UBIQUITI
NETWORKS

UniFi®

Enterprise System Controller

Release Version: 5.4.8

User Guide

Table of Contents

Chapter 1: Software Installation 1
Introduction 1
System Requirements 1
Network Topology Requirements 1
Software Installation 1

Chapter 2: UniFi Cloud 5
Introduction 5
UniFi Cloud Key 5
UniFi Cloud Account 12

Chapter 3: Using the UniFi Controller Software 17
Navigation Bar 17
Common Interface Options 17

Chapter 4: Dashboard 47
Latency 47
Throughput 47
WAN 48
LAN 48
WLAN 49
Download Throughput & Latency 49
Upload Throughput & Latency 49
Devices on 2.4 GHz Channel 50
Devices on 5 GHz Channel 50
Devices 50
Clients 50
Deep Packet Inspection 50

Chapter 5: Map 53
Adding Custom Maps 53
Adding a Google Map 54
Placing Devices on the Map 55
Map Display Options 56
Setting the Map Scale 57
System Topology 57

Chapter 6: Devices 59
All 60
Gateway/Switches 61
APs 62
Phones 65

Chapter 7: Clients 67
All. 68
Wireless 69
Wired 69
Chapter 8: Statistics 71
Overview. 71
Traffic Stats. 73
Chapter 9: Insights 75
Known Clients 76
Neighboring Access Points 76
Past Connections 77
Past Guest Authorizations 77
Switch Stats 78
Port Forward Stats. 81
Dynamic DNS 82
Remote User VPN. 83
AC-EDU Streams. 83
Chapter 10: UniFi Security Gateway Details 85
Properties 85
UniFi Security Gateway – Details 86
UniFi Security Gateway – Networks 86
UniFi Security Gateway – Configuration 87
Chapter 11: UniFi Switch Details 93
Properties 93
UniFi Switch – Details. 94
UniFi Switch – Ports 95
Mirroring. 97
UniFi Switch – Configuration. 98
Chapter 12: UniFi Access Point Details 103
Properties 103
UniFi Access Point – Details 104
UniFi Access Point – Users 107
UniFi Access Point – Guests 108
UniFi Access Point – Configuration 108
Chapter 13: UniFi VoIP Phone Details 115
Properties 115
UniFi VoIP Phone – Details 115
UniFi VoIP Phone – Configuration 116

Chapter 14: Client Details. 117
Properties 117
Wireless Client – Details 117
Wireless Client – Statistics 118
Wireless Client – History 118
Wireless Client – Configuration 119
Wired Client – Details 119
Wired Client – Statistics 119
Wired Client – History 120
Wired Client – Configuration 120
Chapter 15: Hotspot Manager 121
Guests 121
Payments and Transactions 122
Vouchers 122
Operator Accounts 123
Appendix A: Portal Customization with Legacy JSP. 125
Before You Begin 125
Overview. 125
Configuring Portal Customization. 125
Viewing the Default Portal 126
Setup 126
Appendix B: UniFi Discovery Utility 129
Overview. 129
Launching the UniFi Discovery Utility 129
UniFi Discovery Utility Interface 129
Appendix C: UniFi Mobile App 133
Overview. 133
Basic Setup. 133
Controller Mode 136
Appendix D: UniFi EDU Mobile App. 147
Overview. 147
Broadcast 147
Schedule 149
Recordings 150
Volume 151
Settings 151

Appendix E: Controller Scenarios 153
Overview. 153
Hosting Controller Software 153
Deployment Options 153
Layer-3 Adoption 156
Appendix F: Contact Information 159
Ubiquiti Networks Support 159

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.

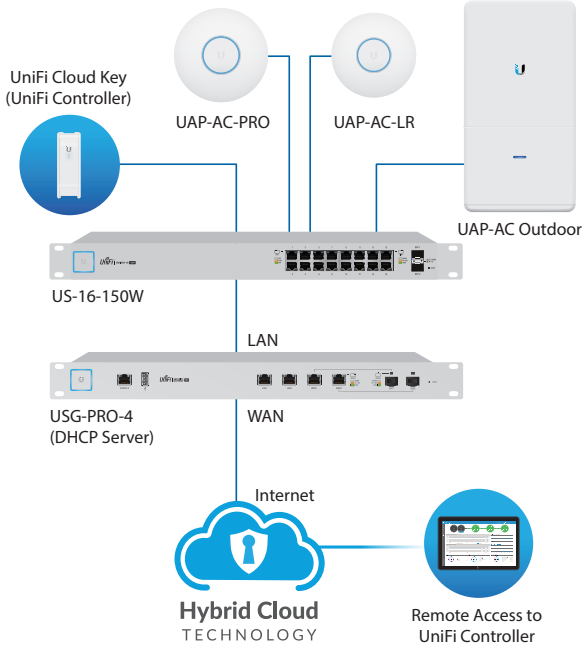
This User Guide is for use with version 5.4.8 or above of the UniFi Controller software.

System Requirements

- Linux, Mac OS X 10.11 (or above), or Microsoft Windows 7/8/10
- Java Runtime Environment 1.6 (1.8 or above recommended)
- Web Browser: Mozilla Firefox, Google Chrome, Microsoft Edge, or Microsoft Internet Explorer 11 (or above)

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 12** for more information.

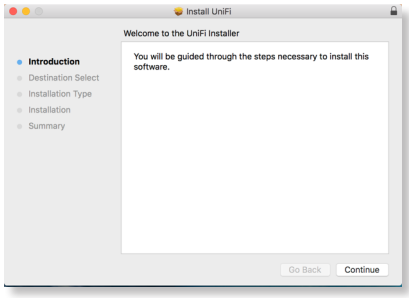
Linux Users

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

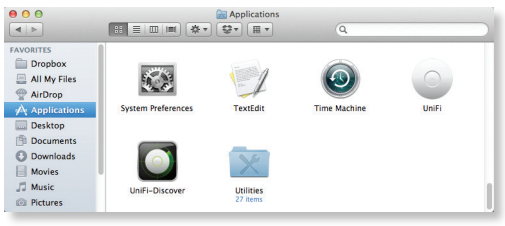
Mac Users

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.

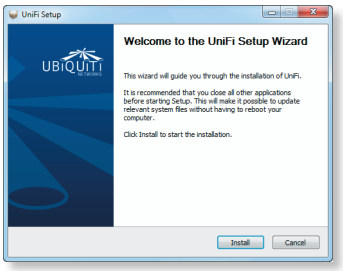


Proceed to **"Configuring the UniFi Controller Software"**

on page 2.

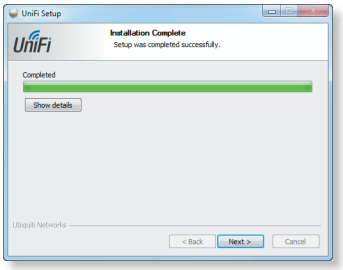
PC Users

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

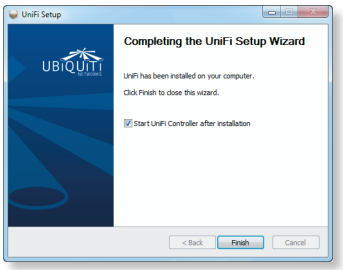


3. If your computer doesn't have Java 1.6 or above installed, you will be prompted to install it. Click **Install** to continue.

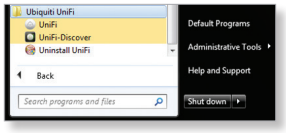
4. Click **Next**.



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**.

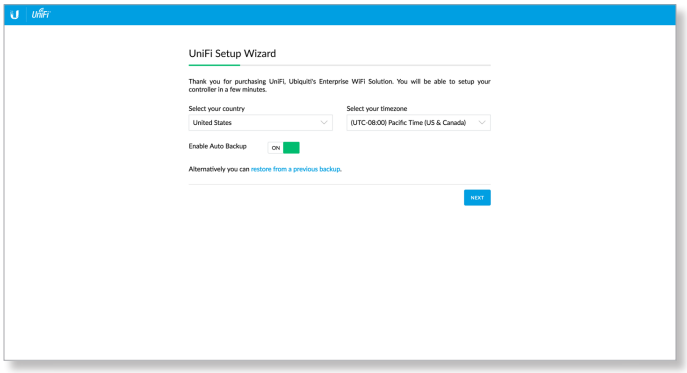


Configuring the UniFi Controller Software

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**

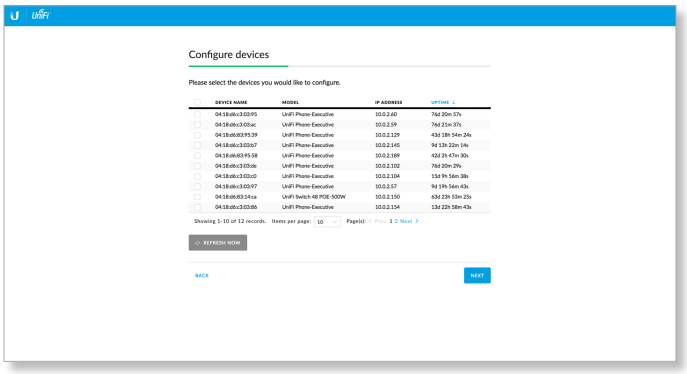
2. Select your country and time zone. Alternatively, you can click **restore from a previous backup** to use a file that contains your backup settings. Click **Next**.



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

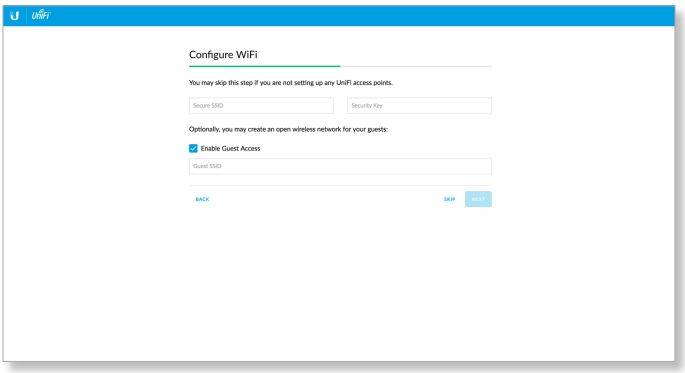
Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

3. Select the devices that you want to configure and click **Next**. You can click **Refresh Now** to have the UniFi Controller repeat its device discovery process.



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:

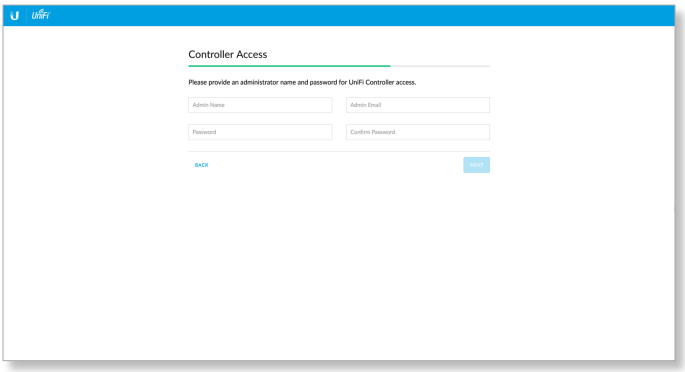
a. Enter the wireless network name (SSID) in the *Secure SSID* field.

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 super admin 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.

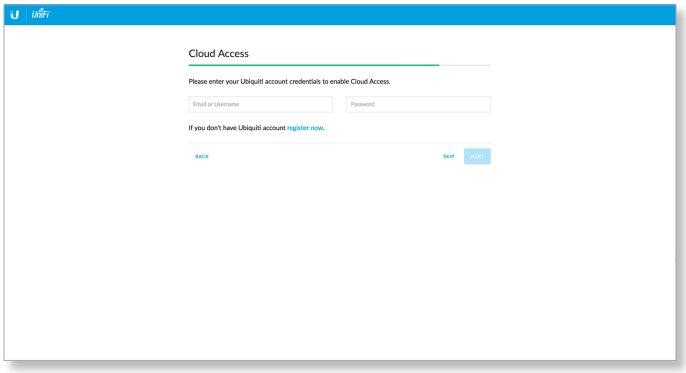
c. Enter a password in the *Password* field to use when accessing the management interface as a super admin.

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

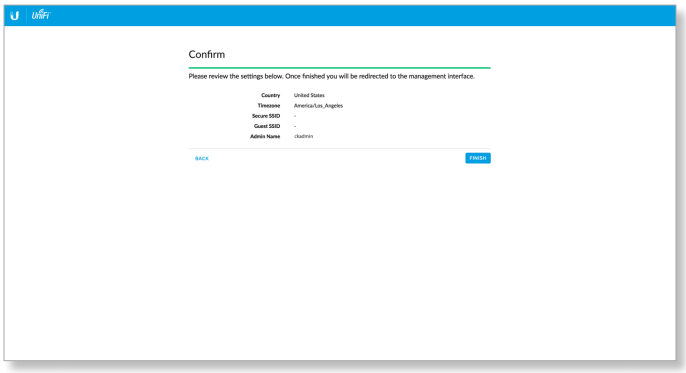
e. Click **Next**.

Note: Only the super admin – not any site admin – can view wired devices that are *Pending Approval* and then adopt them on the UniFi Controller. Ensure that you save the super admin login information for future use.

6. Enter your Ubiquiti account email/username and password to enable to Cloud Access. Alternatively, you can click **register now**, to create a Ubiquiti account. Click **Next**.

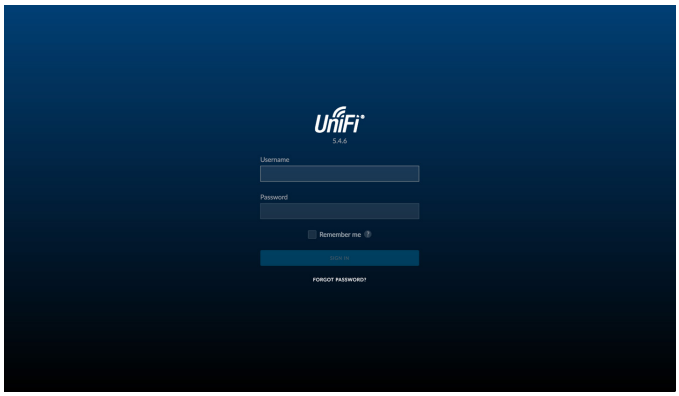


7. Review your settings. Click **Finish** to save your settings or click *Back* to make changes. Once the wizard is finished, the browser will be redirected to the management interface.



Congratulations, your wireless network is now configured.

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.

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 12**

UniFi Cloud Key

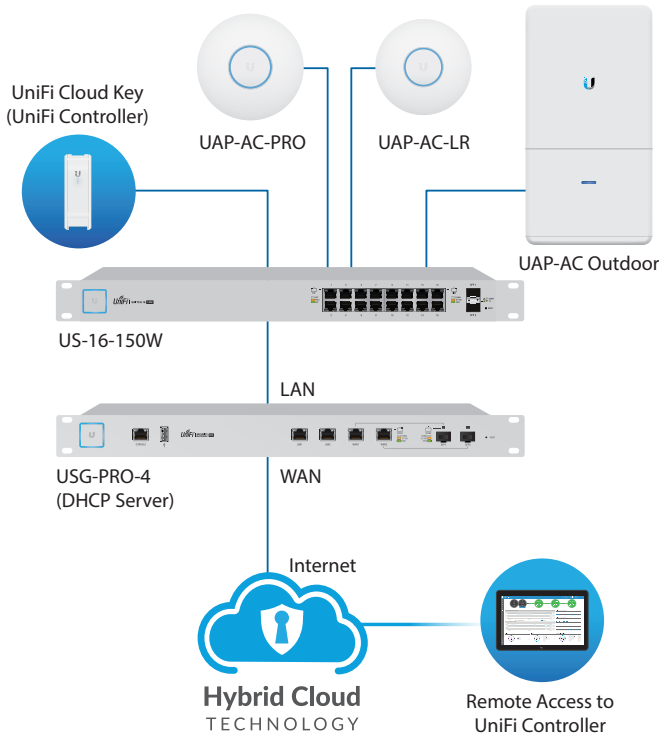
The UniFi Cloud Key includes the pre-installed UniFi Controller software.

System Requirement

Web Browser: Google Chrome, Mozilla Firefox, Microsoft Edge, or Microsoft Internet Explorer 11 (or above)

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:

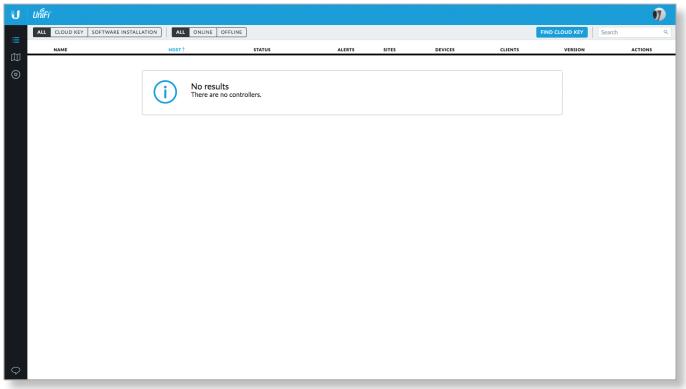
- If you are using Chrome, go to the *Chrome Instructions* section (recommended).
- If you are using a different web browser, go to **"Instructions for Other Web Browsers" on page 7**.

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 **Find Cloud Key**.

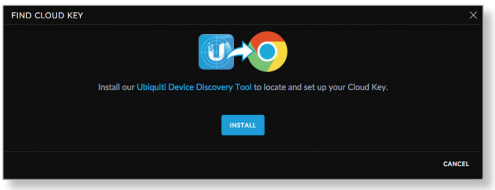


Note: The default fallback IP address of the UniFi Cloud Key is *192.168.1.30*.

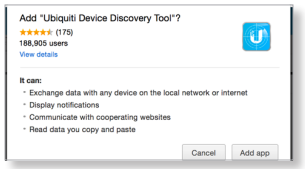
5. If the Ubiquiti® Device Discovery Tool is already installed, proceed to step 7.

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

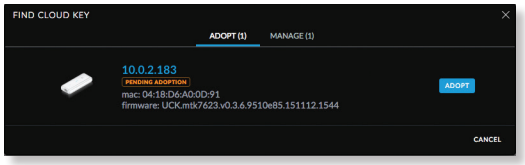
6. To install the tool:
   a. Click **Install**.



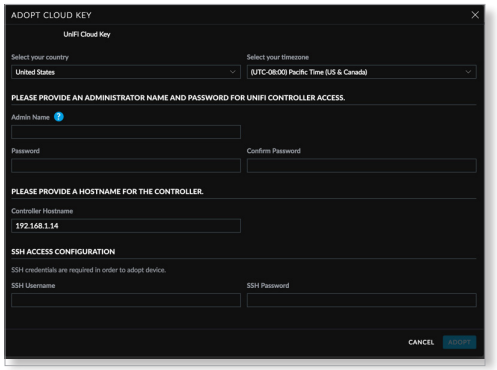
   b. Click **Add app** to confirm.



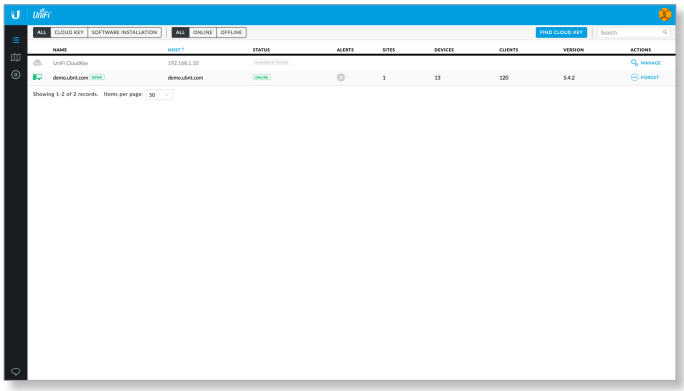
7. The Ubiquiti Device Discovery Tool will search for the UniFi Cloud Key. Select it to continue.



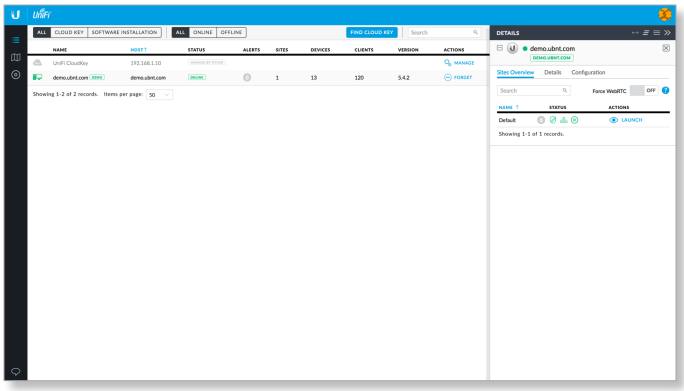
8. Configure the UniFi Controller:
   a. Select the appropriate country.
   b. Select the appropriate time zone.
   c. Enter an admin name in the *Admin Name* field and a password in the *Password* field to use when accessing the management interface.
   d. Confirm your password in the *Confirm Password* field.
   e. Keep the IP address or enter a hostname in the *Controller Hostname* field.
   f. If you want to set up an SSH login for management access to the UniFi Cloud Key, then select **Use non-default SSH credentials**. Enter a username in the *SSH Username* field, and enter a password in the *SSH Password* field.
   g. Click **Submit** to save your changes.



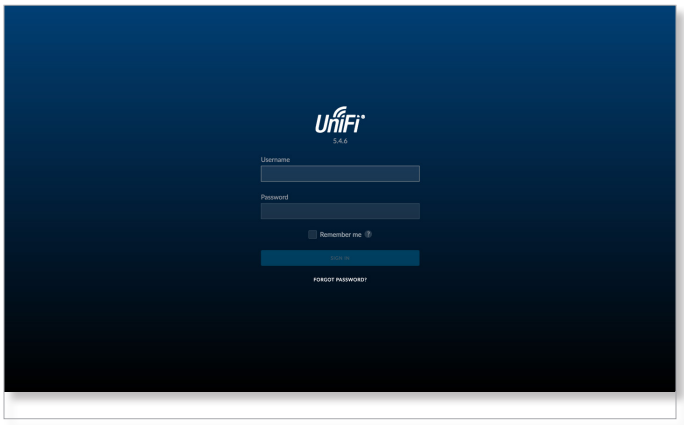
9. Wait for the UniFi Controller to be adopted, and then select it.



10. Click **Launch**.



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: 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.

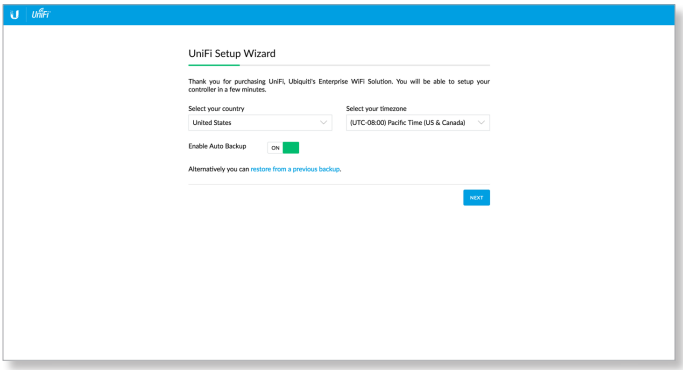
   Note: The default fallback IP address of the UniFi Cloud Key is *192.168.1.30*.

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.

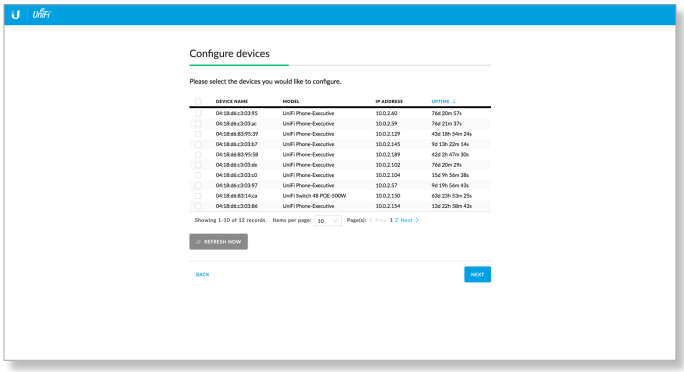
   Note: You can click *Configure* to change the settings of the UniFi Cloud Key (refer to **"UniFi Cloud Key Configuration" on page 8** for more information). The default login is *ubnt/ubnt* or *root/ubnt*.

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

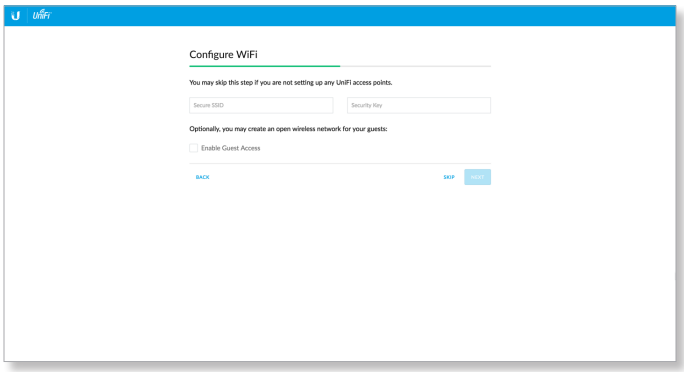


   Note: U.S. product versions are locked to the U.S. Country Code to ensure compliance with FCC regulations.

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



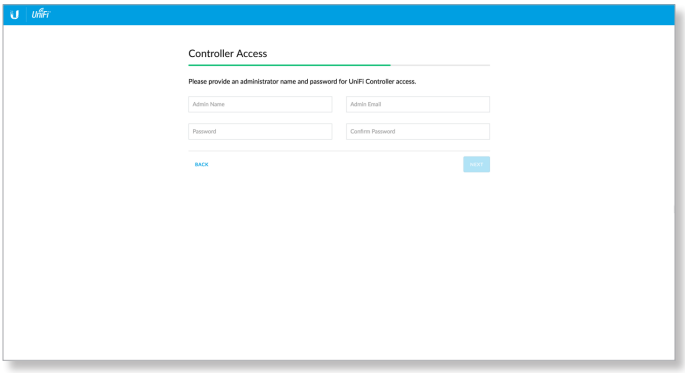
7. The UniFi Setup Wizard will create a secure primary wireless network for your devices.



   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 super admin 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.

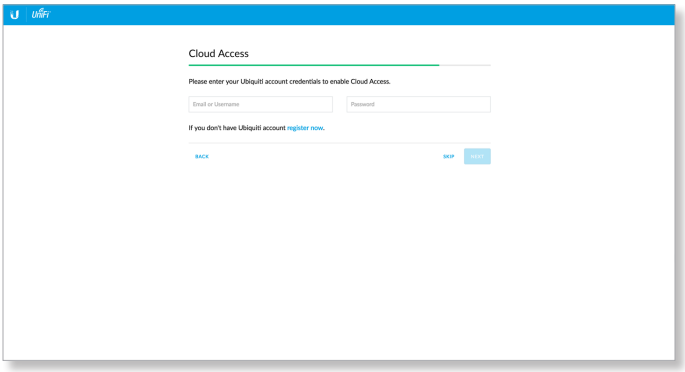
c. Enter a password in the *Password* field to use when accessing the management interface as a super admin.

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

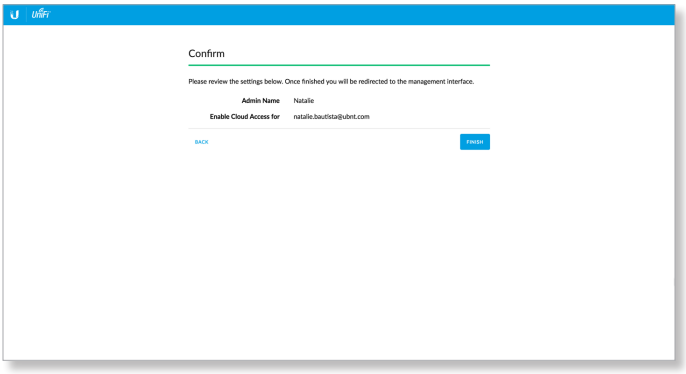
e. Click **Next**.

Note: Only the super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller. Ensure that you save the super admin login information for future use.

9. Enter your Ubiquiti account email/username and password to enable to Cloud Access. Alternatively, you can click **register now**, to create a Ubiquiti account. Click **Next**.

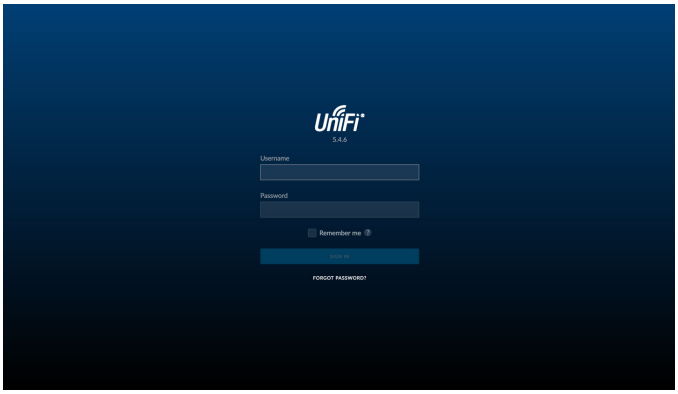


10. Review your settings. Click **Finish** to save your settings or click *Back* to make changes. Once the wizard is finished, the browser will be redirected to the management interface.



Congratulations, your wireless network is now configured.

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: A future feature will enable backup of 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.

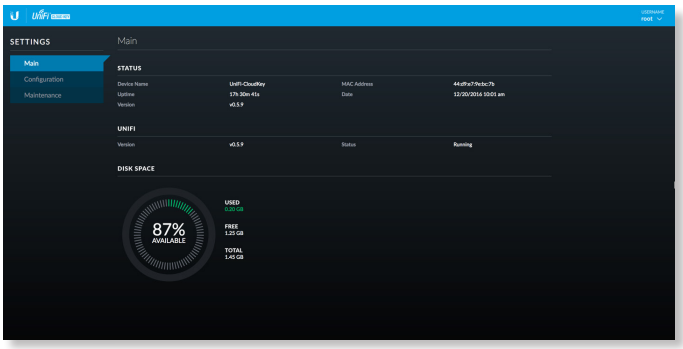
5. After you click *Configure*, enter the *Username* and *Password* (the default login is *ubnt*/*ubnt*). Then click **Login**.

The *Main* screen will appear.

Navigation Bar

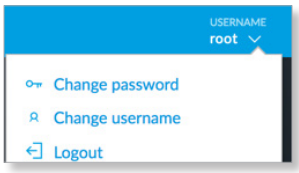
The UniFi Cloud Key configuration consists of three primary pages:

- *Main* (see next column)
- **"Configuration" on page 10**
- **"Maintenance" on page 11**

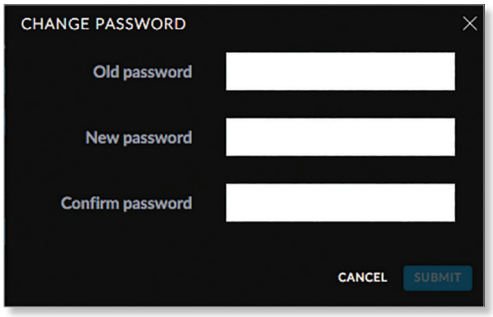


Username

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:

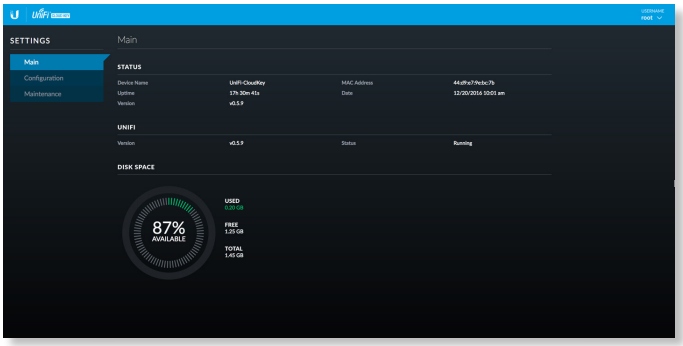


- **Old password** Enter the current password (the default is *ubnt*).
- **New password** Enter the new password.
- **Confirm Password** Enter the new password again.
- **Submit** Click **Submit** to apply changes.
- **Cancel** Click *Cancel* to discard changes.

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.

Disk Space

Available Displays the percentage of available disk space.

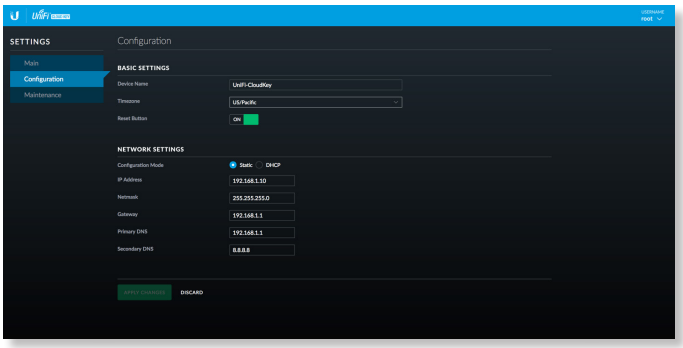
Used Displays the amount of used disk space.

Free Displays the amount of available disk space.

Total Displays the total amount of disk space.

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.

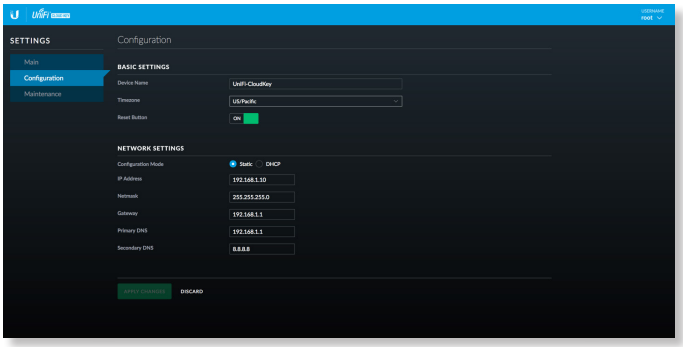
Time Zone Select the appropriate time zone.

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*.

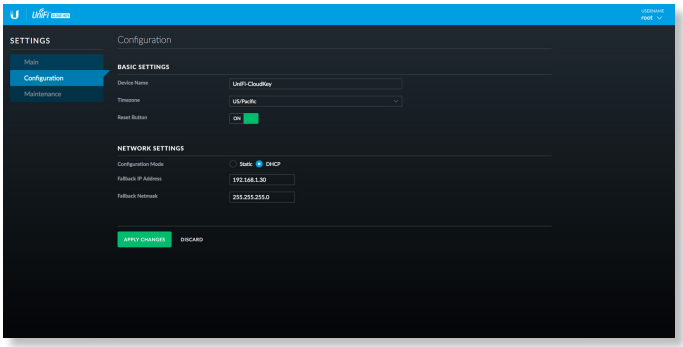
Network Settings

Configuration Mode Select the Internet connection type for your service: **Static** or **DHCP**.

- **Static** 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 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.

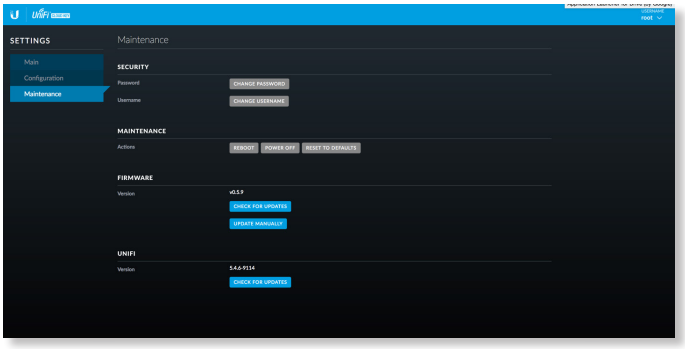


Apply Changes Click **Apply Changes** to save changes.

Discard Click *Discard* to cancel changes.

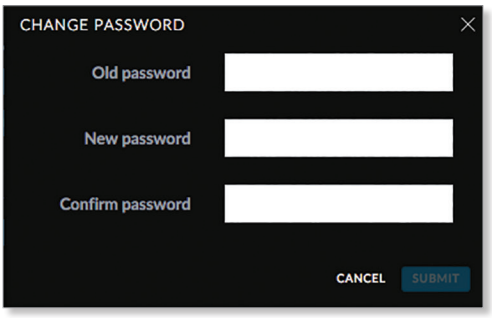
Maintenance

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, 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.

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 43** for more information) before resetting the UniFi Cloud Key to its defaults.

Firmware

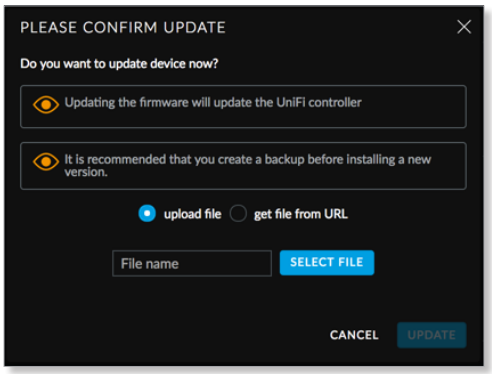
Version Displays the version number of the UniFi Cloud Key firmware.

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.

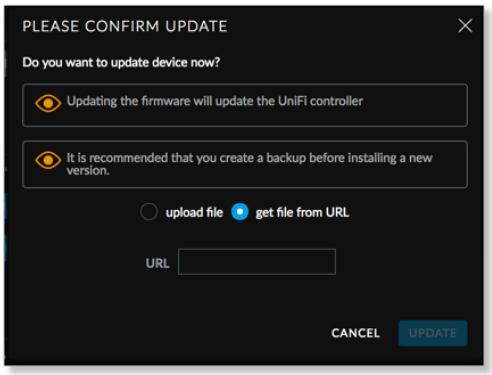
Update Manually Click **Update Manually** to update the firmware. The *Please Confirm Update* screen will appear.

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 43** 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 43** for more information) before upgrading the Unii Controller software.

UniFi Cloud Account

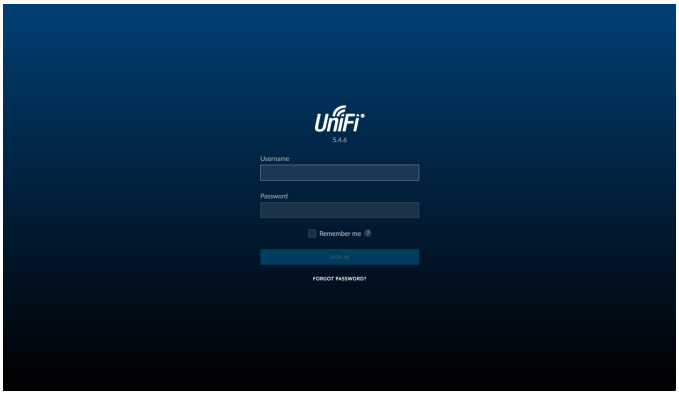
You must be a super admin for initial cloud management. Once cloud access is enabled by the super admin, then any other admin can also enable cloud access.

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

Login Instructions

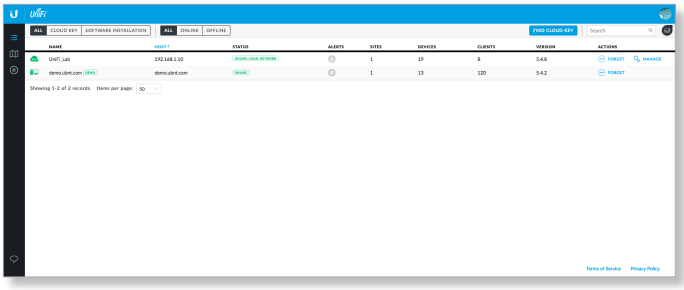
1. Launch the Chrome web browser and type **https://** followed by the appropriate *Controller Hostname/IP* address as specified in **"Settings > Controller" on page 41**. Press **enter** (PC) or **return** (Mac).

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



Note: If you do not have an account, click **Register** and follow the on-screen instructions.

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.

A secondary filter is available:

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

Find 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 14** 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
- **Manage By Other** MANAGE BY OTHER

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.

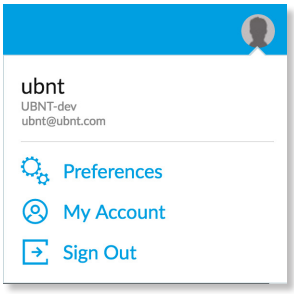
Actions Click a button to perform the desired action:

- **Forget** Click FORGET to remove the UniFi Controller from your cloud account.
- **Manage** Click MANAGE to manage the UniFi Controller or the UniFi cloud key. 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. Proceed to **"UniFi Cloud Key Configuration" on page 8** for more information.

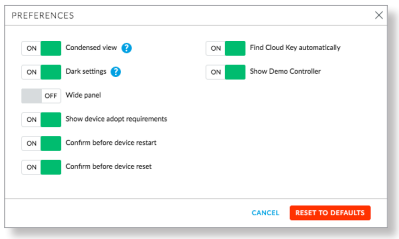
Chat At the lower left of the screen, click to open a window for online chat support.

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:



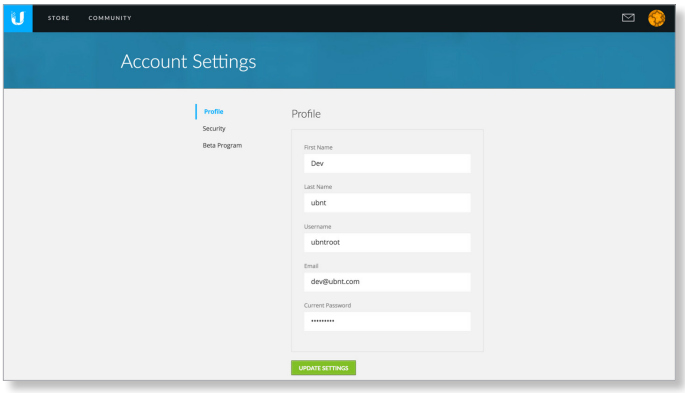
Preferences To change your account preferences, click Preferences. The *Preferences* screen will appear:



The available settings are:

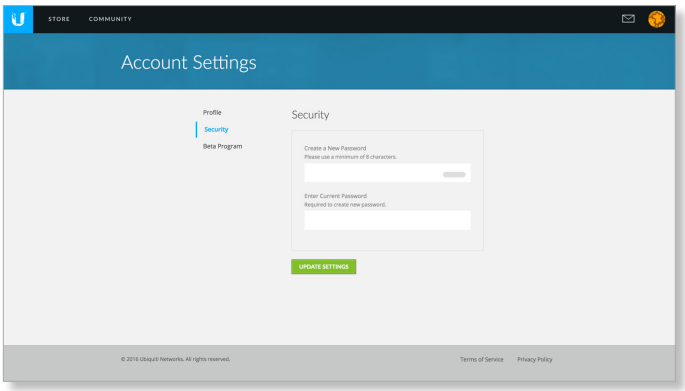
- **Condensed view** Enabled by default. The table padding is condensed and the font size is minimized to fit as much data on the screen as possible.
- **Dark settings** Enabled by default. A dark theme is used on the *Settings* screens.
- **Wide panel** Disabled by default. If enabled, the *Details* 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** Enabled by default.
- **Show Demo Controller** Enabled by default.

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



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

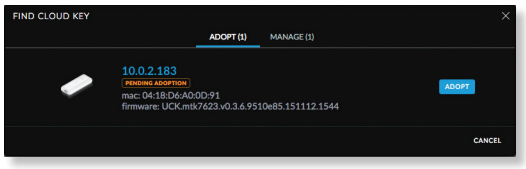


- **Beta Program** Follow the on-screen instructions if you want to join the beta program.

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

Find Cloud Key

To add a UniFi Cloud Key, click **Find Cloud Key** at the top right of the screen. The *Find Cloud Key* screen will appear:



Adopt

IP address Displays the IP address of the UniFi Cloud Key.

(status) Displays the status information: *Pending Adoption*.

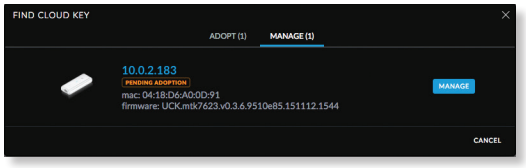
mac Displays the MAC address or hardware identifier of the UniFi Cloud Key.

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

Adopt Click to adopt the UniFi Cloud Key. Refer to step 8 of **"Chrome Instructions" on page 5** for more information.

Cancel Click to exit this screen.

Manage



IP address Displays the IP address of the UniFi Cloud Key.

(status) Displays the status information: *Adopted* or *Pending Adoption*.

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

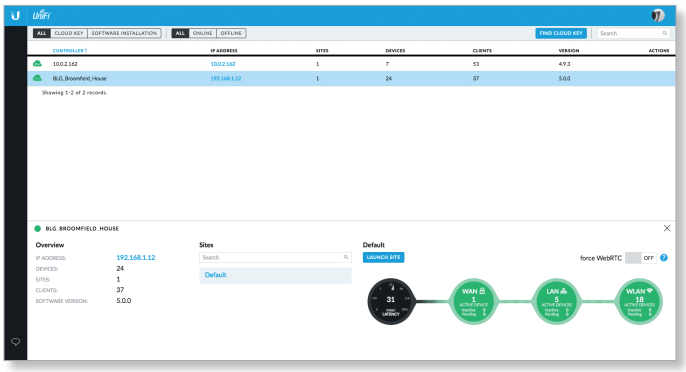
firmware Displays the firmware version number of the UniFi Cloud Key.

Manage Click to configure the UniFi Cloud Key. Refer to **"UniFi Cloud Key Configuration" on page 8** for more information.

Cancel Click to exit this screen.

Additional Details

Select a UniFi Controller to display more information at the bottom of the screen.



- **(icon)** Green indicates an active UniFi Controller. Gray indicates an inactive UniFi Controller.

Overview

- **(controller_name)** Displays the *Controller Hostname/IP* address as specified in **"Settings > Controller" on page 41**.
- **IP Address** Displays the IP address of the device running 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.
- **Software Version** Displays the software version number of your UniFi Controller.
- **Actions** Click a button to perform the desired action:
  - **Remove** Click REMOVE to remove the UniFi Controller from your cloud account.

Sites

- **Search** Search Enter the text you want to search for. Simply begin typing; there is no need to press **Enter**.
- **(site_name)** Displays the name of the site. You can click the name to get additional details on the right.
- **(Unread Alerts)** 6 Displays the number of unread alerts.

(site_name)

- **Launch Site** Click **Launch Site** to access the UniFi Controller. Proceed to **"Using the UniFi Controller Software" on page 17** for more information.

Note: If you have an issue accessing the local Controller, then click **force WebRTC**.

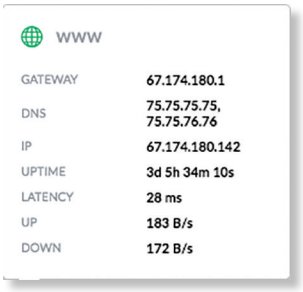
- **(map)** Displays a visual representation of your network's status. The status of each dashboard node is indicated by color:
  - **Black** Black indicates that the Internet connection is active.
  - **Green** Green indicates that the node is active and all devices are online.

  - **Red** Red indicates one of the following:
    - **WWW** Internet connectivity is down.
    - **WAN** The UniFi Security Gateway is offline.
    - **LAN** One or more Switches are offline.
    - **WLAN** More than half of the APs are offline.

  - **Gray** Gray indicates that there is no Internet connection or there are no devices available for that node.

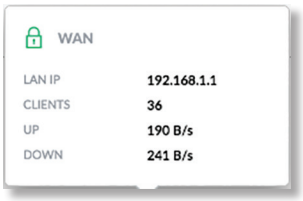
You can place the mouse over each node icon to display basic status information.

- **WWW** The basic details of the Internet connection are displayed.

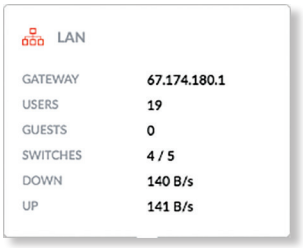


  - **Gateway** Displays the IP address of the service provider's gateway.
  - **DNS** Displays the IP addresses of the Domain Name System (DNS) servers.
  - **IP** Displays the Internet IP address of the UniFi Security Gateway.
  - **Uptime** Displays the length of time the Internet connection has been 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.

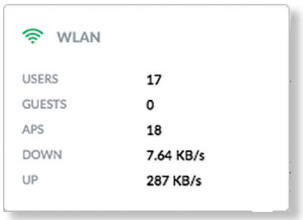
- **WAN** The basic details of the UniFi Security Gateway connection are displayed.



  - **LAN IP** Displays the local IP address of the UniFi Security Gateway.
  - **Clients** Displays the total number of local clients.
  - **Up** Displays the upload rate of the UniFi Security Gateway.
  - **Down** Displays the download rate of the UniFi Security Gateway.
- **LAN** The basic details of the wired network(s) are displayed.



  - **Gateway** Displays the IP address of the service provider's 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 connected to the wired network.
  - **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.



  - **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).

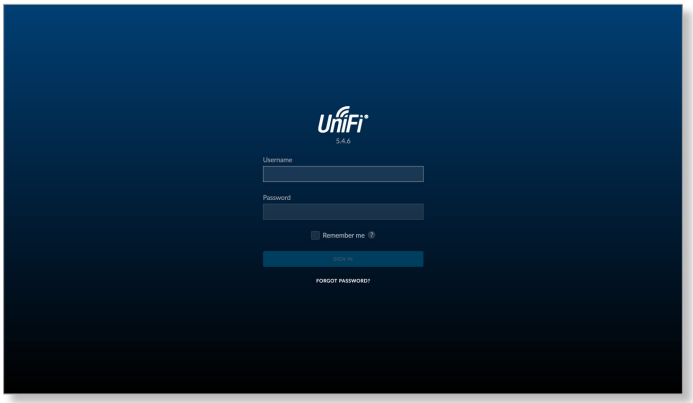
- **APs** Displays the number of APs in the primary wireless network(s) and the number of APs in the guest wireless network(s).
- **Down** Displays the download rate of the wireless network(s).
- **Up** Displays the upload rate of the wireless network(s).

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 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 47

"Map" on page 53

"Devices" on page 59

"Clients" on page 67

"Statistics" on page 71

"Insights" on page 75

Common Interface Options

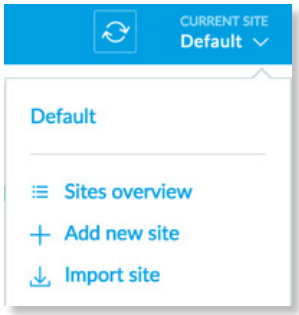
The common interface options are accessible from all tabs in the UniFi interface.

Refresh

Click the *refresh* icon to update the on-screen information.

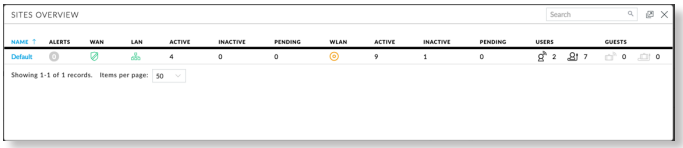
Current Site

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.

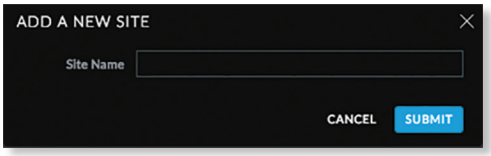


Each site is displayed with the following:

- **Name** Displays the name of the site.
- **Alerts**

- **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 sireless 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 pen 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:

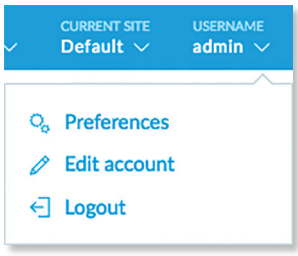


  - **Site Name** Enter a name that describes the site. It will be used in the *Current Site* drop-down menu.
  - **Cancel** Click to discard changes.
  - **Submit** Click to save changes.
- **Import Site** To import a new site, click and the *Import Site* screen will appear.

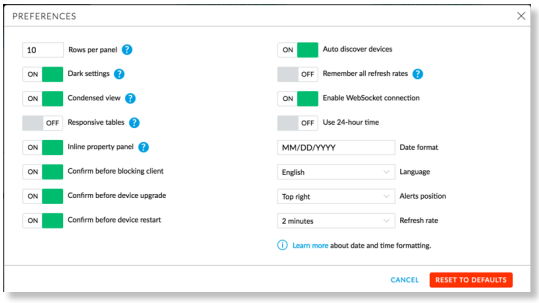
  - **Site Name** Enter a name that describes the site. It will be used in the *Current Site* drop-down menu.
  - **Choose File**
  - **Cancel** Click to discard changes.

Username

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



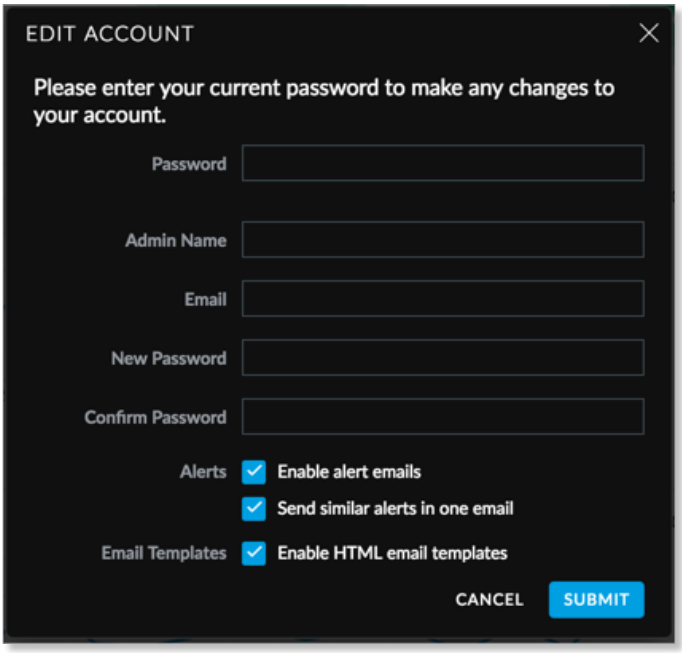
Preferences To change the UI settings, click Preferences.



- **Rows per panel**
- **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.
- **Confirm before blocking client** Enabled by default.
- **Confirm before device upgrade** Enabled by default.
- **Confirm before device restart** Enabled by default.
- **Auto discover devices** Enabled by default.
- **Remember all refresh rates** Disabled by default.
- **Enable WebSocket connection** Enabled by default.
- **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**.

- **Cancel** Click to discard 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**
- **Email Templates**
- **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 85**
- **"UniFi Switch Details" on page 93**
- **"UniFi Access Point Details" on page 103**
- **"UniFi VoIP Phone Details" on page 115**
- **"Client Details" on page 117**

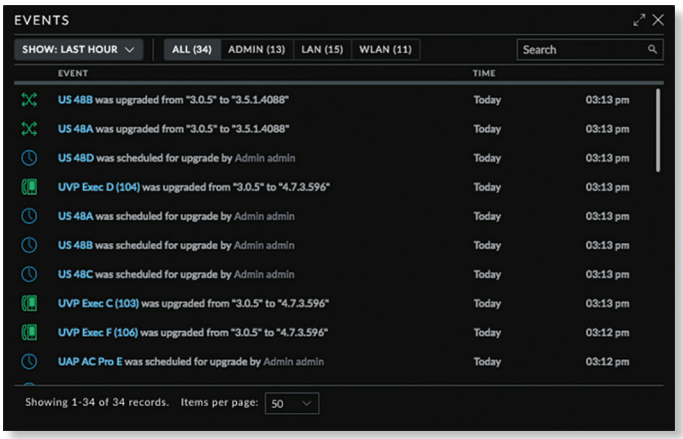
Controls and Live Chat

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

- *Events* (see the next column)
- *Alerts* (see **"Alerts" on page 20**)
- *Settings* (see **"Settings" on page 20**)
- *Chat with Us* (see **"Chat with Us" on page 45**)

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.

Show Filter recent events based on the time period you specify. Select **Last hour**, **Last 8 hours**, **Last 24 hours**, **Last 48 hours**, **7 days**, **2 weeks**, or **30 days**.

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.

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

Icons

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

	Scheduled for upgrade
	UniFi Security Gateway
	UniFi Switch
	UniFi Access Point
	UniFi VoIP Phone

Clicking an Event Device Link

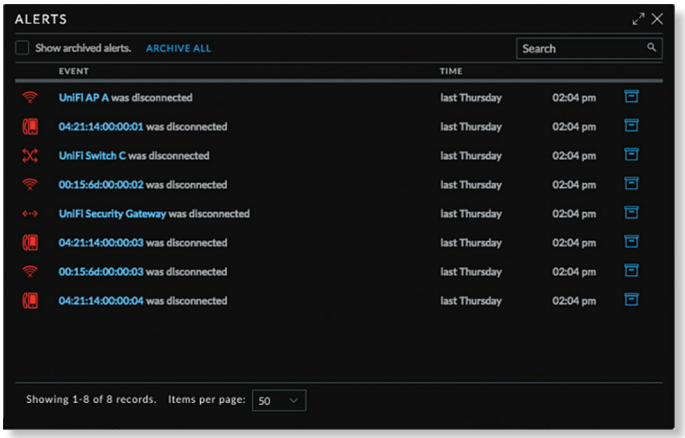
The messages have clickable links for client and UniFi devices:

- **"UniFi Security Gateway Details" on page 85**
- **"UniFi Switch Details" on page 93**
- **"UniFi Access Point Details" on page 103**
- **"UniFi VoIP Phone Details" on page 115**
- **"Client Details" on page 117**

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.

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

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

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

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
- UniFi VoIP Phone

Clicking an Alert Device Link

The messages have clickable links for client and UniFi devices:

- **"UniFi Security Gateway Details" on page 85**
- **"UniFi Switch Details" on page 93**
- **"UniFi Access Point Details" on page 103**
- **"UniFi VoIP Phone Details" on page 115**
- **"Client Details" on page 117**

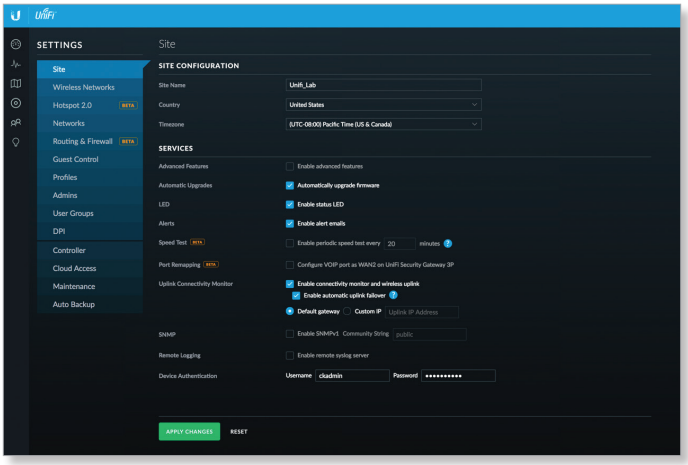
Settings

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

- **Site** Site-related settings.
- **Wireless Networks** Wireless network and group setup, including Zero Handoff Roaming.
- **Hotspot 2.0** Hotspot 2.0 settings.
- **Networks** Wired network setup.
- **Routing & Firewall** Routing and firewall settings.
- **Guest Control** Guest portal and policies.
- **Profiles** RADIUS authentication profiles.
- **Admins** Admin accounts and privileges.
- **User Groups** User group settings.
- **DPI** Deep Packet Inspection settings.
- **Controller** Identity, discovery, and email server settings.
- **Cloud Access** Cloud login credentials.
- **Maintenance** System configuration backup, system configuration restore, and support files.
- **Auto Backup** Auto-backup settings.

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 firmware when an update is available.

LED When enabled, the 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 (Beta) When enabled, you can run a periodic speed test.

Port Remapping (Beta) 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. 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.

- **Remote IP Address** Enter the IP address of the syslog server.
- **Port** Enter the port number of the syslog server. The default is *514*.

Device 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:

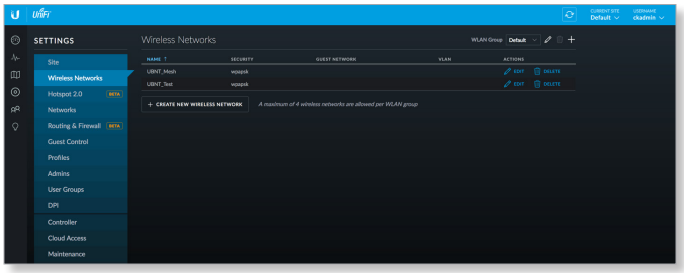
- **Username** Enter the new username.
- **Password** Enter the new password.

Apply Changes Click to save changes.

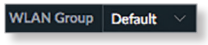
Reset Click to cancel changes.

Settings > Wireless Networks

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

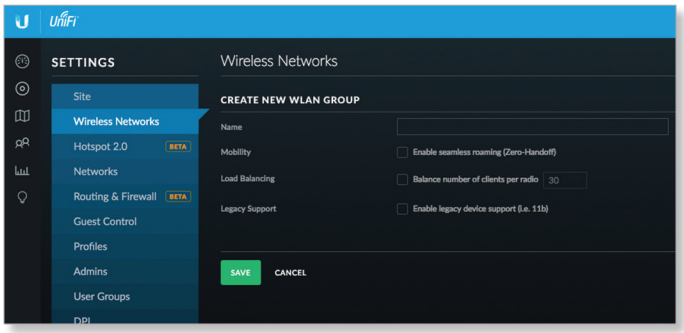


WLAN Group The *Default* WLAN group is automatically created.



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



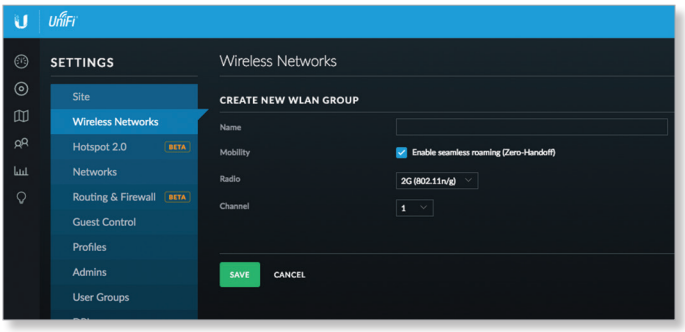
- **Name** Enter or edit a descriptive name for the WLAN group.

- **Mobility** To enable seamless roaming (Zero Handoff), select the checkbox.

  Note: The UAP-AC, UAP-AC-Outdoor, UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU do not 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.

Load Balancing (Not available if you enabled the *Mobility* option.) Select this option to balance the number of clients you specify per radio. Then enter the number of clients in the field provided.

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.

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 21**.

Wireless Networks

Name/SSID Displays the wireless network name or SSID.

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

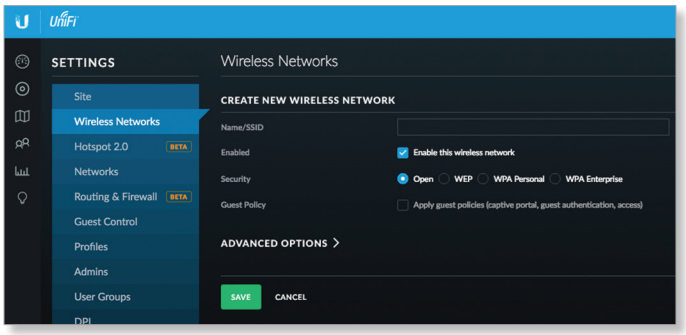
Guest Network Indicates whether or not the network is a guest network.

Actions Click a button to perform the desired action:

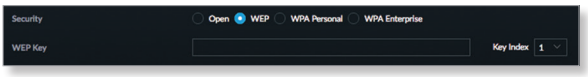
- **Edit** Click EDIT to make changes to the wireless network settings. Go to the *Create or Edit a Wireless Network* section in the next column.
- **Delete** Click DELETE to remove the wireless network.

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

Create or Edit a Wireless Network



- **Name/SSID** Enter or edit the wireless network name or SSID.
- **Enabled** Select this option to make this 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.

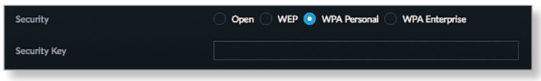


  - **WEP Key** Enter a WEP encryption key in hexadecimal format. You can enter a 64-bit or 128-bit key:

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.

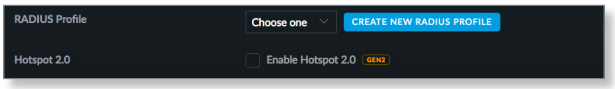
- **Key Index** Specify which Index of the WEP Key to use. Four different WEP keys can be configured at the same time, but only one is used. Select the effective key: **1**, **2**, **3**, or **4**.

- **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.

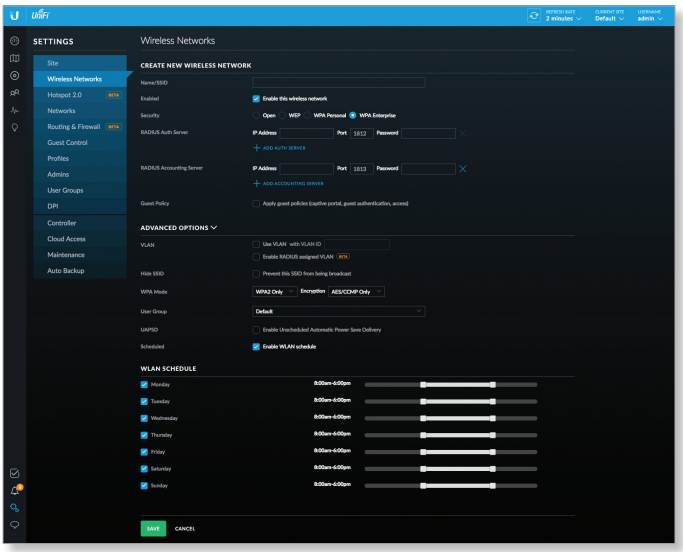


  - **RADIUS Profile** Specify a RADIUS profile:
    - Select a RADIUS profile from the drop-down list, or
    - Click CREATE NEW RADIUS PROFILE to create a new RADIUS profile. Refer to **"Create New RADIUS Profile" on page 39** for detailed information.
  - **Hotspot 2.0** Select this option to enable Hotspot 2.0. Then select a Hotspot profile from the drop-down list.

- **Guest Policy** Select this option to enable guest access policies on this wireless network.

Advanced Options

Click to display options for advanced users.



- **VLAN** To use a VLAN, select **Use VLAN ID** and enter the VLAN ID number. If you enable *WPA Enterprise*, you have another option:

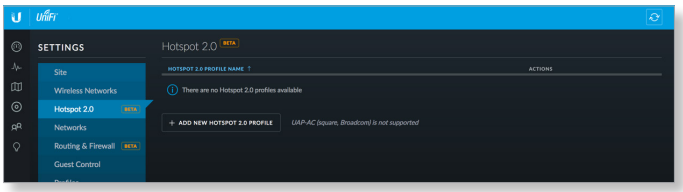
  - **Enable RADIUS assigned VLAN (beta)** Select this option to allow the RADIUS server to dynamically assign a VLAN to a wireless client.

    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.

- **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** Select the appropriate encryption method: **Auto**, **TKIP Only**, or **AES/CCMP Only** (default).
- **User Group** Assign wireless users to a specific user group. For more information about user groups, see **"Settings > User Groups" on page 40**.
- **UAPSD** Disabled by default. Unscheduled Automatic Power Save Delivery. Select this option 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 sliders to select the start and end times of the day's wireless access.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Settings > Hotspot 2.0 (Beta)

Use this option to create Hotspot 2.0 profiles for each site.



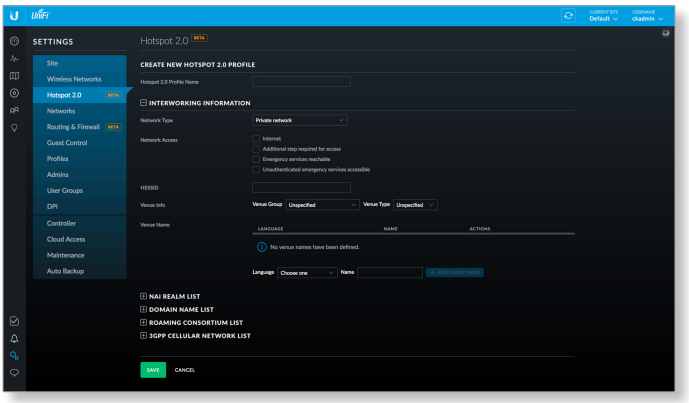
Hotspot 2.0 Profile Name Displays the name of the Hotspot 2.0 profile.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the profile. Go to **"Create or Edit a Hotspot 2.0 Profile" on page 24**.
- **Delete** Click DELETE to delete the profile.

Add New Hotspot 2.0 Profile Click ADD NEW HOTSPOT 2.0 PROFILE to create a new Hotspot 2.0 profile. Go to **"Create or Edit a Hotspot 2.0 Profile" on page 24**.

Create or Edit a Hotspot 2.0 Profile



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

The rest of this screen contains the following sections and options:

- *Interworking Information* (see below)
- **"NAI Realm List" on page 24**
- **"Domain Name List" on page 25**
- **"Roaming Consortium List" on page 25**
- **"3GPP Cellular Network List" on page 25**

Save Click to apply changes made to the profile.

Cancel Click to discard changes.

Interworking Information

Network Type Select the network type: *Private network*, *Private network with guest access*, *Chargable 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:

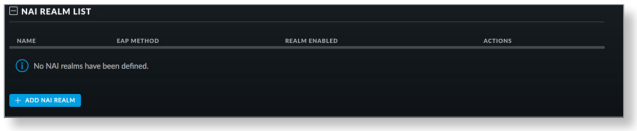
Venue Group	Available Venue Types
Unspecified	*Unspecified*
Assembly	*Unspecified, Arena, Stadium, Passenger terminal, Amphitheater, Amusement Park, Place of worship, Convention center, Library, Museum, Restaurant, Theater, Bar, Coffee shop, Zoo or Aquarium, Emergency coordination center*
Business	*Unspecified, 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 or jail*
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, Mini-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 to the list, fill in the *Language* and *Name* fields, and then click + ADD 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.

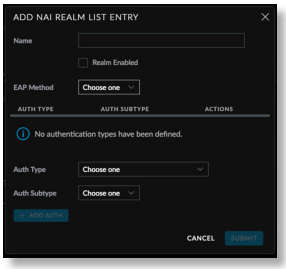
Realm Enabled Displays *Yes* if the realm is enabled or *No* if the realm is not enabled.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the NAI realm. Go to **"Add or Edit a NAI Realm" on page 25**.
- **Delete** Click DELETE to delete the NAI realm.

To add an NAI realm to the list, click + ADD NAI REALM. Go to **"Add or Edit a NAI Realm" on page 25**.

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, fill out the *Auth Type* and *Auth Subtype* fields, and then click + ADD AUTH.

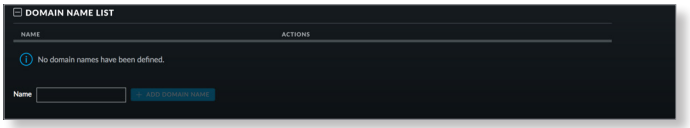
The available authentication subtypes vary depending on the value of *Auth Type*, as shown in the following table:

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*

Cancel Click to discard your changes.

Submit Click to save your changes to the NAI realm list entry.

Domain Name List

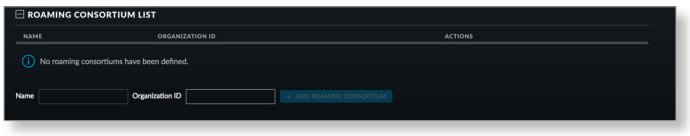


(List of domain names) Displays a list of domain names that have been defined for this NAI realm list entry:

- **Name** Displays the domain name.
- **Actions** Click DELETE to delete the domain name from the list.

To add a domain name to the list, fill out the *Name* field, and then click + ADD DOMAIN NAME.

Roaming Consortium List

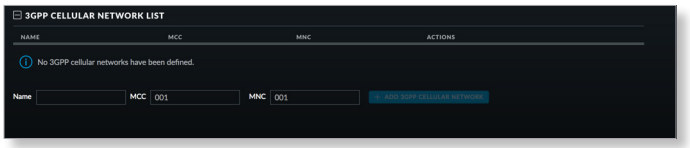


(List of roaming consortiums) Displays a list of roaming consortiums that have been defined for this NAI realm list entry:

- **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



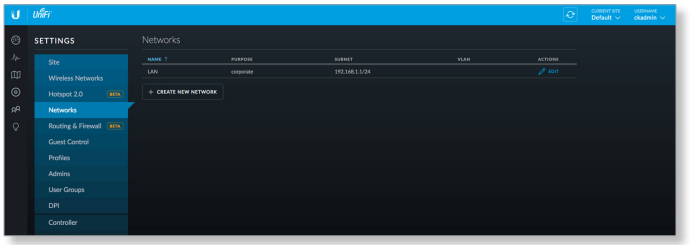
(List of 3GPP cellular networks) Displays a list of 3GPP cellular networks that have been defined for this NAI realm list entry:

- **Name** Displays the name of the 3GPP cellular network.
- **MCC** Displays the Mobile Country Code (MCC).
- **MNC** Displays the Mobile Network Code (MNC).
- **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.

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.

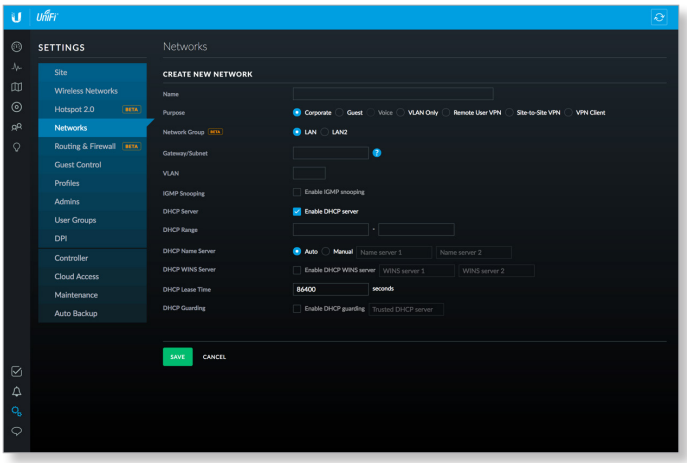
VLAN Displays the VLAN ID, if applicable.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the network settings. Go to **"Create or Edit a Network" on page 26**.
- **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 **"Create or Edit a Network" on page 26**.

Create or Edit a Network

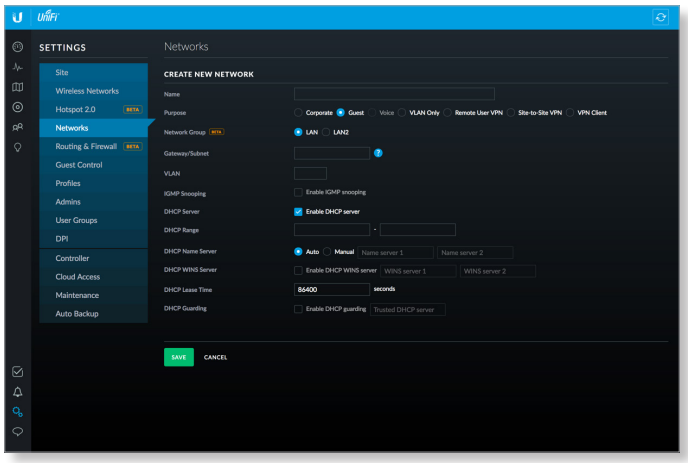


- **Name** Enter or edit the network name.
- **Purpose** Select the most appropriate description:
  - **Corporate** Corporate networks are appropriate for networks containing trusted systems. Corporate networks have no restrictions between them, or from them to the Internet, by default.
  - **Guest** Guest networks are often used in combination with the *Guest Control* feature (refer to **"Settings > Guest Control" on page 32**) 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 USW.
  - **Remote User VPN** Allows configuring a UniFi Security Gateway as a remote access PPTP VPN server, to connect mobile VPN clients. Controller version 5.5 adds L2TP as a second Remote User VPN option.
  - **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 Switch products.

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

Corporate or Guest Network

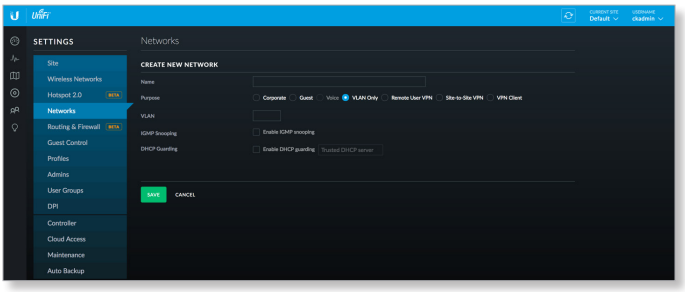


- **Network Group (Beta)** Select the physical interface of the USG that this network will be associated with: **LAN** or **LAN2**.
- **Gateway/Subnet** Enter the IP address and prefix size.
- **VLAN** (Not available for the default *Corporate* network, *LAN*.) Enter the VLAN ID.
- **IGMP Snooping** Select this option to monitor IGMP (Internet Group Management Protocol) traffic and thereby manage multicast traffic.
- **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 manually select name servers.
    - **Name Server 1/2** Enter the IP address of the name server in each field.
- **DHCP WINS Server** Select this option to designate WINS (Windows Internet Naming Service) server(s).
  - **WINS Server 1/2** Enter the IP address of the WINS server in each 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 Guarding** Disabled by default. Select this option to detect and block unauthorized DHCP servers.
  - **Trusted DHCP Server IP** Enter the IP address of the trusted DHCP server.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

VLAN Only

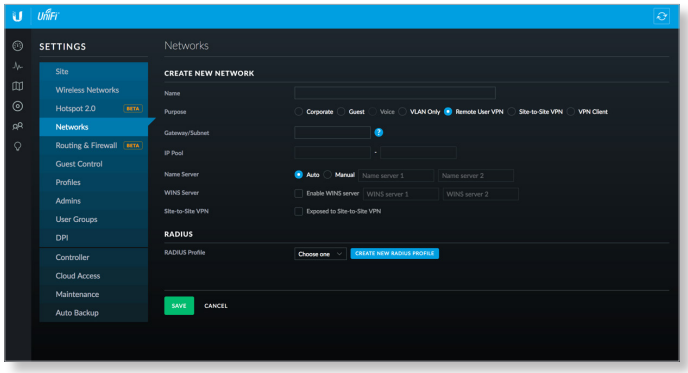
The UniFi Switch is required for this option.



- **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** Select this option to detect and block unauthorized DHCP servers.
  - **Trusted DHCP Server IP** Enter the IP address of the trusted DHCP server.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

Remote User VPN

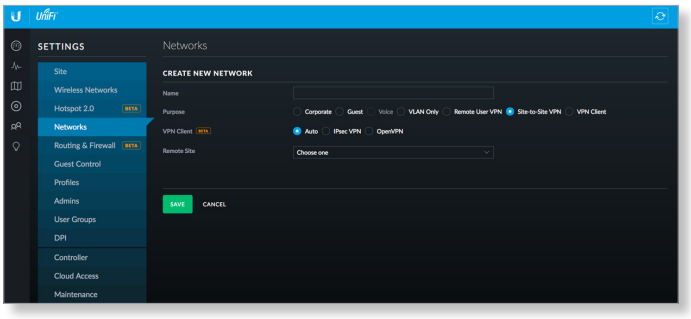
The UniFi Security Gateway is required for this option.



- **IP/Subnet** Enter the IP address and prefix size.
- **IP Pool** The starting and ending IP addresses of the pool automatically appear after you complete the *IP/Subnet* field. These are the IP addresses 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 manually select name servers.
    - **Name Server 1/2** Enter the IP address of the name server in each field.
- **WINS Server** Select this option to designate WINS (Windows Internet Naming Service) server(s).
  - **WINS Server 1/2** Enter the IP address of the WINS server in each field.
- **RADIUS IP** Enter the IP address of the RADIUS server, which is used for authentication.
- **RADIUS Password** Enter the password of the RADIUS server.
- **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.
- **Save** Click to apply changes.
- **Cancel** Click to discard changes.

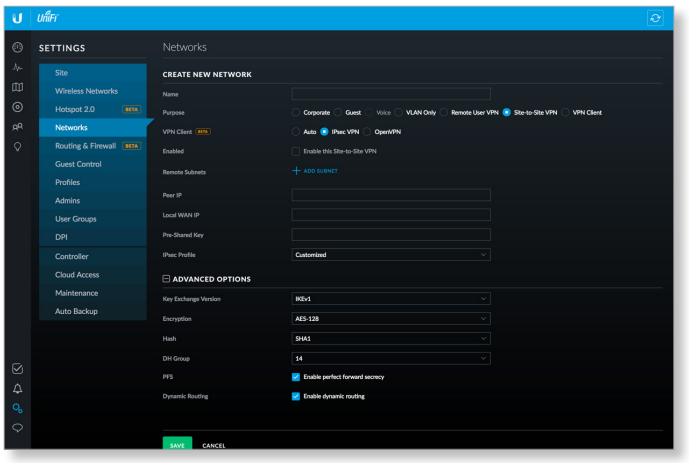
Site-to-Site VPN

The UniFi Security Gateway is required for this option.



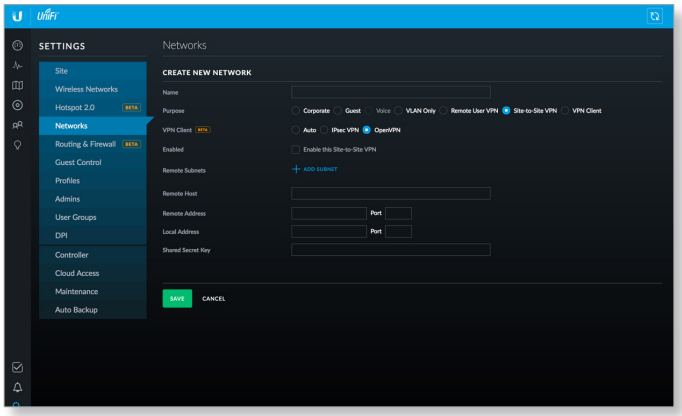
- **VPN Client (Beta)** Select the type of VPN being configured:
  - **Auto** *Auto* is the default. This option lets you connect two sites on the same controller by simply picking the other site. No further configuration is necessary; UniFi automatically creates a secure IPsec VPN, and configures routing between the sites. Also, the created 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 create a VPN that uses IPsec (IP security protocol).
  - **Enabled** Select this option to create an IPsec VPN tunnel over the Internet between two peer routers. (The UniFi Security Gateway is the local peer router.)
  - **Remote Subnets** Click **Add Subnet** to add an address for a remote network.
    - **Add Subnet** If you have another remote subnet, click this option and enter its network address.
  - **Peer IP** Enter the IP address of the peer router.
  - **Local WAN IP** Enter the Internet IP address of the 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).

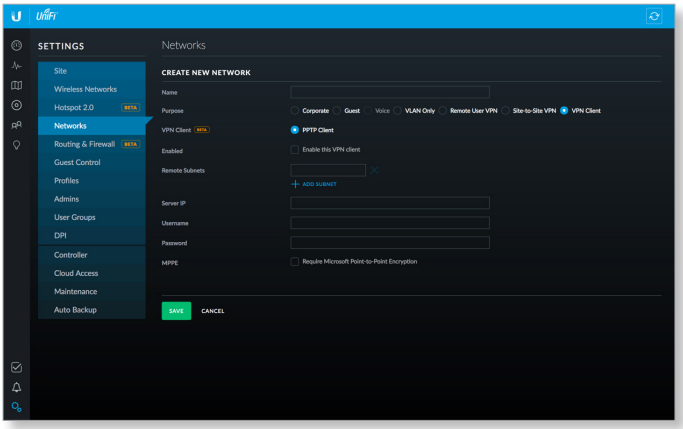
Note: If you selected *Azure dynamic routing* or *Azure static routing*, then the defaults of the *Advanced Options* will also change accordingly.



- **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 over the Internet between two peer routers. (The UniFi Security Gateway is the local peer router.)
  - **Remote Subnets** Click **Add Subnet** to add an address for a remote network.
    - **Add Subnet** If you have another remote subnet, click this option and enter its network address.
  - **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. 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 (Beta)** **PPTP Client** is automatically selected.
- **Enabled** Select this option to enable the VPN client.
- **Remote Subnets** 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.
- **Server IP** 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.

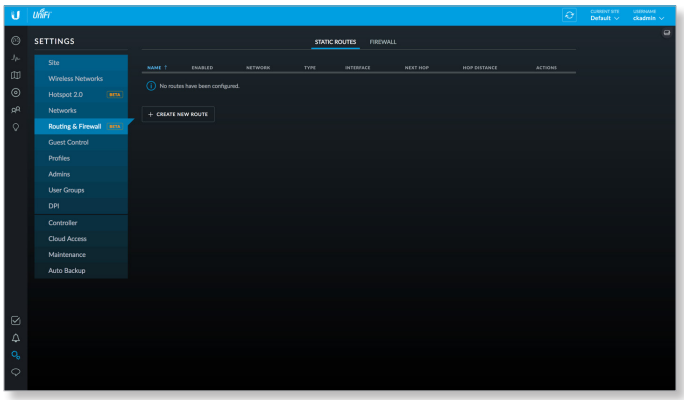
Settings > Routing & Firewall

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

- *Static Routes* tab
- *Firewall* tab

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.

Static Routes Tab



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; displays nothing if the static route is disabled.

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:

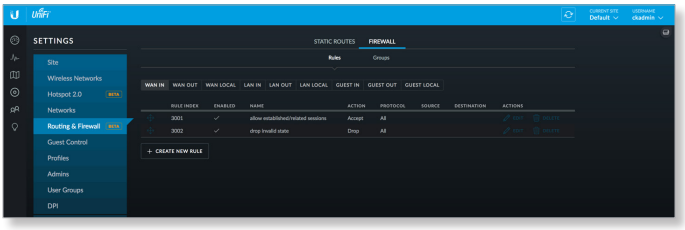
- **Edit** Click EDIT to make changes to the static route entry. Go to **"Create or Edit a Static Route" on page 31**.
- **Delete** Click DELETE to remove the static route.

To create a static route, click + CREATE NEW ROUTE and go to **"Create or Edit a Static Route" on page 31** .

Firewall Tab

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

Firewall > Rules



The *Rules* sub-tab displays existing firewall rules. There are three instances per network type: *In*, *Out*, and *Local*. The interfaces currently are defined as *WAN*, *LAN*, and *GUEST*.

WAN This is your Internet connection.

LAN This is in reference to all corporate networks.

Guest This is in reference to any guest subnets.

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 30**.

The following information is displayed for each rule:

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

Enabled Displays a check mark if the rule is enabled, or nothing if the rule is disabled.

Name Displays the 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 31**.
- **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 31**.

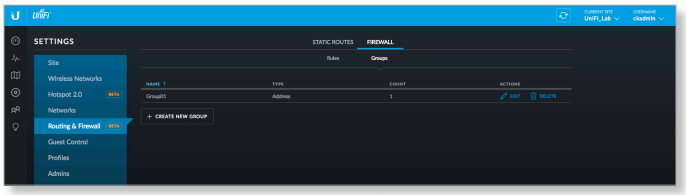
Predefined Firewall Rules

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.

Firewall > Groups



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

Name Displays the name of the group.

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

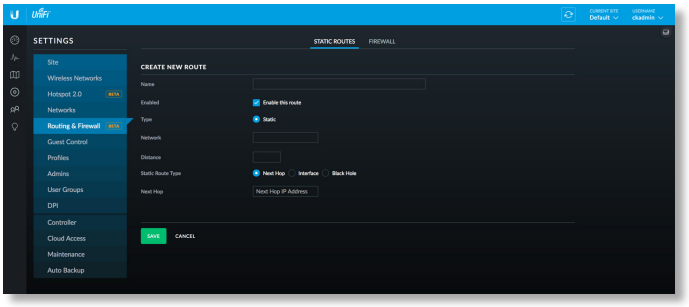
Count Displays the total addresses or ports in the group.

Actions Click a button to perform the desired action:

- **Edit** Click EDIT to make changes to the group. Go to **"Create or Edit a Firewall Group" on page 32**.
- **Delete** Click DELETE to remove the group.

To create a group, click + CREATE NEW GROUP and go to **"Create or Edit a Firewall Group" on page 32**.

Create or Edit a Static Route



Name Enter a name for the static route.

Enabled Check this box checked 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** The IP address of the next hop gateway for the desired routing path. This is the default.
- **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.
- **Black Hole** This is used to forward unwanted traffic into a black hole, or to drop it.

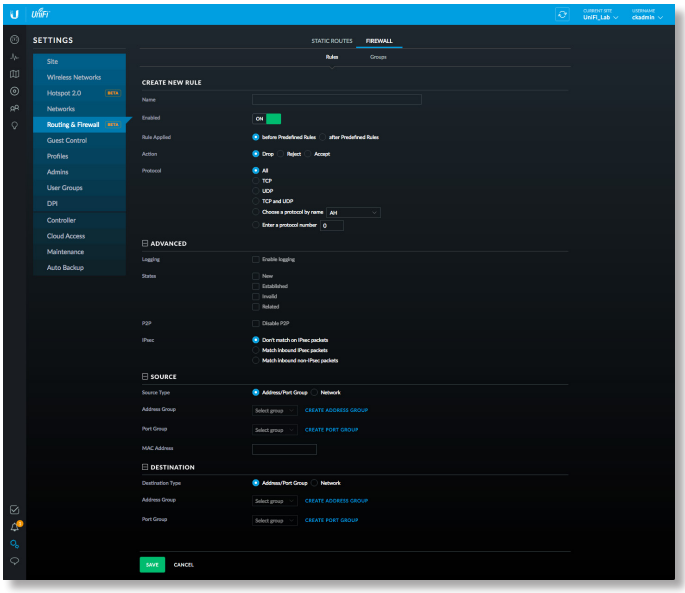
Next Hop (Available if *Static Route Type* is *Next Hop*.) Enter the next hop IP address.

Interface (Available if *Static Route Type* is *Interface*.) Select the interface.

Save Click to apply changes.

Cancel Click to discard changes.

Create or Edit a Firewall Rule



Create New Rule

Name Enter a 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.
- **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).

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): [Please verify this all descriptions below; they are based on info found online]

- **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.

P2P Check the box to disable P2P (unchecked by default).

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 the type of source:

- **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**, and then fill in the *Name* and *Address* fields. To add another address to the group, click **Add**. When finished adding addresses, click **Save**.
  - **Port Group** Select a port group from the drop-down list.

    To create a new port group, click **Create Port Group**, and then fill in the *Name* and *Port* fields. To add another port to the group, click **Add**. When finished adding ports, click **Save**.
- **Network** The source is a network. Specify the following:
  - **Network** Select the network and the IP group (*ADDRv4*) or subnet (*NETv4*) from the drop-down lists.

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.

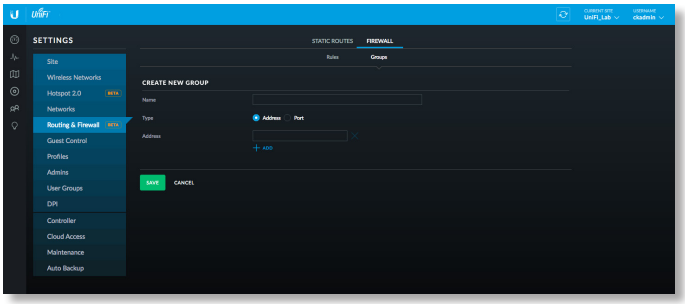
    To create a new address group, click **Create Address Group**, and then fill in the *Name* and *Address* fields. To add another address to the group, click **Add**. When finished adding addresses, click **Save**.
  - **Port Group** Select a port group from the drop-down list.

    To create a new port group, click **Create Port Group**, and then fill in the *Name* and *Port* fields. To add another port to the group, click **Add**. When finished adding ports, click **Save**.
- **Network** The destination is a network. Specify the following:
  - **Network** Select the network and the IP group (*ADDRv4*) or subnet (*NETv4*) from the drop-down lists.

Save Click to apply changes.

Cancel Click to discard changes.

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*.)

Port (Available if *Type* is set to *Port*.)

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

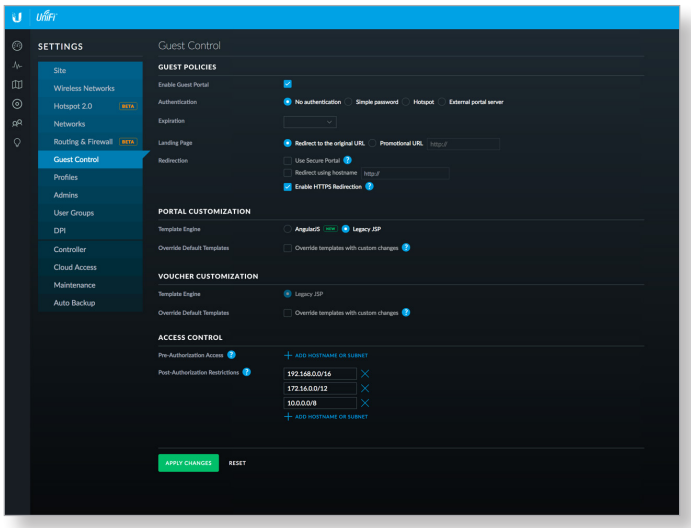
Save Click to apply changes.

Cancel Click to discard changes.

Settings > Guest Control

The *Guest Control* screen displays the following sections:

- *Guest Policies* (see below)
- **"Access Control" on page 39**
- **"Hotspot" on page 36** (for *Hotspot* authentication)
- **"Access Control" on page 39**



Guest Policies

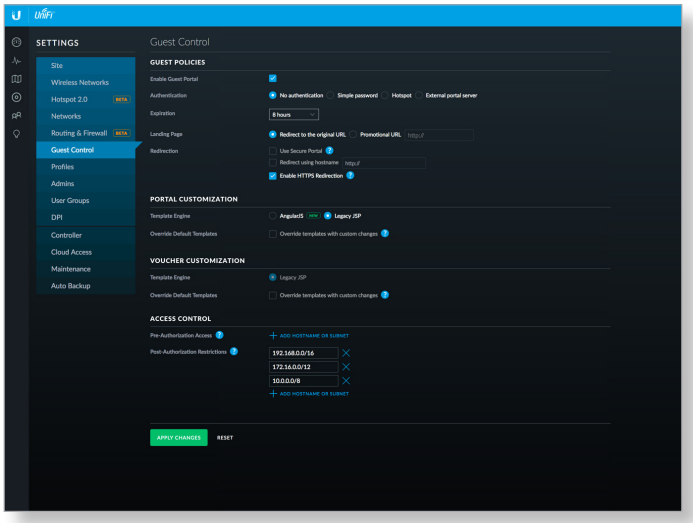
Enable Guest Portal Disabled by default. When disabled, guests can access the Internet without entering a password or accepting the terms of service. When this option is enabled, you can control the *Guest Portal*.

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

- *Authentication > No Authentication* (see below)
- **"Authentication > Simple Password" on page 33**
- **"Authentication > Hotspot" on page 34**
- **"Authentication > External Portal Server" on page 38**

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*, and *days*.

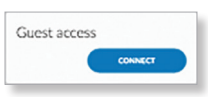
Landing Page After connecting, guests are redirected to the landing page. Select one of the following options:

- **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

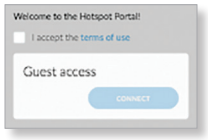
Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal.

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.

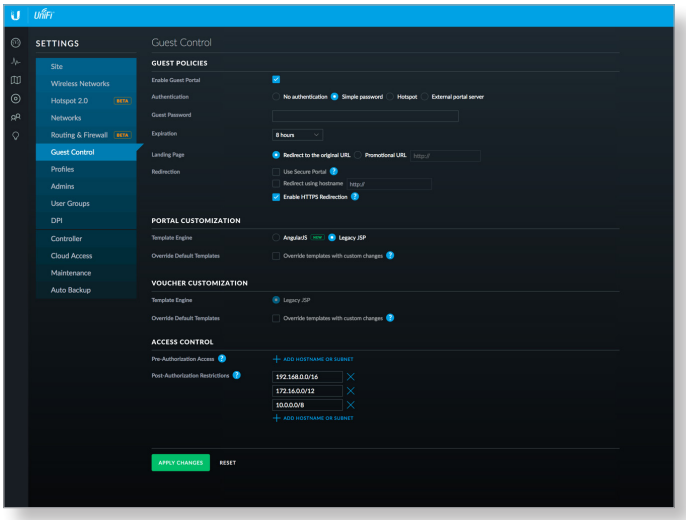


You can select **Enable terms of service** under *Settings > Guest Control > Portal Customization* to enforce selection of the terms of service by the guest. See **"Access Control" on page 39** for more information.

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 23** 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*, and *days*.

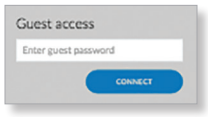
Landing Page After connecting, guests are redirected to the landing page. Select one of the following options:

- **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

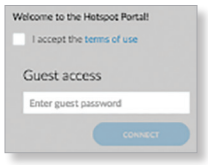
Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal.

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 *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.

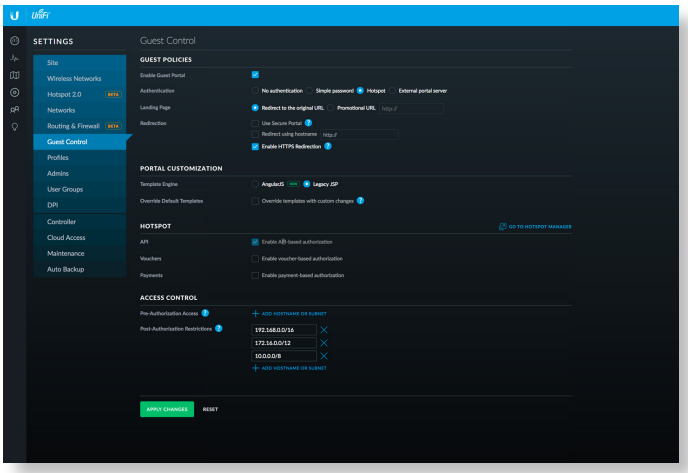


You can select **Enable terms of service** under *Settings* > *Guest Control* > *Portal Customization* to enforce selection of the terms of service by the guest. See **"Access Control" on page 39** for more information.

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

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 23** for more information.



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

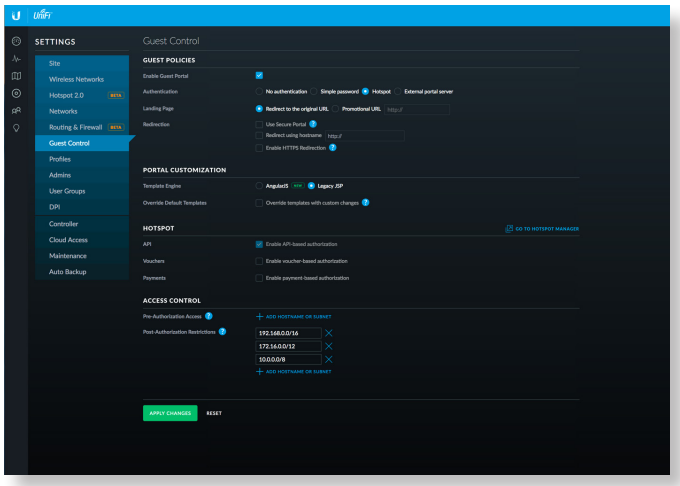
Use Secure Portal When selected, unauthorized guests will be redirected to the HTTPS guest portal.

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

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

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 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).

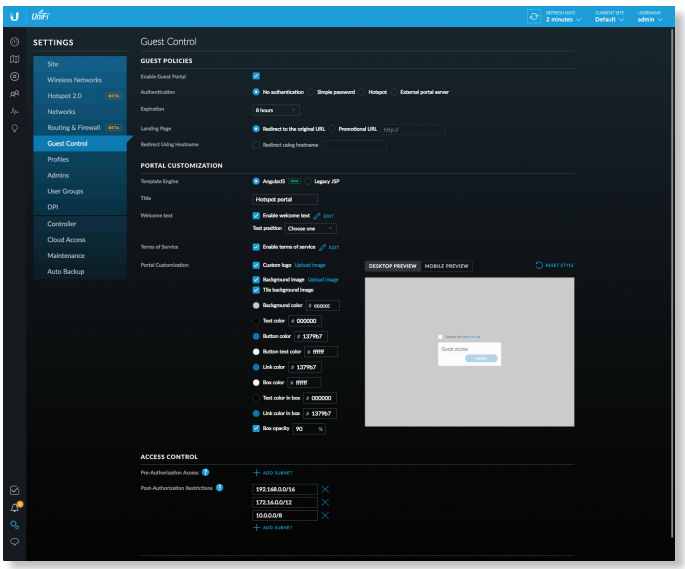
The UniFi Controller offers a built-in editor to customize AngularJS; however, it is not fully customizable at this time.

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.



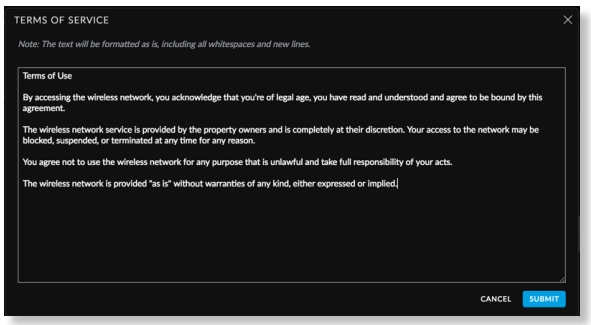
- **Title** Enter the title of your portal. The default is *Hotspot portal*.
- **Welcome Text** Select **Enable welcome text** to add a welcome message.

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.



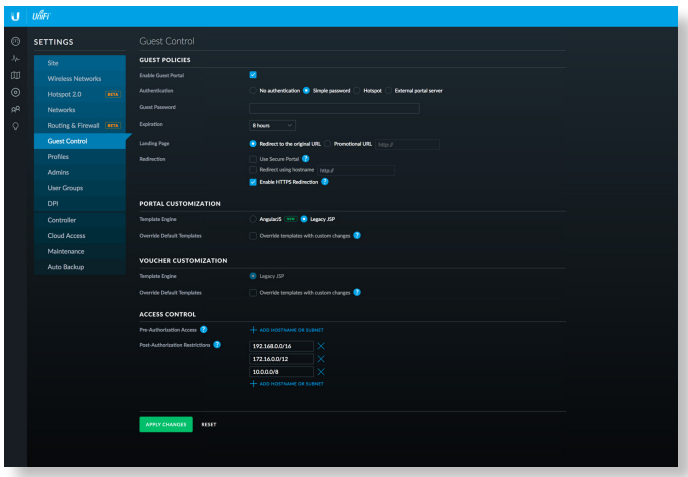
Click **Submit** to save your changes or click *Cancel*.

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

- **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 **Button color** to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#cccccc*.
  - **Text color** Click **Button color** to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#1379b7*.
  - **Button color** Click **Button color** to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#1379b7*.
  - **Button text color** Click **Button text color** to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#ffffff*.
  - **Link color** Click **Link color in box** to select the appropriate color, or enter the hexadecimal HTML color value you want to use. The default is *#1379b7*.
  - **Box color** Click **Box color** 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 **Link color in box** 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 **Link color in box** 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 128** for more information.

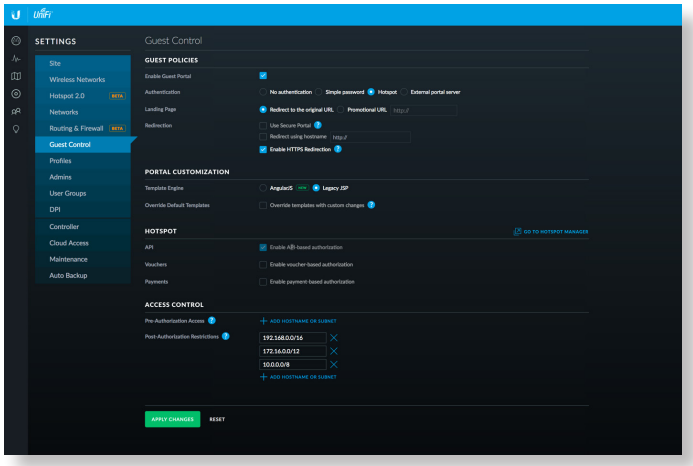
Legacy JSP Server-side rendering is enabled by default.



- **Override Default Templates** Select this option if you want to manually edit templates. See **"Portal Customization with Legacy JSP" on page 125** for more information.

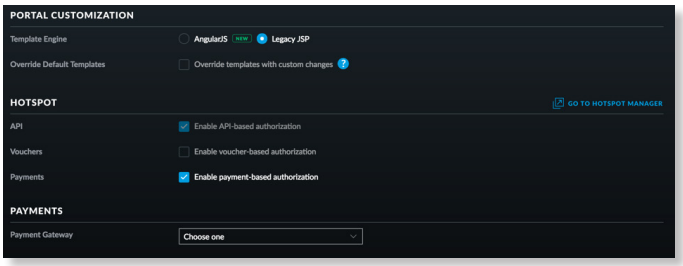
Hotspot

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



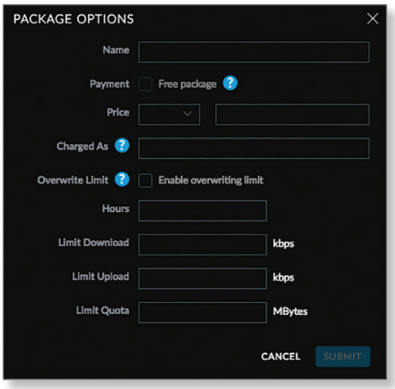
Select the **Voucher** and/or **Payment** method of authorization:

- **Vouchers** Use Hotspot Manager to create vouchers (including distributable code, duration values, and use restrictions). See **"Hotspot Manager" on page 121**.
- **Payments** Set up payment-based authentication.



- **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 the *Add or Edit a Package* section.
  - **Delete** Click DELETE to delete the package.
- **Add Another Package** Click + ADD ANOTHER PACKAGE to create a new package. Go to the *Add or Edit a Package* section.

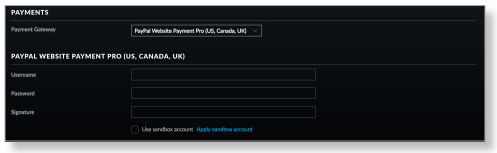
Add or Edit a Package



  - **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, then 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.
  - **Submit** Click to apply changes.
  - **Cancel** Click to discard changes.
- **Payment Field Options** (Available only for payment-based authentication.)
  - **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 field** Select this option to create a field for a zip 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.

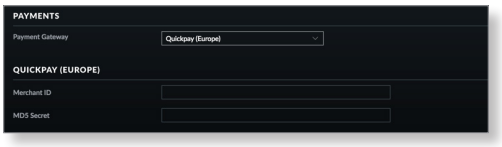
- **Gateway** (Available only for payment-based authentication.) You have multiple options:
  - **PayPal™ Website Payment Pro (US, Canada, UK)** Use your **PayPal Website Payments Pro** account. To manage payments and transactions, click GO TO HOTSPOT MANAGER, and see **"Hotspot Manager" on page 121**.



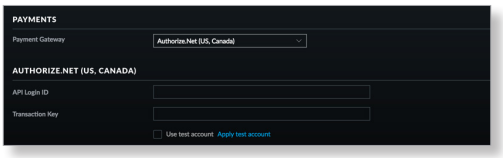
    Enter the PayPal account details:
    - **Username** Enter the corresponding *Username*.
    - **Password** Enter the corresponding *Password*.
    - **Signature** Enter the corresponding *Signature* for the PayPal account that will receive payments.
    - **Use sandbox account** For PayPal testing purposes, select this option. Then click **Apply Sandbox Account** to set up or access your **PayPal Sandbox Test Environment**.
  - **Stripe (US, Canada)** Use your **Stripe** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 121**.

    Enter the Stripe account detail:
    - **API Key** Enter the live secret API key.

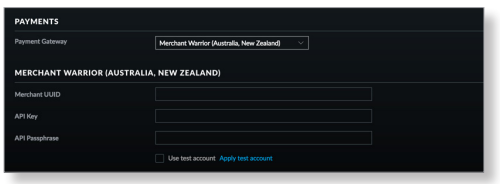
    Note: We recommend that you perform a test transaction with the test secret API key first before using the live secret API key.
  - **Quickpay (Europe)** Use your **Quickpay** account. To manage payments and transactions, click **Go to Hotspot Manager**, and see **"Hotspot Manager" on page 121**.



    Enter the Quickpay account details:
    - **Merchant ID** Enter the ID for your merchant account.
    - **MD5 Secret** Enter the MD5 secret key.
  - **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 121**.



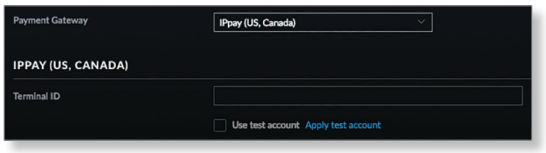
    Enter the Authorize.Net account details:
    - **API Login ID** Enter the API login ID used to identify yourself as an authorized user.
    - **Transaction Key** Enter the key used to authenticate transactions.
    - **Use test account** For Authorize.Net testing purposes, select this option. Then click **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 121**.



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 121**.

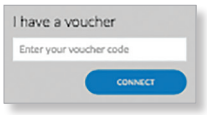


Enter the IPpay account details:

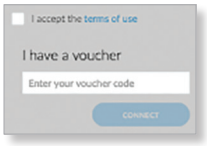
- **Terminal ID** Enter the terminal number for your merchant account.
- **Use test account** For IPpay testing purposes, select this option. Then click **Apply Test Account** to set up or access your **IPpay test account**.

- **Hotspot Operator** Click **Go to Hotspot Manager** to manage *Wireless Guests, Payments/Transactions, Vouchers,* and *Operator Accounts*. See **"Hotspot Manager" on page 121**.

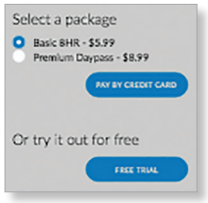
When logging in with voucher-based *Hotspot* authentication, guests will be required to enter the voucher number before gaining access to the Internet.



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.

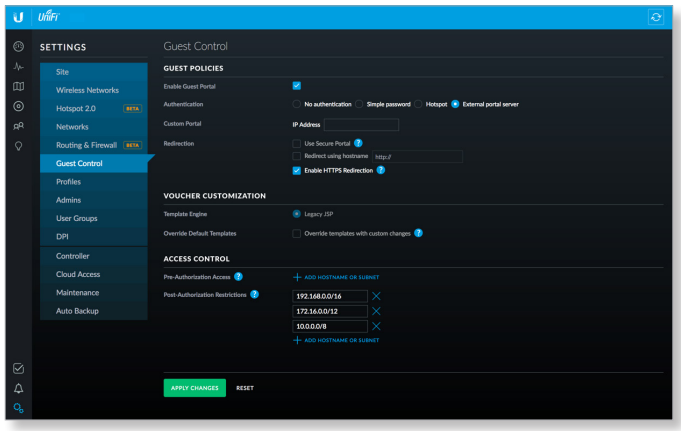


If you enable the terms of service, then guests will be required to accept the terms of use before gaining access to the Internet.

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 125** for more information.

Authentication > External Portal Server

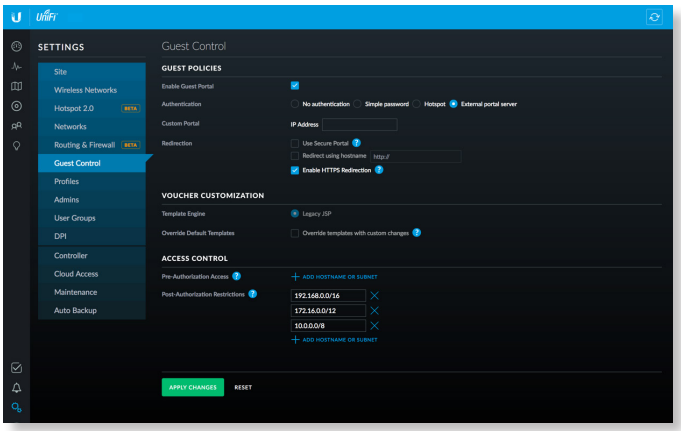
Select this option if you are using an external server to host a custom guest portal.



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

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

Access Control



Pre-Authorization Access Enter any subnets 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 Subnet** Click **Add Subnet** to add more allowed subnets.

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

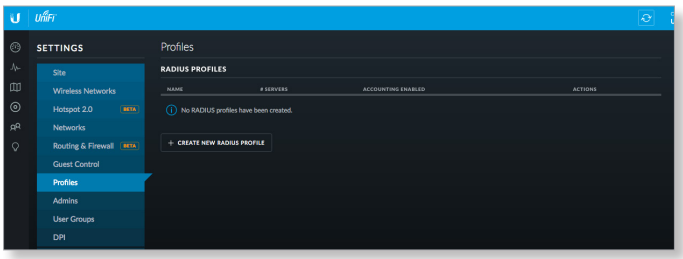
- **Add Subnet** Click **Add Subnet** to add more restricted subnets.

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 computer to connect to and use a network service.



Name Displays the name of the RADIUS authentication profile.

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

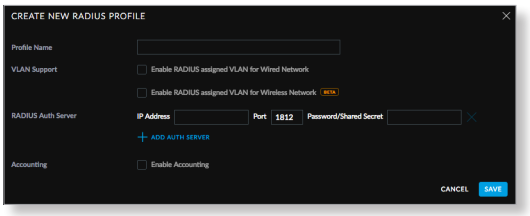
Accounting Enabled Displays a check mark if RADIUS accounting is enabled or nothing if RADIUS accounting is not enabled..

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 New 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.
- **Enable RADIUS assigned VLAN for Wireless Network** Disabled by default.

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 *RADIUS Accounting Server* 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.

Cancel Click to cancel your changes.

Save Click to save the profile.

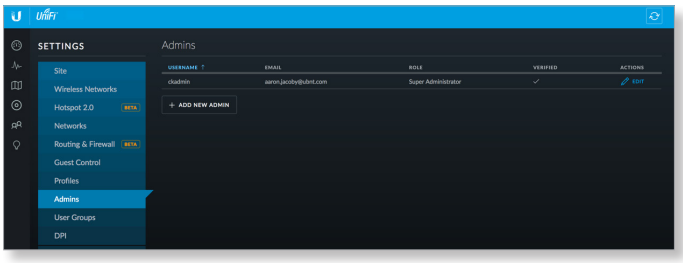
Settings > Admins

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 super admin account is created during the Setup Wizard and has global admin (read/write) access; this super admin account cannot be revoked or re-invited. Only the super admin – not any site admin – can view wired devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: Ensure that you save the super admin login information for future use, including the adoption of new wired devices.

To create operator accounts for the Hotspot Manager, see **"Operator Accounts" on page 123**.



Username Displays the name of the administrator.

Email Displays the email address of the administrator.

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

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

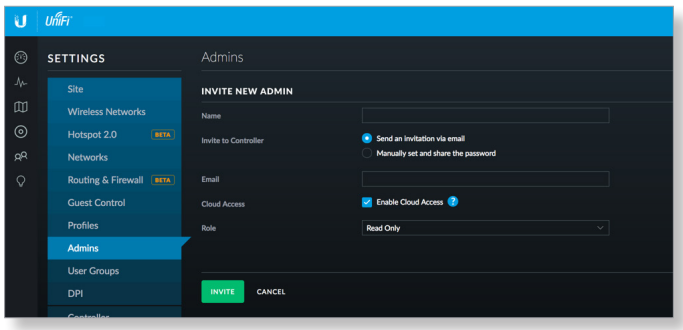
Actions Click a button to perform the desired action:

- **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 site admin. Go to the *Create or Edit an Admin* section.

To create operator accounts for the Hotspot Manager, see **"Operator Accounts" on page 123**.

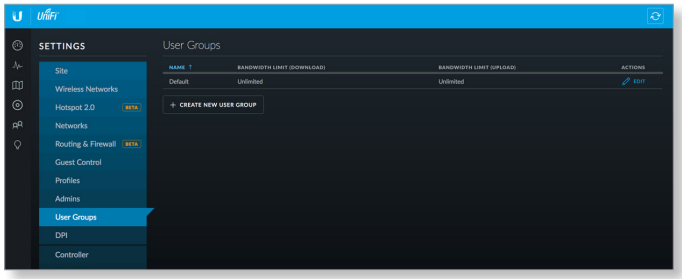
Create or Edit an Admin



- **Email** Enter the email address of the new administrator.
- **Name** Enter the name of the new administrator.
- **Invite to SDN** Select this option to allow the new administrator access to SDN (Software-Defined Networking) settings. The new administrator must use his or her own cloud account (linked to the same email address) to manage the UniFi Controller. The admin who issued the invitation can select which role the new administrator will have with respect to the UniFi Controller.
- **Role** Select **Administrator** (read/write access) or **Read Only**.
- **Invite** Click to send an email invitation.
- **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.

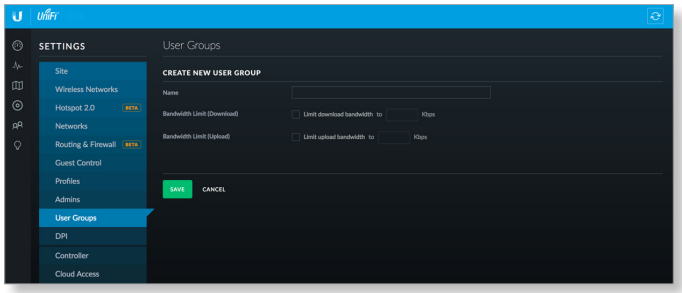
Bandwidth Limit (Upload) Displays the upload limit.

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" on page 40** section below.
- **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



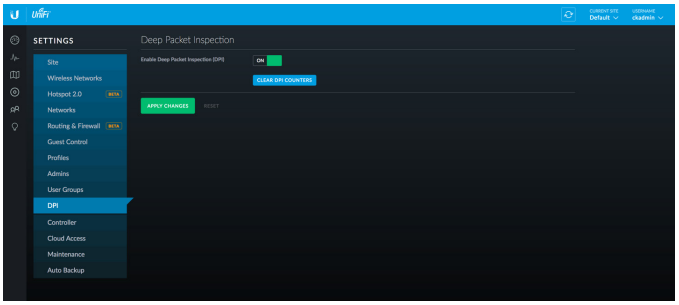
- **Name** Enter or edit the name of the user group.
- **Bandwidth Limit (Download)** Select to limit the download bandwidth. Enter the maximum in Kbps.

- **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 119** or **"Wired Client – Configuration" on page 120** 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 Deep Packet Inspection When enabled, this option turns on the DPI feature of the USG. The data will accumulate until you either click **Clear DPI Counters** (described below) or reboot or upgrade the USG. This feature will not work for any WAN connection when .Smart Queue is enabled on it.

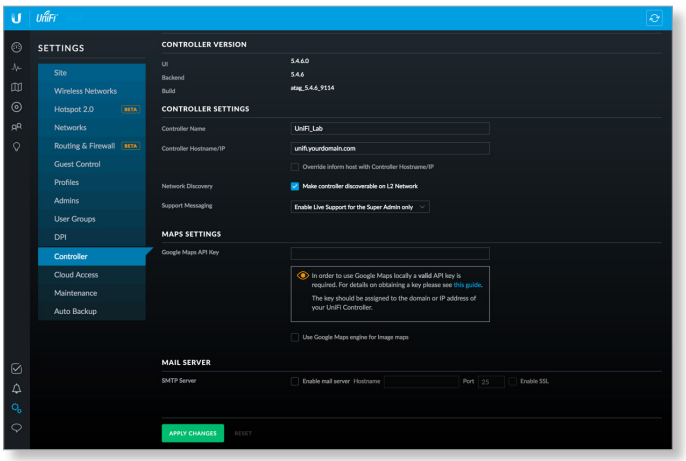
Clear DPI Counters Click this button to clear the DPI counters.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Settings > Controller

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



Controller Settings

Controller Hostname/IP 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.

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**.

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 40**.

SMTP Server Select this option to enable emails.

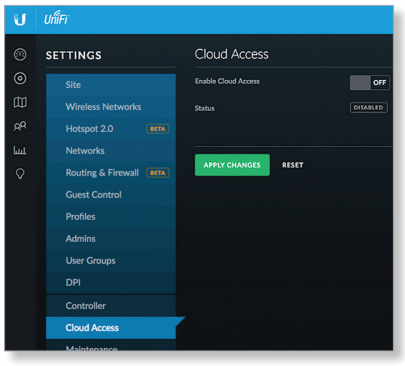
- **Hostname** Enter the outgoing (SMTP) mail server name.
- **Port** The default is *25*. If Secure Sockets Layer (SSL) is enabled, then the port number will automatically change to *465*.
- **Enable SSL** You can enable SSL to enhance secure communications over the Internet.
- **Enable authentication** 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.

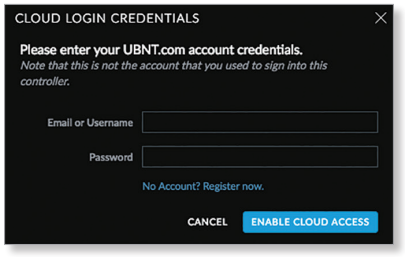
Settings > Cloud Access

Set up the login for cloud access.



Enable Cloud Access Click to configure the login. The *Cloud Login Credentials* screen will appear.

Cloud Login Credentials

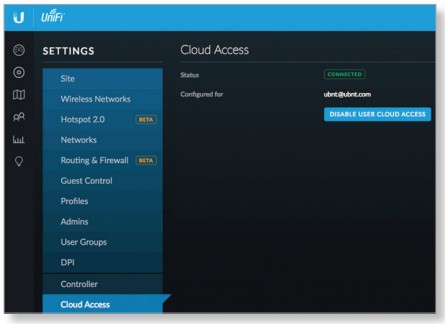


- **Email or Username** Enter the email address or username of your UBNT account.
- **Password** Enter the password of your UBNT account.
- **No account? Register now.** If you do not have a UBNT account, click here to visit this link: **https://account.ubnt.com/register**

  Follow the on-screen instructions to set up an account.
- **Enable Cloud Access** Click to save changes.
- **Cancel** Click to discard changes.

Cloud Access

If the login for cloud access is configured, then the *Cloud Access screen* will appear:

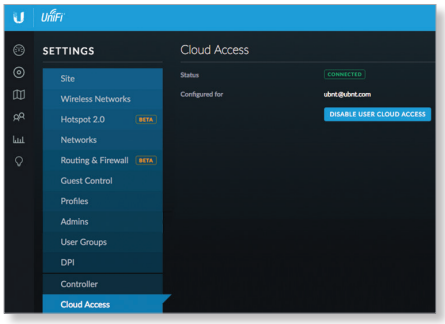


Enable Cloud Access Click to enable or disable cloud access.

Status Displays "Connected" if cloud access is active.

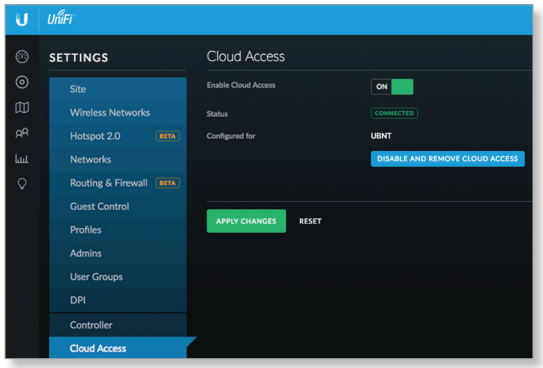
Configured for Displays the username or email address of your UBNT account.

Disable User Cloud Access (Available if you are a site admin.) Click to disable cloud access and remove the cloud login credentials.



Disable and Remove Cloud Access (Available if you are a super-admin.) Click to disable cloud access and remove the cloud login credentials.

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



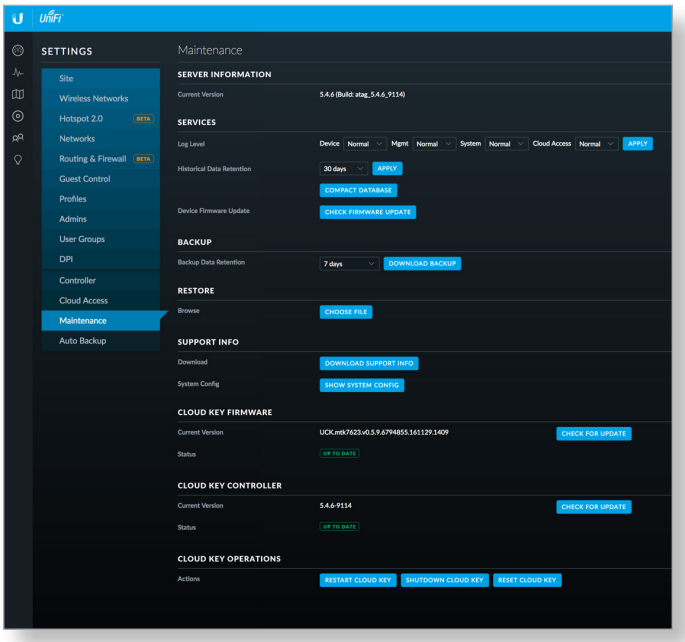
Apply Changes Click to save changes.

Reset Click to cancel changes.

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.

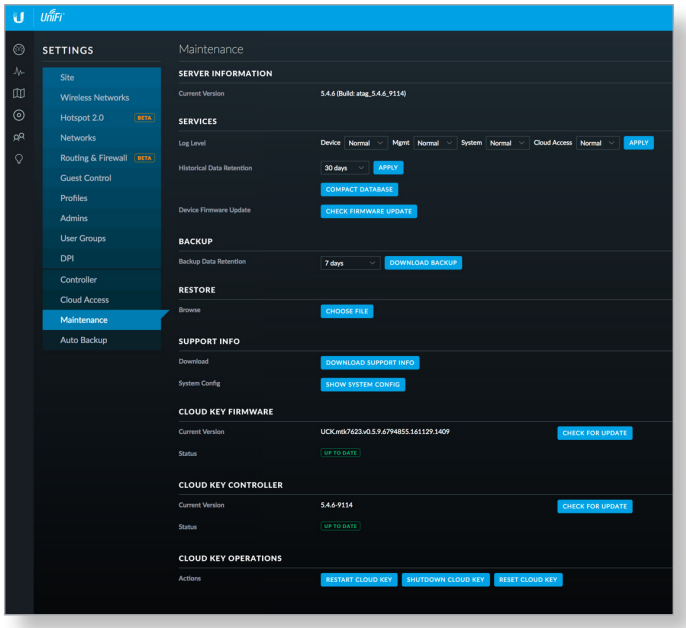
Services

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*.

Historical Data Retention Select the time duration of the historical data retention: **7 days**, **30 days**, **60 days**, **90 days**, **180 days**, **365 days**, or **Disabled**. The default is *Disabled*. Then click **Apply**.

- **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.



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 **All time**. 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

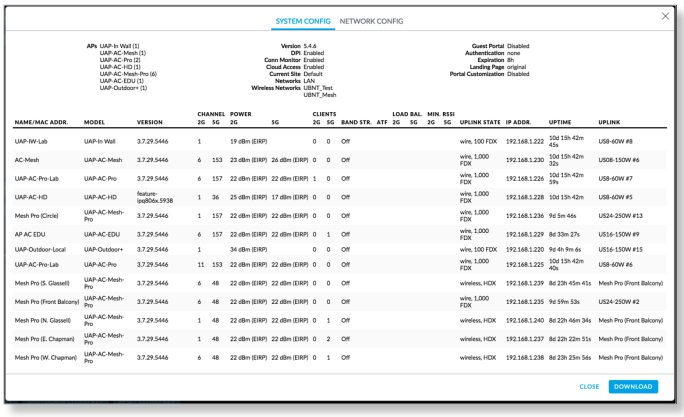
Browse Click **Choose File** to select a backup file that you've already downloaded. Follow the on-screen instructions to restore settings from the selected file.

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

Support Info

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

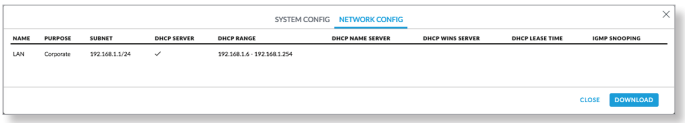
System Config



- **Network Config** Click **Network Config** to view the network configuration settings.

- **Version** Displays the software version.
- **DPI** Displays the status of the *DPI* (Deep Packet Inspection) feature, which is configured in **"Settings > Site" on page 20**.
- **Conn Monitor** Displays the status of the *Uplink Connectivity Monitor* feature, which is configured in **"Settings > Site" on page 20**.
- **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 configured in **"Settings > Guest Control" on page 32**.
- **Authentication** Displays the type of authentication required for guest access, which configured in **"Settings > Guest Control" on page 32**.
- **Expiration** Displays the period of time before a guest login expires, which configured in **"Settings > Guest Control" on page 32**.
- **Landing Page** Displays the type of landing page for guest access, which configured in **"Settings > Guest Control" on page 32**.
- **Portal Customization** Displays the status of the Portal Customization feature, which configured in **"Portal Customization" on page 34**.
- **Close** Click **Close** to exit this screen.
- **Download** Click **Download** to download a screenshot in .png format.

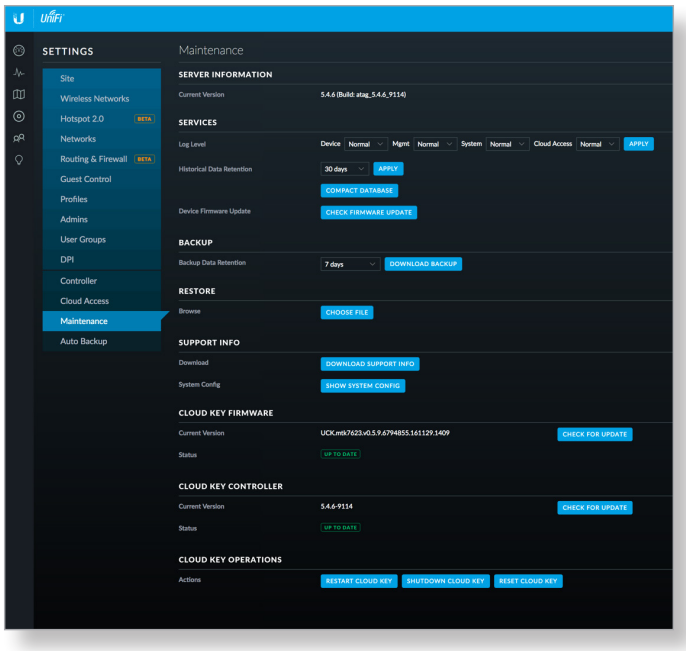
Network Config



- **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 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.

Note: We recommend that you back up your UniFi Controller configuration (refer to **"Backup" on page 43** for more information) before upgrading.

Available Version 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 43** 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*.

Cloud Key Operations

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

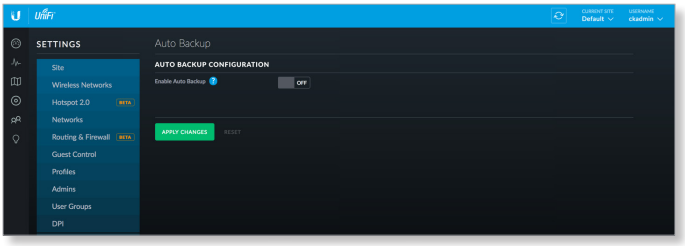
Shut Down Cloud Key Click this option to turn off the UniFi Cloud Key.

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 43** 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 following options:

- **Occurrence** Select how often to perform auto backup: (every) *Hour*, *Day*, *Week*, *Month*, or *Year*.
- **Occurrence Timezone** Select your time zone from the drop-down list.
- **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 *Disabled*.

Apply Changes Click to save changes.

Reset Click to cancel changes.

Chat with Us

Click 💬 to open a window for online chat suport.

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 48**
- **"LAN" on page 48**
- **"WLAN" on page 49**

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 Place your mouse over the *Latency* or *Throughput* monitor to display the following:

WWW

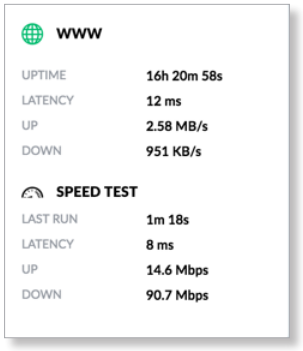
Current status information is displayed.

- **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.

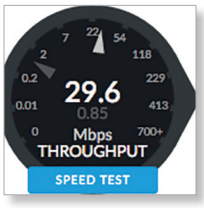
Speed Test

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.

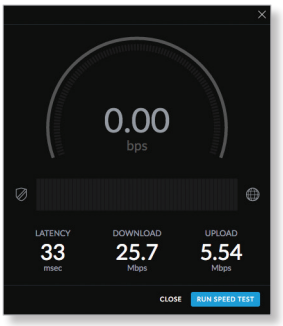


Speed Test Click the monitor to run the Speed Test.



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

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



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

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.

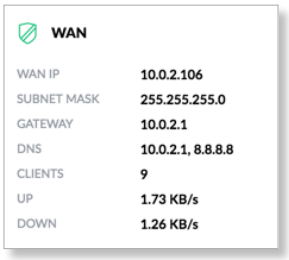
Active Devices Displays the number of Gateway devices adopted and active.

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

Pending Displays the number of Gateway devices pending adoption.

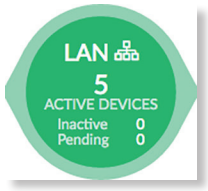
Status information Place your mouse over the monitor to display the following:

- **WAN IP** Displays the IP address of the WAN interface.
- **Subnet Mask** Displays the subnet mask of the WAN interface.
- **Gateway** Displays the Internet 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.

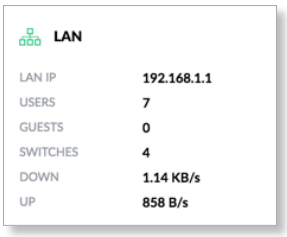
Inactive Displays the number of wired devices adopted but not active.

Pending Displays the number of wired devices pending adoption.

Status information Place your mouse over 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.

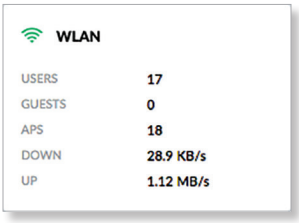
Active Devices Displays the number of APs adopted and active.

Inactive Displays the number of APs adopted but not active.

Pending Displays the number of APs pending adoption.

Status information Place your mouse over the monitor to display the following:

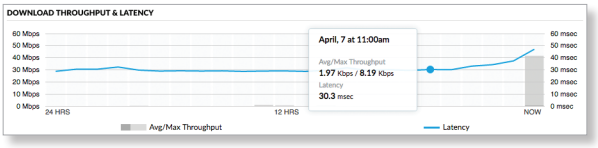
- **Users** Displays the number of clients connected to the primary wireless network(s).
- **Guests** Displays the number of clients connected to the guest wireless network(s).
- **APs** Displays the number of APs managed on this site.
- **Down** Displays the download rate of the wireless network(s).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

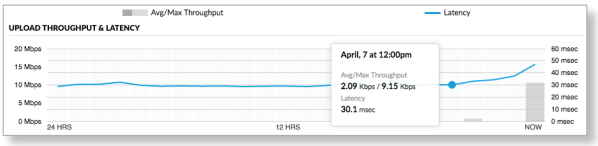
Status information Place your mouse over a specific point to display the following about a date and time:

- **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.

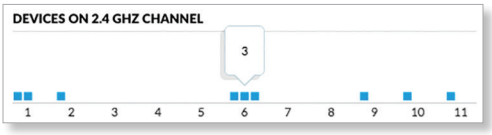
Status information Place your mouse over a specific point to display the following about a date and time:

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

Devices on 2.4 GHz Channel

The 2.4 GHz Channel Occupancy Chart displays the channel use of the 2.4 GHz devices.

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



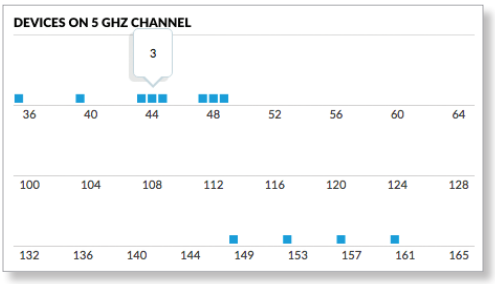
1-11 Each device is displayed as a blue square in its channel.

Status information Place your mouse over a specific channel to display the number of devices using that channel.

Devices on 5 GHz Channel

The 5 GHz Channel Occupancy Chart displays the channel use of the 5 GHz devices.

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

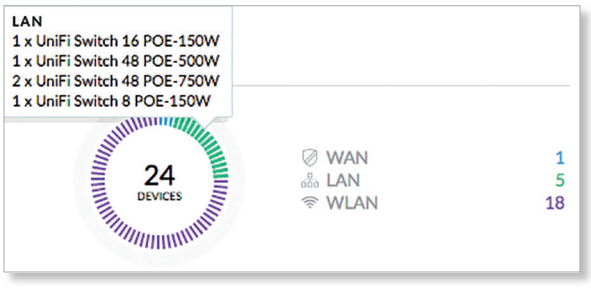


(Channels) Each device is displayed as a blue square in its channel.

Status information Place your mouse over a specific channel to display the number of devices using that channel.

Devices

UniFi devices are displayed.



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

WLAN Displays the number of wireless devices.

LAN Displays the number of wired devices.

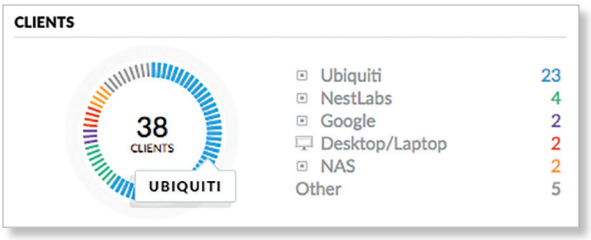
WAN Displays the number of gateway devices.

Status information Place your mouse over 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 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.

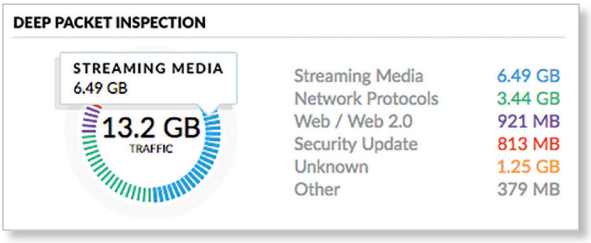
Status information Place your mouse over a specific client category to display the client category name.

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 enabled on the *Settings* > *Site* screen. See **"Settings > Site" on page 20** for more information.



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

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

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

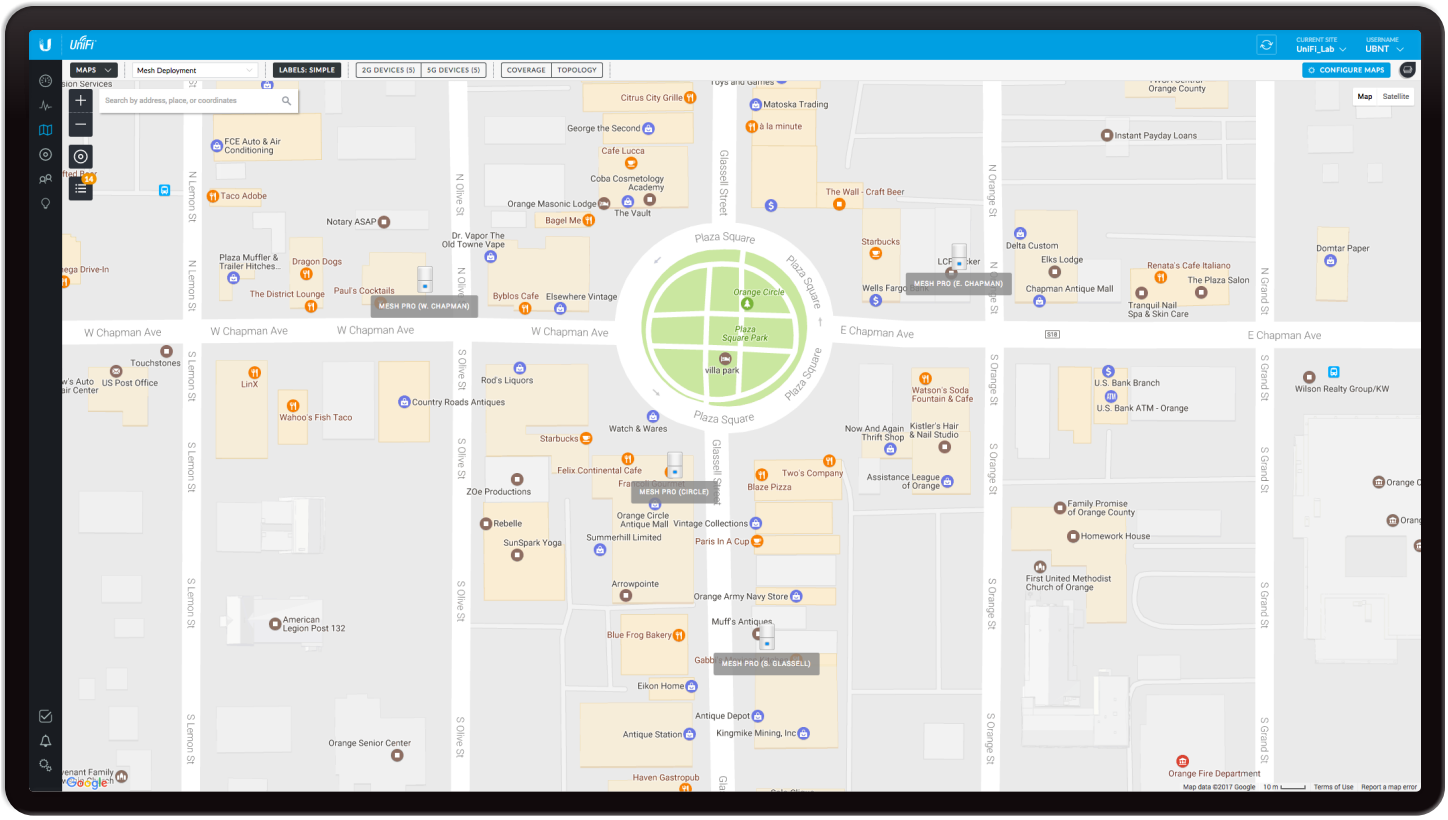
Web / Web 2.0 Displays the amount of data that is identified as web-related traffic.

Security Update Displays the amount of data that is identified as part of a security update.

Unknown Displays the amount of data that is unidentified.

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

Status information Place your mouse over a specific traffic category to display the traffic category name and amount of data.



Chapter 5: Map

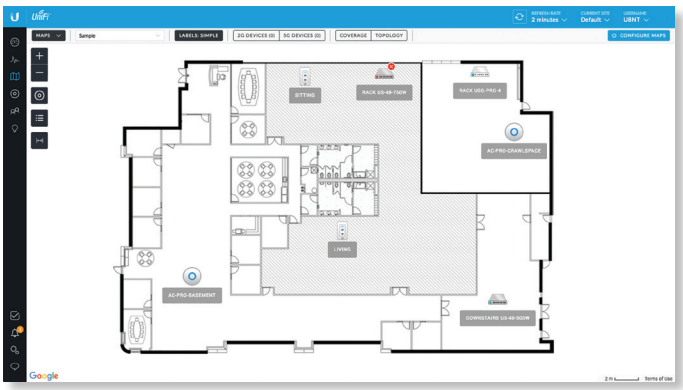
The *Map* screen allows you to upload custom map images of your location(s) or use Google Maps™ for a visual representation of your UniFi network. You can also view the system topology. When you initially launch the UniFi Controller application, a default map is displayed. The map scale is shown in the legend at the bottom of the map.

Adding Custom Maps

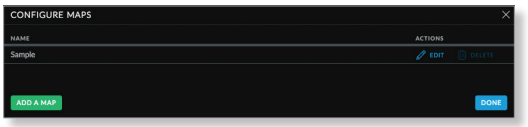
To add a custom map, you must first create the image using an illustration, image editing, or blueprint application that exports a file in .jpg, .gif, or .png file format.

Once you've created the map, you can upload it to the UniFi Controller software:

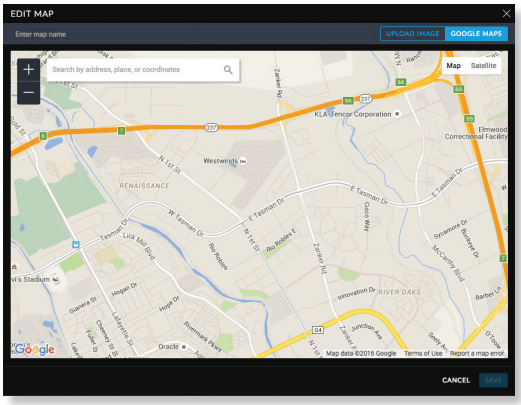
1. Click CONFIGURE MAPS.



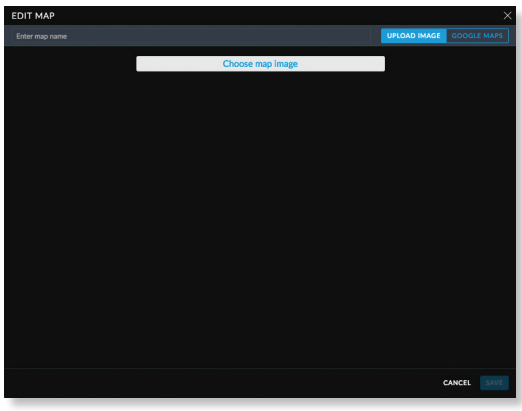
2. Click **Add a Map**.



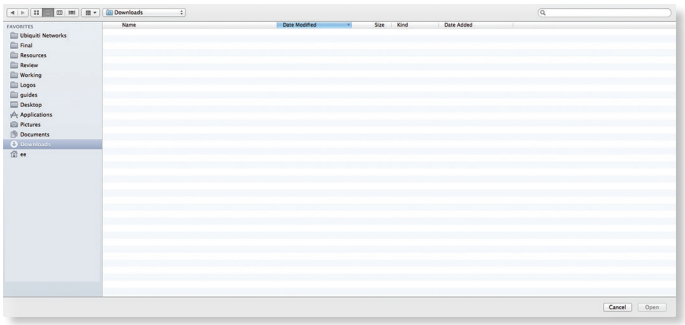
3. The default is *Google Maps*. Click **Upload Image**.



4. Click **Choose map image**.

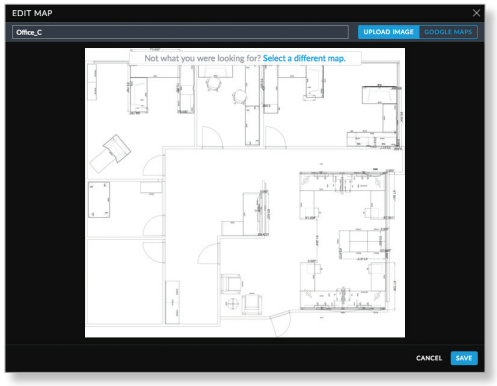


5. Locate the file to use as a map (valid file formats are .jpg, .gif, and .png) and then click **Open**. If you do not want to upload a file, click *Cancel*.



6. Enter a map name in the field provided and click **Save**.

Note: If the map is incorrect, click **Select a different map** and try again.

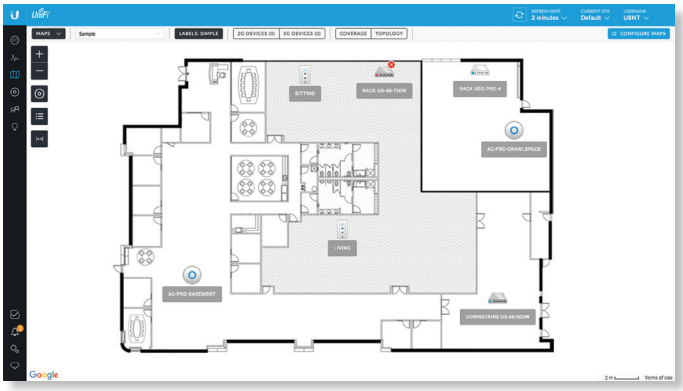


7. Click **Done**.

Adding a Google Map

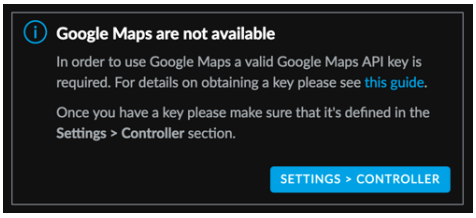
To add a *Google Map* to the UniFi Controller software *Map* view:

1. Click CONFIGURE MAPS.

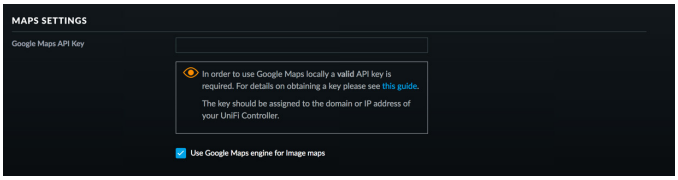


2. Click **Add a Map**.

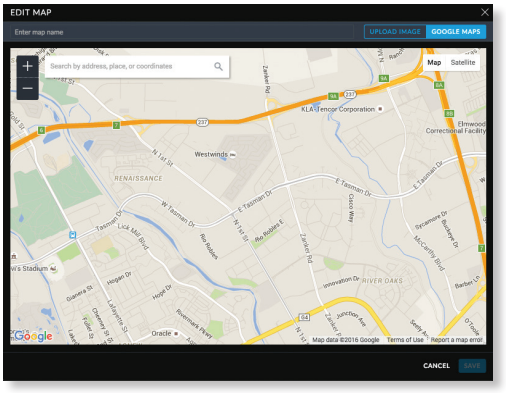
3. Enable this feature by following the provided guide on how to obtain a valid Google Maps API key.



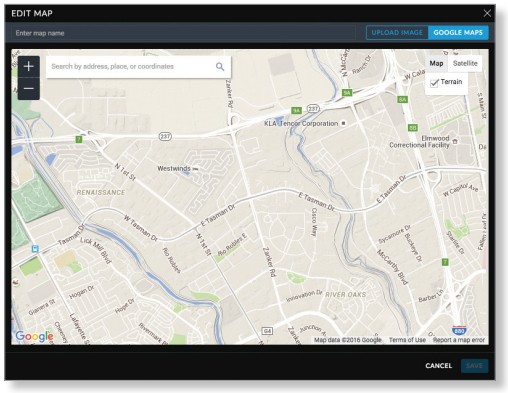
4. Go to the *Settings* > *Controller* section and enter the API key. Check the box to enable Use Google Maps engine for Image maps. Click **Apply Changes**.



5. The default view is *Map* view, which looks like a street map. Click **Terrain** to display enhanced geographical details.



Map View

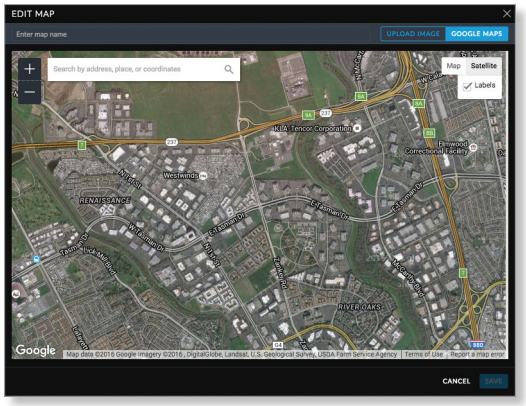


Terrain View

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.

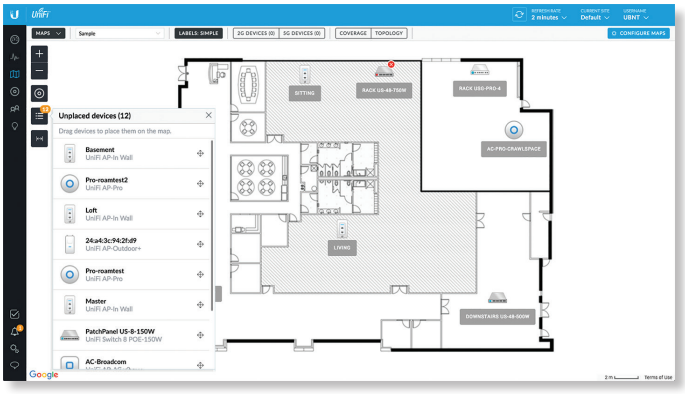


Enter a map name in the field provided and click **Save**.

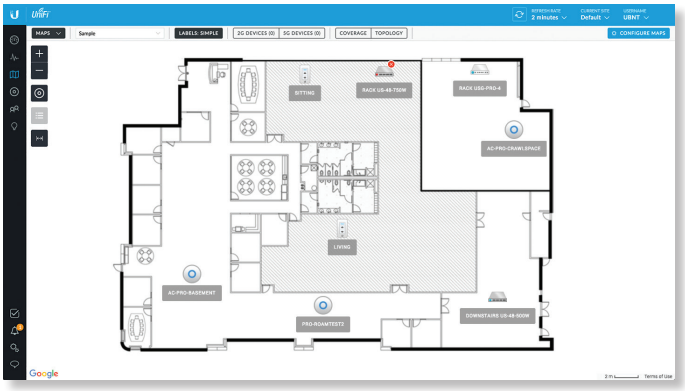
6. Click **Done**.

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.



The device icon will appear in the area that you placed it.



Once all devices have been placed the icon changes from black to gray.

Status

The device icon indicates the UniFi model (not all icons are shown below):

- UniFi AP Pro, UniFi AP AC Lite/LR/Pro
- UniFi AP AC EDU
- UniFi AP 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
- UniFi VoIP Phone/Pro
- UniFi VoIP Phone Executive

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:

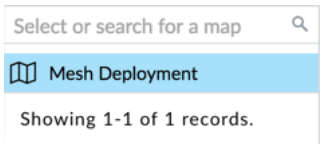
- **"UniFi Security Gateway Details" on page 85**
- **"UniFi Switch Details" on page 93**
- **"UniFi Access Point Details" on page 103**
- **"UniFi VoIP Phone Details" on page 115**

Statistics (Available for the UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU only.) Displays the *RF Environment* screen. For more information, go to **"RF Environment" on page 106**.

Remove Remove the device icon from its location.

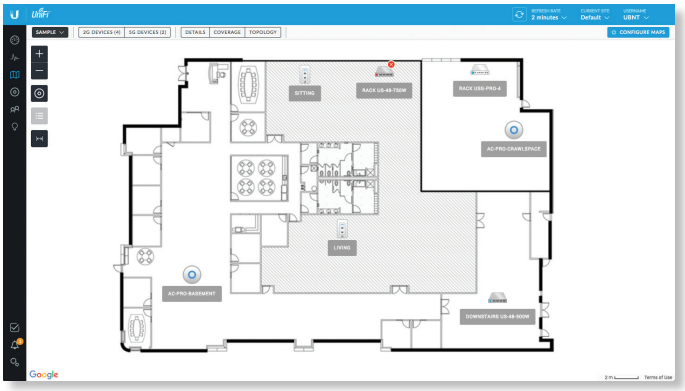
Map Display Options

(Map) If multiple maps have been uploaded, you can select which map you want to by using the Search box. There is no need to press Enter, simply start typing.



You can apply one of the following filters:

- **2G Devices** Displays the 2.4 GHz devices.
- **5G Devices** Displays the 5 GHz devices.



Each device is displayed with its name. If no custom label is applied, the device's MAC address will be displayed.

To change a name applied to a device, refer to *Alias* in the appropriate section:

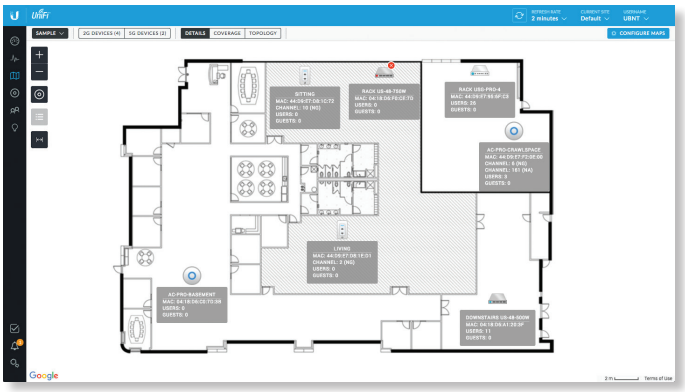
- **"UniFi Security Gateway – Configuration" on page 87**
- **"UniFi Switch – Configuration" on page 98**
- **"UniFi Access Point – Configuration" on page 108**

You can apply one of the following display options:

- Labels (None/Simple/Detailed)
- Coverage
- Topology

Labels Click this button to cycle between the following options for label display:

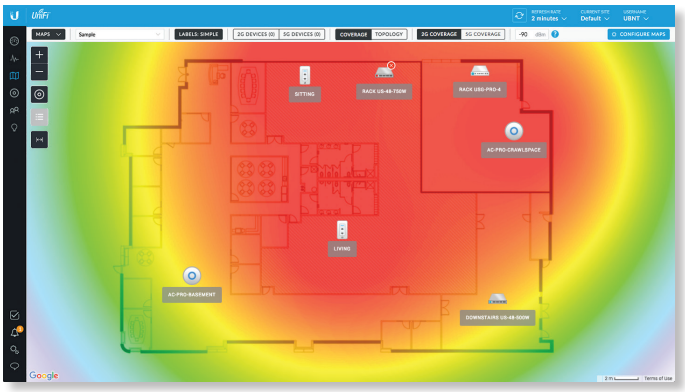
- **None** Do not display device labels.
- **Simple** Display simple device labels containing the device name only.
- **Detailed** Display detailed device labels containing the following information: device name, MAC address, transmit/receive channel(s), number of users connected, and number of guests connected.



Coverage Displays a visual representation of the wireless range covered by any APs.

You can apply one of the following filters:

- **2G Coverage** Displays the coverage by 2.4 GHz devices.
- **5G Coverage** Displays the coverage by 5 GHz devices.
  - **__ dBm** You can change the receiver sensitivity value for more accurate coverage results. The default is *-90* dBm.



Topology 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.

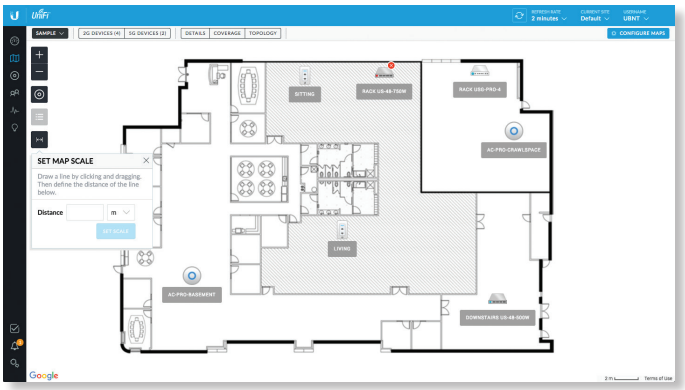
Configure Maps Click CONFIGURE MAPS to add maps or edit the current map(s).

The left side of the map offers the following options:

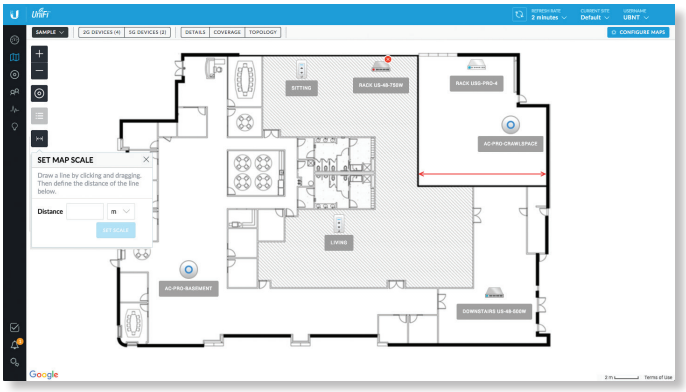
- **Zoom Slider** Use to zoom the map detail in and out.
- **Devices** Click to toggle the size of devices and their labels between normal (default) and large.
- **Unplaced Devices** Drag each device icon from the *Unplaced Devices* list to the appropriate location on the map.
- **Set Map Scale** Use this option to define the scale of the map. You will draw a line and define the distance that the line represents.

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**.

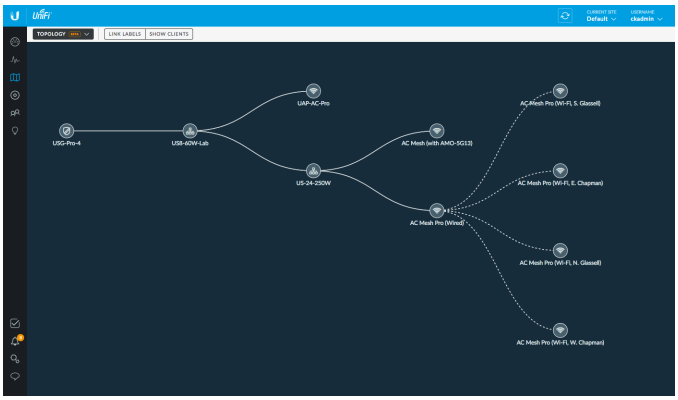


The legend at the bottom of the map shows the new scale of the map.

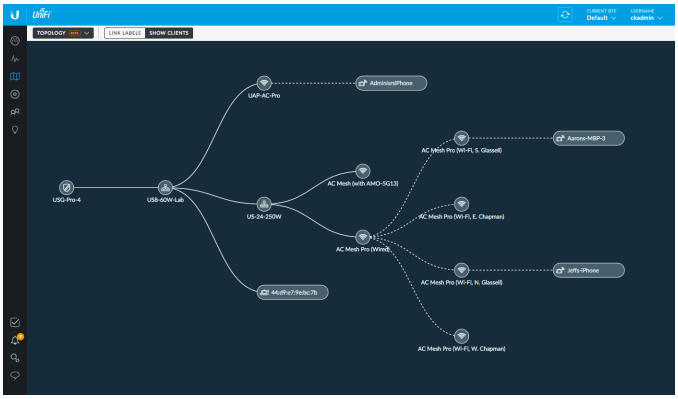
System Topology

1. Click MAPS, and then select **Topology** from the drop-down menu.
2. The UniFi Controller displays a topology diagram of your UniFi system.

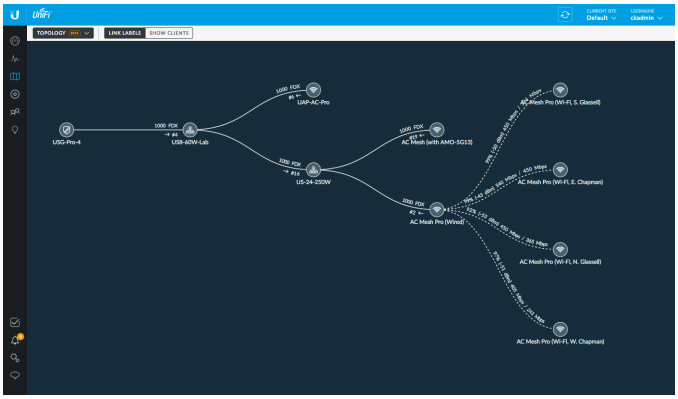
   The default view shows the entire topology tree, except for client devices. Click any node to collapse the branches below (to the right of) that node. Clicking the root node collapses the entire tree.



3. Click **Show Clients** to display client devices.



4. Click **Link Labels** to display labels on each link:



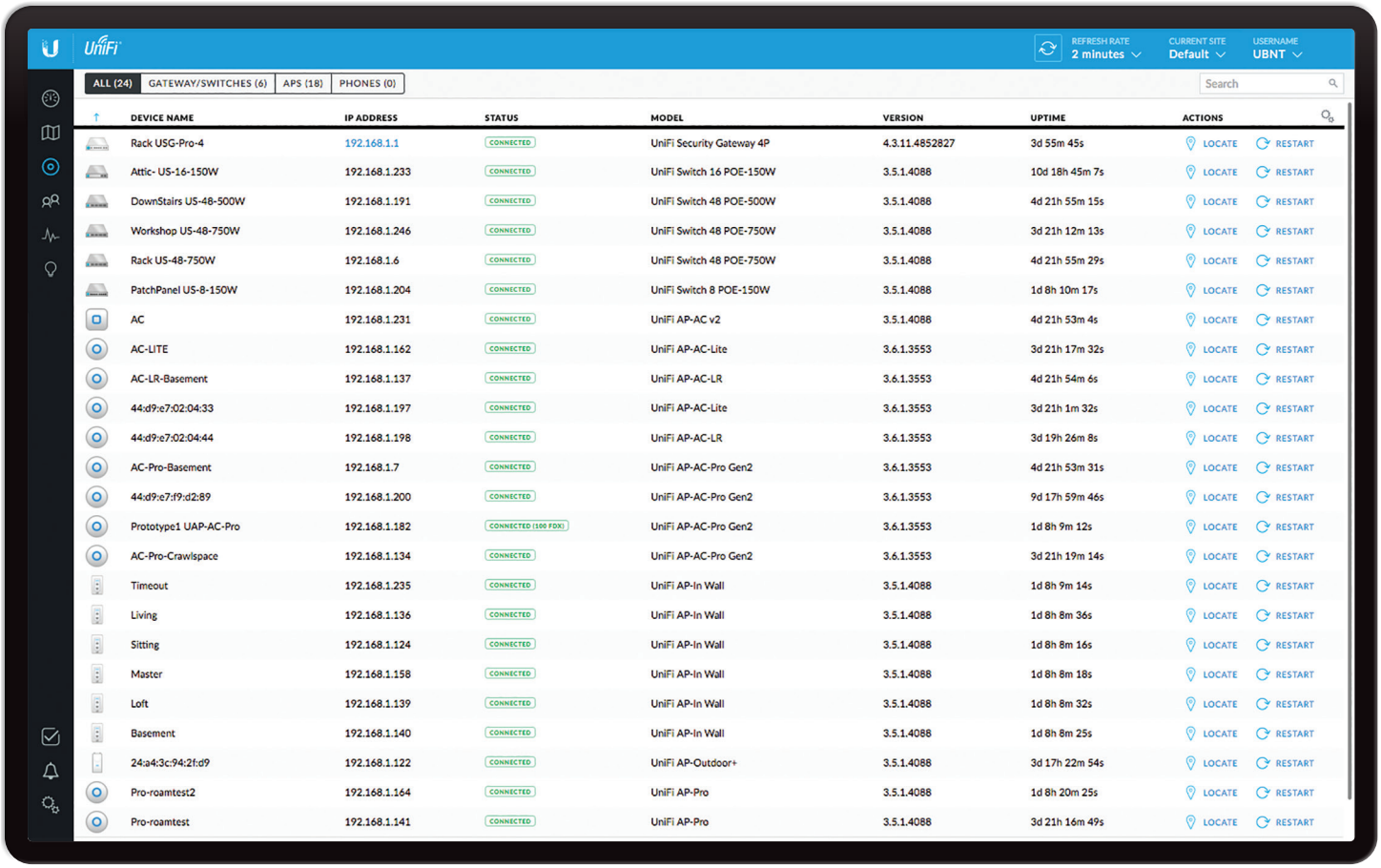
The labels provide the following information:

Wired links

- Data rate in Mbps
- Duplex type: *FDX* for full duplex, *HDX* for half duplex
- Port number to which the device is physically 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 (n Mbps / n Mbps)



Chapter 6: 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.
- **Phones** Displays all UniFi VoIP Phones.

If the *APs* filter is applied, then another filter is available:

- **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 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 Gateway
- Connected Switch
- Connected AP
- Connected Phone
- 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.

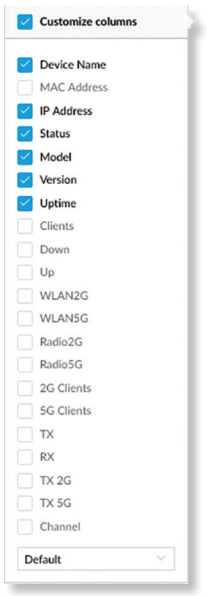
Customize Columns Each primary filter: *All*, *Gateway/Switches*, *APs*, or *Phones* applies a default set of columns to display. If you enable the *Customize Columns* option, then the primary filter no longer changes the columns.

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.

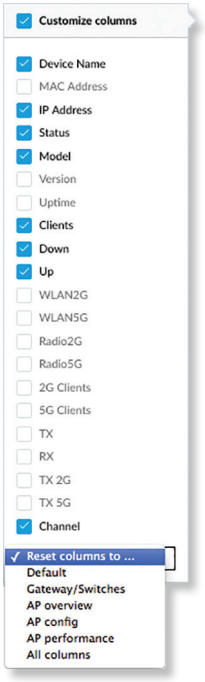
Click to customize the columns used for display.

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*, *APs*, or *Phones* you select. This resets the columns but the UniFi Controller software will not remember your 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*, *Down*, *Up,* and *Actions* columns are displayed.
  - **AP Overview** The *Device Name*, *IP Address*, *Status*, *Model*, *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*, *Clients*, *Down*, *Up*, *WLAN2G*, *WLAN5G*, *Radio2G*, *Radio5G*, *2G Clients*, *5G Clients*, *TX*, *RX*, *TX 2G*, *TX 5G*, *Channel*, *Ch. Util. 2G*, *Ch. Util. 5G,* and *Actions* columns are displayed.



Enable Group Config

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
- UniFi AP AC EDU
- UniFi AP 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

UniFi VoIP Phone/Pro

UniFi VoIP Phone Executive

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 85**
- **"UniFi Switch Details" on page 93**
- **"UniFi Access Point Details" on page 103**
- **"UniFi VoIP Phone Details" on page 115**

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 super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The super admin 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.

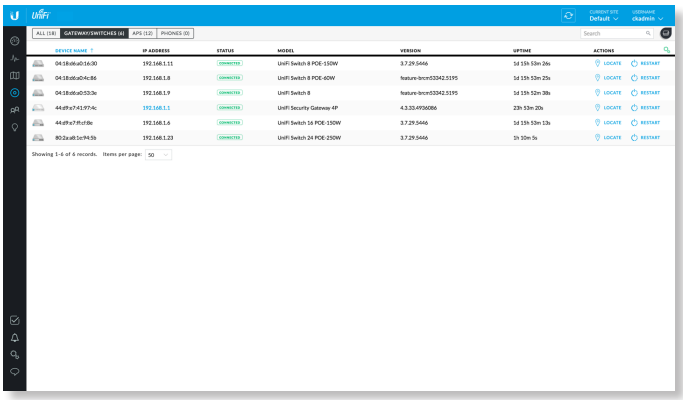
Actions Click a button to perform the desired action:

- **Locate** For most devices, 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.)

  If the device is a Phone, then click LOCATE to ring the Phone and flash the Phone's icon on the *Map* tab so you can locate it. The Phone will ring until you click *Locate* 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 85**
- **"UniFi Switch Details" on page 93**

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 super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The super admin 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.

Down Displays the total amount of data downloaded by the UniFi device.

Up Displays 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.

APs

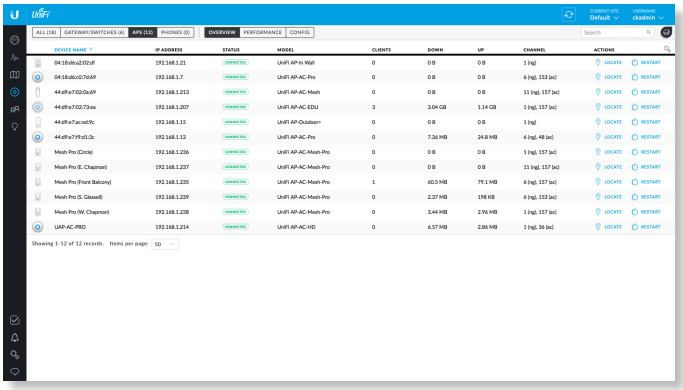
You can apply one of the following filters to display different status information:

- **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
- UniFi AP AC EDU
- UniFi AP 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 103** 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 super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The super admin 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.

Clients Displays the number of clients connected to the AP.

Down Displays the total amount of data downloaded by the AP.

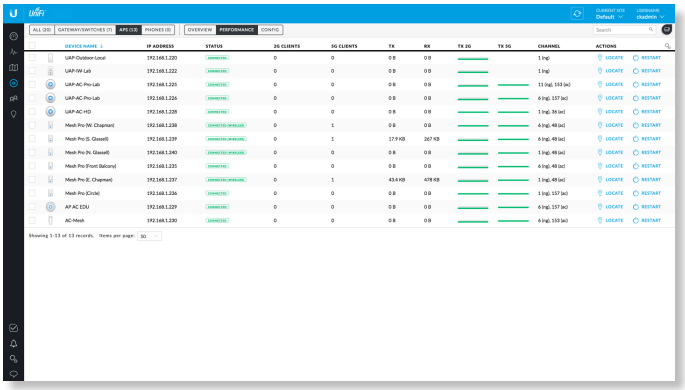
Up Displays the total amount of data uploaded by the AP.

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.

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
- UniFi AP AC EDU
- UniFi AP 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 103** 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 super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

  Note: The super admin 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 the overall TX (transmit) rate.

RX Displays 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:

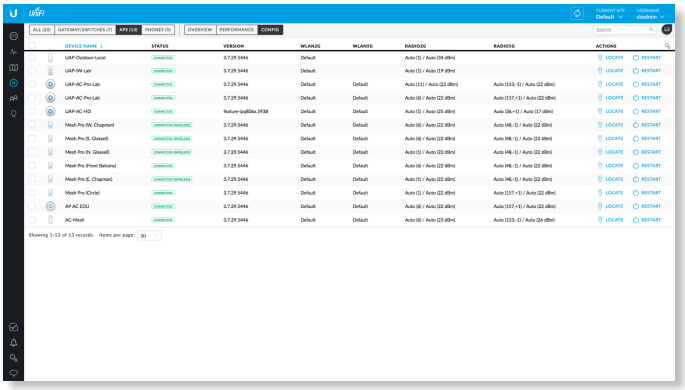
Color	Packet Activity
	Packets sent
	Packets retried
	Packets not sent due to likely interference

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
- UniFi AP AC EDU
- UniFi AP 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 103** 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 super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

  Note: The super admin 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 AP'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.

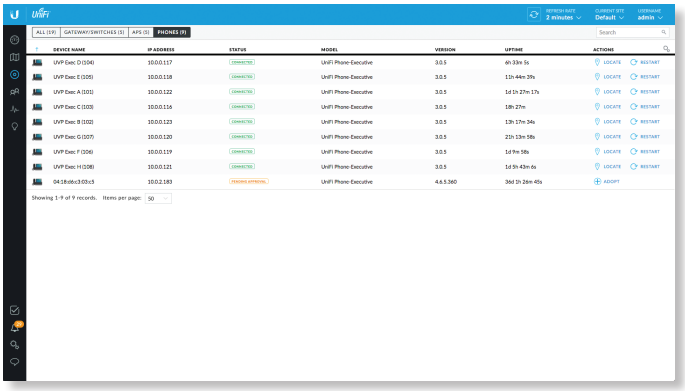
Actions Click a button to perform the desired action:

- **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.

Phones

Important: For management of the UniFi VoIP Phones, please download the UniFi VoIP Controller here: **downloads.ubnt.com/unifi**



(icon) Displays the icon corresponding to the Phone (not all icons are shown below):

UniFi VoIP Phone/Pro

UniFi VoIP Phone Executive

Device Name Displays the hostname, alias, or MAC address of the Phone. You can click the name to get additional details; see **"UniFi VoIP Phone Details" on page 115** for more information.

IP Address Displays the IP address used by the Phone.

Status Indicates the device status: *Connected*, *Disconnected*, *Pending Approval*, *Adopting*, *Upgrading*, or *Managed by Other*.

Only the super admin – not any site admin – can view devices that are *Pending Approval* and then adopt them on the UniFi Controller.

Note: The super admin account was created during the initial installation; for more information, see **"Configuring the UniFi Controller Software" on page 2**.

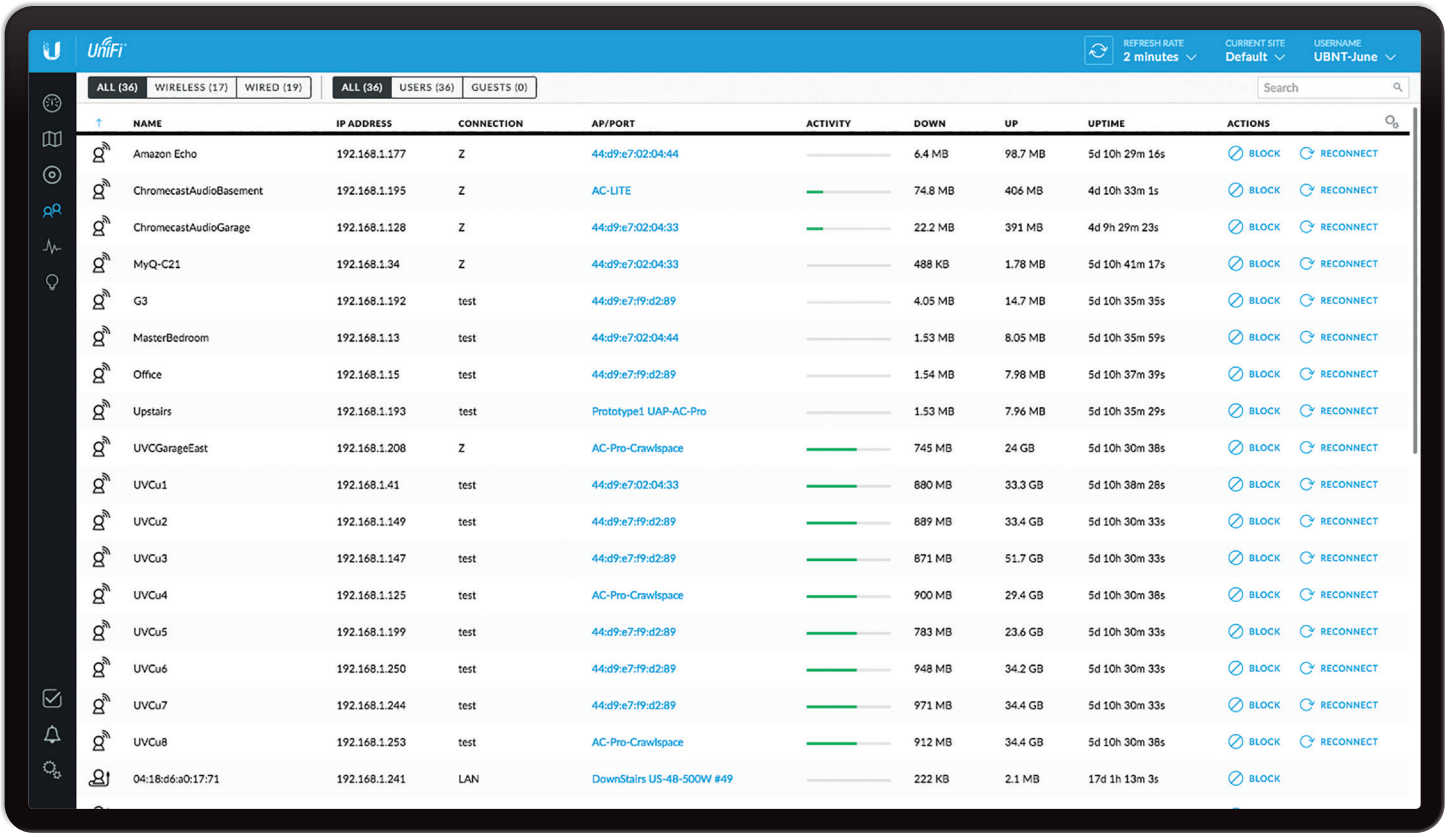
Model Displays the model name of the Phone.

Version Displays the version number of the Phone's firmware.

Uptime Displays the duration of time the Phone has been running.

Actions Click a button to perform the desired action:

- **Locate** Click LOCATE to ring the Phone and flash the Phone's icon on the *Map* tab so you can locate it. The Phone will ring until you click *Locate* 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 7: 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** Only displays users.
- **Guests** Only displays 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.

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:

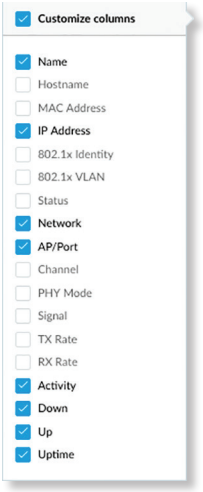
- Connected wireless user
- Connected wireless guest
- Connected wired user
- Connected wired guest

After this sorting is applied, the sort order uses alphabetical order according to the client name.

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 **"Chapter 7: Clients" on page 67** 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.
- **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 103** 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 93** 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.
- **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.
- **Down** Displays the total amount of data downloaded by the client.
- **Up** Displays the total amount of data uploaded by the client.
- **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 guest

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 117** 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.

Down Displays the total amount of data downloaded by the client.

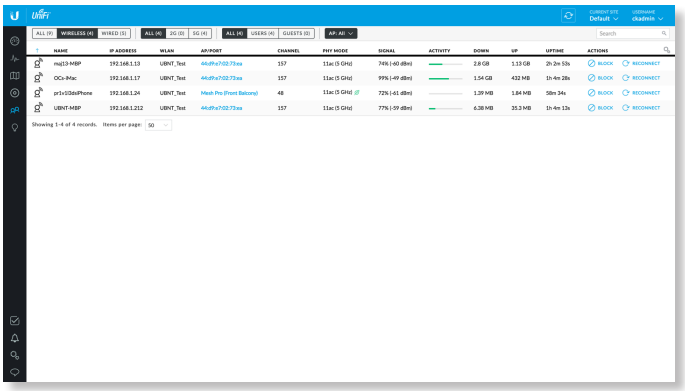
Up Displays the total amount of data uploaded by the client.

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** Only displays 2.4 GHz clients.
- **5G** Only displays 5 GHz clients.

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 117** 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 103** for more information.

Activity Displays the relative level of activity for each client.

Down Displays the total amount of data downloaded by the client.

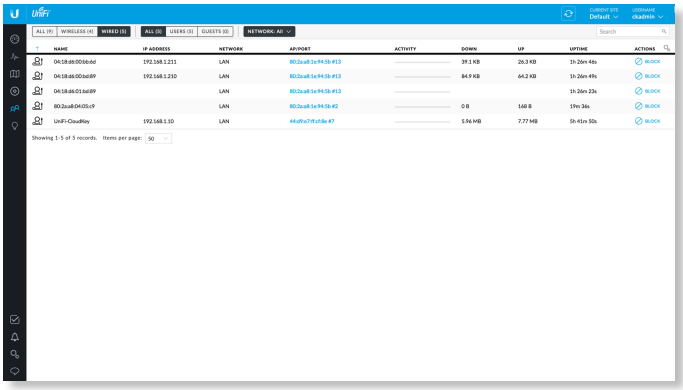
Up Displays the total amount of data uploaded by the client.

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



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 117** 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 93** for more information.

Activity Displays the relative level of activity for each client.

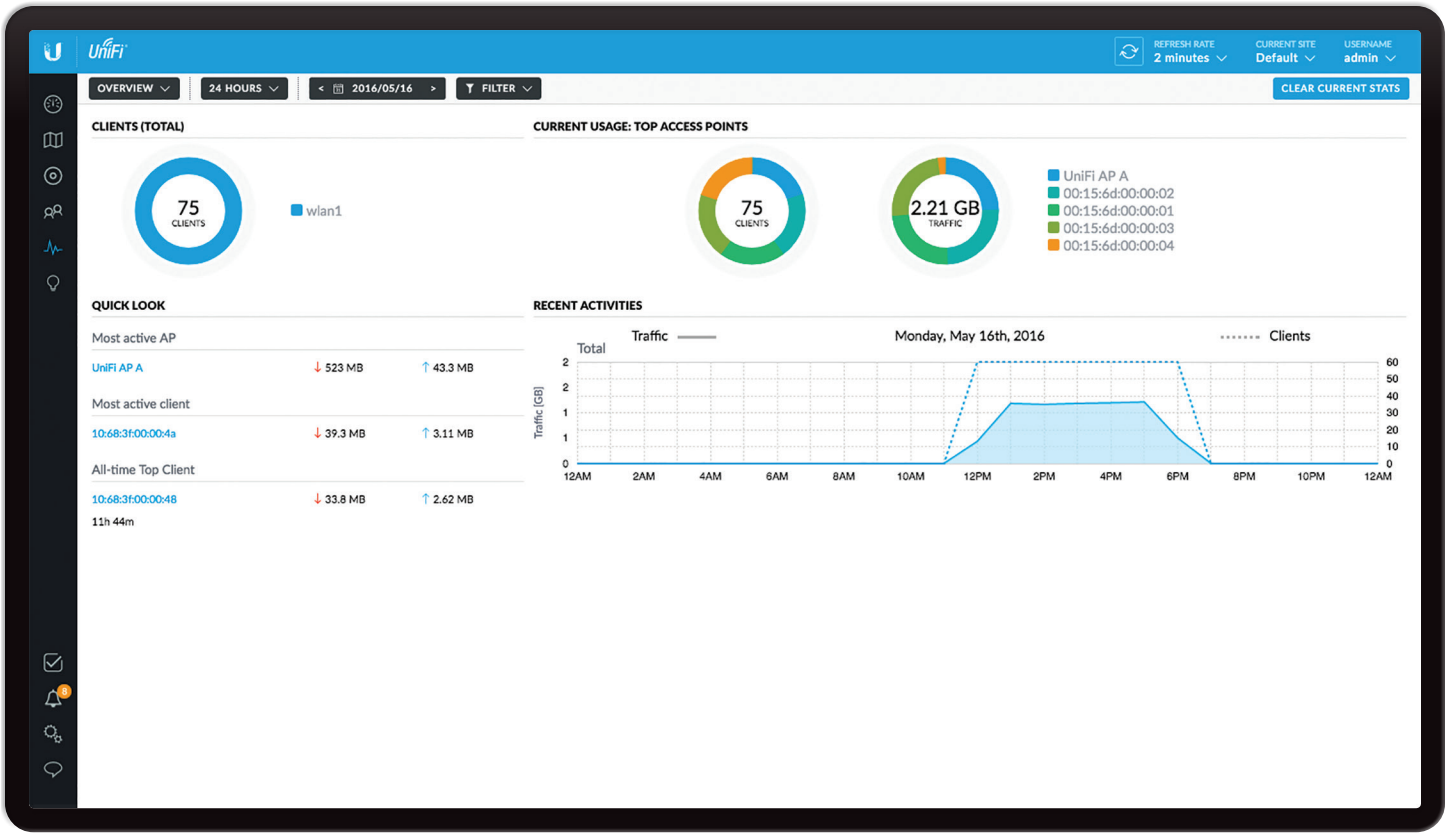
Down Displays the total amount of data downloaded by the client.

Up Displays the total amount of data uploaded by the client.

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 8: Statistics

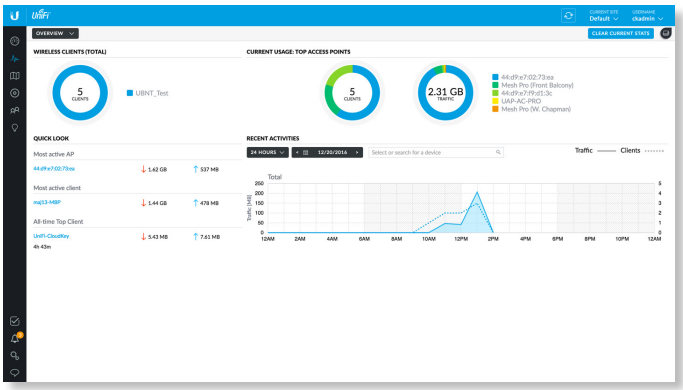
The *Statistics* screen provides a visual representation of the clients and network traffic connected to your managed UniFi network.

There are two views available:

- **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 application usage. Go to **"Traffic Stats" on page 73** for more information.
- **Switch Stats**

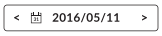
Overview

The *Overview* screen describes the usage by wireless clients and UniFi Access Points.



24 Hours The default view. Select **Week** or **Month** to change the duration interval.

Date Click either arrow to change the date in one-day increments.

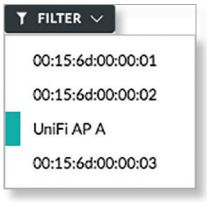


Click the date to display the calendar.

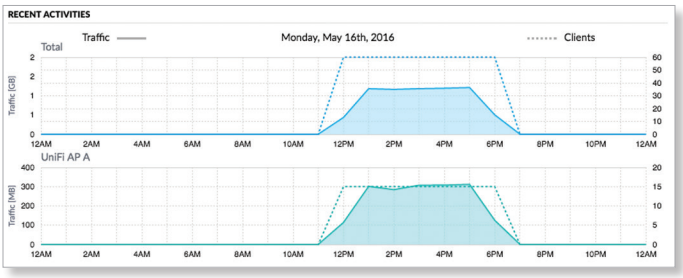
- **Calendar** Click a specific date to display its statistics. Click either arrow to change the calendar in one-month increments.

Filter You can view the number of clients and amount of traffic by UniFi AP. The *Filter* drop-down list displays managed UniFi APs by name or MAC address.

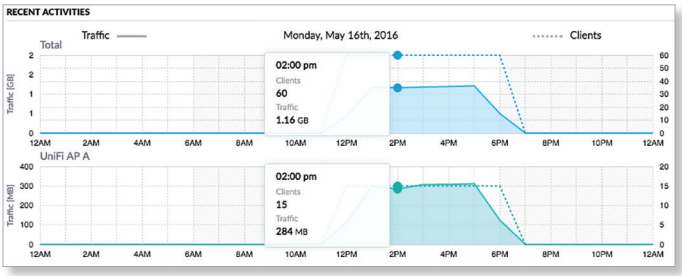
Click FILTER to view the drop-down list. Then click the appropriate AP.



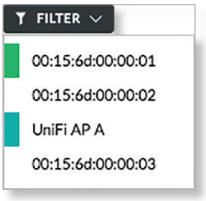
A second graph that is color-coded to the selected AP appears.



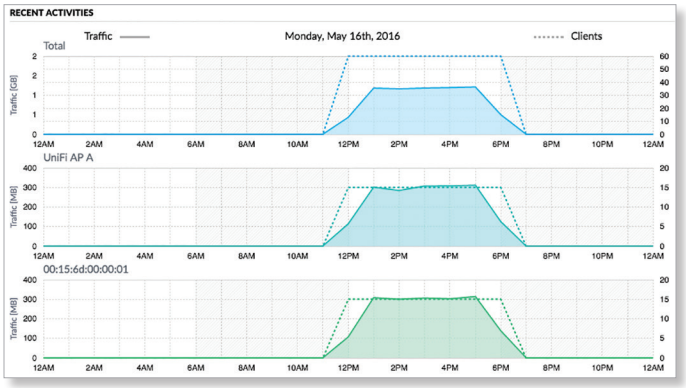
You can place your mouse over an hour or day to display the number of clients and amount of data.



You can select multiple APs for filtering. For example, if you select a second AP:

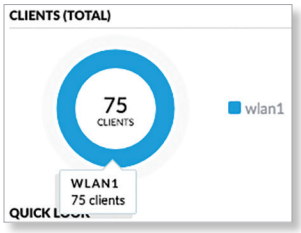


A third graph that is color-coded to the additional AP appears.



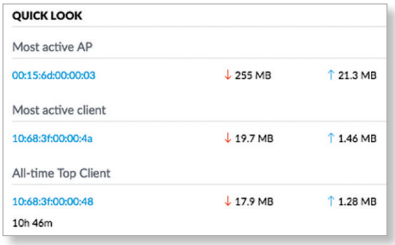
Clear Current Stats Reset the current statistics to start over.

Clients (Total)



# of Clients A visual pie chart represents the client distribution amongst the APs. Place the mouse cursor over the chart for the number of clients per network.

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 103** 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 117** 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.

All-Time Top Client

The details of the all-time, most active client are displayed:

Name or MAC address You can click this link to open the *Client Details* screen. See **"Client Details" on page 117** for additional information.

Uptime Displays the duration of time the client has been connected.

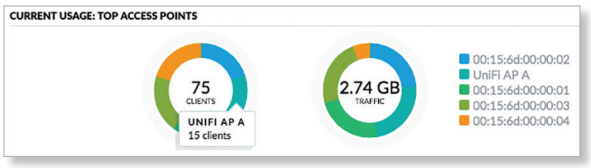
Download Displays the total amount of data downloaded by the client.

Upload Displays the total amount of data uploaded by the client.

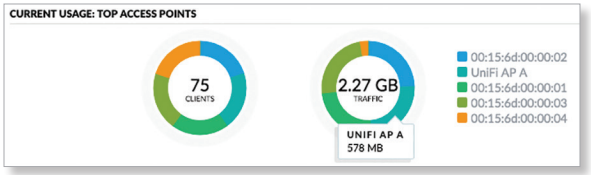
Current Usage: Top Access Points

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. Place the mouse cursor over the chart for the number of clients per specified AP.

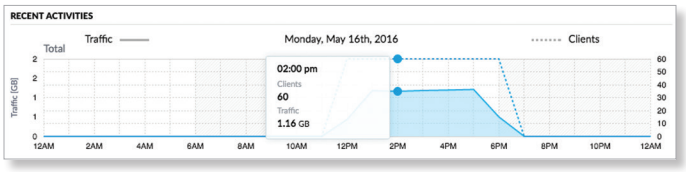


Traffic A pie chart represents traffic on the most active Access Points. Place the mouse cursor over the chart for the amount of traffic per specified AP.



Recent Activities

The details of recent network activities are displayed.



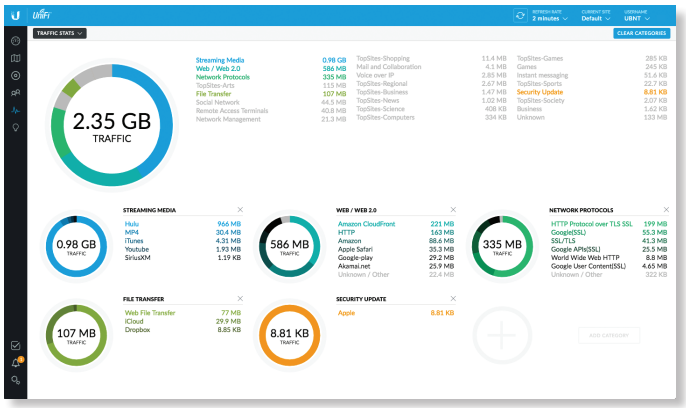
Clients In the graph, a dashed line displays the number of clients connected during the selected time period. Place the mouse cursor over an hour or day to display the exact number.

Traffic In the graph, a solid line displays the network traffic during the selected time period. Place the mouse cursor over an hour or day to display the specific amount of data.

Traffic Stats

(Available if you have a UniFi Security Gateway with the *DPI* feature enabled. Go to **"Settings > Site" on page 20** 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.

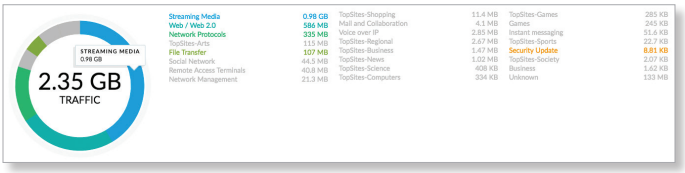


Overall Traffic

Applications are organized by category, such as Streaming Media, Web / Web 2.0, and Network Protocols. 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. Place the mouse cursor over 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.



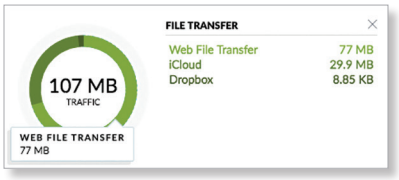
(Category)

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. Place the mouse cursor over the chart for the amount of traffic per application.

A list displays a comprehensive breakdown of the traffic by application.

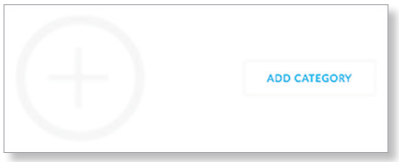
You can click ✕ to remove a category from display.

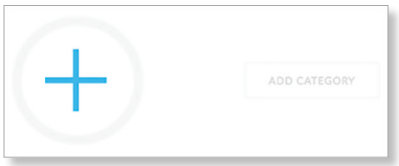


Add Category

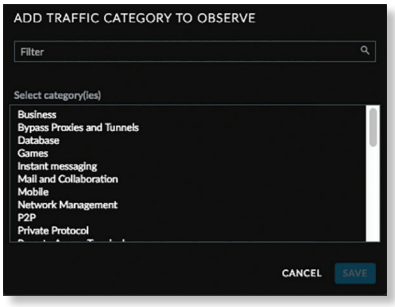
To add a new category for display, follow these steps:

1. Click **Add Category** or the + sign.

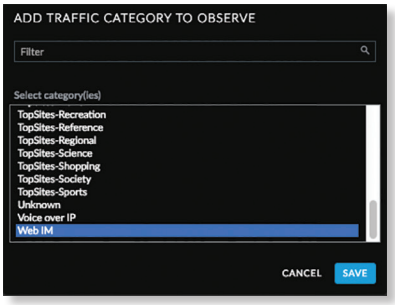


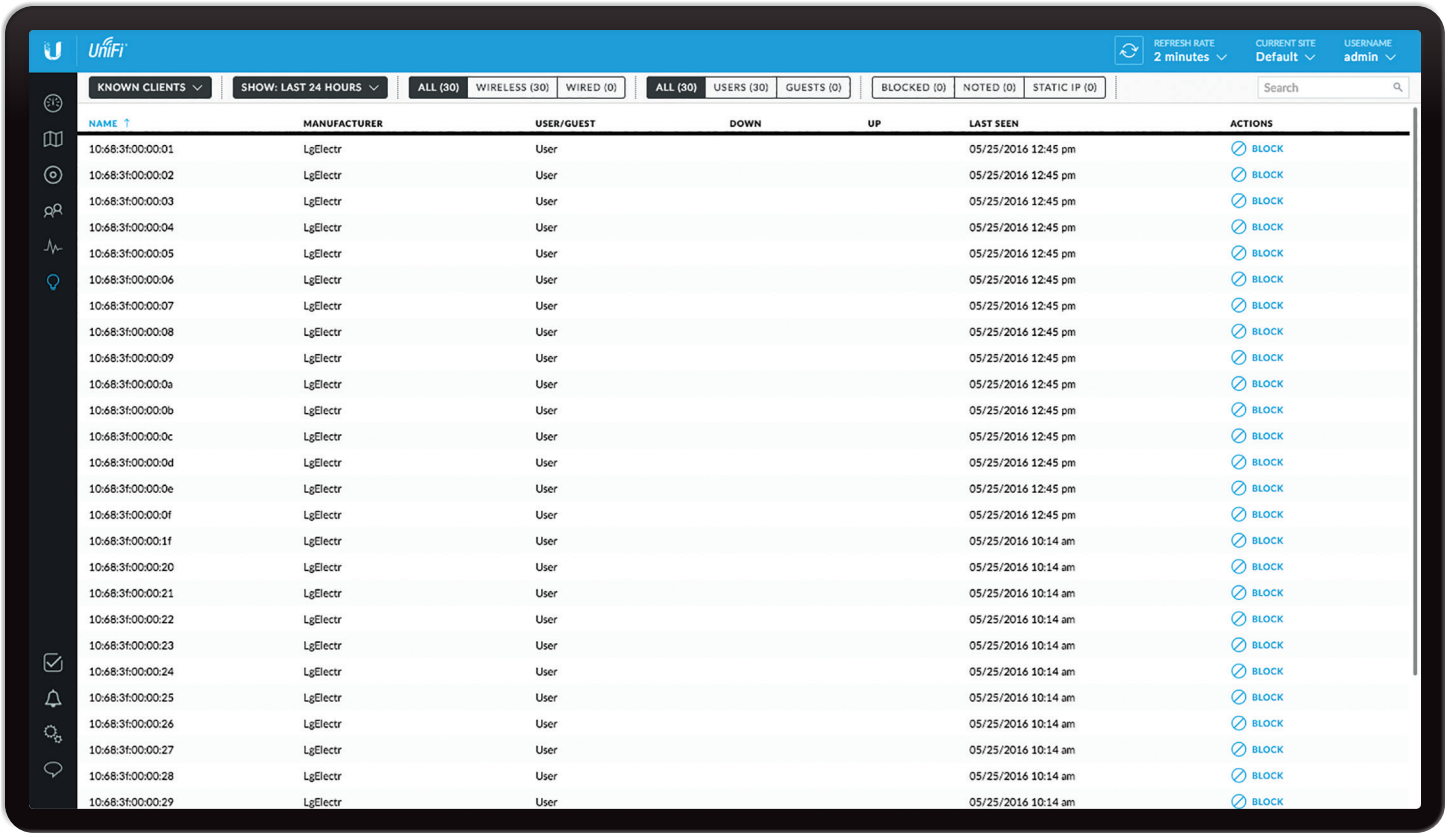


2. Select a category. You can also enter a keyword in the *Filter* field; simply begin typing; there is no need to press *Enter*.



3. Click **Save**.





Chapter 9: Insights

The *Insights* screen displays different kinds of status information. Eight filters are available:

- **Known Clients** Displays information about detected clients.
- **Neighboring Access Points** Displays information about wireless devices not managed by the UniFi Controller.
- **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.

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.

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.

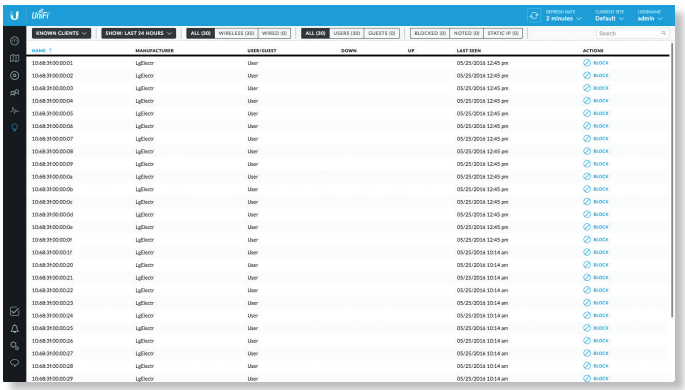
Click to customize the columns used for display.

Select **Customize columns**.

The column options will vary depending on the filter. They are described further in the following sections:

- **"Switch Stats" on page 78**
- **"Port Forward Stats" on page 81**
- **"Dynamic DNS" on page 82**
- **"Remote User VPN" on page 83**
- **"AC-EDU Streams" on page 83**

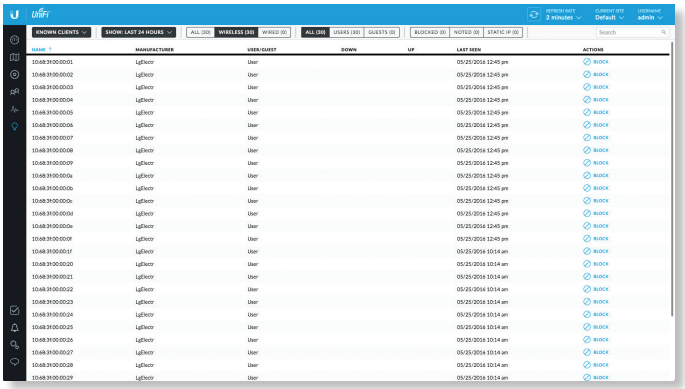
Known Clients



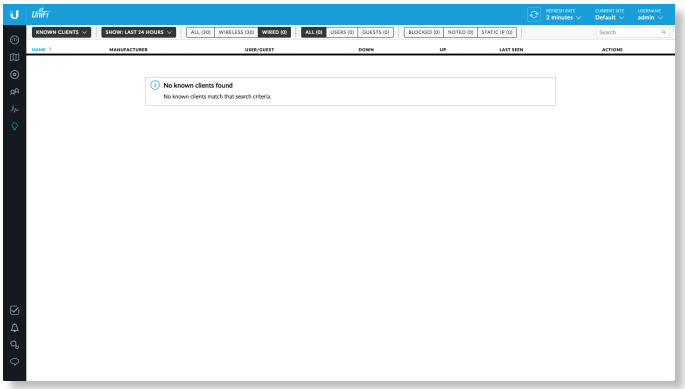
Show Filter the results on the page based on the date the client was last seen. Select **last 24 hours**, **3 days**, **7 days**, **2 weeks**, **30 days**, **120 days**, or **All**.

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:

- **Blocked** Only display blocked clients.
- **Noted** Only display clients whose configurations include notes. (See **"Wireless Client – Configuration" on page 119** or **"Wired Client – Configuration" on page 120** 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 117** for more information.

Manufacturer Displays the name of the device manufacturer.

User/Guest Indicates whether the client is/was connected to a primary or guest network.

Down Displays the total amount of data downloaded by the client.

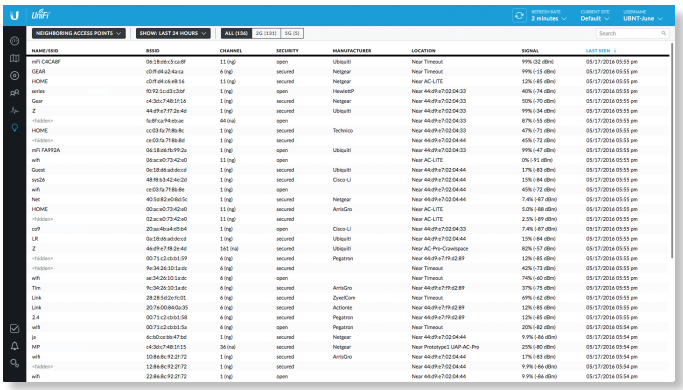
Up Displays the total amount of data uploaded by the client.

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.

Neighboring Access Points



Show Filter the results on the page based on the time the AP 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** Displays all wireless APs.
- **2G** Only displays 2.4 GHz APs.
- **5G** Only displays 5 GHz APs.

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.

Security Displays the security status indicating whether encryption is used.

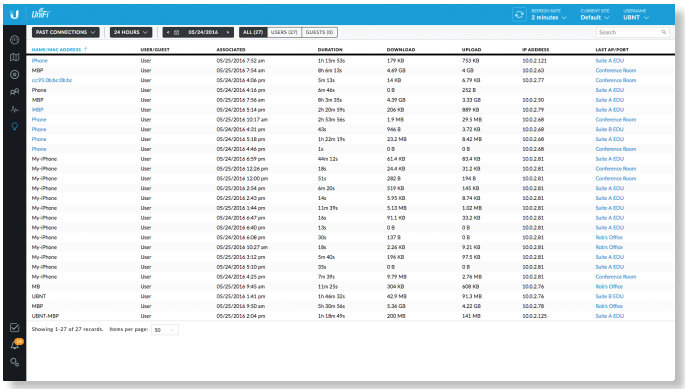
Manufacturer Displays the name of the AP manufacturer.

Location Displays the name of the closest AP managed by the UniFi Controller. You can click the name to get additional details on the AP.

Signal Displays the signal strength level and signal type:

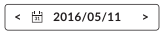
Last Seen Displays the last date and time the AP was connected.

Past Connections



24 Hours The default view. Select **Week** or **Month** 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. Click either arrow to change the calendar in one-month increments.

You can apply one of the following filters:

- **All** Display all users and guests.
- **User** Only display users.
- **Guest** 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 117** 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.

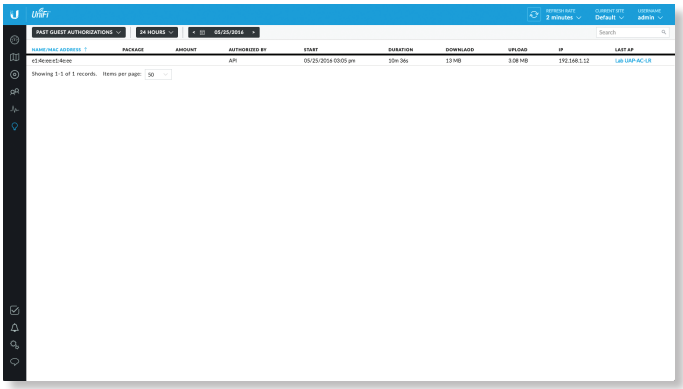
Download Displays the total amount of data downloaded by the client.

Upload Displays the total amount of data uploaded by the client.

IP Address Displays the last known IP address of the client.

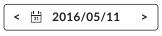
Last AP/Port Displays the name or MAC address of the last AP used by the wireless client or the last port used by the wired client. You can click the device name for more information; refer to **"UniFi Access Point Details" on page 103** or **"UniFi Switch Details" on page 93** .

Past Guest Authorizations



24 Hours The default view. Select **Week** or **Month** 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. Click either arrow to change the calendar in one-month increments.

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/Port Displays the name or MAC address of the last AP used by the wireless guest or the last port used by the wired guest. You can click the device name for more information; refer to **"UniFi Access Point Details" on page 103** or **"UniFi Switch Details" on page 93** .

Switch Stats

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.

You have additional filters:

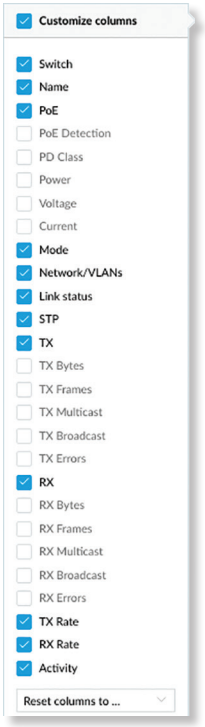
- **All Switch** Displays the ports of all UniFi Switches or a specific Switch.
- **Link Status** Displays the ports of the specified status:
  - **All** Displays all ports.
  - **Connected** Displays all connected ports.
  - **Disconnected** Displays all disconnected ports.

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.

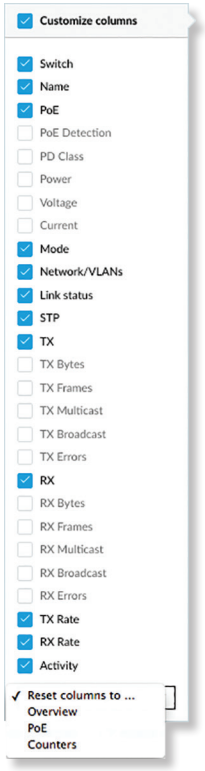
Customize Columns Click to customize the columns used for display.

Select **Customize columns**.

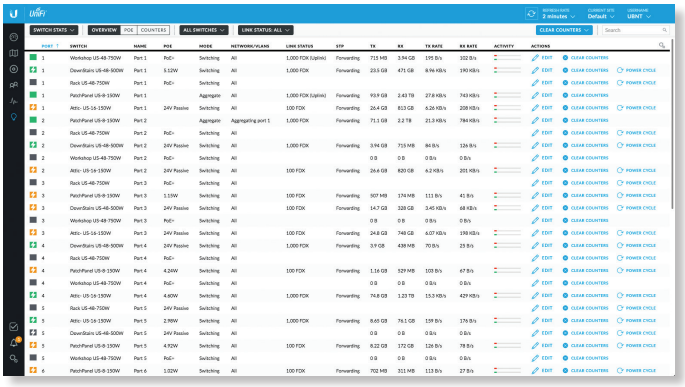


You can add or remove columns for display. The *Customize columns* option will apply, and the filter options: *Overview*, *PoE*, and *Counters* will disappear.

- **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*, *Network/VLANs*, *Link Status*, *STP*, *TX*, *RX*, *TX Rate*, *RX Rate*, 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).

Switch If *All Switches* is selected, 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 93**.

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 95**.
- **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.

Networks/VLANs Displays the networks/VLANs that the port belongs to. If the *Mode* is *Aggregate*, then it displays the aggregation detail.

Link Status Displays the connection speed and duplex mode.

STP Displays the STP (Spanning Tree Protocol) mode.

TX Displays the amount of data transmitted.

RX Displays the amount of data received.

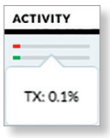
TX Rate Displays the transmit rate.

RX Rate Displays the receive rate.

Activity Displays the level of activity. The different colors represent different types of packet activity.

Color	Packet Activity
	TX rate
	RX rate

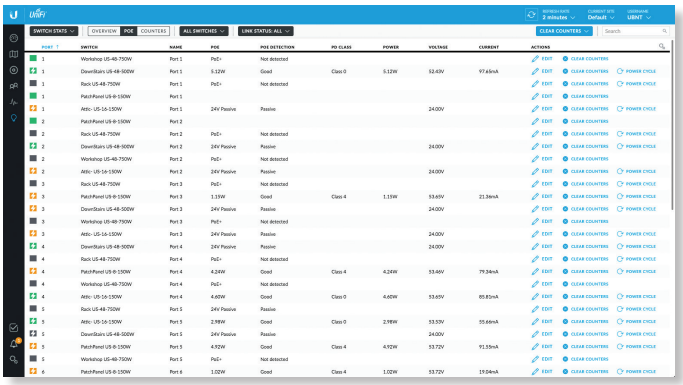
You can place your mouse over the *Activity* icon to display the specific TX or RX rate.



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 93**.
- **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).

Switch If *All Switches* is selected, 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 93**.

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.

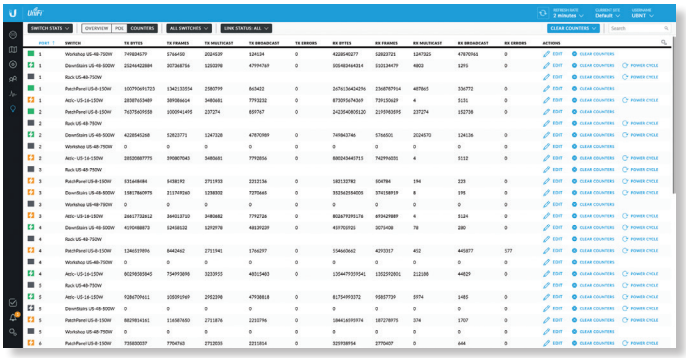
Voltage Displays the voltage output, if applicable.

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 93**.
- **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).

Switch If *All Switches* is selected, 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 93**.

TX Bytes Displays the number of bytes transmitted.

TX Frames Displays the number of frames transmitted.

TX Multicast Displays the number of multicast packets transmitted.

TX Broadcast Displays the number of broadcast packets transmitted.

TX Errors Displays the number of error packets transmitted.

RX Bytes Displays the number of bytes received.

RX Frames Displays the number of frames received.

RX Multicast Displays the number of multicast packets received.

RX Broadcast Displays the number of broadcast packets received.

RX Errors Displays 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 93**.
- **Clear Counters** Click CLEAR COUNTERS to clear the port statistics.
- **Power Cycle** If applicable, click POWER CYCLE to power cycle the port.

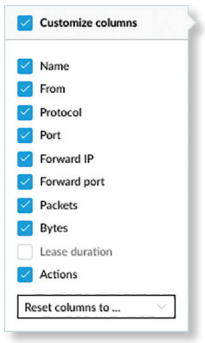
Port Forward Stats

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.

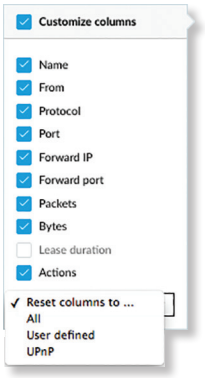
Customize Columns Click to customize the columns used for display.

Select **Customize columns**.

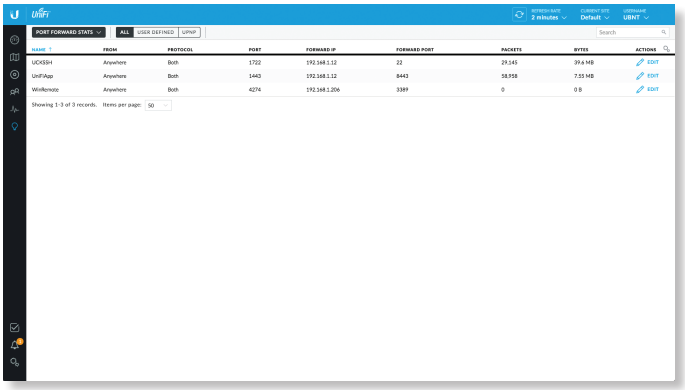


You can add or remove columns for display.

- **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).

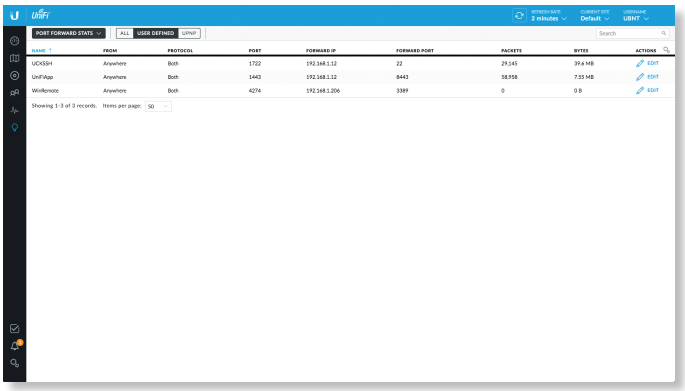
Packets Displays the number of packets transferred.

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 85**.

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).

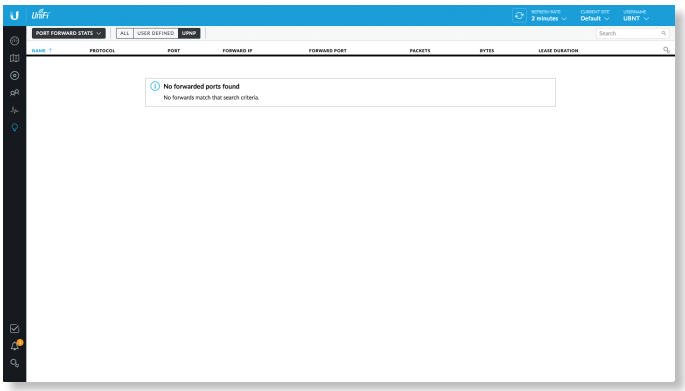
Packets Displays the number of packets transferred.

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 85**.

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.

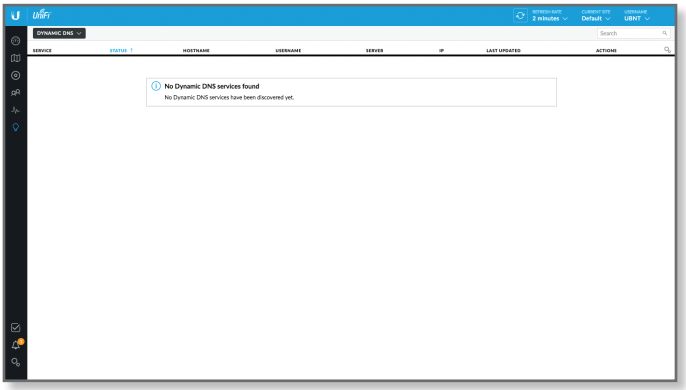
Forward Port Displays the destination port that will receive the forwarded port traffic. Also known as the internal port.

Packets Displays the number of packets transferred.

Bytes Displays the number of bytes transferred.

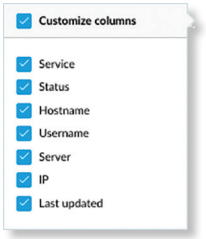
Lease Duration Displays the uptime of the port forwarding entry.

Dynamic DNS



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.

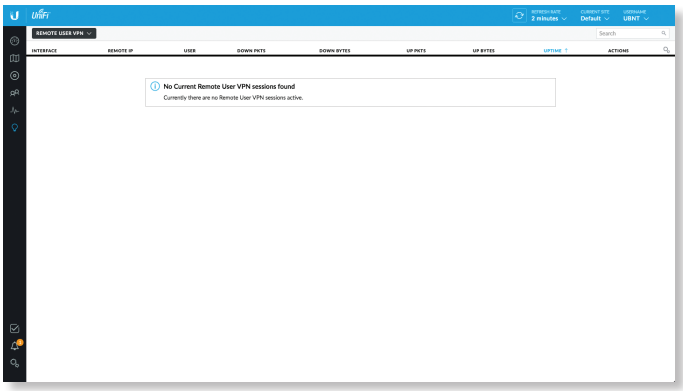
IP Displays the WAN (public) IP address of the hostname.

Last Updated Displays the duration of time since the hostname IP address was last updated.

Actions Click a button to perform the desired action:

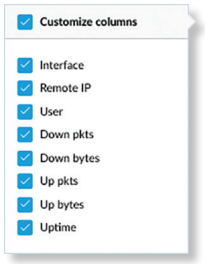
- **Edit** Click EDIT to make changes to the UniFi Security Gateway settings. For more information, see **"UniFi Security Gateway Details" on page 85**.

Remote User VPN



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.

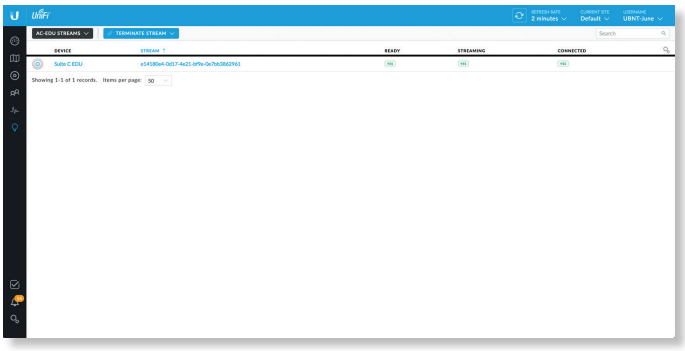
Up Bytes Displays the amount of data uploaded as bytes.

Uptime Displays the duration of time the VPN tunnel has been active without interruption.

Actions Click a button to perform the desired action:

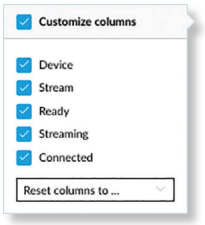
- **Terminate** Click TERMINATE to end the VPN tunnel.

AC-EDU Streams



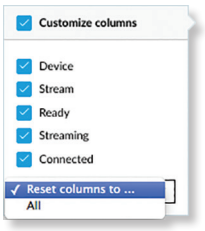
Customize Columns Click to customize the columns used for display.

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 103**.

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*.

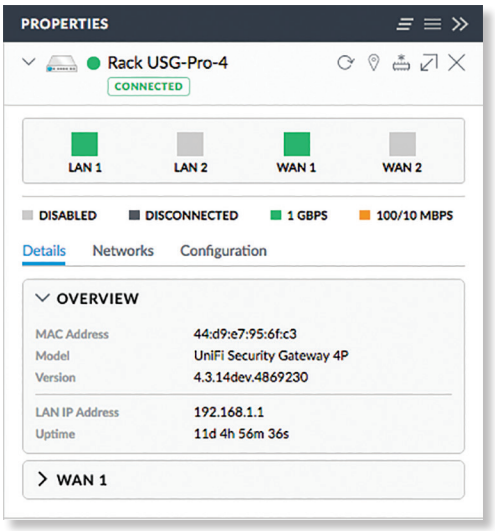
Connected Displays the status of the connection, *Yes* or *No*.

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).

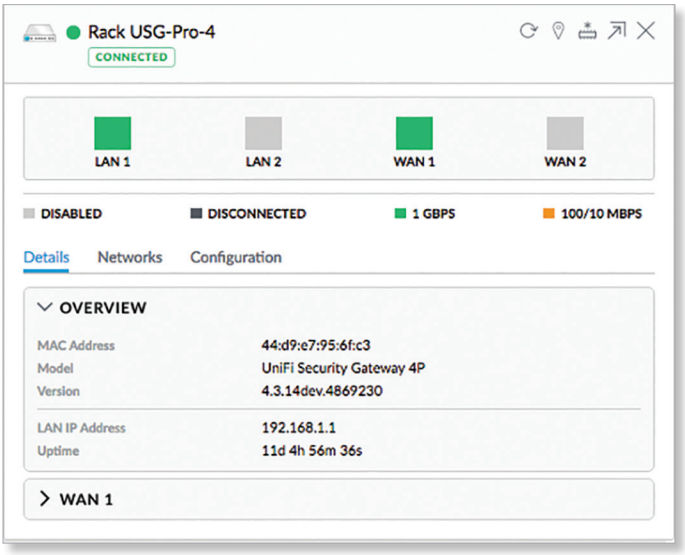
There are three clickable tabs:

- **"UniFi Security Gateway – Details" on page 86**
- **"UniFi Security Gateway – Networks" on page 86**
- **"UniFi Security Gateway – Configuration" on page 87**

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.

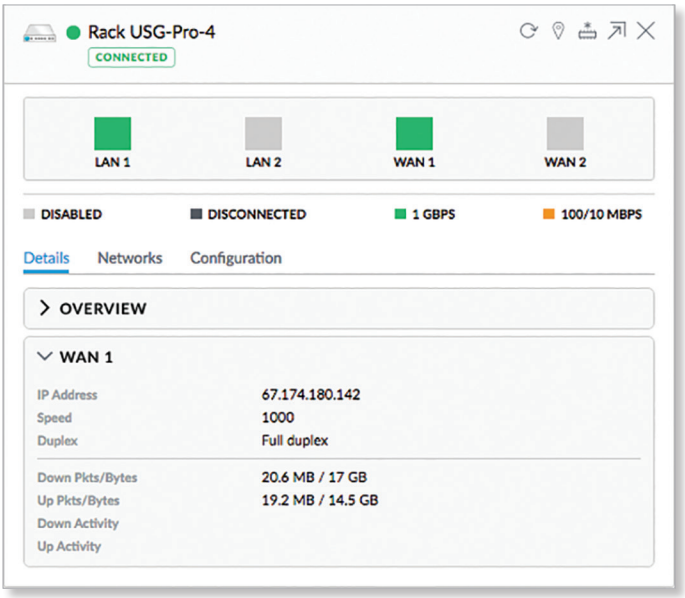
Version Displays the version number of the Gateway's firmware.

LAN IP Address Displays the local IP address of the Gateway.

Uptime Displays the duration of time the Gateway has been running without interruption.

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.

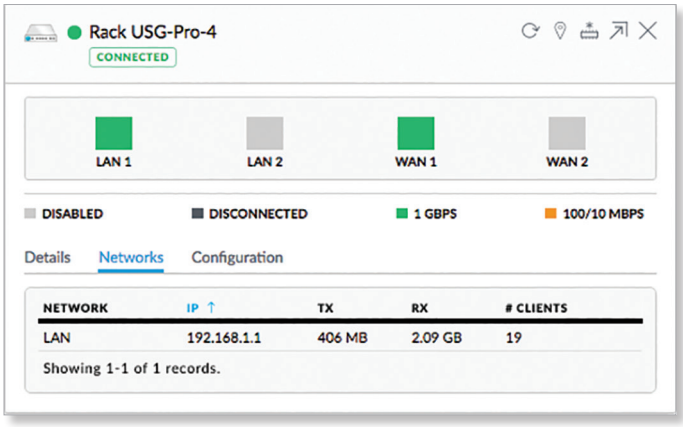
Up Pkts/Bytes Displays the amount of data uploaded as packets and bytes.

Down Activity Displays the level of download activity in Bytes per second.

Up Activity Displays the level of upload activity in Bytes per second.

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.

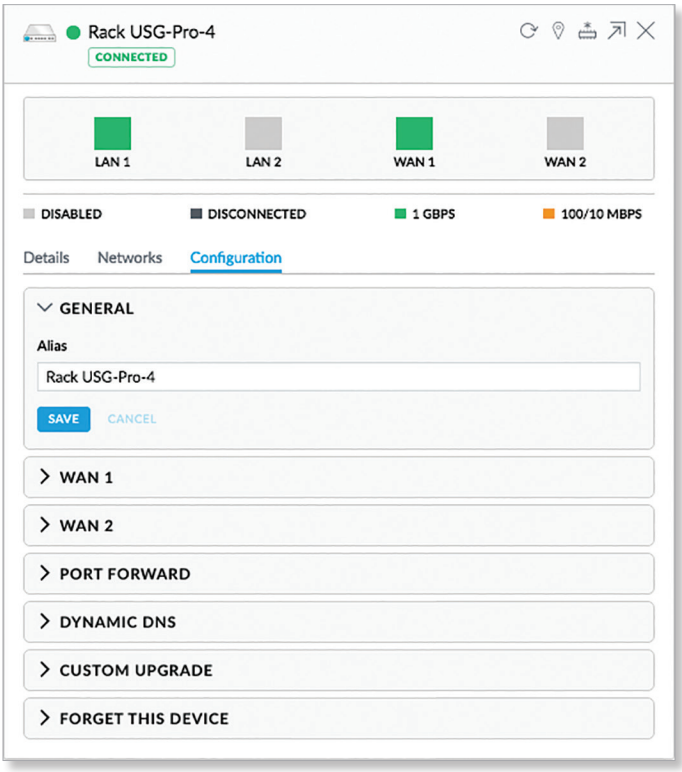
RX Displays the incoming (receive) throughput.

 # 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.

General



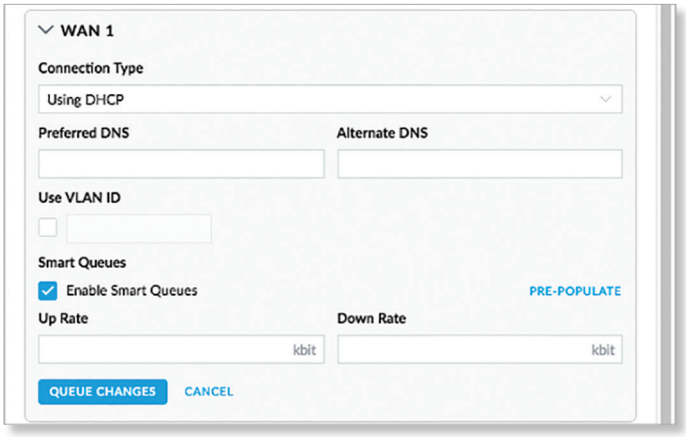
Alias Displays the customizable name or identifier of the Gateway. The *Alias* is also known as the host name.

Save Click **Save** to apply the change.

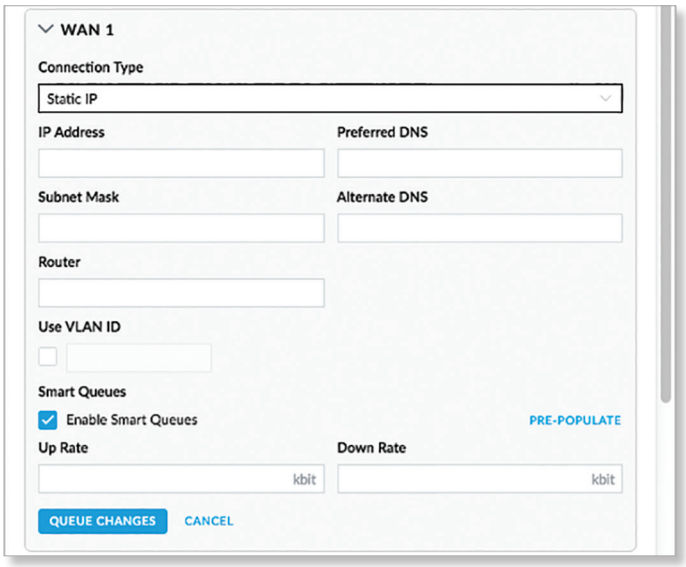
WAN 1/2

Connection Type Select the Internet connection type for your service.

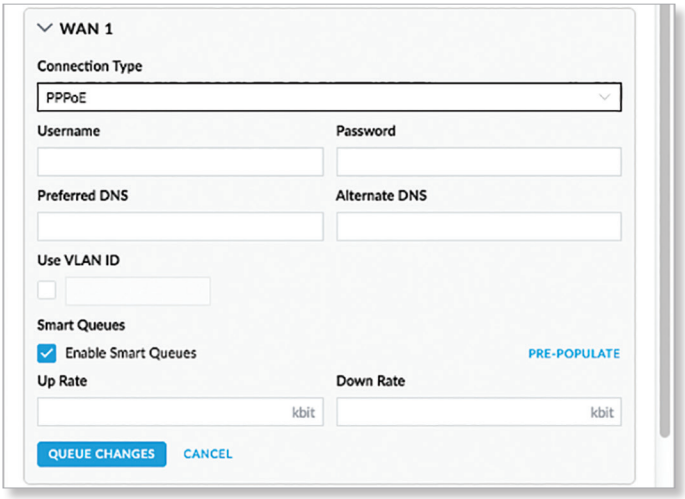
- **Using DHCP** The use of the Dynamic Host Configuration Protocol (DHCP) is the default. The Gateway automatically acquires network settings from the service provider's DHCP server.
  - **Preferred DNS** Enter the IP address of the service provider's primary DNS server.
  - **Alternate DNS** Enter the IP address of the service provider's secondary DNS server.



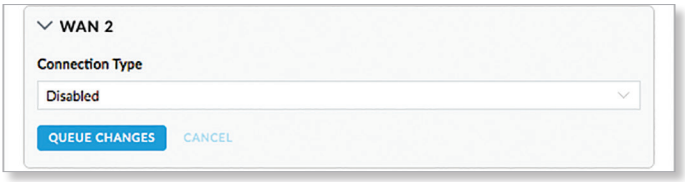
- **Static IP** The service provider assigns fixed network settings to your service for manual entry. Enter the following information:
  - **IP Address** Enter the Internet IP address of the Gateway.
  - **Subnet Mask** Enter the subnet mask of the Gateway.
  - **Router** Enter the IP address of the 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.



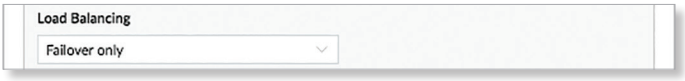
- **Disabled** If you are not using the *WAN 2* port, then select **Disabled**.



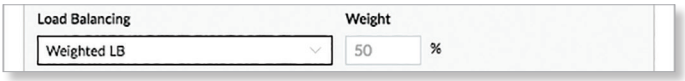
Use VLAN ID To use a VLAN, select **Use VLAN ID** and enter the VLAN ID number.

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.

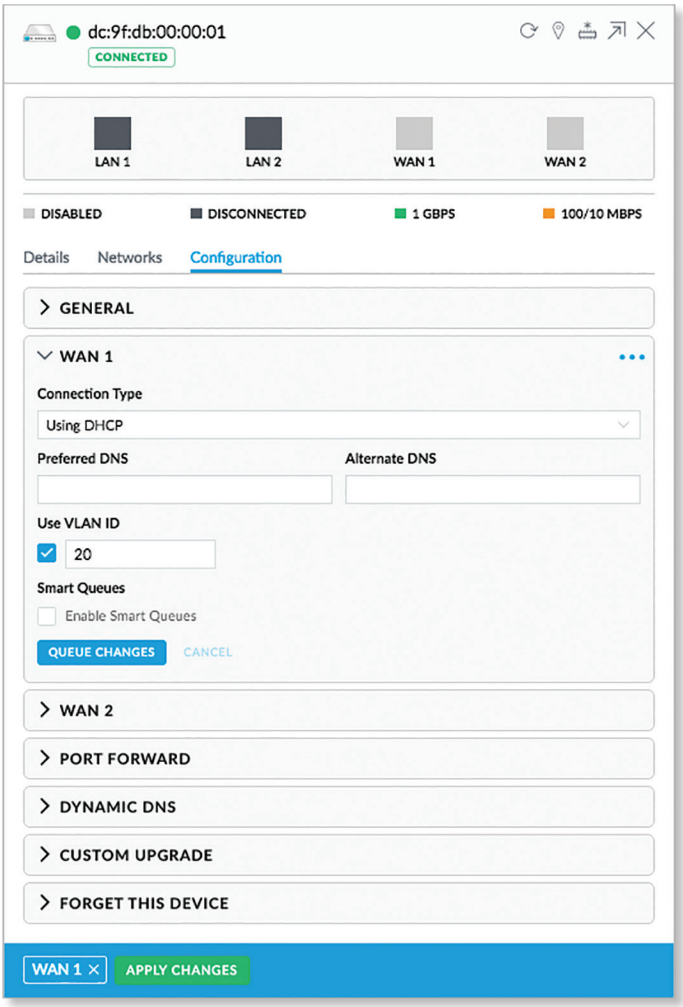
- **Pre-Populate** Click **Pre-Populate** to set the *Up* and *Down Rates* to 80% of the last speed test results.
- **Up Rate** Enter the bandwidth limit in Kbits/sec.
- **Down Rate** Enter the bandwidth limit in Kbits/sec.
- **Pre-Populate** Click **Pre-Populate** to set the *Up* and *Down Rates* to 80% of the last speed test results.

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.

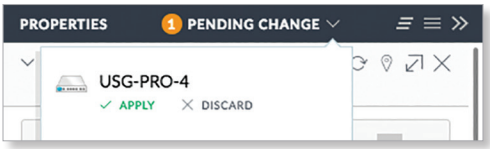
Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section 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 *Cancel* to discard changes.



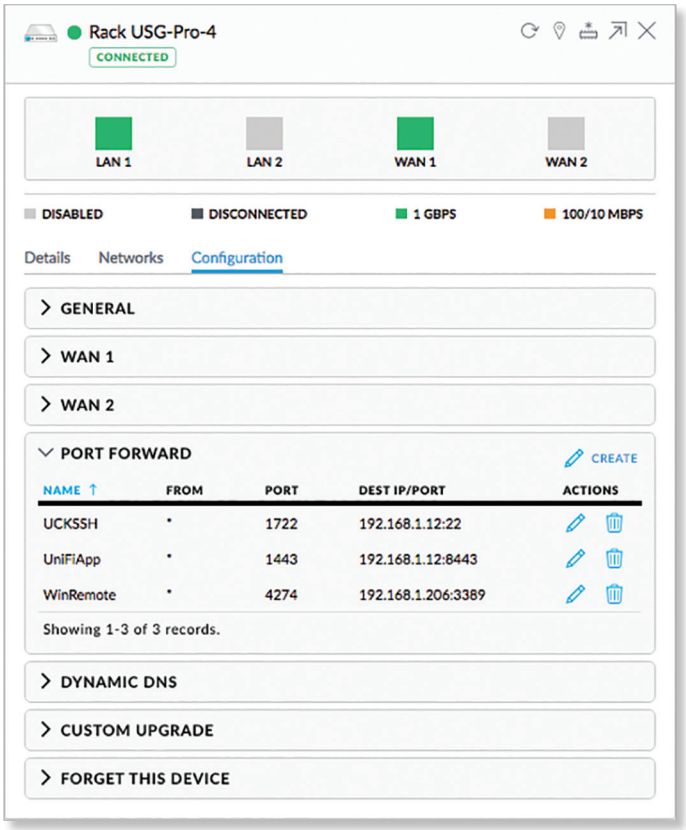
Pending Changes If you want queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.



Apply Click ✓ APPLY to save changes.

Discard Click × DISCARD to cancel changes.

Port Forward



Create Click CREATE to add a new entry. Go to **"Create or Edit Port Forwarding Entry" on page 90**.

Name Displays the name of the port forwarding entry.

From Displays the source IP address, if specified.

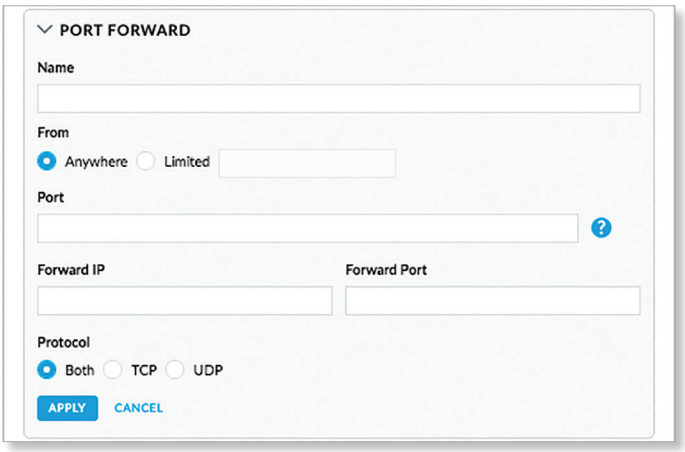
Port Displays the port or ports that will be forwarded to the LAN. Also known as the external port(s).

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 ✎ to edit the port forwarding entry.
- **Delete** Click 🗑 to delete the port forwarding entry.

Create or Edit 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.

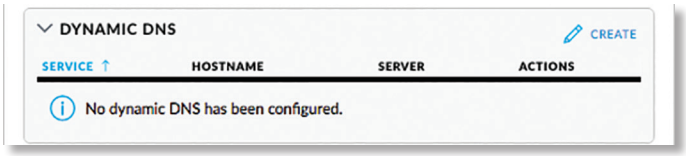
Protocol Select the protocol that will be forwarded: **Both**, **TCP**, or **UDP**.

Apply Click **Apply** to save changes.

Cancel Click *Cancel* to discard 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.



Create Click CREATE to add a new entry. Go to the *Create or Edit DDNS Entry* section on the next page.

Service Displays the name of your Dynamic DNS (DDNS) service provider.

Hostname Displays the host name of the device.

Username Displays the user name of the DDNS account.

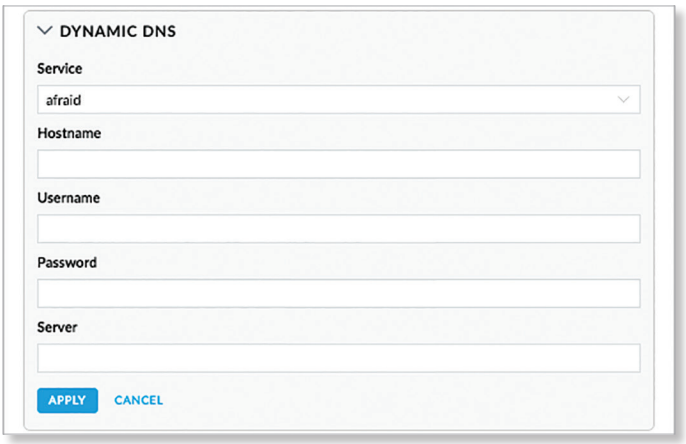
Password Displays the password of the DDNS account.

Server Displays the address of your DDNS server.

Actions Click a button to perform the desired action:

- **Edit** Click to edit the DDNS entry.
- **Delete** Click to delete the DDNS entry.

Create or Edit DDNS Entry



Service If available, select your DDNS service provider from the drop-down list.

Hostname Enter the host name of the device, which has to be updated on the DDNS server. For example: *sample.ddns.com*

Username Enter the user name of the DDNS account.

Password Enter the password of the DDNS account.

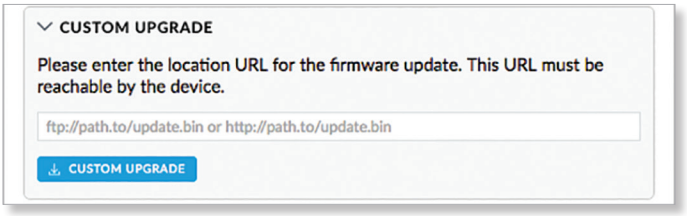
Server Enter the address of your DDNS server.

Apply Click **Apply** to save changes.

Cancel Click *Cancel* to discard changes.

Custom Upgrade

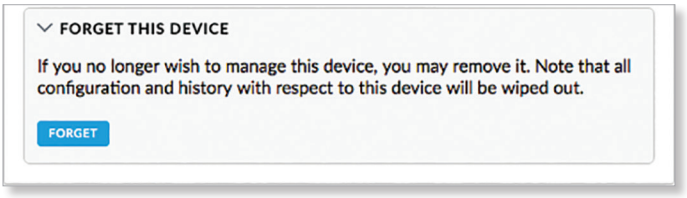
For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, select this option.



(URL) Enter the location URL of the firmware.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Forget This Device



Forget Click **Forget** to remove the Gateway from management by the UniFi Controller software and reset it to factory default settings.

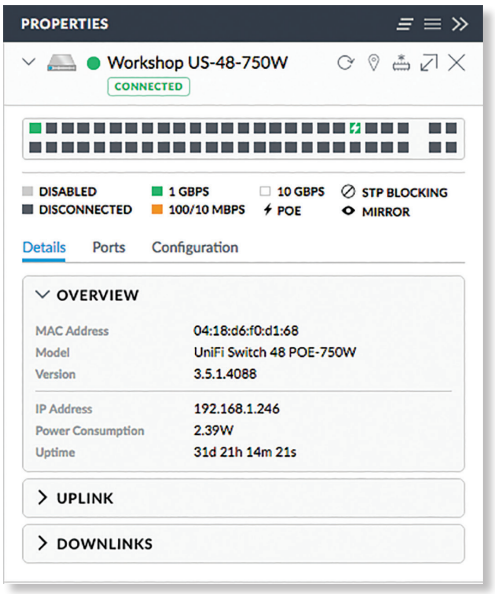
Note: Use caution when clicking *Forget*. This will restore the Gateway to factory default settings while it is in a *Connected* state.

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.

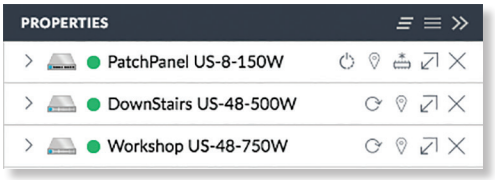
Properties

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:

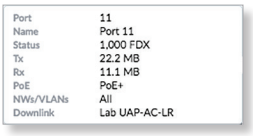
- **Display** Click to display the device information.
- **(icon)** Displays the icon of the device (the icon will vary depending on the model).
- **(status)** Displays to indicate the device status.
  - **Pending Approval** A solid orange circle indicates the default state, available for adoption.
  - **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.

- **Networks/VLANs** Displays the networks/VLANs that the port belongs to.
- **Uplink/Downlink** Displays the name of the uplink or downlink device.

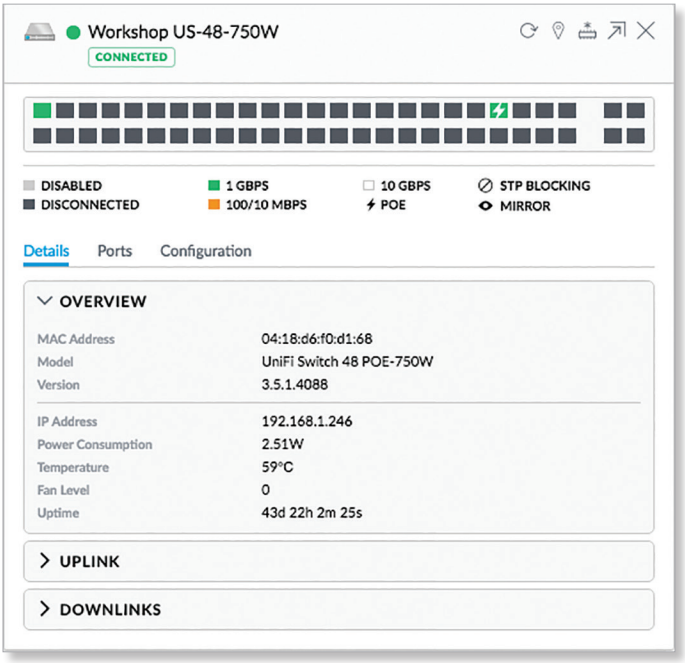
There are three clickable tabs:

- **"UniFi Switch – Details" on page 94**
- **"UniFi Switch – Ports" on page 95**
- **"UniFi Switch – Configuration" on page 98**

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.

IP Address Displays the IP address of the Switch.

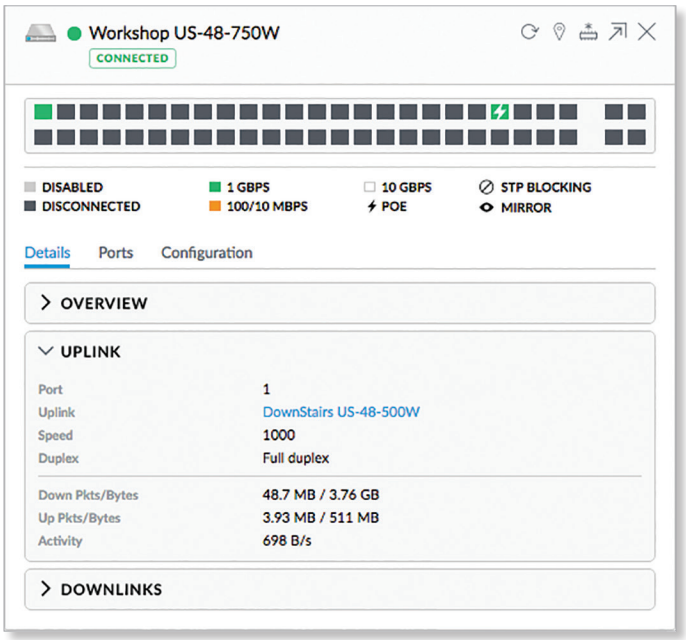
Power Consumption Displays the amount of power used by the Switch.

Temperature Displays the general temperature of the Switch.

Fan Level If the Switch has a fan, then the *Fan Level*, from *0* to *3*, 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.

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.

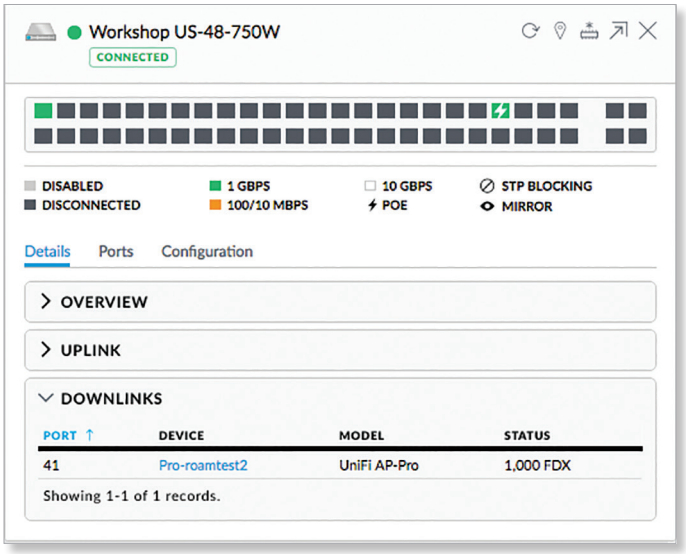
Duplex Displays the mode, *Full Duplex* or *Half Duplex*.

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.

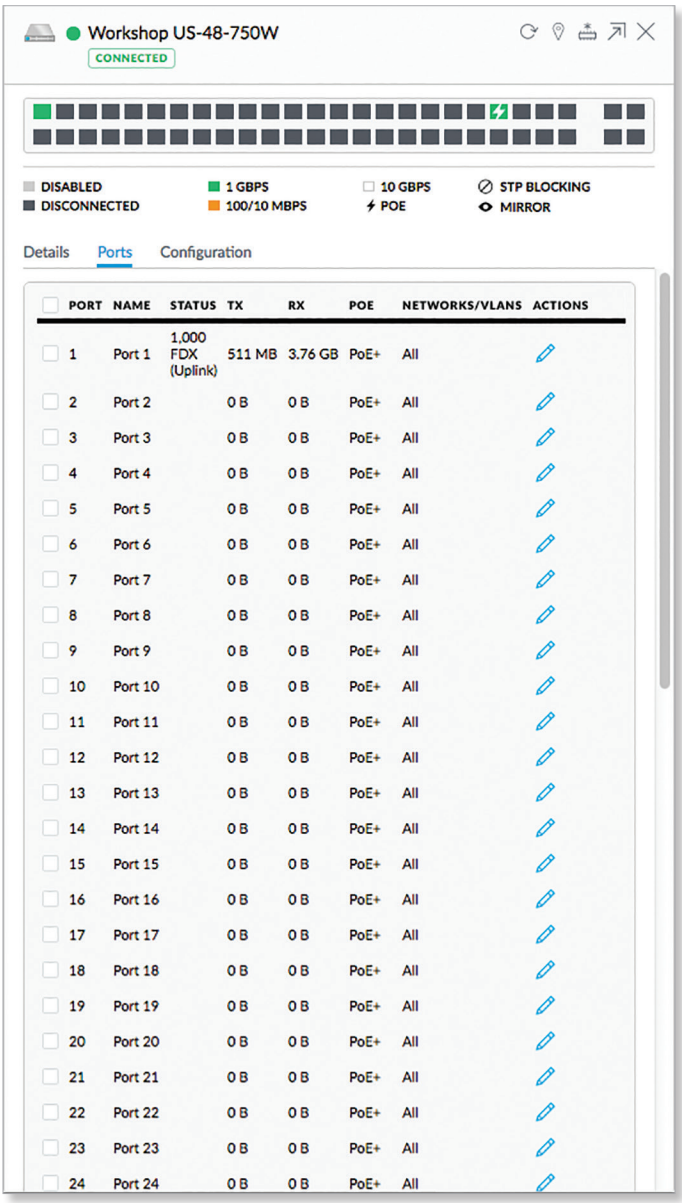
Device Displays the name or MAC address of the downlink device. You can click the name to get additional details.

Model Displays the model number of the downlink device.

Status Displays the connection speed and duplex mode.

UniFi Switch – Ports

Click **Ports** to display the port name, status, TX and RX throughput, PoE setting, and networks/VLANs.



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 Displays the PoE setting:

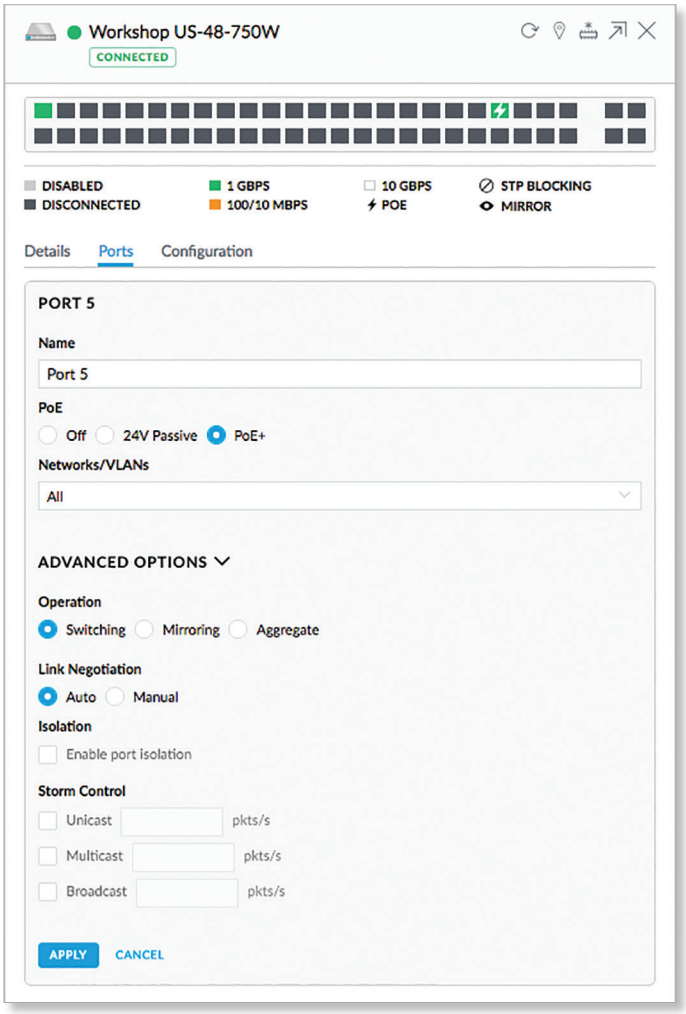
- **Off** PoE is disabled.
- **24V Passive** 24V passive PoE is enabled.
- **__W** Power output is displayed in watts.
- **PoE+** 802.3at/af devices can be plugged in and automatically receive PoE.

Networks/VLANs Displays the networks/VLANs that the port belongs to.

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.

Port Configuration

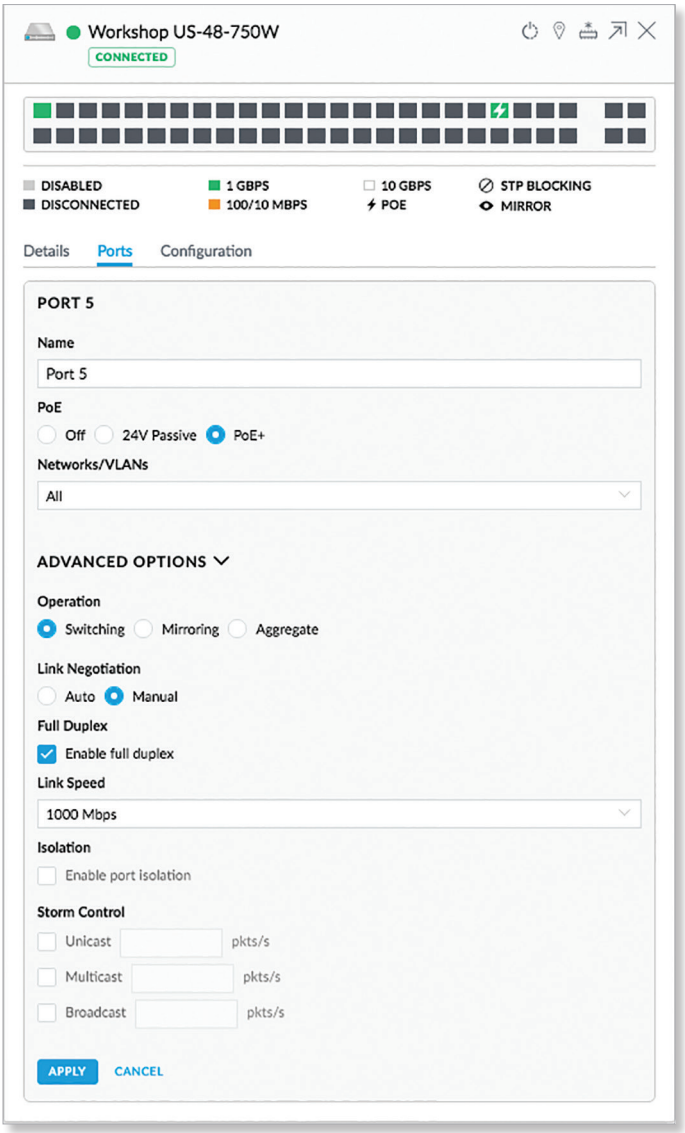


- **Port** Displays the number of the port.
- **Name** Displays the customizable name or identifier of the port.

- **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.
- **Networks/VLANs** Select the appropriate network or VLAN, or select *Disabled* to disable this port. The default is *All*.
- **Advanced Options** Click the icon to display additional options.
- **Operation** Select the operation mode for this port. **Switching**, **Mirroring**, or **Aggregate**. Proceed to the appropriate section.

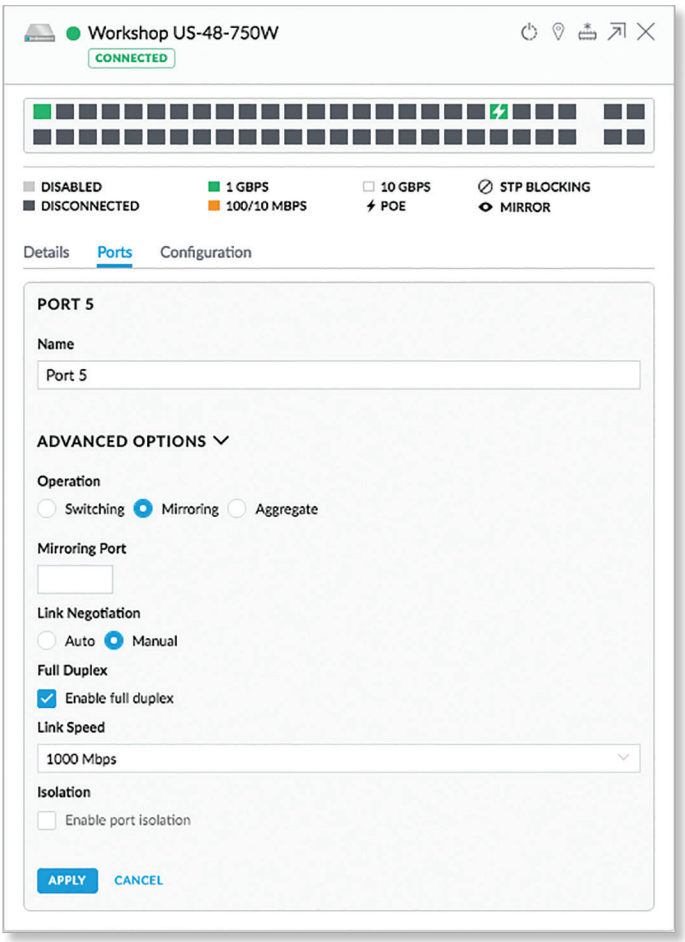
Switching



  - **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.
- **Apply** Click **Apply** to save changes.
- **Cancel** Click *Cancel* to discard changes.

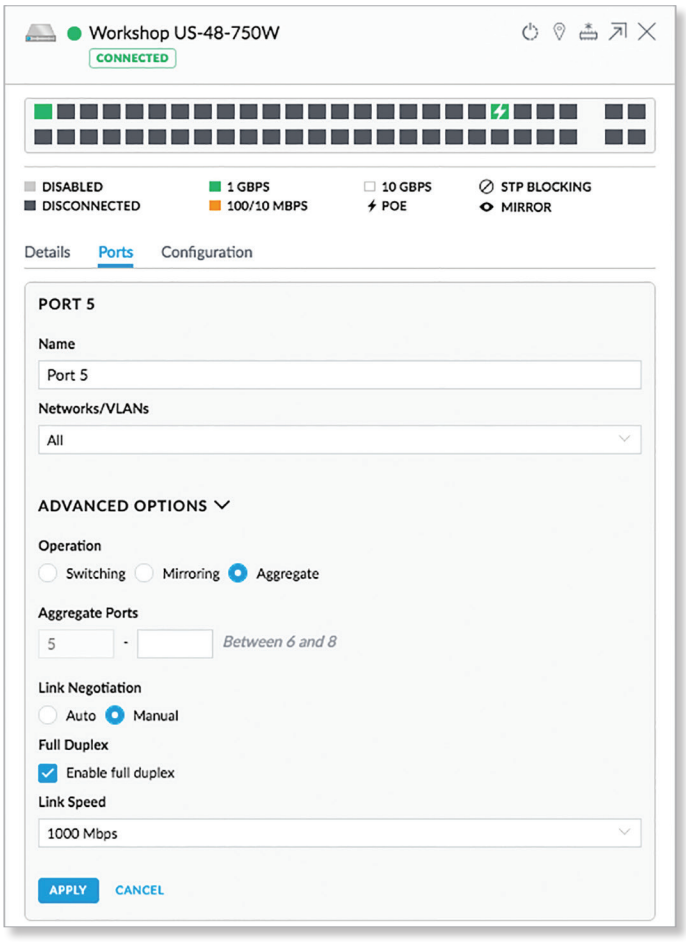
Mirroring



- **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 **Apply** to save changes.
- **Cancel** Click *Cancel* to discard changes.

Aggregate



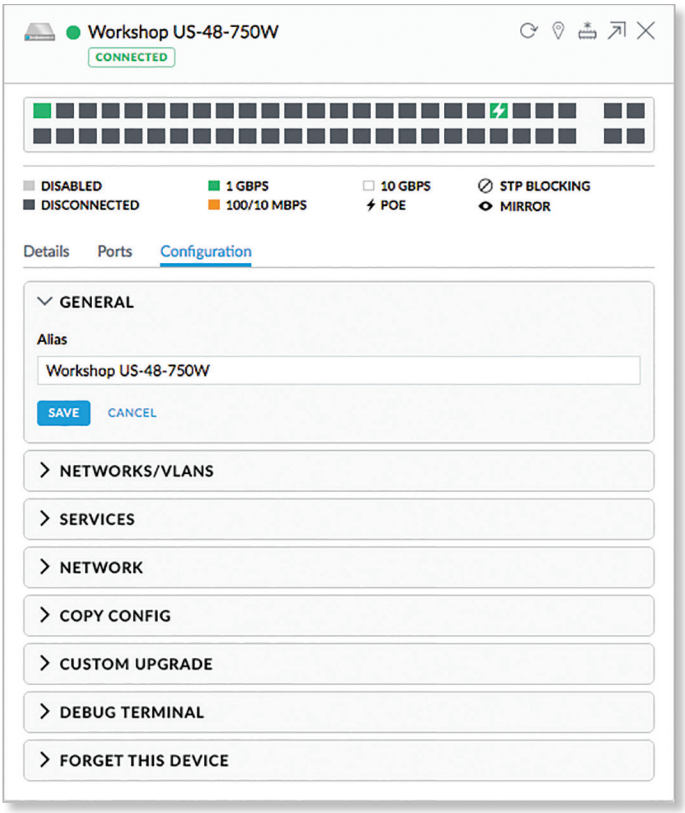
- **Aggregate** A port channel, also known as a Link Aggregation Group (LAG), combines multiple links into a single logical link (single IP address) for load balancing and/or redundancy. If you select this option, then this port becomes the start port of the aggregate link.
  - **Aggregate Ports** Enter 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 need 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 **Apply** to save changes.
- **Cancel** Click *Cancel* 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.

General



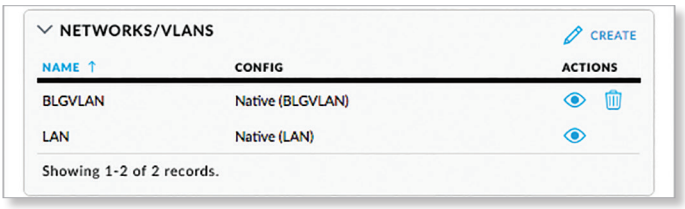
Alias Displays the customizable name or identifier of the Switch. The *Alias* is also known as the host name.

Save Click **Save** to apply your change.

Cancel Click *Cancel* to discard changes.

Networks/VLANs

The *Networks/VLANs* section displays the available VLANs for configuration on this switch, as defined under Settings > Networks. It also displays VLAN groupings that can be managed here, which apply site-wide. VLAN groupings allow creating 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.



Create Click CREATE to add a new entry. Go to the **"Create New Network/VLAN" on page 98** section below.

Name Displays the name of the network/VLAN.

Config Displays the configuration: *Native (____)* or *Customized*. (Networks may be created in **"Settings > Controller" on page 41**.)

Actions Click a button to perform the desired action:

- **View** Click to view the default network.
- **Edit** Click to edit the network/VLAN entry. (Not available for the default network.)
- **Delete** Click to delete the network/VLAN entry. (Not available for the default network.)

Create New Network/VLAN

- **Name** Enter a name to identify this network/VLAN.
- **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 41**.)

- **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:

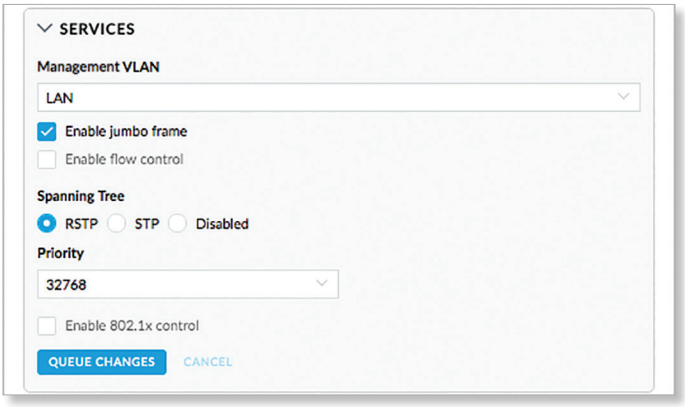
Packet Type	Ingress	Action	Egress
Untagged	Accepted	Assigned to VLAN 1	VLAN header removed and sent out as untagged
Tagged as VLAN 20	Accepted	Remains tagged	Sent out tagged as VLAN 20
Tagged as VLAN 30	Accepted	Remains tagged	Sent out tagged as VLAN 30

  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 41** to create more networks.)

- **Apply** Click **Apply** to save changes.
- **Cancel** Click *Cancel* 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.

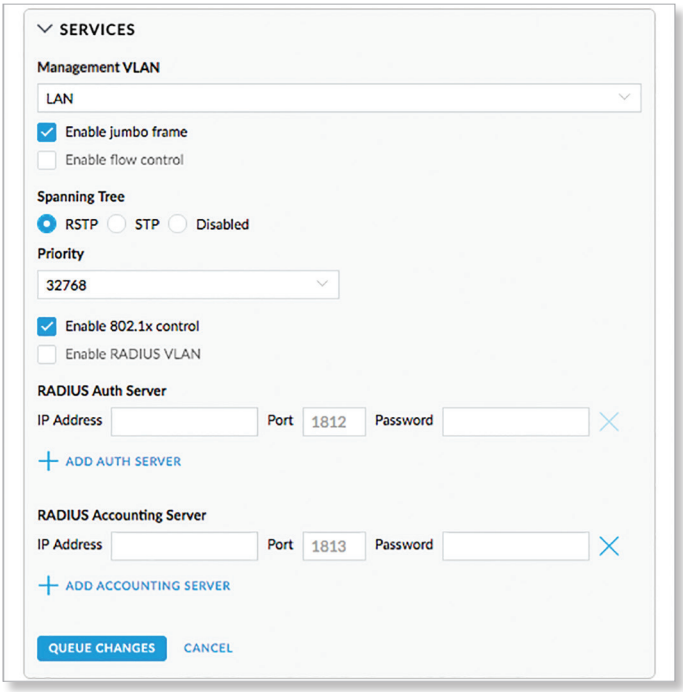
Enable Flow Control Disabled by default. Enabling this option will enable 802.3x Ethernet Flow Control on all ports of this switch. This should remain disabled, unless you have a specific requirement for 802.3x and understand its implications.

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.

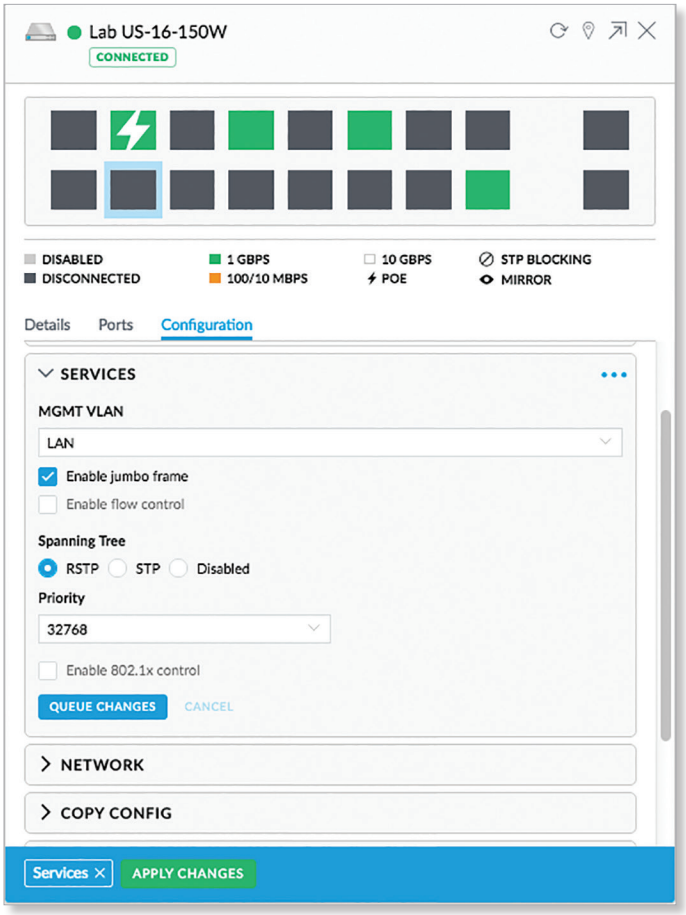


- **Enable RADIUS VLAN** Allows the RADIUS server to dynamically assign a VLAN to a wired client.
- **RADIUS Auth Server** Provide the following information about the RADIUS authentication server:
  - **IP Address** Enter the IP address.
  - **Port** Enter the port number. The default is *1812*.
  - **Password** Enter the password.
  - **Delete** Click the *delete* icon to remove this accounting server.
  - **Add Auth Server** If you have another authentication server, click this option and complete the *IP Address*, *Port*, and *Password* fields.
- **RADIUS Accounting Server** Provide the following information about the RADIUS server:
  - **IP Address** Enter the IP address.
  - **Port** Enter the port number. The default is *1813*.
  - **Password** Enter the password.
  - **Delete** Click the *delete* icon to remove this accounting server.
  - **Add Accounting Server** If you have another accounting server, click this option and complete the *IP Address*, *Port*, and *Password* fields.

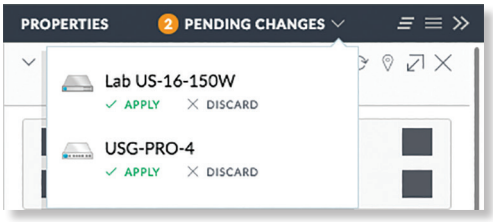
Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section 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 queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click to display the devices.

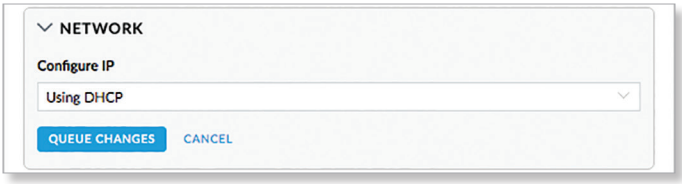


- **Apply** Click APPLY to save changes.
- **Discard** Click DISCARD to cancel changes.

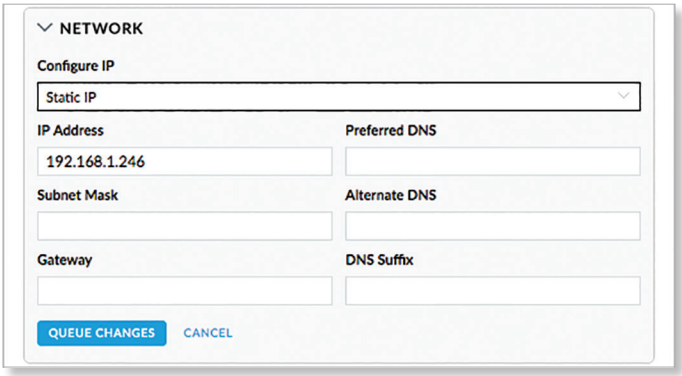
Network

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.)

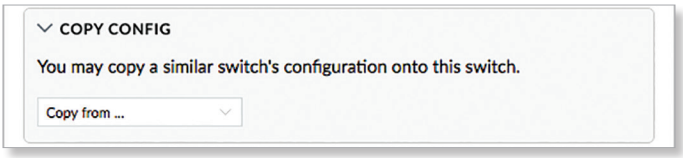
Cancel Click *Cancel* to discard changes.

Pending Changes If you want 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.

Copy Config

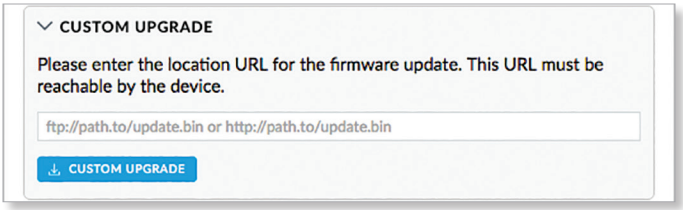
If you have settings that you want to apply to multiple Switches, use this option to copy the configuration.



Copy from Select the appropriate Switch whose configuration will be copied to this Switch. Then click **Confirm** 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.

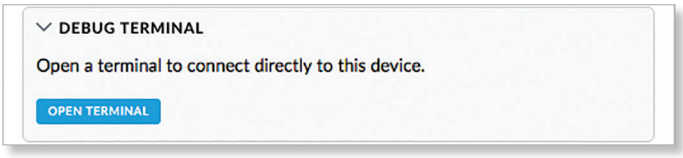


(location URL) Enter the UL of the firmware's location.

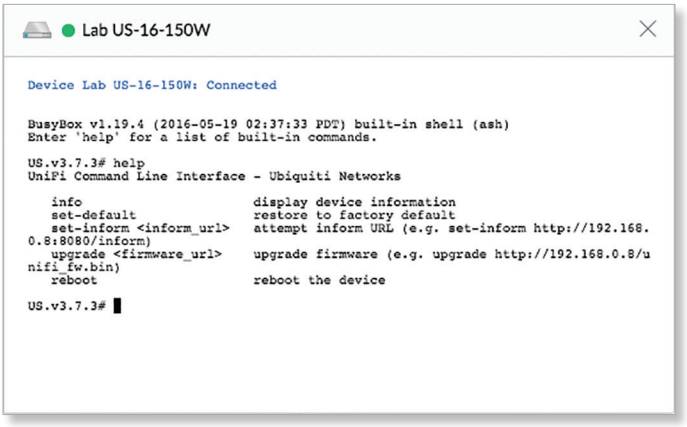
Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Debug Terminal

This option uses a WebRTC connection as transport layer. To use a command-line interface, click **Open Terminal**.

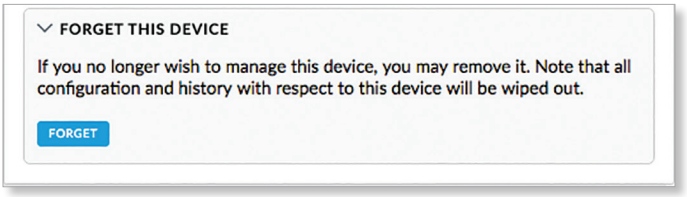


Open Terminal Click **Open Terminal** to connect directly to this Switch. A new window will appear.



- **help** Enter **help** at the command line for a list of built-in commands.

Forget This Switch



Forget Click **Forget** to remove the Switch from management by the UniFi Controller software and reset it to factory default settings.

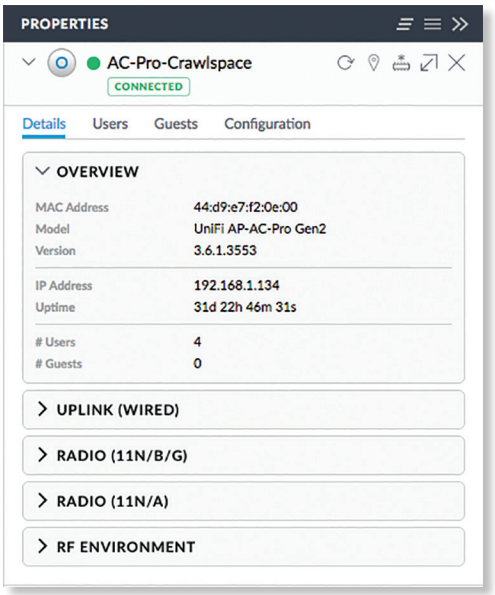
Note: Use caution when clicking *Forget*. This will restore the Switch to factory default settings when it is in a *Connected* state.

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.

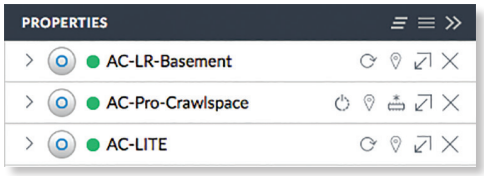
Properties

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.

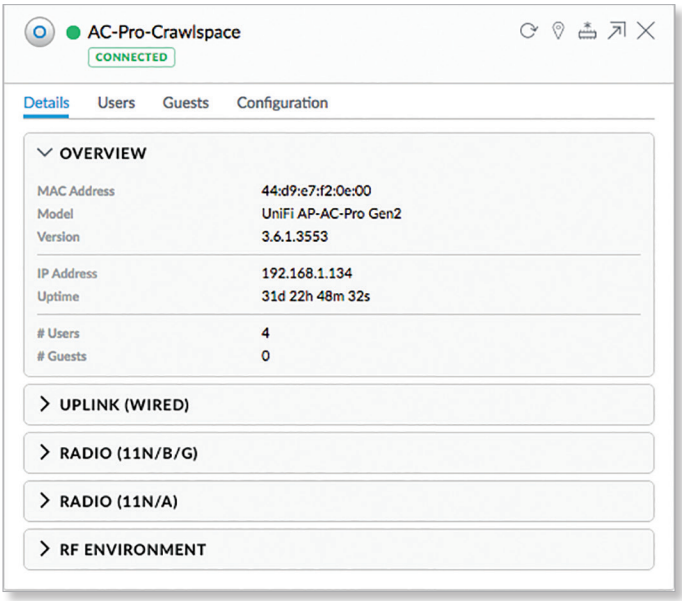
There are four clickable tabs:

- **"UniFi Access Point – Details" on page 104**
- **"UniFi Access Point – Users" on page 107**
- **"UniFi Access Point – Guests" on page 108**
- **"UniFi Access Point – Configuration" on page 108**

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.

IP Address Displays the IP address of the AP.

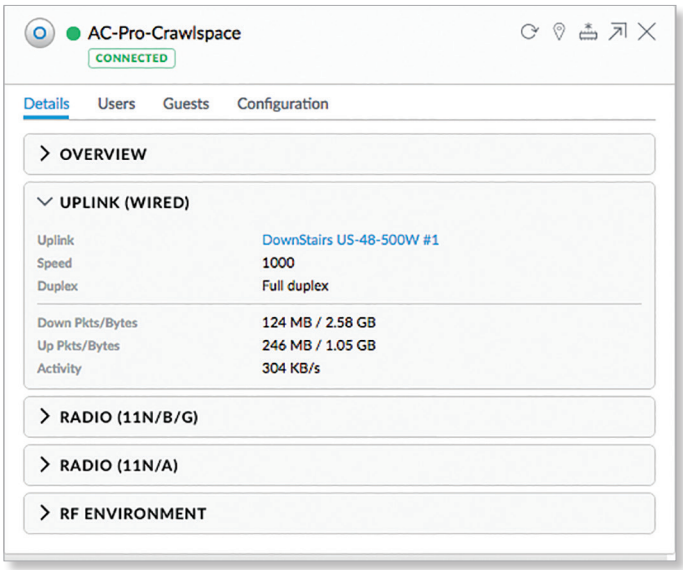
Uptime Displays the duration of time the AP has been running without interruption.

 # 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*.

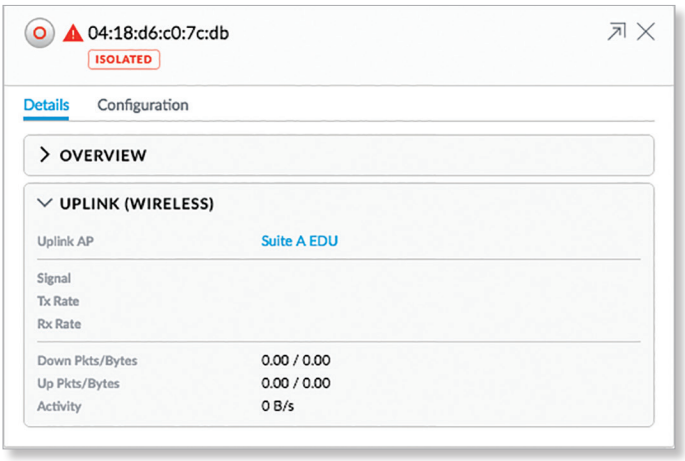
Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

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.

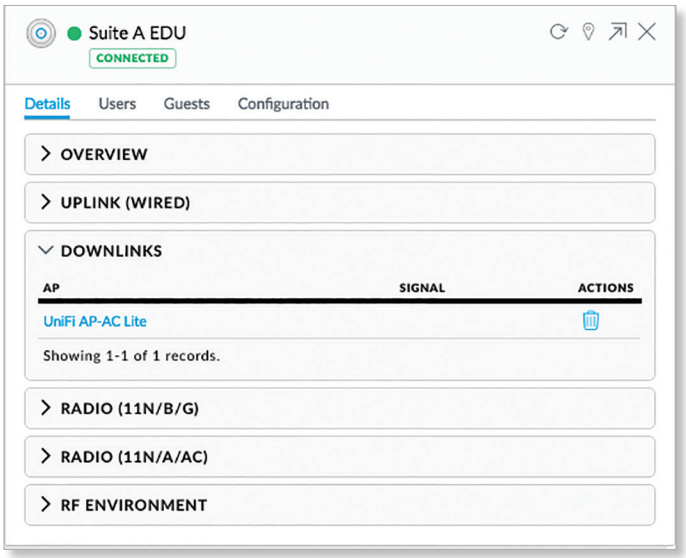
Down Pkts/Bytes Displays the amount of data downloaded as packets and bytes.

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.

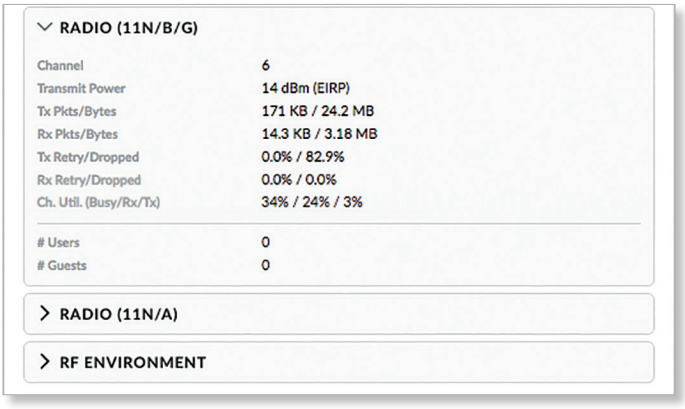
Signal Displays the percentage of signal strength between the two APs.

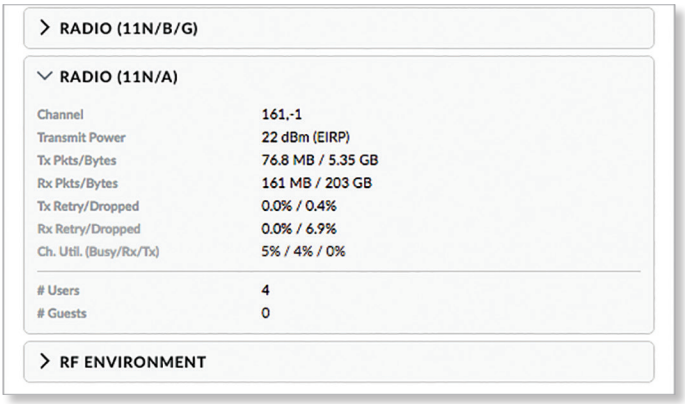
Actions Click a button to perform the desired action:

- **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.

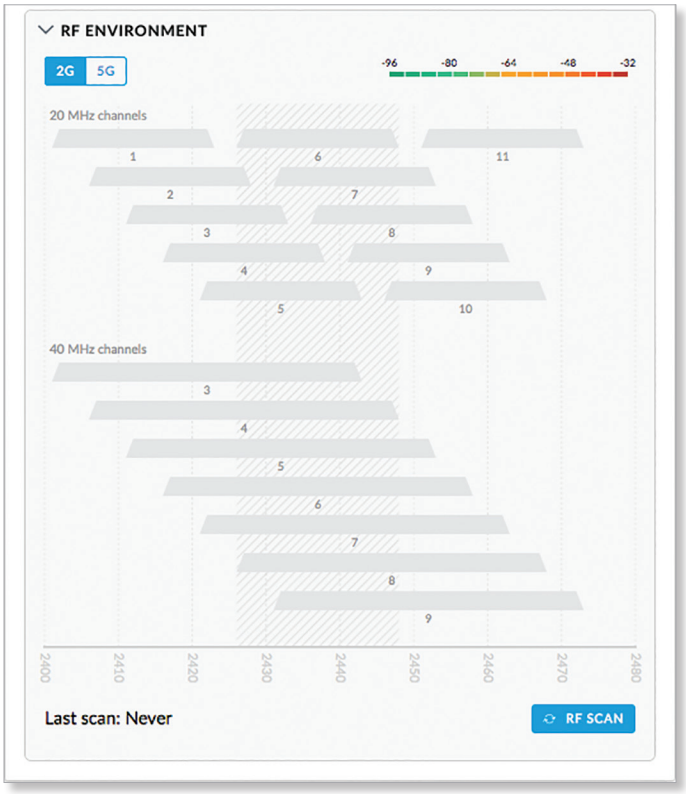
 # Users Displays the number of users connected to the primary network.

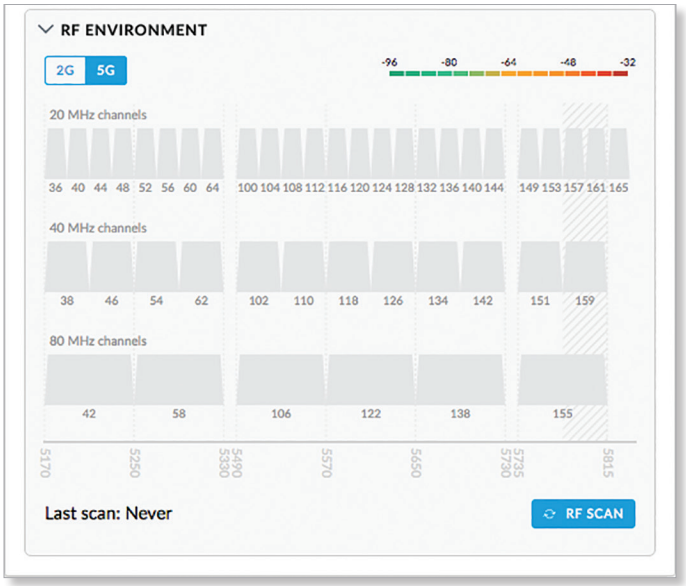
 # Guests Displays the number of guests connected to the guest network.

RF Environment

Note: Only the UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU support spectral analysis.

Click **RF Environment** for spectral analysis to help in channel selection and planning.

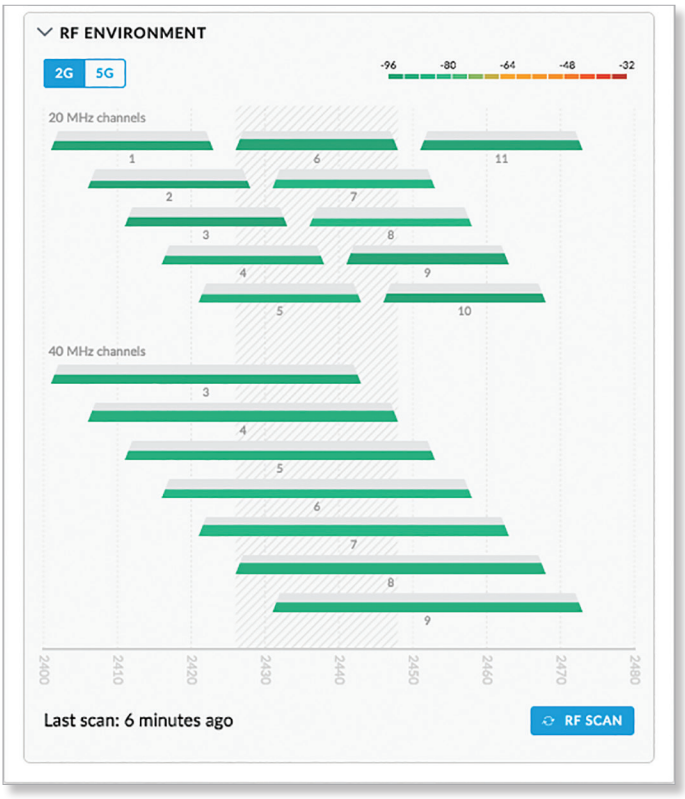




2G/5G Select the frequency band you want to analyze.

RF Scan Click RF 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 represent a channel option and its color-coded level of interference (from green at -96 dBm to red at -32 dBm).

__ **MHz** 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, and 80 MHz.

__ Displays the corresponding channel number for each channel width option.

(outlined) The current channel is outlined.

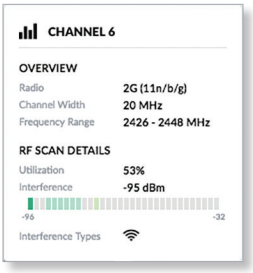
Place your cursor over a channel option to view the following:

Overview

- **Radio** Displays the radio being used.
- **Channel Width** Displays the width of the channel.
- **Frequency Range** Displays the range of frequencies.

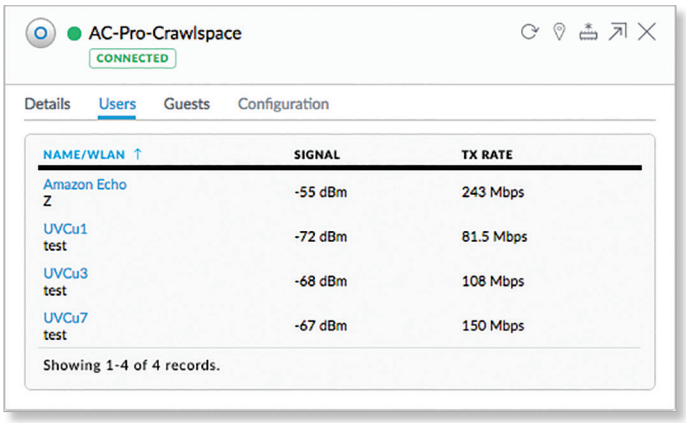
RF Scan Details

- **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.

UniFi Access Point – Users



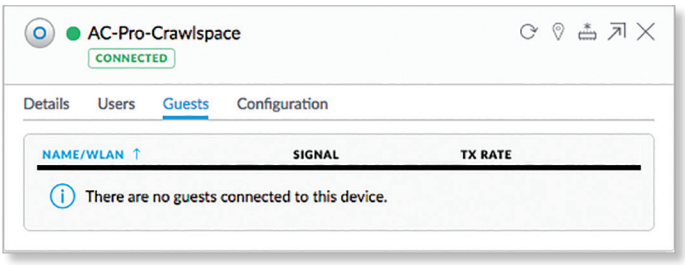
(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Name 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 117** 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 117** for more information.

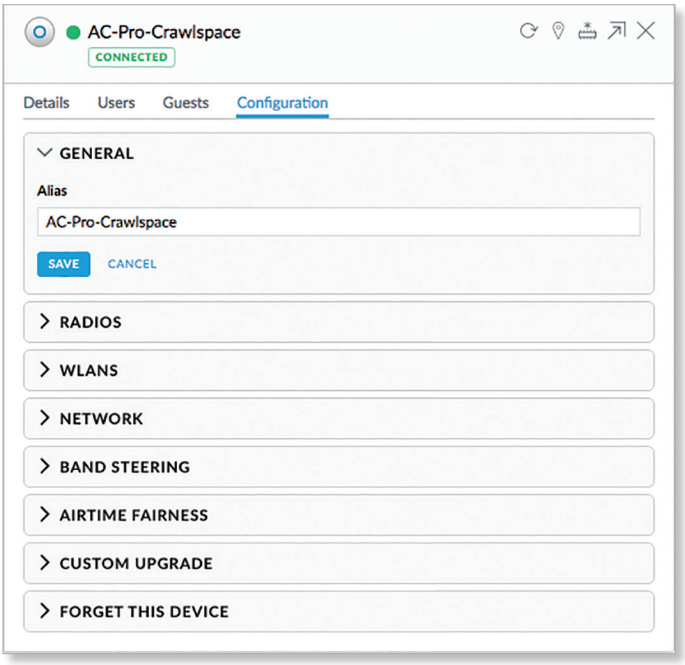
Signal Displays the signal strength between the guest and AP.

TX Rate Displays the transmit rate.

UniFi Access Point – Configuration

Change device configuration settings.

General

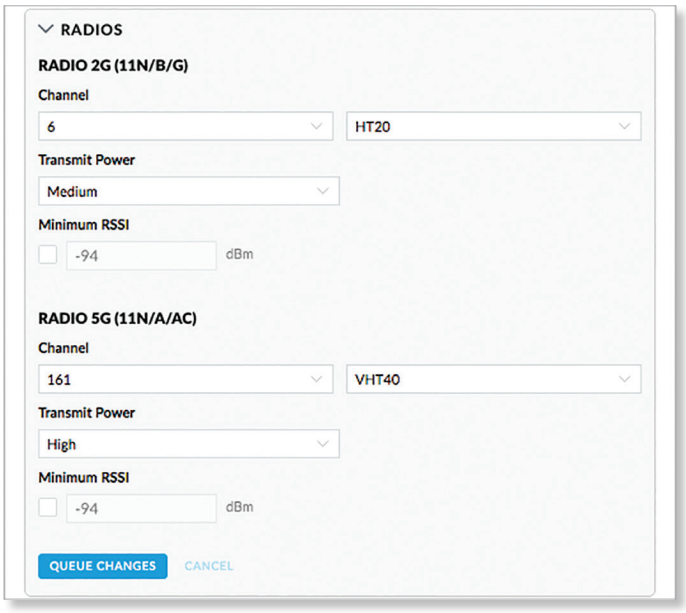


Alias Enter or edit the customizable name or identifier of the AP. The *Alias* is also known as the host name.

Save Click **Save** to apply the change.

Cancel Click *Cancel* to discard changes.

Radios



Channel Select the appropriate settings:

- **Auto/(channel number)** Select a channel number or keep the default, *Auto*.
- **HT20/HT40/HT80** (Available for 2.4 GHz only.) Select **HT20** for 20 MHz operation, **HT40** for 40 MHz operation, or **HT80** 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.

- **VHT20/VHT40/VHT80** (Available for 5 GHz only.) Select V**HT20** for 20 MHz operation, V**HT40** for 40 MHz operation, or V**HT80** 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.

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 Outdoor models) Specify the antenna gain.

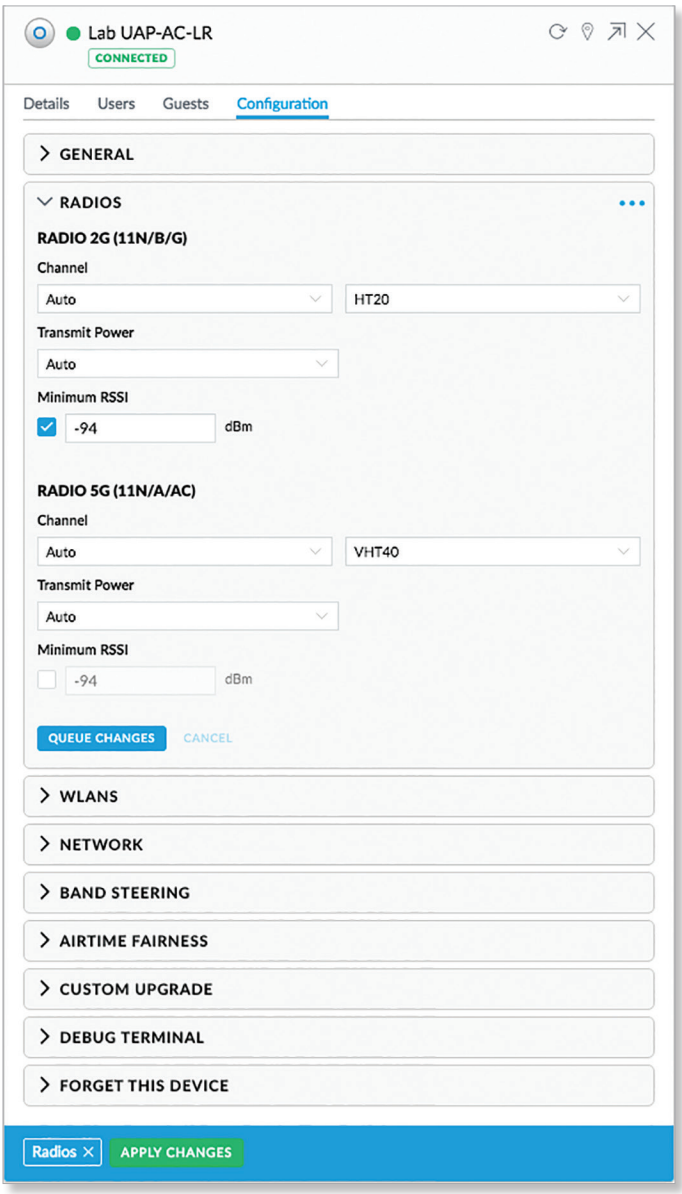
Minimum RSSI Disabled by default. Select this option and enter a minimum threshold (we recommend a value in this range: -70 to -90 dBm). For UniFi, RSSI is synonymous with SNR. If the client signal falls below the specified threshold, then the AP kicks out the client, allowing it to reconnect with a more suitable AP.

Note: If the AP is part of a Zero Handoff WLAN Group, the *Minimum RSSI* setting cannot be changed.

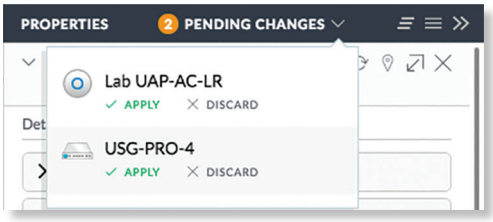
Queue Changes Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section 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.



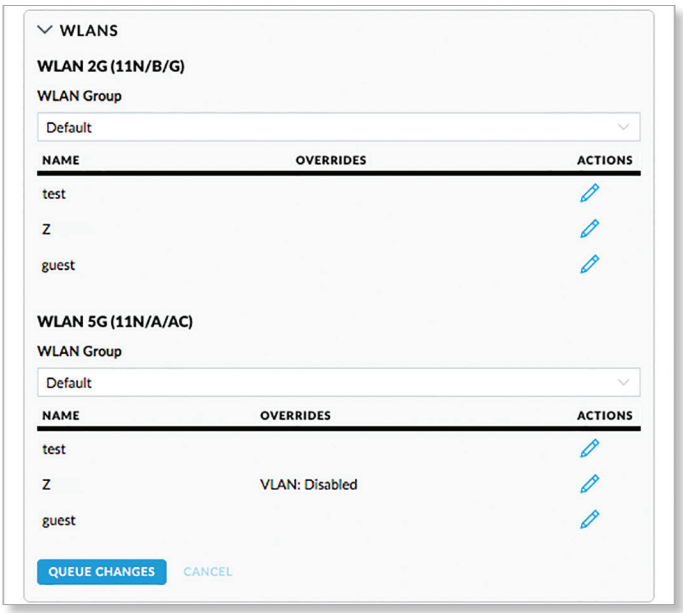
Pending Changes If you want queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click ⌄ to display the devices.



- **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:

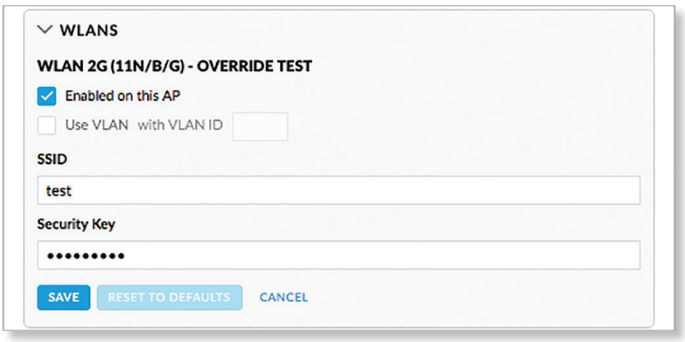
- **Edit** Click ✎ to enable a VLAN (Virtual Local Area Network), set the VLAN ID, and enter the SSID override name to apply to the wireless network.

  Note: The *Override* option is not available for a Zero Handoff WLAN Group.

Queue Changes Click **Queue Changes** to save changes.

Cancel Click *Cancel* 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:

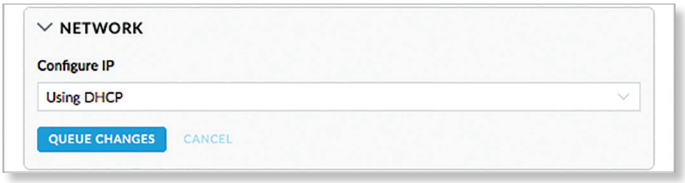
- **Save** Click **Save** to apply changes.
- **Reset to Defaults** Click **Reset to Defaults** to remove any overrides that were applied to the selected wireless network.
- **Cancel** Click *Cancel* to discard changes.

Network

Configure IP Select the Internet connection type for your service, **Using DHCP** or **Static IP**. Proceed to the appropriate instructions.

Using DHCP

- **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.

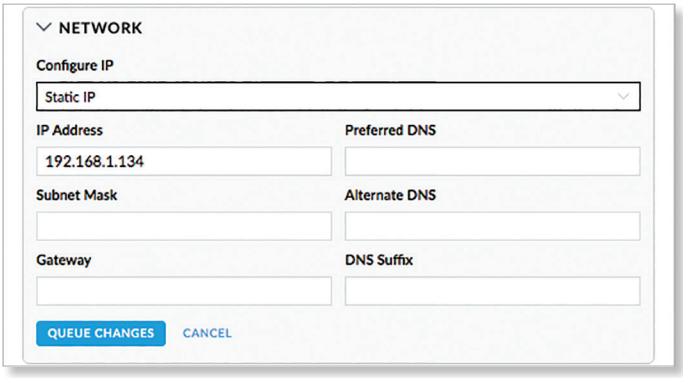


- **Queue Changes** Click **Queue Changes** to line up the changes to take effect. This allows you to make multiple changes to the device and then apply them all at once so that the device doesn't have to re-provision over and over again when you change different sections of the configuration. Each section 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 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.

Static IP

- **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.
- **Queue Changes** Click **Queue Changes** to save changes.
- **Cancel** Click *Cancel* to discard changes.



- **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.
- **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 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

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 the UAP-PRO, UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU models support band steering.

If enabled, the UniFi band steering policy takes two criteria into account:

- channel utilization metrics
- signal quality measurements, including RSSI

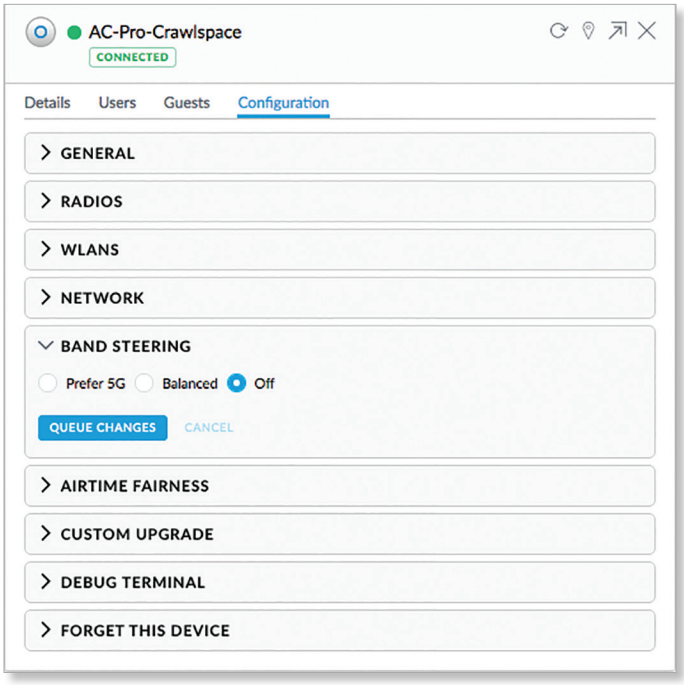
The AP steers the client to the optimal band during association (not after association). If both bands or neither band is overloaded, the AP does not perform band steering; instead, the client chooses a band.

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 *Cancel* to discard changes.

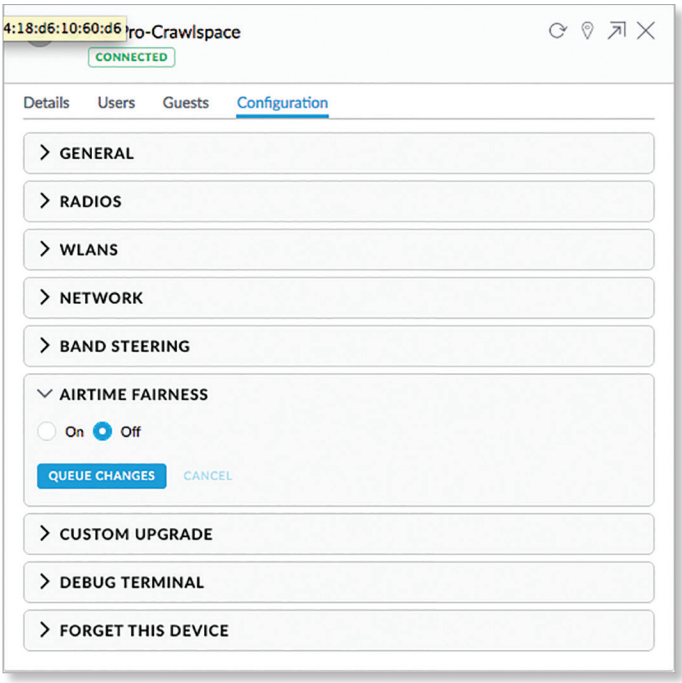
Pending Changes If you want queue changes for multiple devices and then apply them later, the *Pending Changes* option appears in the *Properties* panel. Click to display the devices.

- **Apply** Click APPLY to save changes.
- **Discard** Click DISCARD to cancel changes.

Airtime Fairness

Note: Only the UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU models support airtime fairness.

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.)

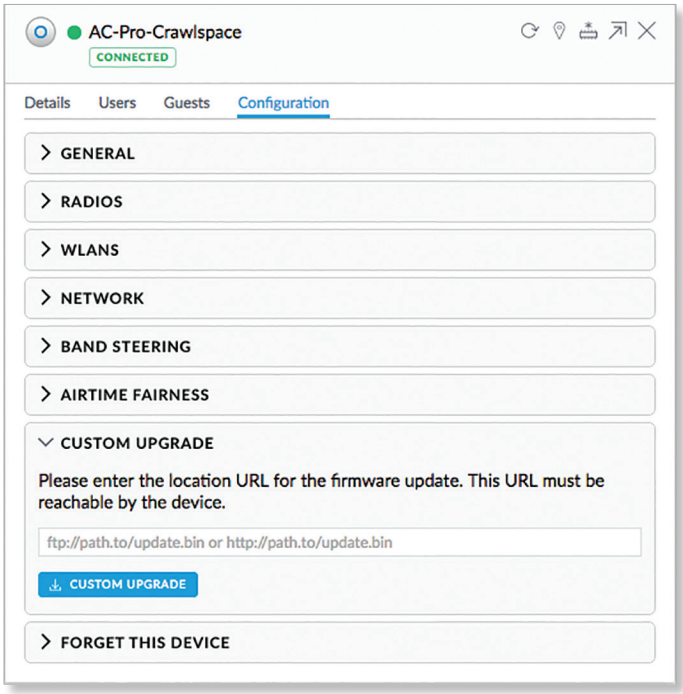
Cancel Click *Cancel* to discard changes.

Pending Changes If you want 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.

Custom Upgrade

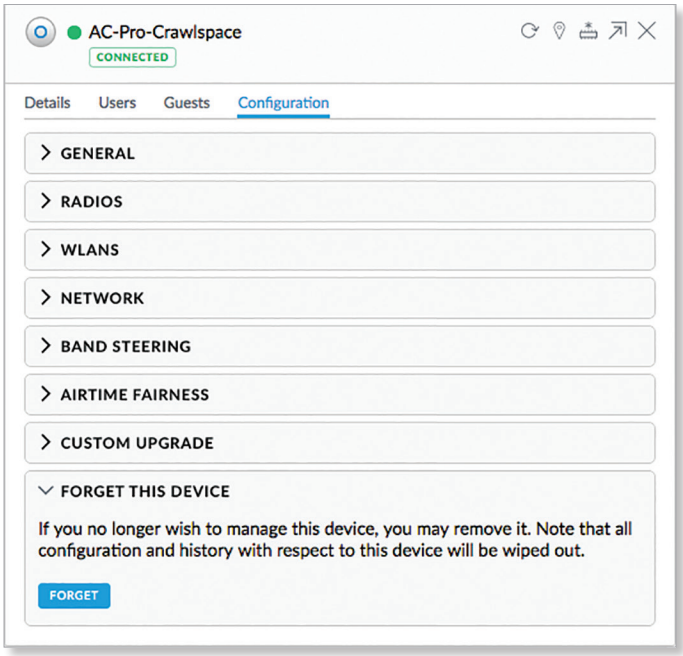
For firmware upgrades, the UniFi devices retrieve the latest firmware from the Ubiquiti website. To specify firmware saved in a custom location, select this option.



(location URL) Enter the UL of the firmware's location.

Custom Upgrade Click CUSTOM UPGRADE to upgrade the firmware from the location you entered.

Forget This AP

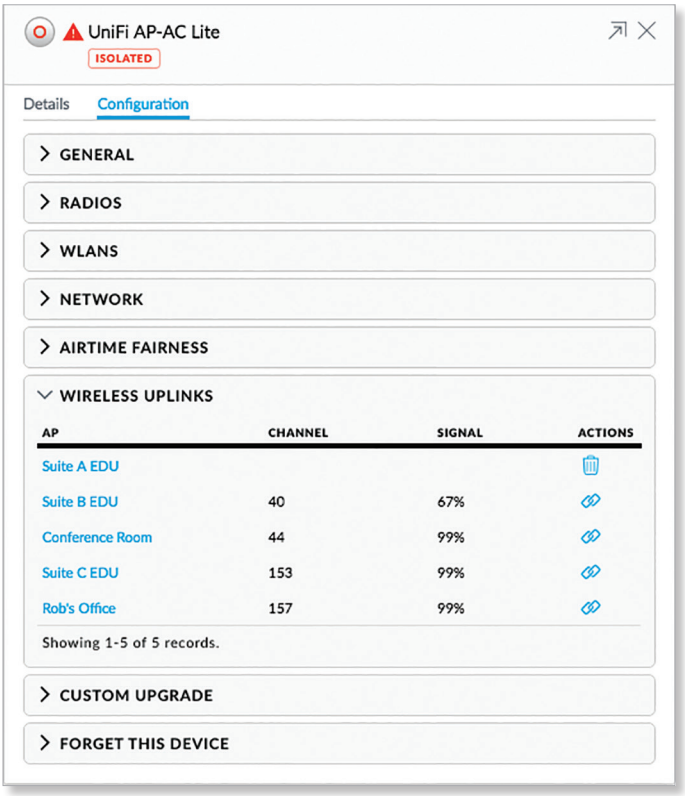


Forget Click **Forget** to remove the AP from management by the UniFi Controller software and reset it to factory default settings.

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:

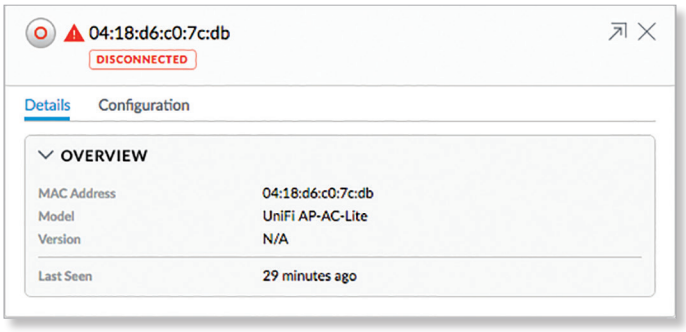
- **Select** Click to connect the wireless AP to the wired AP.
- **Remove** Click to disconnect the wireless AP from the wired AP.

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.

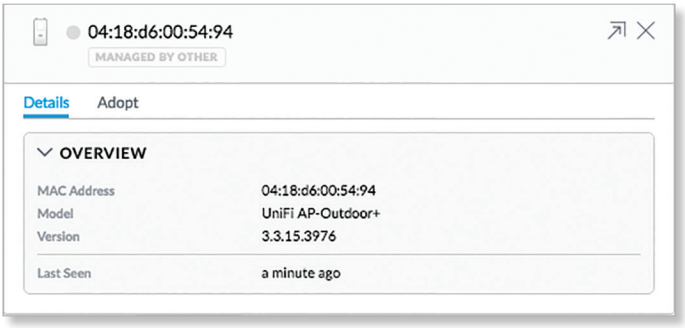
Version Displays the version of software used on the AP.

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



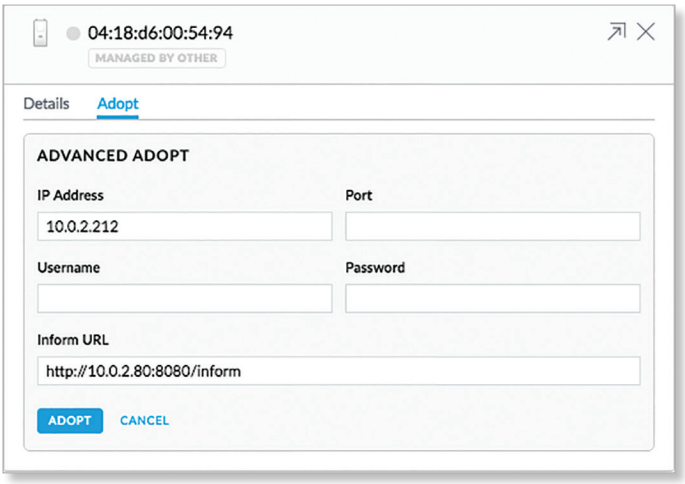
MAC Address Displays the MAC address of the AP.

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 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 20**.

Password Enter the SSH Password for management access. This is the *Device Password* you configured in **"Settings > Site" on page 20**.

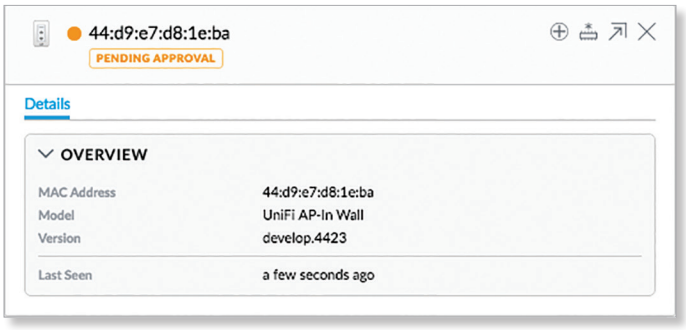
Inform URL This tells the AP where to look for the UniFi Controller. The URL will be automatically displayed but you may need to verify its accuracy as the system may have multiple interfaces.

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.

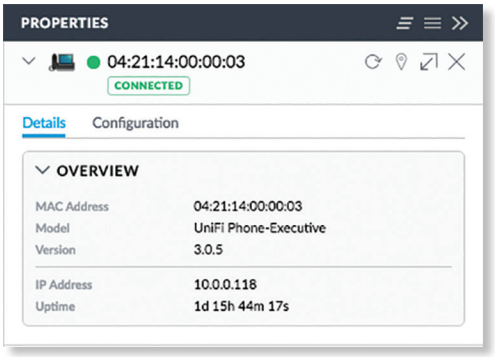
Chapter 13: UniFi VoIP Phone Details

A UniFi VoIP Phone hyperlink opens the UniFi VoIP Phone'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.

Important: For management of the UniFi VoIP Phones, please download the UniFi VoIP Controller here: **downloads.ubnt.com/unifi**

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 ring the Phone and flash the Phone's icon on the *Map* tab so you can locate it. The Phone will ring until you click *Locate* 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.

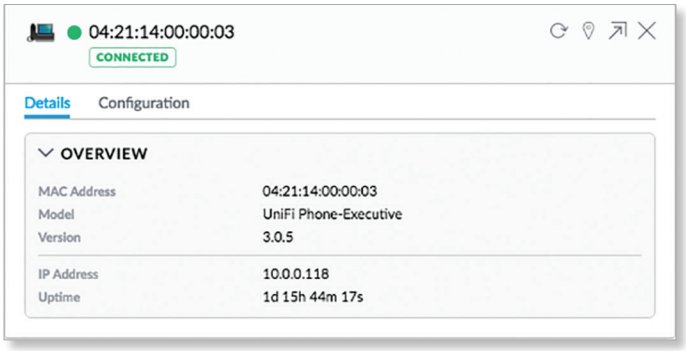
There are two clickable tabs:

- *Details*
- **"UniFi VoIP Phone – Configuration" on page 116**

UniFi VoIP Phone – Details

The *Overview* displays the device specifics and uptime.

Overview



MAC Address Displays the MAC address or unique hardware identifier of the Phone.

Model Displays the model name of the Phone.

Version Displays the version number of the Phone's firmware.

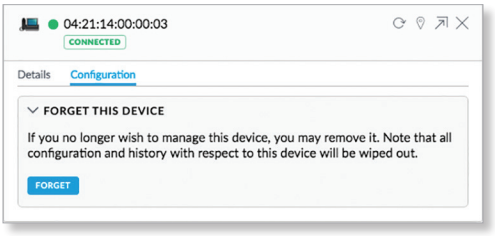
IP Address Displays the IP address of the Phone.

Uptime Displays the duration of time the Phone has been running without interruption.

UniFi VoIP Phone – Configuration

Click **Configuration** to reset the Phone to its factory default settings.

Forget This Phone



Forget Click **Forget** to remove the Phone from management by the UniFi Controller software and reset it to factory default settings.

Note: Use caution when clicking *Forget*. This will restore the Phone to factory default settings when it is in a *Connected* state.

Chapter 14: Client Details

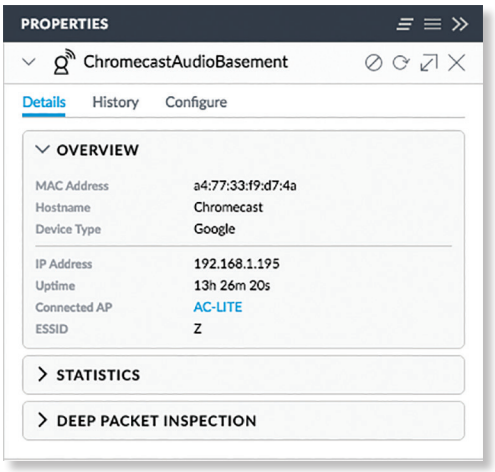
A client hyperlink opens the client's *Details* window either in the *Properties* panel or as a separate popup window. You can always dock this window in the *Properties* panel or detach it as a separate window.

The top of the window displays the device icon and name (or MAC address).

Properties

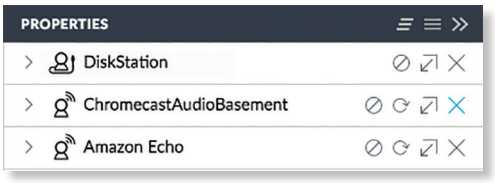
The *Properties* panel appears on the right side of the screen. Information about each selected device appears as a popup within this panel. The information varies depending on whether the client is wired or wireless:

- *Wireless Client – Details*
- **"Wired Client – Details" on page 119**



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:

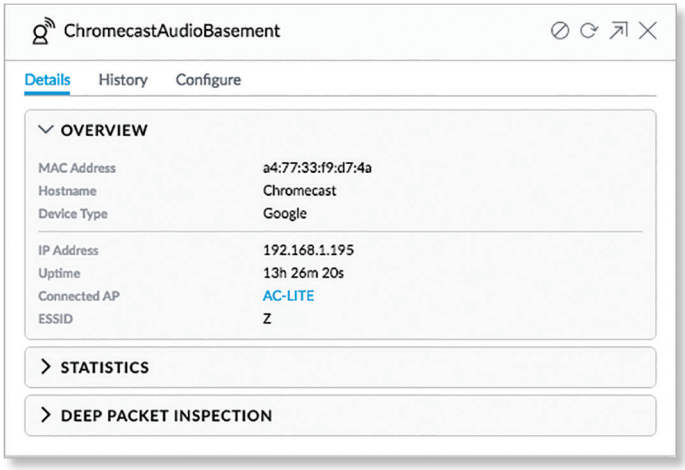
- **Display** Click to display the device information.
- **(icon)** Displays the icon of a wireless or wired device.
- **Name/MAC Address** Displays the hostname, alias, or MAC address of the device.
- **Block** Click to block this client from accessing the network.
- **Reconnect** Click to reconnect a wireless client. You can click o 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 four clickable tabs:

- *Details*
- *Statistics*
- *History*
- *Configuration*

Wireless 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 IP address of the client.

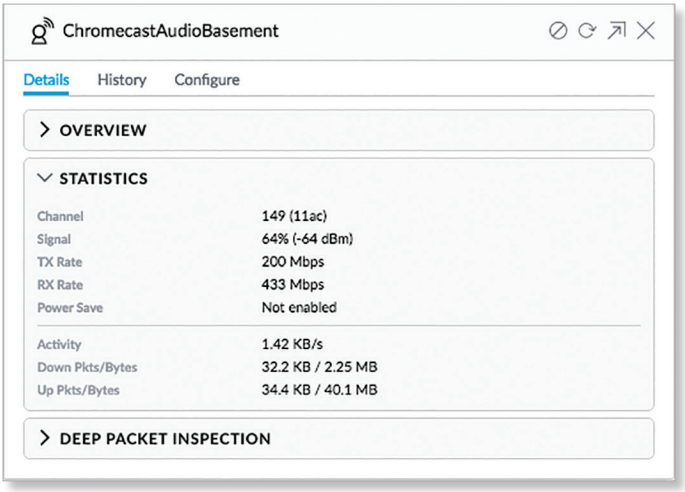
Uptime Displays the duration of time the client has been connected.

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 103** for more information.

ESSID Displays the name of the wireless network.

Wireless Client – Statistics

Overview



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.

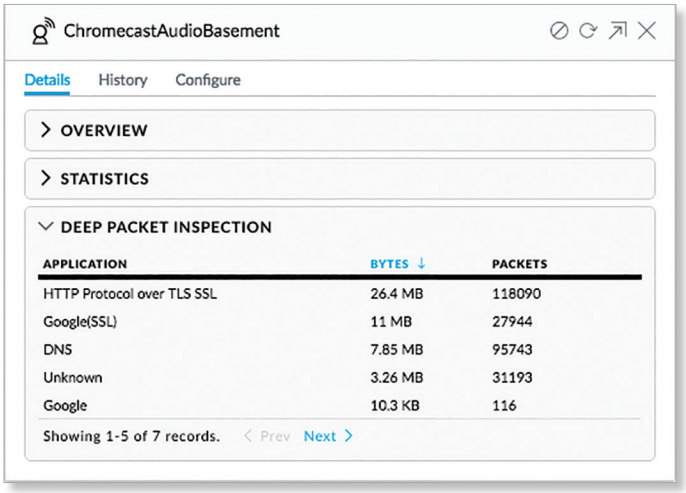
Activity Displays the level of activity in Bytes per second.

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 20** for more information).



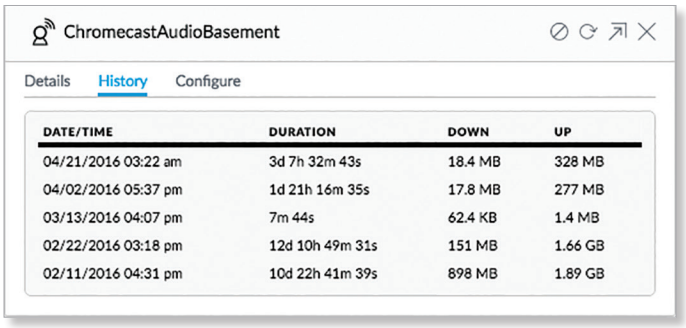
(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

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.

Wireless Client – History



Date/Time Displays the date and time of the connection.

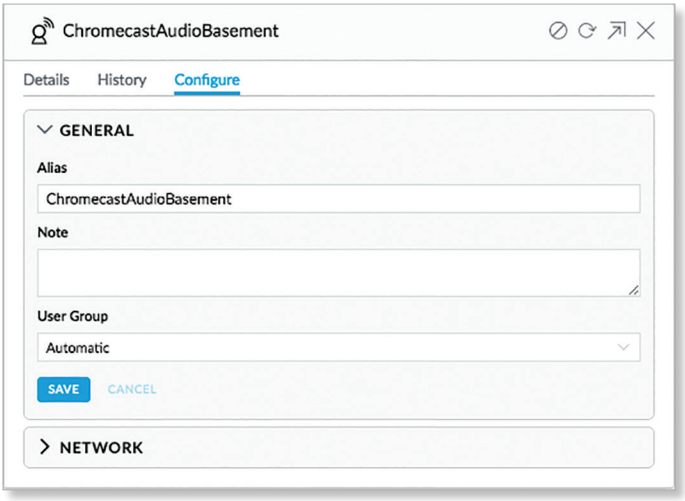
Duration Displays the duration of the connection.

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

Config



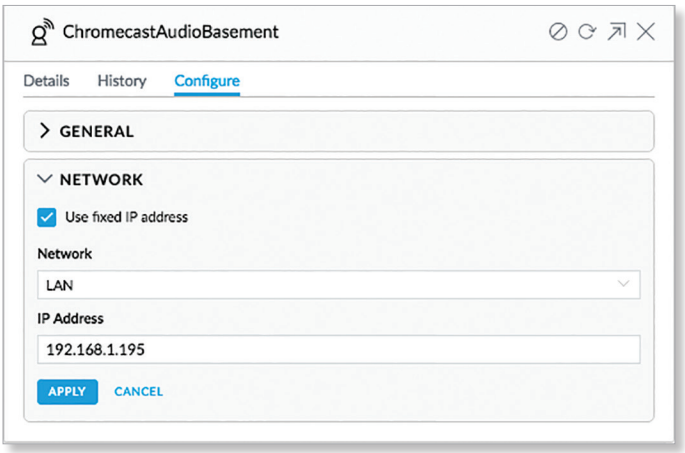
Alias Allows you to change the hostname of the client.

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 40** for more information). The default *User Group* is *Automatic*.

Save Click **Save** to apply changes.

IP Config

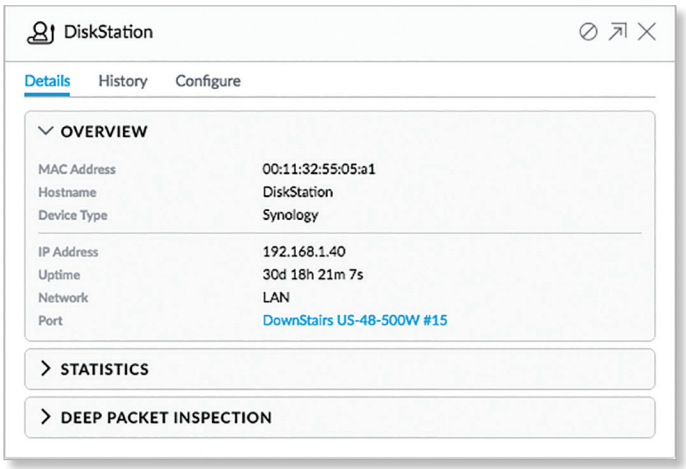


Fixed IP Select this option to assign a static IP address to the client, and configure the settings below. If you want the local DHCP server to assign an IP address to the client, remove the checkmark.

- **Network** Select the appropriate network from the drop-down list.
- **IP Address** Enter the local IP address.

Apply Click **Apply** to save 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.

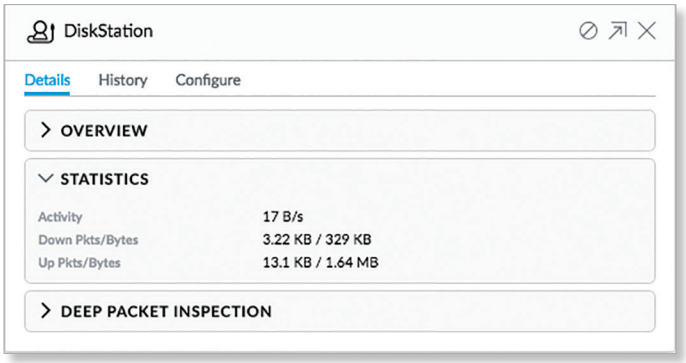
Uptime Displays the duration of time the client has been connected.

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



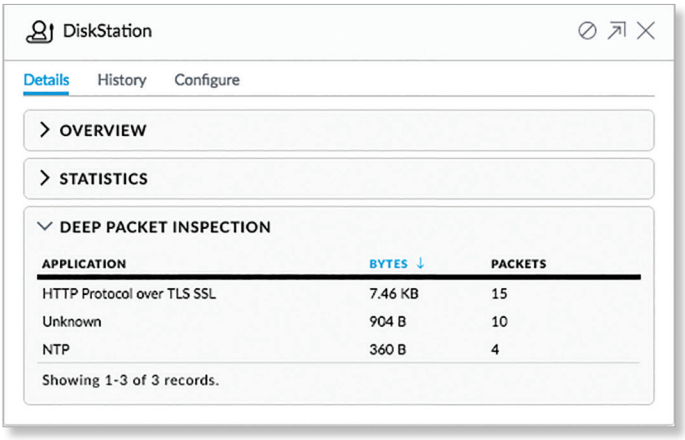
Activity Displays the level of activity in Bytes per second.

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 20** for more information).



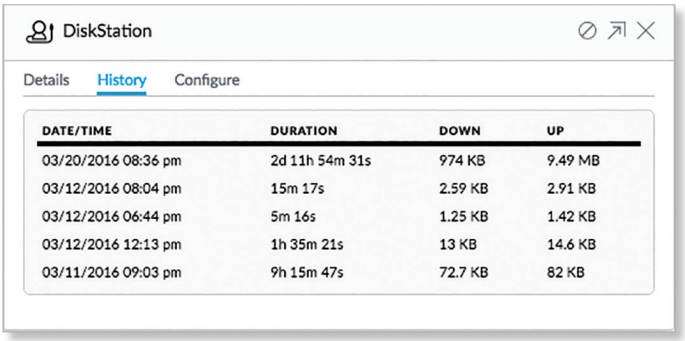
(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

Application Displays the name of the application.

Packets Displays the amount of data uploaded and downloaded as packets.

Bytes Displays the amount of data uploaded and downloaded as bytes.

Wired Client – History



Date/Time Displays the date and time of the connection.

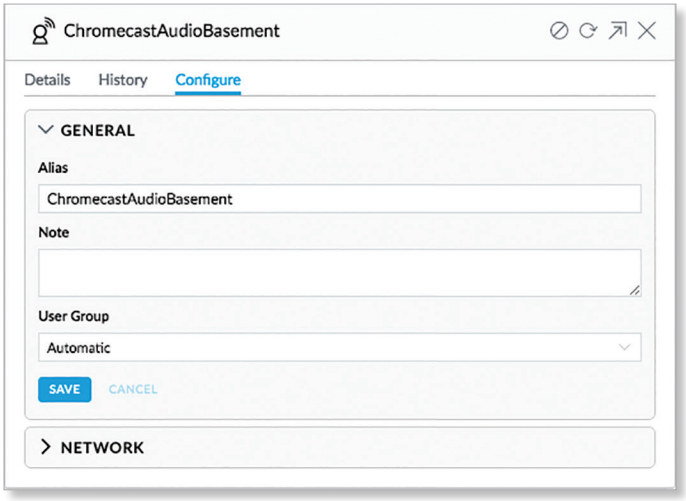
Duration Displays the duration of the connection.

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



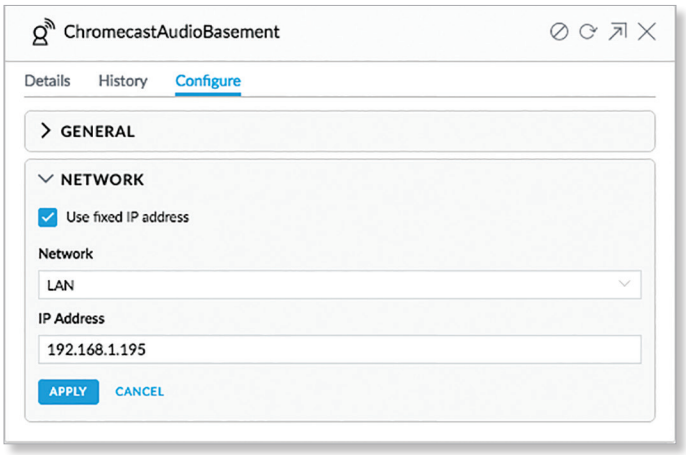
Alias Allows you to change the hostname of the client.

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 40** for more information). The default *User Group* is *Automatic*.

Save Click **Save** to apply changes.

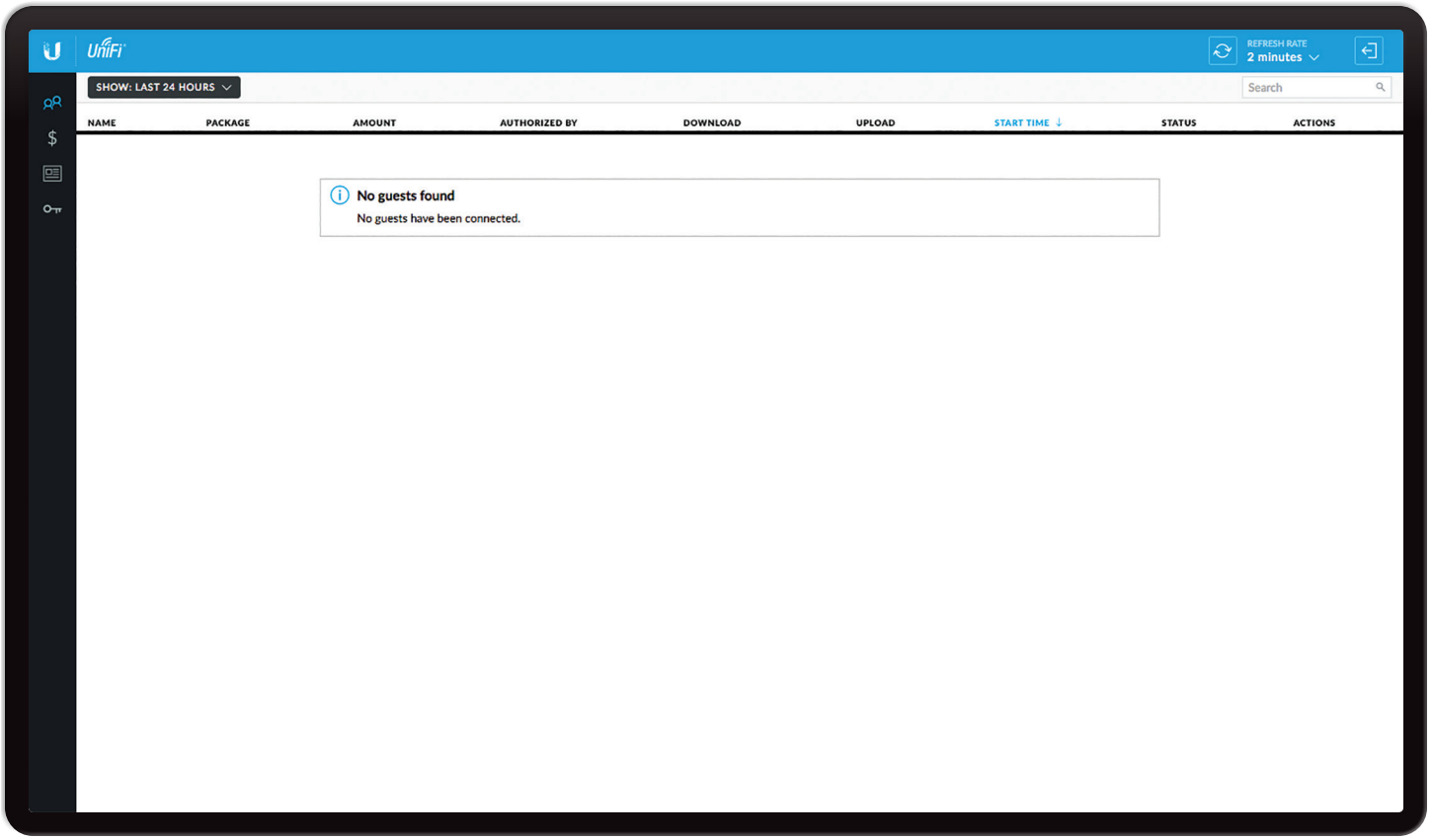
IP Config



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.

Apply Click **Apply** to save changes.



Chapter 15: Hotspot Manager

The Hotspot Manager includes four main tabs when accessed by the UniFi Controller super admin account. For details on a specific tab, refer to the appropriate section.

- *Guests*
- **"Payments and Transactions" on page 122**
- **"Vouchers" on page 122**
- **"Operator Accounts" on page 123**

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 three tabs after login: *Guests*, *Payments*, and *Vouchers*.

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.

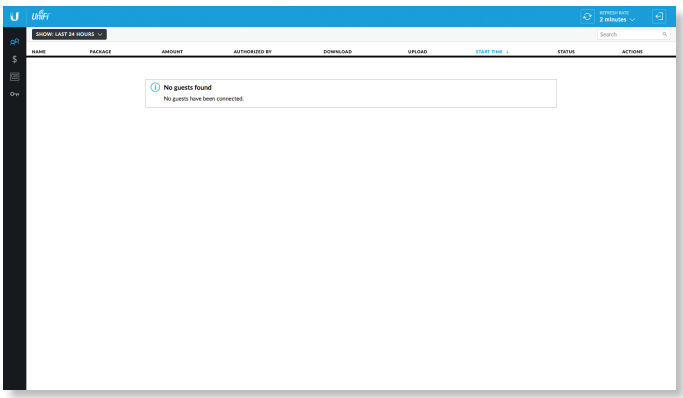
If there is more than one page of entries to display, click the navigation controls or page numbers at the bottom right of the screen to display different pages.

To access the Hotspot Manager, go to **Settings** > **Guest Control**, and click **Go to Hotspot Manager**. See **"Hotspot" on page 36** 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*

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**.

Search Search Enter keywords in the *Search* field to find a specific guest based on *Name/MAC Address*, *Package*, *Amount*, *Authorized By*, or *Status* value.

(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 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.

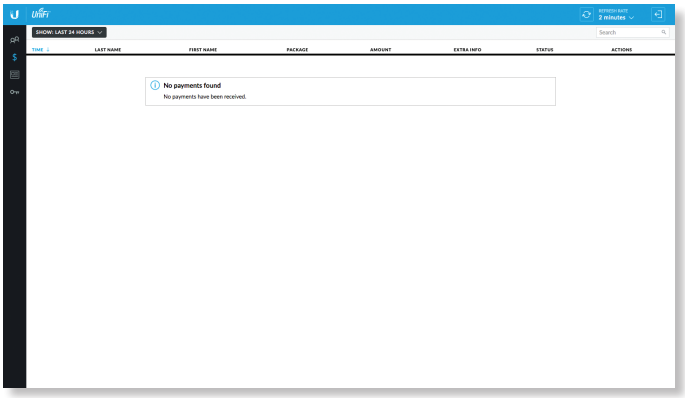
Status Displays the remaining session time for the guest. Displays *Expired* if there is no remaining session time.

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**.

Search Search Enter keywords in the *Search* field to find a specific voucher based on *Time*, *Name*, *Package*, *Amount*, *Extra Info*, or *Status* value.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

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.

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.

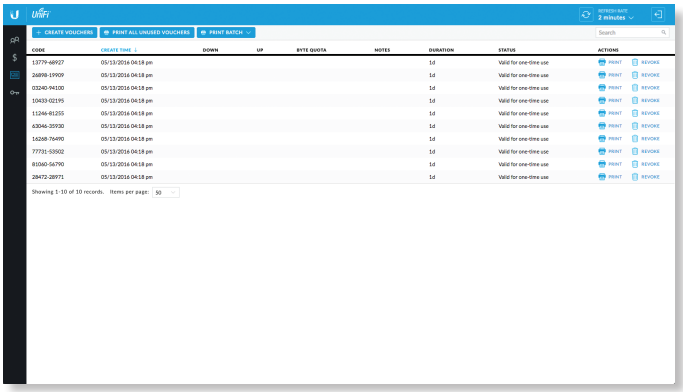
Status Displays the status of the transaction.

Actions Click a button to perform the desired action:

- **Refund** Refund the selected customer if necessary.

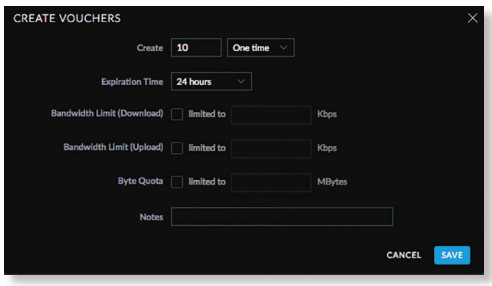
Vouchers

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** or for **Multi-use**.
- **Expiration Time** Select how long the voucher is valid: **8 hours**, **24 hours**, **2 days**, **3 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.
- **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.



Search Search Enter keywords in the *Search* box to find a specific voucher based on *Code*, *Create Time*, *Notes*, *Duration*, or *Status* value.

(sort) You can click any column to sort the displayed list. The selected column displays ↑ or ↓ to indicate ascending or descending order.

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.

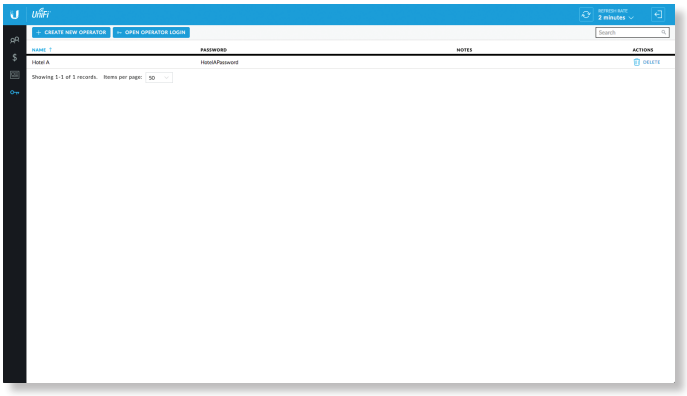
Status Indicates whether the voucher is valid for a single use or multiple uses. Displays *Expired* if the voucher is no longer valid. Displays the number of times used and time until expiration for multi-use vouchers.

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.

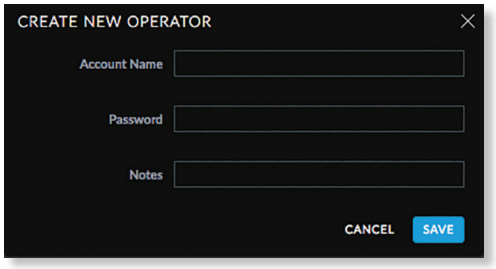
Operator Accounts

(Only available for admins with read/write access to the UniFi Controller). Create *Operator Accounts* that can log in to *Hotspot Manager* to manage guests, payments or transactions, and vouchers.



Create New Operator To create a new operator account, click + CREATE NEW OPERATOR and complete the following:

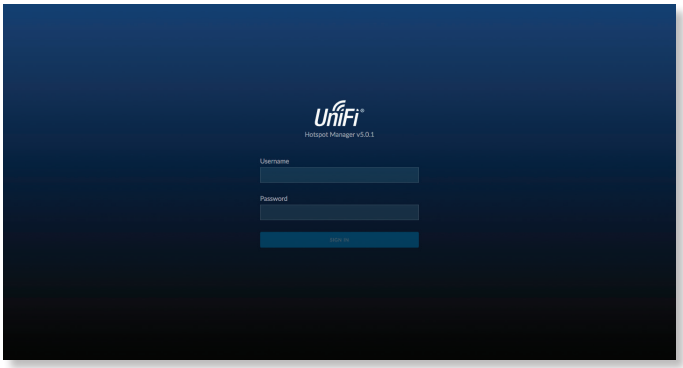
- **Account Name** Enter a name for the operator. The *Account Name* should use A-Z, a-z, or 0-9. Spaces and symbols are allowed but not recommended.
- **Password** Enter a password for the operator. The *Password* has to start with A-Z, a-z, or 0-9. The other characters can only be printable ASCII characters.
- **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.



Open Operator Login Click OPEN OPERATOR LOGIN to test the operator credentials.

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*

The UniFi Hotspot Manager login screen will appear. Enter the username and password in the appropriate fields and click **Sign In**.



Only the *Guests*, *Payments*, and *Vouchers* tabs will appear.

Search Search Enter keywords in the *Search* field to find a specific operator account based on *Name*, *Password*, or *Notes* value.

(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 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.

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 32** 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.

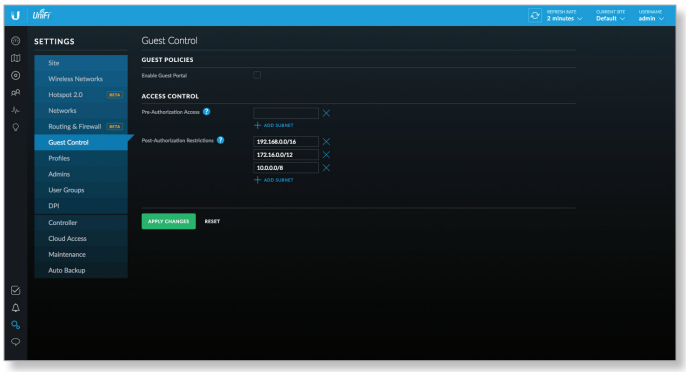
In order to provide the maximum flexibility in your branding effort, the UniFi Controller software provides total access to the portal directory on the system in which it is installed.

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

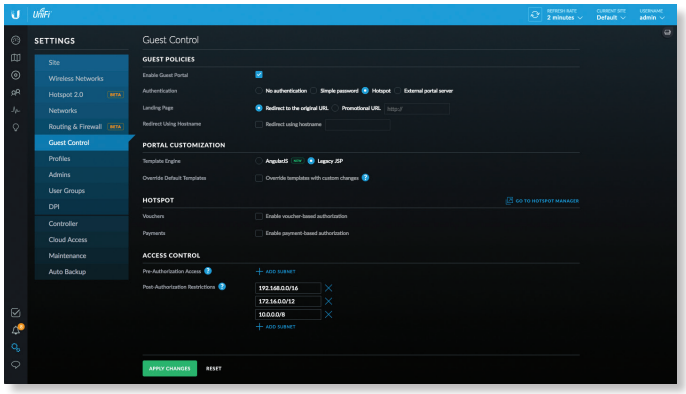
To enable the guest portal with custom Legacy JSP branding, perform the following steps:

1. Go to **Settings** and click **Guest Control**.

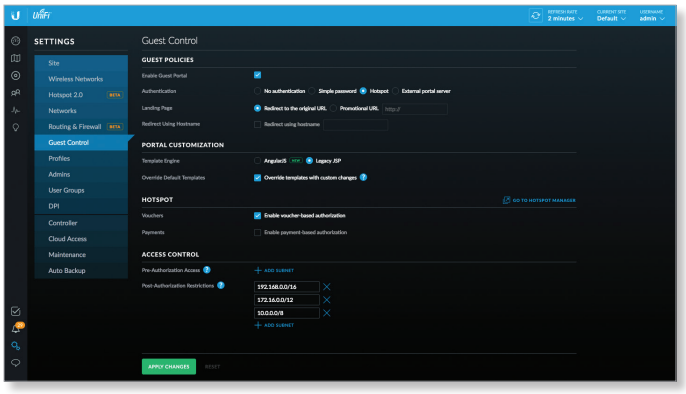


2. Select **Enable Guest Portal** to enable it, and then select an authentication method.

Note: See **"Settings > Guest Control" on page 32** for more information on enabling the *Guest Portal* for the following authentication and landing page options: *No authentication*, *Simple Password*, and *Hotspot*.



3. For the *Template Engine* setting, keep the default, *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 32** 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 32** 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

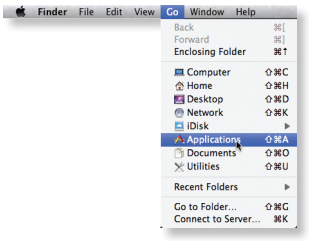
<Drive_Letter>:\Users\<Username>\Ubiquiti UniFi\data\sites\<site_name>\portal

For specific instructions on accessing the files, refer to the specific operating system:

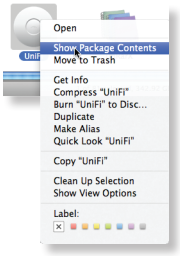
- *Mac*
- **"Windows" on page 128**

Mac

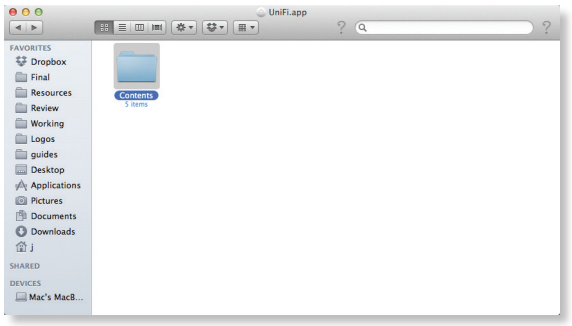
1. Navigate to **Go** > **Applications**.



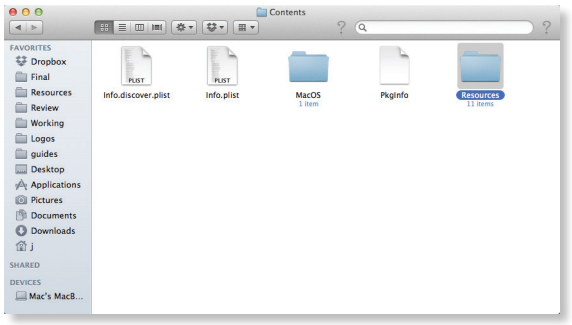
2. Control-click the **UniFi** application and then click **Show Package Contents**.



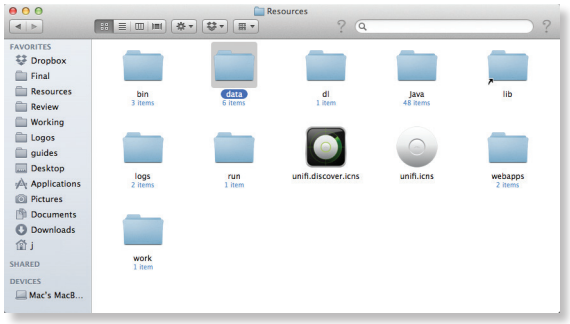
3. Double-click the **Contents** folder to open it.



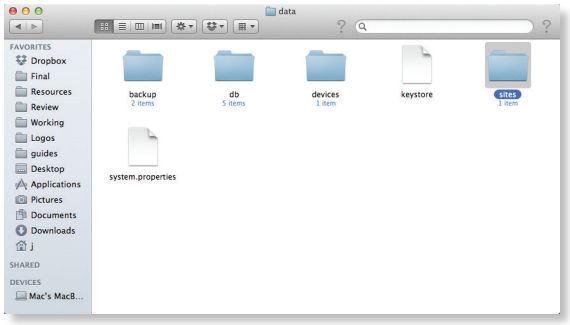
4. Double-click the **Resources** folder to open it.



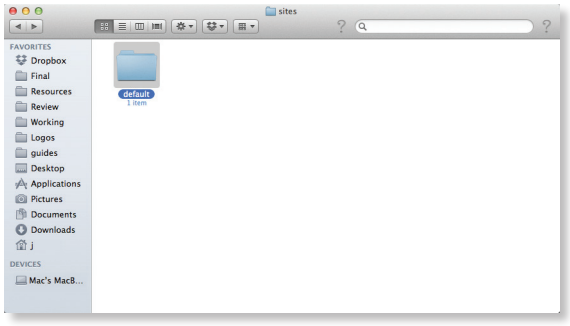
5. Double-click the **data** folder to open it.



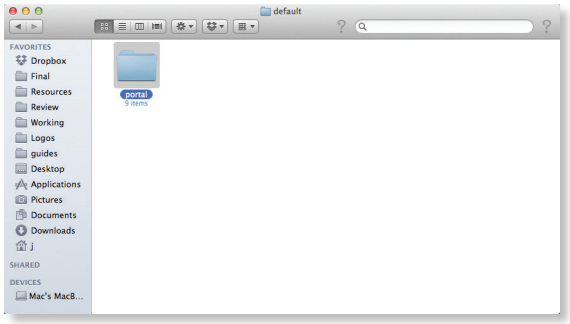
6. Double-click the **sites** folder to open it.



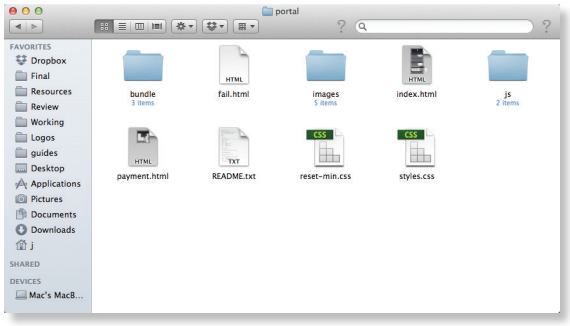
7. Double-click the folder whose name matches the site ID (for example: */manage/s/<site_ID>/dashboard*).



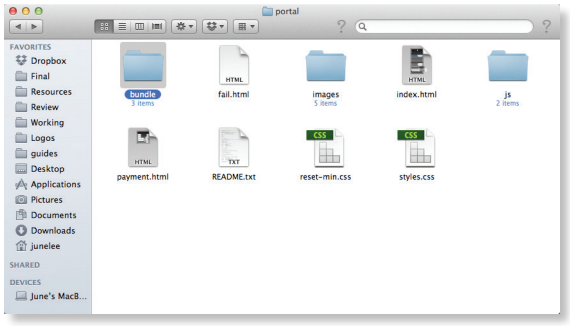
8. Double-click the **portal** folder to open it.



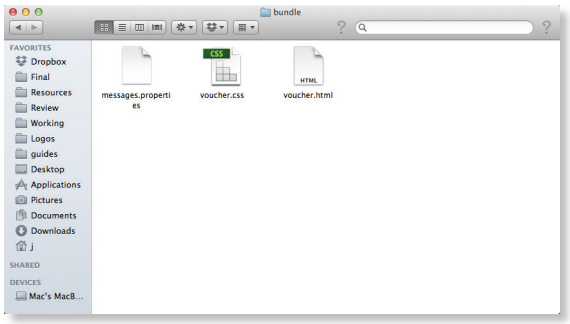
9. You have several files that you can customize in the portal folder (these are described in the *Customizable Default Files* section).



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

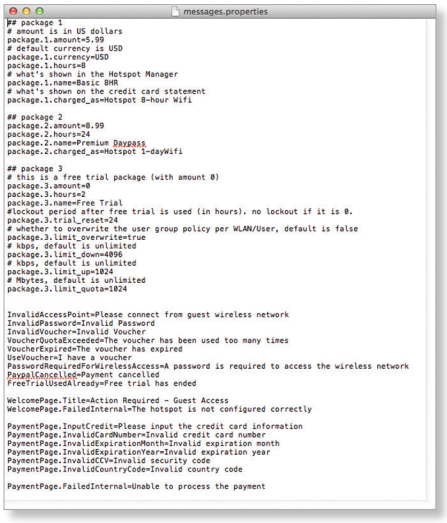
Customizable Default Files

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 Discovery Utility

Overview

The Ubiquiti UniFi Discovery Utility includes tools that allow the discovery and management of UniFi APs. It is installed automatically as part of the UniFi Controller software installation process. See **"Software Installation" on page 1** for more information.

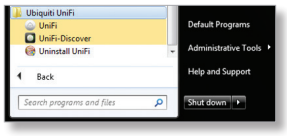
Launching the UniFi Discovery Utility

Mac Users

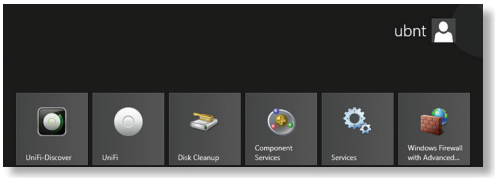
From the Finder, click **Go** > **Applications** and double-click the *UniFi-Discover.app* icon.

PC Users

For most versions of Windows, go to **Start** > **All Programs** > **Ubiquiti UniFi** and double-click the *UniFi-Discover* icon.

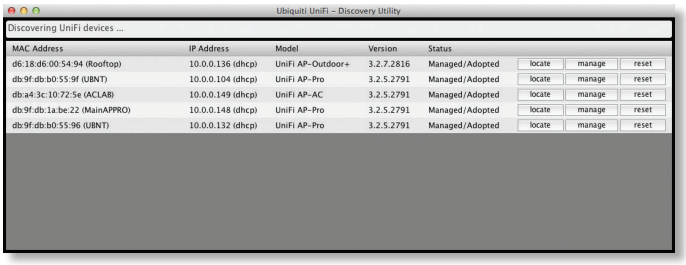


For Windows 8, go to the *Start* menu and double-click the *UniFi-Discover* icon.



UniFi Discovery Utility Interface

Upon launch, the UniFi Discovery Utility listens to Layer-2 broadcast/multicast beacons from UniFi APs in both a factory default state and an unmanaged state (adopted but unable to contact the UniFi Controller software).



MAC Address Displays the MAC address and alias of the AP. The alias is displayed in parentheses if it has been specified; see **"UniFi Access Point – Configuration" on page 108** for details.

IP Address Displays the IP address of the AP and the method used by the AP to obtain an IP address. The method is displayed as *DHCP* or *Static* in parentheses.

Model Displays the model name of the AP.

Version Displays the firmware version installed on the AP.

Status Displays the current status of the AP: *Pending*, *Managed/Adopted*, *Login Failed*, or *IP Unreachable*.

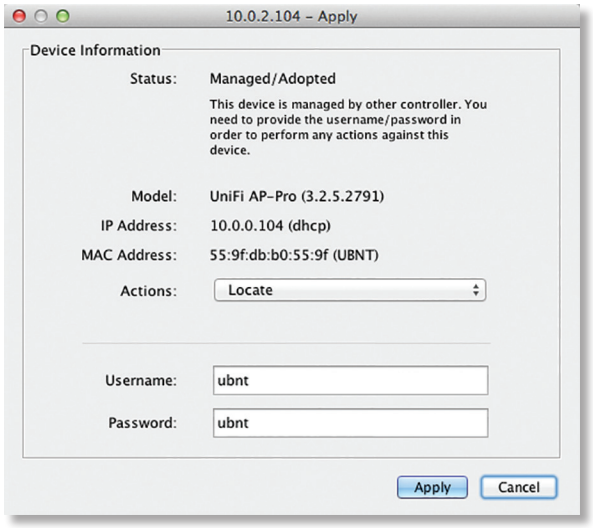
There are three buttons available:

- **"Locate" on page 130**
- **"Manage" on page 130**
- **"Reset" on page 131**

Note: To reboot the AP, click one of the buttons listed above and proceed to **"Reboot" on page 131**.

Locate

Locate the AP. The following window will appear:



Actions If you clicked the *Locate* button, then *Locate* is automatically selected.

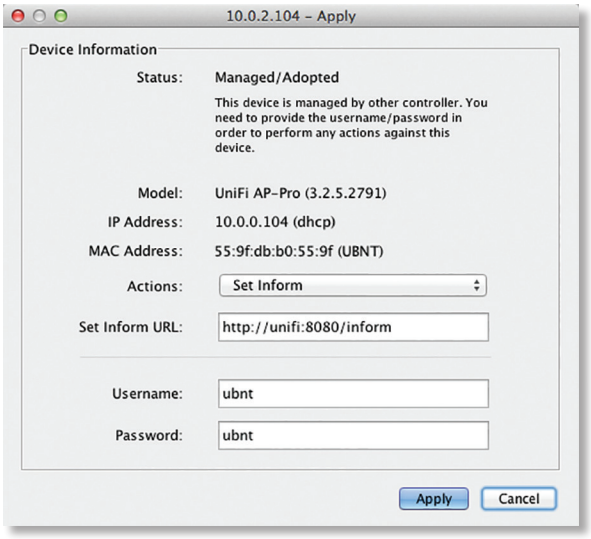
Username If required, enter the device username.

Password If required, enter the device password.

Apply Click **Apply** to locate the AP. The LED on the AP will flash so that it can be differentiated from the other APs.

Manage

Set the inform URL, allowing the AP to be managed by the UniFi Controller software running in a NOC or in the cloud. (See **"Network Topology Requirements" on page 1** for a visual representation of this configuration.) The following window will appear:



Actions If you clicked the *Manage* button, then *Manage* is automatically selected.

Set Inform URL Enter the URL, port, and path to the UniFi Controller software.

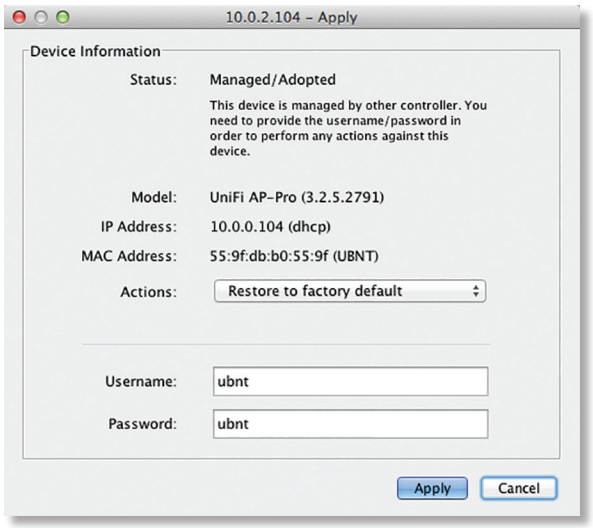
Username If required, enter the device username.

Password If required, enter the device password.

Apply Click **Apply** to save the inform URL.

Reset

Reset the AP to factory default settings. The following window will appear:



Actions If you clicked the *Reset* button, then *Restore to factory default* is automatically selected.

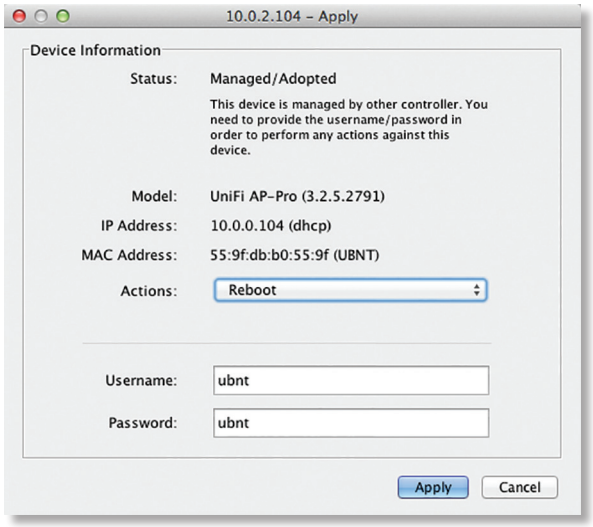
Username If required, enter the device username.

Password If required, enter the device password.

Apply Click **Apply** to reset the AP to factory default settings.

Reboot

To reboot the AP, click any of the buttons (*Locate*, *Manage*, or *Reset*) on the *UniFi Discovery Utility* screen. The following window will appear:



Actions Select **Reboot** from the drop-down menu.

Username If required, enter the device username.

Password If required, enter the device password.

Apply Click **Apply** to reboot the AP.

Appendix C: UniFi Mobile App

Overview

The UniFi app has two general functions:

- You can use a mobile device to provision a UniFi AP for basic functionality without configuring a UniFi Controller. Go to the *Basic Setup* section below.
- You can use a mobile device to access the UniFi Controller. Go to **"Controller Mode" on page 136**.

Basic Setup

You can set up any UniFi AP.

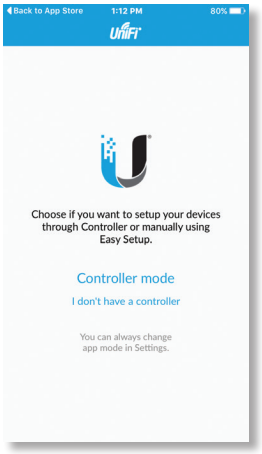
Requirements

- 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

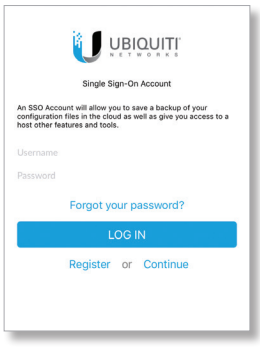
The following instructions describe the iOS version of the app; however, the Android version is similar.

1. Download the UniFi App from the App Store (iOS) or Google Play™ (Android).

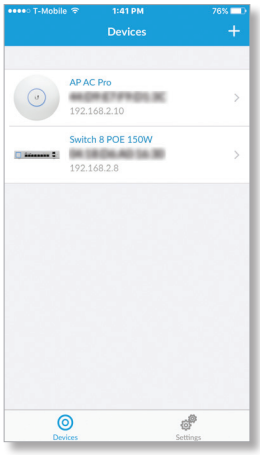
2. Select the functionality you want to use:
   - **Controller mode** Use the app to access the UniFi Controller. Go to **"Controller Mode" on page 136**.
   - **I don't have a controller** Use the app to manually provision a UniFi device for basic functionality without configuring a UniFi Controller. Go to step 3.



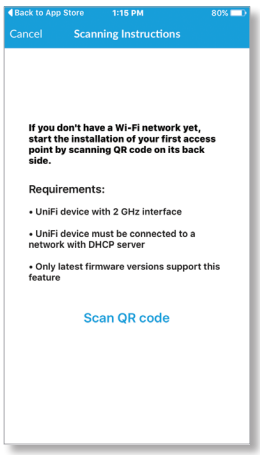
3. Launch the app, and use one of the following options:
   - **Log In** Enter the Username and Password of your Ubiquiti Single Sign-On (SSO) account. Tap **Log In**.
   - **Register** To register for an SSO account, tap **Register**.
   - **Continue** If you do not want to back up or restore configurations, you can skip the login and tap **Continue**.



4. The app will search for new devices. Tap the UniFi AP on the device list and go to step 8.

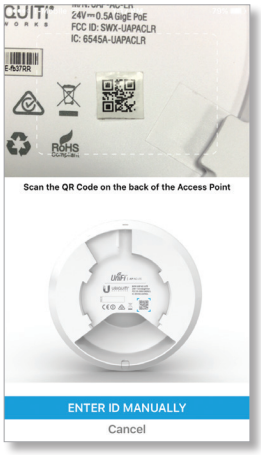


5. If a new device is not detected, tap +.
6. Tap **Scan QR Code**.



7. Scan the QR code on the back of the UniFi AP, or tap **Enter ID Manually** to type the case-sensitive MAC address.

   Note: For Android, the mobile device automatically connects to the helper SSID. For iOS, manually copy and paste the helper SSID and password.

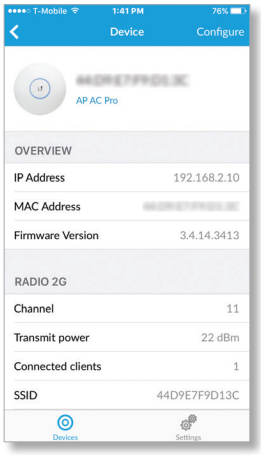


8. You may be prompted to upgrade the UniFi AP to the latest firmware. Please proceed with the upgrade.

Go to the *Device* section below to set up the UniFi AP.

Device

The *Device* screen displays basic status information:



Configure To manage the device, go to the *Configure* section in the next column.

Overview

IP Address Displays the IP address of the device.

MAC Address Displays the MAC address or unique hardware identifier of the device.

Firmware Version Displays the version number of the device's firmware.

Radio 2G

Channel Displays the channel used.

Transmit Power Displays the level of transmit power.

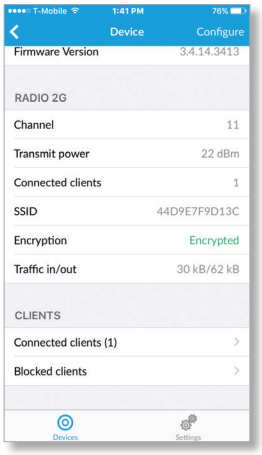
Connected Clients Displays the number of clients connected to this UniFi AP.

SSID Displays the wireless network name.

Encryption Displays *Encrypted*.

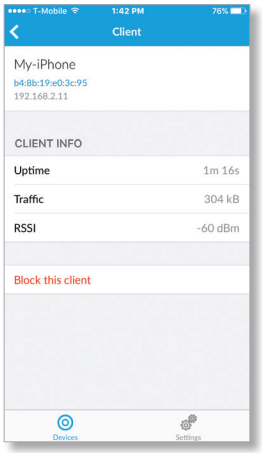
Traffic In/Out Displays the amount of upload and download traffic.

Clients



Connected Clients Displays the number of clients connected to this UniFi AP. Tap to display additional details:

- **Uptime** Displays the duration of time the device has been running without interruption.
- **Traffic** Displays the total amount of data downloaded and uploaded by the client.
- **RSSI** Displays the SNR of the connection.
- **Block this client** Tap to block this client from accessing the network.

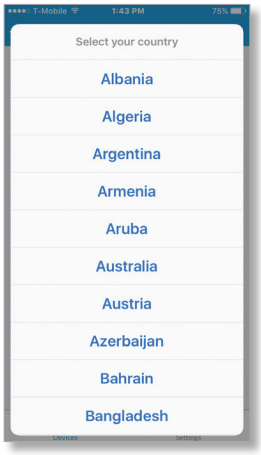


Blocked Clients Displays the number of blocked clients. Tap to display a list of blocked clients.

- **Unblock this client** Tap to allow this client access to the network.

Configure

- **Select your country** Select the appropriate country from the list.

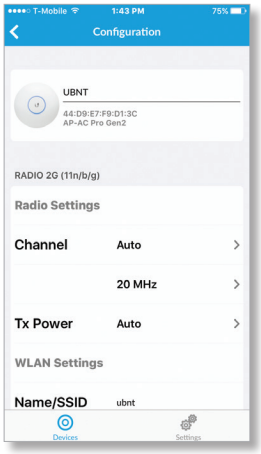


Configure the following settings for each radio:

Radio 2G (11n/b/g)

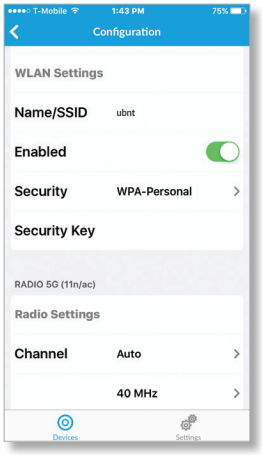
Radio Settings

- **Channel** Select a channel number or keep the default, *Auto*.
- **(channel width)** Select the appropriate channel width.
- **TX Power** The default is *Auto*. Select **High**, **Medium**, or **Low**.



WLAN Settings

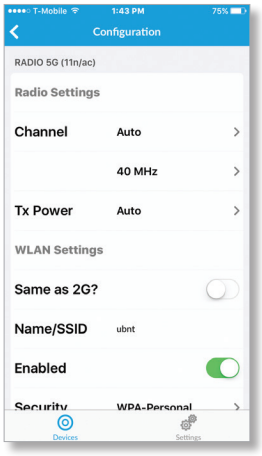
- **Name/SSID** Enter the name of the wireless network.
- **Enabled** Enable or disable wireless functionality.
- **Security** Select the security method you want to use.
- **Security Key** Enter the passphrase.



Radio 5G (11n/ac)

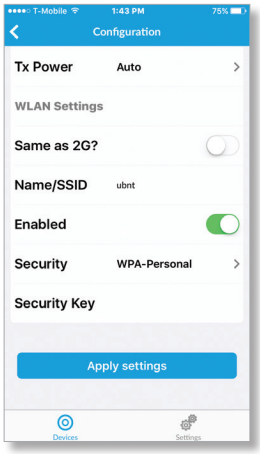
Radio Settings

- **Channel** Select a channel number or keep the default, *Auto*.
- **(channel width)** Select the appropriate channel width.
- **TX Power** The default is *Auto*. Select **High**, **Medium**, or **Low**.



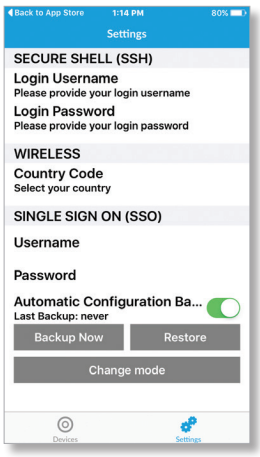
WLAN Settings

- **Same as 2G?** Tap to use the same settings as the 2.4 GHz configuration.
- **Name/SSID** Enter the name of the wireless network.
- **Enabled** Enable or disable wireless functionality.
- **Security** Select the security method you want to use.
- **Security Key** Enter the passphrase.
- **Apply Settings** Tap to save your changes.



Settings

The *Settings* screen offers the following options:



- **Secure Shell (SSH) Login Username** Change the username of the device login.
- **SSH Login Password** Change the password of the device login.
- **Country Code** Change the country selection.
- **Single Sign-On (SSO) Username** Change the username of the SSO account.
- **SSO Password** Change the password of the SSO account.
- **Automatic Configuration Backup** Enable or disable automatic backup of the current configuration.
- **Back Up Now** Back up the current configuration.
- **Restore** Restore the previously saved configuration.
- **Change mode** Select this option if you want to change to *Controller mode*. Go to the *Controller Mode* section in the next column.

Note: For advanced configuration, switch to *Controller mode*.

Controller Mode

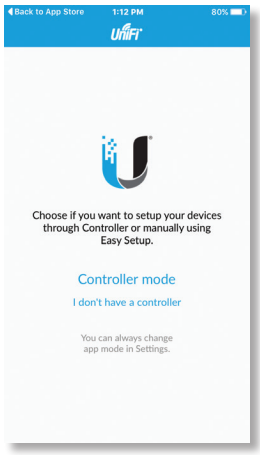
You can access the UniFi Controller through the UniFi mobile app.

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).

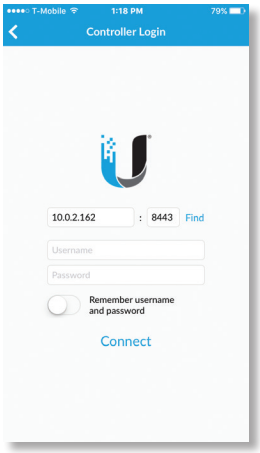
2. Select the functionality you want to use:
   - **Controller mode** Use the app to access the UniFi Controller. Go to step 3.
   - **I don't have a controller** Use the app to manually provision a UniFi AP for basic functionality without configuring a UniFi Controller. Go to **"Basic Setup" on page 133**.



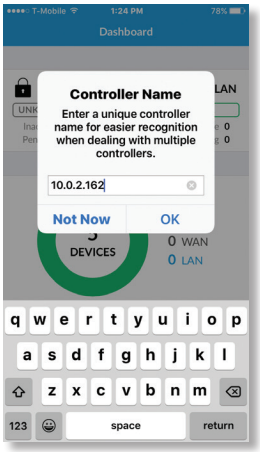
3. Enter the following information:
   - **(IP address)** Enter the IP address of the UniFi Controller.
   - **(port)** Enter the appropriate port number, which is typically *8443*.

   Note: If you do not know the IP address, you can tap *Find* to detect a UniFi Controller and then select it.
   - **(username)** Enter your username for the UniFi Controller.
   - **(password)** Enter your password for the UniFi Controller.
   - **Remember username and password** Tap this option if you want the app to remember your username and password.

   Tap **Connect**.



4. You may be prompted to enter a descriptive name for the Controller if it is currently using an IP address. You can change it now and then tap **OK**, or you can tap *Not Now* to skip this step.

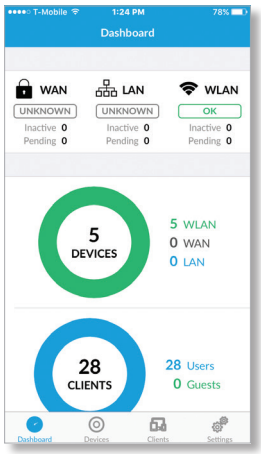


The UniFi app includes four tabs:

- **"Dashboard" on page 137**
- **"Devices" on page 138**
- **"Clients" on page 143**
- **"Settings" on page 145**

Dashboard

The *Dashboard* screen provides an overview of your network's status.



WAN

(status) Displays one of the following:

- **OK** The node is active.
- **Unknown** There is no UniFi Security Gateway.
- **Warning** There is a warning; please investigate further.
- **Error** There is an error; please investigate further.

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

Pending Displays the number of Gateway devices pending adoption.

LAN

(status) Displays one of the following:

- **OK** The node is active.
- **Unknown** There is no UniFi Switch.
- **Warning** There is a warning; please investigate further.
- **Error** There is an error; please investigate further.

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

Pending Displays the number of wired devices pending adoption.

WLAN

(status) Displays one of the following:

- **OK** The node is active.
- **Unknown** There is no UniFi AP.
- **Warning** There is a warning; please investigate further.
- **Error** There is an error; please investigate further.

Inactive Displays the number of APs adopted but not active.

Pending Displays the number of APs pending adoption.

Devices

Devices Displays the total number of devices.

WLAN Displays the number of wireless devices.

WAN Displays the number of Gateway devices.

LAN Displays the number of wired devices.

Scroll down the *Dashboard* screen to view additional status information.

Clients

Clients Displays the total number of clients.

Users Displays the number of connected users.

Guests Displays the number of connected guests.

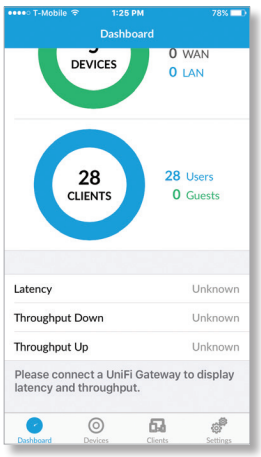
Latency and Throughput

Note: The *Latency* and *Throughput* values require a UniFi Security Gateway.

Latency Displays the amount of time it takes a packet to travel from the UniFi Security Gateway to the service provider's gateway. *Unknown* is displayed if there is no UniFi Security Gateway.

Throughput Down Displays the amount of current download traffic. *Unknown* is displayed if there is no UniFi Security Gateway.

Throughput Up Displays the amount of current upload traffic. *Unknown* is displayed if there is no UniFi Security Gateway.



Devices

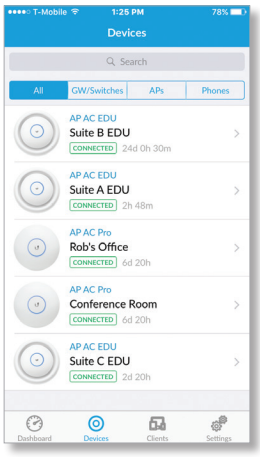
The *Devices* screen displays a list of UniFi devices discovered by the UniFi Controller. Details include the model number, hostname, status, and connection duration. Tap a device for configuration or details.

All Displays all device types.

GW/Switch Displays Gateway and Switch devices only.

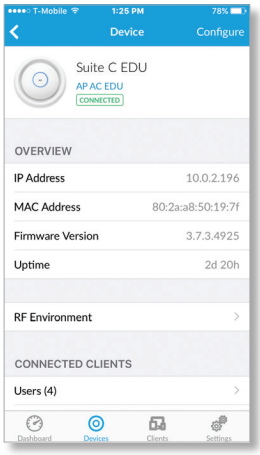
APs Displays UniFi APs only.

Phones Displays UniFi VoIP Phones only.

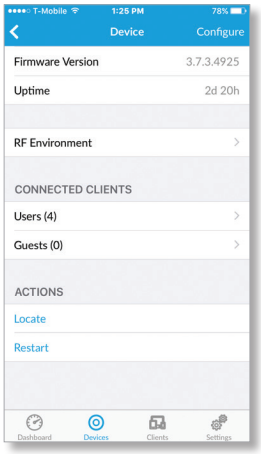


Overview

- **Configure** To manage the device, go to **"Configure" on page 141**.
- **IP Address** Displays the IP address of the device.
- **MAC Address** Displays the MAC address or unique hardware identifier of the device.
- **Firmware Version** Displays the version number of the device's firmware.
- **Uptime** Displays the duration of time the device has been running without interruption.

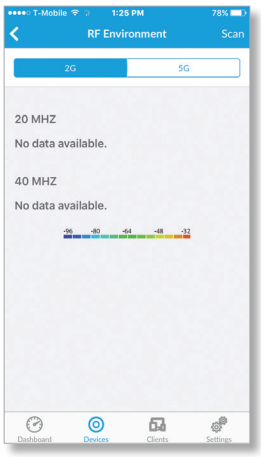


- **RF Environment** (Available only for UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU.) Tap this option for spectral analysis to help in channel selection and planning.



  - **2G/5G** Select the frequency band you want to analyze.
  - **Scan** Tap **Scan** to trigger an RF scan and then tap **Scan** again to continue.

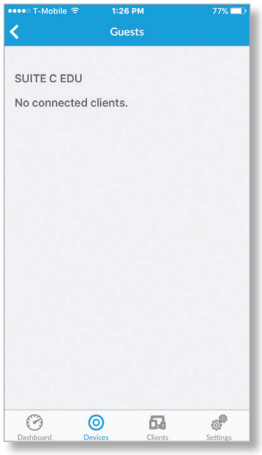
Note: The RF scan may take more than five minutes. All clients using this AP will be disconnected, and the AP will be offline for the duration of the scan.



Connected Clients

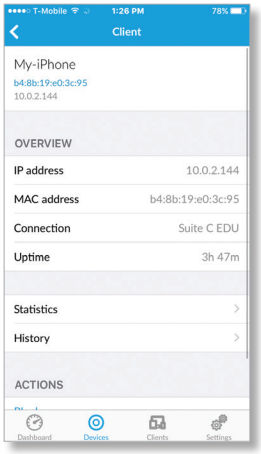
- **Users** Displays a list of connected users, including SSID (wireless network name), *Activity* level, and connection duration. Tap a user for details; go to the *Overview* section below for more information.

- **Guests** Displays a list of connected guests, including SSID (wireless network name), *Activity* level, and connection duration. Tap a guest for details; go to the *Overview* section below for more information.

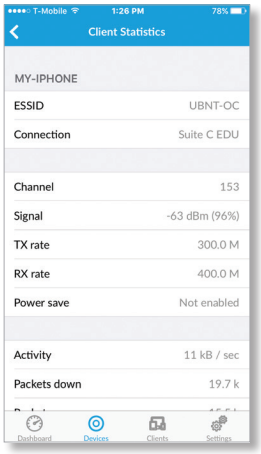


Overview

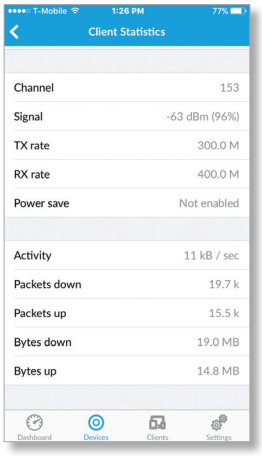
- **IP Address** Displays the IP address of the client.
- **MAC Address** Displays the MAC address or unique hardware identifier of the client.
- **Connection** Displays the hostname, alias, or MAC address of the UniFi device the client is connected to.
- **Uptime** Displays the duration of time the client has been connected without interruption.



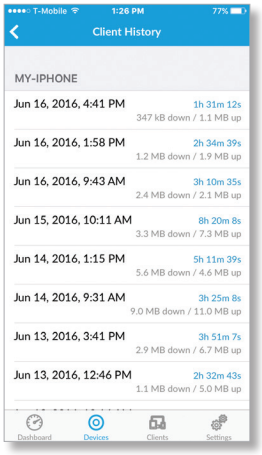
- **Statistics** Displays additional client information:



  - **ESSID** (Available for wireless clients.) Displays the name of the wireless network.
  - **Connection** Displays the hostname, alias, or MAC address of the UniFi device the client is connected to.
  - **Channel** (Available for wireless clients.) Displays the channel being used.
  - **Signal** (Available for wireless clients.) 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.
  - **Activity** Displays the level of activity in Bytes per second.
  - **Packets Down** Displays the amount of data downloaded as packets.
  - **Packets Up** Displays the amount of data uploaded as packets.
  - **Bytes Down** Displays the amount of data downloaded as bytes.
  - **Bytes Up** Displays the amount of data uploaded as bytes.



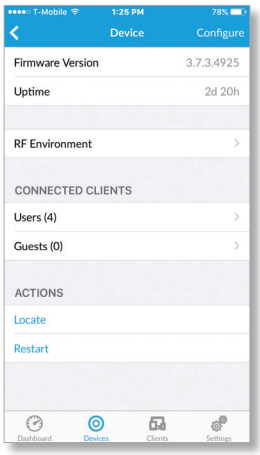
- **History** Displays the historical usage of a client.



  - **(date/time)** Displays the date and time of the connection.
  - **(duration)** Displays the duration of the connection.
  - **(down/up)** Displays the total amount of data downloaded and uploaded by the client.

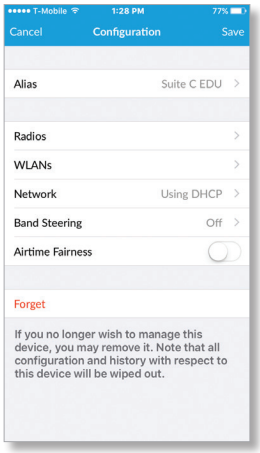
Actions

You can locate or restart the device.

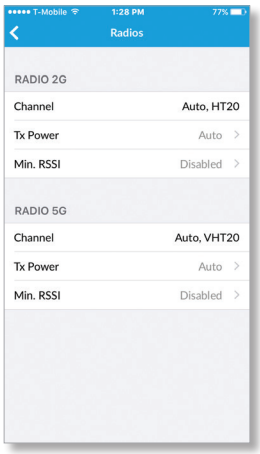


- **Locate** Tap to flash the LED on the device. The LED will flash until *Locate* is tapped again.
- **Restart** Tap to restart the selected device.

Configure



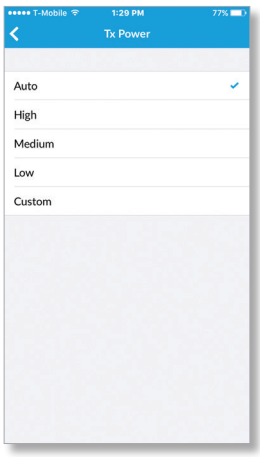
- **Alias** Also known as the host name. Enter or edit the customizable name or identifier of the device.
- **Radios** These settings are available only for APs.



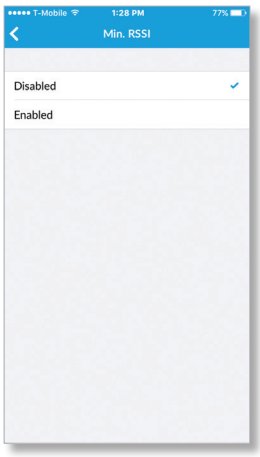
- **Channel** Select the appropriate channel number and channel width.

Note: If the AP is part of a Zero Handoff WLAN Group, then the *Channel* setting cannot be changed.

- **TX Power** Select the appropriate transmit power value. The default is *Auto*.

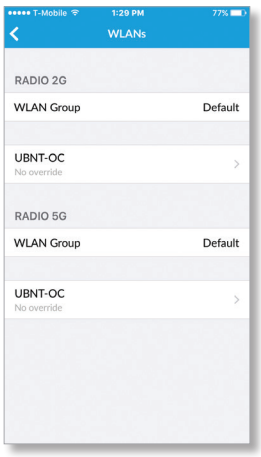


- **Min. RSSI** Disabled by default. Select this option and enter a minimum threshold (we recommend a value in this range: -70 to -90 dBm). For UniFi, RSSI is synonymous with SNR. If the client signal falls below the specified threshold, then the AP kicks out the client, allowing it to reconnect with a more suitable AP.

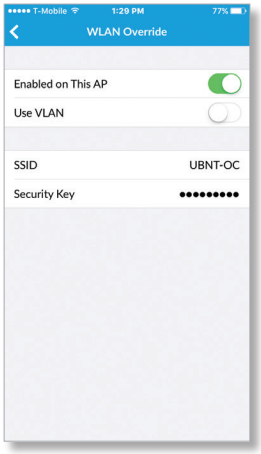


Note: If the AP is part of a Zero Handoff WLAN Group, the *Minimum RSSI* setting cannot be changed.

- **WLAN** These settings are available only for APs.

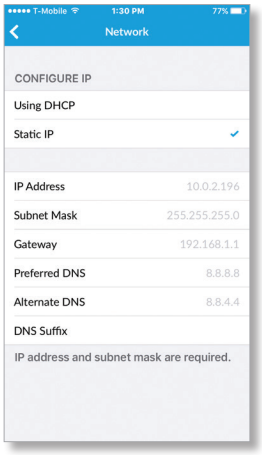


  - **WLAN Group** Select the appropriate group.
  - **(SSID)** Tap to override settings. The WLAN *Override* screen appears.

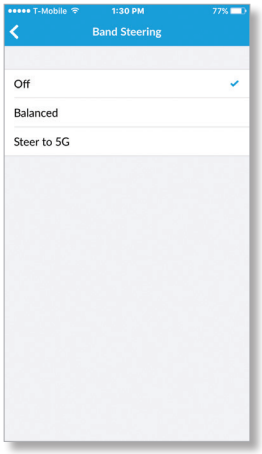


    - **Enabled on This AP** Tap to enable the WLAN for use.
    - **Use VLAN** Tap to enable the VLAN. Then enter the VLAN ID. The VLAN ID is a unique value assigned to each VLAN on a single device. Enter a value between 2 and 4095. For example, in a large deployment where there are multiple buildings, 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.

- **Network** Select the appropriate option:
  - **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.

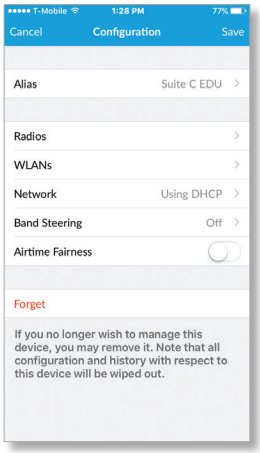


- **Band Steering** (This setting is available only for the UAP-PRO, UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU.) 2.4 GHz networks are typically more congested due to support of legacy clients and multiple sources of 2.4 GHz interference, including Bluetooth devices. Band steering can help distribute the load on 2.4 GHz and 5 GHz networks by steering dual-band clients to the 5 GHz band when appropriate.



- **Off** Keep the default, *Off*, if you do not want to use band steering.
- **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.

- **Airtime Fairness** (This setting is available only for the UAP-AC-LITE, UAP-AC-LR, UAP-AC-PRO, and UAP-AC-EDU.) This helps multiple users to share the bandwidth of a single AP. Tap to enable this option.



- **Forget** Tap **Forget** to remove the AP from management by the UniFi Controller software and reset it to factory default settings.

Note: Use caution when tapping *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.

Clients

The *Clients* screen displays a list of network clients. Details include the hostname, SSID (wireless network name), *Activity* level, and connection duration. Tap a client for details.

You can filter by connection type:

All Displays all connection types.

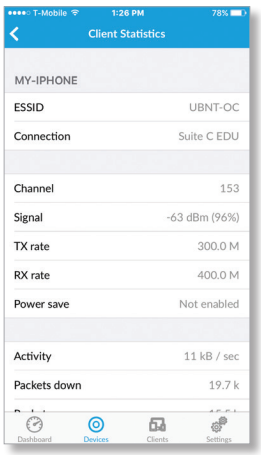
Wireless Displays wireless clients only.

Wired Displays wired clients only.

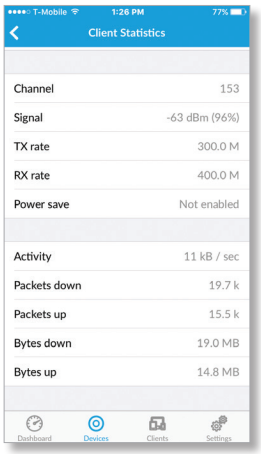
Overview

- **IP Address** Displays the IP address of the client.
- **MAC Address** Displays the MAC address or unique hardware identifier of the client.
- **Connection** Displays the hostname, alias, or MAC address of the UniFi device the client is connected to.
- **Uptime** Displays the duration of time the client has been connected without interruption.

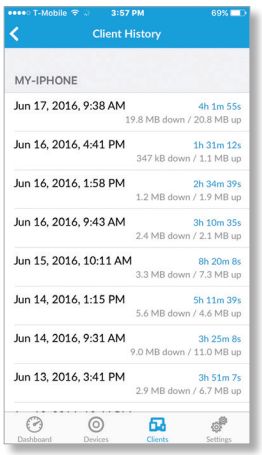
- **Statistics** Displays additional client information:



  - **ESSID** (Available for wireless clients.) Displays the name of the wireless network.
  - **Connection** Displays the hostname, alias, or MAC address of the UniFi device the client is connected to.
  - **Channel** (Available for wireless clients.) Displays the channel being used.
  - **Signal** (Available for wireless clients.) Displays the percentage of signal strength between the AP and client.
  - **TX Rate** Displays the transmit rate.
  - **RX Rate** Displays the receive rate.
  - **Activity** Displays the level of activity in Bytes per second.
  - **Packets Down** Displays the amount of data downloaded as packets.
  - **Packets Up** Displays the amount of data uploaded as packets.
  - **Bytes Down** Displays the amount of data downloaded as bytes.
  - **Bytes Up** Displays the amount of data uploaded as bytes.



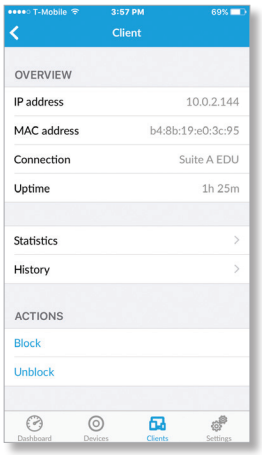
- **History** Displays the historical usage of a client.



  - **(date/time)** Displays the date and time of the connection.
  - **(duration)** Displays the duration of the connection.
  - **(down/up)** Displays the total amount of data downloaded and uploaded by the client.

Actions

You can block or unblock a client device.

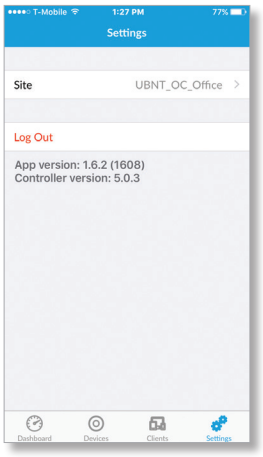


- **Block** Tap to block this client from accessing the network.
- **Unblock** Tap to reconnect a blocked client.

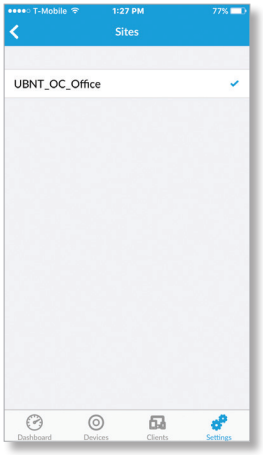
Note: Use caution if you block a client and then exit the *Client* screen. The blocked client will disappear from the client list and then you cannot unblock the client from the UniFi mobile app. Instead, you must access the browser-based UniFi Controller and then unblock the client on the *Insights* screen.

Settings

The current site is displayed on this screen.



Site To change a site, tap the current site and then select a different site.



Log Out To exit the UniFi app or change its mode, tap **Log out**.

Appendix D: UniFi EDU Mobile App

Overview

You can use the UAP-AC-EDU to broadcast announcements with clarity from your mobile device.

Use the UniFi EDU app to broadcast announcements from the UAP-AC-EDU.

Requirements

- UniFi Controller software v4.9.5 or higher
- UAP-AC-EDU firmware v3.4.18 or higher
- A compatible Android or iOS device located on the same Layer-2 network as the UniFi Controller and UniFi APs

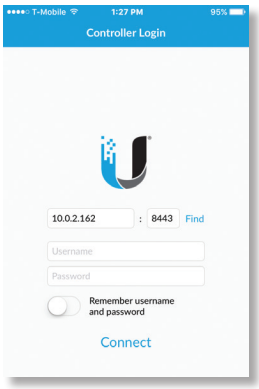
The following instructions describe the iOS version of the app; however, the Android version is similar.

1. Download the UniFi EDU app from the App Store (iOS) or Google Play (Android).

2. Launch the app.
3. Enter the following information:
   - **(IP address)** Enter the IP address of the UniFi Controller.
   - **(port)** Enter the appropriate port number, which is typically *8443*.

   Note: If you do not know the IP address, you can click *Find* to detect a UniFi Controller and then select it.
   - **(username)** Enter your username for the UniFi Controller.
   - **(password)** Enter your password for the UniFi Controller.
   - **Remember username and password** Tap this option if you want the app to remember your username and password.

   Tap **Connect**.

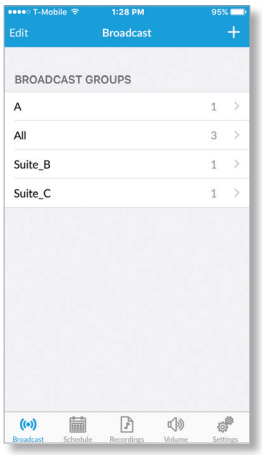


The UniFi EDU app includes five tabs:

- *Broadcast* (see below)
- **"Schedule" on page 137**
- **"Recordings" on page 150**
- **"Volume" on page 151**
- **"Settings" on page 151**

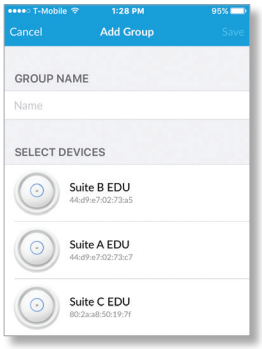
Broadcast

You can organize the UniFi AC EDU APs into multiple broadcast groups.

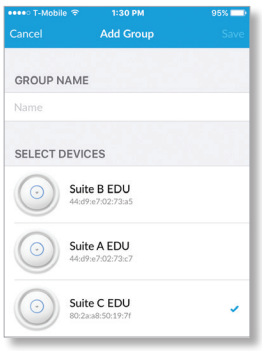


To create a broadcast group, follow these instructions:

1. Click +.
2. Enter a descriptive name in the *Group Name* field.



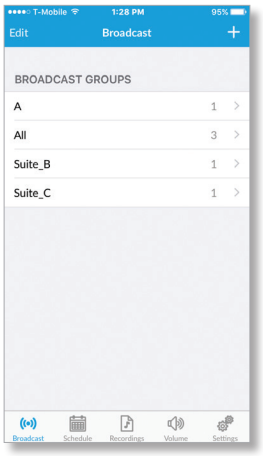
3. Tap the appropriate UniFi AC EDU APs.



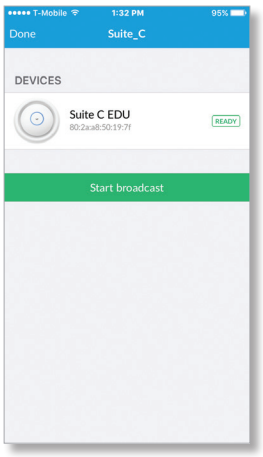
4. Tap **Save** to apply your changes, or tap *Cancel* to discard your changes.

To begin a broadcast, follow these instructions:

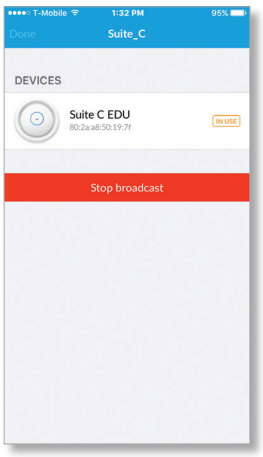
1. Tap the broadcast group you want to use.



2. Tap **Start Broadcast** to start the announcement.



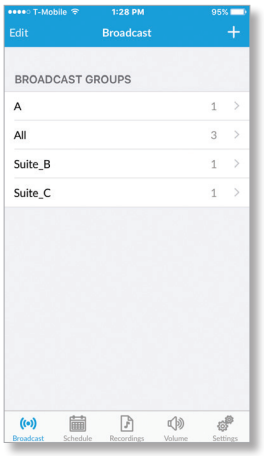
3. Tap **Stop Broadcasting** to end the announcement.



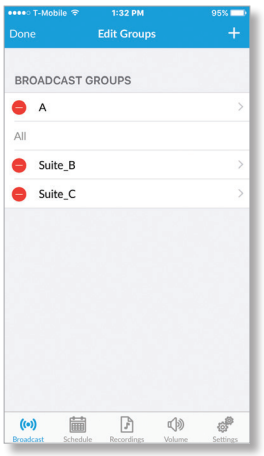
The speakers will automatically be muted when you stop broadcasting.

To edit a broadcast group, follow these instructions:

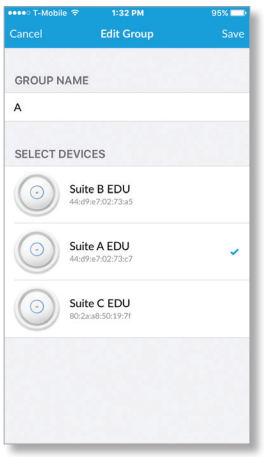
1. Tap **Edit**.



2. To change the name or members of the group, tap the broadcast group.



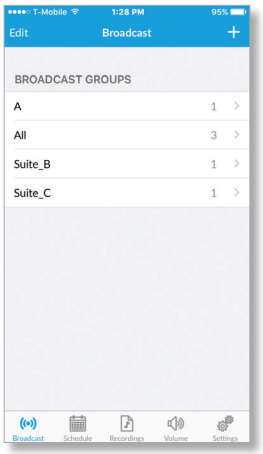
3. Make your changes.



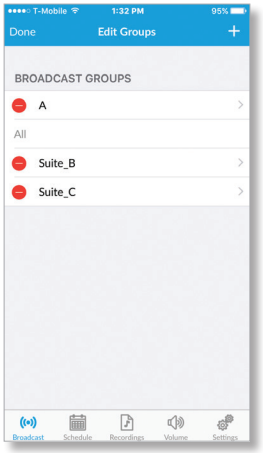
4. Tap **Save** to apply your changes, or tap *Cancel* to discard your changes.

To delete a broadcast group, follow these instructions:

1. Tap **Edit**.



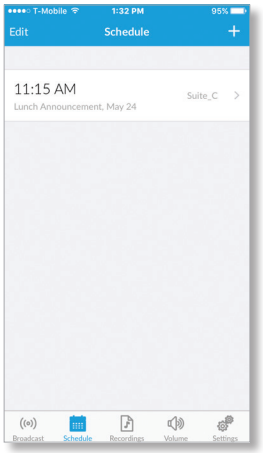
2. To remove a broadcast group, tap .



3. Tap **Done**.

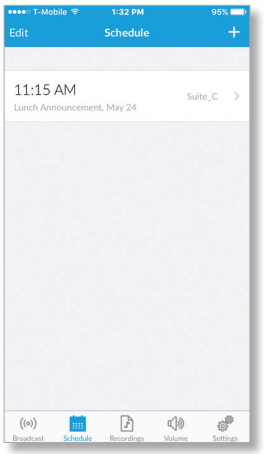
Schedule

You can schedule an announcement.



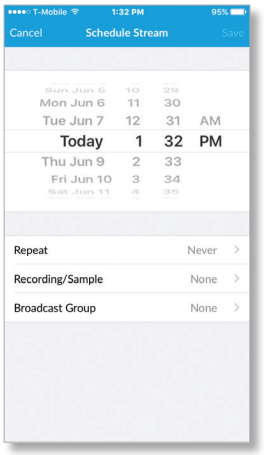
To schedule an announcement, follow these instructions:

1. Tap .



2. Configure the following:
   - **(Date and time)** Select the appropriate date and time.
   - **Repeat** Select this option to specify how often the announcement should recur. Then select **Never**, **Every Day**, **Every Weekday**, or **Custom**.

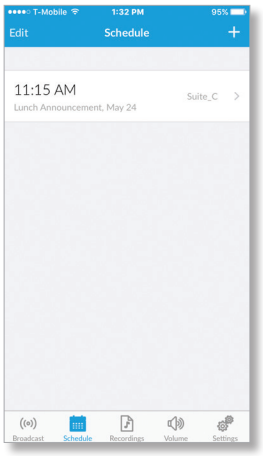
     If you selected *Custom*, select the *Frequency*, **Weekly** or **Monthly**, and then select the appropriate weekday or date.
   - **Recording/Sample** Select the appropriate recording or sample.
   - **Broadcast Group** Select the appropriate group.



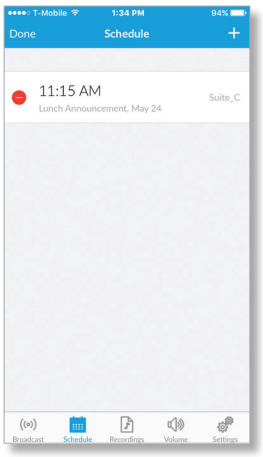
3. Tap **Save** to apply your changes, or tap *Cancel* to discard your changes.

To delete an announcement, follow these instructions:

1. Click **Edit**.



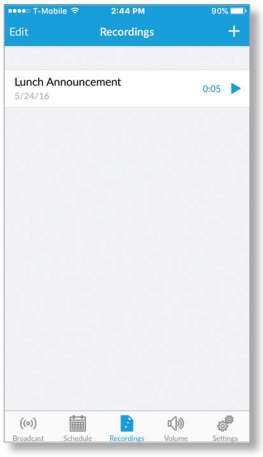
2. To remove an announcement, tap ⊖.



3. Tap **Done**.

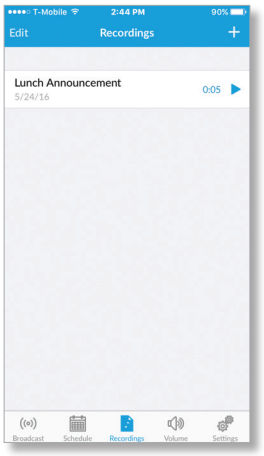
Recordings

You can create a recording.

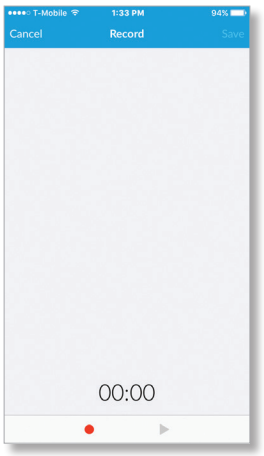


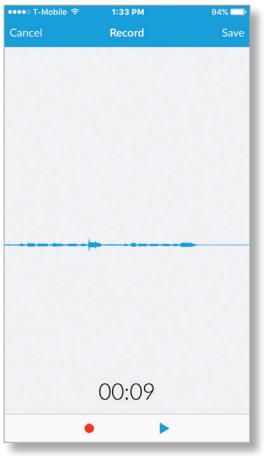
To create a recording, follow these instructions:

1. Tap +.



2. Tap ● to start recording. Tap ● to stop recording. Tap ▶ to play back the recording.

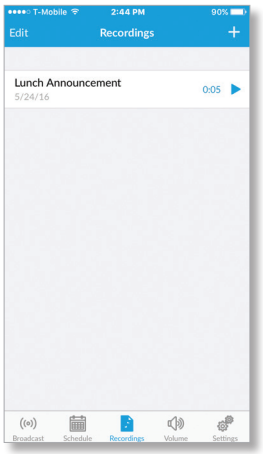




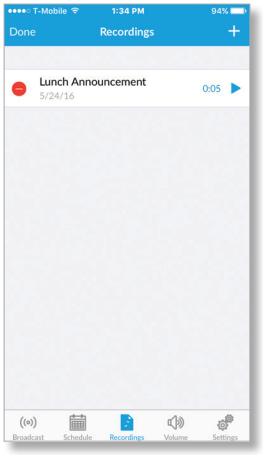
3. Tap **Save** to apply your changes, or tap *Cancel* to discard your changes.

To delete a recording, follow these instructions:

1. Click **Edit**.



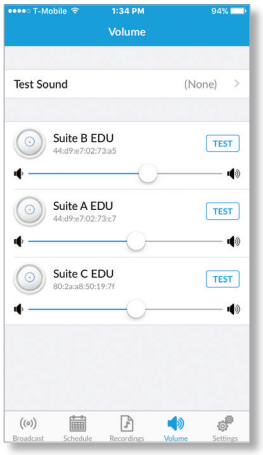
2. To remove a recording, tap .



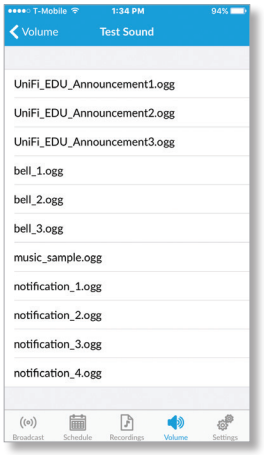
3. Tap **Done**.

Volume

You can select a test sound or adjust the volume of any speaker.



Test Sound Tap **Test Sound** to select a specific sound for testing. Then tap any sound to select it.

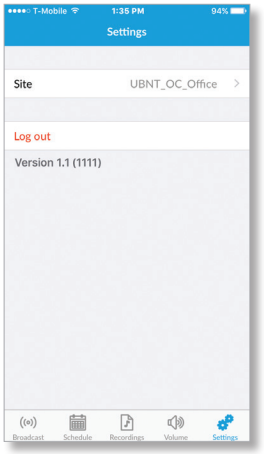


(slider) Use the slider control to adjust the volume for each speaker.

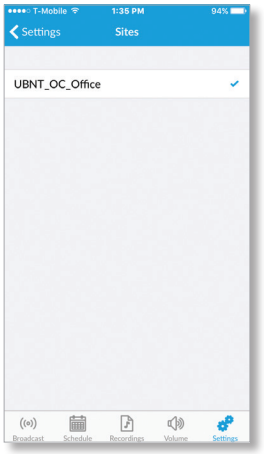
Test To test the sound of any speaker, tap **Test**.

Settings

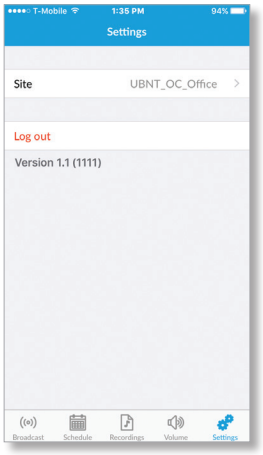
The current site is displayed on this screen.



Site To change a site, tap the current site and then select a different site.



Log Out To exit the UniFi app or change its mode, tap **Log out**.



Appendix E: 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 installation 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 133** 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 154**
- **"Hybrid Deployment" on page 155**

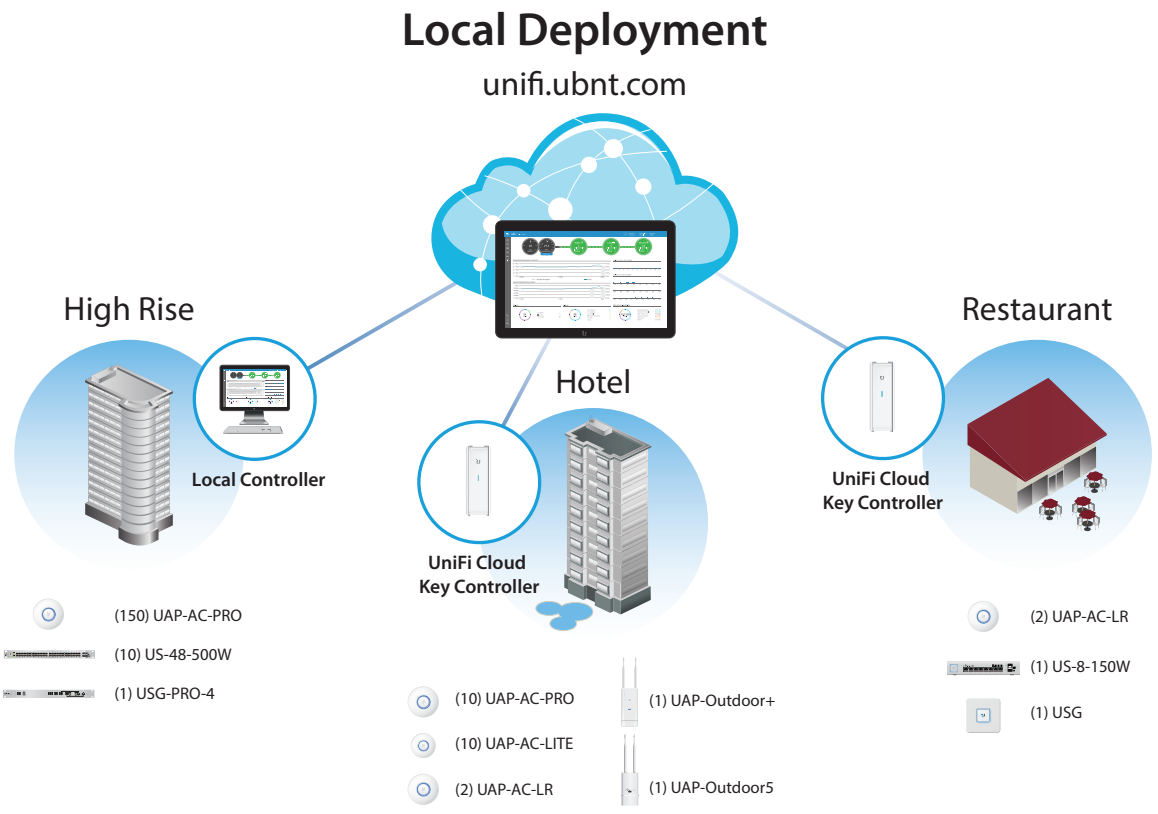
Local Deployment

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).

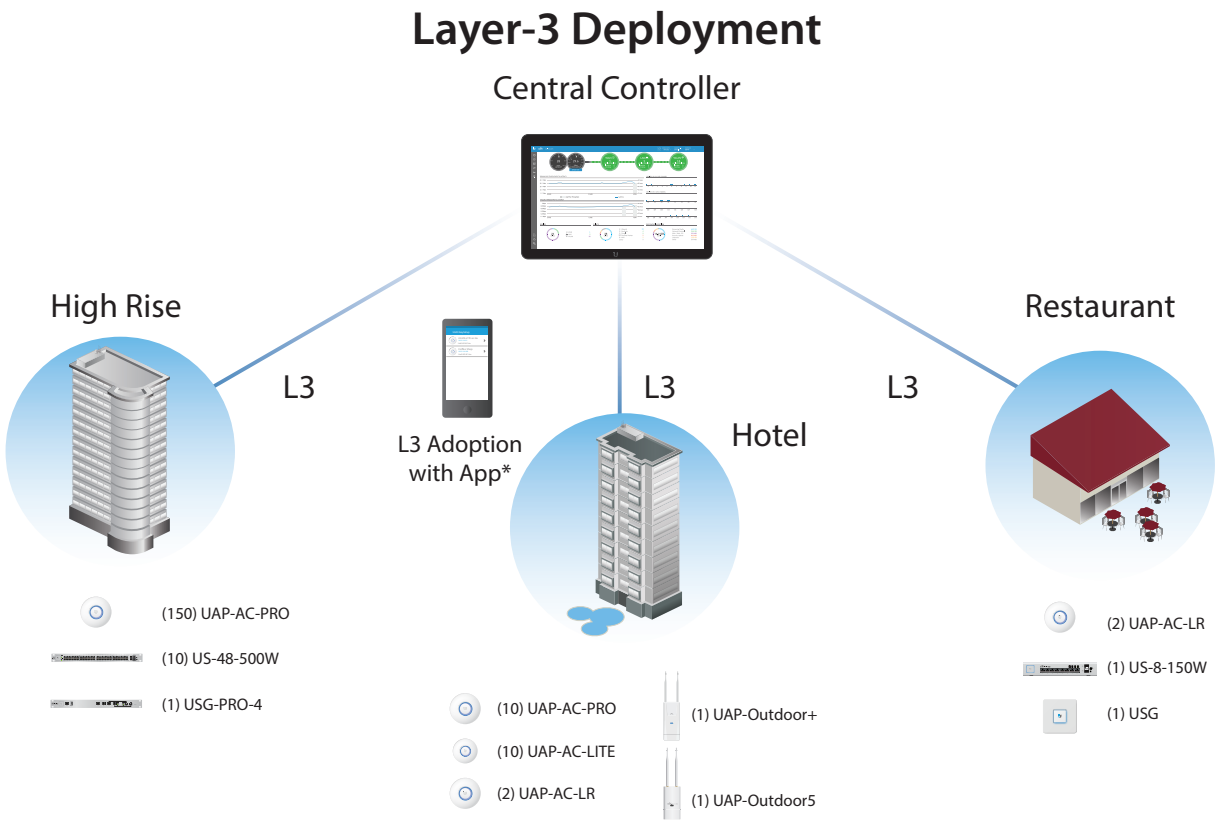
- **High rise** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.
- **Hotel** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.
- **Restaurant** The UniFi Controller is off-site. Use Layer-3 adoption to manage this site.

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 133**
   - **"DNS" on page 157**
   - **"DHCP Option 43" on page 157**
   - **"SSH" on page 158**

For details about Layer-3 adoption, go to **"Layer-3 Adoption" on page 156**.



* Refer to **"Layer-3 Adoption" on page 156** 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 156**.

- **Hotel** The UniFi Controller is running on a UniFi Cloud Key.
- **Restaurant** The UniFi Controller is running on a UniFi Cloud Key.

Remote Access

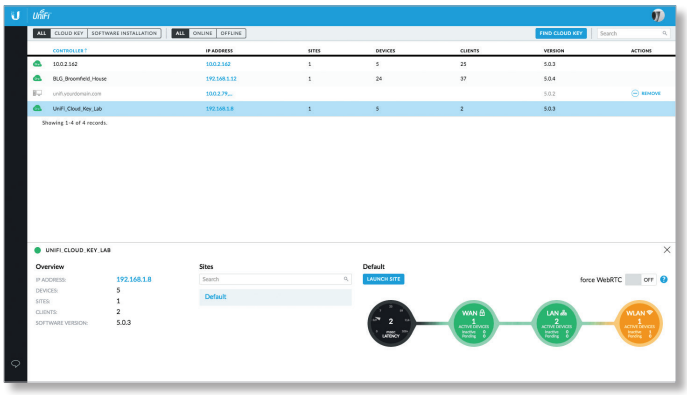
Cloud access is enabled on the UniFi Controllers, so you can use **unifi.ubnt.com** to remotely monitor and access multiple controllers. Each controller, in turn, can manage multiple sites.

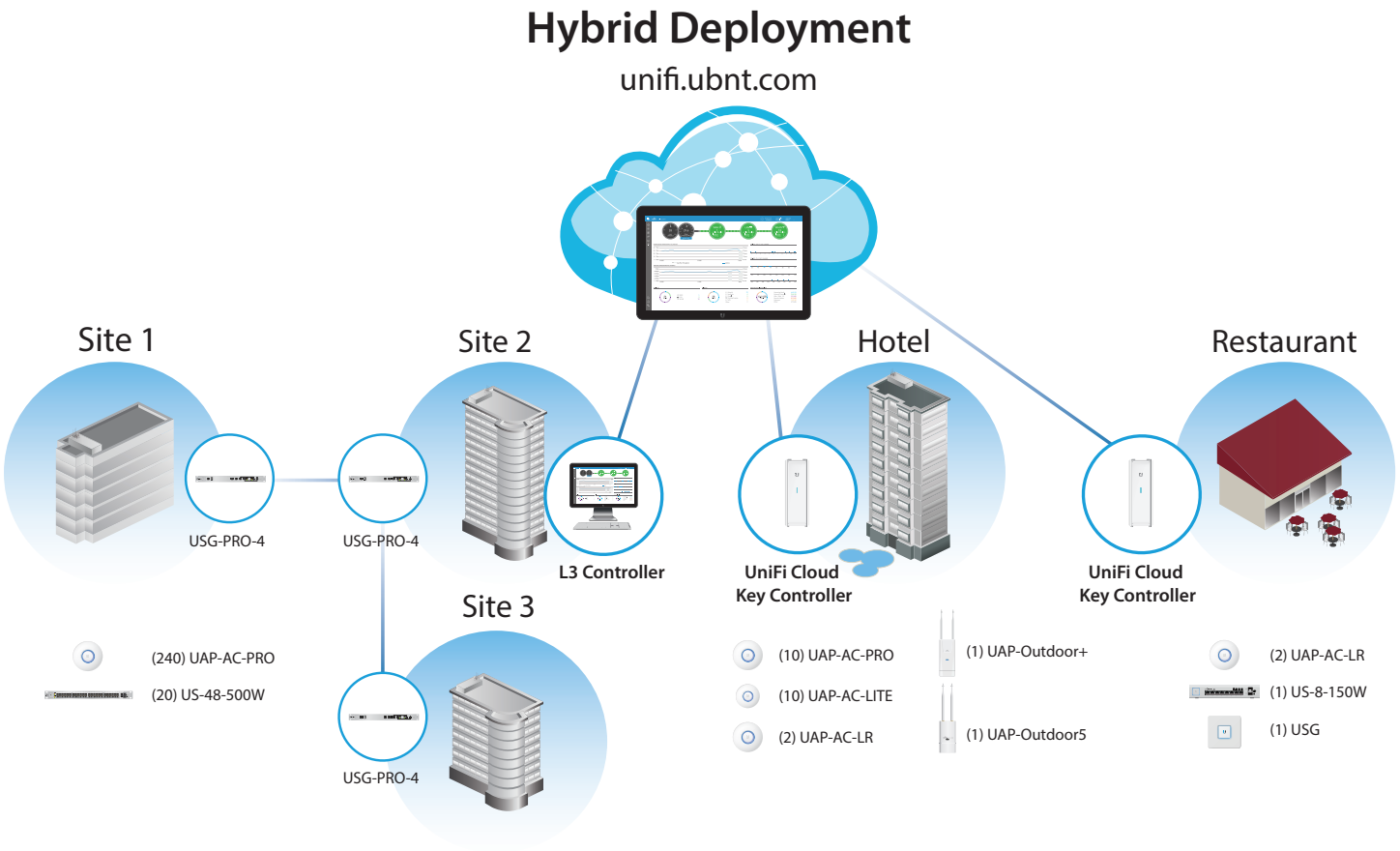
For example, in the application diagram below, you can use **unifi.ubnt.com** to access three controllers:

- 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*

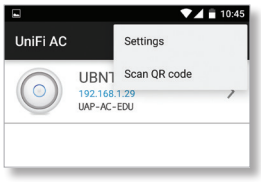
   Use one of the following methods to configure all local APs so they inform back to the UniFi Controller:

   - UniFi EasySetup App (see below)
   - UniFi Discovery Utility (see the next column)
   - **"DNS" on page 157**
   - **"DHCP Option 43" on page 157**
   - **"SSH" on page 158**

UniFi EasySetup App

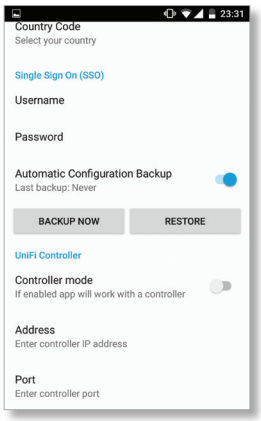
1. Launch the UniFi EasySetup App from your mobile device.

2. Tap **Settings**. If *Settings* is not displayed, then tap the *overflow* ⋮ icon in the upper-right corner, and then tap **Settings**.



3. Scroll down the *Setting* screen to view the *UniFi Controller* settings:

   - **Controller mode** Enable use of the UniFi EasySetup App with a UniFi Controller.
   - **Address** Enter the IP address of the UniFi Controller.
   - **Port** Enter the port number of the UniFi Controller.



For more information about the UniFi EasySetup App, refer to **"UniFi Mobile App" on page 133**.

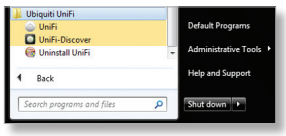
UniFi Discovery Utility

The UniFi Discovery Utility listens to the multicast and broadcast packets from UniFi APs and allows you to tell the UniFi AP to inform any URL you want. (Only APs in the default state or not in contact with any controller will be displayed).

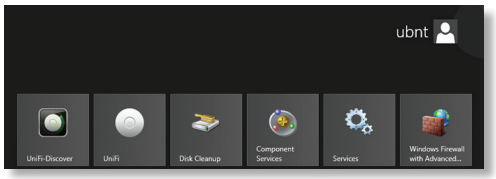
The UniFi Discovery Utility is installed alongside your UniFi Controller. Follow the instructions for the operating system you are using:

Mac Users From the Finder, click **Go** > **Applications** and double-click the *UniFi-Discover.app* icon.

PC Users For most versions of Windows, go to **Start** > **All Programs** > **Ubiquiti UniFi** and double-click the *UniFi-Discover* icon.



For other versions, including Windows 8, go to the *Start* menu and double-click the *UniFi-Discover* icon.

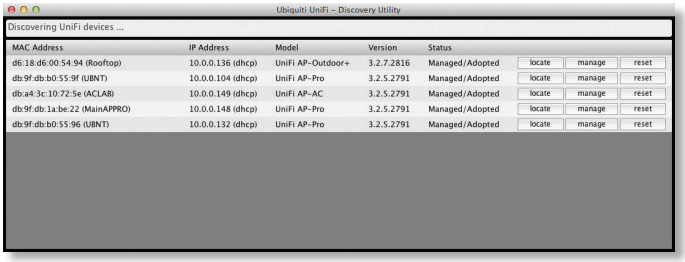


Linux Users Run the following command:

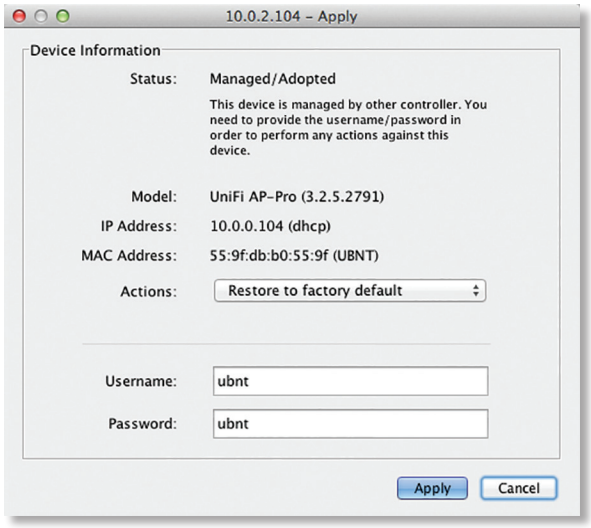
```
java -jar <unifi_base>/lib/ace.jar discover
```

To perform Layer-3 adoption with the UniFi Discovery Utility:

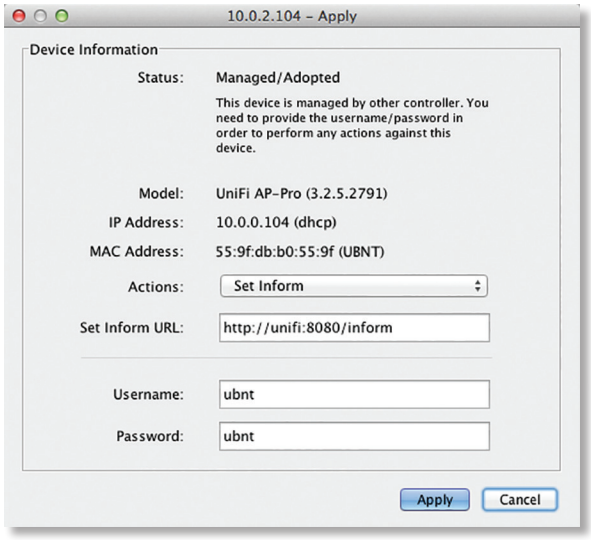
1. Wait for the UniFi AP to be displayed.



2. If the UniFi AP is not in the factory default state, then click **reset**. Enter the SSH username and password, and then click **Apply**.



3. Click **manage**.
4. Change the inform URL. The SSH username and password should be *ubnt/ubnt*. Click **Apply**.



5. Open a browser to the remote UniFi Controller. The UniFi AP should be displayed as *Pending Approval*.
6. Click **approve**. The UniFi AP will change to an *Adopting* state. Eventually it will change to an *Adoption Failed* or *Disconnected* state.
7. Perform step 3 again.

The UniFi AP is now managed by the UniFi Controller. Once adopted, the UniFi Controller will upgrade these APs automatically.

For more information about the UniFi Discovery Utility, refer to **"UniFi Discovery Utility" on page 129**.

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.

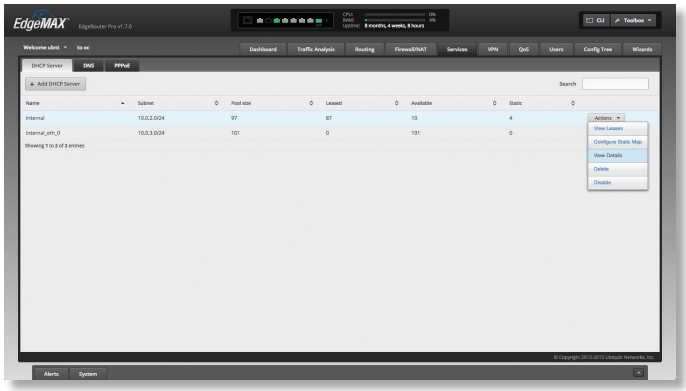
If the UniFi AP has been reset to its factory defaults, then ensure that you have informed the UniFi AP twice (using the UniFi Discovery Utility) about the location of the UniFi Controller.

DHCP Option 43

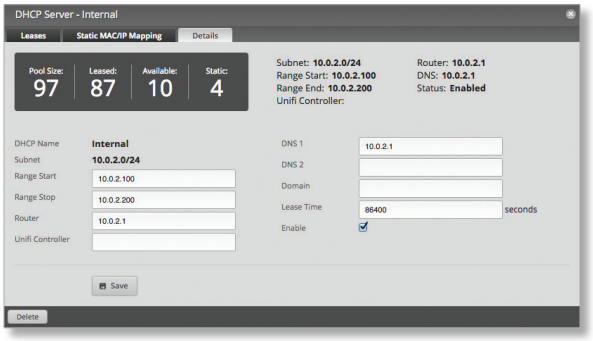
Instructions vary depending on the router you are using.

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 Discovery Utility 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 Discovery Utility 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 F: 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, New York 10017
www.ubnt.com

Online Resources

Support: **ubnt.link/UniFi-Support**

Community: **community.ubnt.com/unifi**

Downloads: **downloads.ubnt.com/unifi**

www.ubnt.com

© 2011-2017 Ubiquiti Networks, Inc. All rights reserved. Ubiquiti, Ubiquiti Networks, the Ubiquiti U logo, the Ubiquiti beam logo, and UniFi are trademarks or registered trademarks of Ubiquiti Networks, Inc. in the United States and in other countries. App Store is a service mark of Apple, Inc. Google, Android, and Google Play are trademarks of Google Inc. All other trademarks are the property of their respective owners.