

Enterprise Network Deployment Guide

Aerohive APs and Dell Switches



This guide describes the integration of Aerohive access points and Dell access switches and shows how to configure both types of devices through HiveManager NG.

It begins by summarizing the entire deployment process of a network in a typical enterprise environment, starting with planning, installing, and onboarding devices to bring them under HiveManager NG management. It then describes the configuration of a network policy and device-specific settings for Aerohive AP250 access points and Dell N1548P access switches plus the supplemental CLI commands required to complete the switch configuration. It next explains how to upload the network policy and device-level configurations to the devices. In conclusion, it provides three options for the creation of PPSK (private preshared key) user accounts for guests.

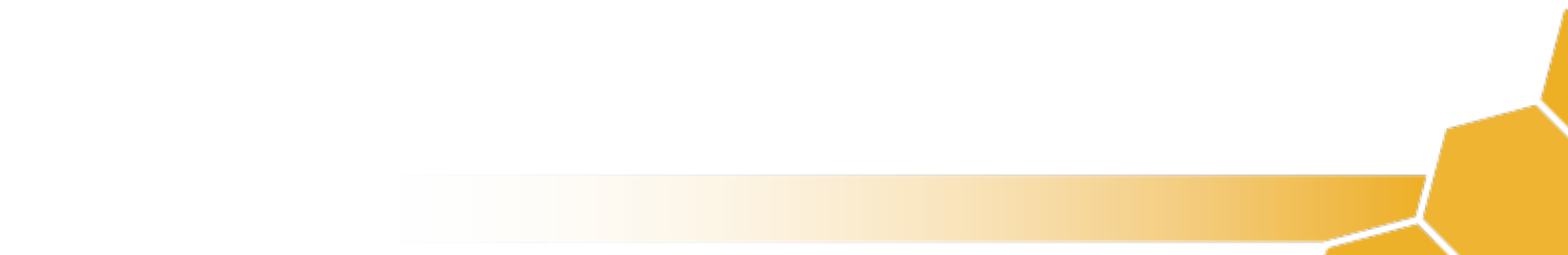
The configuration instructions in this guide are based on HiveManager NG 11.15.2.1.

Document Revision History

| Revision | Date | Notes |
|----------|------------|--|
| 01 | 10/17/2016 | Initial version |
| 02 | 11/2/2016 | A note was added explaining how to specify allowed VLANs on the AP250 uplink port. |
| 03 | 11/23/2016 | The explanation of user profile assignment rules was amended. |

Contents

- Introduction.....3
- Deployment Workflow4
- Planning the Deployment5
 - Dell Access Switches.....5
 - Aerohive Access Points6
- Connecting Devices to the Network7
 - Connecting Switches.....7
 - Connecting APs.....7
- Onboarding Devices.....9
 - Adding Switch Service Tags to HiveManager NG.....9
 - Adding AP Serial Numbers to HiveManager NG9
- Using Maps.....10
- Configuring a Network Policy.....12
 - Wireless Settings13
 - SSID for Employees.....13
 - SSID for Visitors16
 - AP250 Device Template18
 - Switch Settings19
 - Phone and Data Ports.....20
 - Access Ports.....21
 - Trunk Ports22
 - Uplink Ports.....23
 - Additional Settings24
 - DNS Settings.....24
 - Time Zone.....24
- Device-Specific Settings25
- Incorporating Supplemental CLI Commands26
- Uploading Device Configurations27
- Guest Management Administrators28
 - Creating Guest Management Administrators.....28
 - Creating Visitor PPSKs.....29
 - Built-in PPSK Creation.....29
 - Aerohive Guest Check-in Web App30
 - Aerohive iPad Kiosk App.....32

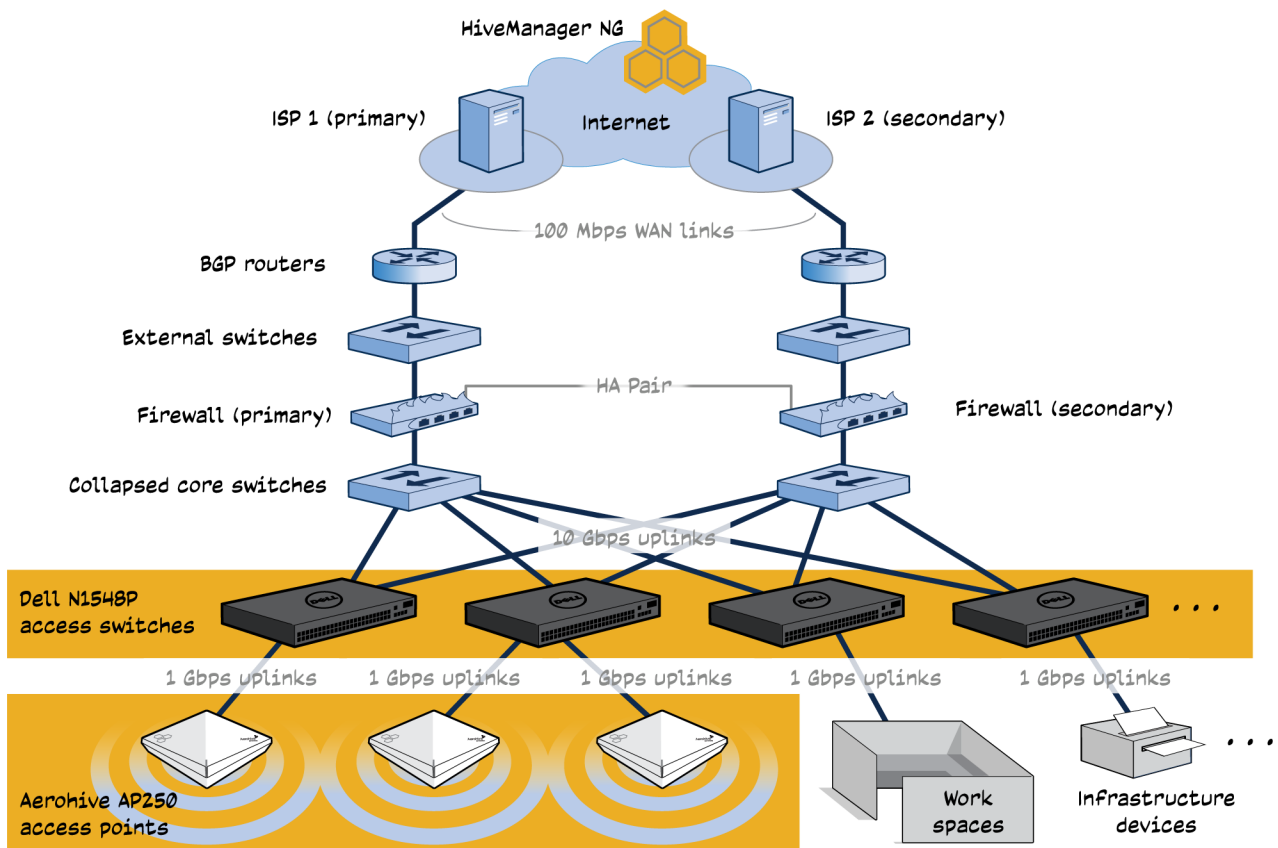


Introduction

This guide covers the planning, deployment, and configuration of an enterprise network consisting of Aerohive access points and Dell switches, both managed by HiveManager. Other devices in the network, such as the firewall, RADIUS server, Active Directory domain controller, and so on will be mentioned but not discussed in detail. The goal here is to provide an overview of the main network components in broad strokes and examine key Aerohive AP and Dell switch configuration points in greater depth.

The following network diagram shows how the APs and switches are deployed in relation to other parts of the network. At the edge of the network is a firewall in an HA pair with links to two ISPs. One ISP is the primary and the other is secondary, each with a 100 Mbps link that passes through an external switch and BGP router.

Behind the firewall are two collapsed core switches; that is, the core and distribution layers are consolidated into a single core/distribution layer. They have eight 10-Gbps ports to which Dell N1548P PoE access switches connect through 10-Gbps SFP+ uplinks. All Aerohive AP250 access points, work spaces, and infrastructure devices like printers connect to the access switches over 1-Gbps uplinks.






The wireless and wired network access devices—Aerohive APs and Dell access switches—are managed and monitored through HiveManager NG. You can upload any switch settings that are not yet available in the HiveManager NG GUI to the switches through the supplemental CLI feature.

Deployment Workflow

The following steps outline the main components in the deployment workflow: planning, installing physical devices, onboarding switches and APs into your HiveManager NG account, and configuring them.

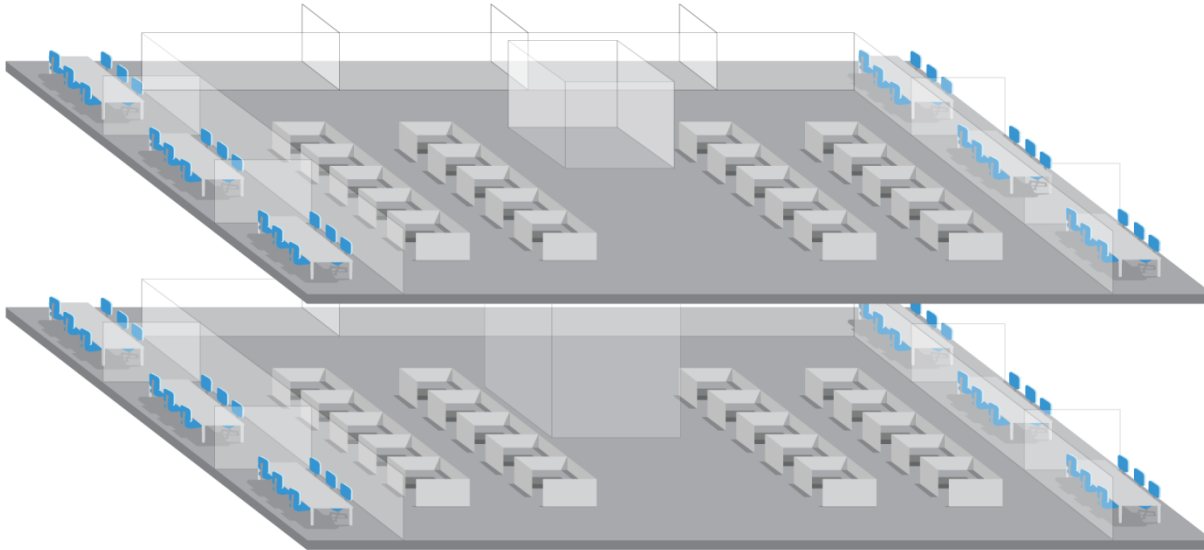
1. Create a plan that provides adequate coverage and capacity for users on the wireless and wired network.
2. If they are not yet in place, set up the core components of the network: BGP routers, external switches, firewall, collapsed core switches, and other devices in the MDF (DNS server, DHCP server, SIP controller, and so on).
3. Rack mount the switches, note their positions in the IDF or MDF and rack—tracking them by service tag number—and connect them to the collapsed core switches.

Note: Dell switches ship preconfigured with HiveAgent, an embedded Aerohive application that looks up cloud-rd.aerohive.com to find its HiveManager NG instance and automatically connects to it using HTTPS.

4. Mount the APs, track their locations, run their cables to the IDF and MDF, and connect them to the access switches. One option for tracking APs is to write the location of each one on its cardboard box, which also contains its serial number printed on a label.
5. Log in to your HiveManager instance and add the Aerohive AP serial numbers and Dell switch service tags by clicking  > **Onboard Devices > Add Real Devices**.
6. After adding the devices, HiveManager NG displays the MONITOR > Devices page. Referring to your notes, AP serial numbers, and switch service tag numbers, rename the devices on that page, giving them meaningful host names based on their locations. (If you already did this for switches through the CLI earlier, then you only need to do this for APs now.)
7. Create maps in the *Plan* section of the GUI and place the device icons on maps.
8. Create a unified network policy for both access points and switches, including a supplemental CLI object to configure certain switch features that are not yet available in HiveManager NG.
9. Assign the network policy to all your APs and switches.
10. Apply the supplemental CLI to the eight switches by selecting the check boxes for all eight of them on the MONITOR > Devices page and then clicking the **Edit** icon . In the *Supplemental CLI* section of the *Modify (Multiple): Device Configuration* dialog box that appears, select **Override Supplemental CLI in the network policy**, clear **[-No Change-]**, click the **Select** icon , choose the supplemental CLI object you created, and then click **Save**.
11. Because the AP250 device template enables both 5 GHz radios on all the APs, manually enable the 2.4 GHz radio in the device-level settings for roughly every third AP.
12. Upload the network policy and device-level settings to the APs.
13. After you have successfully updated all the APs, upload the network policy, device-level settings, and supplemental CLI object to the switches.
14. Connect workspaces and infrastructure devices to the access switch ports.
15. Test various types of wired and wireless clients and monitor the clients in HiveManager NG.

Planning the Deployment

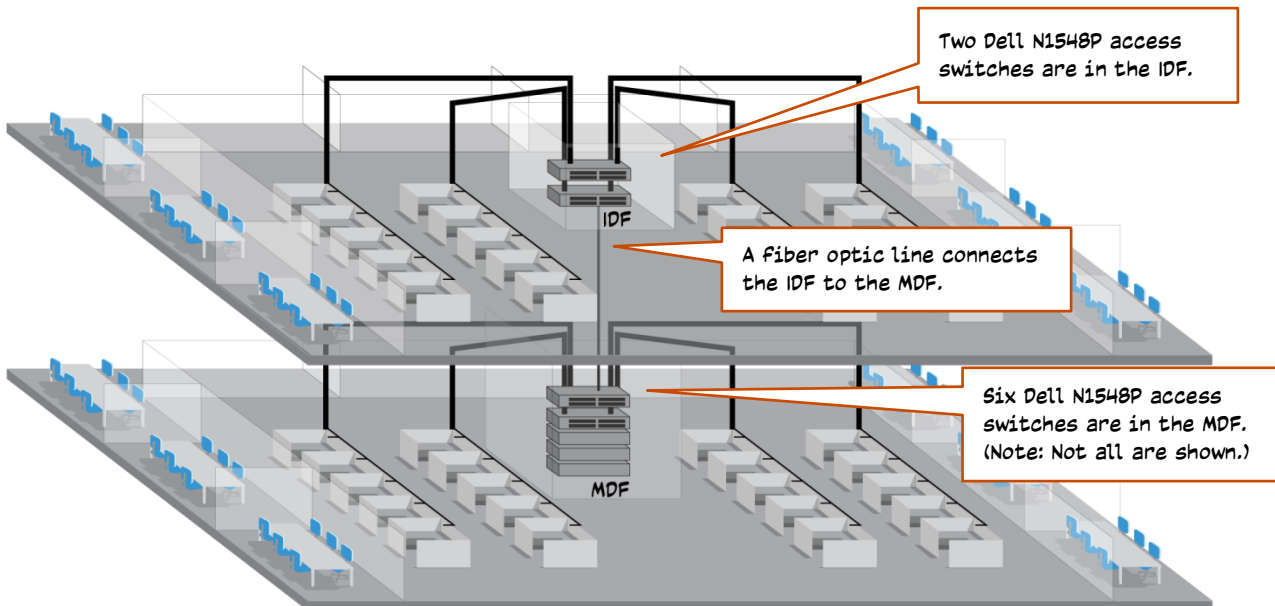
Imagine that the building has two floors and consists primarily of a combination of cubicles, offices, and conference rooms. Here is a highly simplified diagram showing a section of such a space:



By performing predictive and manual site surveys, you can determine the number of access points and access switches to use. Assume, for example, that the area is approximately 70,000 square feet (6500 square meters) and there are approximately 300 users (employees and guests). Your plan provides wired access for approximately 300 laptops and wireless access for approximately 600 devices (laptops and smart devices) through a deployment of 26 AP250 devices and 8 Dell N1548P access switches.

Dell Access Switches

There are two wiring closets with the MDF (main distribution frame) on the first floor and an IDF (intermediate distribution frame) on the second floor. On the second floor 80 cubicles and offices have Ethernet connections to two 48-port Dell switches in the IDF, which also has a UPS (universal power supply, and a fiber optic connection to the MDF. On the first floor, 200 cubicles and offices have Ethernet connections to six 48-port Dell switches in the MDF. Each access switch has two 10-Gbps uplinks to the collapsed core switches, which are also in the MDF.



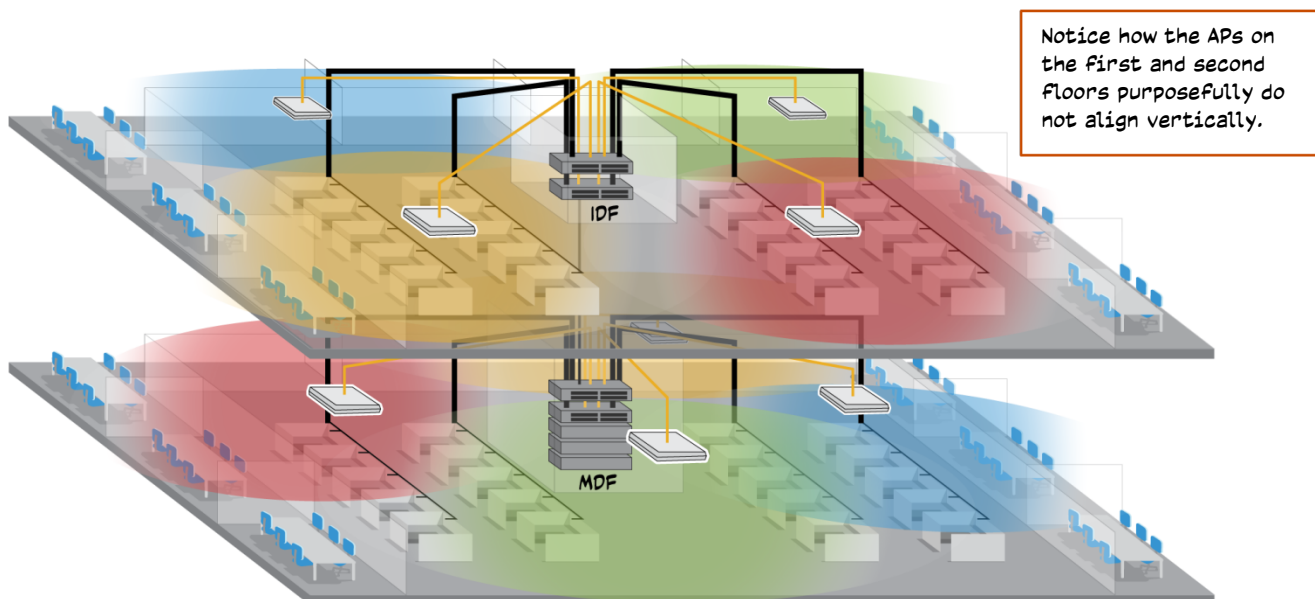
The following is a list of devices in the MDF:

- 6 access switches
- 2 collapsed core switches
- 2 firewalls in an HA pair
- 2 external switches
- 2 BGP routers each linking to a different ISP
- 1 SIP trunk controller for phone service
- 1 RADIUS server
- 1 DHCP server
- 1 DNS server
- 1 Active Directory domain controller
- 1 MAC mini for Apple updates
- Multiple UPS systems (1 UPS per two racks of access switches and 1 UPS per rack for core switches)

Aerohive Access Points

Beginning with the HiveManager NG planning tool, make a predictive site survey for AP250s. Plan for the 5 GHz band as the primary means of client access. Enable the 2.4 GHz radio for client access on every third AP or so and use dual 5 GHz radios on all the other AP250 devices. Then go on site and perform a manual site survey to confirm the predicted AP placements and adjust them as necessary based on real RF signals in the actual environment.

When positioning the APs, strive to arrange them in a sawtooth pattern both horizontally (on the same floor) and vertically (on adjacent floors). This helps reduce CCI (cochannel interference) and ACI (adjacent channel interference) from the signals coming through the flooring from APs on different floors. The following illustration shows a sample where the different colored ovals indicate radio cells on different channels.



Connecting Devices to the Network

Aerohive APs and Dell switches that integrate with HiveManager NG have an automatic mechanism for discovering and connecting to HiveManager NG when they boot up and gain network access. Dell switches run an embedded application called HiveAgent that establishes a connection with HiveManager NG over HTTPS (TCP port 443). Aerohive APs use CAPWAP (UDP port 12222) or, if UDP port 12222 is blocked, HTTP (TCP port 80). Both device types use HTTPS (TCP port 443) to download new firmware image files, certificates, graphics for captive web portals, and full configurations. For these devices to communicate with HiveManager NG, make sure that the external firewall permits outbound HTTPS, CAPWAP, and HTTP traffic.

Connecting Switches

Rack mount two Dell N1548P switches in the IDF and six in the MDF. Connect their SFP/SFP+ ports to two collapsed core switches for redundancy and then connect them to a power source.

Note: RSTP (Rapid Spanning Tree Protocol) is enabled on Dell switches by default to prevent loops.

Note the position of each switch in the IDF or MDF and its rack. You can track Dell switches in HiveManager NG by their service tag number, which you can see from the CLI of each switch. While logged in to a switch, you can also change its host name, which you can do through HiveManager NG too. After logging in, here are the commands to see the system ID and set a host name:

*Note: The default login name is `admin`; there is no default password. After entering `admin` for the login name, simply press the **ENTER** key on your keyboard instead of entering a password.*

```
#show system id
#config
(config)# hostname <hostname>
(config)# exit
#write
```

When a Dell switch goes online, it first gets its network settings through DHCP unless you have already preconfigured it with static network settings. Then the HiveAgent application uses HTTPS to contact an Aerohive redirection server at `cloud-rd.aerohive.com` to look up the HiveManager NG account to which it is assigned. HiveAgent submits the service tag number for the switch, and the redirector checks its database to find where to redirect it. At this point, the redirector will not find a match because the service tag has not yet been associated with your HiveManager NG account. HiveAgent will continue checking until the redirector replies, redirecting it to a master server in a data center hosting the HiveManager NG instance. The master server then links the switch to a specific host server and from that point on, the switch communicates directly via HTTPS with the HiveManager NG instance on that hosted server.

Connecting APs

Mount the Aerohive AP250 devices on walls and ceilings as determined through your site surveys. Run Ethernet cables from their Eth0 ports to ports 1/0/41-45 on the eight switches in the IDF and MDF. When two APs in the same area provide overlapping radio coverage, try to connect them to different switches from one another. In this way, if one switch temporarily goes offline for maintenance or some other reason, the AP connected to the other switch will continue to function and provide wireless access to client devices in their area. The switches automatically power the APs through PoE, so there is no need to connect the APs to a separate power supply.

When an Aerohive AP goes online, it first gets its network settings through DHCP—unless it is manually configured with static settings—and it then starts a CAPWAP search for HiveManager. It first checks if it has manually defined CAPWAP settings or if it automatically received them through DHCP. If not, it next broadcasts CAPWAP Discovery Request messages in search of a local HiveManager appliance. If it does not receive a response, it sends unicast CAPWAP Discovery Request messages to `redirector.aerohive.com`. The redirector checks if the device serial

number is in its database. Because you have not yet added the serial number of the AP to your HiveManager NG instance, it will not be in the database. The AP will keep checking until the redirector replies and redirects the AP to the HiveManager NG instance to which it belongs and to the server hosting that instance. From that point, the AP communicates directly via CAPWAP with the HiveManager NG instance on that hosted server.

Connecting Devices to HiveManager NG Virtual Appliance

If you are using HiveManager NG Virtual Appliance on-premises, you must inform your devices about its IP address or domain name. You can accomplish this through one of the following methods:

DNS Server

One of the easiest methods for a device to locate its on-premises HiveManager NG instance is to use DNS. Configure an A record on the authoritative DNS server for your network mapping "hivemanager" to an IP address:

```
hivemanager IN A <ip_addr>
```

The device learns its domain from DHCP and appends it to "hivemanager". For example: `hivemanager.yourdomain.com`

DHCP Options

Another option is to configure your DHCP server with DHCP vendor class option 43, sub-option 225 or 226, where 225 is the domain name of HiveManager NG, and 226 is its IP address. For a more detailed explanation, including how to configure these options on Linux- and Windows-based DHCP servers, see [HiveManager NG Discovery through DHCP](#).

CLI Commands

If you do not have access to the DNS or DHCP server, log in to devices and enter the following commands.

Dell Switches

```
(config)# hiveagent
(config-hiveagent)# server HMNG-VA
(config-hiveagent-HMNG-VA)# url { <ip_addr> | <domain_name> }
(config-hiveagent-HMNG-VA)# exit
(config-hiveagent)# exit
(config)# write
```

If your switches access HiveManager NG through an HTTP proxy, enter the following command from within the HiveAgent server configuration:

```
(config-hiveagent-HMNG-VA)# proxy-ip-address <ip_addr> port <number> username <name>
password <password>
```

Aerohive AP

```
# capwap client server name { <ip_addr> | <domain> }
# save config
```

If your APs access HiveManager NG through an HTTP proxy, enter the following commands:

```
# capwap client http proxy name { <ip_addr> | <domain> } port <number>
# capwap client http proxy user <name> password <password>
```



Onboarding Devices

At this point in the deployment process, all the devices are on the network but they are not yet under HiveManager management and are still unconfigured. The onboarding process involves entering service tag numbers for Dell switches and serial numbers for Aerohive access points to your account so that the redirector and HiveManager NG can direct them to the correct data center and server hosting your HiveManager NG instance.

Adding Switch Service Tags to HiveManager NG

After installing the Dell switches and noting their service tag numbers, you can either type those serial number directly into HiveManager NG or you can gather them in a .csv file and import that file into HiveManager NG.


To add service tag numbers for Dell switches:

1. In the menu bar at the top of the HiveManager NG GUI, click  > **Onboard Devices**.
2. On the *Add Devices* page, click **Add Real Devices**.
3. Enter the 7-digit service tag numbers for your Dell switches separated by commas or click **Choose** next to the field below "Do you have other devices to add?", navigate to the .csv file, and select it. Optionally, you can select the .csv file and drag it onto the field.
4. Click **Next** to advance to the next page, select **Use an existing network policy** but do not choose anything from the drop-down list, and then click **Next**.
5. Click **Finish**.

Adding AP Serial Numbers to HiveManager NG

When you order Aerohive APs, you receive a list of serial numbers in a .csv file. You must associate those serial numbers with your HiveManager NG account. You can enter them individually or enter them in bulk by importing the .csv file into HiveManager NG.

To add serial numbers for Aerohive APs:

1. In the menu bar at the top of the HiveManager NG GUI, click  > **Onboard Devices**.
2. On the *Add Devices* page, click **Add Real Devices**.
3. Enter the 14-digit serial numbers for your Aerohive APs separated by commas or click **Choose** next to the field below "Please enter the serial numbers of your Aerohive devices", navigate to the .csv file, and select it. Optionally, you can select the .csv file and drag it onto the field.
4. Click **Next** to advance to the next page, select **Use an existing network policy** but do not choose anything from the drop-down list, and then click **Next**.
5. Click **Finish**.

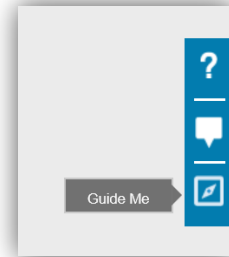
Using Maps

Creating maps is beneficial for both APs and switches. You can use maps for APs to help determine how many APs you need and where to mount them. For switches, there are no planning tools needed for coverage, but maps are still beneficial for specifying the location of switches so to assign switch templates and other configuration objects by location and for filtering data shown in the dashboards and reports based on location.

Before you begin, Aerohive recommends that you already have the following items:

- Building addresses
- An idea of the materials used for walls, floors, and other structures throughout the building
- Floorplans in .png or .jpg format

Note: If you do not have the building floorplan, you can use the Aerohive planner tool to create an estimate using the integrated Google maps functionality. You can use the building address to pull up a Google map and create a perimeter by tracing the building with the drawing tool in the planner. Once you create the perimeter, the planner can calculate the building size. There is a GuideMe option in the interface that guides you through the whole map integration process step by step.

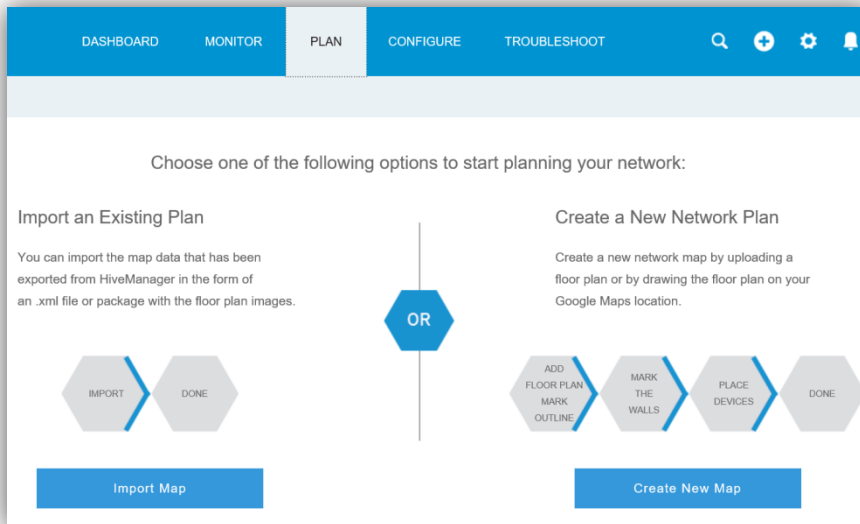


After you gather the items listed above, create planner buildings and floors as described below.

You have the option to upload a floorplan in the form of a .jpg or .png image, import complete plans from another HiveManager, or create floorplans by drawing perimeters around buildings located in an embedded Google map. This example explains how to import existing .jpg images to create floorplans. For detailed instructions, please view the Help topic [Creating a Network Plan](#), or click **PLAN** and then click **?** to access the context-sensitive online Help.

To create an initial topology map:

1. Click **PLAN > Create New Map**, enter the requested organization name and address, and then click **Get Started**.



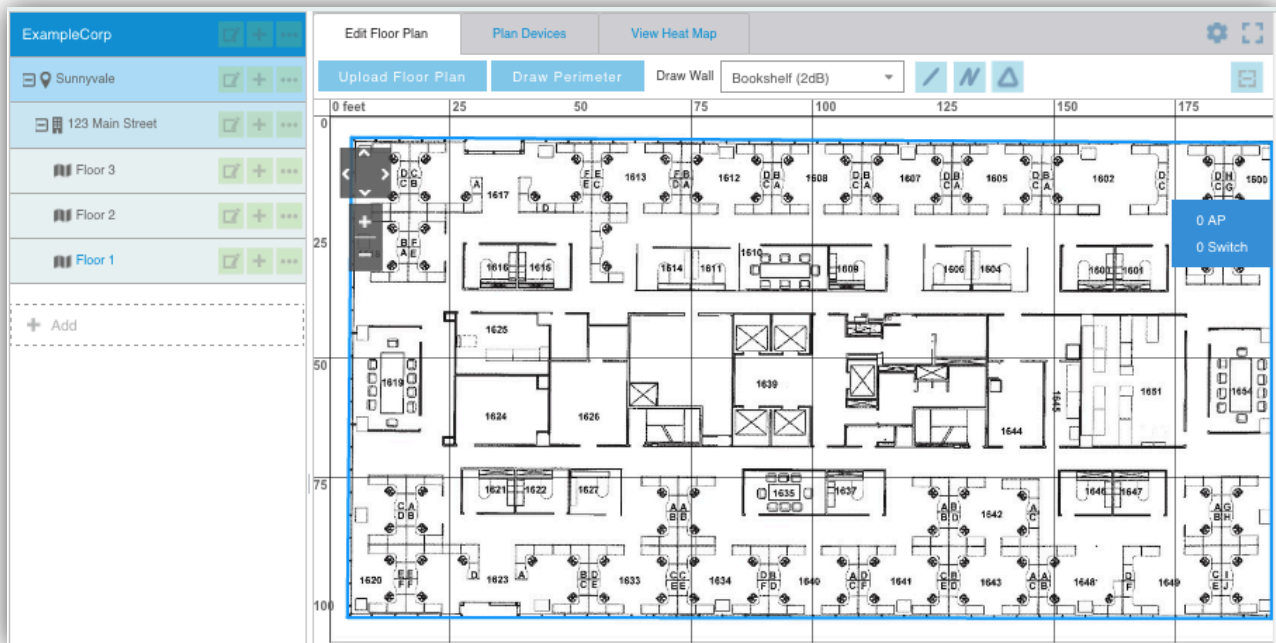
2. Select the location on the left navigation bar, click **Upload Floor Plan > Choose from Library > Upload New from Computer > Choose**, browse to a .jpg or .png image of a floorplan, and then click **Open**.
3. Click **Upload** and then choose either **Save a Selected Area** (and select a specific area of the file to use as the floorplan) or **Save All** (to use the complete file).

4. Click **Choose > Size Floor Plan** and specify a width and height in meters or feet. You can also manually set the size of the floorplan by dragging crosshairs on the screen to mark the edges of a wall, doorway, or something else of a known size. Using the measurement of a larger area, such as the width of a conference room, will be more accurate than that of a smaller one, such as the width of a door. This is because any error will not be magnified proportionally as much when calculating the size of the entire map from the sample measurement.
5. Draw a perimeter around the floor by clicking **Edit Floor Plan>Draw Perimeter**.

Note: If you want to adjust the perimeter, you can click the [-] symbol in the upper-right corner of the drawing area to remove all walls and start again.

6. Add walls, which will be useful for the AP deployment.
7. If you want to clone the floor, or building, you can click the ellipses (...) to the right of the floor or building and then click the **Clone** icon with two squares (■ ■).
8. After you create the floors, you can assign APs and switches to them. The easiest way to do that is from the Actions menu on the *Devices* page in the *MONITOR* section.

The following picture shows an example building with three floors. When adding switches and APs, you can assign them to the appropriate building and floor.



By creating maps, you automatically create a filter context of locations, buildings, and floors that you can use in the dashboard, device configuration and monitoring page, and client monitoring page for ease of access to pertinent data.

Configuring a Network Policy

Through HiveManager NG, you can create a unified network policy for both Aerohive APs and Dell switches. Although the policy applies to both types of devices, HiveManager uploads AP-specific settings just to APs and switch-specific settings just to switches.

1. Log in to your HiveManager NG account and create a new network policy that supports wireless and switching as follows:
2. Click **Configure > Add Network Policy**, enter the following in the *New Policy* panel, and then click **Next**:

Wireless: (select to make wireless settings available in the policy; selected by default)

Switches: (select to make switch settings available; selected by default)

Spanning Tree Protocol: Toggle **ON** to enable RSTP (Rapid Spanning Tree Protocol) on all switch ports.

*Note: You can later check that RSTP is enabled within the network policy by clicking **Additional Settings > Switch Settings > STP Configurations**.*

Policy Name: Enter a name for the policy. It can be up to 32 characters long and cannot have any spaces.

Description: Enter a useful reference note. It can be up to 64 characters long including spaces.

This creates a sort of container for all the settings you will configure for your devices. Suggested settings for your Aerohive access points are explained in the next section and those for your Dell switches following that.

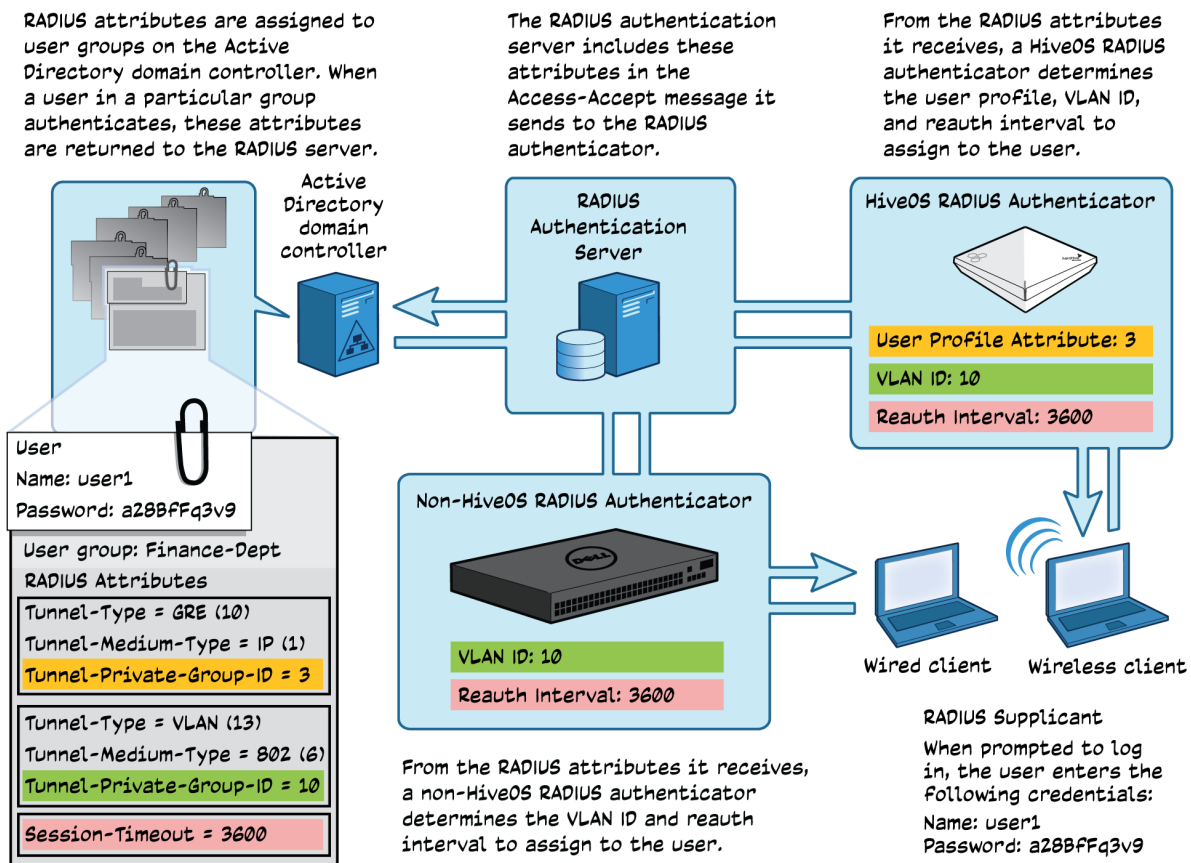
Wireless Settings

Using no more than three SSIDs helps reduce the amount of management overhead, which can have a serious impact on performance, as shown in the [Wi-Fi SSID Overhead Calculator](#) created by Andrew von Nagy. In this section, you configure two SSIDs and one device template for your AP250 devices.

SSID for Employees

User entries for employees are stored on an Active Directory domain controller. When wireless clients authenticate, the RADIUS attributes that accompany the Access-Accept message from the authentication server indicate which user profile, VLAN, and reauth interval to assign. Wired clients connecting to a port configured for 802.1X authentication on a non-HiveOS switch are not assigned a user profile (because that is a HiveOS construct) but they are assigned the same VLAN and reauth interval as those assigned to wireless clients.

The set of three attributes that indicate a user profile, the set of three attributes that indicate a VLAN, and the attribute that indicates the reauth interval are shown in the illustration below.

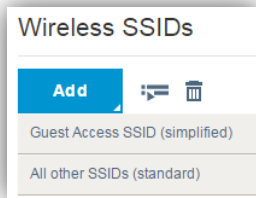


If the user group on the domain controller and the user profile on the HiveOS RADIUS authenticator both specify a VLAN ID, the Aerohive device applies the one defined in the user group. It only applies a VLAN ID defined in a user profile when RADIUS attributes do not indicate one.

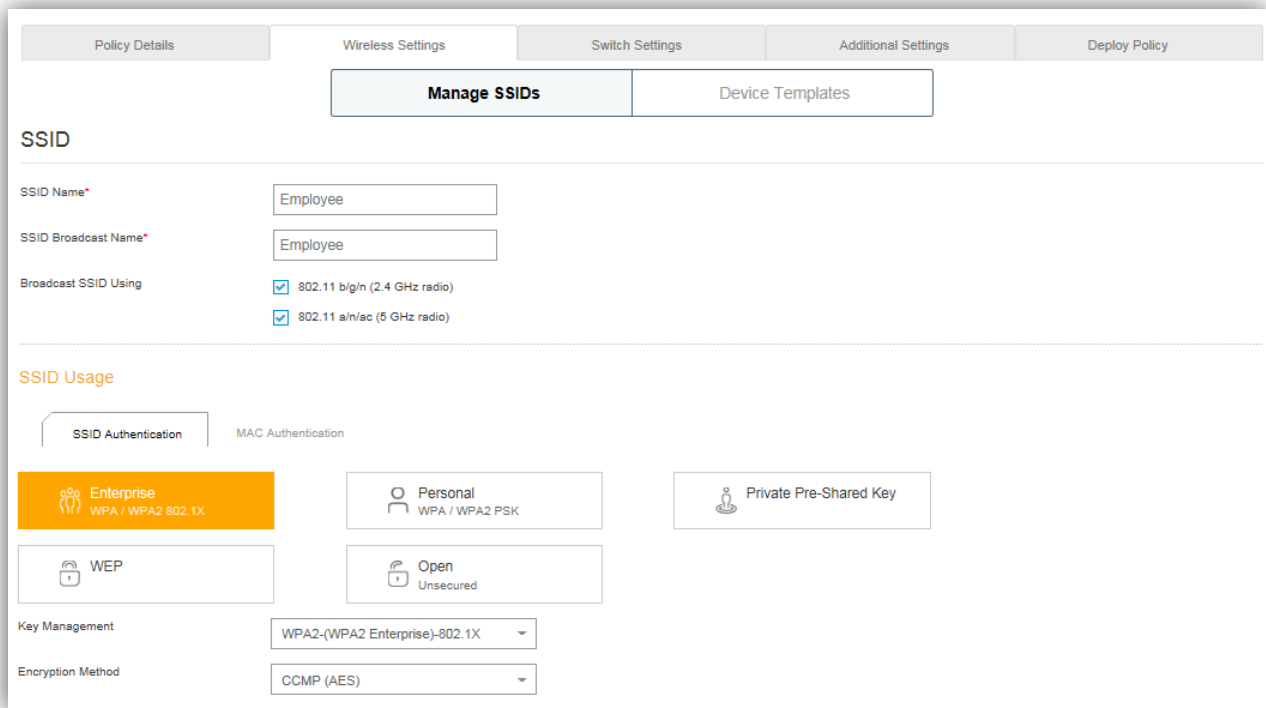
If the user's authentication attempt is unsuccessful or if the returned attributes for an authenticated user do not match any user profile associated with the SSID, the HiveOS RADIUS authenticator denies access to the network.

If the authentication attempt is successful and there is no set of attributes indicating a user profile, the HiveOS RADIUS authenticator applies the default user profile for the SSID to that user's traffic.

1. Click **Add > All other SSIDs (standard)**.



2. Create an 802.1X SSID that requires employees to authenticate against the RADIUS server in the MDF.



3. In the *Authentication Settings* section, click **+** next to Default RADIUS Server Group.

Configure RADIUS Server Group

4. In the *Configure RADIUS Server Group* dialog box that appears, enter a name for the group of servers, such as **Corp-RADIUS-Group**, and then click **Add > External RADIUS Server**. This choice indicates that the RADIUS server group will consist of one or more third-party RADIUS servers.

There can be up to four RADIUS servers in a group, their position in the *RADIUS Server Group* dialog box indicating their priority: top=primary, second from the top=backup-1, third from the top=backup-2, and bottom=backup-3. In this example, the group consists of just one server.

External RADIUS Server

5. In the *External RADIUS Server* dialog box, enter a name for the external RADIUS server and a useful description for later reference. For IP Address/Host Name click **+ > IP Address**.

New IP Address or Host Name

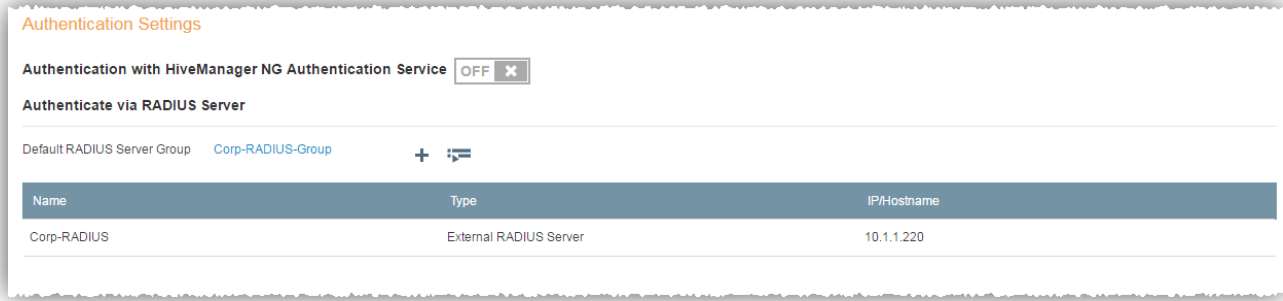
6. In the *New IP Address or Host Name* dialog box, enter a name for the IP address object and the IP address itself and then click **Save**.

External RADIUS Server

7. Back in the *External RADIUS Server* dialog box, choose the IP address object you just defined, enter the same shared secret as that on the RADIUS server, and then click **Save**.

Configure RADIUS Server Group

8. To save the RADIUS server group and close its dialog box, click **Save**.



SSID

9. In the *User Access Settings* section, click **+** next to Default User Profile.

Create User Profile

10. Create a user profile that APs will apply to users that successfully authenticate against the RADIUS server and either the RADIUS server does not return any attributes assigning them to another user profile or it returns attributes assigning them to the default user profile.
11. Create other user profiles for people in different corporate departments. User groups in the Active Directory domain controller are configured to return RADIUS attributes that assign users to user profiles and VLANs and specify how long they remain authenticated before having to reauthenticate. This has several benefits. You can assign different user groups different firewall and QoS policies, availability schedules, SLA levels and actions, and traffic limits based on data or time. This approach also keeps broadcast domains small to limit broadcast and multicast traffic to reasonable levels so that they do not negatively affect overall network performance.

User Profile Assignment Rules

In addition to assigning user profiles based on returned RADIUS attributes, you can also create rules that assign user profiles if clients match one of the following attributes:

Operating system – You might assign one user profile to laptops and another to handhelds.

MAC addresses or OUIs – You might assign a different user profile to corporate-issued client devices that you can identify because you already have a list of their MAC addresses or OUIs.

Location – (Locations are defined by maps in the planner.) For example, if a college campus has multiple buildings, you can assign faculty members a user profile in their own department building that differs from what they get elsewhere.

Schedule – You might give users different types of access at different times, such as one user profile for students during school hours and another one for after school and weekends.

If you use more than one assignment rule, APs assign the user profile in the first rule that matches in descending order. For example, imagine three rules based on RADIUS attributes, client OS, and a schedule and organized in that order from the top. APs first attempt to assign the user profile linked to the top rule if returned RADIUS attributes match those specified in the rule. If not, they attempt to assign the user profile linked to the OS specified in the second rule if that is what the client device is running. If not, they attempt to assign the user profile in the third rule if a user initiated network access while the schedule specified in that rule was in effect. If none of the rules match, then APs assign the default user profile. With this rich set of options, you have very granular control over user profile assignments.

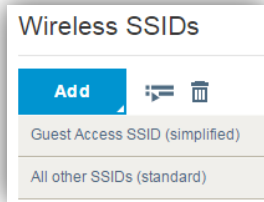
12. Save each user profile you create and then save the Employee SSID.

SSID for Visitors

Create a secure SSID that requires visitors to enter a PPSK and then accept a use policy agreement on a captive web portal before gaining Internet access. People defined as guest management administrators generate and distribute PPSKs to visitors as needed. They can be people who greet guests in the reception area as well as employees who frequently meet with visitors who require Internet access while on site.

Note: To learn how to create guest management accounts, see [Guest Management Administrators on p. 28](#).

1. Click **Add > All other SSIDs (standard)**.



Note: The 11.15.2.1 HiveManager NG release introduces a new, simplified workflow for configuring guest access SSIDs. Although the simplified workflow streamlines the configuration of a guest SSID, it does not support the creation of both a captive web portal and PPSK groups as described here. A standard workflow must be used.

2. Add a PPSK SSID to the network policy.

SSID

SSID Name*

SSID Broadcast Name*

Broadcast SSID Using

- 802.11 b/g/n (2.4 GHz radio)
- 802.11 a/n/ac (5 GHz radio)

SSID Usage

SSID Authentication

MAC Authentication

Enterprise
WPA / WPA2 802.1X

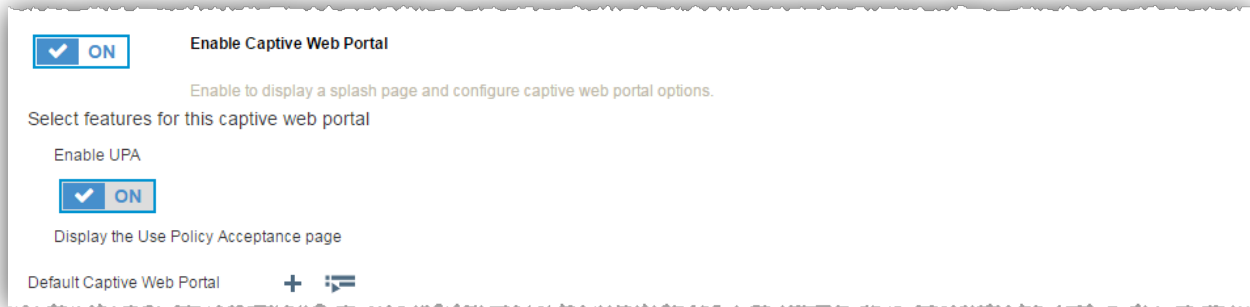
Personal
WPA / WPA2 PSK

Private Pre-Shared Key

WEP

Open
Unsecured

3. Enable a captive web portal that requires visitors to accept a network use policy, and then click **+** next to Default Captive Web Portal to create one for the SSID.



New Captive Web Portal

4. In the *New Captive Web Portal* panel that appears, enter the following, leave the other settings at their default values, and then click **Save**:

Name: Corp-Visitor

Redirect clients after a successful login attempt: (select)

To the initial page: (select)

SSID

5. In the *Authentication Settings* section, click **Add** to add a PPSK user group for which keys are valid for 24 hours.

New User Group

6. In the *New User Group* panel that appears, enter the following, leave other settings at their default values, and then click **Save**:

User Group Name: 1Day

Password DB Location: SERVICE (This stores the PPSKs in the cloud rather than on local Aerohive APs.)

Generate Password Using: Letters, Numbers

Account Expiration: Valid for time period in 24 hours after First Login

Access key must be used within 7 days

Deliver Access Key by:

Text Messages (SMS): (select); **Default PPSK SMS Template**

Email: (select); **Default PPSK Email Template**

Note: These are default SMS and email templates that determine the appearance of the notification message that the visitor sees when receiving a PPSK. If you want to customize the notification, you can create new templates on the CONFIGURE > Common Objects > BASIC > Notification Templates page.

SSID

7. In the *Authentication Settings* section, click **Add** to add a PPSK user group with keys valid for seven days.
8. In the *User Access Settings* section, click **+** to add a user profile limiting visitors to Internet access only over an exclusive VLAN for guests.


Create User Profile

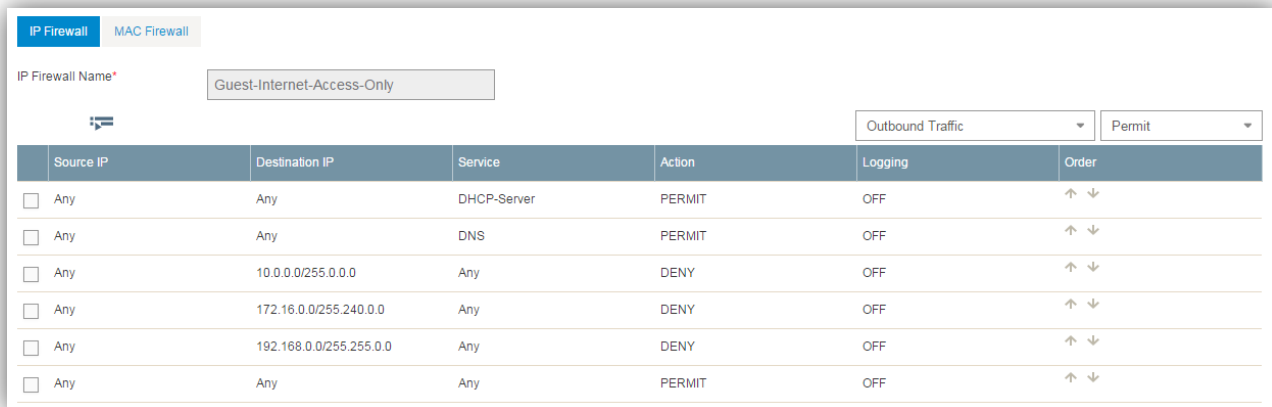
9. In the *Create User Profile* panel, enter **Guest** in the Name field, and then click **+** next to Connect to VLAN.

New VLAN Object

10. In the Name field, enter **Guest-VLAN**, enter the ID for a VLAN dedicated exclusively to guest traffic on your network, and then click **Save**.

Create User Profile

11. In the *Security* tab in the *Create User Profile* panel, toggle Firewall Rules to **ON**. With the *IP Firewall* tab active, click  and then choose **Guest-Internet-Access-Only**, which comprises the following rules:



| Source IP | Destination IP | Service | Action | Logging | Order |
|------------------------------|-------------------------|-------------|--------|---------|-------|
| <input type="checkbox"/> Any | Any | DHCP-Server | PERMIT | OFF | ↑ ↓ |
| <input type="checkbox"/> Any | Any | DNS | PERMIT | OFF | ↑ ↓ |
| <input type="checkbox"/> Any | 10.0.0.0/255.0.0.0 | Any | DENY | OFF | ↑ ↓ |
| <input type="checkbox"/> Any | 172.16.0.0/255.240.0.0 | Any | DENY | OFF | ↑ ↓ |
| <input type="checkbox"/> Any | 192.168.0.0/255.255.0.0 | Any | DENY | OFF | ↑ ↓ |
| <input type="checkbox"/> Any | Any | Any | PERMIT | OFF | ↑ ↓ |

As in all firewall policies, rules are checked in order from the top until a match is found. The rules shown above permit clients to access DHCP and DNS servers, deny them access to all private IP address spaces, and then permit them to access everything else.

12. Click **Save** to save the Guest user profile and close the *Create User Profile* panel.

SSID

13. Save the Visitor SSID.

AP250 Device Template


The next part in the wireless settings section of the network policy is the configuration of a device template for the AP250. The device template determines how its Ethernet ports will function and how the 2.4 GHz and 5 GHz radios will operate.

Because the wireless deployment was designed with access primarily in the 5 GHz band, you create a template for AP250 devices that configures them with dual 5 GHz radios. This is applied to all radios through the network policy. However, you manually override that on several AP250 devices scattered throughout the building by changing one radio back to the 2.4 GHz band for clients that must use that band.


Note: Setting radio profiles per device or in a device template in the network policy depends on the environment. If your deployment must provide more access in the 2.4 GHz band, then you would reverse the setup described here. That is, configure a device template in the network policy with one 2.4 GHz radio profile and one 5 GHz radio profile and override that with dual 5 GHz radio profiles for individual AP250 devices.

1. To create a new device template for the AP250, click **Device Templates > Add > AP250**.

AP250 Template

2. Enter a name for the template, such as **AP250-Dual-5GHz**.
3. Leave ETH0 and ETH1 with their default assignments as uplink ports and leave Wireless 1  with its default assignment of the radio_ng_na0 radio profile.

Note: If you use the default port type (Uplink Port), it cannot be modified and all VLANs will be allowed on ETH0 and ETH1. To allow traffic only on specific VLANs, you must create a new uplink port type.

4. Select **Wireless 0** , click **Assign > Choose Existing**, select **radio_ng_ac0** in the *Radio Profile Assignment* dialog box that appears, and then click **Save**.

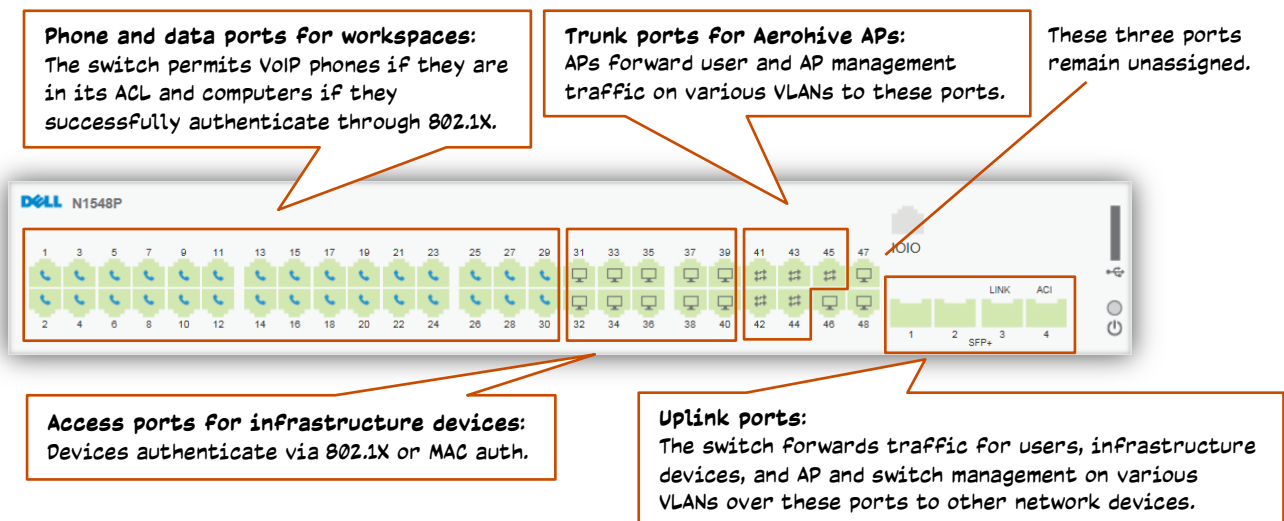
By assigning a radio profile that supports 802.11ac, the radio will operate in the 5 GHz band even though the icon in the GUI still shows "2.4 GHz".

5. To save the AP250 device template and close the configuration panel, click **Save**.

Switch Settings

There is one device template for all eight Dell N1548P access switches. The switch ports are organized as follows:

- Ports 1-30: For administrative convenience, these ports are connected to workspaces—mainly cubicles—in numerical order, so switch port 1 is cabled to cube 1 in a row of cubes, switch port 2 to cube 2, switch port 3 to cube 3, and so on. These are phone and data ports. The switch uses an ACL to restrict access to the voice VLAN only to company-issued IP phones and 802.1X authentication to restrict access to data VLANs only to the computers of users with valid credentials. These ports must allow traffic for the voice VLAN and all the data VLANs of the various users.
- Ports 31-40: The next ten ports are access ports for infrastructure devices like printers and Apple TVs. They use 802.1X and MAC address authentication methods. They allow traffic on the VLAN for infrastructure devices.
- Ports 41-45: These ports host 802.1Q trunk links for the AP250 access points. The allowed VLANs match those assigned to wireless users, the management VLAN for the APs, and the native (untagged) VLAN.
- Ports 46-48: These three ports are kept open to use as needed; for example, to mirror traffic.
- SFP+ Ports 1-2: The SFP+ ports are trunk ports for uplinks. They allow traffic for all VLANs allowed on other ports.



Create a device template for the N1548 switch by clicking **Switch Settings > Add > N1548P** and then naming it something like **HQ-N1548P**. The configuration for the following four port types in the template is provided below:

- Phone and Data Ports
- Access Ports on p. 21
- Trunk Ports on p. 22
- Uplink Ports on p. 23

Phone and Data Ports

A common setup in office cubicles is to connect a VoIP phone to the wired network and then connect a computer to the network through the data port on the phone. Dell switches permit phones if they appear in an ACL, and they permit computers when users successfully authenticate through 802.1X. If successful, they get assigned to the VLAN for their user group and allowed on the network. If they are unsuccessful, the switch denies them access.

Note: The ACL is defined in the Incorporating Supplemental CLI Commands section on p. 26.

1. To set ports 1-30 as phone and data ports, click-drag over those ports, and then click **Assign > Create New**.

New Port Type

2. Enter the following in the *New Port Type* section, leaving the other settings with their default values:

Name: Phone-Data-Auth-Port

Description: Settings for phone and data ports

Port Usage Settings

Phone with a data port: (select)

Wired Connectivity

User Authentication: ON

Default RADIUS Server Group: Click  .

RADIUS Server Groups

3. In the *RADIUS Server Groups* dialog box that appears, select the check box for **Corp-RADIUS-Group**, which is the same one you created earlier for the Employee SSID, and then click **Select**.

New Port Type

4. Click **+** next to Voice VLAN to define the VLAN for voice traffic from VoIP phones connected to the voice and data ports, enter a name and ID for the VLAN, and then click **Save**.

Switches notify connected VoIP phones what the voice VLAN ID is through LLDP-MED.

5. Click **+** next to Data VLAN to create a default VLAN for traffic to and from a computer connected to the data port on the phone, enter a name and ID for the VLAN, and then click **Save**.

Switches apply the default data VLAN if the RADIUS server returns an Access-Accept message without any attributes indicating a VLAN or with attributes matching the default.

6. Click the *MAC Authentication* tab and ensure that MAC Authentication is toggled **OFF**.

Although not supported in the HiveManager NG GUI, you can use the supplemental CLI feature to assign unauthenticated users to the guest VLAN. These would be users who did not authenticate themselves but are still allowed on the network with Internet-only access.

7. Click **Save** to save the port type configuration and return to the device template.

Access Ports

The access ports provide wired network access to devices such as printers, servers, Apple TVs, and other types of infrastructure devices. When a client with a RADIUS supplicant connects, 802.1X is used and the RADIUS server prompts the client for a user name and password to authenticate. When a client without a RADIUS supplicant connects, the RADIUS server tries MAC authentication, which is also referred to as MAB (MAC authentication bypass). If neither method succeeds, the client is denied access to the network.

On the Active Directory domain controller, set up a group for computers. Create entries for clients supporting 802.1X with user names and passwords. For all other clients, create entries using their MAC address as both their user name and password.

MAC Authentication and Dell N-Series Switches

Dell N-series switches use EAP-MD5 when communicating with a RADIUS server to perform MAC authentication. However, Microsoft Server 2008 and Windows Vista do not support MD5 encryption by default. To enable MD5 support, you must edit the registry as explained in the following Microsoft Support article: <https://support.microsoft.com/en-us/kb/922574>. In addition, if there are already entries in the Active Directory database for devices that will use MAC authentication (VoIP phones in this case) when you change the registry, you will need to re-enter their passwords.

Note that FreeRADIUS supports MD5 encryption without the need to edit registry keys and re-enter passwords.

1. To set ports 31-40 as access ports with 802.1X and MAC Auth, click **Deselect All Ports** to clear your previous selections of ports 1-30, click-drag over ports 31-40, and then click **Assign > Create New**.

New Port Type

2. Enter the following in the *New Port Type* section, leaving the other settings with their default values:

Name: Access-Auth-Port

Description: Settings for access ports with 802.1X and MAC authentication

Port Usage

Access port: (select)

Wired Connectivity

User Authentication: ON

Default RADIUS Server Group: Click .

RADIUS Server Groups

3. In the *RADIUS Server Groups* dialog box, select the check box for **Corp-RADIUS-Group**, which is the same one you used for the phone and data port type, and then click **Select**.

New Port Type

4. To prevent anyone from connecting a hub to a port, authenticating just the first device and letting subsequent devices on without authentication, clear **Allow multiple clients connected to the same port on the same VLAN**.
5. Click **+** next to the VLAN field to create a default VLAN for all infrastructure devices, enter a name and ID for the VLAN, and then click **Save**.
6. Click **MAC Authentication**, toggle MAC Authentication **ON**, and then choose **MS CHAP v2** from the Authentication Protocol drop-down list.

In the *Authentication Method Priority* section, notice that 802.1X has priority over MAC AUTH. The RADIUS authentication server first attempts to prompt the client for a user name and password. If the client does not have a RADIUS supplicant, the RADIUS server then checks if it can authenticate the client using its MAC address as both user name and password.

| AUTH Type | Order |
|-----------|-------|
| 802.1X | ↑ ↓ |
| MAC AUTH | ↑ ↓ |

7. Click **Save**.

Trunk Ports

The trunk ports are the ones through which the Aerohive APs connect to the wired network. They support 802.1Q tagging and must allow all the VLANs to which the APs assign user traffic, the management VLAN for the APs, and the native (untagged) VLAN.

Allowing traffic to traverse trunk ports only on the set of VLANs that APs use—as opposed to allowing traffic on all VLANs—accomplishes two things. It limits the broadcasts that APs transmit on their wireless interfaces and enters those VLANs in the VLAN database on the switch.

1. To set ports 41-45 as trunk ports, click **Deselect All Ports** to clear your previous selections of ports 31-40, select ports 41-45, and then click **Assign > Create New**.

New Port Type

2. Enter the following in the *New Port Type* section, leave the other settings with their default values, and then click **Save**:

Name: Trunk-APs

Description: Settings for AP trunk ports

Port Usage

Trunk Port (802.1Q VLAN Tagging): (select)

Trunk VLANs

3. In the *Trunk VLANs* dialog box that appears, set the native VLAN for network, specify the VLANs of all the different types of users that the connected APs serve, and then click **Save**.

Uplink Ports

The uplink ports are the ones through which the Dell N1548P switch connects to the rest of the network. These are SFP+ ports that provide 10 Gbps throughput each over fiber optic cables to the collapsed core switching fabric. These ports and those on the switches to which they connect must support VLANs for all the various types of users and devices whose traffic it forwards.

1. To set SFP+ ports 1-2 as uplink ports, click **Deselect All Ports** to clear your previous selections of ports 41-45, click-drag over the four port icons labeled 1-4 in the lower right corner of the device template, and then click **Assign > Create New**.

New Port Type

2. Enter the following in the *New Port Type* section, leave the other settings with their default values, and then click **Save**:

Name: Uplink-Ports

Description: Settings for the SFP+ uplink ports

Port Usage

Trunk Port (802.1Q VLAN Tagging): (select)

Trunk VLANs

3. In the *Trunk VLANs* dialog box that appears, set the native VLAN for the network, specify the VLANs of all the different types of users and devices that connect to the switch through its other ports, and then click **Save**.
4. Click the **Save** button in the lower right to save the device template.

Additional Settings

Configure additional settings for DNS and the time zone for the devices to which the network policy applies.

DNS Settings

You might want to configure a DNS server that APs and switches use to look up domain names for defined services such as syslog servers, SNMP servers, and RADIUS servers.

To configure DNS settings:

1. From your network policy, click **Additional Settings > MANAGEMENT SERVER > DNS Server**, and then enter the following in the *Default DNS Server* section:

Name: Enter a descriptive name for the DNS server configuration object, such as *Internal-DNS*.

Domain Name: Enter the name of the domain to which devices using this network policy belong. For Example: *yourcompany.com*.

2. To remove all existing DNS sever IP addresses from the list, select the check box next to DNS Server and then click the trash icon.
3. To add the IP address for a new DNS server—such as an internal DNS server—click **+**, enter its IP address, and then click **Add**.
4. Repeat the previous step to add another IP address, such that for a secondary internal DNS server.
5. To save the DNS server configuration, click **Save**.

Time Zone

To set the time zone for the APs and switches to which the network policy applies, click **POLICY SETTINGS > Device Time Zone**, choose a time zone from the drop-down list, and then click **Save**.

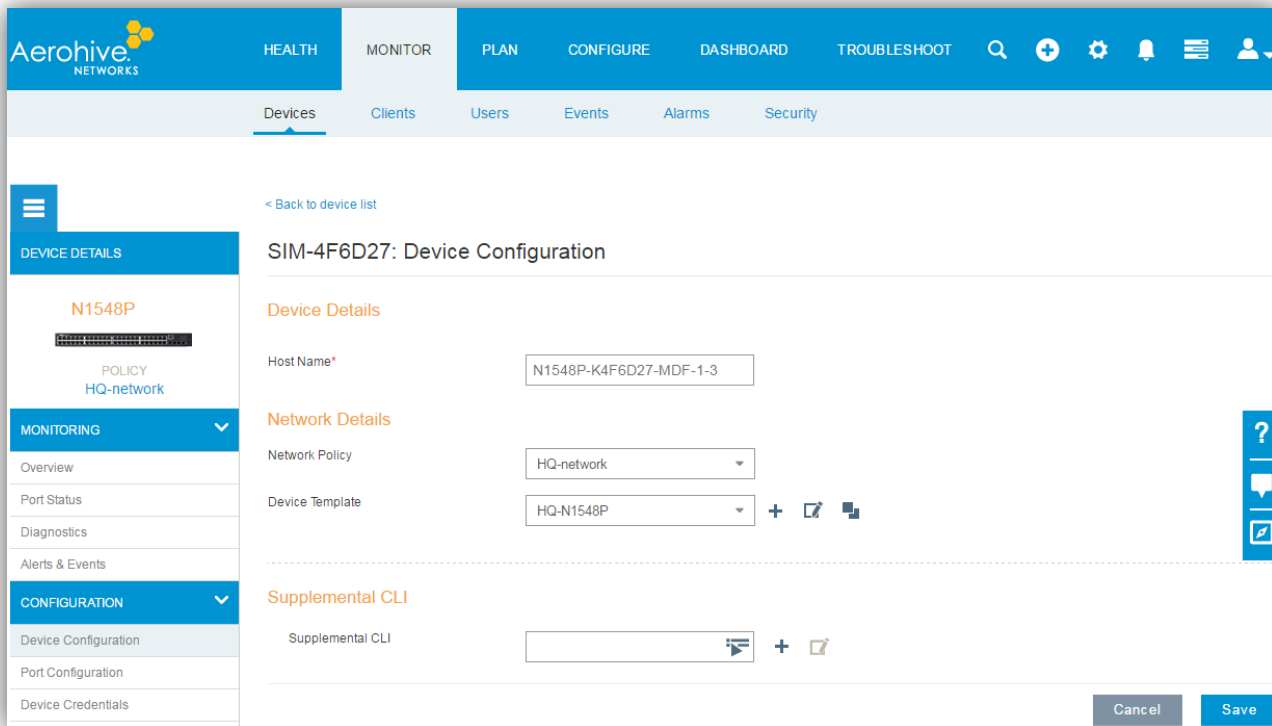
If the network policy applies to devices in multiple time zones, you can assign different time zones to them by classifying them by location.

Device-Specific Settings

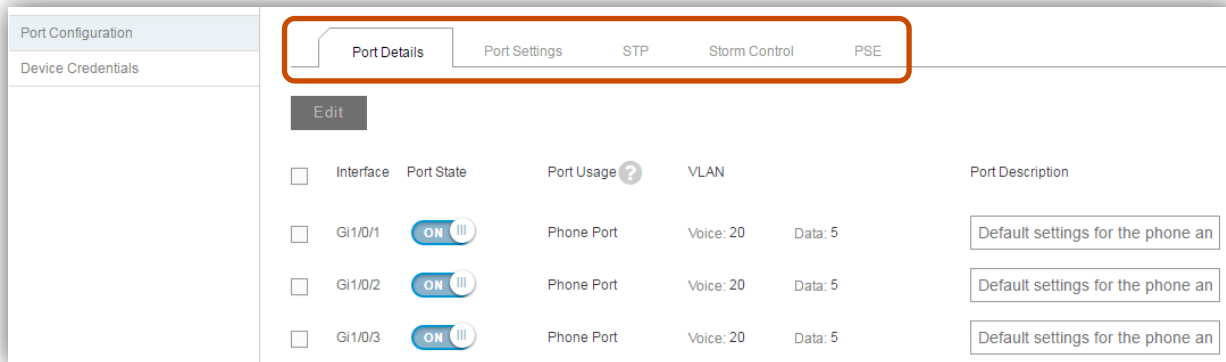
Key Points: Along with the network policy, which is a global set of configuration settings for devices, you can configure device-specific settings, which override settings configured in the network policy, including the device template and VLANs assigned to ports.

You can configure device-specific settings in the *MONITOR* section. Click the host name of a device to see details about it. You can monitor and configure device- and port-level settings; set its host name, power settings, network policy, and device template; and add supplemental CLI commands to its configuration.

Note: The supplemental CLI feature is covered in the next section.



From the *CONFIGURATION > Port Configuration > Port Details* tab, you can administratively enable or disable ports, override access port VLANs configured in the device template, and enter port descriptions. You can also select other tabs to configure physical port settings, STP, storm control, and PSE power settings. The following screenshot shows an example of the switch configuration settings and the available tabs.



Incorporating Supplemental CLI Commands

You can configure much of the configuration for non-HiveOS switches through the HiveManager NG GUI; however, there are some settings that you must add through the supplemental CLI feature.

HiveManager NG basically converts the configuration you define through the GUI into a series of CLI commands when it uploads them to devices. By using the supplemental CLI, you can add more commands to those derived from the GUI and append them to the configuration.

You can add supplemental CLI commands at the network policy level and individual device level. However, when a network policy applies to both HiveOS devices and non-HiveOS devices, as is the case here (AP250 and N1548P), you must add supplemental commands for both types of devices at the device level because of their different command syntaxes.

The supplemental CLI feature is disabled by default in HiveManager NG. To enable it, click the gear icon  > **ADMINISTRATION > VHM Management**, and then toggle Supplemental CLI to **ON**.

To create a supplemental CLI object from within the context of your network policy, click **Additional Settings > POLICY SETTINGS > Supplemental CLI > Add**. Enter a name for the supplemental CLI configuration object, a description for future reference, the commands listed below, and then click **Save**.

The commands below configure the phone and data ports on the Dell switches (Gi1/0/1- Gi1/0/30) with the following functionality:

- Computers are authenticated through 802.1X
- An ACL permitting only VoIP phones with a specific OUI is assigned to VLAN 20 (the voice VLAN in this example)
- Guests and unauthenticated users are directed to VLAN 20 and are then denied access by the ACL

```
enable
configure
mac access-list extended Permit-Phones
1000 permit 30F7.0D5F.416E FFFF.FF00.0000 any vlan eq 20
! All the phones begin with the OUI 30F70D. To make a rule using an OUI, enter a source MAC
  address with the correct OUI and FFFF.FF00.0000 as the source MAC mask.
2000 deny any any vlan eq 20
2001 permit any any
exit
!
interface range gigabitethernet 1/0/1-30
dot1x port-control mac-based
dot1x guest-vlan 20
dot1x unauth-vlan 20
authentication order dot1x
authentication priority dot1x
mac access-group Permit-Phones in 1
exit
```


Uploading Device Configurations


Key Points: Aerohive provides flexible and verifiable configuration and image updates.

Unlike some systems where you update one master device, which then updates all the connected devices, with Aerohive, HiveManager NG is updated independently from its managed devices. Once HiveManager NG receives an update, you can update the configuration and firmware on its managed devices as you like. You can update a single device, a subset of devices, or all devices. This lets you try out new settings first on a few devices before updating everything. This is especially important if you have devices in different time zones and for facilities that run 24x7 where there is no single time window for updates.

To update device configurations, you must assign a network policy and device settings to each device. If you did not initially make these configuration assignments, you can do this later as explained below.

Network Policy Application

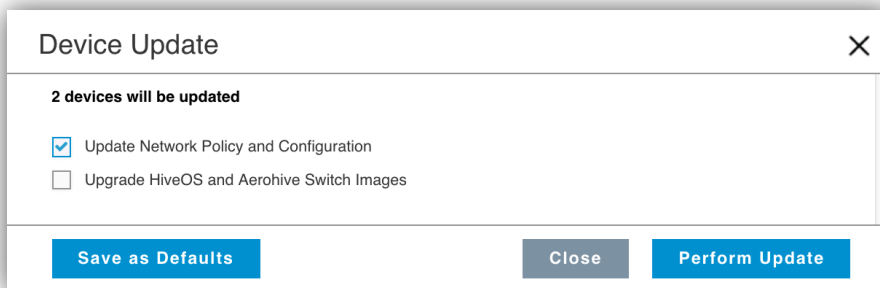
1. Assign the network policy by clicking **MONITOR > Devices**, select the check box next to devices you want to assign, click the **Modify** icon , choose a network policy from the drop-down list, and then click **Save**.
2. To return to the MONITOR > Devices page, click **< Back to device list**.
3. Select the check box next to devices you want to update.

You can use the filters on the left side to narrow the list. You can also select the check box next to Status in the table header to select all the devices listed  **Status**.

Note: It is recommended that you select one or two devices to begin with instead of all of them. Once the update is complete and you have achieved acceptable results, then update more devices.


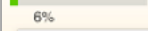
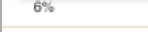

Device Update

4. Click **Update Devices** in the upper right side of the MONITOR > Devices page.
5. Select **Update Network Policy and Configuration** and then click **Perform Update**.



For a configuration update, HiveManager NG instructs the switch to obtain its configuration from HiveManager over HTTPS (TCP port 443). The switch then obtains and applies its configuration, a process that can take several minutes to complete.

6. Monitor the upload status by watching the green status bar in the Updated On column. An example of an update in progress is shown on the right. You can see the status column change to a green hexagon and a green check box when done. The Last Updated On column eventually displays the time the update was completed.

| Updated On | Management Status |
|--|-------------------|
|  6% | Managed |
|  6% | Managed |
|  6% | managed |
|  6% | Managed |

Guest Management Administrators

Aerohive provides several options for generating PPSKs and distributing them to visitors. For all of them, you first create guest management accounts for the people who register visitors or who enable visitors to self-register.

Creating Guest Management Administrators

1. Click **CONFIGURE > Users > Employee Groups > Add**, enter the following, and then click **Save**:

Group Name: Enter a descriptive name such as **Guest-PPSK-Creators**.

Admin Account: **Guest Management Role User**

Guest Management User: Enter the email addresses of the people for whom you just created guest management accounts.


Credential Restriction

Restrict the number of credentials per employee to: (select) Enter a number from 1 to 99999 depending on how many PPSK users you want each guest management admin to be able to create. This limit is applied to the number of concurrently active PPSK users. When a user expires, it no longer counts toward this maximum. (When using the Aerohive iPad Kiosk app, everyone who self-registers does so under the login of the guest management admin who launches the app on the iPad. Therefore, make sure that he or she can create plenty of PPSK users.)

Registration Operation

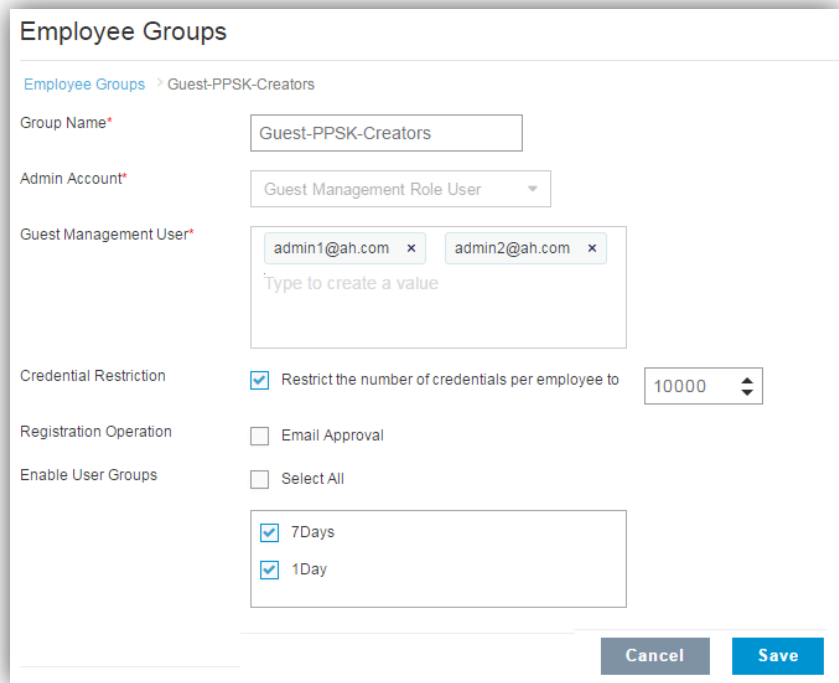
Email Approval: (clear); Selecting this requires one of the guest management users to approve PPSK user access by email before a visitor can access the network.

Enable User Groups: Select all the PPSK user groups for which the administrators specified in the Guest Management User field can create users.

2. Click the gear icon  in the top toolbar and then click **Add** in the *Account Management* section.
3. Create a guest management account for one or more people whom you want to be able to create and distribute PPSK users.

After you create each account, HiveManager NG automatically sends a message to the email address associated with it, prompting the recipient to set up a password and access the *Configure > Users* page to create PPSK user accounts for visitors.

The guest management admin can either log in to the HiveManager NG GUI directly or access it through the iPad Kiosk app, which is one of two PPSK user creation apps that Aerohive provides.



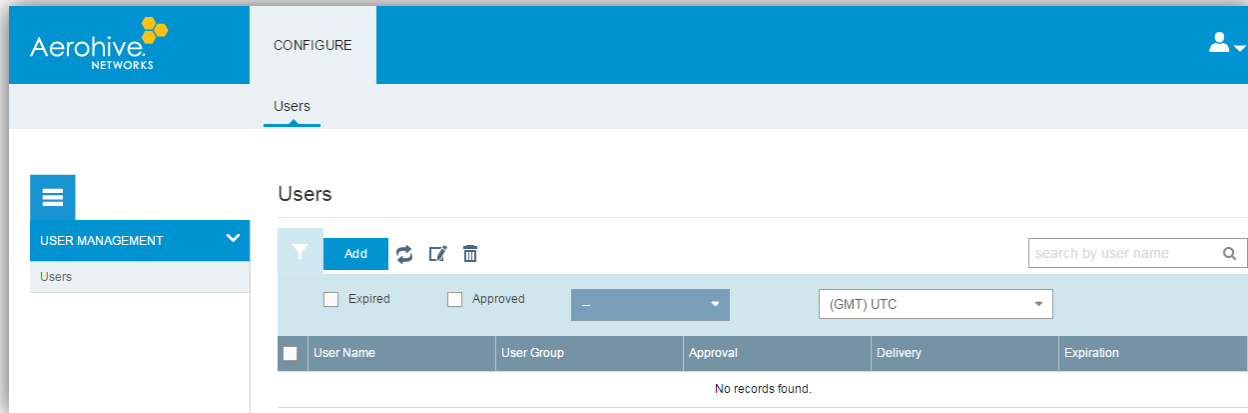
The screenshot shows the 'Employee Groups' configuration interface. The breadcrumb path is 'Employee Groups > Guest-PPSK-Creators'. The 'Group Name' field contains 'Guest-PPSK-Creators'. The 'Admin Account' dropdown is set to 'Guest Management Role User'. The 'Guest Management User' field contains two email addresses: 'admin1@ah.com' and 'admin2@ah.com'. Under 'Credential Restriction', the checkbox 'Restrict the number of credentials per employee to' is checked, and the value '10000' is entered in the adjacent field. Under 'Registration Operation', the 'Email Approval' checkbox is unchecked. Under 'Enable User Groups', the 'Select All' checkbox is unchecked, and the '7Days' and '1Day' checkboxes are checked. 'Cancel' and 'Save' buttons are located at the bottom right of the form.

Creating Visitor PPSKs

There are several ways for guest management administrators to access the PPSK user creation mechanism.

Built-in PPSK Creation

One approach is to restrict guest management administrators to one section of the HiveManager NG GUI. After they log in to HiveManager NG, they are only permitted to access the Configure > Users page.



To create a PPSK user for a visitor, click **Add**, enter the following, and then click **Save**:

Create account in user group: Choose one of the two PPSK user groups you created in "SSID for Visitors" on p. 16.

Enter information about the visitor for tracking purposes in the fields from Name to Phone Number.

Either manually enter a 10-character password composed of letters and numbers (as defined in the user group settings when you created them) or click **Generate** to create one automatically.

Finally select the options for delivering the PPSK and enter the recipient's email address, phone number, or both.

Users

Users > New User

Create account in user group*

Name*

Organization

Purpose of Visit

Email Address

Phone Number

Password*

Show Password

Description

Deliver Password

Email Address

Text Message

The PPSK user groups you created earlier appear here for the Visitor SSID and that you enabled in Guest-PPSK-Creators employee group appear in this drop-down list.

Personal information about the visitor for tracking purposes

This is the address is to which HiveManager NG sends the PPSK. It does not have to be the same as that for the user. For example, this might be the receptionist's address or someone else's who will distribute the PPSK some other way.

Aerohive Guest Check-in Web App

This web app is intended for use by lobby or front desk personnel to check in visitors individually and in bulk and deliver PPSK user credentials to them.

For bulk creation, you can import a .CSV file with PPSK user creation details. It also supports various PPSK delivery methods: email, SMS, and print.

It is available here: <https://aerohive.emanatelabs.com/>. Employee management administrators log in with their HiveManager NG admin name and password. They are then prompted to choose which VHM to authorize, which is important for people with access to multiple VHMs.

After logging in to the web app, click **New Visitor**, enter the following information for the visitor, and then click **Enter**:

Visitor Info

1 Peter Piesque
FULL NAME*

ppiesque@gac.com
EMAIL*

+1415-555-1212
PHONE

7Days
1Day

Add Visitor

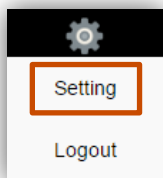
What company are they from?
Enter company name

Who are they here to see?
Enter contact name

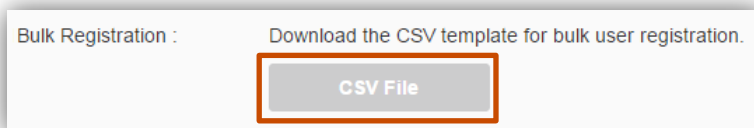
ENTER CANCEL

The title of this field is *Type*. When you click it, a drop-down list appears with the PPSK user groups that you assigned to the guest management admin group to which the current admin belongs.

To import users in bulk, click the gear icon and then choose **Setting**.



Click **CSV File** and save it to your system.




Add entries with information in the provided columns: CompanyName, WhomToSee, Name, Email, Phone, Type.

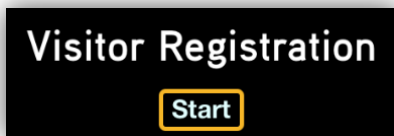
Click **Import CSV** on the web app dashboard, navigate to the file you saved, and select it.



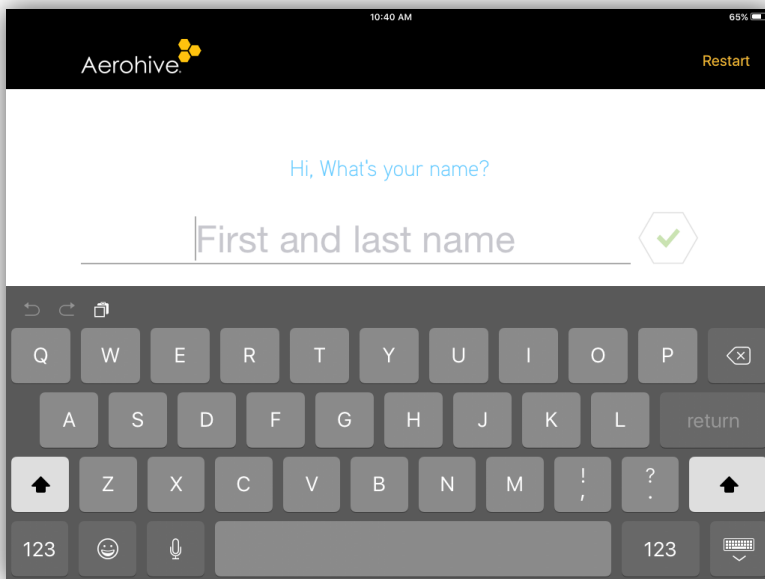
Aerohive iPad Kiosk App

This app is intended for use in unattended lobby areas, or in reception areas where guests register themselves for temporary wireless access at the organization they are visiting.

The guest management administrator who sets up the app on an iPad must log in first, choose his or her HiveManager NG account, and authorize the app to communicate with it. Next, a list of credential types (PPSK user groups) for which the admin can create PPSK users appears, which in the example here are 1Day or 7Days. The admin chooses one PPSK user group and then taps the check mark icon  to lock the app to the guest management administrator's account and the selected PPSK user group. Then everyone else who self-registers does so under that administrator's login. Therefore, it is important that he or she can create plenty of PPSK users.



The app supports visitor sign-in using an email or phone number, an optional employee lookup and approval process (using LDAP), and various PPSK delivery methods: SMS, email, print, and QR code for Androids.



It is possible to exit the app by rebooting the iPad or double-clicking the **Home** button and sliding the app off screen. However, by putting the iPad in Guided Access mode, you can lock the screen so that users cannot switch to another app:

1. Press the **Home** button and then tap **Settings > General > Accessibility**.
2. Enable **Guided Access**, select **Passcode Settings > Set Guided Access Passcode**, and then enter a passcode.
3. Return to the home screen and tap the **Aerohive Kiosk** icon to launch the app.
4. Triple-click the **Home** button. In the Hardware Buttons Options menu, disable **Sleep/Wake Button** so that people cannot turn off the iPad. Also enable **Keyboards** and **Touch** so they can enter information as they register. Then tap **Start** to enter Guided Access mode.
5. To exit, triple-click the **Home** button, enter the passcode, and then tap **End**.

The Aerohive iPad Kiosk app is [available for download from the app store](#) and works on iPads running iOS 8.0 or later.