file to your computer with information about your configuration. You can email this file to our support team.

System Config Click **Show System Config** to view configuration settings. The *System Config* screen appears.

System Config

- **Network Config** Click **Network Config** to view the network configuration settings.
- **APs** Displays the APs by model and quantity.
- **Version** Displays the software version.
- **DPI** Displays the status of the *DPI* (Deep Packet Inspection) feature, which is configured in **"Settings > Site" on page 21**.
- **Conn Monitor** Displays the status of the *Uplink Connectivity Monitor* feature, which is configured in **"Settings > Site" on page 21**.
- **Cloud Access** Displays the status of the *Cloud Access* feature.
- **Current Site** Displays the name of the current site.
- **Networks** Displays the name(s) of the current network(s).
- **Wireless Networks** Displays the name(s) of the current wireless networks.
- **Guest Portal** Displays the status of the Guest Portal feature, which is configured in **"Settings > Guest Control" on page 37**.
- **Authentication** Displays the type of authentication required for guest access, which is configured in **"Settings > Guest Control" on page 37**.
- **Expiration** Displays the period of time before a guest login expires, which is configured in **"Settings > Guest Control" on page 37**.
- **Landing Page** Displays the type of landing page for guest access, which is configured in **"Settings > Guest Control" on page 37**.
- **Portal Customization** Displays the status of the Portal Customization feature, which is configured in **"Portal Customization" on page 40**.
- **Name/MAC Addr.** Displays the hostname, alias, or MAC address of the device.
- **Model** Displays the model number of the device.
- **Version** Displays the version number of the firmware.
- **Channel 2G/5G** Displays the channel used on each radio band.
- **Power 2G/5G** Displays the TX power used on each radio band.
- **Clients 2G/5G** Displays the number of clients on each radio band.
- **Band Str.** Displays the status of the band steering feature.
- **ATF** Displays the status of the airtime fairness feature.
- **Load Bal. 2G/5G** Displays the load balancing for the 2.4 and 5 GHz radio bands.
- **Min. RSSI 2G/5G** Displays the minimum client signal threshold for each radio band.
- **Uplink State** Displays the status of the uplink, if applicable.
- **IP Addr.** Displays the local IP address of the device.
- **Uptime** Displays the duration of time the device has been running.
- **Uplink** Displays the duration of the uplink connection.
- **Close** Click **Close** to exit this screen.
- **Download** Click **Download** to download a screenshot in .png format.

Network Config

- **Name** Displays the name of the local wired network.
- **Purpose** Displays a description of this network.
- **Subnet** Displays the IP address and prefix size.
- **DHCP Server** Displays the status of the DHCP server feature.
- **DHCP Range** Displays the range of available IP addresses.
- **DHCP Name Server** Displays the IP address of the DNS server.
- **DHCP WINS Server** Displays the IP address of the WINS server.
- **DHCP Lease Time** Displays the lease time for any assigned IP address.
- **IGMP Snooping** Displays the status of the *IGMP Snooping* feature.
- **Close** Click **Close** to exit this screen.
- **Download** Click **Download** to download a screenshot in .png format.

Cloud Key

If you have a Cloud Key, go to the following sections:

- *Cloud Key Firmware*
- *Cloud Key Controller*
- *Cloud Key Operations*

Firmware

The *Firmware* section displays firmware versions according to the following filters:

(device) Select the appropriate filter: **All**, **Known Devices**, or **Site Devices**.

(firmware version) Select the appropriate filter: **All**, **Cached**, or **Available.**

Device Displays the device name.

Size (MB) Displays the size of the file.

Version Displays the firmware version number.

Actions Click a button to perform the desired action.

- **Cache** Click CACHE to save the firmware version for local hosting. This can be used for batch upgrades to groups of devices.

Cloud Key Firmware

The *Cloud Key Firmware* section is available if you are using a UniFi Cloud Key.

Current Version Displays the version number of the UniFi Cloud Key firmware. Click **Check for Update** to see if there is a newer firmware version. If there is, then you can follow the on-screen instructions to upgrade now.

Available Update If there is an available update, then the available firmware version number is displayed. Click **Apply Update** to upgrade the firmware.

Status Displays the current status, *Up to Date* or *Update Available*.

Cloud Key Controller

The *Cloud Key Controller* section is available if you are using a UniFi Cloud Key.

Current Version Displays the version number of the UniFi Controller software. Click **Check for Update** to see if there is a newer software version. If there is, then you can follow the on-screen instructions to upgrade now.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before upgrading.

Available Update If there is an available update, then the available software version number is displayed. Click **Apply Update** to upgrade the software.

Status Displays the current status, *Up to Date* or *Update Available*.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before upgrading.

Cloud Key Operations

Restart Cloud Key Click this option to powercycle the UniFi Cloud Key.

Shut Down Cloud Key Click this option to turn off the UniFi Cloud Key.

Reset Cloud Key Click this option to reset the UniFi Cloud Key to its factory default settings. This option will reboot the UniFi Cloud Key, and all factory default settings will be restored.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 60** for more information) before resetting the UniFi Cloud Key to its defaults.

Settings > Auto Backup

Configure the automatic backup settings for the UniFi Controller.

Note: If you are using a UniFi Cloud Key, make sure to insert an SD memory card before enabling this feature.

Enable Auto Backup Enable this option to turn on the automatic backup feature. Then configure the options:

- **Occurrence** Select how often to perform auto backup: (every) *Hour*, *Day*, *Week*, *Month*, or *Year*. Then select the appropriate time, day, and/or month, if applicable.
- **Occurrence Timezone** Select your time zone.
- **Maximum Number of Files** Specify the maximum number of backup files to save. The default is *7*.
- **Data Retention Days** Specify the length of time in days that data will be retained: **Settings only**, **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **No limit**.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Chat with Us

(Available if you are a superadmin or you are allowed to access live chat.) Click 💬 to open a window for online chat support.

Chapter 4: Dashboard

The *Dashboard* screen provides a visual representation of your network's status. Basic information is provided for each node:

- Latency
- Throughput
- **"WAN" on page 64**
- **"LAN" on page 64**
- **"WLAN" on page 65**

Latency

The latency value from the latest Speed Test is displayed. The monitor is color-coded to indicate status:

Black A UniFi Security Gateway is active, and the Speed Test is available.

Red The Speed Test is not available because it requires an active UniFi Security Gateway.

Throughput

The throughput value from the latest Speed Test is displayed. The monitor is color-coded to indicate status:

Black A UniFi Security Gateway is active, and the Speed Test is available.

Red The Speed Test is not available because it requires an active UniFi Security Gateway.

Status information Click the *Latency* or *Throughput* monitor to display the following:

WWW

Current status information is displayed.

- **Uptime** Displays the length of time the internet connection has been active.
- **Latency** Displays the amount of time it takes a packet to travel from the UniFi Security Gateway to the service provider's gateway.
- **Up** Displays the upload rate of your internet connection.
- **Down** Displays the download rate of your internet connection.

Speed Test

Results from the latest Speed Test are displayed.

- **Last Run** Displays the duration of time since the last Speed Test.

- **Latency** Displays the amount of time it takes a packet to travel from the UniFi Security Gateway to the service provider's gateway.
- **Up** Displays the upload speed.
- **Down** Displays the download speed.
- **Run Speed Test** Click to run the Speed Test.

Speed Test Click to run the Speed Test.

After the Speed Test is complete, the following will be displayed:

- *Download* speed
- *Upload* speed
- *Latency*, duration of the average Ping round-trip time

- **Close** Click to exit the Speed Test.
- **Run Speed Test** Click to run the test again.

WAN

The basic details of the UniFi Security Gateway are displayed.

The monitor is color-coded to indicate status:

Green The WAN connection is active.

Red The WAN connection is inactive.

Active Devices Displays the number of Gateway devices adopted and active.

Inactive Displays the number of Gateway devices adopted but not active.

Pending Displays the number of Gateway devices pending adoption.

Status information Click the monitor to display the following:

- **Gateway** Displays the IP address of the UniFi Security Gateway.
- **DNS** Displays the IP addresses of the Domain Name System (DNS) servers.
- **Clients** Displays the total number of local clients.
- **Up** Displays the upload rate of your internet connection.
- **Down** Displays the download rate of your internet connection.

LAN

The basic details of the wired network(s) are displayed.

The monitor is color-coded to indicate status:

Green The wired network is active.

Red The wired network is inactive.

Active Devices Displays the number of wired devices adopted and active.

Inactive Displays the number of wired devices adopted but not active.

Pending Displays the number of wired devices pending adoption.

Status information Click the monitor to display the following:

- **LAN IP** Displays the local IP address of the UniFi Security Gateway.
- **Users** Displays the number of clients connected to the wired network.
- **Guests** Displays the number of clients connected to the guest wired network.
- **Switches** Displays the number of UniFi Switches managed on this site.
- **Down** Displays the download rate of the wired network(s).
- **Up** Displays the upload rate of the wired network(s).

WLAN

The basic details of the wireless network(s) are displayed.

The monitor is color-coded to indicate status:

Green The wireless network is active.

Red The wireless network is inactive.

Active Devices Displays the number of APs adopted and active.

Inactive Displays the number of APs adopted but not active.

Pending Displays the number of APs pending adoption.

Status information Click the monitor to display the following:

- **Users** Displays the number of clients connected to the primary wireless network(s).
- **Guests** Displays the number of clients connected to the guest wireless network(s).
- **APs** Displays the number of APs managed on this site.
- **Down** Displays the download rate of the wireless network(s).
- **Up** Displays the upload rate of the wireless network(s).

Download Throughput & Latency

The historical chart displays the download traffic in terms of throughput and latency over a 24-hour period.

Note: A UniFi Security Gateway must be active to enable this chart.

Avg/Max Throughput Average throughput is displayed as a dark gray bar. Maximum throughput is displayed as a light gray bar.

Latency Latency is displayed as a blue line.

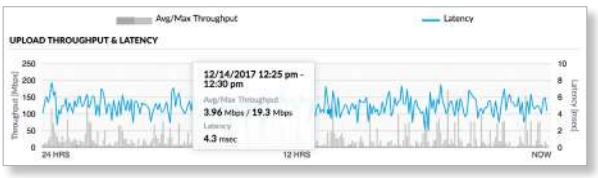
Status information Click a specific point to display the following about a date and time:

- **Avg/Max Throughput** Displays the average and maximum throughput values.
- **Latency** Displays the latency value.

Upload Throughput & Latency

The historical chart displays the upload traffic in terms of throughput and latency over a 24-hour period.

Note: A UniFi Security Gateway must be active to enable this chart.



Avg/Max Throughput Average throughput is displayed as a dark gray bar. Maximum throughput is displayed as a light gray bar.

Latency Latency is displayed as a blue line.

Status information Click a specific point to display the following about a date and time:

- **Avg/Max Throughput** Displays the average and maximum throughput values.
- **Latency** Displays the latency value.

Devices on 2.4 GHz Radio Band

The 2.4 GHz Channel Occupancy Chart displays the channel use of the 2.4 GHz band on a per-AP basis.

Note: At least one 2.4 GHz UniFi AP must be active to enable this chart.

1-11 Each AP is represented by a square icon, which is located in the channel to which the AP is currently assigned. The gray peak associated with each channel indicates the relative percentage of channel utilization on each assigned channel.

The color of the square icon indicates the percentage of channel utilization on each AP assigned to the displayed channel:

Color	Status	Percentage of Utilization
	Ideal	Low: <50%
	Acceptable	Medium: 50-75%
	Warning (potential performance implications)	High: >75%

Over time, if channel utilization is consistently high on a given channel, this may indicate a need for improved AP channel assignments.

Status information Click a specific channel to display the following information:

- **Utilization per AP** The minimum, average, and maximum percentage are displayed.
- **Clients per AP** The minimum, average, and maximum number of clients are displayed.

Devices on 5 GHz Radio Band

The 5 GHz Channel Occupancy Chart displays the channel use of the 5 GHz band on a per-AP basis.

Note: At least one 5 GHz UniFi AP must be active to enable this chart.

(Channels) Each AP is represented by a square icon, which is located in the channel to which the AP is currently assigned. The gray peak associated with each channel indicates the relative percentage of channel utilization on each assigned channel.

The color of the square icon indicates the percentage of channel utilization on each AP assigned to the displayed channel:

Color	Status	Percentage of Utilization
	Ideal	Low: <50%
	Acceptable	Medium: 50-75%
	Warning (potential performance implications)	High: >75%

Over time, if channel utilization is consistently high on a given channel, this may indicate a need for improved AP channel assignments.

Status information Click a specific channel to display the following information:

- **Utilization per AP** The minimum, average, and maximum percentage are displayed.
- **Clients per AP** The minimum, average, and maximum number of clients are displayed.

Clients on 2.4 GHz Radio Band

Click **Clients** above the Channel Occupancy Charts to display the number of clients on each specific channel.

Note: At least one 2.4 GHz UniFi AP must be active to enable this chart.

1-11 Each client is represented by a circular icon, which is located in the channel it is using. The gray peak associated with each channel indicates the relative amount of traffic.

The color of the circular icon represents the quality of the RX rate associated with the client. This indicates the quality of the connection between the client and AP:

Color	Status	RX Rate
●	Ideal	High: > 40 Mbps
●	Acceptable	Medium: < 40 Mbps
●	Warning (poor performance with this client)	Low: < 10 Mbps

Over time, if client rates are consistently poor, this may indicate a need for greater or improved coverage, or may help identify clients experiencing issues.

Status information Click a specific channel to display the following information:

- **RX Rate per Client** The minimum, average, and maximum RX rates are displayed.
- **TX Rate per Client** The minimum, average, and maximum TX rates are displayed.

Clients on 5 GHz Radio Band

Click **Clients** above the Channel Occupancy Charts to display the number of clients on each specific channel.

Note: At least one 5 GHz UniFi AP must be active to enable this chart.

(Channels) Each client is represented by a circular icon, which is located in the channel it is using. The gray peak associated with each channel indicates the relative amount of traffic.

The color of the circular icon represents the quality of the RX rate associated with the client. This indicates the quality of the connection between the client and AP:

Color	Status	RX Rate
●	Ideal	High: > 40 Mbps
●	Acceptable	Medium: < 40 Mbps
●	Warning (poor performance with this client)	Low: < 10 Mbps

Over time, if client rates are consistently poor, this may indicate a need for greater or improved coverage, or may help identify clients experiencing issues.

Status information Click a specific channel to display the following information:

- **RX Rate per Client** The minimum, average, and maximum RX rates are displayed.
- **TX Rate per Client** The minimum, average, and maximum TX rates are displayed.

Devices

UniFi devices are displayed.

Traffic Displays the total number of devices and a color-coded breakdown of the device types.

WLAN Displays the number of wireless devices.

LAN Displays the number of wired devices.

WAN Displays the number of gateway devices.

Status information Click a specific device category to display the device models and their quantities.

Clients

Network clients are displayed.

Note: The DPI feature must be enabled to display client information.

Traffic Displays the total number of devices and a color-coded breakdown of the device types.

Ubiquiti Displays the number of Ubiquiti clients.

(Various) Displays the number of clients that belong in each of the remaining client categories.

Other Displays the number of clients that don't belong in the aforementioned categories.

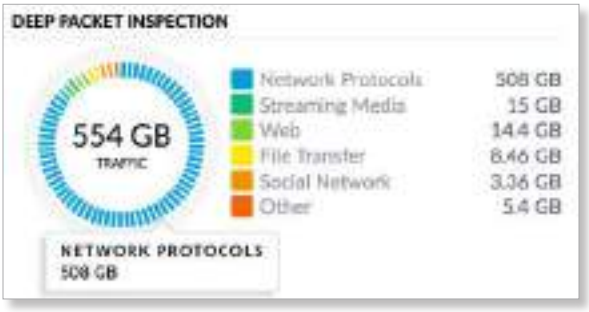
Status information Click a specific client category to display the client category name.

Deep Packet Inspection

Deep Packet Inspection (DPI) is more advanced than conventional Stateful Packet Inspection (SPI) filtering for traffic analysis. Ubiquiti's proprietary DPI engine includes the latest application identification signatures to track which applications (and IP addresses) are using the most bandwidth.

The DPI feature requires the following:

- A UniFi Security Gateway must be active to enable this feature.
- DPI must be enabled on the *Settings* > *Site* screen. See **"Settings > Site" on page 21** for more information.



Traffic Displays the total amount of traffic and a color-coded breakdown of the traffic types.

Network Protocols Displays the amount of data that is identified as network protocol traffic.

Streaming Media Displays the amount of data that is identified as streaming media.

Web Displays the amount of data that is identified as web-related traffic.

File Transfer Displays the amount of data that is identified as files being transferred.

Social Network Displays the amount of data that is identified as social networking traffic.

Other Displays the amount of data that doesn't belong in the aforementioned categories.

Status information Click a specific traffic category to display the traffic category name and amount of data.

Dynamic Dashboard (beta)

You can enable the *Dynamic Dashboard (beta)* setting using your account preferences. For more information, go to **"Username" on page 18**.

Once *Dynamic Dashboard (beta)* is enabled, then you can customize the *Dashboard* display. You can move, add, or remove the sections of the display. (Each section uses a widget for its status information.)

Unlock The *Dashboard* is locked by default. Click UNLOCK to unlock the display.

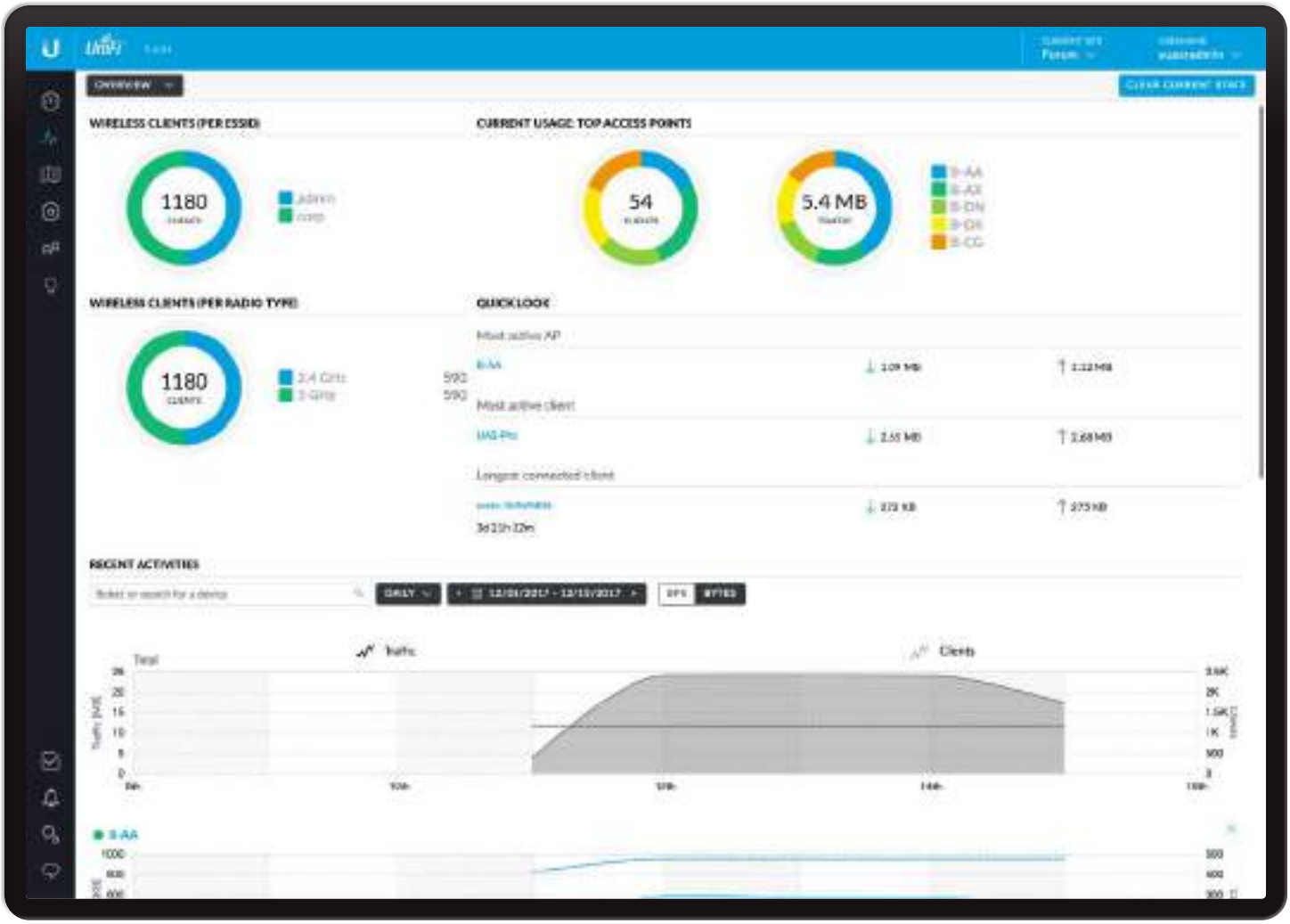
Once unlocked, you can click ✕ to remove a widget or click ✥ to move a widget.

Reset You can reset the *Dashboard* to its factory default settings. Click RESET.

Add Widget You can add widgets back to the display. Click ADD WIDGET.

- **Select widget** Select the widget you want to add.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Lock Once you are finished with your changes, click LOCK to save your display options.



Chapter 5: Statistics

The *Statistics* screen provides a visual representation of the clients and network traffic connected to your managed UniFi network.

Here are the available options:

- **Overview** The default view describes the wireless clients and network traffic. Please refer to the next column for more information.
- **Traffic Stats** (Available if you have a UniFi Security Gateway with the *DPI* feature enabled.) The *Traffic Stats* screen describes the network traffic by category, application, and client usage. Go to **"Traffic Stats" on page 73** for more information.
- **Performance** The *Performance* screen describes the device performance by CPU and memory usage, traffic, packets, dropped packets, and errors. Go to **"Performance" on page 76** for more information.
- **Switch Stats** The *Switch Stats* screen describes the ports and port traffic. Go to **"Switch Stats" on page 77** for more information.
- **Speed Test Stats** The *Speed Test Stats* screen describes the speed test results. Go to **"Speed Test Stats" on page 78** for more information.
- **Debugging Metrics** This beta offers wireless device and client statistics for debugging. Go to **"Debugging Metrics" on page 78** for more information.

Overview

The *Overview* screen describes the usage by wireless clients and UniFi Access Points.

Clear Current Stats Reset the current statistics to start over.

Wireless Clients (Per ESSID)

# of Clients A visual pie chart represents the client distribution amongst the wireless networks (SSIDs). Click the chart for the number of clients per network.

Wireless Clients (Per Radio Type)

# of Clients A visual pie chart represents the client distribution between the radio bands. Click the chart for the number of clients per band.

Current Usage: Top Access Points

The details of the most active Access Points in current use are displayed.

# of Clients A pie chart represents the client distribution on the most active Access Points. Click the chart for the number of clients per specified AP.

Traffic A pie chart represents traffic on the most active Access Points. Click the chart for the amount of traffic per specified AP.

Quick Look

Most Active AP

The details of the most active Access Point are displayed:

Name or MAC address You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

Download Displays the total amount of data downloaded by the AP.

Upload Displays the total amount of data uploaded by the AP.

Most Active Client

The details of the most active client in current use are displayed:

Name or MAC address You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.

Download Displays the total amount of data downloaded by the client.

Upload Displays the total amount of data uploaded by the client.

Longest Connected Client

The details of the client connected for the longest period of time are displayed:

Name or MAC address You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.

Uptime Displays the duration of time the client has been connected.

Download Displays the total amount of data downloaded by the client.

Upload Displays the total amount of data uploaded by the client.

Recent Activities

The details of recent network activities are displayed.

Recent Activities 

You can view the number of clients and amount of traffic by UniFi AP. The drop-down list displays managed UniFi APs by name or MAC address. Select the appropriate AP or enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(daily) The default view. Select **5 minutes**, **hourly**, or **daily** to change the duration interval.

Date Click either arrow to change the date in one-day increments.

Click the date to display the calendar.

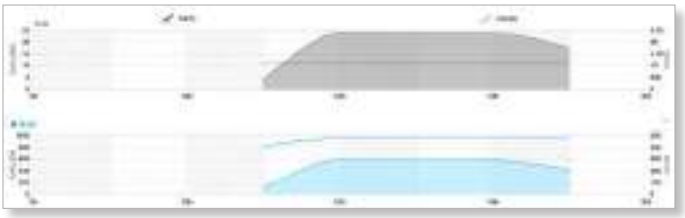
- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

(bytes) The default view. Select **bps** to change the unit of measurement.

The top graph displays the total number of clients and amount of data for all APs.

Clients In the graph, a dashed line displays the number of clients connected during the selected time period. Click a point on the line to display the exact number.

Traffic In the graph, a solid line displays the network traffic during the selected time period. Click a point on the line to display the specific amount of data.



When you select an AP, an additional graph that is color-coded to the selected AP appears. (You can select multiple APs for filtering.)

You can click ✕ to remove an AP from display.

Traffic Stats

(Available if you have a UniFi Security Gateway with the *DPI* feature enabled. Go to **"Settings > Site" on page 21** for more information.) The *Traffic Stats* screen describes the network traffic by application usage.

Deep Packet Inspection (DPI) is more advanced than conventional Stateful Packet Inspection (SPI) filtering for traffic analysis. Ubiquiti's proprietary DPI engine includes the latest application identification signatures to track which applications (and IP addresses) are using the most bandwidth.

Clear Categories Reset the category listings. To reset the statistics to start over, go to the *Settings > DPI* screen and click **Clear CPI Counters**. For more information go to **"Settings > DPI" on page 55**.

Applications are organized by category, such as Network Protocols, Streaming Media, Web, File Transfer, and Social Network. The total amount of traffic is broken down by category.

Amount of Traffic A pie chart represents the traffic distribution by the most popular categories. Click the chart for the amount of traffic per category.

A list displays a comprehensive breakdown of the traffic by category. You can click any category to have it displayed with a detailed breakdown of the application usage within that category.

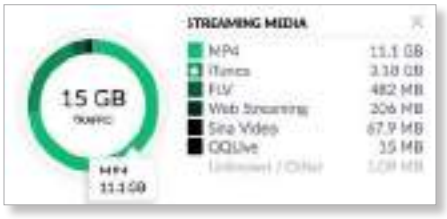
There are three views available: Overview, Apps, and Users.

Overview

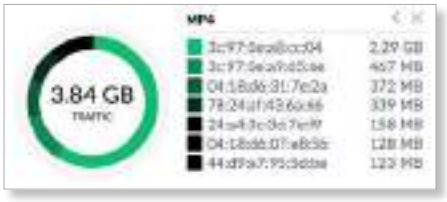
The most popular categories are displayed with the amount of traffic broken down further by application.

Amount of Traffic A pie chart represents the traffic distribution by the most popular applications. Click the chart for the amount of traffic per application.

A list displays a comprehensive breakdown of the traffic by application.



Click a specific application to display a list of clients.

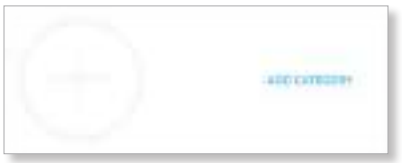


You can click ✕ to remove a category from display.

Add Category

To add a new category for display, follow these steps:

1. Click **Add Category** or the + sign.



2. Select a category. You can also enter a keyword in the *Filter* field; simply begin typing; there is no need to press *Enter*.

3. Click **Save**.

Apps

The most popular applications are displayed.

(icon) Displays the representative icon, if applicable.

App Name Displays the name or description.

Up Displays the total amount of data uploaded by the app.

Down Displays the total amount of data downloaded by the app.

Active Users Displays the number of users currently using the app.

Click any app to display the amount of traffic broken down further by client.

Clear Applications Reset the current statistics to start over.

(amount of traffic) A pie chart represents the traffic distribution by the relevant applications. Click the chart for the specific amount of traffic per application.

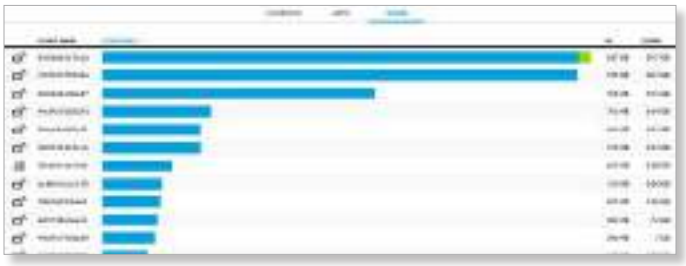
A list displays a comprehensive breakdown of the application traffic by client.

- **Client Name** You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.
- **Applications** The bar graph displays the percentage of the app traffic generated by the client. Click to display additional statistics:
  - **Up Pkts/Bytes** Displays the number of packets and bytes uploaded.
  - **Down Pkts/Bytes** Displays the number of packets and bytes downloaded.

- **Up** Displays the total amount of data uploaded by the app for this client.
- **Down** Displays the total amount of data downloaded by the app for this client.

Users

The users are displayed with the amount of traffic broken down further by category.



(icon) The client device icon is displayed if available.

Client Name You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.

Categories The bar graph displays the percentage of the traffic per category generated by the client. Click to display additional statistics:

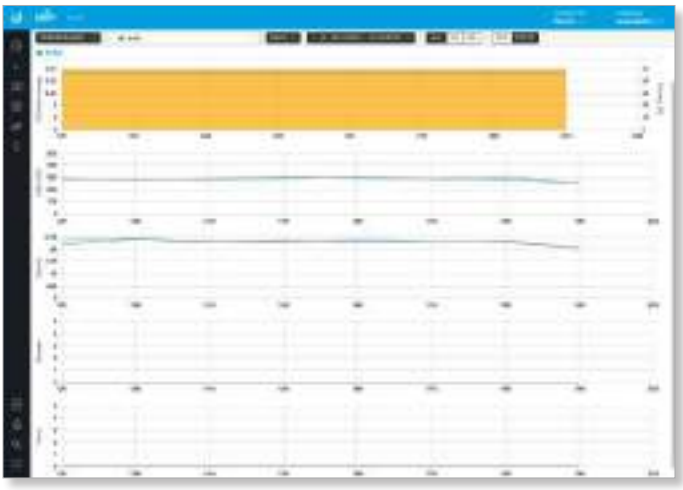
- **Up Pkts/Bytes** Displays the number of packets and bytes uploaded.
- **Down Pkts/Bytes** Displays the number of packets and bytes downloaded.

Up Displays the total amount of data uploaded by the user for this app.

Down Displays the total amount of data downloaded by the user for this app.

Performance

The *Performance* screen describes the device performance by CPU and memory usage, traffic, packets, dropped packets, and errors.



(device) 

You can view the performance statistics by device. The drop-down list displays managed UniFi devices by name or MAC address. Select the appropriate device or enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(daily) The default view. Select **5 minutes**, **hourly**, or **daily** to change the duration interval.

Date Click either arrow to change the date in one-day increments.

Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

Additional display options will vary depending on the device type:

- **Gateway** Click the port whose statistics you want to view: **LAN 1**, **LAN 2**, **WAN 1**, or **WAN 2**.
- **SW** You can select the **Switch Stats** option for more information.
- **AP** You have two options:
  - **(radio band)** Select the radio band you want to view: **All**, **5G**, or **2G**.
  - **(bytes)** The default view. Select **bps** to change the unit of measurement.

Multiple color-coded graphs are displayed. Click a point on the line to display the specific values.

CPU and Memory

CPU Load Average The graph displays the average load on the CPU during the selected time period.

Memory (%) The graph displays the percentage of memory used during the selected time period.

Traffic

Received A solid green line displays the bytes of data received.

Transmitted A solid purple line displays the bytes of data transmitted.

Packets

Received A solid green line displays the number of packets received.

Transmitted A solid purple line displays the number of packets transmitted.

Dropped

Received A solid green line displays the number of receive packets dropped.

Transmitted A solid purple line displays the number of transmit packets dropped.

Errors

Received A solid green line displays the number of receive errors.

Transmitted A solid purple line displays the number of transmit errors.

Switch Stats

The *Performance* screen describes the ports and port traffic of the selected UniFi Switch.

(device) 

You can view the ports and their traffic by UniFi Switch. The drop-down list displays managed UniFi Switches by name or MAC address. Select the appropriate switch or enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(daily) The default view. Select **5 minutes**, **hourly**, or **daily** to change the duration interval.

Date Click either arrow to change the date in one-day increments.

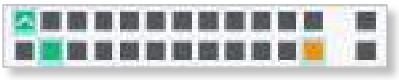
Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

Additional display options are available:

- **Sort** Click the appropriate sort order: **Natural** (numerical port order), **Transmitted**, **Received**, or **Total**.
- **(bps)** The default view. Select **bytes** or **packets** to change the unit of measurement.

The upper part of the detached popup screen has an icon for each port.



Indicates a 10/100 Mbps connection.

Indicates a 1 Gbps (1000 Mbps) connection.

Indicates a 10 Gbps connection.

Indicates 1 Gbps (1000 Mbps) connection with PoE.

Indicates the connection is disabled (no network or VLAN is enabled).

Indicates no connection (the network or VLAN is enabled, but the port is not in use).

Indicates STP blocking.

Indicates mirroring mode.

Indicates an uplink.

Place your cursor over a port to view details.

- **Port** Displays the port number.
- **Name** Displays the name of the port.
- **Status** Displays the connection speed and duplex mode.
- **TX** Displays the amount of data transmitted.
- **RX** Displays the amount of data received.
- **Profile** Displays the Switch Port profile assigned to it. Switch Port profiles are configured in *Settings* > **"Switch Ports" on page 46**.

Click an active port to display its color-coded graph. Click a point on the line to display the specific values.

Port

Received A solid green line displays the bytes of data received.

Transmitted A solid purple line displays the bytes of data transmitted.

Speed Test Stats

The *Speed Test Stats* screen describes the speed test results.

Date Click either arrow to change the date in one-day increments.

Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

Two color-coded graphs are displayed. Click a point on the line to display the specific values.

Latency

Latency Displays the amount of time it takes a packet to travel from the UniFi Security Gateway to the service provider's gateway.

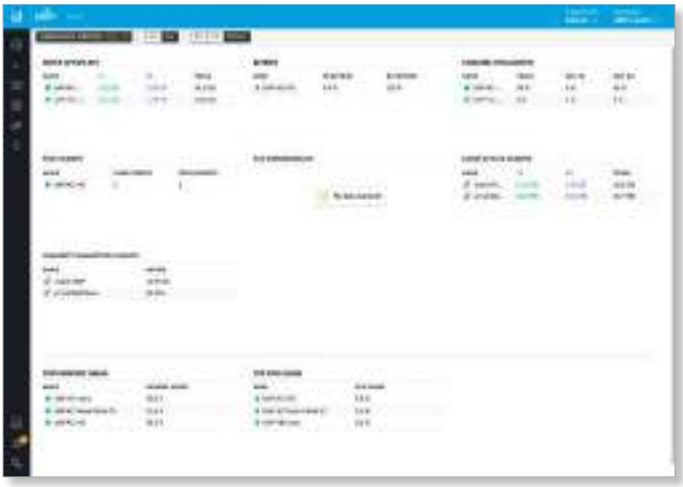
Speed

Download Displays the download speed.

Upload Displays the upload speed.

Debugging Metrics

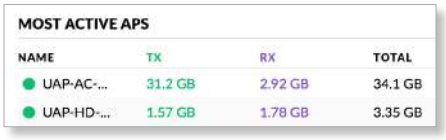
The beta *Debugging Metrics* screen offers statistics about your wireless devices and clients.



2G/5G Select the radio band whose statistics you want to view.

RX/TX/Total Select the type of data you want to view: **RX** (receive), **TX** (transmit), or **Total** (all data).

Most Active APs



Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

TX Displays the amount of data transmitted using the selected radio band.

RX Displays the amount of data received using the selected radio band.

Total Displays the amount of data transmitted and received using the selected radio band.

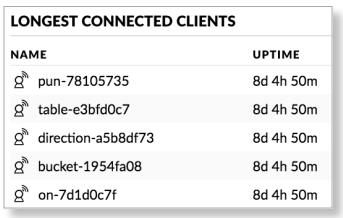
Top Clients

Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

_ GHz Clients Displays the number of clients using the selected radio band.

Total Clients Displays the total number of clients.

Longest Connected Clients



Name You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.

Uptime Displays the duration of time the client has been connected.

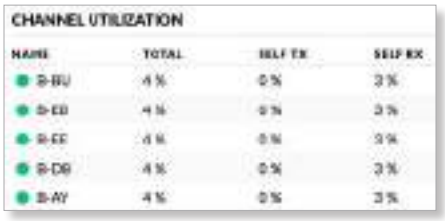
Retries

Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

TX Retries Displays the percentage of data transmitted that is comprised of retries.

RX Retries Displays the percentage of data received that is comprised of retries.

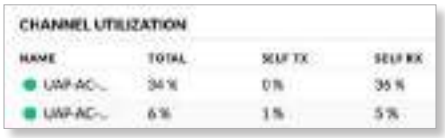
Top Interference



Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

Interference Displays the percentage of interference experienced by the AP.

Channel Utilization



Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

Total Displays the total percentage of the channel that is being used.

Self TX Displays the percentage of the channel that is being used by the AP for transmitting data.

Self RX Displays the percentage of the channel that is being used by the AP for receiving data.

Most Active Clients

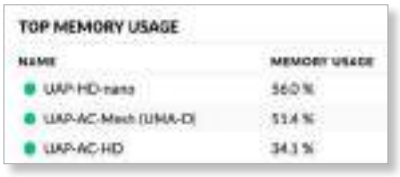
Name You can click this link to open the *Client Details* screen. See **"Client Details" on page 147** for additional information.

TX Displays the amount of data transmitted using the selected radio band.

RX Displays the amount of data received using the selected radio band.

Total Displays the amount of data transmitted and received using the selected radio band.

Top Memory Usage



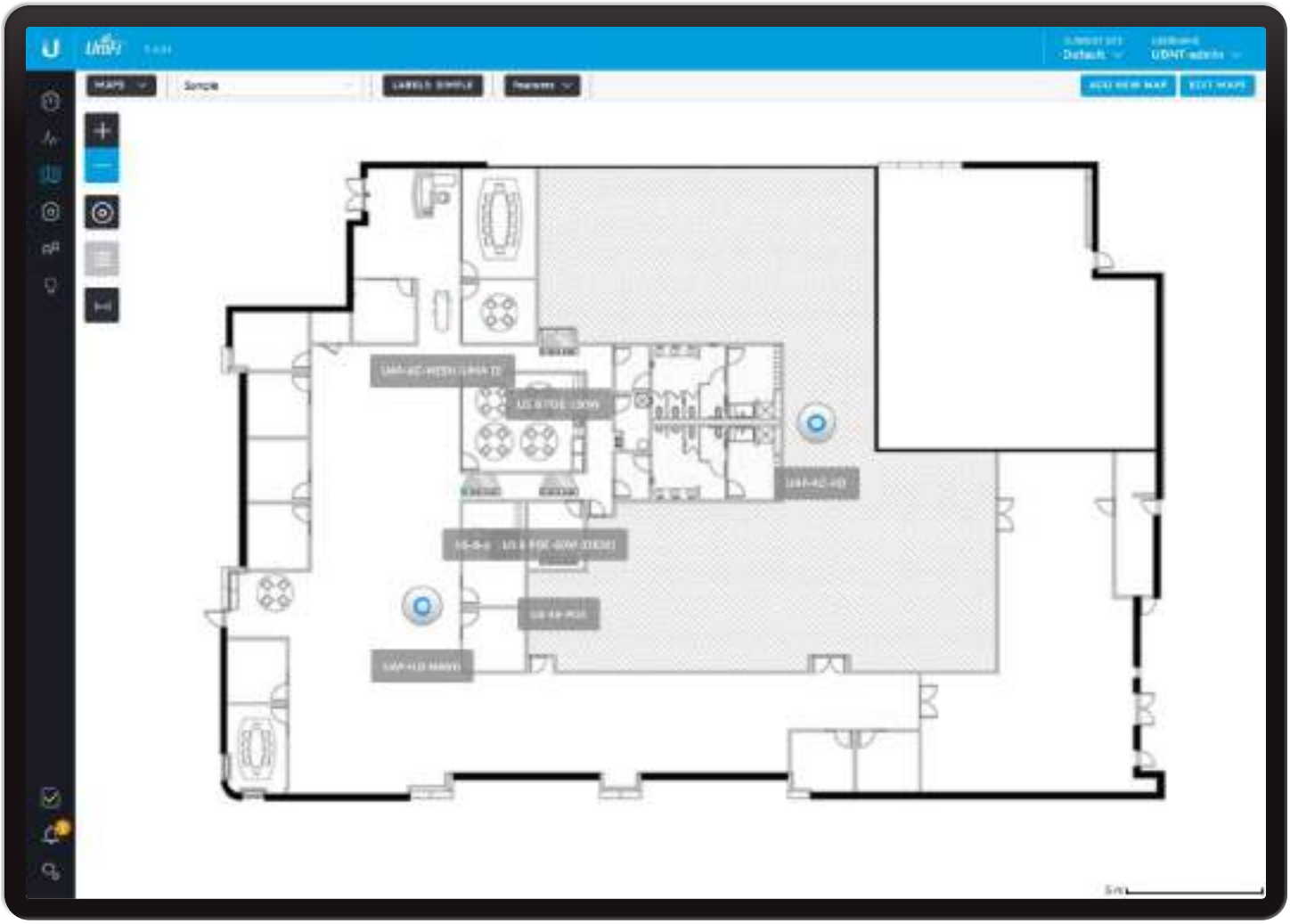
Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

Memory Usage Displays the percentage of device memory being used.

Top CPU Usage

Name You can click this link to open the *AP Details* screen. See **"UniFi Access Point Details" on page 131** for additional information.

CPU Usage Displays the percentage of CPU processing power being used.



Chapter 6: Map

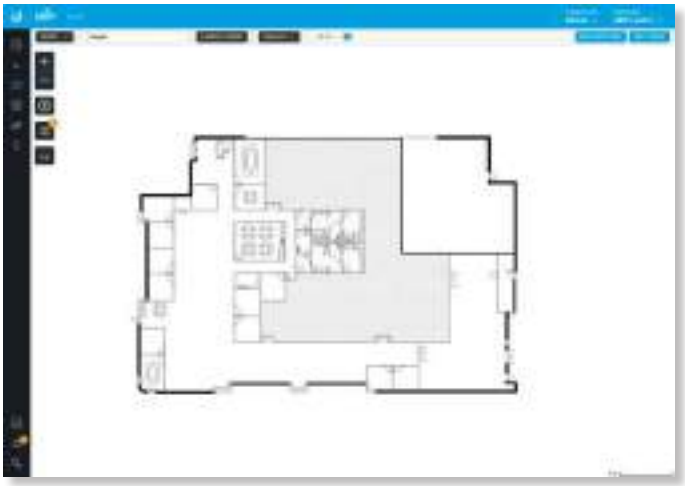
The *Map* screen allows you to upload custom map images of your location(s) or use Google Maps™ for a visual representation of your UniFi network. You can also view the system topology. When you initially launch the UniFi Controller application, a default map is displayed. The map scale is shown in the legend at the bottom of the map.

Adding Custom Maps

To add a custom map, you must first create the image using an illustration, image editing, or blueprint application that exports a file in .jpg, .gif, or .png file format.

Once you've created the map, you can upload it to the UniFi Controller software:

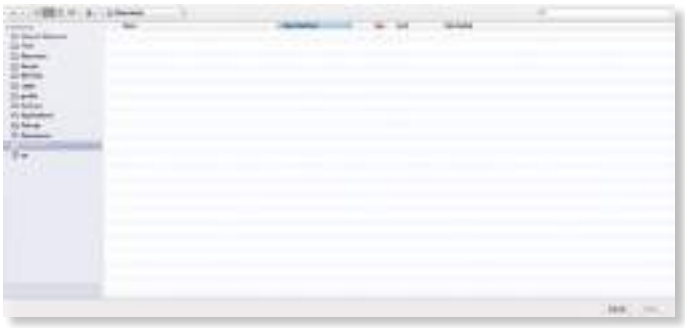
1. Click **Add New Map.**



2. The default is *Google Maps*. Click **Image**.

3. Click **Choose Map Image**.

4. Locate the file to use as a map (valid file formats are .jpg, .gif, and .png) and then click **Open**. If you do not want to upload a file, click *Cancel*.



5. Enter a map name in the field provided.

   Select **Keep placed devices** if you want to keep them on the image you uploaded.

   Keep **Optimize image enabled** if you want the UniFi Controller to automatically reduce the size of a large image for better performance.

   Note: If the map is incorrect, click **Select a different map** and try again.

6. There are two tabs available, *Designer* (default) and *Legacy*.
   - **Designer** You have these features: predictive coverage, 2D or 3D views, solid or heatmap views, and the capability to add walls.
   - **Legacy** You can filter by radio band and display coverage and topology.

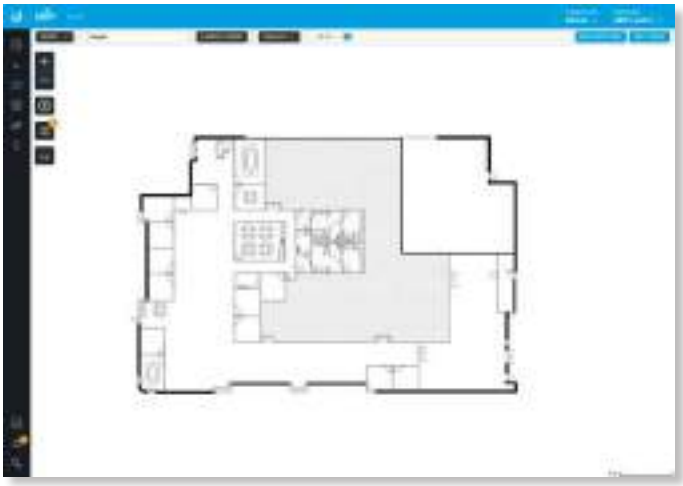
   Click **Save.**

7. Click **Done**.

Adding a Google Map

To add a *Google Map* to the UniFi Controller software *Map* view:

1. Click **Add New Map**.



2. The default is *Google Maps*.

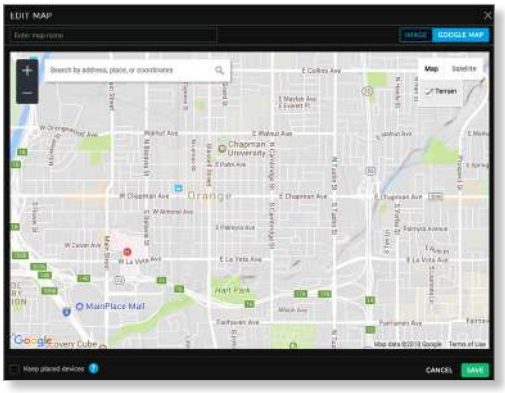
3. If Google Maps is not enabled yet, then enable this feature by following the provided guide on how to obtain a valid Google Maps API key:

   https://developers.google.com/maps/documentation/javascript/get-api-key#get-an-api-key

4. Go to the *Settings* > *Controller* section and enter the API key. Check the box to enable *Use Google Maps engine for Image maps*. (For more information, go to **"Maps Setting" on page 56**.) Click **Apply Changes**.

5. The default view is *Map* view, which looks like a street map. Click **Terrain** to display enhanced geographical details.

Map View



Terrain View

Use the tools to navigate the map or adjust the zoom using the *zoom* control.

In the field provided, enter an address or the latitude and longitude of a specific location. Then press **Enter** or **Return**.

You can also click *Satellite* for a bird's-eye view. Click **Labels** to display street and location names.

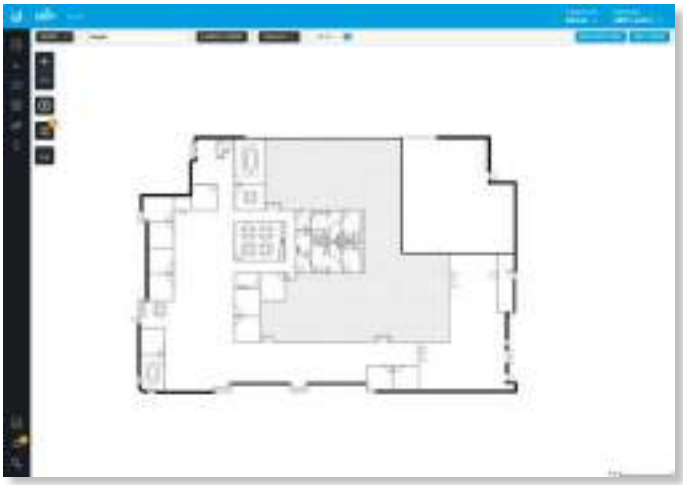
Enter a map name in the field provided and click **Save**.

6. Click **Done**.

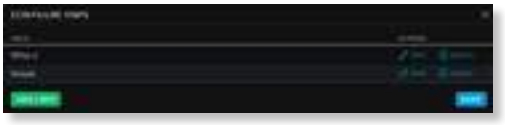
Editing a Map

You can edit or delete a map.

1. Click **Edit Maps**.



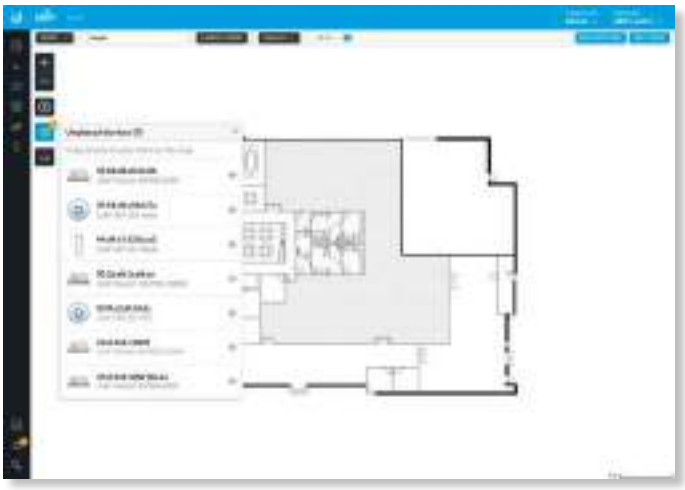
2. There is a list of existing maps.
   - **Edit** Click EDIT to make changes.
   - **Delete** Click DELETE to remove the map.



Placing Devices on the Map

1. Click at the lower left.
2. Drag each device icon from the *Unplaced Devices* list to the appropriate location on the map.

Note: If you cannot drag and drop a device, ensure that you are logged in as a superadmin.



Each device icon will appear in the area where you placed it.

Once all devices have been placed the icon changes from black to gray.

Device Information

Status

The device icon indicates the UniFi model (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro/HD/SHD
- UniFi AP AC EDU
- UniFi AP AC Mesh
- UniFi AP AC Mesh Pro
- UniFi AP In-Wall/AP AC In-Wall
- UniFi AP/AP LR
- UniFi AP AC
- UniFi AP AC Outdoor
- UniFi AP Outdoor+
- UniFi AP Outdoor5
- UniFi Security Gateway
- UniFi Security Gateway Pro
- UniFi 24-Port Switch
- UniFi 48-Port Switch

The LED color of the icon indicates the device status.

- **Blue/Green** Indicates the device is connected.
- **Red/Orange** Indicates the device is disconnected. A *disconnected* icon also marks the device icon.

Device Options

Click a UniFi icon to reveal options. Click the UniFi icon again to hide them.

- **Lock** Lock the device icon to its current location.
- **Details** Display the *Details* screen. For more information, go to the appropriate chapter:
  - **"UniFi Security Gateway Details" on page 115**
  - **"UniFi Switch Details" on page 121**
  - **"UniFi Access Point Details" on page 131**
- **Statistics** (Available for the second and third generation UniFi AC APs only.) Displays the *RF Environment* screen. For more information, go to **"RF Environment" on page 141**.
- **Remove** Remove the device icon from its location.

Map Display Options

(Map) If multiple maps have been uploaded, you can select which map you want from the drop-down list or search for keywords. There is no need to press Enter; simply start typing.

Labels

Each device can be displayed with its name. If no custom label is applied, the device's MAC address will be displayed.

Click this button to cycle between the following options for label display:

None Do not display device labels.

Simple Display simple device labels containing the device name only.

Detailed Display detailed device labels containing the following information: device name, MAC address, transmit/receive channel(s), number of users connected, and number of guests connected.

To change a name applied to a device, refer to *Alias* in the appropriate section:

- **"UniFi Security Gateway – Configuration" on page 117**
- **"UniFi Switch – Configuration" on page 127**
- **"UniFi Access Point – Configuration" on page 135**

Features

You have multiple display options available, some of which vary depending on the Designer/Legacy option:

Legacy

Designer

Filter Devices

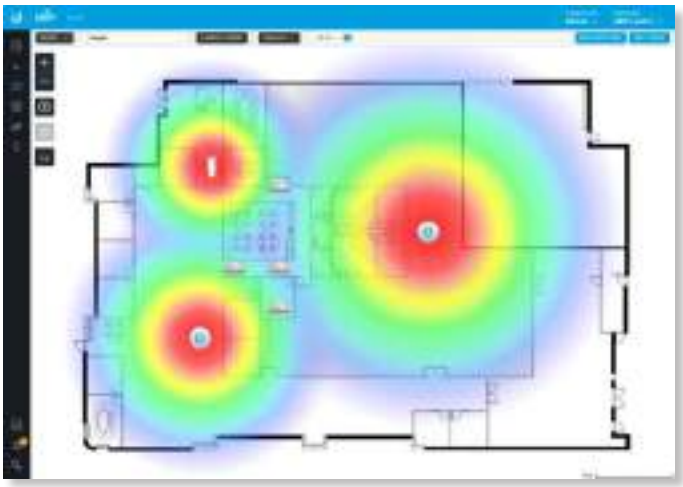
2G Devices Displays the 2.4 GHz devices.

5G Devices Displays the 5 GHz devices.

Layers

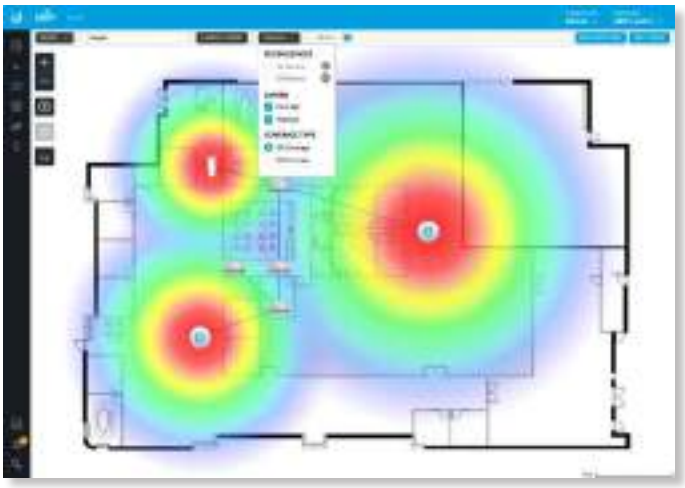
Coverage Displays a visual representation of the wireless range covered by any APs.

- **__ dBm** You can change the receiver sensitivity value for more accurate coverage results. The default is *-90* dBm.



Precision (Designer option only) To fine-tune the predictive coverage, select a dBm value from the drop-down list: **0.1 dBm**, **0.5 dBm**, **1 dBm**, **2 dBm**, or **4 dBm**.

Topology (Legacy option only.) Displays a visual representation of the network configuration and connections between any APs. A dashed line will indicate the wirelessly connected AP and its uplink to a wired AP, even if the wirelessly connected AP is isolated.



Coverage Type

If *Coverage* is enabled, you have the following options:

2G Coverage Displays the coverage by 2.4 GHz devices.

5G Coverage Displays the coverage by 5 GHz devices.

Performance

(Available for Designer option) If *Performance* is enabled, you have the following option:

Live Update Automatically updates in real time.

Scheme

(Available for Designer option) If *Scheme* is enabled, you have the following options:

Solid Displays the coverage as solid colors.

Heatmap Displays the coverage as a heatmap.

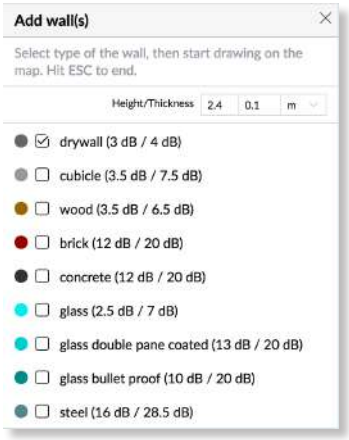
Additional Options

The left side of the map offers the following options:

- **Zoom Slider** Use to zoom the map detail in and out.
- **Devices** (Legacy option only.) Click to toggle the size of devices and their labels between small and large.
- **2D/3D** (Designer option only.) Click to toggle between two- and three-dimensional views of the devices and walls.
- **Unplaced Devices** Drag each device icon from the list to the appropriate location on the map. (This option may require superadmin access.)
- **Move** (Designer option only.) Click to move placed devices or the map.
- **Draw Walls** (Designer option only.) Use this option to select the type of wall and then draw it on the image. Press **ESC** to end the wall.
- **Set Map Scale** Use this option to define the scale of the map. You will draw a line and define the distance that the line represents.

Drawing Walls

1. Click the *draw walls* button.
2. Select the type of wall you want to draw. You can change the default height and thickness values in the fields provided. By default they are specified in meters but you can switch to feet using the drop-down menu on the right.



3. Draw the wall and press **ESC** to end the wall.

4. You can select a different type of wall and add it to the map.

After you have added the UniFi APs, the interference caused by the walls will be predicted and displayed in both the *Solid* and *Heatmap* views.

Setting the Map Scale

1. Click the *set map scale* button.
2. Click and hold to draw a line in the area that you want to use to set the scale of the map. If you need to redraw the line, just click and hold again to draw a new line.

3. Enter the distance that the line represents in the *Distance* field. By default, the distance is specified in meters but you can switch to feet using the drop-down menu on the right. Click **Set Scale**.

The legend at the bottom of the map shows the new scale of the map.

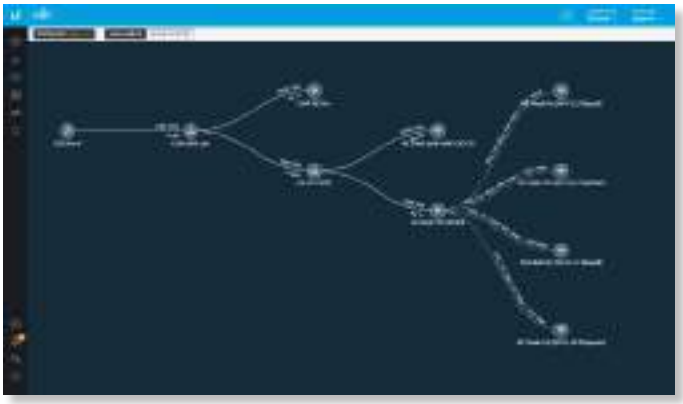
System Topology

1. Click MAPS, and then select **Topology** from the drop-down menu.
2. The UniFi Controller displays a topology diagram of your UniFi system.

   The default view shows the entire topology tree, except for client devices. Click any node to collapse the branches below (to the right of) that node. Clicking the root node collapses the entire tree.

3. Click **Show Clients** to display client devices.

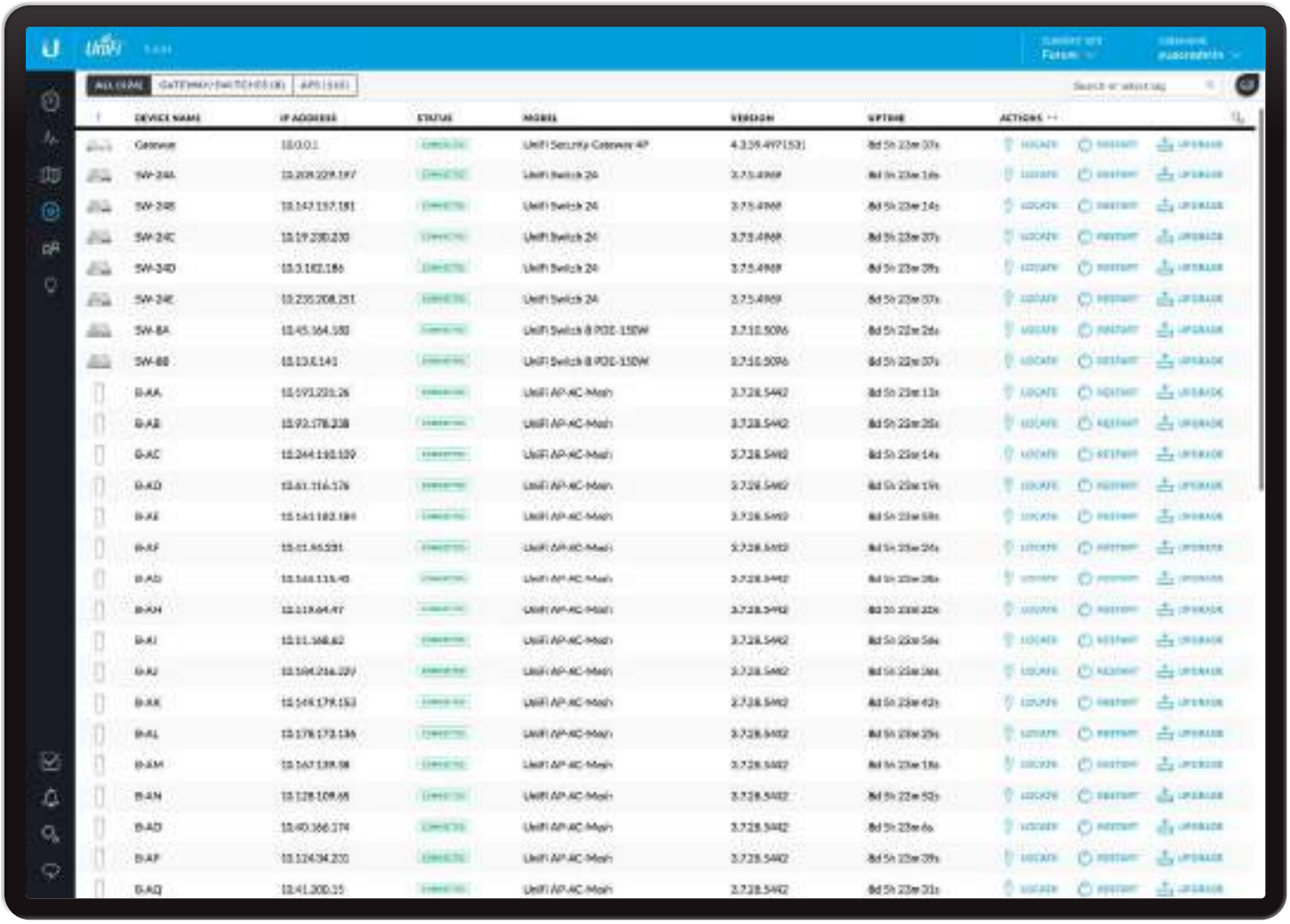
4. Click **Link Labels** to display labels on each link:



The labels provide the following information:

- Wired links
  - Data rate in Mbps
  - Duplex type: *FDX* for full duplex, *HDX* for half duplex
  - Port number to which the device is connected
- Wireless links
  - RSSI expressed as a percentage
  - RSSI displayed in dBm

  Note: The displayed RSSI value is from the AP side of the link; i.e., it is how the AP hears the client.
- Negotiation Rate (__ Mbps / __ Mbps)



Chapter 7: Devices

The *Devices* screen displays a list of UniFi devices discovered by the UniFi Controller. You can click any of the column headers to change the list order.

You can apply one of the following primary filters:

- **All** Displays all UniFi devices.
- **Gateway/Switches** Displays all UniFi Security Gateways and Switches.
- **APs** Displays all UniFi APs.

If the *APs* filter is applied, then another filter is available (unless columns have been customized):

- **Overview** Displays the number of clients, amount of data downloaded, amount of data uploaded, and channel setting.
- **Performance** Displays the number of 2.4 GHz and 5 GHz clients, overall transmit rate, overall receive rate, transmit rates in the 2.4 GHz and 5 GHz radio bands, and channel setting.
- **Config** Displays the WLAN and radio settings for the 2.4 GHz and 5 GHz radio bands.

Items per page Select how many results are displayed per page: **10**, **25**, **50**, or **100**.

If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

Search Search or select tag Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*. You can also select a device tag (configured in the *Configuration* section of a device).

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

The icon column sorts by state, and for connected devices it also sorts by device type. This is the order:

- Connected Gateway
- Connected Switch
- Connected AP
- Any device that is being upgraded or provisioned
- Any device that is being adopted or is restarting
- Any device that is pending
- Any device that is disconnected or in an error state

After this sorting is applied, the sort order uses alphabetical order according to the device name.

Settings To enable group or batch configuration or customize the column layout, click this option.

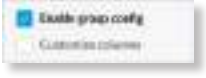
- **Enable Group Config (Switch)** Use this feature to configure an entire group of UniFi Switches at the same time. The following settings can be changed with batch configuration:
  - Enable/disable LED
  - Management VLAN
  - Jumbo Frame
  - Flow Control
  - Spanning Tree
  - Priority
  - 802.1X Control
  - Custom Upgrade
  - Force Provision
  - Forget These Devices

  To configure a group of switches, click and then select **Enable group config**.

  For more information, go to **"Group Configuration" on page 92**.

- **Enable Group Config (AP)** Use this feature to configure an entire group of UniFi APs at the same time. The following AP settings can be changed with batch configuration:
  - Enable/disable LED
  - Radio Channel
  - Radio Channel Width
  - Radio Transmit Power
  - WLAN Groups
  - Custom Upgrade
  - Force Provision
  - Disable These Devices
  - Forget These Devices

  To configure a group of APs, click and then select **Enable group config**.



  For detailed instructions and information on AP group configuration, refer to the following online help article: **ubnt.link/UniFi-AP-Group-Configuration**

- **Customize Columns** Each primary filter: *All*, *Gateway/Switches*, or *APs* applies a default set of columns to display. If you enable the *Customize Columns* option, then the primary filter no longer changes the columns.

  The very first time you enable the *Customize Columns* option, the UniFi Controller software will detect which columns are currently visible and remember your selection. For example:

1. Enable the *Customize Columns* option on the *APs* > *Performance* screen.
2. Disable customization.
3. Apply the *Gateway/Switches* filter.
4. Enable the *Customize Columns* option again.
5. The columns of the *APs* > *Performance* screen will be displayed.

  Click to customize the columns used for display.

  Select **Customize columns**.

  You can select additional columns for display.

  - **Reset columns to** Click the drop-down at the bottom of the *Customize columns* screen to display the *Reset columns to ...* options. The option you select will apply no matter which primary filter: *All*, *Gateway/Switches*, or *APs*, you select. This resets the columns (the UniFi Controller software will not remember your original selection).

- **Default** The *Device Name*, *IP Address*, *Status*, *Model*, *Version*, *Uptime,* and *Actions* columns are displayed.
- **Gateway/Switches** The *Device Name*, *IP Address*, *Status*, *Model*, *Version*, *Down*, *Up,* and *Actions* columns are displayed.
- **AP Overview** The *Device Name*, *IP Address*, *Status*, *Model*, *Version*, *Clients*, *Down*, *Up*, *Channel* and *Actions* columns are displayed.
- **AP Performance** The *Device Name*, *IP Address*, *Status*, *2G Clients*, *5G Clients*, *TX*, *RX*, *TX 2G*, *TX 5G*, *Channel,* and *Actions* columns are displayed.
- **AP Config** The *Device Name*, *Status*, *Version*, *WLAN2G*, *WLAN5G*, *Radio2G*, *Radio5G,* and *Actions* columns are displayed.
- **All columns** The *Device Name*, *MAC Address*, *IP Address*, *Status*, *Model*, *Version*, *Uptime*, *Mem. Usage*, *Load Avg.*, *Clients*, *Down*, *Up*, *WLAN2G*, *WLAN5G*, *Radio2G*, *Radio5G*, *2G Clients*, *5G Clients*, *TX*, *RX*, *TX 2G*, *TX 5G*, *Channel*, *Ch. Util. 2G*, *Ch. Util. 5G*, *BSSID*, and *Actions* columns are displayed.

All

All UniFi device types are displayed.

(icon) Displays the icon corresponding to the UniFi device (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro/HD/SHD
- UniFi AP AC EDU
- UniFi AP AC Mesh
- UniFi AP AC Mesh Pro
- UniFi AP In-Wall/AP AC In-Wall
- UniFi AP/AP LR
- UniFi AP AC
- UniFi AP AC Outdoor
- UniFi AP Outdoor+
- UniFi AP Outdoor5
- UniFi Security Gateway
- UniFi Security Gateway Pro
- UniFi 24-Port Switch
- UniFi 48-Port Switch

If displayed, the LED color of the device icon indicates the device status.

- **Blue/Green** Indicates the device is connected.
- **Gray** Indicates the device is pending approval.
- **Red/Orange** Indicates the device is disconnected or not managed by this site (*Pending Approval* or *Managed by Other*).

Device Name Displays the hostname, alias, or MAC address of the UniFi device. You can click the name to get additional details. For more information, see the appropriate chapter:

- **"UniFi Security Gateway Details" on page 115**
- **"UniFi Switch Details" on page 121**
- **"UniFi Access Point Details" on page 131**

IP Address Displays the IP address used by the UniFi device.

Status Indicates the device status: *Connected*, *Disconnected*, *Pending Approval*, *Adopting*, *Upgrading*, *Managed by Other*, or *Isolated* (APs only).

Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The superadmin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

Model Displays the model name of the UniFi device.

Version Displays the version number of the UniFi device's firmware.

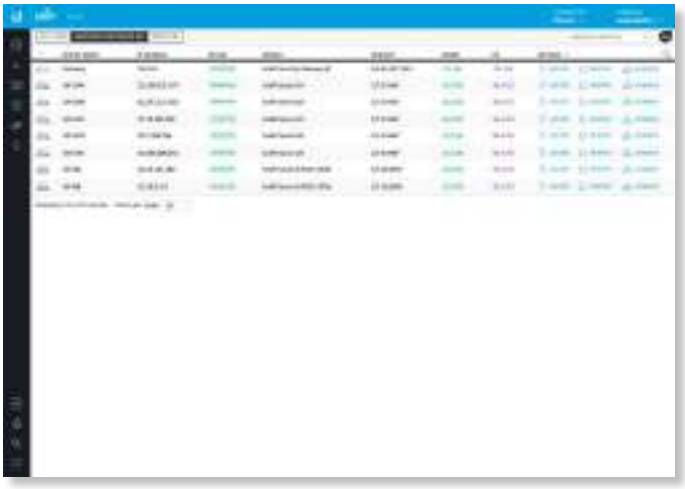
Uptime Displays the duration of time the UniFi device has been running.

Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to flash the LED on the physical device and the device's icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Restart** Click RESTART to restart the selected device.
- **Upgrade** If a software upgrade is available for the device, click UPGRADE to install the latest UniFi firmware on the device. The *Status* will appear as *Upgrading* until the process is complete and the device reconnects to the UniFi Controller software.
- **Adopt** Click ADOPT to adopt a device that appears as *Pending Approval* for its status. The *Status* will appear as *Adopting* until the device is connected.

Gateway/Switches

All UniFi Gateway and Switch devices are displayed.



(icon) Displays the icon corresponding to the UniFi device (not all icons are shown below):

- UniFi Security Gateway
- UniFi Security Gateway Pro
- UniFi 24-Port Switch
- UniFi 48-Port Switch

The LED color of the device icon indicates the device status.

- **Green** Indicates the device is connected.
- **Gray** Indicates the device is pending approval.
- **Red** Indicates the device is disconnected or not managed by this site (*Pending Approval* or *Managed by Other*).

Device Name Displays the hostname, alias, or MAC address of the UniFi device. You can click the name to get additional details. For more information, see the appropriate chapter:

- **"UniFi Security Gateway Details" on page 115**
- **"UniFi Switch Details" on page 121**

IP Address Displays the IP address used by the UniFi device.

Status Indicates the device status: *Connected*, *Disconnected*, *Pending Approval*, *Adopting*, *Upgrading*, or *Managed by Other*.

Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The superadmin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

Model Displays the model name of the UniFi device.

Version Displays the version number of the UniFi device's firmware.

Down Displays in green the total amount of data downloaded by the UniFi device.

Up Displays in purple the total amount of data uploaded by the UniFi device.

Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to flash the Status LED on the Gateway/Switch and its icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Restart** Click RESTART to restart the selected device.
- **Upgrade** If a software upgrade is available for the device, click UPGRADE to install the latest UniFi firmware on the device. The *Status* will appear as *Upgrading* until the process is complete and the device reconnects to the UniFi Controller software.
- **Adopt** Click ADOPT to adopt a device that appears as *Pending Approval* for its status. The *Status* will appear as *Adopting* until the device is connected.

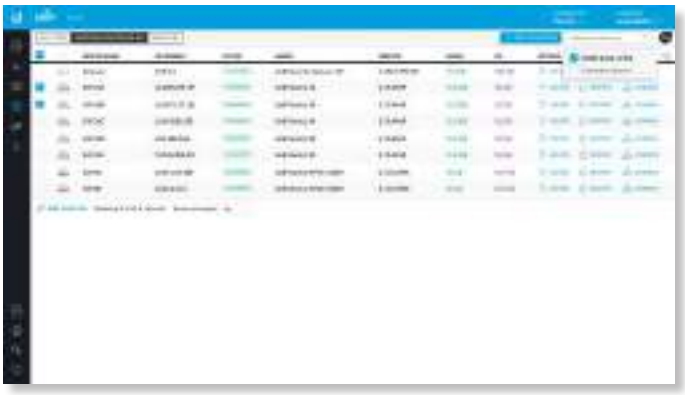
Group Configuration

To enable group or batch configuration, follow these instructions:

1. Click and then select **Enable group config**.

2. Select the appropriate switches.

3. Click EDIT SELECTED.

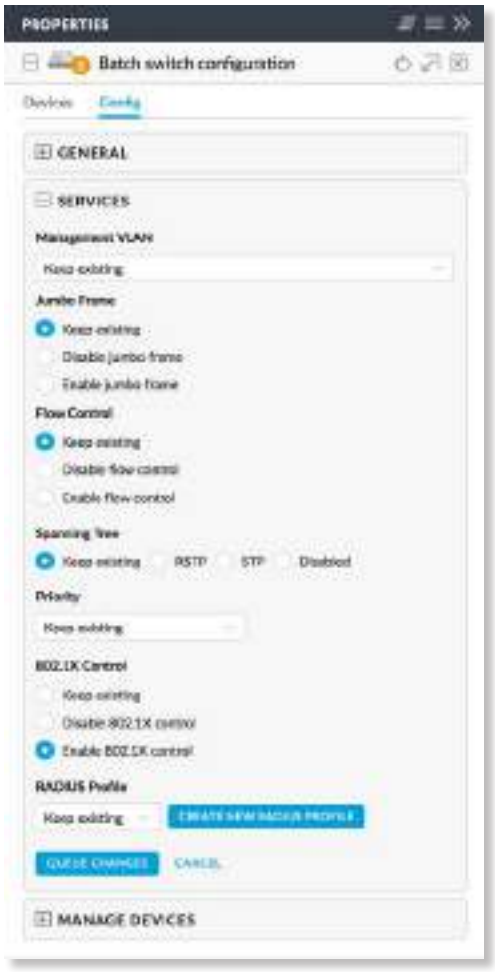


4. The *Properties* panel opens. Click the + icon to expand the appropriate section:

5. In the *General* section, make the appropriate change:

- **LED** Select **Keep existing** (behavior), **Use site settings**, **On**, or **Off**.
- **Queue Changes** Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis. When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)
- **Cancel** Click *Cancel* to discard changes.
- **Common Device Tags** Select or search for a device tag. You can also enter a keyword and press **Enter** to save a new device tag.

6. In the *Services* section, make the appropriate changes:



- **Management VLAN** The Management VLAN specifies the VLAN ID that will be used for the management IP address of the switch. The IP configuration configured under the switch's *Network* panel will be applied to this VLAN ID. The default is *Keep existing* (setting).
- **Jumbo Frame** The Maximum Transmission Unit (MTU) is the maximum packet size (in bytes) that a network interface can transmit or receive. The standard Ethernet MTU is 1500 bytes. Enable jumbo frames to allow usage of MTUs up to 9216 bytes on all ports of this switch. The default is *Keep existing* (setting).

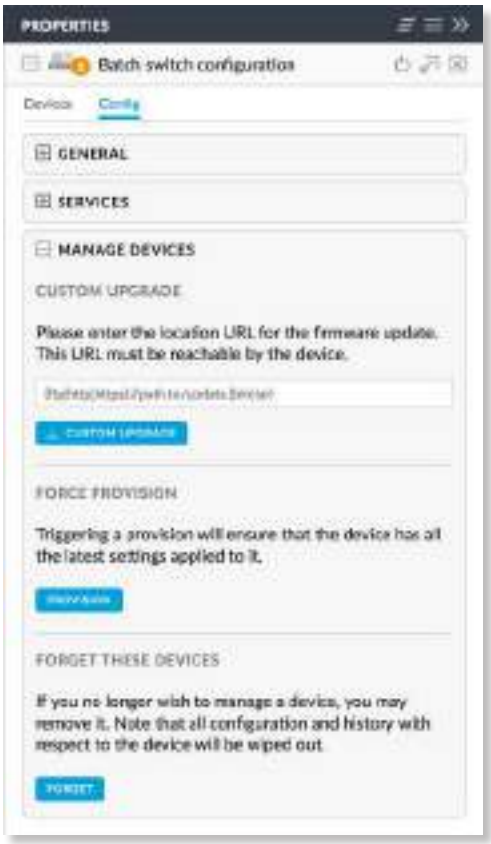
- **Flow Control** Enabling this option will enable 802.3x Ethernet Flow Control on all ports of this switch. This should remain disabled, unless you have a specific requirement for 802.3x and understand its implications. The default is *Keep existing* (setting).
- **Spanning Tree** Ethernet networks cannot have multiple active paths between switches (absent aggregation such as LAG), as this causes a switching loop, where broadcast and multicast traffic are amplified and repeated in a never-ending loop. Spanning Tree prevents switching loops, and allows for redundant interconnections between switches. Interfaces with redundant paths are put into STP blocking mode, leaving the port down unless the current best active path fails.

  Select the appropriate option: **RSTP** (Rapid Spanning Tree Protocol), **STP** (Spanning Tree Protocol), or **Disabled**. RSTP is the default and is recommended because topology changes apply much more quickly (usually within 6 seconds, rather than the 30-50 seconds of STP). STP will enable the older 802.1D STP on this switch instead of RSTP. Disabled will disable all versions of spanning tree; however, this is not recommended, as it can leave the network susceptible to being taken down by an inadvertently created switching loop. The default is *Keep existing* (setting).
- **Priority** STP uses the priority value as part of the calculation in electing a root bridge of the spanning tree. It is best to configure a lower priority number (higher preference in root bridge elections) on one or two of the switches you consider the "core" of your network. For instance, if you have two 10 Gb switches, and several gigabit switches, configure a lower priority on the two 10 Gb switches to ensure that they are preferred as the STP root bridge. The default is *Keep existing* (setting).
- **802.1x Control** Select this option to use a RADIUS server for user authentication on the switch's ports. The default is *Keep existing* (setting).

  If you enable 802.1X control, then the *RADIUS Profile* setting appears.
- **RADIUS Profile** The default is *Keep existing* (setting). You can click **Create New RADIUS Profile** to create a new one to use. Go to **"Create or Edit a RADIUS Profile" on page 45** for instructions.
- **Queue Changes** Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

  When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)
- **Cancel** Click *Cancel* to discard changes.

7. In the *Manage Devices* section, make the appropriate changes:



   - **Custom Upgrade** For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, enter the URL of the firmware's location and then click CUSTOM UPGRADE to upgrade the firmware.
   - **Force Provision** Click **Provision** to ensure that the device has all of the latest settings applied to it.
   - **Forget These Devices** Click **Forget** to remove the Switches from management by the UniFi Controller software and reset them to factory default settings.

     Note: Use caution when clicking *Forget*. This will restore the Switches to factory default settings when they are in a *Connected* state.
8. Click the **Devices** tab to view the selected Switches.

- **Device Name** Displays the hostname, alias, or MAC address of the Switch.
- **Model** Displays the model name.
- **(properties)** Click to get additional details; see **"UniFi Switch Details" on page 121** for more information.
- **(remove)** Click to remove the Switch from this group configuration.

APs

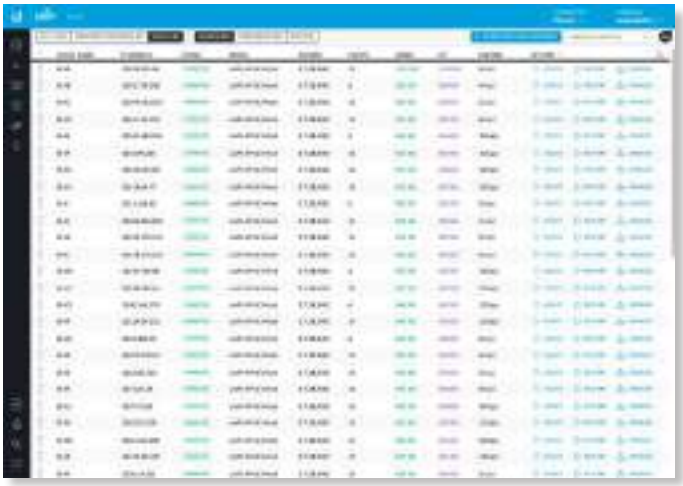
You can apply one of the following filters to display different status information:

- **Overview** Displays the number of clients, amount of data downloaded, amount of data uploaded, and channel setting.
- **Performance** Displays the number of 2.4 and 5 GHz clients, overall transmit rate, overall receive rate, 2.4 and 5 GHz transmit rates, and channel setting.
- **Config** Displays the WLAN and radio settings for the 2.4 GHz and 5 GHz radio bands.

On any sub-tab, you can initiate a rolling upgrade of the firmware for all APs.

Start Rolling Upgrade (Available if any AP has an upgrade available.) Click START ROLLING UPGRADE to begin automatically upgrading APs, one by one, except for wirelessly uplinked APs, which are intentionally excluded from upgrading.

Overview



(icon) Displays the icon corresponding to the AP model (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro/HD/SHD
- UniFi AP AC EDU
- UniFi AP AC Mesh
- UniFi AP AC Mesh Pro
- UniFi AP In-Wall/AP AC In-Wall
- UniFi AP/AP LR
- UniFi AP AC
- UniFi AP AC Outdoor
- UniFi AP Outdoor+
- UniFi AP Outdoor5

The LED color of the icon indicates the device status.

- **Blue/Green** Indicates the device is connected.
- **Gray** Indicates the device is pending approval.
- **Red/Orange** Indicates the device is disconnected or not managed by this site (*Pending Approval* or *Managed by Other*).

Device Name Displays the hostname, alias, or MAC address of the AP. You can click the name to get additional details; see **"UniFi Access Point Details" on page 131** for more information.

IP Address Displays the IP address of the AP.

Status Displays the connection status.

- **Connected** The AP is physically wired to the network.
- **Connected (100 FDX)** The AP is physically wired to the network at 100 Mbps in full-duplex mode.
- **Connected (wireless)** The AP is wirelessly uplinked to a physically wired AP.
- **Disconnected** The AP is unreachable by the UniFi Controller software.
- **Isolated** A managed AP is unable to locate its uplink.
- **Managed by Other** The AP is not in the default state but it is not controlled by the UniFi Controller.
- **Pending Approval** The AP is in the default state and is available for adoption.

  Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

  Note: The superadmin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

Model Displays the model name of the UniFi device.

Version Displays the version number of the UniFi device's firmware.

Clients Displays the number of clients connected to the AP.

Down Displays in green the total amount of data downloaded by the AP.

Up Displays in purple the total amount of data uploaded by the AP.

Channel Displays the transmit/receive channel being used by the AP. The radio band is represented as *(ng)* for 2.4 GHz and *(na)/(ac)* for 5 GHz.

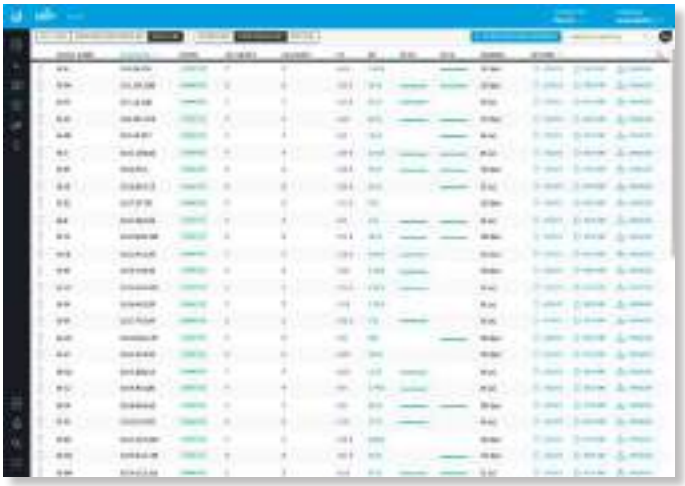
Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to flash the LED on the AP and the AP's icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Restart** Click RESTART to restart the selected device.
- **Upgrade** If a software upgrade is available for the device, click UPGRADE to install the latest UniFi firmware on the device. The *Status* will appear as *Upgrading* until the process is complete and the device reconnects to the UniFi Controller software.
- **Adopt** Click ADOPT to adopt a device that appears as *Pending Approval* for its status. The *Status* will appear as *Adopting* until the device is connected.

Group Configuration

For detailed instructions and information on AP group configuration, refer to the following online help article: **ubnt.link/UniFi-AP-Group-Configuration**

Performance



(icon) Displays the icon corresponding to the AP model (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro/HD/SHD
- UniFi AP AC EDU
- UniFi AP AC Mesh
- UniFi AP AC Mesh Pro
- UniFi AP In-Wall/AP AC In-Wall
- UniFi AP/AP LR
- UniFi AP AC
- UniFi AP AC Outdoor
- UniFi AP Outdoor+
- UniFi AP Outdoor5

The LED color of the icon indicates the device status.

- **Blue/Green** Indicates the device is connected.
- **Gray** Indicates the device is pending approval.
- **Red/Orange** Indicates the device is disconnected or not managed by this site (*Pending Approval* or *Managed by Other*).

Device Name Displays the hostname, alias, or MAC address of the AP. You can click the name to get additional details; see **"UniFi Access Point Details" on page 131** for more information.

IP Address Displays the IP address of the AP.

Status Displays the connection status.

- **Connected** The AP is physically wired to the network.
- **Connected (100 FDX)** The AP is physically wired to the network at 100 Mbps in full-duplex mode.
- **Connected (wireless)** The AP is wirelessly uplinked to a physically wired AP.
- **Disconnected** The AP is unreachable by the UniFi Controller software.
- **Isolated** A managed AP is unable to locate its uplink.
- **Managed by Other** The AP is not in the default state but it is not controlled by the UniFi Controller.
- **Pending Approval** The AP is in the default state and is available for adoption.

  Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

  Note: The superadmin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

2G Clients Displays the number of clients connected to the AP using the 2.4 GHz band.

5G Clients Displays the number of clients connected to the AP using the 5 GHz band.

TX Displays in purple the overall TX (transmit) rate.

RX Displays in green the overall RX (receive) rate.

TX 2G Displays the overall TX rate for the 2.4 GHz radio band. The different colors represent different types of packet activity:

Color	Packet Activity
	Packets sent
	Packets retried
	Packets not sent due to likely interference

TX 5G Displays the overall TX rate for the 5 GHz radio band. The different colors represent different types of packet activity:

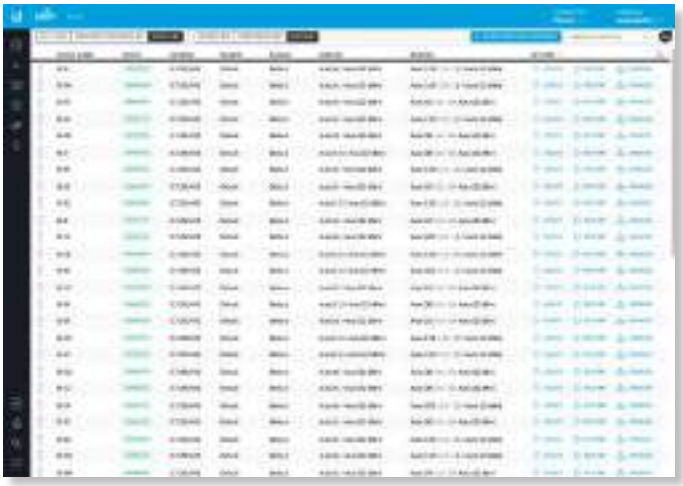
Color	Packet Activity
	Packets sent
	Packets retried
	Packets not sent due to likely interference

Channel Displays the transmit/receive channel being used by the AP. The radio band is represented as *(ng)* for 2.4 GHz and *(na)/(ac)* for 5 GHz.

Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to flash the LED on the AP and the AP's icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Restart** Click RESTART to restart the selected device.
- **Upgrade** If a software upgrade is available for the device, click UPGRADE to install the latest UniFi firmware on the device. The *Status* will appear as *Upgrading* until the process is complete and the device reconnects to the UniFi Controller software.
- **Adopt** Click ADOPT to adopt a device that appears as *Pending Approval* for its status. The *Status* will appear as *Adopting* until the device is connected.

Config



(icon) Displays the icon corresponding to the AP model (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro/HD/SHD
- UniFi AP AC EDU
- UniFi AP AC Mesh
- UniFi AP AC Mesh Pro
- UniFi AP In-Wall/AP AC In-Wall
- UniFi AP/AP LR
- UniFi AP AC
- UniFi AP AC Outdoor
- UniFi AP Outdoor+
- UniFi AP Outdoor5

The LED color of the icon indicates the device status.

- **Blue/Green** Indicates the device is connected.
- **Gray** Indicates the device is pending approval.
- **Red/Orange** Indicates the device is disconnected or not managed by this site (*Pending Approval* or *Managed by Other*).

Device Name Displays the hostname, alias, or MAC address of the AP. You can click the name to get additional details; see **"UniFi Access Point Details" on page 131** for more information.

Status Displays the connection status.

- **Connected** The AP is physically wired to the network.
- **Connected (100 FDX)** The AP is physically wired to the network at 100 Mbps in full-duplex mode.
- **Connected (wireless)** The AP is wirelessly uplinked to a physically wired AP.
- **Disconnected** The AP is unreachable by the UniFi Controller software.
- **Isolated** A managed AP is unable to locate its uplink.
- **Managed by Other** The AP is not in the default state but it is not controlled by the UniFi Controller.
- **Pending Approval** The AP is in the default state and is available for adoption.

  Only the superadmin and admins who have permission to adopt devices can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

  Note: The superadmin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

Version Displays the version number of the UniFi device's firmware.

WLAN 2G Displays the name of the WLAN group using the 2.4 GHz radio band.

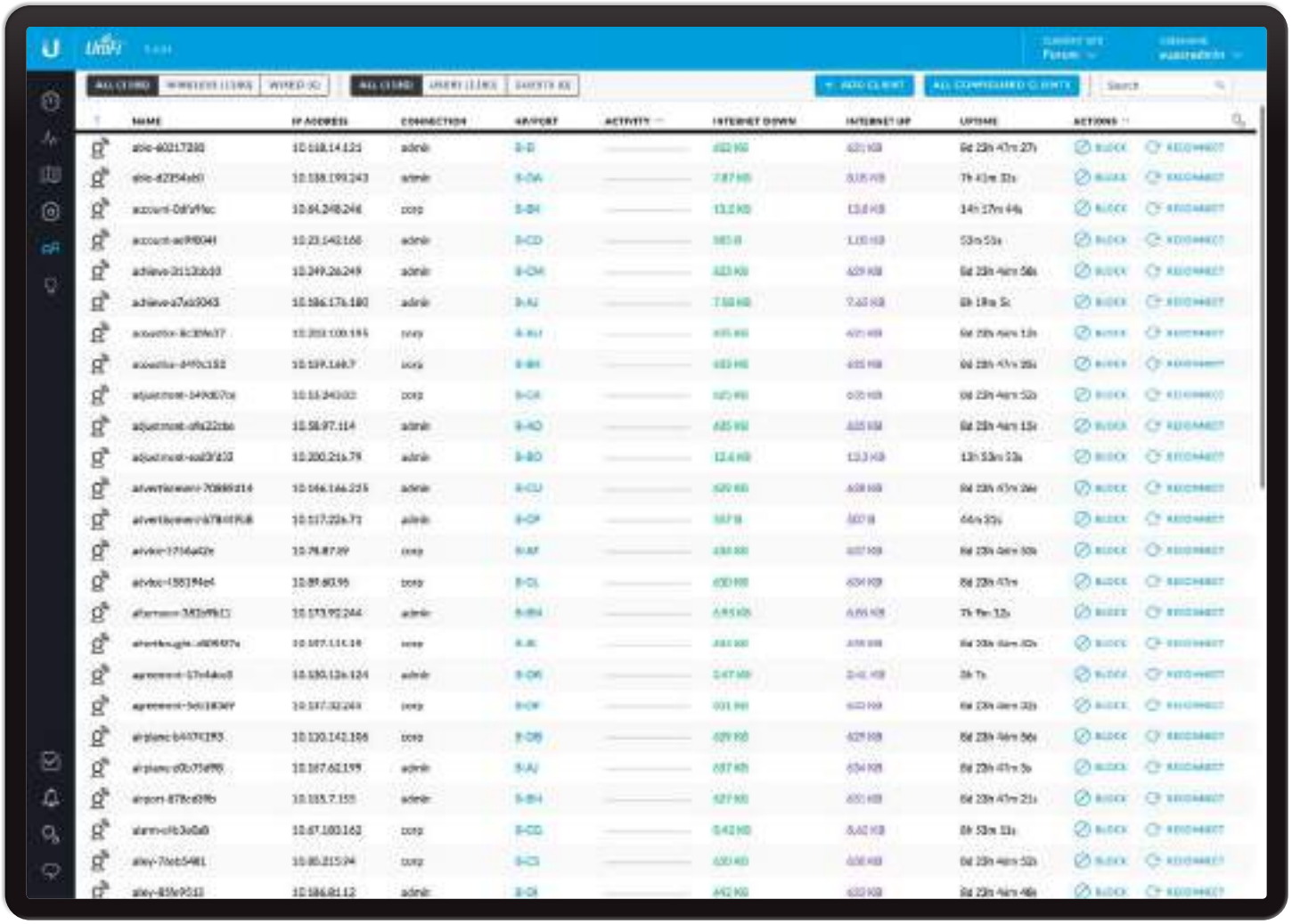
WLAN 5G Displays the name of the WLAN group using the 5 GHz radio band.

Radio 2G Displays the channel and TX power settings used in the 2.4 GHz radio band.

Radio 5G Displays the channel and TX power settings used in the 5 GHz radio band.

Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to flash the LED on the AP and the AP's icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Restart** Click RESTART to restart the selected device.
- **Upgrade** If a software upgrade is available for the device, click UPGRADE to install the latest UniFi firmware on the device. The *Status* will appear as *Upgrading* until the process is complete and the device reconnects to the UniFi Controller software.
- **Adopt** Click ADOPT to adopt a device that appears as *Pending Approval* for its status. The *Status* will appear as *Adopting* until the device is connected.



Chapter 8: Clients

The *Clients* screen displays a list of network clients. You can click any of the column headers to change the list order.

You can apply one of the following primary filters:

- **All** Displays all clients, regardless of connection type.
- **Wireless** Displays all wireless clients.
- **Wired** Displays all wired clients.

A secondary filter is available:

- **All** Displays all users and guests.
- **Users** Displays only users.
- **Guests** Displays only guests.

Items per page Select how many results are displayed per page: **10**, **25**, **50**, **100**, or **200**.

The columns of information vary depending on which primary filter (*All*, *Wireless*, or *Wired*) is applied.

If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

Add Client Click to add a client to your network.

Configure the following:

- **MAC Address** Enter the MAC address or unique hardware identifier of the client.
- **Alias** Allows you to change the hostname of the client.
- **User Group** Allows you to assign the client to a User Group. User Groups are set up under the *Settings* tab > *User Groups* option (see **"Settings > User Groups" on page 54** for more information). The default *User Group* is *Automatic*.

- **Fixed IP** If you want to assign a static IP address to the client, select this option. Then configure the settings below.
  - **Network** Select the appropriate network from the drop-down list.
  - **IP Address** Enter the static IP address.
- **Add** Click to save changes.
- **Cancel** Click to cancel changes.

All Configured Clients Click to view all clients that you have manually added. The *Insight* > *Known Clients* screen appears. Go to **"Known Clients" on page 106** for more information.

Search Search Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

The icon column sorts by state, and for connected devices it also sorts by device type. This is the order:

- Connected wireless user
- Connected wireless guest
- Connected wired user
- Connected wired guest

After this sorting is applied, the sort order uses alphabetical order according to the client name.

Settings To enable group or batch configuration or customize the column layout, click this option.

- **Enable Group Config** Use this feature to configure an entire group of clients at the same time. The following settings can be changed with batch configuration:
  - Note
  - User Group
  - IP Address

Group Configuration

To enable group or batch configuration, follow these instructions:

1. Click and then select **Enable group config**.

2. Select the appropriate clients.

3. Click EDIT SELECTED.

4. The *Properties* panel opens.
5. Click the + icon to expand the appropriate section:

6. In the *General* section, make the appropriate changes:

- **Note** Allows you to enter comments about the client. Once saved, the client will be designated as a "Noted" client on the *Insights* > *Known Clients* tab.

- **User Group** Allows you to assign the client to a User Group. User Groups are set up under the *Settings* tab > *User Groups* option (see **"Settings > User Groups" on page 54** for more information). The default *User Group* is *Automatic*.
- **Queue Changes** Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

  When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

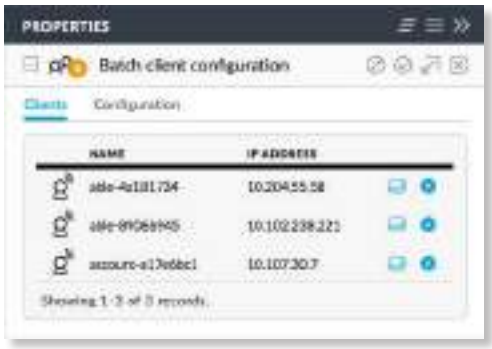
7. In the *Network* section, make the appropriate changes:

- **Fixed IP Address** The default is *Keep existing* (setting). If you want the local DHCP server to assign an IP address to the client, select **Don't use fixed IP address**.

  If you want to assign a static IP address to the client, select **Use fixed IP address**. Then configure the settings below.
- **Network** Select the appropriate network from the drop-down list
- **IP Addresses** Enter the static IP address for each client listed.
- **Show Current IPs** If you want the current IP addresses shown, click this option. Otherwise, the current IP addresses are hidden.
- **Queue Changes** Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

  When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

8. Click the **Clients** tab to view the selected clients.



- **(icon)** Displays the icon corresponding to a wireless or wired client.
- **Name** Displays the hostname, alias, or MAC address of the client.
- **IP Address** Displays the IP address used by the client.
- **(properties)** Click to get additional details; see **"Client Details" on page 147** for more information.
- **(remove)** Click to remove the client from this group configuration.

Customize Columns

Each primary filter: *All*, *Wireless*, or *Wired* applies a default set of columns to display. If you enable the *Customize Columns* option, then the primary filter no longer changes the columns.

Click to customize the columns used for display.

Select **Customize columns**.

You can select additional columns for display. Options include the following:

- **Name** Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; refer to **"Client Details" on page 147** for more information.
- **Hostname** Displays the hostname of the connected client.
- **MAC Address** Displays the MAC address of the connected client.
- **IP Address** Displays the IP address used by the client.
- **802.1X Identity** Displays the identity used for 802.1x authentication.
- **802.1X VLAN** Displays the VLAN (Virtual Local Area Network) used for 802.1x authentication.
- **Status** Displays *Authorized* for all authorized guests or *Pending* for guests pending authorization.
- **User Group** Displays the User Group of the client (if any).
- **Network** Indicates which local network is used.
- **AP/Port** For wireless clients, displays the name of the connected AP or port. You can click the name to get additional details; refer to **"UniFi Access Point Details" on page 131** for more information.

  For wired clients, displays the name of the network device and port number used by the client. You can click the name to get additional details; refer to **"UniFi Switch Details" on page 121** for more information.
- **Channel** Displays the channel used.
- **PHY Mode** Displays the wireless standard and frequency band used by the signal. Displays a leaf icon if the device uses power save mode.
  - 11na (5 GHz)
  - 11ac (5 GHz)
  - 11ng (2.4 GHz)
  - 11b (2.4 GHz)
- **FT** FT is Fast Transition or IEEE 802.11r-2008. It enables roaming with continuous connectivity and seamless handoffs between APs.
- **Signal** Displays the signal strength level and signal type.
- **TX Rate** Displays the overall TX (transmit) rate.
- **RX Rate** Displays the overall RX (receive) rate.
- **Activity** Displays the relative level of activity for each client.
- **Internet Down** Displays in green the total amount of data downloaded by the client from the internet.
- **Internet Up** Displays in purple the total amount of data uploaded by the client to the internet.
- **LAN Down** Displays the total amount of data downloaded by the client from the local network.
- **LAN Up** Displays the total amount of data uploaded by the client to the local network.
- **Uptime** Displays the amount of time the client has been connected for this session.

All

(icon) Displays the icon corresponding to a wireless or wired client:

wireless user

wireless guests

wired user

wired guest

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; refer to **"Client Details" on page 147** for more information.

IP Address Displays the IP address used by the client.

Connection Indicates which local network is used. If the connection is wireless, then this displays the wireless network name or SSID.

AP/Port Indicates which AP or switch port is used.

Activity Displays the relative level of activity for each client.

Internet Down Displays in green the total amount of data downloaded by the client from the internet.

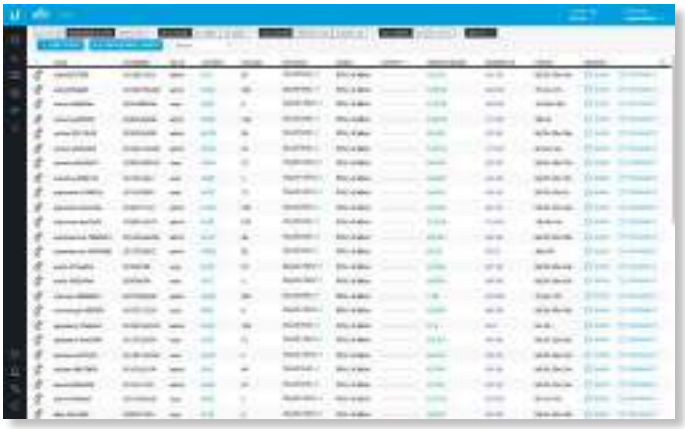
Internet Up Displays in purple the total amount of data uploaded by the client to the internet.

Uptime Displays the amount of time the client has been connected for this session.

Actions Click a button to perform the desired action:

- **Block** Click BLOCK to block this client from accessing the network. Click UNBLOCK to unblock this client.
- **Reconnect** Click RECONNECT to reconnect a wireless client. You can click RECONNECT to kick out a client, which usually reconnects back quickly; this is useful for troubleshooting or resolving a problematic wireless connection.
- **Unauthorize/Authorize** (Available for *Guests* only.) Click UNAUTHORIZE to remove authorization of guest access and disconnect the guest, or click AUTHORIZE for guests pending authorization.

Wireless



Frequency band If the *Wireless* filter is applied, then the *Frequency band* filter is available:

- **All** Displays all wireless clients.
- **2G** Displays only 2.4 GHz clients.
- **5G** Displays only 5 GHz clients.

Client Type If the *Wireless* filter is applied, then the *Client type* filter is available:

- **All** Displays all wireless clients.
- **Users** Displays only clients who are not guests.
- **Guests** Displays only clients with guest access.

Status If the *Wireless* filter is applied, then the *Status* filter is available:

- **All** Displays all wireless clients.
- **Active** Displays only clients that are currently active.

AP Select the AP whose clients you want displayed. Each option in the drop-down list also indicates the number of wireless clients in parentheses.

(icon) Displays the icon corresponding to a wireless client:

wireless user

wireless guest

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; refer to **"Client Details" on page 147** for more information.

IP Address Displays the IP address used by the client.

WLAN Displays the name of the wireless network.

AP/Port Displays the name of the connected AP. You can click the name to get additional details; refer to **"UniFi Access Point Details" on page 131** for more information.

Channel Displays the channel used.

Phy Mode Displays the wireless standard and frequency band used by the signal. Displays a leaf icon if the device uses power save mode.

- 11na (5 GHz)
- 11ac (5 GHz)
- 11ng (2.4 GHz)
- 11b (2.4 GHz)

Signal Displays the signal strength level and signal type.

Activity Displays the relative level of activity for each client.

Internet Down Displays in green the total amount of data downloaded by the client from the internet.

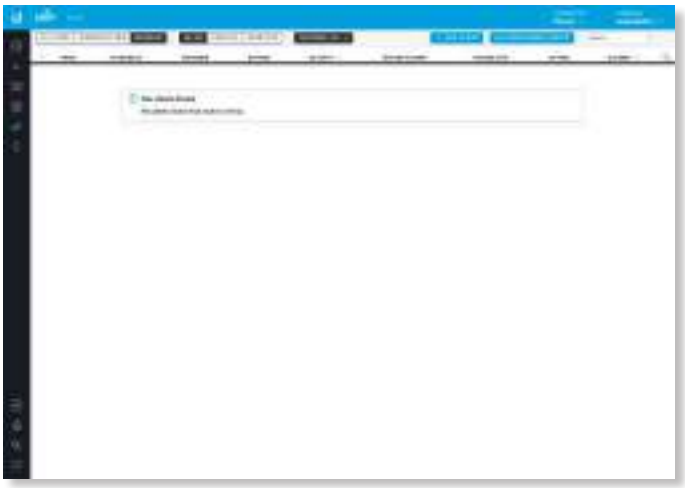
Internet Up Displays in purple the total amount of data uploaded by the client to the internet.

Uptime Displays the amount of time the client has been connected for this session.

Actions Click a button to perform the desired action:

- **Block** Click BLOCK to block this client from accessing the network. Click UNBLOCK to unblock this client.
- **Reconnect** Click RECONNECT to reconnect a wireless client. You can click RECONNECT to kick out a client, which usually reconnects back quickly; this is useful for troubleshooting or resolving a problematic wireless connection.
- **Unauthorize/Authorize** (Available for *Guests* only.) Click UNAUTHORIZE to remove authorization of guest access and disconnect the guest, or click AUTHORIZE for guests pending authorization.

Wired



Client Type If the *Wired* filter is applied, then the *Client type* filter is available:

- **All** Displays all wired clients.
- **Users** Displays only clients who are not guests.
- **Guests** Displays only clients with guest access.

Network If the *Wired* filter is applied, then the *Network* filter is available. Each option in the drop-down list also indicates the number of wired clients in parentheses.

- **All** Displays all wired clients.
- **(name)** Select the network whose clients you want displayed.

(icon) Displays the icon corresponding to a wired client:

wired user

wired guest

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; refer to **"Client Details" on page 147** for more information.

IP Address Displays the IP address used by the client.

Network Indicates which local network is used.

AP/Port Displays the name of the network device and port number used by the client. You can click the name to get additional details; refer to **"UniFi Switch Details" on page 121** for more information.

Activity Displays the relative level of activity for each client.

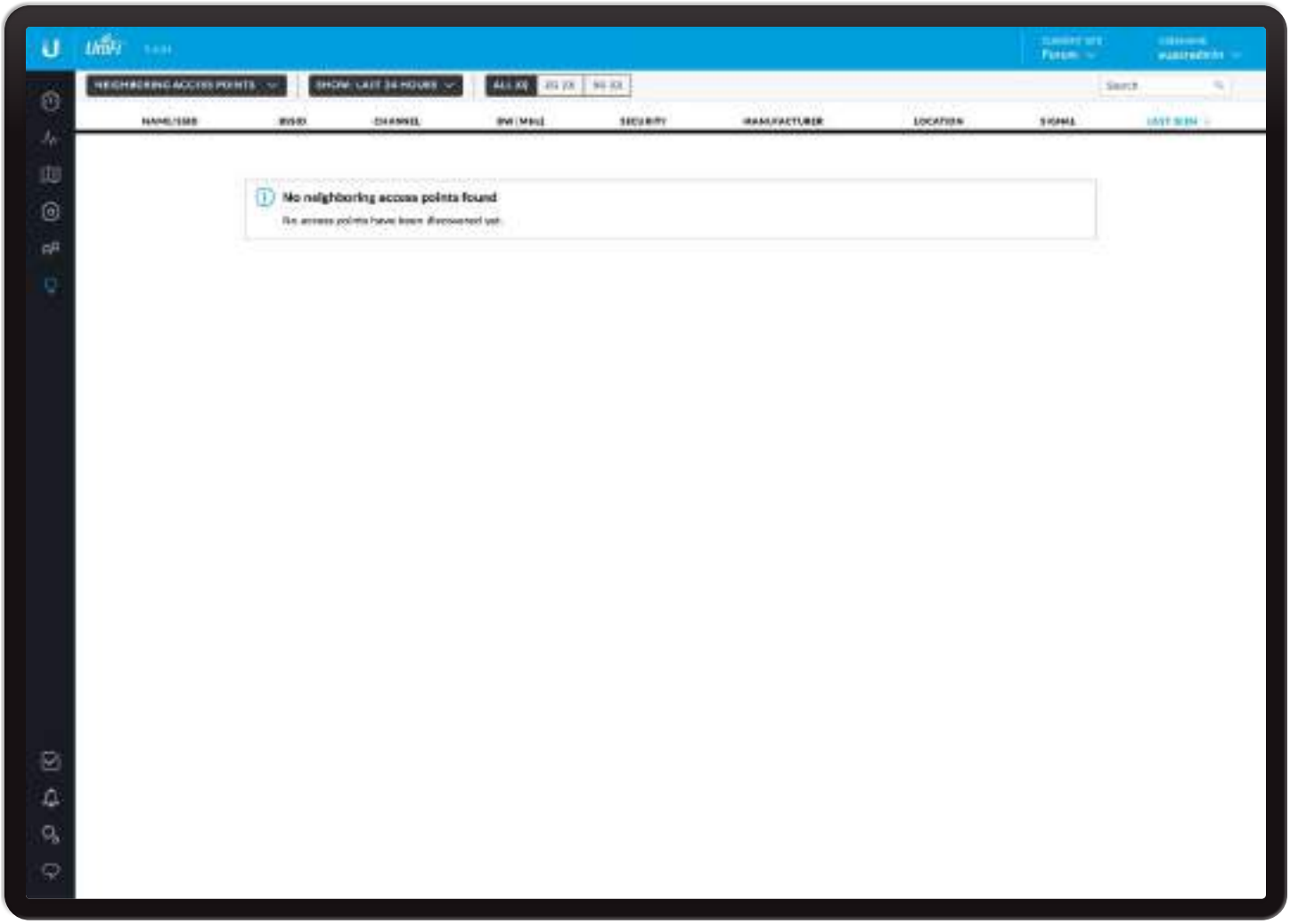
Internet Down Displays in green the total amount of data downloaded by the client from the internet.

Internet Up Displays in purple the total amount of data uploaded by the client to the internet.

Uptime Displays the amount of time the client has been connected for this session.

Actions Click a button to perform the desired action:

- **Block** Click BLOCK to block this client from accessing the network. Click UNBLOCK to unblock this client.
- **Unauthorize/Authorize** (Available for *Guests* only.) Click UNAUTHORIZE to remove authorization of guest access and disconnect the guest, or click AUTHORIZE for guests pending authorization.



Chapter 9: Insights

The *Insights* screen displays different kinds of status information. The following filters are available:

- **Neighboring Access Points** Displays information about wireless devices not managed by the UniFi Controller.
- **Known Clients** Displays information about detected clients.
- **Past Connections** Displays information about previous client connection sessions (for example, a client can have multiple sessions from different days).
- **Past Guest Authorizations** Displays information about the authorization of previous guest connections.
- **Switch Stats** Displays information about the status, ports, PoE, and traffic activity of the UniFi Switches.
- **Port Forward Stats** Displays information about the port forwarding entries used by the UniFi Security Gateway.
- **Dynamic DNS** Displays information about the use of DDNS services.
- **Remote User VPN** Displays information about the remote user VPN connections.
- **AC-EDU Streams** Displays information about the streaming by the UniFi AC EDU Access Points.
- **Controller Logs** Displays device, management, and system log entries.

These sub-tabs share common options:

Items per page Select how many results are displayed per page: **10**, **50**, **100**, or **200**.

On any sub-tab, you can click any of the column headers to change the list order.

If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

Search Search Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Settings To enable group or batch configuration or customize the column layout, click this option.

- **Enable Group Config** Available for *Known Clients*. Select to configure multiple clients at the same time. Go to **"Group Configuration" on page 100** for instructions.

Customize Columns Each of these filters: *Switch Stats*, *Port Forward Stats*, *Dynamic DNS*, *Remote User VPN*, and *AC-EDU Streams,* applies a default set of columns to display. If you enable the *Customize Columns* option, then the selected columns are displayed.

Click to customize the columns used for display.

Select **Customize columns**.

The column options will vary depending on the filter. They are described further in the following sections:

- **"Switch Stats" on page 108**
- **"Port Forward Stats" on page 111**
- **"Dynamic DNS" on page 113**
- **"Remote User VPN" on page 113**
- **"AC-EDU Streams" on page 114**

Neighboring Access Points

This screen displays information about wireless devices not managed by the UniFi Controller.

Show Filter the results on the page based on the time the AP was last seen. Select **Last hour**, **Last 8 hours**, **Last 12 hours**, **Last 24 hours**, **3 days**, **7 days**, **2 weeks**, **30 days**, **120 days**, or **All**.

You can apply one of the following filters:

- **All** Displays all wireless APs.
- **2G** Only displays 2.4 GHz APs.
- **5G** Only displays 5 GHz APs.

(number) Displays the number of managed UniFi APs that are nearby. You can click the + button to display the list of UniFi APs.

Rogue Displays a to indicate a rogue AP.

Name/SSID Displays the name of the wireless network.

BSSID Displays the MAC address of the AP's wireless interface.

Channel Displays the channel setting that the AP was detected on.

BW (MHz) Displays the channel width that the AP was using.

Security Displays the security status indicating whether encryption is used.

Manufacturer Displays the name of the AP manufacturer.

Location Displays the name of the closest AP managed by the UniFi Controller.

Signal Displays the signal strength level and signal type.

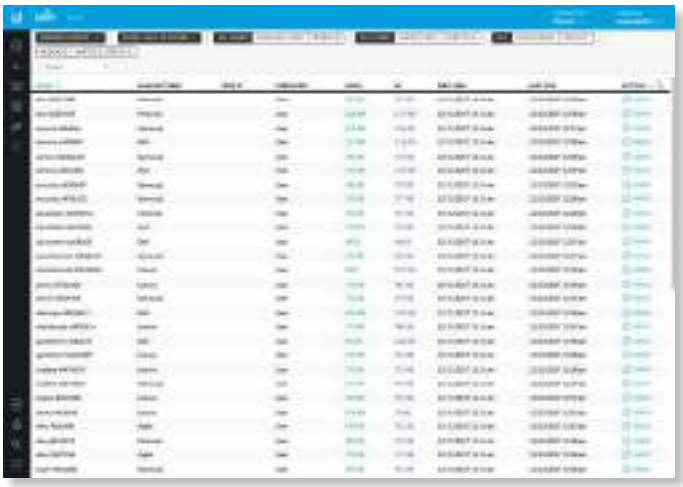
Last Seen Displays the last date and time the AP was connected.

Actions Click a button to perform the desired action:

- **Mark as Known** If the rogue AP is known to you, then you can click MARK AS KNOWN so it will not be marked as a rogue AP.

Known Clients

This screen displays information about detected clients.



Show Filter the results on the page based on the date the client was last seen. Select **last 24 hours**, **3 days**, **7 days**, **2 weeks**, **30 days**, **120 days**, or **All**.

You can apply one of the following filters:

- **All** Display all clients, regardless of connection type.
- **Wireless** Display all wireless clients.
- **Wired** Display all wired clients.

You can also apply one of the following filters:

- **All** Display all users and guests.
- **User** Only display users.
- **Guest** Only display guests.

An additional filter is available:

- **All** Displays all known clients.
- **Configured** Displays clients that you have added on the *Clients* screen.
- **Default** Displays clients that have not been assigned a fixed IP address, or have not been put in a user group.

A cumulative filter is available, so you can apply one, two, or all three of these filters at the same time:

- **Blocked** Only display blocked clients.
- **Noted** Only display clients whose configurations include notes. (See **"Wireless Client – Configuration" on page 148** or **"Wired Client – Configuration" on page 150** for more information.)
- **Static IP** Only display clients using static IP addresses.

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name for more details; see **"Client Details" on page 147** for more information.

Manufacturer Displays the name of the device manufacturer.

Fixed IP Displays the fixed IP address, if applicable.

User/Guest Indicates whether the client is/was connected to a primary or guest network.

Down Displays in green the total amount of data downloaded by the client.

Up Displays in purple the total amount of data uploaded by the client.

First Seen Displays the date and time the client was initially connected.

Last Seen Displays the last date and time the client was connected.

Actions Click a button to perform the desired action:

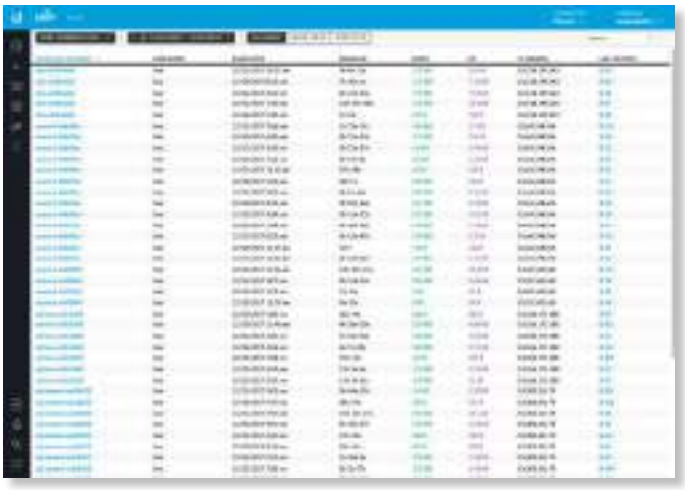
- **Block** Click BLOCK to block this client from accessing the network. Click UNBLOCK to unblock this client.
- **Reconnect** Click RECONNECT to reconnect a wireless client. You can click RECONNECT to kick out a client, which usually reconnects back quickly; this is useful for troubleshooting or resolving a problematic wireless connection.
- **Unauthorize/Authorize** (Available for *Guests* only.) Click UNAUTHORIZE to remove authorization of guest access and disconnect the guest, or click AUTHORIZE for guests pending authorization.

Settings To enable group or batch configuration, click this option.

- **Enable Group Config** Configure multiple clients at the same time. Go to **"Group Configuration" on page 100** for instructions.

Past Connections

This screen displays information about previous client connection sessions (for example, a client can have multiple sessions from different days).



Date Click either arrow to change the date in one-day increments.

< 12/08/2017 - 12/15/2017 >

Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

You can apply one of the following filters:

- **All** Display all users and guests.
- **Users** Only display users.
- **Guests** Only display guests.

Name/MAC Address Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; see **"Client Details" on page 147** for more information.

User/Guest Indicates whether the client is/was connected to a primary or guest network.

Associated Displays the date and time the client first connected.

Duration Displays the length of time the client was connected.

Down Displays in green the total amount of data downloaded by the client.

Up Displays in purple the total amount of data uploaded by the client.

IP Address Displays the last known IP address of the client.

Last AP/Port Displays the name or MAC address of the last AP used by the wireless client or the last port used by the wired client. You can click the device name for more information; refer to **"UniFi Access Point Details" on page 131** or **"UniFi Switch Details" on page 121** .

Past Guest Authorizations

This screen displays information about the authorization of previous guest connections.

Date Click either arrow to change the date in one-day increments.

Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

Name/MAC Address Displays the hostname, alias, or MAC address of the previous guest.

Package Displays the name of the guest access package.

Amount Displays the amount paid by the guest.

Authorized By Displays the name of the authorizing body.

Start Displays the start date and time of the session.

Duration Displays the length of time the guest was connected.

Download Displays the total amount of data downloaded by the guest.

Upload Displays the total amount of data uploaded by the guest.

IP Displays the last known IP address of the guest.

Last AP Displays the name or MAC address of the last AP used by the wireless guest. You can click the device name for more information; refer to **"UniFi Access Point Details" on page 131**.

Switch Stats

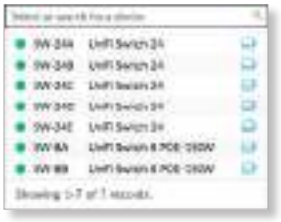
This screen displays information about the status, ports, PoE, and traffic activity of the UniFi Switches.

You can apply one of the following filters:

- **Overview** Displays the general status information of each port.
- **PoE** Displays the specific PoE configuration and status of each port.
- **Counters** Displays the specific TX and RX rates for each port.

Search 

You can view the statistics by UniFi Switch. The drop-down list displays managed UniFi Switches by name or MAC address (you can click for additional details). Select the appropriate switch or enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.



You have an additional filter:

- **Link Status** Displays the ports of the specified status:
  - **All** Displays all ports.
  - **Connected** Displays all connected ports.
  - **Disconnected** Displays all disconnected ports.

Clear Counters Click CLEAR COUNTERS and select one of the following:

- **All** Resets all counters to zero.
- **(switch_name)** Resets the counters of the selected UniFi Switch to zero.

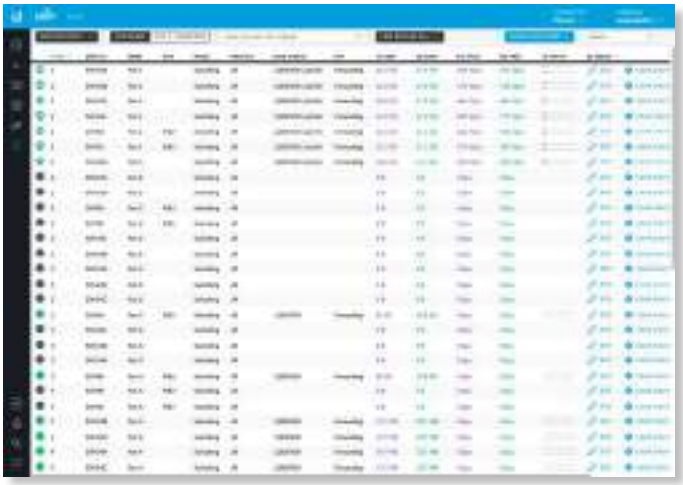
Customize Columns Click to customize the columns used for display.

Select **Customize columns**.

You can add or remove columns for display. The *Customize columns* option will apply, and the filter options: *Overview*, *PoE*, and *Counters* will disappear.

- **Reset columns to** Click the drop-down at the bottom of the *Customize columns* screen to display the *Reset columns to* ... options.
  - **Overview** The *Switch*, *Name*, *PoE*, *Mode*, *Profile*, *Link Status*, *STP*, *TX SUM (Summary)*, *RX Sum* (Summary), *TX TPUT (Throughput)*, *RX TPUT (Throughput)*, and *Activity* columns are displayed.
  - **PoE** The *Switch*, *Name*, *PoE*, *PoE Detection*, *PD Class*, *Power*, *Voltage*, and *Current* columns are displayed.
  - **Counters** The *Switch*, *TX Bytes*, *TX Frames*, *TX Multicast*, *TX Broadcast*, *TX Errors*, *RX Bytes*, *RX Frames*, *RX Multicast*, *RX Broadcast*, and *RX Errors* columns are displayed.

Overview



Port The ports display their status and port number:

- Indicates a 10/100 Mbps connection.
- Indicates a 1 Gbps (1000 Mbps) connection.
- Indicates a 10 Gbps connection.
- Indicates 1 Gbps (1000 Mbps) connection with PoE.
- Indicates the connection is disabled (no network or VLAN is enabled).
- Indicates no connection (the network or VLAN is enabled, but the port is not in use).
- Indicates a uplink.

Switch If all switches are displayed, then this displays the hostname, alias, or MAC address of the UniFi Switch. You can click the name to get additional details. For more information, see **"UniFi Switch Details" on page 121**.

Name Displays the name of the port.

PoE Displays the PoE setting:

- **(blank)** PoE is disabled.
- **24V Passive** 24V passive PoE is enabled.
- **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.
- **__W** Power output is displayed in watts.

Mode Displays the operation mode:

- **Switching** The default mode.
- **Mirroring** The network traffic of this port will receive the mirrored traffic from the port selected in **"Port Configuration" on page 125**.
- **Aggregate** This port is part of an aggregate link. A port channel, also known as a Link Aggregation Group (LAG), combines multiple links into a single logical link (single IP address) for load balancing and/or redundancy.

Profile Displays the Switch Port profile assigned to it. Switch Port profiles are configured in *Settings* > **"Switch Ports" on page 46**.

Link Status Displays the connection speed and duplex mode.

STP Displays the STP (Spanning Tree Protocol) mode.

TX SUM Displays in purple the amount of data transmitted.

RX SUM Displays in green the amount of data received.

TX TPUT Displays in purple the transmit throughput rate.

RX TPUT Displays in green the receive throughput rate.

Activity Displays the level of activity. The different colors represent different types of packet activity.

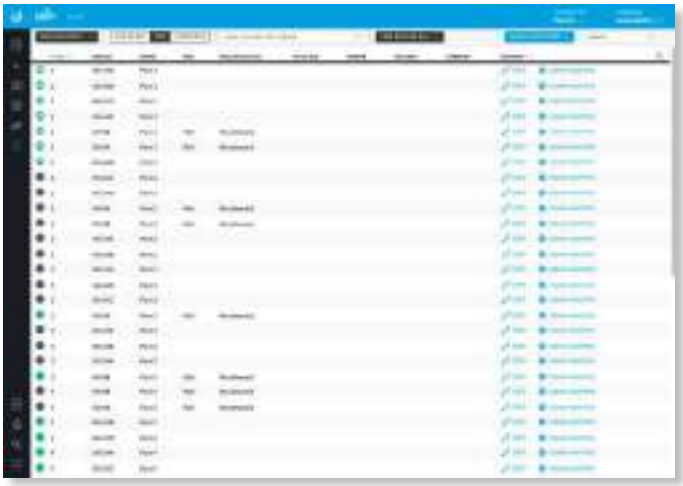
Color	Packet Activity
	TX throughput rate
	RX throughput rate

You can place your mouse over the *Activity* icon to display the specific TX or RX rate.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the port settings. For more information, see **"UniFi Switch Details" on page 121**.
- **Clear Counters** Click CLEAR COUNTERS to clear the port statistics.
- **Power Cycle** If applicable, click POWER CYCLE to power cycle the port.

PoE



Port The ports display their status and port number:

- Indicates a 10/100 Mbps connection.
- Indicates a 1 Gbps (1000 Mbps) connection.
- Indicates a 10 Gbps connection.
- Indicates 1 Gbps (1000 Mbps) connection with PoE.
- Indicates the connection is disabled (no network or VLAN is enabled).
- Indicates no connection (the network or VLAN is enabled, but the port is not in use).
- Indicates a uplink.

Switch If all switches are displayed, then this displays the hostname, alias, or MAC address of the UniFi Switch. You can click the name to get additional details. For more information, see **"UniFi Switch Details" on page 121**.

Name Displays the name of the port.

PoE Displays the PoE setting:

- **(blank)** PoE is disabled.
- **24V Passive** 24V passive PoE is enabled.
- **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.
- **__W** Power output is displayed in watts.

PoE Detection Displays the PoE status:

- **(blank)** PoE is disabled.
- **Not detected** No 802.3at/af device is detected.
- **Passive** 24V passive PoE is enabled.
- **Good** An 802.3at/af device is plugged in and automatically receiving PoE.

PD Class Displays the PD (Powered Device) class of the detected device, if applicable; this indicates its power requirements.

Power Displays the power output in watts, if applicable.

Voltage Displays the voltage output, if applicable.

Current Displays the current output in amperes, if applicable.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the port settings. For more information, see **"UniFi Switch Details" on page 121**.
- **Clear Counters** Click CLEAR COUNTERS to clear the port statistics.
- **Power Cycle** If applicable, click POWER CYCLE to power cycle the port.

Counters

Port The ports display their status and port number:

- Indicates a 10/100 Mbps connection.
- Indicates a 1 Gbps (1000 Mbps) connection.
- Indicates a 10 Gbps connection.
- Indicates 1 Gbps (1000 Mbps) connection with PoE.
- Indicates the connection is disabled (no network or VLAN is enabled).
- Indicates no connection (the network or VLAN is enabled, but the port is not in use).
- Indicates a uplink.

Switch If all switches are displayed, then this displays the hostname, alias, or MAC address of the UniFi Switch. You can click the name to get additional details. For more information, see **"UniFi Switch Details" on page 121**.

TX Bytes Displays in purple the number of bytes transmitted.

TX Frames Displays in purple the number of frames transmitted.

TX Multicast Displays in purple the number of multicast packets transmitted.

TX Broadcast Displays in purple the number of broadcast packets transmitted.

TX Errors Displays in purple the number of error packets transmitted.

RX Bytes Displays in green the number of bytes received.

RX Frames Displays in green the number of frames received.

RX Multicast Displays in green the number of multicast packets received.

RX Broadcast Displays in green the number of broadcast packets received.

RX Errors Displays in green the number of error packets received.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the port settings. For more information, see **"UniFi Switch Details" on page 121**.
- **Clear Counters** Click CLEAR COUNTERS to clear the port statistics.
- **Power Cycle** If applicable, click POWER CYCLE to power cycle the port.

Port Forward Stats

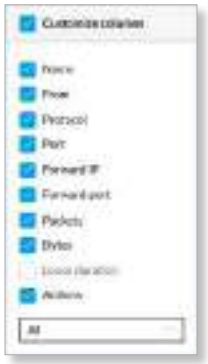
This screen displays information about the port forwarding entries used by the UniFi Security Gateway.

You can apply one of the following primary filters:

- **All** Displays all port forwarding entries.
- **User-Defined** Displays the user-defined port forwarding entries.
- **UPnP** Displays the UPnP port forwarding entries.

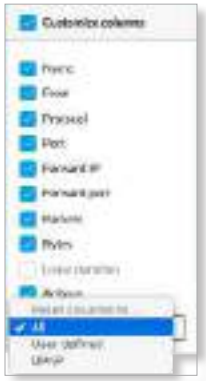
Customize Columns Click to customize the columns used for display.

Select **Customize columns**.



You can add or remove columns for display.

- **Reset columns to** Click the drop-down at the bottom of the *Customize columns* screen to display the *Reset columns to ...* options.
  - **All** The *Name*, *From*, *Protocol*, *Port*, *Forward IP*, *Forward Port*, *Packets*, *Bytes*, *and Actions* columns are displayed.
  - **User Defined** The *Name*, *From*, *Protocol*, *Port*, *Forward IP*, *Forward Port*, *Packets*, *Bytes*, and *Actions* columns are displayed.
  - **UPnP** The *Name*, *Protocol*, *Port*, *Forward IP*, *Forward Port*, *Packets*, *Bytes*, and *Lease Duration* columns are displayed.



All

Name Displays the name of the port forwarding entry.

From Displays the source IP address, if specified, or *Anywhere*.

Protocol Displays the protocol that will be forwarded.

Port Displays the port or ports that will be forwarded to the LAN. Also known as the external port(s).

Forward IP Displays the destination IP address that will receive the forwarded port traffic.

Forward Port Displays the destination port or ports that will receive the forwarded port traffic. Also known as the internal port(s).

Packets Displays the number of packets transferred.

Bytes Displays the number of bytes transferred.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the UniFi Security Gateway settings. For more information, see **"UniFi Security Gateway Details" on page 115**.

User-Defined

Name Displays the name of the port forwarding entry.

From Displays the source IP address, if specified, or *Anywhere*.

Protocol Displays the protocol that will be forwarded.

Port Displays the port or ports that will be forwarded to the LAN. Also known as the external port(s).

Forward IP Displays the destination IP address that will receive the forwarded port traffic.

Forward Port Displays the destination port or ports that will receive the forwarded port traffic. Also known as the internal port(s).

Packets Displays the number of packets transferred.

Bytes Displays the number of bytes transferred.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the UniFi Security Gateway settings. For more information, see **"UniFi Security Gateway Details" on page 115**.

UPnP

Name Displays the name of the port forwarding entry.

Protocol Displays the protocol that will be forwarded.

Port Displays the port or ports that will be forwarded to the LAN. Also known as the external port(s).

Forward IP Displays the destination IP address that will receive the forwarded port traffic.

Forward Port Displays the destination port that will receive the forwarded port traffic. Also known as the internal port.

Packets Displays the number of packets transferred.

Bytes Displays the number of bytes transferred.

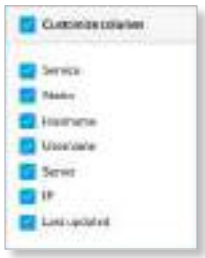
Lease Duration Displays the uptime of the port forwarding entry.

Dynamic DNS

This screen displays information about the use of DDNS services.

Customize Columns Click to customize the columns used for display.

Select **Customize columns**.



You can add or remove columns for display.

Service Displays the name of the DDNS service.

Status Displays the status of the latest DDNS update.

Hostname Displays the hostname registered with the DDNS service.

Username Displays the username of the DDNS account.

Server Displays the IP address or hostname of the DDNS server that should receive DDNS updates.

IP Displays the WAN (public) IP address of the hostname.

Last Updated Displays the duration of time since the hostname IP address was last updated.

Actions Click a button to perform the desired action:

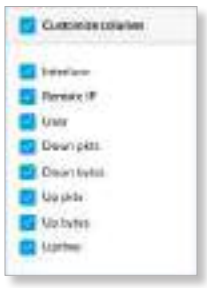
- **Edit** Click EDIT to make changes to the UniFi Security Gateway settings. For more information, see **"UniFi Security Gateway Details" on page 115**.

Remote User VPN

This screen displays information about the remote user VPN connections.

Customize Columns Click to customize the columns used for display.

Select **Customize columns**.



You can add or remove columns for display.

Interface Displays the interface being used.

Remote IP Displays the IP address of the remote user.

User Displays the username of the remote user.

Down Pkts Displays the amount of data downloaded as packets.

Down Bytes Displays the amount of data downloaded as bytes.

Up Pkts Displays the amount of data uploaded as packets.

Up Bytes Displays the amount of data uploaded as bytes.

Uptime Displays the duration of time the VPN tunnel has been active without interruption.

Actions Click a button to perform the desired action:

- **Terminate** Click TERMINATE to end the VPN tunnel.

AC-EDU Streams

This screen displays status information about the streaming by the UniFi AC EDU Access Points.

Customize Columns Click to customize the columns used for display.

Select **Customize columns**.

You can add or remove columns for display.

- **Reset columns to** Click the drop-down at the bottom of the *Customize columns* screen to display the *Reset columns to* ... options.
  - **All** The *Device*, *Stream*, *Ready*, *Streaming*, and *Connected* columns are displayed.

Terminate Stream Click TERMINATE and then click the live stream you want to terminate.

Device Displays the hostname, alias, or MAC address of the UniFi AC EDU AP. You can click the name to get additional details. For more information, see **"UniFi Access Point Details" on page 131**.

Stream Displays the unique identifier for this live stream.

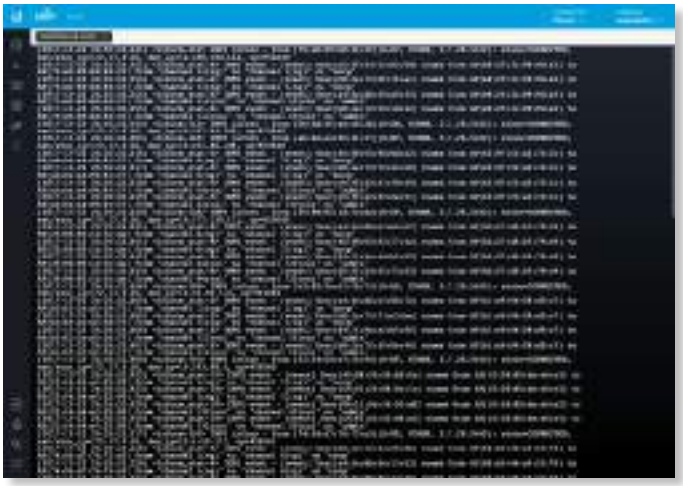
Ready Displays the status of the UniFi AC EDU AP, *Yes* or *No*.

Streaming Displays the duration of the live streaming, *Yes* or *No*.

Connected Displays the status of the connection, *Yes* or *No*.

Controller Logs

This screen displays device, management, and system log entries.



Chapter 10: UniFi Security Gateway Details

The UniFi Security Gateway hyperlink opens the UniFi Security Gateway's *Details* window either in the *Properties* panel or as a separate popup window. You can always dock this window in the *Properties* panel or detach it as a separate window.

Properties

The *Properties* panel appears on the right side of the screen. Information about each selected device appears as a popup within this panel.

Remove All Click to close the *Properties* panel.

Collapse All Click to collapse all of the popups to rows.

The top of the popup remains and displays the following:

- **Display** Click + to display the device information.
- **(icon)** Displays the icon of the device (the icon will vary depending on the model).
- **(status)** Displays to indicate the device status.
  - **Pending Approval** A solid orange circle indicates the default state, available for adoption.
  - **Connected** A solid green circle indicates a managed connection.
  - **Managed by Other** A solid gray circle indicates that the device is not in the default state but not controlled by the current UniFi Controller.
  - **Disconnected** A red warning icon indicates no connection.
- **Name/MAC Address** Displays the device name or MAC address of the device.
- **Restart** Click to restart the selected device.
- **Locate** Click to flash the LED on the device and the device icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Upgrade** Click to upgrade the device. (This icon does not appear if an upgrade is not available or there are pending changes.)
- **Undock from Properties Panel** Click to display the same information in a separate popup screen that can be moved anywhere within the browser screen.
- **Close Properties** Click to close the device popup.

Hide Property Panel Click to hide the *Properties* panel but allow the device popups to remain accessible from this panel. Click the *properties* icon to re-open it.

The upper part of the detached popup screen has an icon for each port.

Indicates a 10/100 Mbps connection.

Indicates a 1 Gbps (1000 Mbps) connection.

Indicates the connection is disabled (no network or VLAN is enabled).

Indicates no connection (the network or VLAN is enabled, but the port is not in use).

There are three clickable tabs:

- **"UniFi Security Gateway – Details" on page 116**
- **"UniFi Security Gateway – Networks" on page 117**
- **"UniFi Security Gateway – Configuration" on page 117**

UniFi Security Gateway – Details

Click **Details** to display the device specifics, LAN/WAN connection details, and uptime.

Overview

MAC Address Displays the MAC address or unique hardware identifier of the Gateway.

Model Displays the model name of the Gateway.

Version Displays the version number of the Gateway's firmware.

LAN IP Address Displays the local IP address of the Gateway.

Uptime Displays the duration of time the Gateway has been running without interruption.

PHY Displays the temperature of the circuitry for the PHY (physical) layer functions.

CPU Displays the temperature of the CPU.

Board (PHY) Displays the temperature of the PHY board.

Board (CPU) Displays the temperature of the CPU board.

WAN 1

The number of *WAN* sections will vary depending on the number of active WAN ports.

IP Address Displays the WAN (public) IP address of the WAN interface.

Speed Displays the connection speed in Mbps.

Duplex Displays the mode, *Full Duplex* or *Half Duplex*.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Down Activity Displays the level of download activity in bytes per second.

Up Activity Displays the level of upload activity in bytes per second.

Performance (Last 24 H)

CPU (%) The graph displays the percentage of CPU processing power used during the last 24 hours.

Memory (%) The graph displays the percentage of memory used during the last 24 hours.

UniFi Security Gateway – Networks

Click **Networks** to display the network name, IP address, TX and RX throughput, and number of clients.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Network Displays the name of the network.

IP Displays the local IP address of the network.

TX Displays the outgoing (transmit) throughput.

RX Displays the incoming (receive) throughput.

 # Clients Displays the number of clients on the network.

UniFi Security Gateway – Configuration

Click **Configuration** to configure the alias, WAN settings, port forwarding, Dynamic DNS, and custom upgrade entries. You can also remove the Gateway from management by this UniFi Controller.

Additional options are available in the Settings section. Go here for more information:

- **"Settings > Routing & Firewall" on page 31**
- **"Settings > Networks" on page 27**
- **"Settings > Services" on page 48**

General

Alias Displays the customizable name or identifier of the Gateway. The *Alias* is also known as the host name.

LED Select the appropriate option: **Use site settings** (default), **On**, or **Off**. For more information about site settings, go to **"Settings > Site" on page 21**.

Save Click to apply changes.

Cancel Click to discard changes.

WAN 1/2

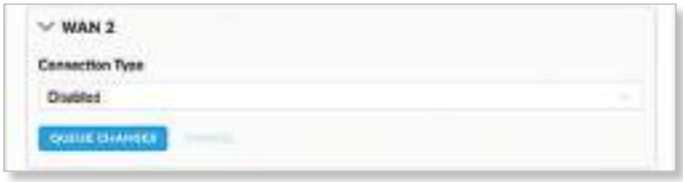
Connection Type Select the internet connection type for your service.

- **Using DHCP** The use of the Dynamic Host Configuration Protocol (DHCP) is the default. The Gateway automatically acquires network settings from the service provider's DHCP server.
  - **Preferred DNS** Enter the IP address of the service provider's primary DNS server.
  - **Alternate DNS** Enter the IP address of the service provider's secondary DNS server.

- **Static IP** The service provider assigns fixed network settings to your service for manual entry. Enter the following information:
  - **IP Address** Enter the internet IP address of the Gateway.
  - **Subnet Mask** Enter the subnet mask of the Gateway.
  - **Router** Enter the IP address of the service provider's gateway router.
  - **Preferred DNS** Enter the IP address of the service provider's primary DNS server.
  - **Alternate DNS** Enter the IP address of the service provider's secondary DNS server.

- **PPPoE** Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. Enter the following information:
  - **Username** Enter the username used to connect to the PPPoE server.
  - **Password** Enter the password used to connect to the PPPoE server.
  - **Preferred DNS** Enter the IP address of the service provider's primary DNS server.
  - **Alternate DNS** Enter the IP address of the service provider's secondary DNS server.

- **Disabled** If you are not using the *WAN 2* port, then select **Disabled**.



Use VLAN ID To use a VLAN, select **Use VLAN ID** and enter the VLAN ID number.

Load Balancing (Available for *WAN 2* if *Using DHCP*, *Static IP*, or *PPPoE* is enabled.) Set up basic load balancing with two internet connections from different Internet Service Providers (ISPs).

- **Failover only** Select this option if you want to use *WAN 2* only if *WAN 1* fails.

- **Weighted LB** Select this option if you want the load balanced between the two WAN ports. Then enter a weight in the field provided; the default is *50*.

Smart Queues The Smart Queue feature provides FQ-CODEL (Fair Queuing with Controlled Delay) + HTB (Hierarchical Token Bucket) function and supports dynamic interfaces, even if the dynamic interfaces do not exist yet (the policy will be applied later when the interface comes up).

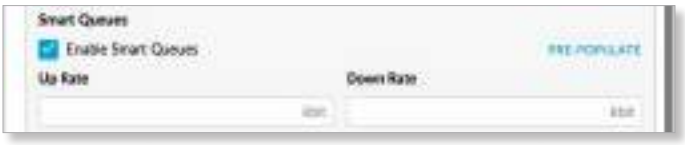
The HTB rate limiting is computation-intensive, so the rate limiting will not work well (cannot achieve the specified rate) above a certain threshold rate. The actual threshold (applied to the sum of the upload and download rates) depends on the specific Gateway model and conditions of the actual environment.

It may require some testing to find the actual threshold in a specific environment, depending on the actual setup, traffic patterns, and other conditions. You can use the *Pre-Populate* option as a starting point for the *Up* and *Down Rates*. The actual rate limits will be set to 95% of the specified value, so you can experiment with different values if necessary.

The smart queue policy applies to a single interface. If you are using more than one WAN interface, then you would configure a separate smart queue policy for the *WAN 2* port in the *WAN 2* section.

- **Pre-Populate** Click **Pre-Populate** to set the *Up* and *Down Rates* to 80% of the last speed test results.
- **Up Rate** Enter the bandwidth limit in Kbits/sec.
- **Down Rate** Enter the bandwidth limit in Kbits/sec.

Note: If you enable the *Smart Queues* option, then you will not be able to use the *DPI* feature as traffic will not be offloaded.

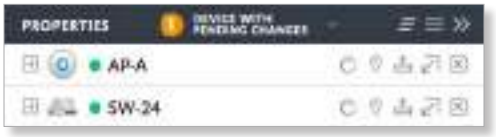


Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.



Apply Click ✓ APPLY to save changes.

Discard Click × DISCARD to cancel changes.

Advanced

The *Advanced* section offers a variety of options for advanced users.

MSS Clamping

MSS (Maximum Segment Size) clamping is typically used when Path MTU Discovery is not working properly.

Using ICMP messages, Path MTU Discovery determines the highest allowable MTU (Maximum Transmission Unit) of traffic traveling between two hosts to avoid fragmentation.

TCP uses MSS, which is the MTU minus the IP and TCP headers. The sender should limit its data so it does not exceed the MSS reported by the receiver.

Sometimes security firewalls or other issues interfere with the Path MTU Discovery process (for example, ICMP messages are blocked), so you can use a workaround, TCP MSS clamping, which sets the MSS value for all TCP connections.

MSS Clamping Select the appropriate option: **Auto** (default), **Custom**, or **Disabled**. If you select *Custom*, enter the MSS value in the field provided. *1412* is the default.

Hardware Offload

You have three options available:

Enable hardware offload Enabled by default. This option can significantly improve packet forwarding performance while reducing CPU utilization. (If you enable the Smart Queue feature, then it bypasses hardware offload.)

Enable offload scheduler Reserved for future use. This option will implement rate limiting on user groups.

Enable offload layer 2 blocking Reserved for future use. This option will offload blocking of hosts to the hardware.

Echo Server

You can monitor latency by pinging a server on the internet. (An ICMP echo request is sent, and then an answer is received.)

Echo Server Select **ping.ubnt.com** (default), or select the custom option and enter the IP address or hostname to ping for the latency monitor.

Apply Click to save changes.

Cancel Click to discard changes.

Manage Device

There are three options to manage the UniFi Security Gateway.

Custom Upgrade

For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, select this option.

(URL) Enter the location URL of the firmware.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Force Provision

You can force a provision to apply the latest settings to a device. It ensures that the device is in sync with all of the applicable settings in the UniFi Controller, like a settings reset so the device has the settings it should have.

Provision Apply the latest settings to the Gateway.

Forget This Device

Forget Click **Forget** to remove the Gateway from management by the UniFi Controller software and reset it to factory default settings.

Move this device to... If you want to move the device to another site, select the appropriate site from the drop-down list.

Note: Use caution when clicking *Forget*. This will restore the Gateway to factory default settings while it is in a *Connected* state.

Chapter 11: UniFi Switch Details

A UniFi Switch hyperlink opens the UniFi Switch's *Details* window either in the *Properties* panel or as a separate popup window. You can always dock this window in the *Properties* panel or detach it as a separate window.

Properties

The *Properties* panel appears on the right side of the screen. Information about each selected device appears as a popup within this panel.

Remove All Click to close the *Properties* panel.

Collapse All Click to collapse all of the popups to rows.

The top of the popup remains and displays the following:

- **Display** Click + to display the device information.
- **(icon)** Displays the icon of the device (the icon will vary depending on the model).
- **(status)** Displays to indicate the device status.
  - **Pending Approval** A solid orange circle indicates the default state, available for adoption.
  - **Connected** A solid green circle indicates a managed connection.
  - **Managed by Other** A solid gray circle indicates that the device is not in the default state but not controlled by the current UniFi Controller.
  - **Disconnected** A red warning icon indicates no connection.
- **Name/MAC Address** Displays the device name or MAC address of the device.
- **Restart** Click to restart the selected device.
- **Locate** Click to flash the LED on the device and the device icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Upgrade** Click to upgrade the device. (This icon does not appear if an upgrade is not available or there are pending changes.)
- **Undock from Properties Panel** Click to display the same information in a separate popup screen that can be moved anywhere within the browser screen.
- **Close Properties** Click to close the device popup.

Hide Property Panel Click to hide the *Properties* panel but allow the device popups to remain accessible from this panel. Click the *properties* icon to re-open it.

The upper part of the detached popup screen has an icon for each port.

- Indicates a 10/100 Mbps connection.
- Indicates a 1 Gbps (1000 Mbps) connection.
- Indicates a 10 Gbps connection.
- Indicates 1 Gbps (1000 Mbps) connection with PoE.
- Indicates the connection is disabled (no network or VLAN is enabled).
- Indicates no connection (the network or VLAN is enabled, but the port is not in use).
- Indicates STP blocking.
- Indicates mirroring mode.

Place your cursor over a port to view details.

- **Port** Displays the port number.
- **Name** Displays the name of the port.
- **Status** Displays the connection speed and duplex mode.
- **TX** Displays the amount of data transmitted.
- **RX** Displays the amount of data received.

- **PoE** (Not applicable to the SFP ports.) Displays the PoE setting:
  - **Off** PoE is disabled.
  - **24V Passive** 24V passive PoE is enabled.
  - **__W** Power output is displayed in watts.
  - **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.
- **Profile** Displays the switch port profile. The default is *All*.
- **Uplink/Downlink** Displays the name of the uplink or downlink device.

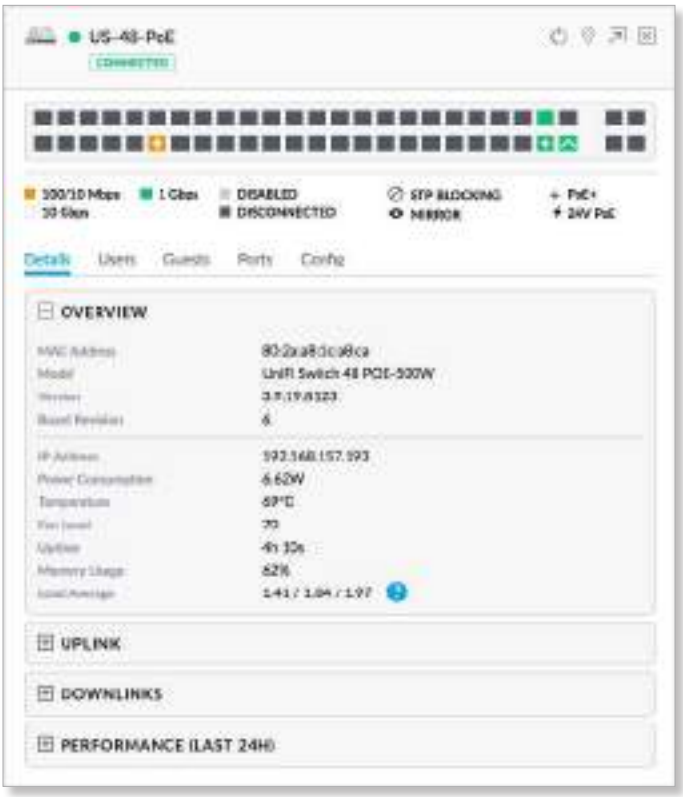
There are four clickable tabs:

- *Details*
- **"UniFi Switch – Users" on page 123**
- **"UniFi Switch – Guests" on page 123**
- **"UniFi Switch – Ports" on page 124**
- **"UniFi Switch – Configuration" on page 127**

UniFi Switch – Details

Click **Overview** to display the device specifics, connection details, and uptime.

Overview



MAC Address Displays the MAC address or unique hardware identifier of the Switch.

Model Displays the model name of the Switch.

Version Displays the version number of the Switch's firmware.

Board Revision Displays the revision number of the hardware board.

IP Address Displays the IP address of the Switch.

Power Consumption Displays the amount of power used by the Switch.

Temperature Displays the general temperature of the Switch.

Fan Level If the Switch has a fan, then the *Fan Level*, from *0* to *100*, is displayed. If the Switch does not have a fan, then the *Fan Level* is not displayed.

Uptime Displays the duration of time the Switch has been running without interruption.

Memory Usage Displays the percentage of memory used.

Load Average Displays the number of jobs in the run queue or waiting for input/output averaged over 1, 5, and 15 minutes.

Uplink

Port Displays the port number.

Uplink Displays the name or MAC address of the uplink device. You can click the name to get additional details.

Speed Displays the connection speed in Mbps.

Duplex Displays the mode, *Full Duplex* or *Half Duplex*.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the number of packets and total bytes uploaded by the device.

Activity Displays the level of activity in bytes per second.

Downlinks

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Port Displays the number of the connected port.

Device Displays the name or MAC address of the downlink device. You can click the name to get additional details.

Status Displays the connection speed and duplex mode.

Model Displays the model number of the downlink device.

Performance (Last 24 H)

CPU (%) The graph displays the percentage of CPU processing power used during the last 24 hours.

Memory (%) The graph displays the percentage of memory used during the last 24 hours.

UniFi Switch – Users

Click **Overview** to display the device specifics, connection details, and uptime.

Overview

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; see **"Client Details" on page 147** for more information.

IP Address Displays the IP address assigned to the client.

UniFi Switch – Guests

Click **Overview** to display the device specifics, connection details, and uptime.

Overview

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Name Displays the hostname, alias, or MAC address of the connected client. You can click the name to get additional details; see **"Client Details" on page 147** for more information.

IP Address Displays the IP address assigned to the client.

UniFi Switch – Ports

Click **Ports** to display the port name, status, TX and RX throughput, PoE setting, and profile.

Displays the port number.

Name Displays the name of the port.

Status Displays the connection speed and duplex mode.

TX Displays the amount of data transmitted.

RX Displays the amount of data received.

PoE Displays the PoE setting:

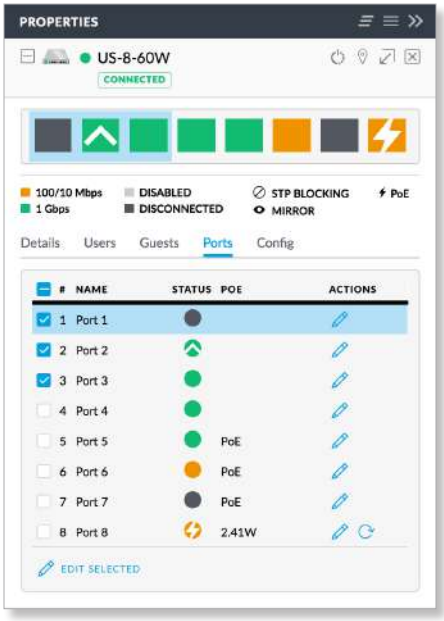
- **Off** PoE is disabled.
- **24V Passive** 24V passive PoE is enabled.
- **__W** Power output is displayed in watts.
- **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.

Profile Displays the switch port profile. The default is *All*.

Actions Click a button to perform the desired action:

- **Edit** Click to change the port configuration. Proceed to the following section, *Port Configuration*.
- **Powercycle** (Available only if the connected devices uses PoE.) Click to restart the connected device.

Edit Selected Select multiple ports and click EDIT SELECTED to make the same changes to those selected ports.



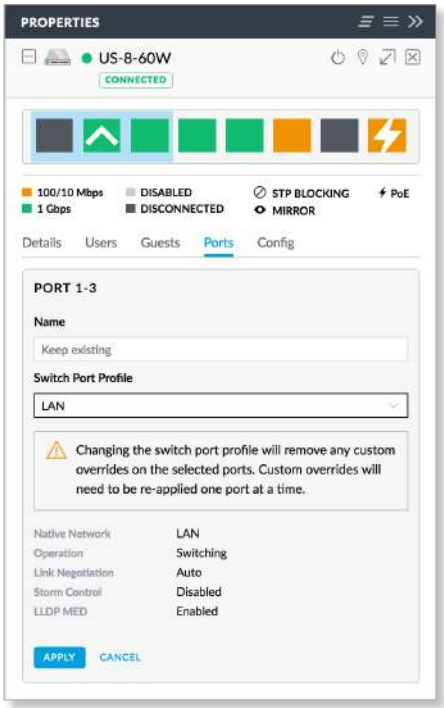
Name The existing names are kept.

Switch Port Profile Select the appropriate profile from the drop-down list. Custom overrides will be removed from the selected ports, so they will need to be re-applied, one port at a time.

For the selected profile, the *Native Network, Operation, Link Negotiation, Storm Control*, and *LLDP MED* settings are displayed.

Apply Click to save changes.

Cancel Click to discard changes.



Port Configuration

Port

- **Port __** Displays the number of the port.
- **Name** Displays the customizable name or identifier of the port.
- **Switch Port Profile** Displays the switch port profile. The default is *All*. To configure a profile, go to **"Switch Ports" on page 46** for more information.

Profile Overrides

You can override the configuration of a profile.

Note: Settings marked with * will override the profile default.

- **PoE** All ports are set to auto-sensing *PoE+* by default.
  - **Off** Disable PoE.
  - **24V Passive** Select this option to power devices that support 24V passive PoE.

    Note: Before activating 24V passive PoE, ensure that the connected device supports PoE and the supplied voltage.
  - **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.
- **Operation** Select the operation mode for this port. **Switching**, **Mirroring**, or **Aggregate**. Proceed to the appropriate section.

Switching

- **Switching** The default mode.
  - **Link Negotiation** The default is *Auto*, enabling Ethernet autonegotiation. This is the appropriate configuration for almost all circumstances. Never use *Manual* unless the device being connected to the port has also been set manually; if so, then switch to **Manual** to disable autonegotiation and enable manual configuration of duplex and speed:
    - **Full Duplex** (Available for RJ45 ports only.) If this option is enabled, the port will be set to full duplex. If disabled, it will be set to half duplex. Full-duplex transmission is enabled by default.
    - **Link Speed** Set the link speed of the interface as needed to match the device plugged into the port. For RJ45 ports, select **1000 Mbps**, **100 Mbps**, or **10 Mbps**. For SFP+ ports, select **10 Gbps** or **1000 Mbps**. SFP ports must be set to **1000 Mbps**.
- **Isolation** Select this option to mark this port as an isolated port. Isolated ports cannot communicate directly with any other isolated port.
- **Storm Control** Monitor the unicast, multicast, and/or broadcast traffic for this port. If the specified type of traffic on this port exceeds the threshold rate you specify, then the UniFi Switch drops the excess traffic.
  - **Unicast** Select this option to monitor unicast traffic. Enter the threshold value in packets per second.
  - **Multicast** Select this option to control unicast traffic destined to unknown MAC addresses. Enter the threshold in packets per second.

Note: Unlike *Broadcast* and *Multicast* storm control, the *Unicast* storm control does not apply to all unicast traffic. It applies only to traffic destined to a MAC address not found in the switch's MAC address table. Most devices should have a very low rate of such traffic. High rates of such traffic are indicative of malicious activity, or a broken device. Blocking excessive rates of such traffic may prevent problems on other devices on the network.

  - **Broadcast** Select this option to monitor broadcast traffic. Enter the threshold in packets per second.

- **LLDP-MED** You can use LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and configuration of IP phones.
  - **Enable LLDP-MED** Enabled by default.
  - **Enable topology change notification** Disabled by default. This allows the Switch to receive notifications about any IP phone topology changes.

- **Apply** Click to save changes.
- **Remove Overrides** Click to discard profile overrides.
- **Cancel** Click to discard changes.

Mirroring

- **Mirroring** This port's network traffic will receive the mirrored traffic from the port listed below for analysis:
  - **Mirroring Port** Enter the number of the port that will be mirrored.
  - **Link Negotiation** The default is *Auto*, enabling Ethernet autonegotiation. This is the appropriate configuration for almost all circumstances. Never use *Manual* unless the device being connected to the port has also been set manually; if so, then switch to **Manual** to disable autonegotiation and enable manual configuration of duplex and speed:
    - **Full Duplex** (Available for RJ45 ports only.) If this option is enabled, the port will be set to full duplex. If disabled, it will be set to half duplex. Full-duplex transmission is enabled by default.
    - **Link Speed** Set the link speed of the interface as needed to match the device plugged into the port. For RJ45 ports, select **1000 Mbps**, **100 Mbps**, or **10 Mbps**. For SFP+ ports, select **10 Gbps** or **1000 Mbps**. SFP ports must be set to **1000 Mbps**.
  - **Isolation** Select this option to mark this port as an isolated port. Isolated ports cannot communicate directly with any other isolated port.
- **Apply** Click to save changes.
- **Remove Overrides** Click to discard profile overrides.
- **Cancel** Click to discard changes.

Aggregate

- **Aggregate** A port channel, also known as a Link Aggregation Group (LAG), combines multiple links into a single logical link (single IP address) for load balancing and/or redundancy. If you select this option, then this port becomes the start port of the aggregate link.
  - **Aggregate Ports** Enter the end port number of the LAG. (Two to four ports are permitted per LAG.)
  - **Link Negotiation** The default is *Auto*, enabling Ethernet autonegotiation. This is the appropriate configuration for almost all circumstances. Never use *Manual* unless the device being connected to the port has also been set manually; if so, then switch to **Manual** to disable autonegotiation and enable manual configuration of duplex and speed:
    - **Full Duplex** (Available for RJ45 ports only.) If this option is enabled, the port will be set to full duplex. If disabled, it will be set to half duplex. Full-duplex transmission is enabled by default.
    - **Link Speed** Set the link speed of the interface as needed to match the device plugged into the port. For RJ45 ports, select **1000 Mbps**, **100 Mbps**, or **10 Mbps**. For SFP+ ports, select **10 Gbps** or **1000 Mbps**. SFP ports must be set to **1000 Mbps**.

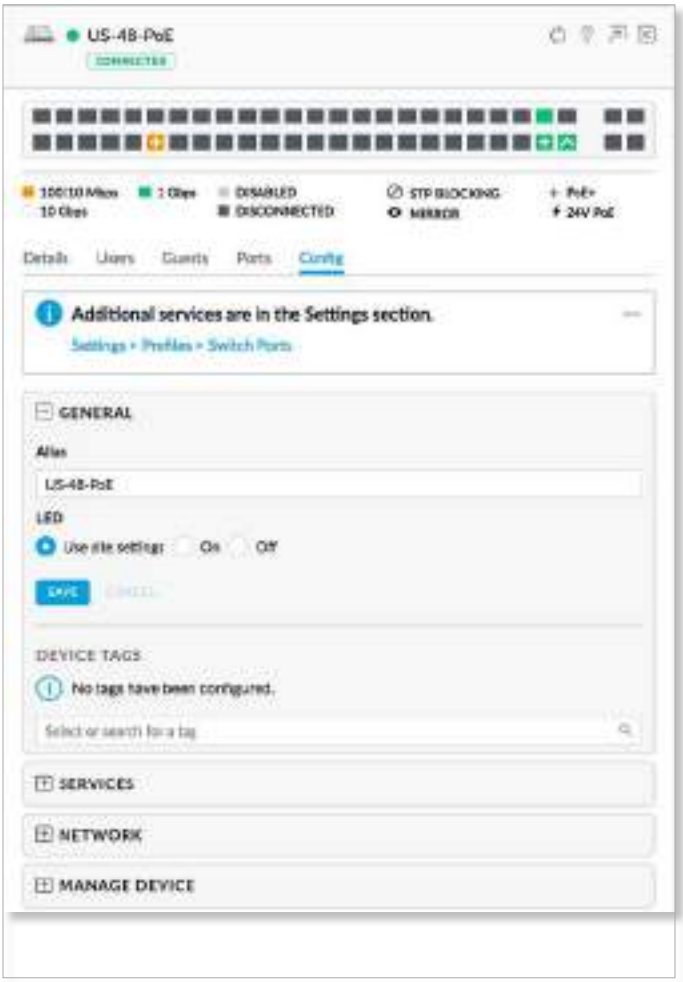
- **Apply** Click to save changes.
- **Remove Overrides** Click to discard profile overrides.
- **Cancel** Click to discard changes.

UniFi Switch – Configuration

Click **Configuration** to configure the alias, network/VLANs, services, and network settings. You can also use this tab to copy another switch's configuration to this Switch, perform a custom upgrade, gain terminal access to the Switch, or remove the Switch from management.

Additional options are available in the Settings section. Go to **"Switch Ports" on page 46** for more information.

General



Alias Displays the customizable name or identifier of the Switch. The *Alias* is also known as the host name.

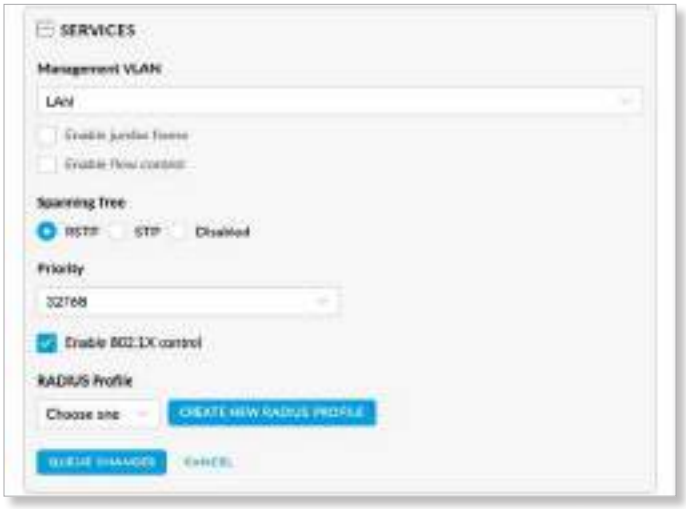
LED Select the appropriate option: **Use site settings** (default), **On**, or **Off**. For more information about site settings, go to **"Settings > Site" on page 21**.

Device Tags Select or search for a device tag. You can also enter a keyword and press **Enter** to save a new device tag.

Save Click to apply changes.

Cancel Click to discard changes.

Services



Management VLAN The Management VLAN specifies the VLAN ID that will be used for the management IP address of the switch. The IP configuration configured under the switch's *Network* panel will be applied to this VLAN ID.

Enable Jumbo Frame Disabled by default. The Maximum Transmission Unit (MTU) is the maximum packet size (in bytes) that a network interface can transmit or receive. The standard Ethernet MTU is 1500 bytes. Enable jumbo frames to allow usage of MTUs up to 9216 bytes on all ports of this switch.

Enable Flow Control Disabled by default. Enabling this option will enable 802.3x Ethernet Flow Control on all ports of this switch. This should remain disabled, unless you have a specific requirement for 802.3x and understand its implications.

Spanning Tree Ethernet networks cannot have multiple active paths between switches (absent aggregation such as LAG), as this causes a switching loop, where broadcast and multicast traffic are amplified and repeated in a never-ending loop, melting down the entire network. Spanning Tree prevents switching loops, and allows for redundant interconnections between switches. Interfaces with redundant paths are put into STP blocking mode, leaving the port down unless the current best active path fails.

Select the appropriate option: **RSTP** (Rapid Spanning Tree Protocol), **STP** (Spanning Tree Protocol), or **Disabled**. RSTP is the default and is recommended because topology changes apply much more quickly (usually within 6 seconds, rather than the 30-50 seconds of STP). STP will enable the older 802.1D STP on this switch instead of RSTP. Disabled will disable all versions of spanning tree; however, this is not recommended, as it can leave the network susceptible to being taken down by an inadvertently created switching loop.

Priority STP uses the priority value as part of the calculation in electing a root bridge of the spanning tree. It is best to configure a lower priority number (higher preference in root bridge elections) on one or two of the switches you consider the "core" of your network. For instance, if you have two 10 Gb switches, and several gigabit switches, configure a lower priority on the two 10 Gb switches to ensure that they are preferred as the STP root bridge. The default is *32768*.

Enable 802.1x control Select this option to use a RADIUS server for user authentication on the switch's ports. The following options appear.

- **RADIUS Profile** Specify a RADIUS profile:
  - Select a RADIUS profile from the drop-down list, or
  - Click **Create New RADIUS Profile** to create a new RADIUS profile. Refer to **"Create or Edit a RADIUS Profile" on page 45** for detailed information.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

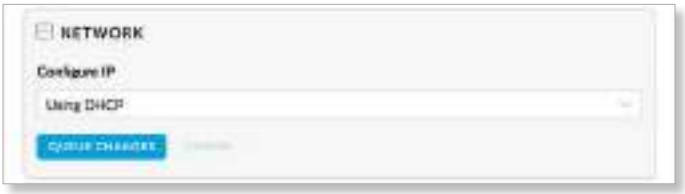
Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.

- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

Network

Configure IP Select the management IP configuration of the switch, **Using DHCP** or **Static IP**.

- **Using DHCP** The use of the Dynamic Host Configuration Protocol (DHCP) is the default. The Switch automatically acquires network settings from the network's DHCP server.



- **Static IP** Assign fixed network settings to the Switch. Enter the following information:
  - **IP Address** Enter the IP address for the Switch.
  - **Subnet Mask** Enter the subnet mask of the Switch.
  - **Gateway** Enter the IP address of the gateway (for example, the UniFi Security Gateway).
  - **Preferred DNS** Enter the IP address of the primary DNS server.
  - **Alternate DNS** Enter the IP address of the secondary DNS server.
  - **DNS Suffix** Enter the Fully Qualified Domain Name (FQDN) without the hostname.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen, or click *Cancel* to discard changes. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the **Properties** panel. Click ⌄ to display the devices.

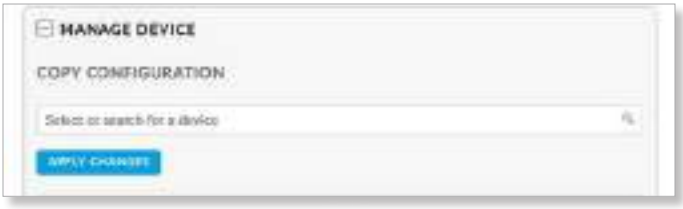
- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

Manage Device

There are four options to manage the UniFi Switch.

Copy Configuration

If you have settings that you want to apply to multiple Switches, use this option to copy the configuration.



Select or search for a device Select or search for the appropriate Switch whose configuration will be copied to this Switch.

Apply Changes Click to overwrite its current configuration with the configuration of the selected Switch.

Custom Upgrade

For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, select this option.

(location URL) Enter the UL of the firmware's location.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Force Provision

You can force a provision to apply the latest settings to a device. It ensures that the device is in sync with all of the applicable settings in the UniFi Controller, like a settings reset so the device has the settings it should have.

Provision Apply the latest settings to the Switch.

Forget This Device

Forget Click **Forget** to remove the Switch from management by the UniFi Controller software and reset it to factory default settings.

Note: Use caution when clicking *Forget*. This will restore the Switch to factory default settings while it is in a *Connected* state.

Chapter 12: UniFi Access Point Details

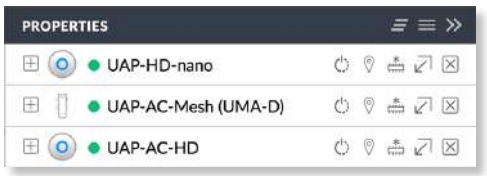
A UniFi AP hyperlink opens the UniFi AP's *Details* window either in the *Properties* panel or as a separate popup window. You can always dock this window in the *Properties* panel or detach it as a separate window.

Properties

The *Properties* panel appears on the right side of the screen. Information about each selected device appears as a popup within this panel.

Remove All Click to close the *Properties* panel.

Collapse All Click to collapse all of the popups to rows.



The top of the popup remains and displays the following:

- **Display** Click + to display the device information.
- **(icon)** Displays the icon of the device (the icon will vary depending on the model).
- **(status)** Displays to indicate the device status.
  - **Pending Approval** A solid orange circle indicates the default state, available for adoption.
  - **Connected** A solid green circle indicates a managed connection.
  - **Managed by Other** A solid gray circle indicates that the device is not in the default state but not controlled by the current UniFi Controller.
  - **Disconnected or Isolated** A red warning icon indicates no connection. To establish a connection to the UniFi Controller, perform one of the following actions:
    - Reconnect the AP to the gateway or router.
    - Connect an Ethernet cable from the *Secondary Ethernet Port* (if available) of the isolated AP to the *Secondary Ethernet Port* (if available) of another UniFi AP that is connected to the gateway or router.
    - Establish a wireless uplink to a wired AP.
- **Name/MAC Address** Displays the device name or MAC address of the device.
- **Restart** Click to restart the selected device.
- **Locate** Click to flash the LED on the device and the device icon on the *Map* tab so you can locate it. The LED will flash until the *Locate* button is clicked again. (The icon on the *Map* tab will flash three times and stop.)
- **Upgrade** Click to upgrade the device. (This icon does not appear if an upgrade is not available or there are pending changes.)
- **Undock from Properties Panel** Click to display the same information in a separate popup screen that can be moved anywhere within the browser screen.
- **Close Properties** Click to close the device popup.

Hide Property Panel Click to hide the *Properties* panel but allow the device popups to remain accessible from this panel. Click the *properties* icon to re-open it.

Here are the clickable tabs:

- **"UniFi Access Point – Details" on page 132**
- **"UniFi Access Point – Users" on page 134**
- **"UniFi Access Point – Guests" on page 134**
- **"UniFi Access Point – Configuration" on page 135**
- **"UniFi Access Point – Tools" on page 141**

(2.4 GHz) Displays the active channel with a bar graph indicating its percentages of the following: *RX Frames* (green), *TX Frames* (light green), *Interference* (amber), and *Free* bandwidth (gray). The percentage of channel utilization is also displayed with the corresponding evaluation.

(5 GHz) Displays the active channel with a bar graph indicating its percentages of the following: *RX Frames* (green), *TX Frames* (light green), *Interference* (amber), and *Free* bandwidth (gray). The percentage of channel utilization is also displayed with the corresponding evaluation.

You can click a point on either bar graph for more details:

- **TX Pkts/Bytes** Displays the amount of data transmitted as packets and bytes.
- **RX Pkts/Bytes** Displays the amount of data received as packets and bytes.
- **TX Retry/Dropped** Displays the percentage of transmit packets that needed to be re-sent and the percentage of packets that were dropped.
- **RX Retry/Dropped** Displays the percentage of receive packets that needed to be re-sent and the percentage of packets that were dropped.
- **Ch. Util. (Busy/Rx/Tx)** Displays channel utilization statistics:
  - **Busy** This number indicates how busy the channel is. This represents the sum of Tx, Rx, and also non-WiFi interference.
  - **Rx** This number indicates how often the radio is in active receive mode (calculated for all traffic received on the channel, whether for this AP or not).
  - **Tx** This number indicates how often the radio is in active transmit mode.

UniFi Access Point – Details

Click **Overview** to display the device specifics, connection details, uptime, and user statistics.

Overview

MAC Address Displays the MAC address or unique hardware identifier of the AP.

Model Displays the model name of the AP.

Version Displays the version number of the AP's firmware.

Board Revision Displays the revision number of the hardware board.

IP Address Displays the IP address of the AP.

Uptime Displays the duration of time the AP has been running without interruption.

Memory Usage Displays the percentage of memory used.

Load Average Displays the number of jobs in the run queue or waiting for input/output averaged over 1, 5, and 15 minutes.

 # Users Displays the number of users connected to the primary network.

 # Guests Displays the number of users connected to the guest network.

Uplink (Wired)

If your AP has a wired uplink connection, click **Uplink (Wired)** to display details about the wired uplink.

Uplink Displays the name, alias, or MAC address of the switch or other uplink device being used by the AP. You can click the name to get additional details on the device.

Speed Displays the connection speed in Mbps.

Duplex Displays the mode, *Full Duplex* or *Half Duplex*.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Activity Displays the level of activity in bytes per second.

Uplink (Wireless)

If your AP has a wireless uplink connection, click **Uplink (Wireless)** to display details about the wireless uplink.

Uplink AP Displays the name, alias, or MAC address of the uplink AP. You can click the name to get additional details on the uplink AP.

Signal Displays the percentage of signal strength between the two APs.

TX Rate Displays the transmit rate.

RX Rate Displays the receive rate.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Activity Displays the level of activity in bytes per second.

Downlink

The wireless APs currently connected to the wired AP are displayed.

Note: *Downlinks* will only be visible under the *Details* tab when a wireless AP is connected.

AP Displays the name, alias, or MAC address of the downlink AP. You can click the name to get additional details on the device.

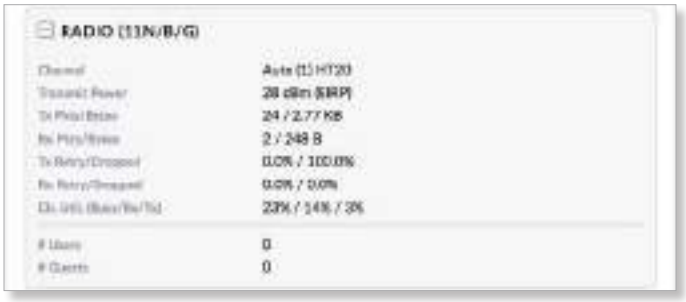
Signal Displays the percentage of signal strength between the two APs.

Actions Click a button to perform the desired action:

- **Remove** Click to remove the wireless AP from the wired AP.

Radio (11N/B/G) or Radio (11N/A/AC)

Click **Radio (11N/B/G)** or **Radio (11N/A/AC)** to display the channel and transmit/receive statistics.



Channel Displays the channel being used.

Transmit Power Displays the EIRP in dBm.

TX Pkts/Bytes Displays the amount of data transmitted as packets and bytes.

RX Pkts/Bytes Displays the amount of data received as packets and bytes.

TX Retry/Dropped Displays the percentage of transmit packets that needed to be re-sent and the percentage of packets that were dropped.

RX Retry/Dropped Displays the percentage of receive packets that needed to be re-sent and the percentage of packets that were dropped.

Ch. Util. (Busy/Rx/Tx) Displays channel utilization statistics:

- **Busy** This number indicates how busy the channel is. This represents the sum of Tx, Rx, and also non-WiFi interference.
- **Rx** This number indicates how often the radio is in active receive mode (calculated for all traffic received on the channel, whether for this AP or not).
- **Tx** This number indicates how often the radio is in active transmit mode.

 # Users Displays the number of users connected to the primary network.

 # Guests Displays the number of guests connected to the guest network.

WLANs

You can deploy multiple wireless networks organized into WLAN groups on different APs.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

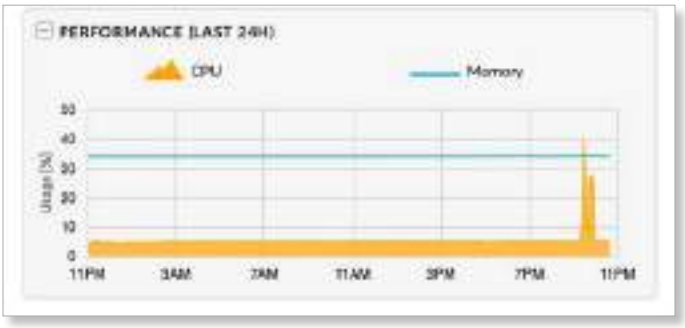
Name Displays the name of the WLAN group.

BSSID Displays the BSSID or MAC address of the Access Point.

ESSID Displays the network name of the wireless network.

Channel Displays the channel being used.

Performance (Last 24 H)



CPU (%) The graph displays the percentage of CPU processing power used during the last 24 hours.

Memory (%) The graph displays the percentage of memory used during the last 24 hours.

UniFi Access Point – Users

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Name/WLAN Displays the hostname, alias, or MAC address of the connected client and the name or SSID of the wireless network in use. You can click the name to get additional details; see **"Client Details" on page 147** for more information.

Signal Displays the signal strength between the user and AP.

TX Rate Displays the transmit rate.

UniFi Access Point – Guests

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Name/WLAN Displays the hostname, alias, or MAC address of the connected guest and the name or SSID of the wireless network in use. You can click the guest name to get additional details; see **"Client Details" on page 147** for more information.

Signal Displays the signal strength between the guest and AP.

TX Rate Displays the transmit rate.

UniFi Access Point – Configuration

Change device configuration settings.

General

Alias Enter or edit the customizable name or identifier of the AP. The *Alias* is also known as the host name.

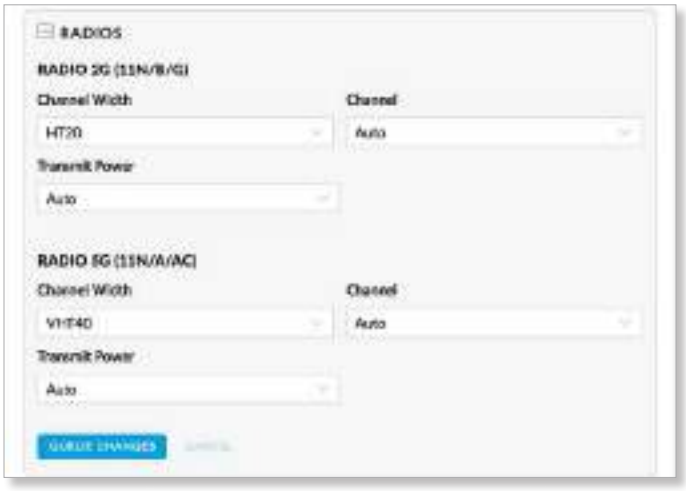
LED Select the appropriate option: **Use site settings** (default), **On**, or **Off**. For more information about site settings, go to **"Settings > Site" on page 21**.

Device Tags Select or search for a device tag. You can also enter a keyword and press **Enter** to save a new device tag.

Save Click to apply changes.

Cancel Click to discard changes.

Radios



Channel Width Select the appropriate setting:

- **HT20/HT40** (Available for 2.4 GHz only.) Select **HT20** for 20 MHz operation or **HT40** for 40 MHz operation.

Note: If the AP is part of a Zero Handoff WLAN Group, then the *Channel* settings cannot be changed.

- **VHT20/VHT40/VHT80** (Available for 5 GHz only.) Select **VHT20** for 20 MHz operation, **VHT40** for 40 MHz operation, or **VHT80** for 80 MHz operation in the 5 GHz band.

Note: If the AP is part of a Zero Handoff WLAN Group, then the *Channel* settings cannot be changed.

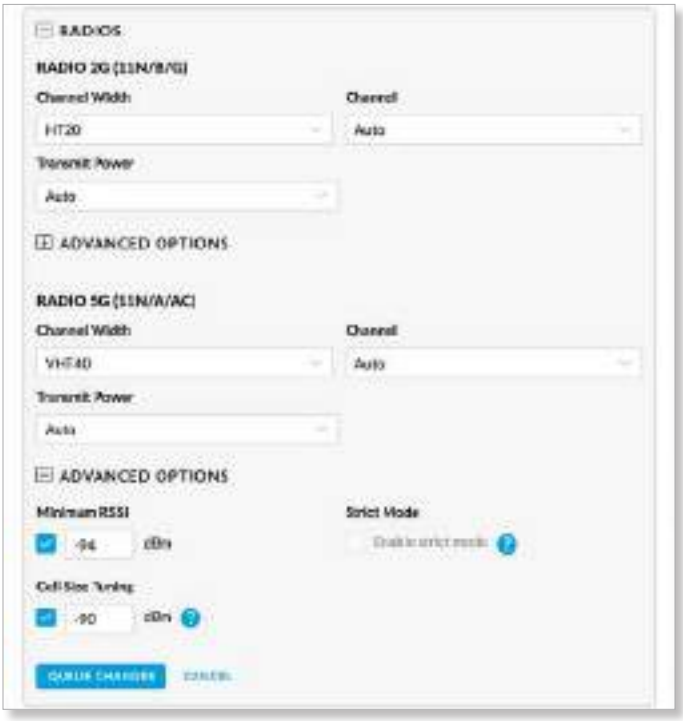
Channel Select a channel number or keep the default, *Auto*.

Transmit Power By default the transmit power is set to *Auto*. You can also manually select the following:

- **High** The highest TX power available.
- **Medium** Halfway between *High* and *Low*.
- **Low** The lowest TX power available.
- **Custom** Custom setting that you specify in the field provided.
- **Antenna Gain** (Only available for specific models.) Specify the antenna gain.

Advanced Options

These options are available if they are enabled. Go to **"Settings > Site" on page 21** for more information.



Minimum RSSI Disabled by default. Select this option and enter a minimum threshold (we recommend a value in this range: -70 to -90 dBm). For UniFi, RSSI is synonymous with SNR. If the client signal falls below the specified threshold, then the AP kicks out the client, allowing it to reconnect with a more suitable AP.

Note: If the AP is part of a Zero Handoff WLAN Group, the *Minimum RSSI* setting cannot be changed.

Strict Mode Available if *Minimum RSSI* is enabled. This option is disabled by default. If enabled, the AP will ignore signals below the minimum RSSI. Use with caution and only for high-density tuning. Enabling *Cell Size Tuning* disables *Strict Mode* as *Cell Size Tuning* provides similar functionality but with finer control.

Cell Size Tuning Disabled by default. *Cell Size Tuning* adjusts the level at which the AP will ignore and transmit over interference. Use only in high-density applications if *Cell Size Tuning* is required for channel re-use. If you enable this option, enter the appropriate value.

Note: DFS signatures at all powers are still processed and triggered.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click *Cancel* to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.

- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

WLANs

You can deploy multiple wireless networks organized into WLAN groups on different APs.

WLAN Group Select the appropriate group.

Name Displays the network name or SSID of the available wireless network.

Overrides Displays the SSID override information applied to the wireless network.

Actions Click a button to perform the desired action:

- **Edit** Click ✎ to enable a VLAN (Virtual Local Area Network), set the VLAN ID, and enter the SSID override name to apply to the wireless network.

  Note: The *Override* option is not available for a Zero Handoff WLAN Group.

Queue Changes Click **Queue Changes** to save changes.

Cancel Click to discard changes.

Override

Enabled on this AP Select the checkbox to enable the WLAN for use.

Use VLAN Select the checkbox to enable the VLAN.

- **with VLAN ID** The VLAN ID is a unique value assigned to each VLAN on a single device. Enter a value between 2 and 4095. For example, in a large deployment where there are multiple buildings, you can use a different VLAN ID for each building while all of the VLANs remain on the same corporate network.

SSID Enter the SSID override name to apply to the wireless network.

Security Key If the WPA-Personal security option has been applied to the WLAN under *Settings* > *Wireless Networks*, then the Pre-Shared Key (PSK) for the SSID specified will automatically appear in this field.

Actions Click a button to perform the desired action:

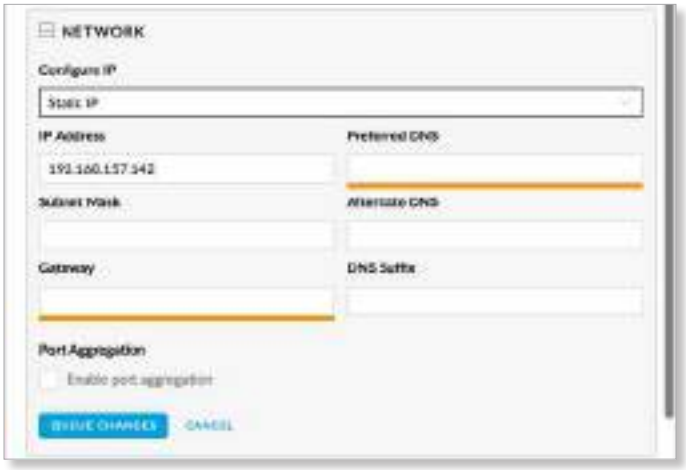
- **Save** Click to apply changes.
- **Reset to Defaults** Click **Reset to Defaults** to remove any overrides that were applied to the selected wireless network.
- **Cancel** Click to discard changes.

Network

Configure IP Select the internet connection type for your service, **Using DHCP** or **Static IP**. Proceed to the appropriate instructions.

- **Using DHCP** The use of the Dynamic Host Configuration Protocol (DHCP) is the default. The AP automatically acquires network settings from the network's DHCP server.

- **Static IP** Assign fixed network settings to the AP. Enter the following information:
  - **IP Address** Enter the IP address for the AP.
  - **Subnet Mask** Enter the subnet mask of the AP.
  - **Gateway** Enter the IP address of the gateway (for example, the UniFi Security Gateway).
  - **Preferred DNS** Enter the IP address of the primary DNS server.
  - **Alternate DNS** Enter the IP address of the secondary DNS server.
  - **DNS Suffix** Enter the Fully Qualified Domain Name (FQDN) without the hostname.



Port Aggregation Available for the UAP-AC-HD and UAP-AC-SHD. Select this option to aggregate the AP's ports. You must enable port aggregation on the Switch after you enable this option.

Note: Ensure that you enable port aggregation on the downstream Switch AFTER enabling port aggregation on the AP.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.

- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

Band Steering

This option is available if advanced features are enabled. Go to **"Settings > Site" on page 21** for more information.

2.4 GHz networks are typically more congested due to support of legacy clients and multiple sources of 2.4 GHz interference, including Bluetooth devices. Band steering can help distribute the load on 2.4 GHz and 5 GHz networks by steering dual-band clients to the 5 GHz band when appropriate.

Some dual-band clients are band-steering unfriendly for various reasons and are marked as such by the AP. Such clients are not steered to any band even when conditions would justify it.

Note: Only generation 2 and 3 UniFi APs support band steering.

If enabled, the UniFi band steering policy takes two criteria into account:

- channel utilization metrics
- signal quality measurements, including RSSI

The AP steers the client to the optimal band during association (not after association). If both bands or neither band is overloaded, the AP does not perform band steering; instead, the client chooses a band.

If the 2.4 GHz band is overloaded, and the RSSI of the client is above the threshold for association on the 5 GHz band, then the AP will steer the client to the 5 GHz band by withholding probe responses.

If the client still attempts to associate on the 2.4 GHz band, the AP will send auth failure frames in response to auth requests from the client.

If the 5 GHz band is overloaded and the 2.4 GHz band is not, then clients are steered to the 2.4 GHz band (RSSI is not a factor). The RSSI thresholds are 30 dBm or better for the 5 GHz band. For example, if the 2.4 GHz network has low utilization, then the *Steer to 5G* option does not steer all clients to 5 GHz.

All APs must use the same SSID for the 2.4 GHz and 5 GHz bands. For example, if you have multiple WLANs in your default WLAN group, you cannot override the 5 GHz SSID name in one of the WLANs and still use band steering on the other two WLANs. All APs must use band steering – or none of them do.

Prefer 5G Select this option to steer clients to the 5 GHz band at a lower channel utilization threshold than the *Balanced* option. The threshold is not a single value; instead it is a function of two values: the 2.4 GHz channel utilization and 5 GHz channel utilization.

Balanced (Not available for the UAP-PRO.) Select this option to steer clients to the 5 GHz band channel at a higher channel utilization threshold than the *Steer to 5G* option.

Off Keep the default, *Off*, if you do not want to use band steering.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.

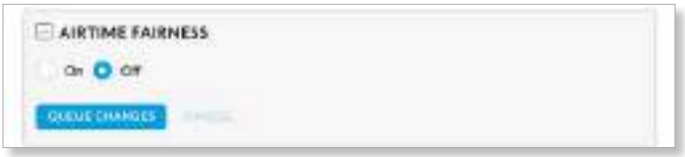
- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

Airtime Fairness

Note: Only generation 2 and 3 UniFi APs support airtime fairness.

This option is available if advanced features are enabled. Go to **"Settings > Site" on page 21** for more information.

The *Airtime Fairness* option helps multiple users to share the bandwidth of a single AP.



On/Off Disabled by default. Select **On** to enable this option.

Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section with pending changes is highlighted by an ellipsis.

When you are done with your changes, click **Apply Changes** at the bottom of the screen. (You can cancel the changes of any section by clicking *X* of the appropriate section.)

Cancel Click to discard changes.

Pending Changes If you want to queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.

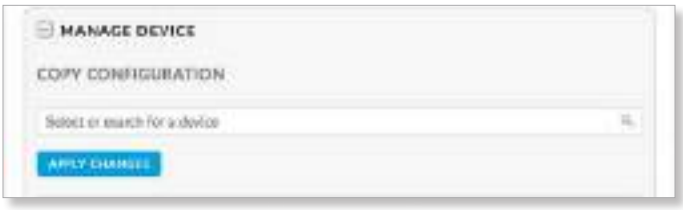
- **Apply** Click ✓ APPLY to save changes.
- **Discard** Click × DISCARD to cancel changes.

Manage Device

There are five options to manage the UniFi AP.

Copy Configuration

If you have settings that you want to apply to multiple Switches, use this option to copy the configuration.



Select or search for a device Select or search for the appropriate AP whose configuration will be copied to this AP.

Apply Changes Click to overwrite its current configuration with the configuration of the selected AP.

Custom Upgrade

For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, select this option.

(location URL) Enter the UL of the firmware's location.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Force Provision

You can force a provision to apply the latest settings to a device. It ensures that the device is in sync with all of the applicable settings in the UniFi Controller, like a settings reset so the device has the settings it should have.

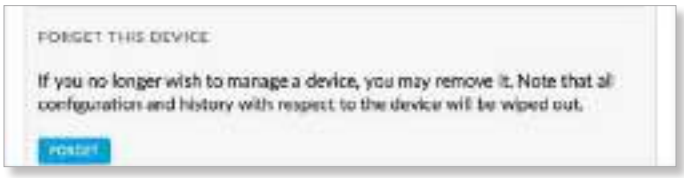
Provision Apply the latest settings to the Switch.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Disable This Device

Disable Click **Disable** to turn off the LED and wireless capabilities of an AP. It will also be excluded from the Dashboard status and device count.

Forget This AP



Forget Click **Forget** to remove the AP from management by the UniFi Controller software and reset it to factory default settings.

Note: Use caution when clicking *Forget*. This will restore the AP to factory default settings when it is in a *Connected* state. Do not use the *Forget* option when the AP is in an *Isolated* or *Disconnected* state. If you do, the only way to make the AP accessible from the UniFi Controller is to take it down and connect by wire.

Wireless Uplinks

When an AP is not connected by a wire, the *Wireless Uplinks* section lists potential uplink APs that can be selected to establish a wireless connection.

AP Displays the hostname, alias, or MAC address of the potential Uplink AP. You can click the name to get additional details.

Channel Displays the channel in use for wireless communication.

Signal Displays the percentage of signal strength.

Actions Click a button to perform the desired action:

- **Select** Click to connect the wireless AP to the wired AP.
- **Remove** Click to disconnect the wireless AP from the wired AP.

Note: An AP can only uplink to another AP using the same radio band. For example, the UAP-Outdoor 5G can only uplink to another UniFi AP using the 5 GHz radio band.

Access Point - Isolated/Disconnected

When an AP is in an *Isolated* or *Disconnected* state, you can re-establish a connection to the UniFi Controller software using one of three methods:

- Reconnect the AP to the gateway/router.
- Connect an Ethernet cable from the *Secondary Ethernet Port* (if available) of the isolated AP to the *Secondary Ethernet Port* (if available) of another UniFi AP that is connected to the gateway/router.
- Establish a wireless uplink to a wired AP. See the *Wireless Uplinks* section to find, select, and connect to a wired AP.

In an *Isolated* or *Disconnected* state, the *Map* tab displays the AP icon with a red/orange LED and *disconnected* icon.

The LED on the actual device will be steady green or blue with occasional flashing. This AP doesn't provide any wireless service.

Note: Do not use the *Forget this AP* option when the AP is in an *Isolated* or *Disconnected* state. If you do, then the only way to make the AP accessible from the UniFi Controller is to take it down and connect it by wire.

Overview

MAC Address Displays the MAC address of the AP.

Model Displays the model number.

Version Displays the version of software used on the AP.

Last Seen Displays the amount of time that has passed since the Access Point was last seen.

Access Point - Managed by Other

The *Managed by Other* state indicates that the AP is not in the default state but it is not controlled by the UniFi Controller.

Overview

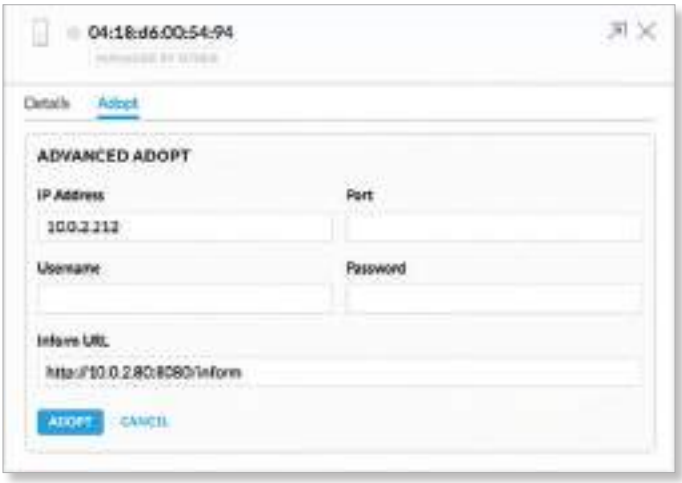
MAC Address Displays the MAC address of the AP.

Model Displays the model number.

Version Displays the version of software used on the AP.

Last Seen Displays the amount of time that has passed since the Access Point was last seen.

Adopt



IP Address Displays the IP address of the AP.

Port Displays the SSH port of the AP.

Username Enter the SSH Username for management access. This is the *Device Username* you configured in **"Settings > Site" on page 21**.

Password Enter the SSH Password for management access. This is the *Device Password* you configured in **"Settings > Site" on page 21**.

Inform URL This tells the AP where to look for the UniFi Controller. The URL will be automatically displayed but you may need to verify its accuracy as the system may have multiple interfaces.

Adopt Click **Adopt** to adopt the AP so you can manage it using the UniFi Controller software.

Cancel Click *Cancel* to discard changes.

Access Point - Pending Approval

The *Pending Approval* state indicates that the Access Point is in the default state and is available for adoption.

MAC Address Displays the MAC address of the AP.

Model Displays the model number.

Version Displays the version of software used on the AP.

Last Seen Displays the amount of time that has passed since the AP was last seen.

If you want to manage this AP using the UniFi Controller software, then click **Adopt** on the *Devices* screen.

UniFi Access Point – Tools

RF Environment

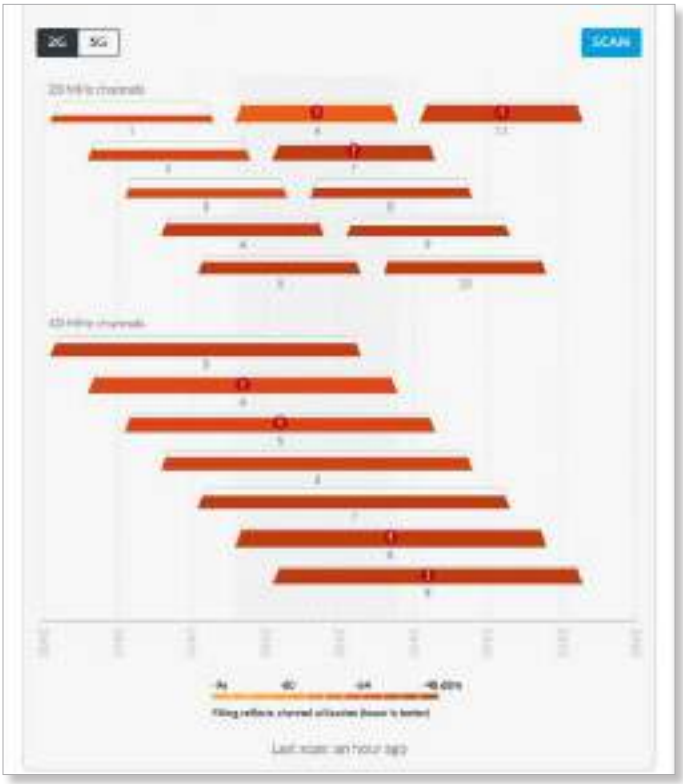
Note: Only generation 2 and 3 UniFi APs support spectral analysis.

Click **RF Environment** for spectral analysis to help in channel selection and planning.

2G/5G Select the frequency band you want to analyze.

Scan Click **Scan** to scan the RF environment and then click **Confirm** to continue.

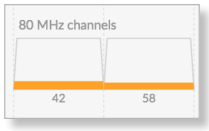
Note: The RF scan may take more than five minutes. All clients using this AP will be disconnected, and the AP will be offline for the duration of the scan.



Each bar graph represents a channel option and its color-coded level of interference (the legend is displayed at the bottom). An exclamation mark icon denotes the channels with the most channel utilization.

MHz channels The 2.4 GHz results are displayed in channel widths of 20 and 40 MHz. The 5 GHz results are displayed in channel widths of 20, 40, 80, and 160 MHz.

Displays the corresponding channel number for each channel width option. For example, channels 42 and 58 are two of the 80 MHz channels.



(outlined) The current channel is outlined.

(frequencies) The frequency range is depicted at the bottom of the *RF Environment* section.

Place your cursor over a channel option to view the following:

Overview

- **Radio** Displays the radio being used.
- **Channel Width** Displays the width of the channel.
- **Used Channels** These are the channels in use.
- **Frequency Range** Displays the range of frequencies.

RF Scan Details

- **Utilization** Displays the percentage of the frequency range already in use.
- **Interference** Displays the level of interference.
- **Interference Types** Displays the type of interference being detected.

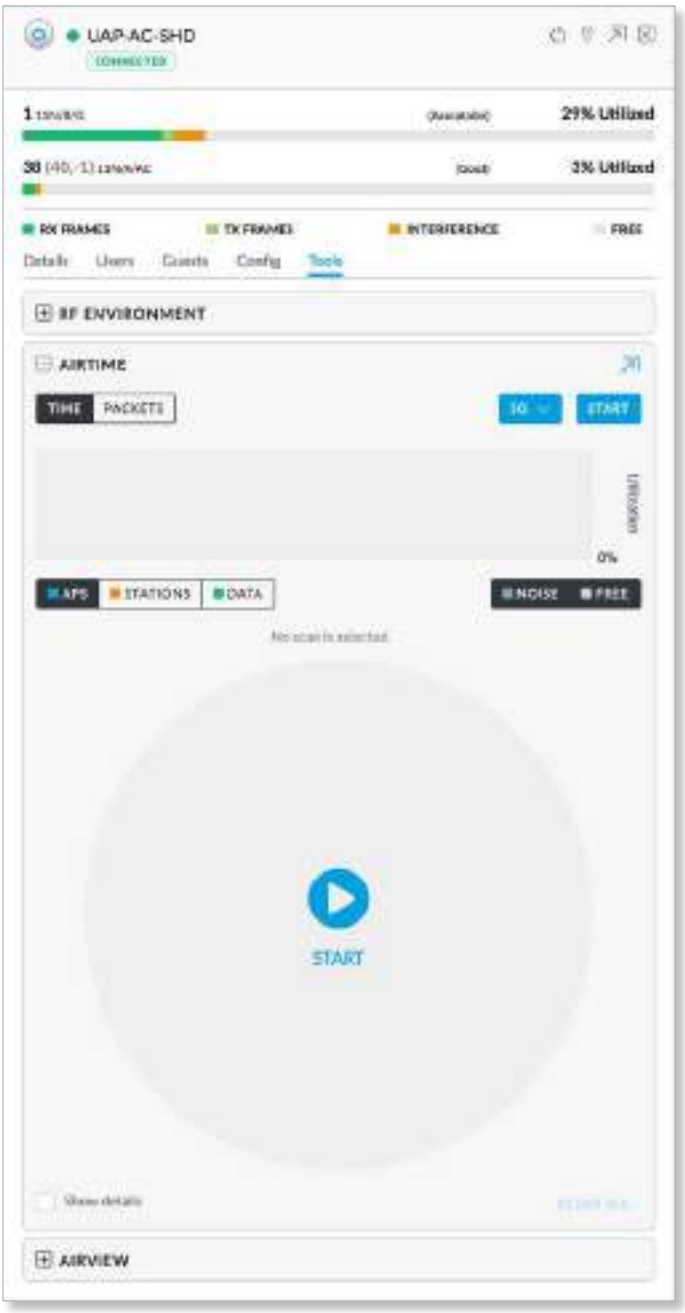
Last scan Displays the duration of time since the last scan.

airTime

Note: Only generation 3 UniFi APs with a dedicated security radio support airTime™.

Click **airTime** to use the airTime tool, which visualizes and analyzes how the APs use channels in real time. The breakdown is by frame type, clients, neighboring APs, protocols, and interference.

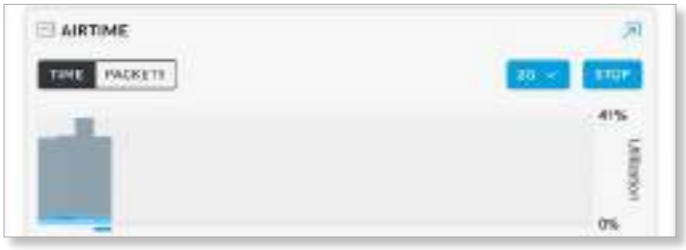
Spectrum view and Wi-Fi packet analysis can be done simultaneously, without affecting stations, for a total view of the RF environment and channel utilization.



(expand) Click ↗ to display a second *airTime* screen.

(bar graph) Click the appropriate display option, **Time** or **Packets**.

- **Time** Click **Time** to track channel utilization over time in the bar graph.



- **Packets** Click **Packets** to track by the number of packets in the bar graph.

2G/5G Select the frequency band you want to analyze.

Start/Stop Click to begin or stop using the scan.

Click any slice of the scan results for the following:

(SSID) Displays the wireless network name.

(MAC address) Displays the BSSID or MAC address of the AP.

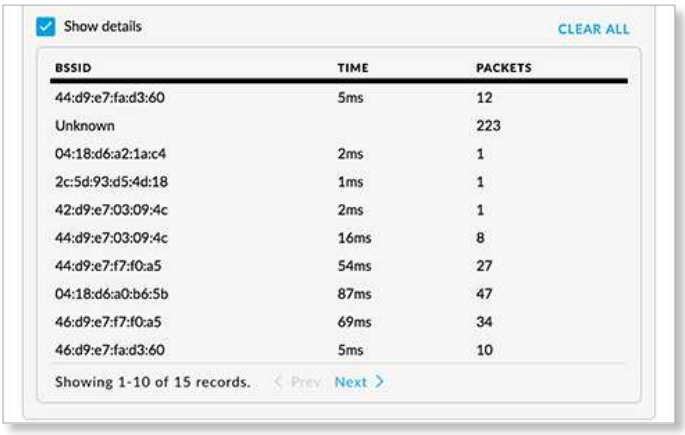
Utilization Displays the percentage of the channel that is being utilized.

Packets Displays the number of packets in transit.

Clear All Clear all scan results.

Show details Click to display the following information:

- **BSSID** Displays the BSSID or MAC address of the AP.
- **Time** Displays the duration of the utilization.
- **Packets** Displays the number of packets in transit.



You can apply the following filters:

APs Displays scan information for APs. (This filter is always applied.)

Stations Displays scan information for the stations.

Data Displays scan information for the data being transmitted and received.

airView

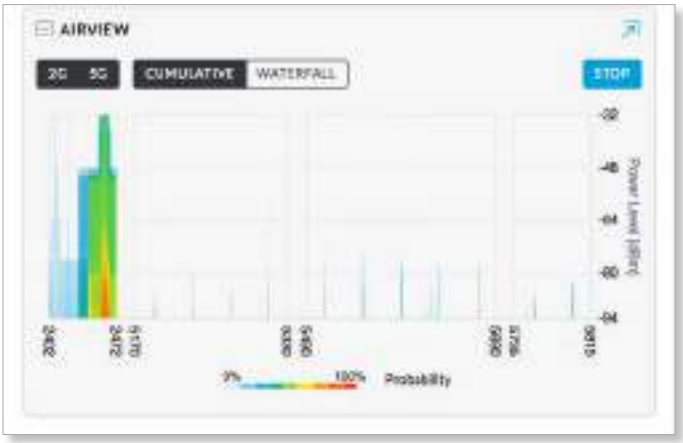
Note: Only generation 3 UniFi APs with a dedicated security radio support airView®.

Click **airView** for real-time visibility into your RF spectrum. Because it uses the dedicated security radio, it analyzes all of your available RF channels without affecting performance or disrupting client activity.

Spectrum view and Wi-Fi packet analysis can be done simultaneously, without affecting stations, for a total view of the RF environment and channel utilization.

(expand) Click ↗ to display a second *airView* screen.

2G/5G Select the frequency band you want to analyze. You can click both tabs to display the scan results side by side.



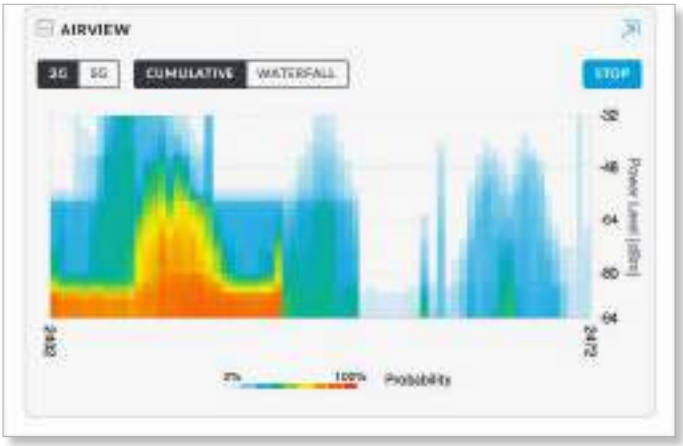
(view) Select the appropriate display option, **Cumulative** or **Waterfall**.

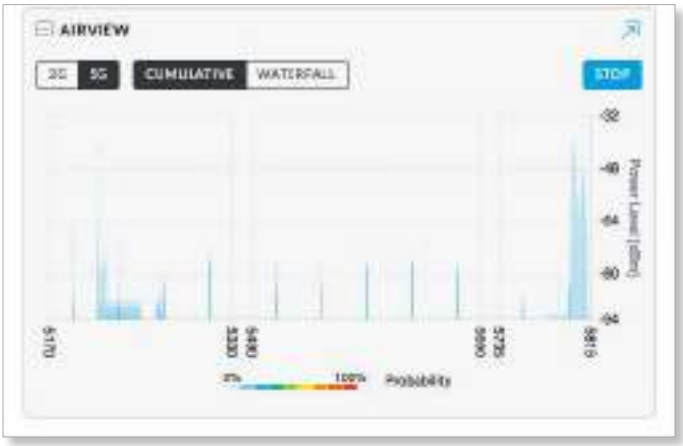
- **Cumulative** Select **Cumulative** to track the aggregate energy collected since the start of the airView session. The power of the energy (in dBm) is shown across the frequency span. Cooler colors (such as blue and darker colors) represent energy of a specific strength and frequency appearing at a relatively low occurrence rate, whereas increasingly warmer colors (from green to yellow to orange to red) represent energy of a specific strength and frequency appearing at a higher rate of occurrence.

  Note: Energy is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

  The spectral view over time essentially displays the steady-state RF energy signature of a given environment.

  The legend at the bottom provides a numerical guide associating the various colors to probability levels, from 0% (least likely to occur) to 100% (most likely to occur).



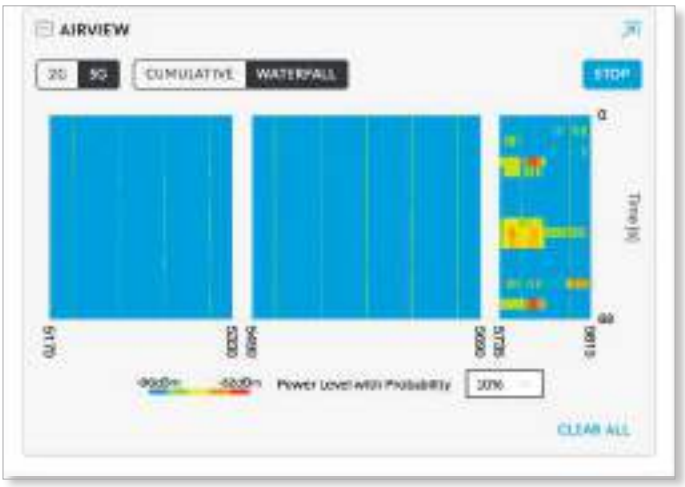


- **Waterfall** Select **Waterfall** to track the aggregate energy collected since the start of the airView session for each frequency. The power of the energy (in dBm) is displayed across the frequency span, and a new row is inserted every few seconds.

  The energy color designates the amplitude (or strength) of the signal. Cooler colors represent lower energy levels (with blue representing the lowest levels) in that frequency bin, and warmer colors (yellow, orange, or red) represent higher energy levels in that frequency bin.

  The legend at the bottom provides a numerical guide associating the various colors to power levels (in dBm).

  - **Probability** Select the appropriate level of probability from the drop-down list (the lower the number, the less likely to occur). The default is **10%**.



Start/Stop Click to begin or stop using the scan.

Clear All Clear all scan results.

Chapter 13: Client Details

A client hyperlink opens the client's *Details* window either in the *Properties* panel or as a separate popup window. You can always dock this window in the *Properties* panel or detach it as a separate window.

The top of the window displays the device icon and name (or MAC address).

Properties

The *Properties* panel appears on the right side of the screen. Information about each selected device appears as a popup within this panel. The information varies depending on whether the client is wired or wireless:

- *Wireless Client – Details*
- **"Wired Client – Details" on page 149**

Remove All Click to close the *Properties* panel.

Collapse All Click to collapse all of the popups to rows.

The top of the popup remains and displays the following:

- **Display** Click + to display the device information.
- **(icon)** Displays the icon of a wireless or wired device.
- **Name/MAC Address** Displays the hostname, alias, or MAC address of the device.
- **Block** Click to block this client from accessing the network.
- **Reconnect** Click to reconnect a wireless client. You can click to kick out a client, which usually reconnects back quickly; this is useful for troubleshooting or resolving a problematic wireless connection.
- **Unauthorize/Authorize** (Available for *Guests* only.) Click to remove authorization of guest access and disconnect the guest, or click for guests pending authorization.
- **Undock from Properties Panel** Click to display the same information in a separate popup screen that can be moved anywhere within the browser screen.
- **Close Properties** Click to close the device popup.

Hide Property Panel Click to hide the *Properties* panel but allow the device popups to remain accessible from this panel. Click the *properties* icon to re-open it.

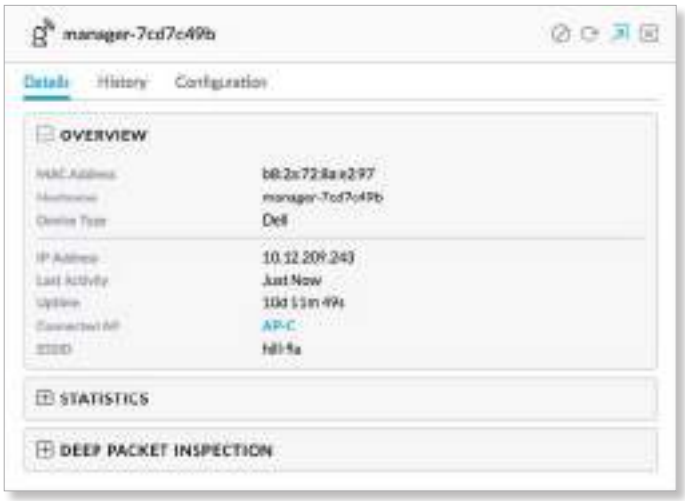
There are three clickable tabs:

- *Details*
- *History*
- *Configuration*

Wireless Client – Details

Click **Overview** to display the device specifics, connection details, uptime, statistics, and Deep Packet Inspection (DPI) information.

Overview



MAC Address Displays the MAC address or unique hardware identifier of the client.

Hostname Displays the customizable name or identifier of the client.

Device Type Displays the type of device.

IP Address Displays the IP address of the client.

Last Activity Displays the time of the most recent activity.

Uptime Displays the duration of time the client has been connected.

Connected AP Displays the hostname, alias, or MAC address of the UniFi AP. You can click the name to get additional details; see **"UniFi Access Point Details" on page 131** for more information.

ESSID Displays the name of the wireless network.

Statistics

Channel Displays the channel being used.

Signal Displays the percentage of signal strength between the AP and client.

TX Rate Displays the transmit rate.

RX Rate Displays the receive rate.

Power Save Displays the status of the power save mode.

Internet

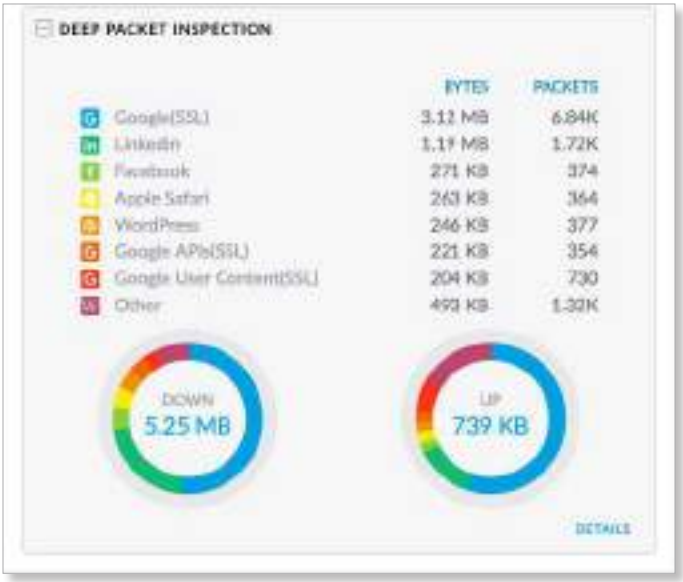
Activity Displays the level of activity in bytes per second.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Deep Packet Inspection

The *Deep Packet Inspection* information is available if the DPI feature is enabled (refer to **"Settings > Site" on page 21** for more information).



(application) Displays the name of the application.

Bytes Displays the amount of data uploaded and downloaded as bytes.

Packets Displays the amount of data uploaded and downloaded as packets.

Down A visual pie chart represents the download distribution amongst the applications.

Up A visual pie chart represents the upload distribution amongst the applications.

Wireless Client – History

Date/Time Displays the date and time of the connection.

Duration Displays the duration of the connection.

Down Displays the total amount of data downloaded by the client.

Up Displays the total amount of data uploaded by the client.

Wireless Client – Configuration

General

Alias Allows you to change the hostname of the client.

Note Allows you to enter comments about the client. Once saved, the client will be designated as a "Noted" client on the *Insights* > *Known Clients* tab.

User Group Allows you to assign the client to a User Group. User Groups are set up under the *Settings* tab > *User Groups* option (see **"Settings > User Groups" on page 54** for more information). The default *User Group* is *Automatic*.

Save Click to apply changes.

Cancel Click to discard changes.

Network

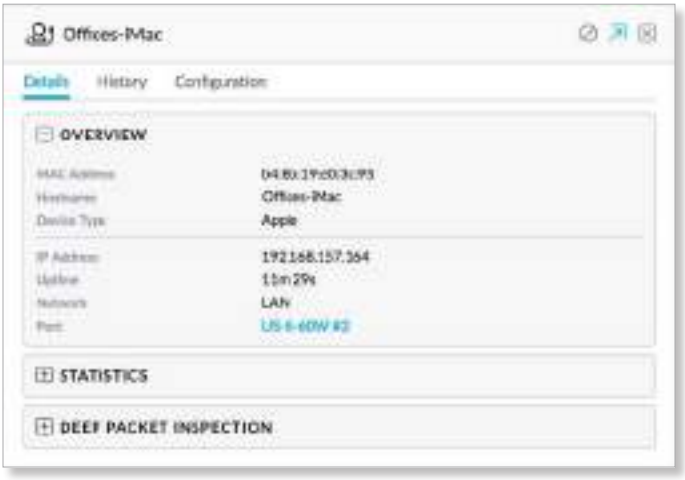
Use fixed IP address Select this option to assign a static IP address to the client, and configure the settings below. If you want the local DHCP server to assign an IP address to the client, remove the checkmark.

- **Network** Select the appropriate network from the drop-down list.
- **IP Address** Enter the local IP address.

Save Click to apply changes.

Cancel Click to discard changes.

Wired Client – Details



MAC Address Displays the MAC address or unique hardware identifier of the client.

Hostname Displays the customizable name or identifier of the client.

Device Type Displays the type of device.

IP Address Displays the local IP address of the client.

Uptime Displays the duration of time the client has been connected.

Network Displays the network used by the client.

Port Displays the name and port of the UniFi device being used by the client. You can click the name to get additional details on the UniFi device.

Wired Client – Statistics

Overview

Internet

Activity Displays the level of activity in bytes per second.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

LAN

Activity Displays the level of activity in bytes per second.

Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Deep Packet Inspection

The *Deep Packet Inspection* information is available if the DPI feature is enabled (refer to **"Settings > Site" on page 21** for more information).

Application Displays the name of the application.

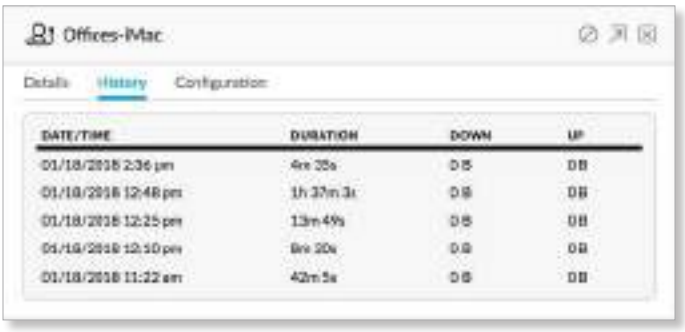
Bytes Displays the amount of data uploaded and downloaded as bytes.

Packets Displays the amount of data uploaded and downloaded as packets.

Down A visual pie chart represents the download distribution amongst the applications.

Up A visual pie chart represents the upload distribution amongst the applications.

Wired Client – History



Date/Time Displays the date and time of the connection.

Duration Displays the duration of the connection.

Down Displays the total amount of data downloaded by the client.

Up Displays the total amount of data uploaded by the client.

Wired Client – Configuration

Config

Alias Allows you to change the hostname of the client.

Note Allows you to enter comments about the client. Once saved, the client will be designated as a "Noted" client on the *Insights* > *Known Clients* tab.

User Group Allows you to assign the client to a User Group. User Groups are set up under the *Settings* tab > *User Groups* option (see **"Settings > User Groups" on page 54** for more information). The default *User Group* is *Automatic*.

Save Click **Save** to apply changes.

Cancel Click to discard changes.

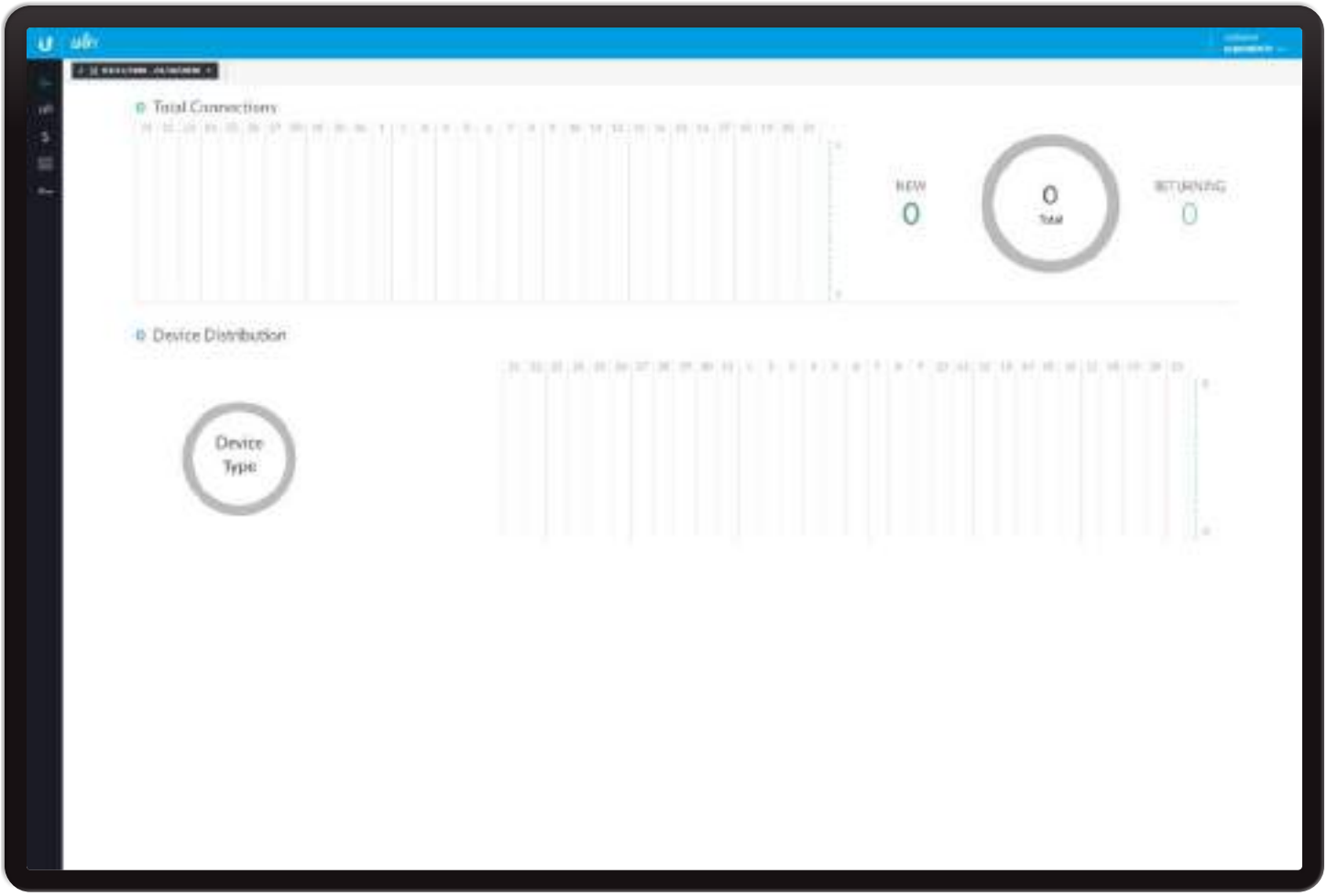
IP Config

Fixed IP Select this option to assign a static IP address to the client, and configure the settings below. If you want the local DHCP server to assign an IP address to the client, remove the checkmark.

- **Network** Select the appropriate network from the drop-down list.
- **IP Address** Enter the local IP address.

Save Click **Save** to apply changes.

Cancel Click to discard changes.



Chapter 14: Hotspot Manager

The Hotspot Manager includes five main tabs when accessed by the UniFi Controller superadmin or admin with read/write access. For details on a specific tab, refer to the appropriate section.

To access the Hotspot Manager, go to **Settings** > **Guest Control**, and click **Go to Hotspot Manager**. See **"Hotspot" on page 41** for more information.

If you create a bookmark for the Hotspot Manager, ensure that you include the site name in the URL, which should be in this format:
https://*unifi.yourdomain.com*:8443/hotspot/s/*site_name*

Only admins with read/write access to the UniFi Controller can create operator accounts for the Hotspot Manager. Operator accounts are designed for use by hotels or other businesses to service guests and have no access to other UniFi administrative features. Operator accounts will have access to four tabs after login: *Analytics*, *Guests*, *Payments*, and *Vouchers*.

For the *Guests*, *Payments*, and *Vouchers* tabs, you have the following options:

Items per page Select how many results are displayed per page: **10**, **50**, **100**, or **200**.

On any sub-tab, you can click any of the column headers to change the list order.

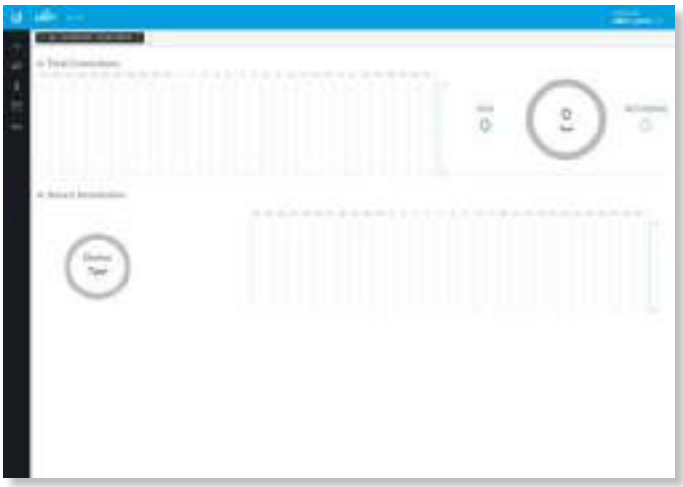
If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

Search Search Enter the text you want to search for. Simply begin typing; there is no need to press *Enter*.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Analytics

The total number of connections and distribution of devices are displayed.



Date Click either arrow to change the date or range in one-day increments.

Click the date to display the calendar.

- **Calendar** Click a specific date to display its statistics. For a range of dates, click both the start and end dates, which are color-coded orange; the intervening dates are color-coded blue. Click either arrow to change the calendar in one-month increments.
  - **Apply** Click to save changes.
  - **Cancel** Click to cancel changes.

Total Connections The number of connections are displayed per day of the range selected.

New Displays the number of new connections.

Total Displays the total number of connections.

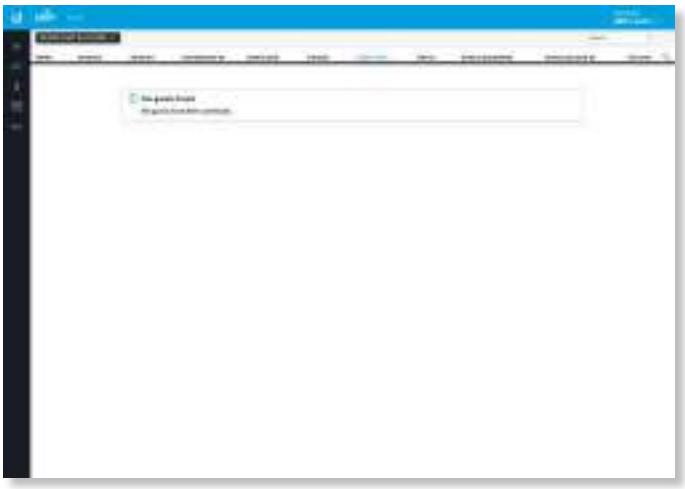
Returning Displays the number of returning connections.

Device Distribution The number of devices are displayed per day of the range selected.

Device Type Displays the number of devices per type.

Guests

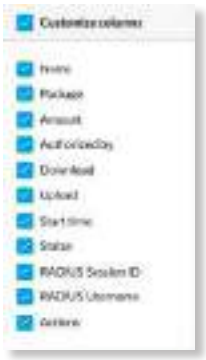
The Hotspot's active guests are displayed.



Show Filter by time duration: **last 24 hours**, **3 days**, **7 days**, **2 weeks**, **30 days**, and **120 days**.

Customize Columns Click to customize the columns used for display.

Select **Customize columns**.



You can add or remove columns for display.

Name Displays the guest's device name or MAC address.

Package Displays the description of the package that was purchased (if applicable).

Amount Displays the amount paid for access (if applicable).

Authorized By Displays the authorization method. If there is no authorization, then *None* is displayed.

Download Displays the total amount of data downloaded.

Upload Displays the total amount of data uploaded.

Start Time Displays the start time of the guest access.

Status Displays the remaining session time for the guest. Displays *Expired* if there is no remaining session time.

RADIUS Username Displays the username used for RADIUS authentication.

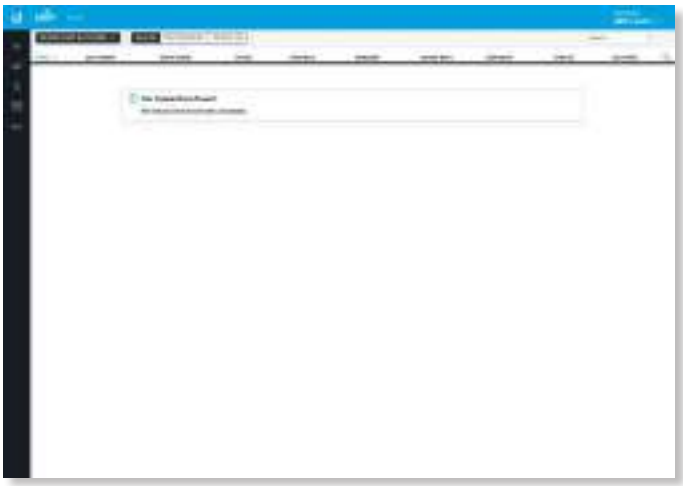
RADIUS Session ID Displays the session ID used for RADIUS authentication.

Actions Click a button to perform the desired action:

- **Disconnect** Immediately disconnect the selected guest.
- **Extend** Extend a guest's session for an additional 24 hours. For example, if you click it three times, you will extend guest access for three more days.

Payments and Transactions

The Hotspot's payments and transactions are displayed.



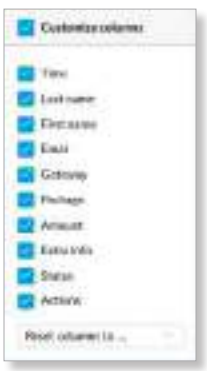
Show Filter by time duration: **last 24 hours**, **3 days**, **7 days**, **2 weeks**, **30 days**, and **120 days**.

You can apply one of the following primary filters:

- **All** Displays all payments and transactions.
- **Payments** Displays only payments.
- **Social** Displays the social media transactions, such as Facebook or Google+ authentication.

Customize Columns Click ⚙ to customize the columns used for display.

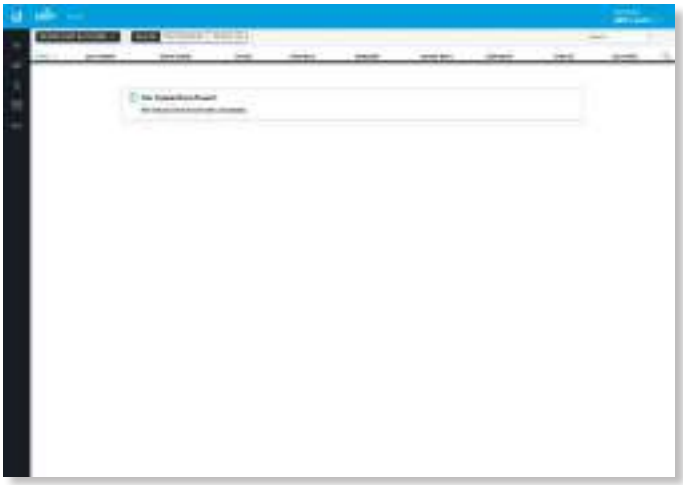
Select **Customize columns**.



You can add or remove columns for display.

- **Reset columns to** Click the drop-down at the bottom of the *Customize columns* screen to display the *Reset columns to* ... options.
  - **All** The *Last Name, First Name, Email, Package, Amount, Extra Info, Gateway, Status*, and *Actions* columns are displayed.
  - **User Defined** The *Last Name, First Name, Email, Package, Amount, Extra Info, Gateway, Status*, and *Actions* columns are displayed.
  - **Social** The *Last Name, First Name, Email, Gateway,* and *Status* columns are displayed.

All



Time Displays the date and time of the transaction.

Last Name Displays the user's last name.

First Name Displays the user's first name.

Email Displays the user's email address.

Package Displays the description of the package.

Amount Displays the amount of the transaction.

Extra Info If the user paid by credit card, the *Extra Info* field will display the type of credit card and the last four digits of the credit card used. If the user paid by an alternative method such as PayPal, the *Extra Info* field may display information such as the email address associated with the PayPal account.

Gateway Displays the gateway.

Status Displays the status of the transaction.

Actions Click a button to perform the desired action:

- **Refund** Refund the selected customer if necessary.

Payments

Time Displays the date and time of the transaction.

Last Name Displays the user's last name.

First Name Displays the user's first name.

Email Displays the user's email address.

Package Displays the description of the package.

Amount Displays the amount of the transaction.

Extra Info If the user paid by credit card, the *Extra Info* field will display the type of credit card and the last four digits of the credit card used. If the user paid by an alternative method such as PayPal, the *Extra Info* field may display information such as the email address associated with the PayPal account.

Gateway Displays the payment gateway.

Status Displays the status of the transaction.

Actions Click a button to perform the desired action:

- **Refund** Refund the selected customer if necessary.

Social

Time Displays the date and time of the transaction.

Last Name Displays the user's last name.

First Name Displays the user's first name.

Email Displays the user's email address.

Gateway Displays the payment gateway.

Status Displays the status of the transaction.

Vouchers

Create vouchers that include distributable codes, duration values, and use restrictions.

Create Vouchers To create a batch of vouchers, click + CREATE VOUCHERS and complete the following:

- **Create __** Enter the number of vouchers to create.
- **One time/Multi-use** Select how often the voucher can be used: **One time**, **Multi-use**, or **Multi-use (unlimited)**.
- **Expiration Time** Select how long the voucher is valid: **8 hours**, **24 hours**, **2 days**, **4 days**, **7 days**, or **User-defined**. If you select *User-defined*, enter a number and specify **day**, **minute**, or **hour**.
- **Bandwidth Limit (Download)** Select to limit the download bandwidth. Enter the maximum in Kbps.
- **Bandwidth Limit (Upload)** Select to limit the upload bandwidth. Enter the maximum in Kbps.
- **Byte Quota** Select to limit the amount of data transfer allowed per session. Enter the maximum in megabytes. *Byte Quota* is per use. If you have chosen *Multi-Use*, then the total data will be multiplied by the number of uses.
- **Notes** Enter any notes specific to this batch of vouchers.
- **Save** Click **Save** to create the vouchers as specified.
- **Cancel** Click *Cancel* to discard changes.

Print all Unused Vouchers Click PRINT ALL UNUSED VOUCHERS to send a page to your printer with the codes and durations of unused vouchers.

Print Batch A batch is a group of vouchers created at the same time. Click PRINT BATCH to display a list of dates with times. Select the date with time of the batch you want to retrieve. A tab will open with the vouchers ready for printing.

Code Displays each active voucher code.

Create Time Displays the date and time a voucher was created.

Down Displays the maximum download bandwidth allowed.

Up Displays the maximum upload bandwidth allowed.

Byte Quota Displays the maximum amount of data transfer allowed per session.

Notes Displays any notes that were added using the *Notes* option during voucher creation.

Duration Displays the duration of minutes, hours, or days that the voucher enables the user to access the internet.

Status Indicates whether the voucher is valid for a single use or multiple uses. Displays *Expired* if the voucher is no longer valid. Displays the number of times used and time until expiration for multi-use vouchers.

Actions Click a button to perform the desired action:

- **Print** Click PRINT to print an individual voucher.
- **Revoke** Click REVOKE to immediately deactivate the selected voucher.

Operator Accounts

(Only available for admins with read/write access to the UniFi Controller). Create *Operator Accounts* that can log in to *Hotspot Manager* to view analytics and manage guests, payments or transactions, and vouchers.

Create New Operator To create a new operator account, click + CREATE NEW OPERATOR and complete the following:

- **Account Name** Enter a name for the operator. The *Account Name* should use A-Z, a-z, or 0-9. Spaces and symbols are allowed but not recommended.
- **Password** Enter a password for the operator. The *Password* has to start with A-Z, a-z, or 0-9. The other characters can only be printable ASCII characters.
- **Notes** (Optional) Enter a note to identify or describe the operator.
- **Save** Click **Save** to create the new operator account.
- **Cancel** Click *Cancel* to discard changes.

Name Displays the name of the operator.

Password Displays the password.

Notes Displays any descriptive notes.

Actions Click a button to perform the desired action:

- **Delete** Click DELETE to remove an operator account.

Operator Login

If you create a bookmark for the Hotspot Manager, ensure that you include the site name in the URL, which should be in this format:
https://*unifi.yourdomain.com*:8443/hotspot/s/*site_name*

To test the operator credentials, log out of your admin account and go to the URL of the Hotspot Manager.

The UniFi Hotspot Manager login screen will appear. Enter the username and password in the appropriate fields and click **Sign In**.

Only the *Analytics*, *Guests*, *Payments*, and *Vouchers* tabs will appear.

Appendix A: Portal Customization with Legacy JSP

Before You Begin

Starting with UniFi v5, you have two options for portal customization: AngularJS and Legacy JSP.

AngularJS

AngularJS is the new option for client-side rendering. We recommend AngularJS unless you are using old templates.

Note: AngularJS is not compatible with old templates because the old templates were designed to work with JSP (Java Server Pages).

The UniFi Controller offers a built-in editor to customize AngularJS; however, it is not fully customizable at this time.

AngularJS is a single-page app, so it should work more quickly. However, AngularJS uses JS (JavaScript), which may not work with some really old web browsers or newer browsers with JS support disabled.

AngularJS uses responsive design, so it will adapt to the size of a mobile device, such as a tablet or smartphone.

Appendix A: Portal Customization with Legacy JSP is for Legacy JSP implementation only. See **"Settings > Guest Control" on page 37** for more information about the built-in editor for AngularJS.

Legacy JSP

Legacy JSP is the pre-existing option for server-side rendering. Legacy JSP is fully customizable and uses old HTML, so it should work with any web browser. You can customize Legacy JSP only by overriding files. Legacy JSP works more slowly and is not responsive by default.

Overview

With Legacy JSP, the UniFi Controller software allows complete branding of a portal implementation, allowing you to "white label" your wireless internet service as if you had developed it yourself.

In order to provide the maximum flexibility in your branding effort, the UniFi Controller software provides total access to the portal directory on the system in which it is installed.

This open architecture allows you to include unlimited content while keeping development simple through the use of plain .html (hand code or use any editor of your choice). Testing is simple and immediate; simply reload changes from any browser.

Configuring Portal Customization

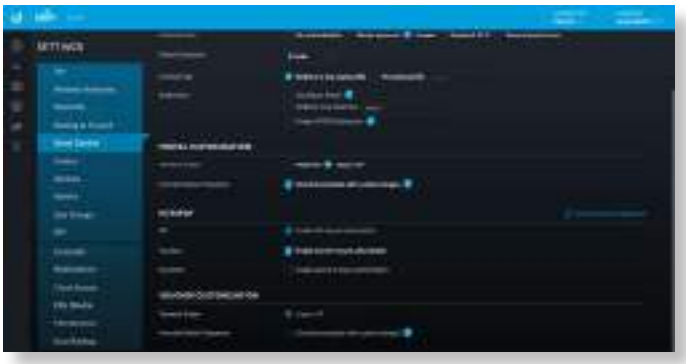
To enable the guest portal with custom Legacy JSP branding, perform the following steps:

1. Go to **Settings** and click **Guest Control**.

2. Select **Enable Guest Portal** to enable it, and then select an authentication method.

Note: See **"Settings > Guest Control" on page 37** for more information.

3. For the *Template Engine* setting, select **Legacy JSP**.
4. For the *Override Default Templates* setting, select **Override templates with custom changes**.



5. Click **Apply Changes**.

Viewing the Default Portal

Once *Guest Portal* and *Override Default Templates* are enabled, connect to the *Guest Network SSID* as shown below, depending on your platform.

Windows

1. Go to **Connect to Network**.
   - **Windows 8** Go to the *Settings* menu and click the *Network* icon.
   - **Windows 10/7** Right-click the *Network* icon.
2. Select the *Guest Network* SSID and click **Connect**.
3. Depending on the security type applied to the network, enter the security key or password. Click **OK** or **Connect**.
4. Launch your web browser and you will be directed to the default portal page for the authentication type configured on the *Guest Portal* (see **"Settings > Guest Control" on page 37** for screenshots of default portal pages by authentication method).

Mac

1. Click the *AirPort* icon in the menu bar (top right side of the screen).
2. Select the *Guest Network* SSID and click **Connect**.
3. Depending on the security type applied to the network, enter the security key or password. Click **OK**.
4. Once connected, the *AirPort* icon will change from gray to solid black. The number of black lines indicates the signal strength.
5. Launch your web browser and you will be directed to the default portal page for the authentication type configured on the *Guest Portal* (see **"Settings > Guest Control" on page 37** for screenshots of default portal pages by authentication method).

Setup

The html and css files are located on the system that the UniFi Controller software has been installed on. The files are in the following locations:

UniFi Cloud Key

/srv/unifi/data/sites/<site_name>/portal

Mac

/Applications/UniFi.app/Contents/Resources/data/sites/<site_name>/portal

Windows

<Drive_Letter>:\Users\<Username>\Ubiquiti UniFi\data\sites\<site_name>\portal

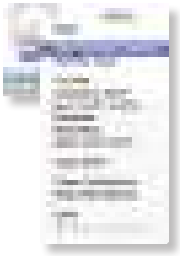
For specific instructions on accessing the files, refer to the specific operating system:

- *Mac*
- **"Windows" on page 160**

Mac

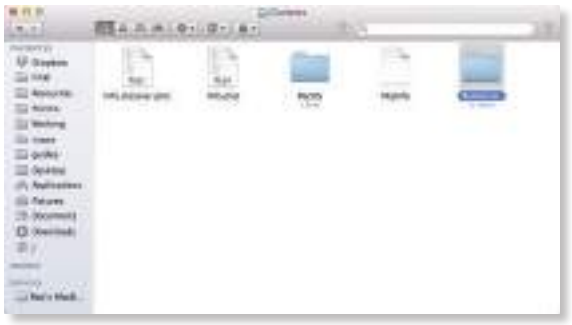
1. Navigate to **Go** > **Applications**.

2. Control-click the **UniFi** application and then click **Show Package Contents**.



3. Double-click the **Contents** folder to open it.

4. Double-click the **Resources** folder to open it.



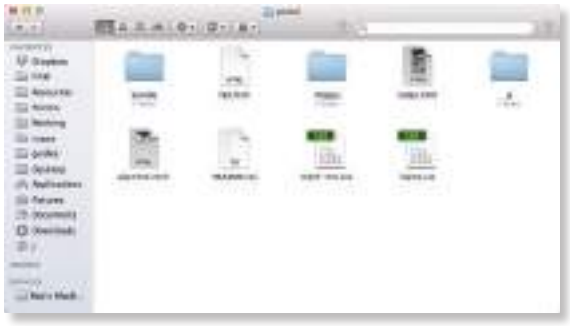
5. Double-click the **data** folder to open it.

6. Double-click the **sites** folder to open it.

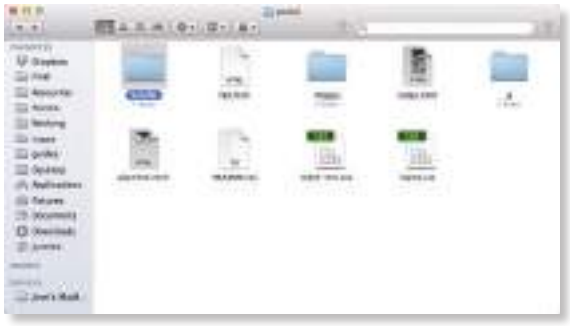
7. Double-click the folder whose name matches the site ID (for example: */manage/s/<site_ID>/dashboard*).

8. Double-click the **portal** folder to open it.

9. You have several files that you can customize in the portal folder (these are described in the *Customizable Default Files* section).



10. To customize the voucher, double-click the **bundle** folder to open it.



11. You can customize voucher.css and voucher.html to fit your needs.

Windows

The Windows files are located in the following location:
<Drive_Letter>:\Users\<Username>\Ubiquiti UniFi\data\sites\<site_name>\portal

Customizable Default Files

The following default customizable html and css files are located in the *portal* folder:

- **index.html** Main landing page that displays pricing to the guest.
- **payment.html** Used to submit credit card information. It requires https and also serves as an example of an additional .html page.
- **fail.html** Displayed when there is an error handling a guest login.
- **reset-min.css** Standardizes the rendering of HTML elements across browsers.
- **styles.css** Controls the style of HTML elements.

The following default files are located in the *bundle* folder:

- **voucher.html** Page for vouchers.
- **voucher.css** Standardizes the rendering of HTML elements across browsers.
- **messages.properties** You can edit this file using a text editor such as TextEdit. This file defines package costs, duration of access, duration of a free trial period, package titles, and how the charge will appear on a customer's credit card account. Error messages are also defined by this file.

Additional details on portal customization can be found in our community site at:
http://ubnt.link/UniFi-Portal-Customization

Appendix B: UniFi Mobile App

Overview

The UniFi app can be used for standalone and Controller modes. For more information about the UniFi app, as well as the UniFi EDU app, go to: http://ubnt.link/UniFi-Mobile-Apps

Standalone Mode

You can use a mobile device to provision a UniFi AP for basic functionality without configuring a UniFi Controller. You have two options:

- Device Discovery
- **"QR Code" on page 162**

UniFi Controller Mode

You can use a mobile device to access the UniFi Controller and adopt a device. Go to **"Controller Mode" on page 164**.

Standalone Mode

We strongly recommend that you change the default login credentials.

1. On the *Account* screen, tap **Standalone Devices**.

2. Enter a unique username and password in the *Username* and *Password* fields. Then change the *Country* if applicable. To save your changes, tap **Done**.

The credentials will be applied to your device the next time you save its configuration.

Device Discovery

You can set up any UniFi AP.

Requirements

- An Ethernet connection from the UniFi AP to the LAN with DHCP
- Firmware version 3.4.4.3231 or higher
- A compatible Android or iOS device

The following instructions describe the iOS version of the app; however, the Android version is similar.

1. Download the UniFi App from the App Store® (iOS) or Google Play™ (Android).

2. On the *Devices Nearby* screen, wait for your device to be discovered. If it is not detected, tap + and go to **"QR Code" on page 162**.

3. Tap the discovered device.

4. You can change the *Device Name* and other settings. For more information, go to **"UniFi Access Point – Configuration" on page 135**.

5. You may be prompted to upgrade the UniFi AP to the latest firmware. Please proceed with the upgrade.

6. Tap **Save** to apply your changes.
7. The new settings are displayed. To make any changes, tap **Configure**.

QR Code

If you don't have an existing Wi-Fi network, you can create one using any UniFi AP.

Requirements

- A UniFi AP with a 2.4 GHz interface
- An Ethernet connection from the UniFi AP to the LAN with DHCP
- Firmware version 3.4.4.3231 or higher
- A compatible Android or iOS device

The following instructions describe the iOS version of the app; however, the Android version is similar.

1. Download the UniFi App from the App Store (iOS) or Google Play (Android).

2. On the *Devices Nearby* screen, tap +.

3. On the *Setup Wizards* screen, tap **Connect to AP's Wi-Fi**.

4. On the *UniFi AP* screen, tap **Next**.

5. Go to **Settings > Wi-Fi** and select **Other...** and follow these instructions:
   a. Tap **Copy** to copy the *Name* from the *Connect to AP's Wi-Fi* screen and paste it in the *Name* field of the *Other Network* screen.
   b. Select **WPA2** for the *Security* setting.
   c. Tap **Copy** to copy the *Password* from the *Connect to AP's Wi-Fi* screen and paste it in the *Password* field of the *Other Network* screen.
   d. Tap **Join**.

Note: For Android, the mobile device automatically connects to the helper SSID. For iOS, manually copy and paste the helper SSID and password.

Connect to AP's Wi-Fi

Other Network

6. Scan the QR code on the back of the UniFi AP.

7. Tap **Done**.

Controller Mode

You can access the UniFi Controller and adopt a device.

Requirements

- An Ethernet connection from the UniFi device to the LAN with DHCP
- Firmware version 3.4.4.3231 or higher
- A compatible Android or iOS device

1. Download the UniFi App from the App Store (iOS) or Google Play (Android).

2. On the *Direct Access* screen, tap the appropriate UniFi Controller.

3. On the *Controller Login* screen, enter your username and password as needed. Then tap **Log In**.

4. On the *Dashboard* screen, tap **Devices**.

5. On the *Devices* screen, tap the device that is pending adoption.

6. Scroll down and tap **Adopt**.

You can use the icons at the bottom of the screen to navigate the various screens of the UniFi Controller.

Appendix C: Controller Scenarios

Overview

The UniFi Controller is a software program that sets up, manages, and monitors UniFi devices, which do not have individual configuration interfaces (except for the UniFi Cloud Key); instead, you use the UniFi Controller as a network management system to configure settings.

For very small installations that don't require a guest portal or advanced features, you can set up UniFi APs in stand-alone mode. Refer to **"UniFi Mobile App" on page 161** for details.

Hosting Controller Software

The UniFi Controller can be hosted on any of the following:

- a local UniFi Cloud Key (a low-power dedicated network device)
- a local server running Linux, Mac OS X 10.11 (or above), or Microsoft Windows 7/8/10
- a remote server running Linux, Mac OS X 10.11 (or above), or Microsoft Windows 7/8/10

Note: The remote controller option requires Layer-3 adoption and management.

Only one instance of the UniFi Controller is required. For example, use either the UniFi Cloud Key or a local server, not both.

A UniFi Cloud Key can be used as a remote controller. For example, if you have a campus-wide UniFi network and each building has its own router, then Layer-3 adoption is required.

Deployment Options

There are different scenarios for the deployment of the UniFi Controller. This chapter describes three examples of typical deployments:

- Local (see below)
- **"Layer-3 Deployment" on page 166**
- **"Hybrid Deployment" on page 167**

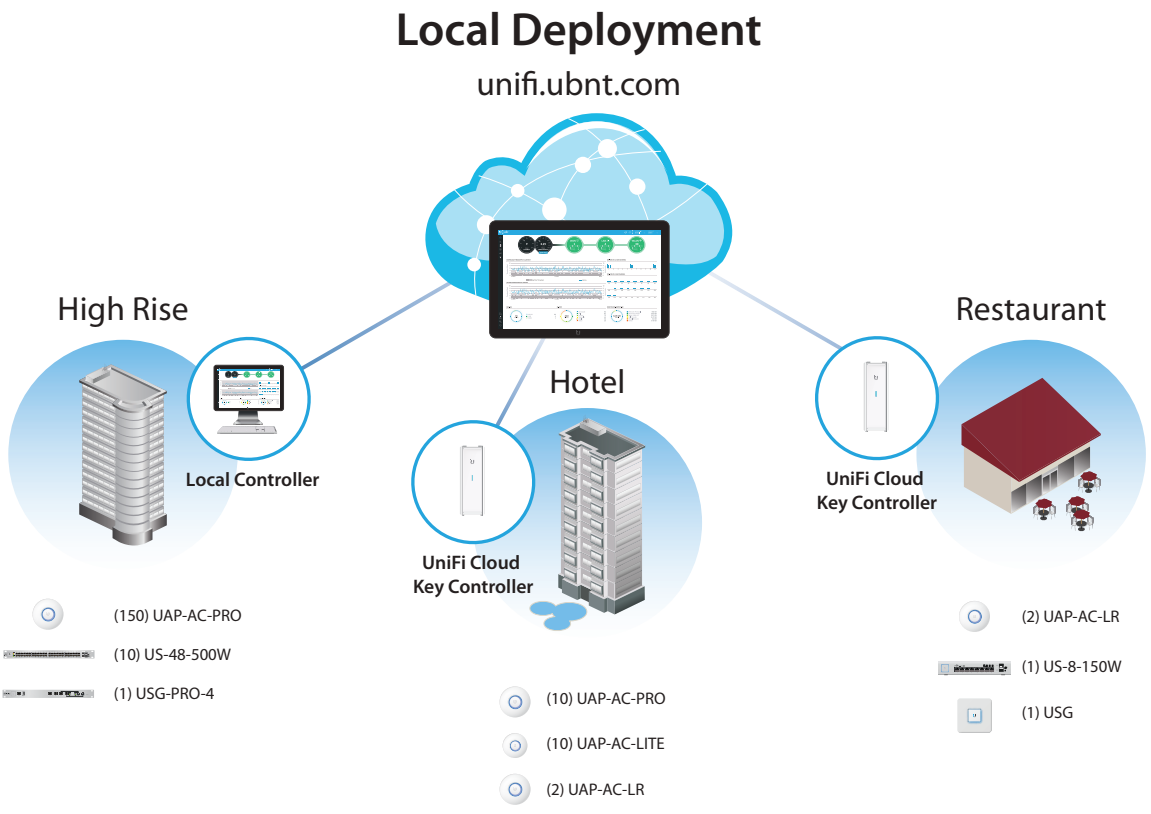
Local Deployment

The application diagram below shows an example of a deployment using local controllers. Each site has a local instance of the UniFi Controller:

- **High rise** The UniFi Controller is running on a computer.
- **Hotel** The UniFi Controller is running on a UniFi Cloud Key.
- **Restaurant** The UniFi Controller is running on a UniFi Cloud Key.

Remote Access

Cloud access is enabled on the UniFi Controllers, so you can use **unifi.ubnt.com** to remotely monitor and access multiple controllers. Each controller, in turn, can manage multiple sites.



Layer-3 Deployment

The application diagram below shows an example of a deployment using a remote controller.

The UniFi Controller is running in the cloud or your NOC (Network Operating Center).

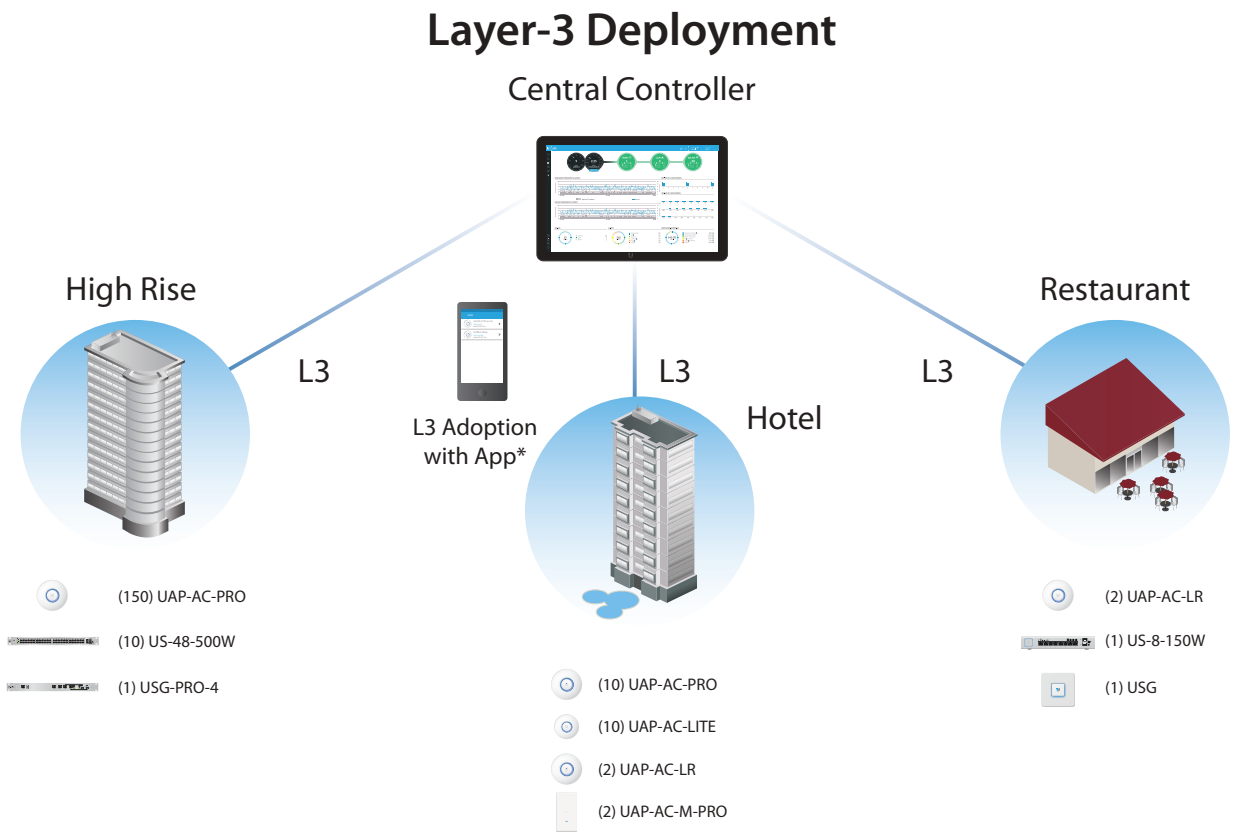
- **High rise** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.
- **Hotel** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.
- **Restaurant** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.

There are multiple methods to carry out Layer-3 adoption.

Here is an overview of a typical example:

1. Create a remote controller.
2. At the customer site, open a browser to the remote controller.
3. Use one of the following methods to configure all local APs so they inform back to the UniFi Controller:
   - **"UniFi Mobile App" on page 168**
   - **"DNS" on page 169**
   - **"DHCP Option 43" on page 169**
   - **"SSH" on page 169**

For details about Layer-3 adoption, go to **"Layer-3 Adoption" on page 168**.



* Refer to **"Layer-3 Adoption" on page 168** for other methods that can be used.

Hybrid Deployment

The application diagram below shows an example of a deployment using local and remote controllers.

Your sites use a mixture of controller types. Some sites have local instances of the UniFi Controller, while other sites have a remote UniFi Controller.

- **Sites 1, 2, and 3** The UniFi Controller is off-site. Use Layer-3 adoption to manage these sites.

  Note: For details about Layer-3 adoption, go to **"Layer-3 Adoption" on page 168**.

- **Hotel** The UniFi Controller is running on a UniFi Cloud Key.
- **Restaurant** The UniFi Controller is running on a UniFi Cloud Key.

Remote Access

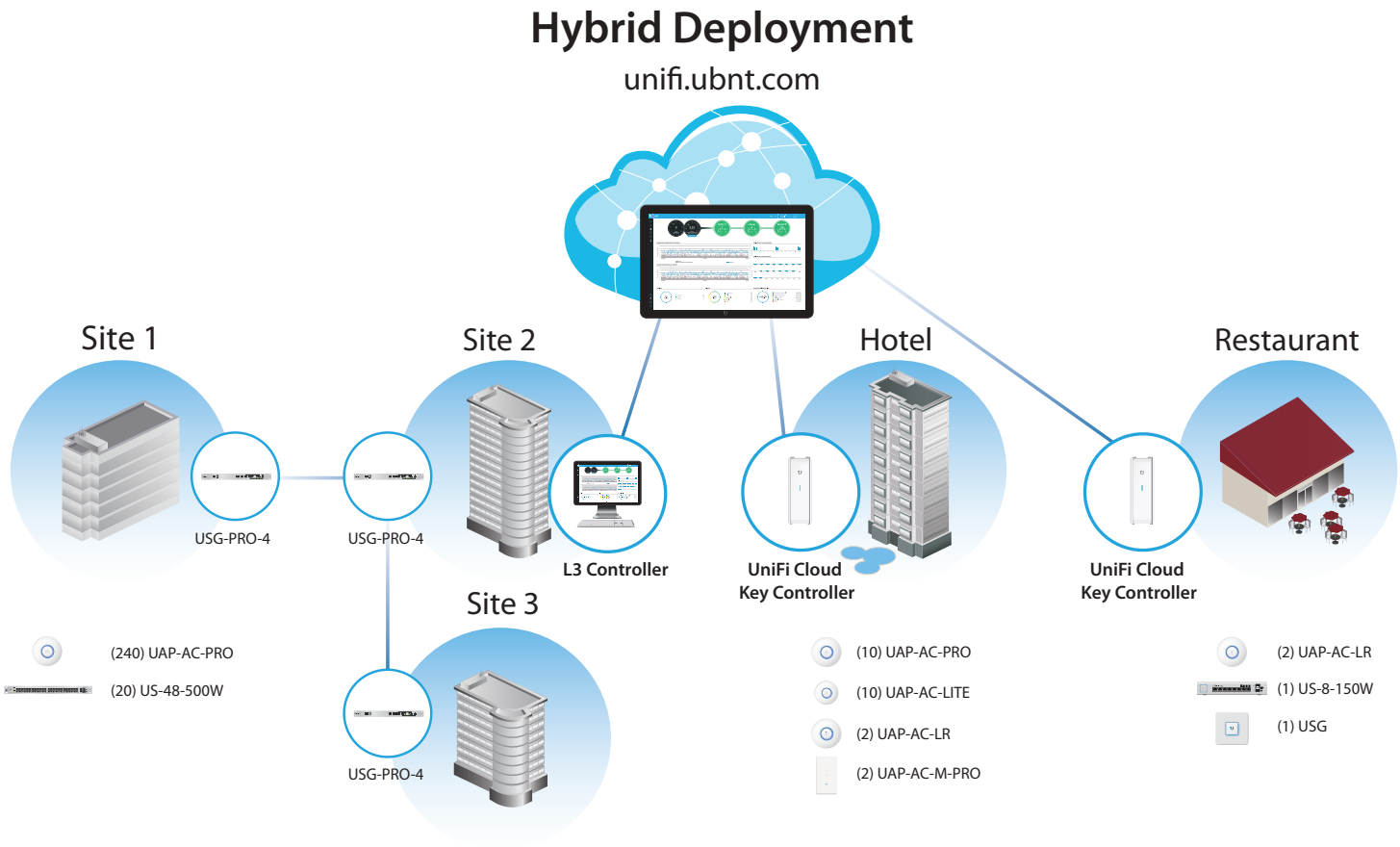
Cloud access is enabled on the UniFi Controllers, so you can use **unifi.ubnt.com** to remotely monitor and access multiple controllers. Each controller, in turn, can manage multiple sites.

For example, in the application diagram below, you can use **unifi.ubnt.com** to access three controllers:

- remote controller
- UniFi Cloud Key controller for the hotel
- UniFi Cloud Key controller for the restaurant

In turn, the remote controller manages three sites:

- Site 1
- Site 2
- Site 3



Layer-3 Adoption

Here is an overview of a typical example:

1. Create your controller.
2. At the customer site, open a browser to the UniFi Controller.
3. Every UniFi AP has a default inform URL: *http://unifi:8080/inform*

   Use one of the following methods to configure all local APs so they inform back to the UniFi Controller:

   - UniFi Mobile App
   - **"DNS" on page 169**
   - **"DHCP Option 43" on page 169**
   - **"SSH" on page 169**

UniFi Mobile App

1. Launch the UniFi mobile app from your mobile device.

2. On the *Direct Access* screen, tap the appropriate UniFi Controller.

3. On the *Controller Login* screen, enter your username and password as needed. Then tap **Log In**.

4. Tap **More**.
5. Tap **Layer 3 Adoption**.

6. Tap the device you want to adopt.

7. Tap **Adopt** to confirm.

DNS

You have a couple of options:

DNS resolution Configure your DNS server to resolve *unifi* to the IP address of the UniFi Controller.

Ensure that the UniFi AP can resolve the domain name of the UniFi Controller. For example, if you have configured *http://<XYZ>:8080/inform*, then ping the UniFi Controller from the UniFi AP to determine if *<XYZ>* can be resolved or reached.

FQDN Use FQDN for the inform URL of the UniFi Controller: *http://FQDN:8080/inform*

If the UniFi AP (using a static IP address) fails to connect to the remote UniFi Controller, then ensure that you have properly configured the IP address of the DNS server when you changed the UniFi AP from DHCP to static in the UniFi Controller UI. If not properly configured, then the UniFi AP cannot contact the DNS server to resolve the domain name of the UniFi Controller.

If the UniFi AP has been reset to its factory defaults, then ensure that you have informed the UniFi AP twice (using the UniFi mobile app) about the location of the UniFi Controller.

DHCP Option 43

Instructions vary depending on the router you are using.

EdgeMAX If you are using a Ubiquiti® EdgeMAX® or EdgePoint® router, then follow these instructions:

1. Access the user interface of the EdgeMAX router.
2. Click the **Services** tab.
3. Go to **Actions > View Details** for the appropriate DHCP server.

4. In the *UniFi Controller* field, enter the IP address of the UniFi Controller. Then click **Save**.

The DHCP server will return the IP address of the UniFi Controller to its DHCP clients, so if a client is a UniFi AP, it will know how to contact the UniFi Controller.

Linux ISC DHCP Server Configure the dhcpd.conf file:

```
# ...
option space ubnt;
option ubnt.unifi-address code 1 = ip-address;
class “ubnt” {
   match if substring (option vendor-class-identifier,
   0, 4) = “ubnt”;
   option vendor-class-identifier “ubnt”;
   vendor-option-space ubnt;
}
subnet 10.10.10.0 netmask 255.255.255.0 {
   range 10.10.10.100 10.10.10.160;
   option ubnt.unifi-address 201.10.7.31;  ### UniFi
   Controller IP ###
   option routers 10.10.10.2;
   option broadcast-address 10.10.10.255;
   option domain-name-servers 168.95.1.1, 8.8.8.8;
   # ...
}
```

Note: You can also use the IP address of the UniFi Controller instead of the domain name in the inform URL.

Instructions for other DHCP servers are available at: **http://ubnt.link/UniFi-Layer3-Adoption**

SSH

If you can SSH into the UniFi AP, then you can perform the Layer-3 adoption via CLI command:

1. Use the UniFi mobile app to ensure that the UniFi AP is running the same firmware as the UniFi Controller. If it is not, then follow the instructions at: **http://ubnt.link/UniFi-SSH-Firmware-Upgrade**
2. Use the UniFi mobile app to ensure that the UniFi AP is in the factory default state. If it is not, then SSH into the UniFi AP and run:

   ```
   syswrapper.sh restore-default
   ```

3. SSH into the UniFi AP and enter:

   ```
   mca-cli
   set-inform http://<ip-of-controller>:8080/inform
   ```

Appendix D: Contact Information

Ubiquiti Networks Support

Ubiquiti Support Engineers are located around the world and are dedicated to helping customers resolve software, hardware compatibility, or field issues as quickly as possible. We strive to respond to support inquiries within a 24-hour period.

Ubiquiti Networks, Inc.
685 Third Avenue, 27th Floor
New York, NY 10017 USA
www.ubnt.com

Online Resources

Support: **ubnt.link/UniFi-Support**

Community: **community.ubnt.com/unifi**

Downloads: **downloads.ubnt.com/unifi**

JLAI022318

www.ubnt.com