

Wired + Wireless Cloud-managed Campus Deployment Guide – Branch, Small Campus and Distributed Sites

Dell Networking Solutions Engineering
September 2016

Revisions

Date	Description	Authors
September 2016	v1.0 – Initial release	Colin King, Davis Smith

©2016 Dell Inc., All rights reserved.

Except as stated below, no part of this document may be reproduced, distributed or transmitted in any form or by any means, without express permission of Dell.

You may distribute this document within your company or organization only, without alteration of its contents.

THIS DOCUMENT IS PROVIDED “AS-IS”, AND WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED. IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE SPECIFICALLY DISCLAIMED. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT:

<http://www.dell.com/learn/us/en/vn/terms-of-sale-commercial-and-public-sector-warranties> Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell's recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell EMC logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. QLogic® is a registered trademark of QLogic Corporation. Aerohive® and HiveManager® are registered trademarks of Aerohive Networks, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.

Table of contents

Revisions.....	2
Introduction	4
1 Cloud-managed networking devices	6
1.1 Cloud-managed wired access switches	6
1.2 Cloud-managed wireless access points	6
2 Cloud-managed, small campus deployment	7
2.1 Cloud management assumptions	8
2.2 Goals	8
3 Deployment example – preparing for deployment	9
3.1 Prerequisites.....	9
3.1.1 Security and internet connectivity prerequisites	9
3.1.2 Access layer prerequisites.....	10
3.2 Recommendations and precautions	10
4 No-touch deployment procedures	12
4.1 Firewall initial setup	13
4.2 Access layer switches initial setup	14
4.3 Wireless AP initial setup	15
4.4 Onboarding Dell Networking N-Series switches and Aerohive APs to HiveManager NG.....	15
4.5 Network policy configuration.....	19
4.6 Supplemental CLI	34
A Software versions	39
B Additional resources.....	40
Support and feedback.....	41
About Dell EMC	41

Introduction

IT managers are looking to support rapidly changing and diverse user-access requirements across their networks without committing additional administration resources. They must adapt to address the needs of key business functions while providing reliability, performance and flexibility from their wired and wireless networks. These networks must be capable of delivering rich applications and access to corporate resources regardless of device form factors.

Deployment of campus networks in remote locations can be a costly and time-consuming task. Retail and remote office environments have unique requirements related to deployment timeframes and geographical constraints. Often, multiple locations require simultaneous deployment. Figure 1 shows a wired and wireless, cloud-managed network; it is an example of one of the most critical deployment scenarios.

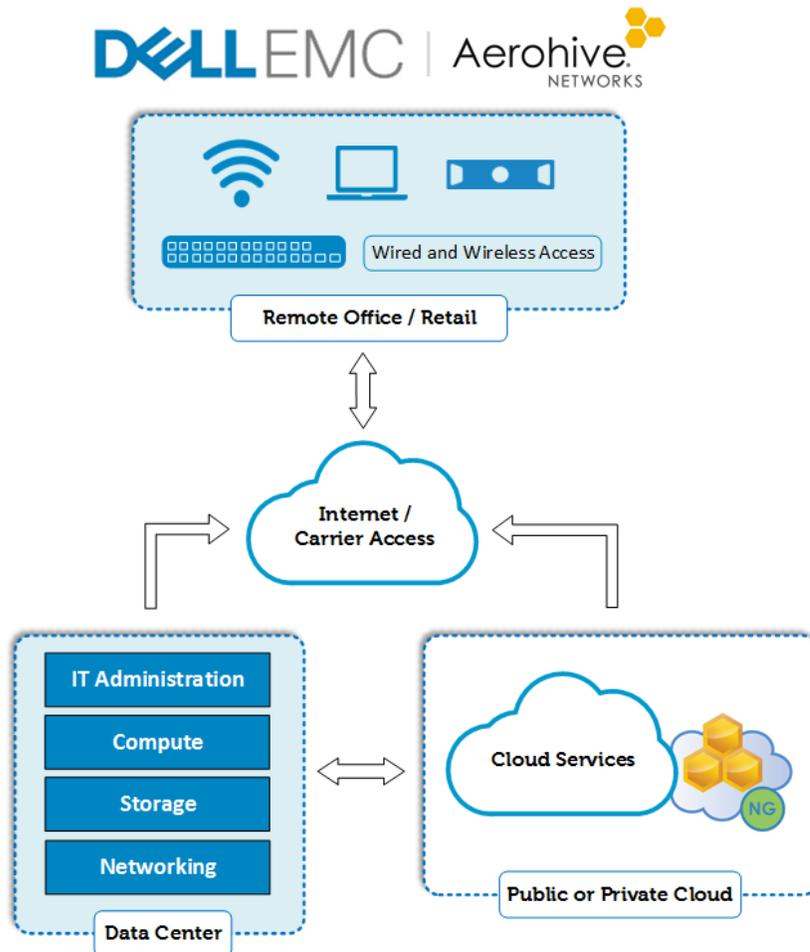


Figure 1 Cloud-managed campus global view

This Deployment Guide addresses the following topics:

- Mass deployment of switches and access points, with minimal touch
- Cloud management of wired and wireless access devices
- Incorporation of cloud management into the modern, end-to-end campus network
- Delivery of the latest technology through cloud management

This guide describes the creation and maintenance of a wired and wireless network that performs well and meets current business and user needs. It presents a network built on a solid enterprise infrastructure that enables the business and its goals to scale on demand.

1 Cloud-managed networking devices

This chapter discusses Dell Networking devices that provide cloud management for wired and wireless access solutions.

1.1 Cloud-managed wired access switches

Dell Networking OS version 6.3.0.16 firmware supports and automatically enables HiveManager NG capability. Ensure all cloud-managed switches are upgraded to version 6.3.0.16 or later prior to onboarding to HiveManager NG.

Dell Networking switches supported in HiveManager NG:

- N3000 Series
 - N3024
 - N3024F
 - N3024P
 - N3048
 - N3048P
- N2000 Series
 - N2024
 - N2024P
 - N2048
 - N2048P
- N1500 Series
 - N1524
 - N1524P
 - N1548
 - N1548P

1.2 Cloud-managed wireless access points

HiveManager NG also manages Aerohive® wireless access points (APs). HiveManager® NG allows for converged wired and wireless networking policies and monitoring.

Aerohive 802.11ac wireless APs

- AP130
- AP230
- AP250
- AP550
- AP245X
- AP1130

2 Cloud-managed, small campus deployment

The goal of the cloud-managed small campus deployment is to help IT administrators deploy and manage their access networks. This document shows how to use HiveManager NG to deploy both wired and wireless devices while also providing continuous cloud management functionality.

This section provides detailed information about a small business network topology. Small business networks are typically comprised of a single access layer for switching, access points, and a single firewall as seen in Figure 2:

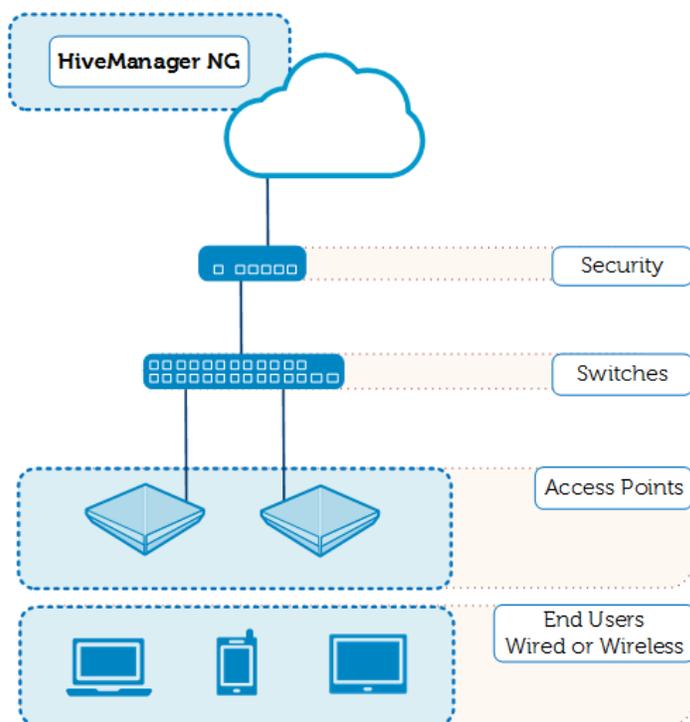


Figure 2 Cloud-managed campus topology, small business

This deployment guide describes a simple access network supporting a small office or retail environment as an example topology. Figure 2 shows all the devices and infrastructure necessary to support typical numbers of employees and guests.

This deployment guide documents devices and the use case for a single access network. Businesses with numerous sites can use this example to scale across multiple sites and multiple geographical locations.

Validation of this example used the following devices:

- SonicWALL TZ300 firewall
- Dell Networking N1524P switch
- Aerohive AP230 APs

2.1 Cloud management assumptions

The example topology assumes the following factors:

- Internet access from the ISP provides a single public IP.
On-site IT support is limited.

2.2 Goals

Dell Networking designed the example topology with the following goals:

- Zero-touch deployment of APs and switches
- Entirely offsite network administration
- Unified wired and wireless network policy
- Wireless guest access
- Wired and wireless connectivity for PCs and peripherals

3 Deployment example – preparing for deployment

This chapter describes deployment prerequisites and procedures for cloud-managed networks in small campus environments.

3.1 Prerequisites

This section describes security and set-up prerequisites for cloud-managed networks in small campus environments.

3.1.1 Security and internet connectivity prerequisites

The small business topology diagram in Figure 2 shows a single SonicWALL firewall. Validation of this document used a SonicWALL TZ300. Performance and feature requirements of the network determine the particular firewall model used.

The WAN interface enables SonicWALL administration.

3.1.1.1 Security and internet assumptions

Small campus networks assume the following security and internet connectivity conditions exist in the environment:

- Internet access is established and available onsite.
- The IP address assigned to the WAN port on the firewall is available remotely.
 - This example does not include additional routing equipment outside the firewall.
- All internal traffic from guest and employee networks is routed through the VLAN 1 management interface to the firewall.

3.1.1.2 Summary of configuration items:

Small campus network deployment configurations include the following items:

- WAN interface and zone, management-enabled
- LAN interface and zone
 - LAN IP address on same subnet as connected switch interface
 - Used as the gateway for all external traffic
- Routing policies set for VLAN 1 subnet
 - Any Source to VLAN 1 destination
- NAT policy for VLAN 1 in place

Note: This example uses the default SonicWALL firewall access rules. Administrators can make security settings more robust and in-line with final security requirements mandated by the organization's IT security policy after the network is established. This guide does not detail full security settings.

3.1.1.3 Key setup instructions:

Cable a single 1 GbE connection from the X0 firewall interface to the Dell N-Series switch, as Figure 3 shows:

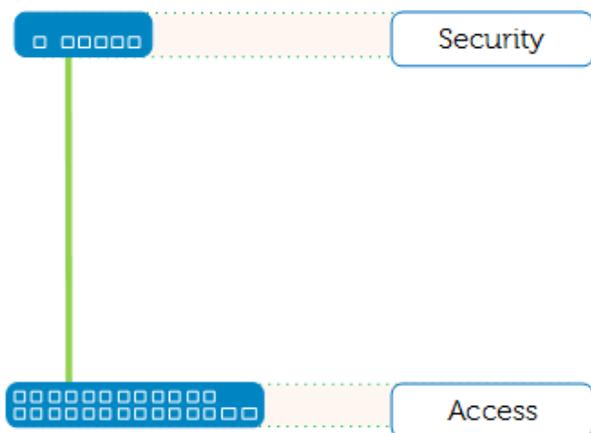


Figure 3 Initial setup for the firewall and access switch

3.1.2 Access layer prerequisites

The HiveManager NG cloud management solution deploys and manages the access layer that includes both switches and access points. The Dell Networking switch models and Aerohive access points identified in Section 1 all work in this example. For additional details on the cloud-managed switches, see the [Wired + Wireless Cloud-managed Campus Reference Architecture](#) and the [HiveManager NG Cloud Management](#) product webpage.

3.1.2.1 Access layer assumptions

Small campus networks assume the following conditions exist at the access layer:

- All switches are in their factory, out-of-the-box condition or reset to factory defaults.
- VLAN1 provides the only administrative access.
- Aerohive access points are reset to their default configurations.

Note: Dell Networking designs N3000 series switches with an out-of-band (OOB) interface that administrators can configure for management purposes. The Dell N1500 and N2000 series switches have no OOB interfaces. The deployment steps in this document only detail public cloud management and no-touch deployment through VLAN 1 on in-band interfaces.

3.1.2.2 Minimum configuration items

No configuration required, retain or reset to factory defaults.

3.2 Recommendations and precautions

The HiveManager NG solution delivers a very powerful management and monitoring tool. When utilized with Dell switches and Aerohive APs, it can offer an infinite number of customizations and configurable features.

The list below offers some recommendations when utilizing the combination of HiveManager NG Network Policies, Supplemental CLIs, and traditional console configuration.

- Have a backup method to access devices through the console or SSH
 - Errors in configuration can leave devices disconnected from cloud management
- Continuous connectivity must be maintained for full configuration push
 - Interruption in connectivity can cause an incomplete update
- The order of updating devices can be important
 - Evaluate configuration changes to best maintain connectivity
 - Separate configuration updates by device type or location within the topology
- The Supplemental CLI script executes its commands in order from top to bottom.
 - Ensure commands that require sub-configuration modes are executed within the appropriate mode or interface.
- Ensure that the script executes properly before remote deployments.
- Complex configurations may require intermediate steps via multiple configuration updates
- Update only one Device Configuration parameter per device update action.
 - Updating the Network Policy, Device Template, and Supplemental CLI concurrently may cause unintentional results.
- A new Supplemental CLI script can be applied to and updated on the same Dell switch each time the device is updated. A set of commands applied to the switch through a Supplemental CLI script is not removed by changing the Supplemental CLI script.
 - Supplemental CLI script commands can be removed by applying a new script with the appropriate “no” commands.
 - Ensure that subsequent Supplemental CLI scripts do not conflict with running configurations.
- Device template settings do not show configurations completed through the Supplemental CLI.
 - Dell Networking recommends using features in the Supplemental CLI only if they are un-supported in the device template or Additional Settings.
- Check Active Alerts for configuration errors when using the Supplemental CLI.
- Prepare a proof of concept on a test setup prior to a large scale deployment

4 No-touch deployment procedures

This section provides the test environment deployment with the example topology in Figure 2. The design of this process uses the simplest initial configuration on all devices required to establish a basic small campus network.

Note: Always perform a proof-of-concept for large scale, multiple-remote-site deployment scenarios.

Site Preparation and Standard Deployment

- Physical installation and cabling
- Configure firewalls
- Power on access switch and APs

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

4.1 Firewall initial setup

The no-touch example uses a SonicWALL TZ300 model firewall. Dell does not intend the interfaces used, including the speed and other capabilities, to be identical to your deployment. The documented interface port numbers allow the reader to follow the methodology.

Note: Diagram device icons are for conceptual purposes. Dell does not intend the exact port location and form factor to be accurate for all models.

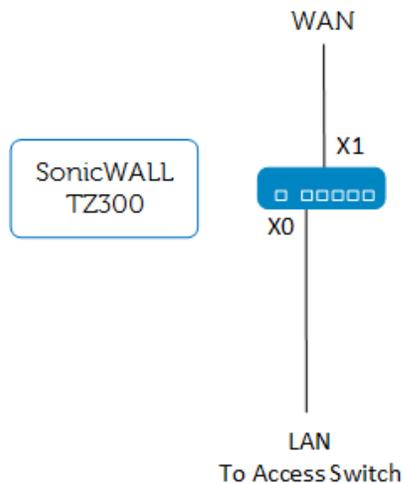


Figure 4 Firewall cabling

The firewall is the path from the internet (WAN) to the access switch (LAN). For this example, the WAN interface, not the HiveManager NG cloud management solution, serves as the management interface for the firewall.

Note: Configuration steps vary by firewall model and vendor. Therefore, this document does not provide step-by-step instructions for the firewall.

Configuration steps:

1. X1 interface: assign the public IP address, gateway and DNS server for the WAN zone on the firewall.
 - a. X1 can be assigned statically or through DHCP. Consult your internet service provider.
2. X0 interface: assign the private IP address for the LAN zone on the primary firewall.
 - a. This address serves as the gateway for your private network's traffic to the internet. This example uses 10.1.1.99/24.
 - b. The address should be in the VLAN 1 subnet. This example uses VLAN 1 on 10.1.1.0/24.
 - c. Set VLAN sub-interfaces for all subnets. This example uses VLAN 10 (employee) and VLAN 20 (guest). The IP addresses for each are 10.1.10.99/24 and 10.1.20.99/24, respectively.

3. Set the DHCP server to deliver at least three addresses to the 10.1.1.0/24 subnet. (One switch, two APs)
 - a. The DHCP server should be enabled by default; reduce the lease scope if desired.
 - b. Ensure the DHCP server is enabled in DHCPv4 Server Settings and DHCPv4 Server Lease Scopes.
 - c. Set DHCP scopes for all subnets, including the VLAN sub-interfaces, at this time.

Note: Step 3c is optional if not using the firewall as the DHCP server.

4. Leave other settings as their defaults.
5. Connect the cable to the access switch.

When completed, the firewall has an active internet link through interfaces X1 and X0 to the access switch.

4.2 Access layer switches initial setup

The no-touch example uses a N1524P model switch. Documentation of interface port numbers allows the reader to follow the methodology. HiveManager NG also deploys and manages N2000 and N3000 series switches, if desired. Configuration and deployment steps are the same and have been validated.

The active path to the internet and HiveManager NG passes through the firewall, as Figure 5 shows. The access switches require no configuration. Factory default settings are preferred for the access switches for the initial setup.

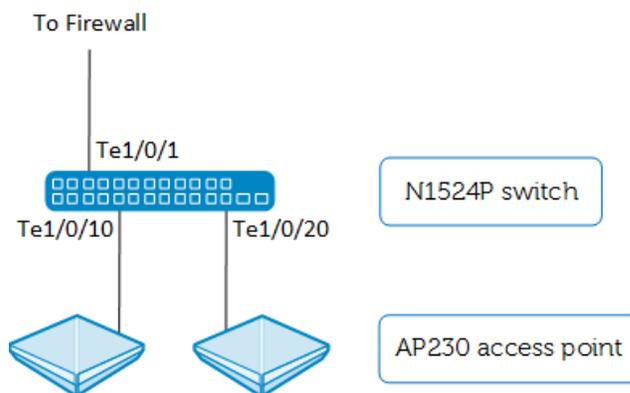


Figure 5 Switch cabling

Complete the following steps for initial setup:

1. Connect the cable from the firewall to the access switch if not already connected.
2. Connect wireless APs to the switch.
3. From factory default state, power-on the switch.
4. Let the Dell Easy Setup Wizard time out (boot time + 60 seconds).

Note: Admins that monitor local CLI access can manually decline the wizard.

Access switches request IP addresses via DHCP on VLAN 1 by factory default. VLAN1 is the default PVID for all interfaces.

The Dell Networking N-Series switches with firmware 6.3.0.16 and later have embedded capability that enables the switch to communicate with HiveManager NG. The switches require no additional configuration as these settings are enabled by default. For further details, see the *Dell Networking N-Series N1500, N2000, N3000, and N4000 Switches CLI Reference Guide v6.3.0.0*, found on the [Dell Support site](#). After the switch service tag is associated with your account, the Monitor Devices section of HiveManager NG shows the devices.

Note: HiveManager NG must be accessible from the internal network via HTTPS, using TCP port 443, to deploy and manage the access switches. Ensure that security measures allow access to the internet from the management subnet.

4.3 Wireless AP initial setup

The no-touch example uses Aerohive AP230 APs. HiveManager NG can deploy and manage all Aerohive wireless APs sold through Dell. Choose the AP model appropriate for your deployment.

Complete the following step for initial wireless setup:

- Connect the wireless AP to the switch if not already connected.

Aerohive wireless APs contact HiveManager NG by factory default. After the device serial number is associated with your account, the Monitor Devices section of HiveManager NG shows the devices.

Note: HiveManager NG must be accessible from the internal network via HTTPS, using TCP port 443, to deploy and manage the access points. Ensure that security measures allow access to the internet from the management subnet.

Site Preparation and Standard Deployment

- Physical installation and cabling
- Configure firewalls
- Power on access switch and APs

4.4 Onboarding Dell Networking N-Series switches and Aerohive APs to HiveManager NG

This example assumes that the customer has already created an account for HiveManager NG (<https://cloud.aerohive.com/dell>) and applied all the required licenses. For further information on obtaining licenses, please contact your Dell sales and support representative.

The first step in deploying the access switches is to onboard the devices into HiveManager NG.

Log into your HiveManager NG account and complete the following steps to onboard access switches into HiveManager NG:

1. Navigate to **Monitor > Devices**, click the **Add** icon in the device table and click the box **Add Real Devices**.

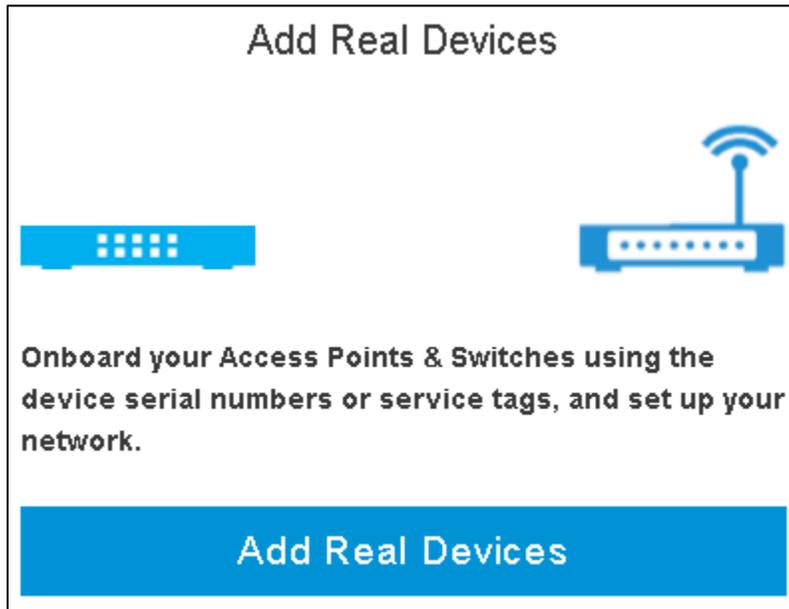


Figure 6 Add devices in HiveManager NG

2. Enter Dell service tag(s) for the switches to be onboarded into HiveManager NG, separated by commas, into the **Dell service tags** field, as Figure 7 shows, and click **Next**.

Add Devices

Step 1 of 2: Import / Enter Devices

Please enter the serial numbers of your Aerohive devices

Choose a file or drag directly here

Aerohive serial numbers

Serial Numbers (separated by a comma)

Example: 12345678900000, 12345678900001

Do you have other devices to add?

Choose a file or drag directly here

Dell service tags

ABC123D

Example: 8ZK47M1, 9ZK47M2

Figure 7 Add Dell service tag(s)

Add Devices

Step 2 of 2: Configure Your Devices (optional)

Configuration settings can be modified after adding devices.

Use an existing network policy:

--

OR

Create a new network policy:

Policy Name*

SSID Name*

Authentication*

A single network password is shared by all users

Network Password*

Figure 8 Optional network policy assignment and creation

3. Do not assign or create a network policy at this time.
 - a. This example shows detailed steps to create a network policy from the Network Policies page in the next section. Users can assign or create network policies here when it is convenient to do so.
4. Click **Next** and **Finish**.

Within a short time, each Dell Networking access switch contacts HiveManager NG. After onboarding has completed, the resulting device list shows your switches and should look similar to Figure 9.

<input type="checkbox"/>	Status	Make	Hostname	Firmware Version	Updated On
<input type="checkbox"/>	  	Dell	console	6.3.0.16	2016-08-25 11:02:02

Figure 9 Device list

This completes the onboarding process for Dell Networking switches.

The process for adding Aerohive APs is exactly the same and can be completed at the same time as the switch. The steps below show onboarding APs separate from the switch.

5. Navigate to **Monitor > Devices**, click the **Add** icon on the device table and click the box **Add Real Devices**
6. Enter Aerohive serial numbers(s), separated by commas, into the **Aerohive serial numbers** field, as Figure 7 shows.
7. Do not assign or create a network policy at this time.
8. Click Next and Finish.

After a short time, each Aerohive AP contacts HiveManager NG. The device list should look similar to Figure 10 after the addition of the switches and APs.

Note: You can customize the information contained in the columns by selecting the icon in the upper right hand side of the list.

<input type="checkbox"/>	Status	Make	Hostname	Firmware Version	Updated On
<input type="checkbox"/>	   	Aerohive	AH-594440	6.8r1	2016-08-25 11:24:40
<input type="checkbox"/>	   	Aerohive	AH-598640	6.8r1	2016-08-25 11:24:40
<input type="checkbox"/>	  	Dell	console	6.3.0.16	2016-08-25 11:02:02

Figure 10 Device list with APs

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

4.5 Network policy configuration

The network policy contains all device templates and common settings for the wired and wireless network.

A sample network policy includes the following information:

- Wired switch configuration
 - VLAN 1 for management
 - VLAN for employees
 - VLAN for guests
- Wireless
 - SSID for employees
 - SSID for guests
 - Employee authentication
 - Secure guest access using PPSK with self-registration

Note: The example above simplifies the features to show deployment methodology. You can add other settings and features for your network at any point in the deployment or management of the network.

Configure a network policy using the following steps:

1. Log into your HiveManager NG account.
2. Navigate to the Configure tab > Network Policies.
3. Click ADD NETWORK POLICY.
4. Policy Details tab
 - a. Ensure the **Wireless** and **Switches** checkboxes are checked (default).
 - b. Type a name in the **Policy Name** field, for example, *Small_Business_Deployment*.
 - c. Turn on the **Spanning Tree Protocol** by changing the slide button to **ON** as in Figure 11.

New Policy

What type of policy are you creating?

Wireless
 Switches

i For Dell switches, we recommend you turn ON Spanning Tree Protocol (STP).

Spanning Tree Protocol
▼ ON

Please name your policy

Policy Name*
Small_Business_Deployment

Description

Figure 11 New policy details page

- d. Click **Next**.
5. Employee SSID: Navigate to **Wireless Settings** tab, **Manage SSIDs**.
 - a. Click the **Add** icon, choose **All other SSIDs**.
 - b. Enter an SSID for the employee network in the **SSID name** field, for example, *AAA_Employee*.
 - c. Click **SSID Broadcast Name** to auto-populate the field with the previous SSID name.

SSID

SSID Name*
AAA_Employee

SSID Broadcast Name*
AAA_Employee

Broadcast SSID Using
 802.11 b/g/n (2.4 GHz radio)
 802.11 a/n/ac (5 GHz radio)

Figure 12 SSID name

- d. Click **Enterprise** for SSID Authentication.

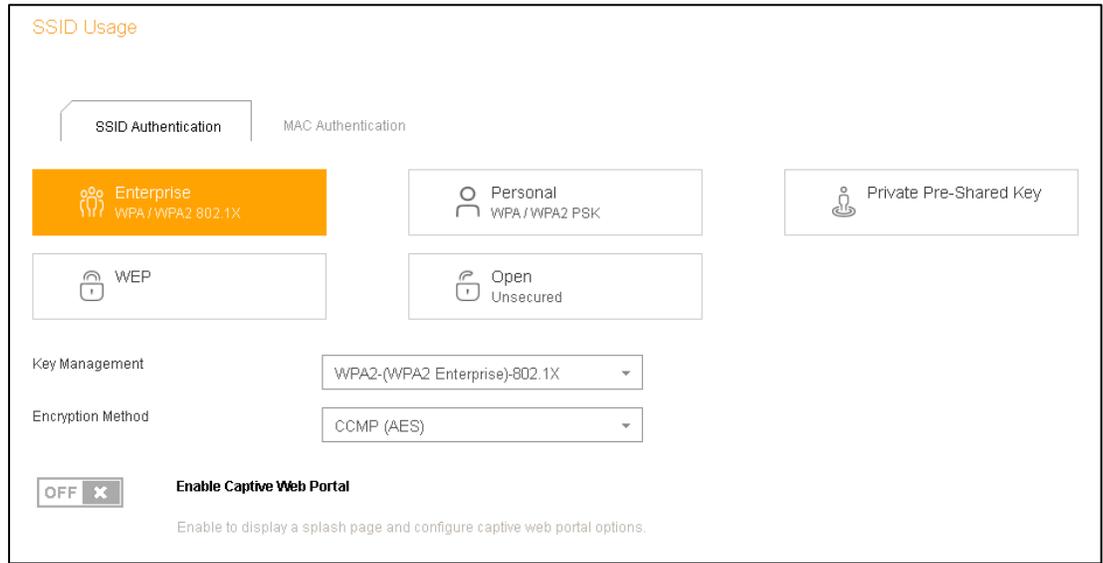


Figure 13 SSID Usage

- e. Find the **Authentication Settings** section.
- f. Activate the **Authentication with HiveManager NG Authentication Service** by changing the slide button to **ON**.
- g. Click the **Add** icon under **User Groups**.
- h. Enter a **User Group Name**, for example, *Employee*.
- i. Check **Email** under **Delivery Settings**.
- j. Leave all other options as their defaults.

New User Group

User Group Name*

Password DB Location

Password Type

Description

Allow Renewal Allow Renewal

Enable CWP Register Enable CWP Register

Password Settings

Generate Password Using* Letters Numbers Special Characters
 Enforce the use of

Generate Password Length
Maximum Password Length is 63

Expiration Settings

Require Authentication After Seconds

Account Expiration

Delivery Settings

Deliver Access Key by* Text Messages(SMS)

Email

Figure 14 User Group for Employees

k. Click **Save**.

The screenshot shows the 'Authentication Settings' page. At the top, it says 'Authentication with HiveManager NG Authentication Service' with a dropdown menu set to 'ON'. Below this is a section titled 'User Groups'. There is an 'Add' button and a trash icon. A table lists the user groups:

<input type="checkbox"/>	User Group Name	Password DB Location	# of Users
<input type="checkbox"/>	Employee	SERVICE	1 Add

Figure 15 Authentication Settings

- l. Click the **Add** link under the **# of Users** column for the Employee user group.
- i. Enter a **Name**, for example, *Employee 1*, and generate a **Password** by clicking the **Generate** box.
- 1) For an actual user, fill in the form with the employee information.
 - 2) The **Deliver Password, Email Address** can be the actual employee or an administrative intermediary.
 - 3) A message with login credentials and instructions is emailed after you click **Save**.

The screenshot shows the 'New User Account' form. It has the following fields and options:

- Create account in user group*: Employees
- Name*: Employee1
- Organization: [Empty field]
- Purpose of Visit: [Empty field]
- Email Address: [Empty field]
- Phone Number: Country Code + Phone
- Password*: [Masked field] with a 'Generate' button and a 'Show Password' checkbox.
- Description: [Empty text area]
- Deliver Password: [Section header]
- Email Address: abc@aaa.com

Figure 16 New User Account

- ii. Click **Save**.
 - 1) Repeat the steps starting with step k, for each additional user.
 - 2) Add Users at any time after completing the network policy.
- m. Find the **User Access Settings** section.
 - i. Create a new **Default User Profile** by clicking the **+** icon in the section.
 - ii. Enter a **User Profile Name** in the field, for example, *Employee*.

Figure 17 User Profile

- iii. Add a new VLAN by clicking the **+** icon next to the **Connect to VLAN** field.
- iv. Enter a VLAN name in the **Name** field, for example, *EmployeeVLAN10*.
- v. Enter a VLAN number in the **VLAN ID** field, for example, *10*.

Figure 18 New VLAN object

- vi. Click **Save**.
- vii. The **Connect to VLAN** field populates with the new VLAN object.
- viii. Leave other settings as default,
- ix. Click **Save**.
- x. The **Default User Profile** populates with the new object created above.
- n. Leave all other settings as their defaults.
- o. Click **Save**.

6. Guest Access SSID (self-registration with PPSK): Navigate to **Wireless Settings** tab > **Manage SSIDs**
 - a. Click the **Add** icon, choose **Guest Access SSID**.
 - b. Enter an SSID for the employee network in the **SSID name** field, for example, *BBB_Guests*.
 - c. Click on the **SSID Broadcast Name** field and the field auto populates with the previous SSID name, as in Figure 19.
 - d. Find the **Authentication Type > Private PSK** section.
 - i. Choose **Guests can self-register, then sign in**, as in Figure 20.
 - ii. Enter an SSID in the **Guest Self-Registration SSID** field, for example, *BBB_Guest_registration*.

New Guest Access SSID

*SSID Name

*SSID Broadcast Name

Authentication Type Note: You will not be able to edit the Authentication Type after saving.

> Unsecured (Open) Network

▼ Private PSK

Set the maximum number of clients per private PSK Range 0-15, 0 = no limit

Create credentials for guests to login to your network. [Customize Captive Web Portal >](#)

Guests can self-register, then sign in. As an option, an employee can approve.

Enable employee approval.

*Guest Self-Registration SSID

Save

Figure 19 New Guest Access SSID

- e. Click on the box labeled **Customize Captive Web Portal**.
 - i. Change the **Name** field to a descriptive name, for example, *BBB_Guest_web_portal*.
 - ii. All other settings within this section can be left as default.

Figure 20 Guest Captive Web Portal

- iii. Click **< Done**.
- f. Click on the box labeled **Pre-Defined Settings**.
 - i. Enter a descriptive **Name**, for example, *BBB_Guest_Access_profile*.
 - ii. Add a new **VLAN** by clicking the **+** icon next to the **Connect to VLAN** field.
 - 1) Enter a VLAN name in the **Name** field, for example, *GuestVLAN20*.
 - 2) Enter a VLAN number in the **VLAN ID** field, for example, *20*.
 - 3) Click **Save**.
 - 4) The **Connect to VLAN** field populates with the new VLAN object created above.
 - iii. Leave other settings as default.

- iv. Click **Save**.

New Guest Access SSID

< Cancel Save

Pre-Defined Guest Access Settings

For advanced settings, go to Common Objects > User Profiles.

This SSID will use the default User Profile unless you create one below.

Rename Guest Access Settings

Name*

VLAN

Connect to VLAN* +

Firewall Policy Used

Firewall settings have been disabled for this profile.

Pre-Defined Settings >

User Group Settings >

Save Cancel

Figure 21 Guest User profile settings

- g. Click on the box labeled **User Group Settings**.
 - i. Enter a **User Group Name** in the field, for example, *BBB_Guest_User_Group*
 - ii. Leave all other settings as default, if desired.

- iii. Click **Save**.

Figure 22 Guest User Group settings

- h. Leave all other settings as default.
- i. Click **Save**.
- j. Click **Close**.
 - i. The open SSID for guest registration and the secure SSID for guest access have been created and can be seen in the **Wireless SSIDs** list.

SSID	Guest Access	Access Security	VLAN
ABC_Employee		WPA / WPA2 802.1X (Enterprise)	General100
BBB_Guest_registration	Edit	Unsecured (Open) Network	
BBB_Guests	Edit	Private PSK	Guest/VLAN20

Figure 23 Wireless SSID list

- 7. Navigate to Wireless Settings tab, Device Templates.
 - a. Click the **Device Templates** box next to **Manage SSIDs**.
 - b. Click the **Add** icon above the records table.
 - i. Choose the appropriate model of AP.
 - ii. If more than one model exists in the network, repeat steps 7.a. thru 7.e. for each model.
 - c. Enter a **Template Name**, for example, *AP230_AAA*.
 - i. Keep all other settings as default.
 - d. Click **Save**.

- e. Click **Next**.



Figure 24 Device template

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

8. Switch Settings tab, Device Templates.
- a. Click the **Add** icon located above the records table.
 - b. Choose the switch model being deployed, for example, *N1524P*.
 - c. Enter a name in the **Template Name** field, for example, *N1524P_AAA*.
 - d. Click port 1 (Gi1/0/1) to highlight the connection to the firewall.
 - e. Click **Assign, Create New** with port 1 highlighted.
 - f. Enter a **Name** for the new port type, for example, *to_firewall*.
 - g. Find the **Port Usage Settings** section.
 - i. Select **Trunk Port**.
 - h. Click **Save** within the **New Port Type** section.
 - i. Configure **Trunk VLANs** as follows:
 - i. Keep VLAN 1 as **Native VLAN**.
 - ii. Enter VLANs 1, 10, 20 into the **Allowed VLANs** field.

- iii. Click **Save**.

New Port Type

Name*

Description

Port Status ON

Port Usage Settings

Port Usage

- Access Port
- Phone with a data port
- Trunk Port (802.1Q VLAN Tagging)

Figure 25 New Port Type

Trunk VLANs

Native VLAN:

Allowed VLANs:

Note: VLANs can be configured as ranges or individually. Indicate a range with a hyphen (-). Separate VLAN entries with commas (,), for example, 1-30, 100-200, 500.

Cancel Save

Figure 26 Trunk VLANs

- j. Click ports 10 and 20 (Gi1/0/10 and Gi1/0/20) to highlight the connection to the wireless APs (ensure port 1 is not highlighted by deselecting it if necessary).
- k. Click **Assign, Create New** with port 10 and 20 highlighted.
- l. Enter a **Name** for the new port type, for example, *to_AP*s.
- m. Find the **Port Usage Settings** section.
 - i. Select **Trunk Port** as the **Port Usage**.
- n. Click **Save** in the **New Port Type** section.

- o. Configure **Trunk VLANs** as follows:
 - i. Keep VLAN 1 as **Native VLAN**.
 - ii. Enter VLANs 1, 10, 20 into the **Allowed VLANs** field.
 - iii. Click **Save**
- p. Click port 2 (Gi1/0/2). Ensure all other ports are not highlighted.
- q. Click **Assign, Create New** with port 2 highlighted.
- r. Enter a **Name** for the new port type, for example, *wired_access_employee_PC*.
- s. Find the **Port Usage Settings** section.
 - i. Ensure **Access Port** is selected (default).
- t. Find the **VLAN ID** section.
- u. Configure VLAN ID as follows:
 - i. Using the list icon: , select the **EmployeeVLAN10** setting that was configured in the previous steps.
 - ii. Click **Save** within the **New Port Type** section

N1524P Template

Template Name*

N1524P Switch Template



Port Type in Use

Port Type Name	Applied to Ports	Authentication	VLAN
Access Port	3,4,5,6,7,8,9,11,12,13,14,15,16,17,18,19,21,22,23,24 SFP+: 1,2,3,4	...	1
to_firewall	1	...	1[Allowed: 1,10,20]Select...
wired_access_employee_PC	2	...	10
to_APs	10,20	...	1[Allowed: 1,10,20]Select...

Figure 27 Final Template settings

- v. Click **Save**
- w. Click **Next**

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

9. Additional Settings

- a. Find the **DNS Server** settings on the left-hand side.
 - i. Turn off the **DNS Server** using the slide button (this example sets the DNS addresses through DHCP).
 - ii. Click **Save**.
- b. Find the **NTP Server** settings on the left-hand side.
 - i. Turn off **NTP Server** using the slide button. (This example does not use an NTP Server, but you can configure this setting at any time.)
- c. Click **Save**.
- d. This example leaves all other Settings within **Additional Settings** as default.
- e. Click **Next**.

10. Deploy Policy

- a. Select the switch device(s) by clicking on the check box next to each switch.
- b. Click **Upload**.
- c. Ensure **Update Network Policy and Configuration** is checked.
 - i. Do not check the Upgrade Dell Switch Images.
- d. Click **Perform Update** and wait for the update to complete.
- e. Select the AP devices by clicking on the check box next to each AP.
- f. Click **Upload**.
- g. Ensure only **Update Network Policy and Configuration** is checked.
- h. Select **Complete Configuration Update** under **Update Network Policy and Configuration**
 - i. First-time network policy applications require a complete Configuration Update.
 - ii. Subsequent changes to the network policy can use Delta Configuration Update.
- i. Click **Perform Update** and wait for the update to complete.

At this point, a fully functional, basic configuration for a retail or small business office is complete. Administrators can modify and add to the configuration at any time.

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

4.6 Supplemental CLI

HiveManager NG provides GUI-based configuration for the most popular and frequently used switch features. For more advanced features and features that most users prefer to configure via CLI, HiveManager NG provides the Supplemental CLI feature. This section steps through a Supplemental CLI example configuration.

Before starting the network policy configuration, ensure that the Supplemental CLI feature is enabled. To enable the feature, use the following steps:

1. Click **Account Details** In the upper right-hand corner of the screen, as Figure 28 shows:

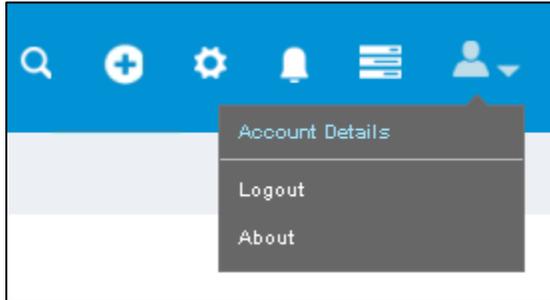


Figure 28 Account Details

2. Select **VHM Management** on the left-hand side.
3. Turn on the Supplemental CLI by changing the **Supplemental CLI** slide button to **ON** in the VHM Management section, as in Figure 29:

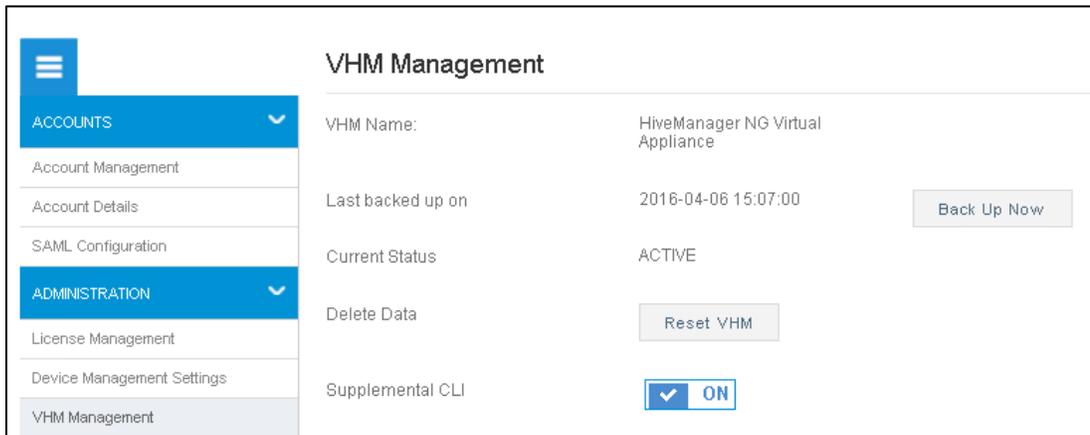


Figure 29 Supplemental CLI – on

By enabling the Supplemental CLI, the GUI exposes the Supplemental CLI at the device-level configuration for Dell Switches.

Note: The Supplemental CLI for Dell switches is only available at the device level configuration. For additional information on the use of the Supplemental CLI for APs, see HiveManager NG documentation at docs.aerohive.com/dellcloud.

4. Navigate to the **Monitor** tab > **Devices** list.
 - a. Select the checkbox next to the Dell switch
 - b. Click on the **Edit** icon:  near the top of the list to edit the device configuration as Figure 30 shows.



Figure 30 Editing device configuration

- c. Click on **Device Configuration** from the left-hand column
- d. Click on the + icon on the Supplemental CLI field
- e. Enter a **Name**
- f. Enter a **Description** (optional)
- g. Enter the command script in the **CLI Commands** field
 - i. If following the example as written, the CLI commands below can be copy/pasted directly into the text field.
 - ii. Make necessary changes to the CLI commands below if your network is different than this step-by-step example.
- h. Click **Save**.

Note: The commands placed into the CLI Commands text box execute in order, just as if typed into the actual CLI. Commands such as “configure” and “exit” are necessary to enter and exit the required modes. If the script commands “exit” and “end” cause the command line to leave the configuration mode, subsequent configuration commands in the script do not execute.

Sample CLI commands for input into the CLI Commands text box:

```
enable
configure

ip routing

interface vlan 10
ip address 10.1.10.10 255.255.255.0

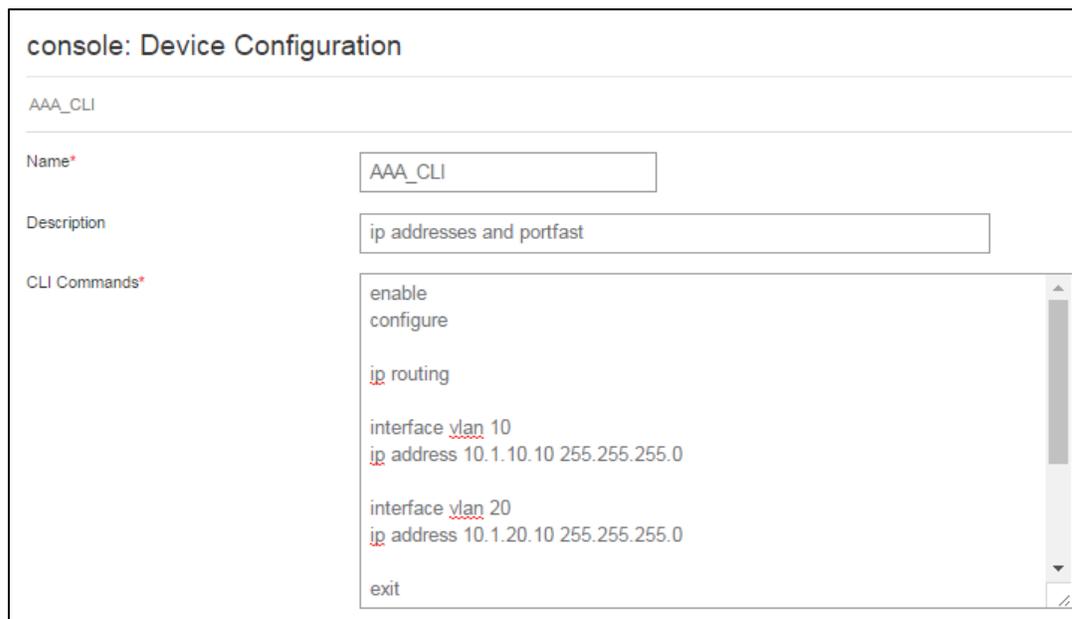
interface vlan 20
ip address 10.1.20.10 255.255.255.0

exit

interface gil/0/2
spanning-tree portfast
spanning-tree portfast bpdufilter default

end
```

Note: The previous example Supplemental CLI script illustrates the format of a standard script. Each retail or small business office environment requires specific commands features.



The screenshot shows a web-based configuration interface titled "console: Device Configuration". It features a form for creating a supplemental CLI script. The form has three main sections: "Name*", "Description", and "CLI Commands*".

- Name*:** A text input field containing "AAA_CLI".
- Description:** A text input field containing "ip addresses and portfast".
- CLI Commands*:** A large text area containing the following commands:

```
enable
configure

ip routing

interface vlan 10
ip address 10.1.10.10 255.255.255.0

interface vlan 20
ip address 10.1.20.10 255.255.255.0

exit
```

The CLI Commands* field has a vertical scrollbar on the right side, indicating it can hold more text. There is a small icon in the bottom right corner of the text area, possibly for clearing or saving the content.

Figure 31 Supplemental CLI configuration screen

console: Device Configuration

Device Details

Host Name*

Network Details

Network Policy

Device Template +

Supplemental CLI

Supplemental CLI +

Figure 32 Device Configuration with Supplemental CLI

The following process applies the Supplemental CLI to the appropriate Dell switch.

- i. Ensure the correct **Supplemental CLI** name is selected in the dropdown menu.
- j. Review the settings for **Network Policy** and **Device Template**.
- k. The settings pushed via the Network Policy, Deploy Policy tab should be currently listed; no action is needed.
- l. Click **Save**.
 - i. This **Save** commits the script shown in the pulldown menu. Edits to or addition of a new script does not apply the script to the device, even though it auto-populates the field.
- m. Navigate back to the **Device** List.
- n. Ensure the checkbox next to the appropriate Dell Switch device is checked.
- o. Click **Update Devices** in the upper right corner of the list.
- p. Ensure **Update Network Policy and Configuration** is checked.
 - i. Do not check the Upgrade Dell Switch Images.
- q. Click **Perform Update**.

A best practice when using the Supplemental CLI is to verify that the commands sent via the device-level configuration push successfully execute on the switch. Verification of the running configuration may require local console access or an SSH connection.

Cloud Deployment

- Onboard access switches
- Onboard APs
- Configure Network Policy
 - Configure WLAN SSIDs and AP template
 - Configure access switch template
- Deploy network policy to access switch and APs
- Configure access switch with Supplemental CLI
- Deploy Supplemental CLI to access switch

A Software versions

Table 1 Minimum software versions

Component	Description
Dell Networking OS	v6.3.0.16 or later (N1500, N2000, N3000 series switches)
Aerohive AP230 firmware	v6.8r1
HiveManager NG cloud	Automatic updates
HiveManager NG Virtual Appliance	v11.14.0.3

B Additional resources

The following websites and documents provide further helpful information:

[Support.dell.com](http://support.dell.com)

The Dell support site is focused on meeting your needs with proven services and support.

DellTechCenter.com

TechCenter is an IT Community where you can connect with Dell Customers and Dell employees for the purpose of sharing knowledge, best practices, and information about Dell products and installations.

[HiveManager NG Technical Documentation](#)

The technical documentation website is a location to find information about the latest release, new hardware, supported software, devices, browsers, and other guides.

[HiveManager NG Product Page](#)

Dell product page describing HiveManager NG, supported switches and APs.

Table 2 Supplemental documents

Wired + Wireless Cloud Managed Campus Reference Architecture
http://en.community.dell.com/techcenter/networking/m/networking_files/20442898
Wired + Wireless Cloud Managed Campus Deployment Guide – Large Campus
http://en.community.dell.com/techcenter/networking/m/networking_files/20442897

Support and feedback

Please use the information below to provide feedback on how we could make this reference architecture more useful for your circumstances.

Contacting Technical Support

Support Contact
Information

Web: <http://Support.Dell.com/>

Telephone: USA: 1-800-945-3355

Feedback for this document

We encourage readers of this publication to provide feedback on the quality and usefulness of this deployment guide by sending an email to Dell_Networking_Solutions@Dell.com.

Note: Please include the document title and version in the subject of the email.

About Dell EMC

Dell EMC is a worldwide leader in data center and campus solutions, which includes the manufacturing and distribution of servers, network switches, storage devices, personal computers, and related hardware and software. For more information on these and other products, please visit the Dell EMC website at <http://www.dell.com>.