

Wired + Wireless Cloud-managed Campus Deployment Guide – Large Campus

Dell Networking Solutions Engineering
September 2016

Revisions

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

Copyright © 2016 Dell Inc. or its subsidiaries. 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 logo, Dell Boomi™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of Dell. 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. 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. 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 QLogic is a registered trademark of QLogic Corporation. 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, large campus deployment	7
2.1 Cloud-managed reference design topology, large campus.....	7
2.1.1 Description, goals and assumptions.....	8
3 Deployment example – Preparing for deployment	9
3.1 Prerequisites.....	9
3.1.1 Security and internet connectivity prerequisites	9
3.2 Aggregation layer prerequisites.....	10
3.3 Access layer prerequisites.....	11
3.3.1 Minimum configuration items:.....	11
3.4 Cloud management network.....	11
3.5 Recommendations and precautions	13
4 Deployment example - Step by step instructions	14
4.1 Firewall initial setup	15
4.2 Aggregation layer initial setup	16
4.3 Management switch initial setup.....	17
4.4 Access layer switches initial setup	18
4.5 Onboarding Dell Networking N-Series switches to HiveManager NG.....	20
4.6 Network policy configuration.....	23
4.7 Supplemental CLI	38
4.8 Aerohive AP onboarding to HiveManager NG.....	45
4.9 HiveManager NG Virtual Appliance	47
A Software versions	48
B Additional resources.....	49
C Support and feedback	50
About Dell EMC	50

Introduction

IT managers are looking to support rapidly changing and diverse user access requirements across their networks without added administration resources. They must adapt their networks to address the needs of key business functions while providing reliability, performance and flexibility. Today's businesses require campus networks to provide reliable, high-performance wired and wireless connectivity. These networks must be capable of delivering rich applications and access to corporate resources regardless of device form factors.

Deploying large campus networks in local or remote locations can be a costly and time consuming task. Figure 1 shows a wired and wireless, cloud-managed network; it is an example of one of the most critical deployment scenarios. Monitoring and maintaining such networks throughout their lifetimes requires less effort and fewer resources.

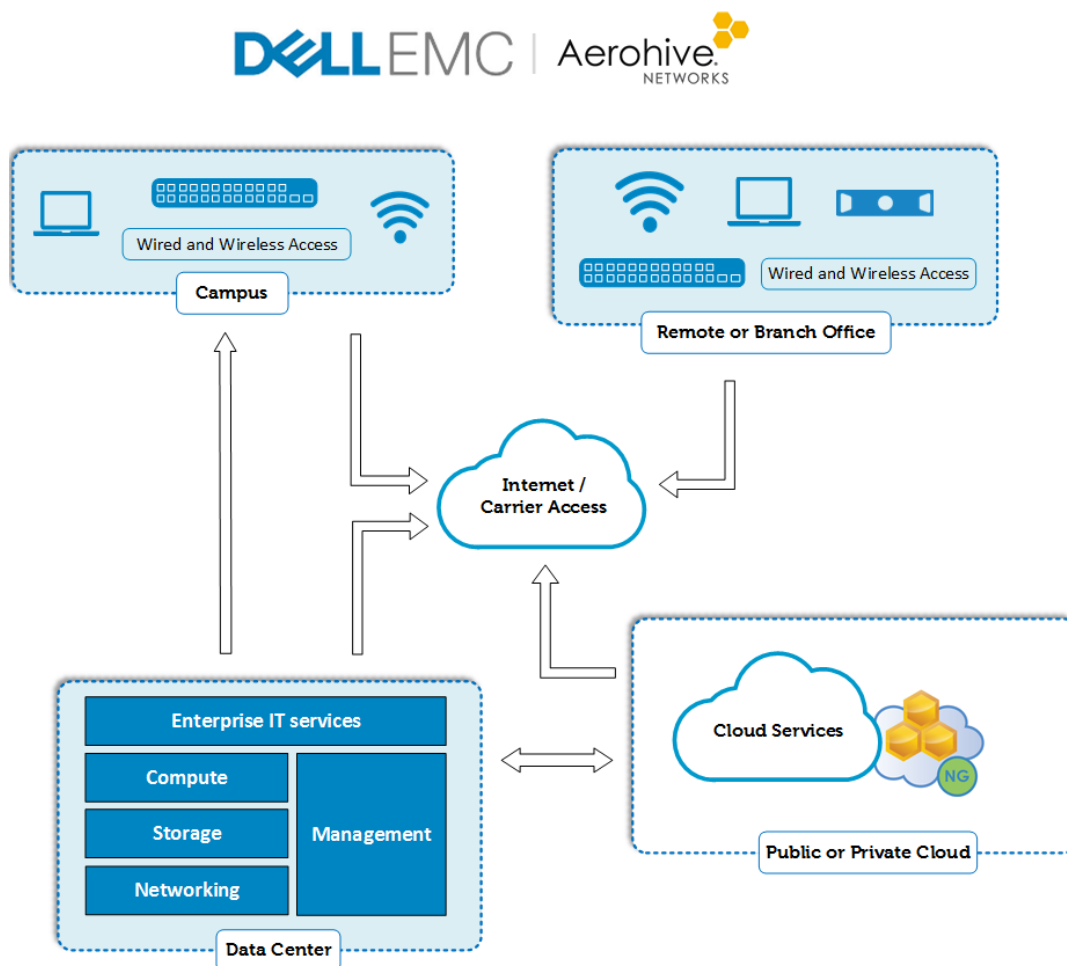


Figure 1 Cloud-managed campus – global view

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
- Incorporating cloud management into the modern, end-to-end campus network
- Delivery of the latest technology to address speed, bandwidth, redundancy and failure-resistant networks

This guide describes the creation and maintenance of a wired and wireless network that performs well and meets modern 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 by 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 wireless access points

- AP130
- AP230
- AP250
- AP245X
- AP1130

2 Cloud-managed, large campus deployment

The goal of the cloud-managed large campus deployment is to help IT administrators deploy and manage their access network. This document shows the methodology for using HiveManager NG to deploy both wired and wireless devices, along with continuous cloud management functionality.

2.1 Cloud-managed reference design topology, large campus

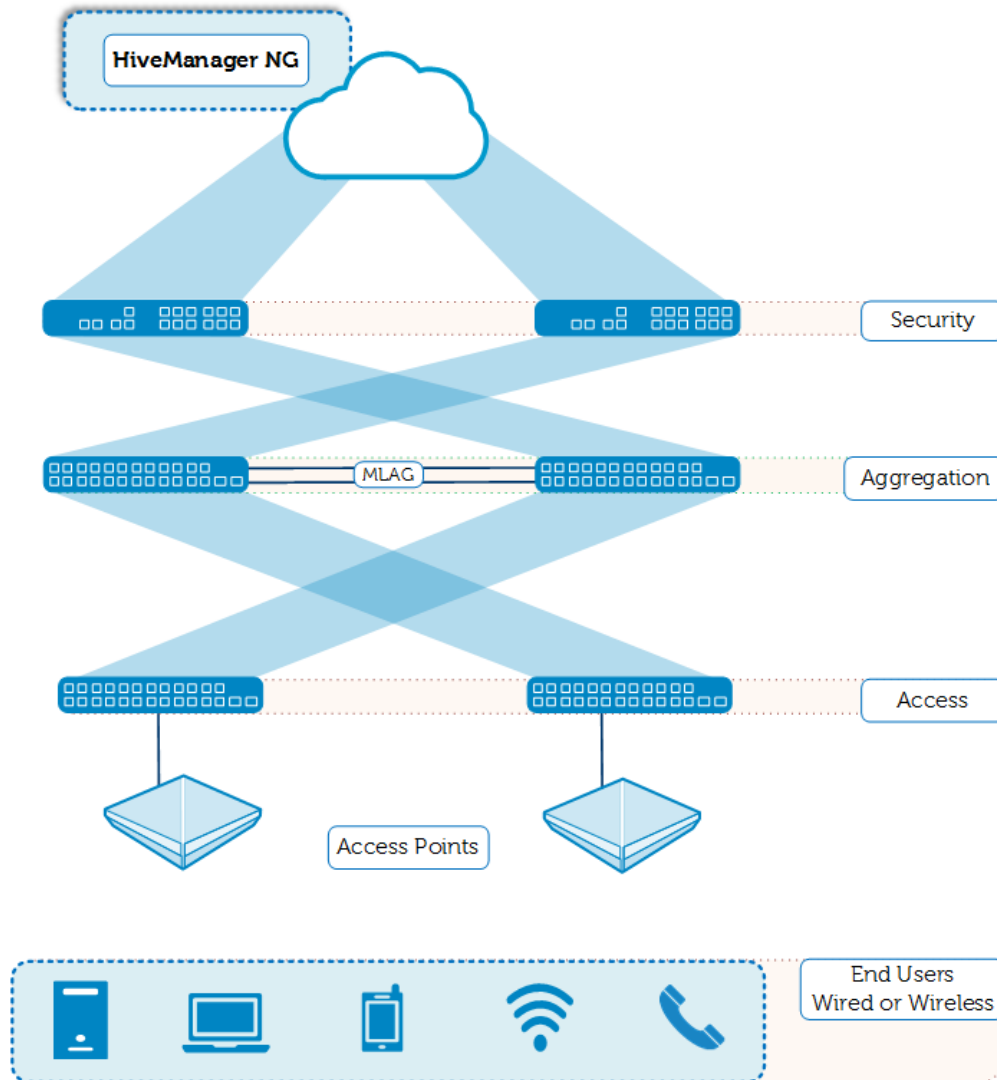


Figure 2 Cloud-managed campus topology, large campus

Note: Deployment via HiveManager NG requires a dedicated management network to the access switches. Figure 2 does not show the management switch detailed in section 4.4.

2.1.1 Description, goals and assumptions

Large business networks are typically designed with multi-layer redundant switching, access points, and firewalls with High Availability (HA) as seen in Figure 2. For additional information on large campus networks, see the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#).

The devices and use-case documented in this guide reflect a single campus network. Many businesses have numerous sites and can use this example to scale across multiple sites and geographical locations.

Devices used in validation:

- SonicWALL NSA 6600 firewalls
- Dell Networking N4064F switches (aggregation layer)
- Dell Networking N3048P and N3024F switches (access layer)
- Dell Networking N3024 switch for the management network
- Aerohive AP230 access points

Assumptions:

- Single public IP for WAN
- RADIUS, DNS, AD, NPS, CA services are available

Goals:

- Zero-touch deployment of access switches and access points
- Network administration of access devices through HiveManager NG
- Unified wired and wireless network policy
- Wireless guest access
- Wired and wireless connectivity for PCs and peripherals

3 Deployment example – Preparing for deployment

This section discusses requirements and procedures for deploying a large-campus, cloud-managed network.

3.1 Prerequisites

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

3.1.1 Security and internet connectivity prerequisites

The large campus topology diagram in Figure 2 shows two SonicWALL firewalls in a high availability (HA) configuration. The model used for validating this document is the SonicWALL NSA 6600. Use the firewall model that fits the performance and feature requirements of the network.

Administration of the SonicWALL is enabled through the WAN interface for remote deployment and test purposes.

- Assumptions:
 - Internet access is established and available onsite.
 - The IP address assigned to the WAN port on the firewall supports remote access.
 - This example omits any additional routing equipment outside the firewall.
- Minimum configuration items:
 - WAN interface and zone
 - LAN interfaces and zone
 - > LAN interface for cloud management network (VLAN1 subnet)
 - > LAN interface for standard internet traffic
 - Routing policies set for VLAN 1 subnet
 - > Any Source-to-VLAN 1 destination
 - Routing policies set for the internet traffic subnet
 - > Any Source-to-VLAN 50 destination
 - NAT policies for VLAN 1 and VLAN 50 in place
 - HA configuration
 - > Primary and Secondary IP addresses assigned
 - > Mode set to Active/Standby
 - > HA Data Link and HA-Link interfaces in place

Note: This example uses the default SonicWALL firewall access rules. After establishing the network, configure further security settings to meet organizational security requirements.

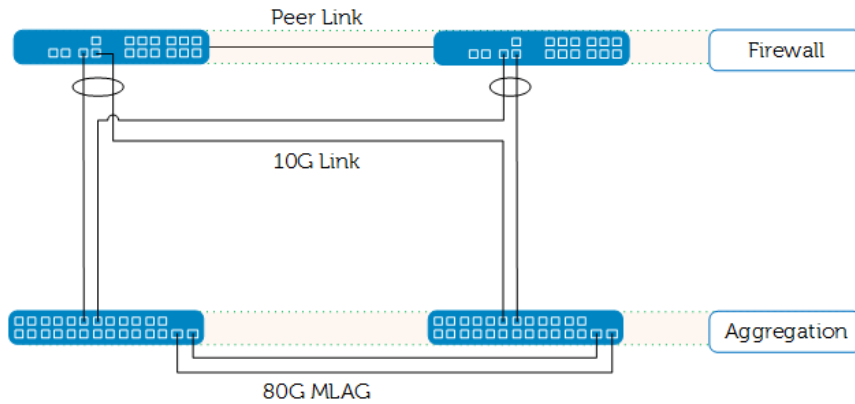


Figure 3 Initial setup for SonicWALL to aggregation

Note: Figure 3 does not show connection to the management network. See section 4.4 for details.

3.2 Aggregation layer prerequisites

The foundation of the Cloud-managed Campus Reference Architecture is the N-Series topology of the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#). This reference architecture uses Multi-chassis Link Aggregation (MLAG) to provide high availability and full bandwidth utilization.

- Assumptions:
 - Both N4064F switch command line interfaces (CLI) support remote access.
- Minimum configuration items:
 - Interfaces to the firewall
 - > Port channels configured, active LAG
 - MLAG Peer link
 - VPC domain
 - VRRP for all VLANs
 - Default route set to firewall LAN IP address
 - Inter VLAN routing enabled
 - RSTP-PV

- Optional configurations for initial deployment:
 - Additional VLANs for non-management traffic
 - Port interfaces for connections to clients and servers not involved in deployment
 - Other miscellaneous features not interfering with traffic during deployment

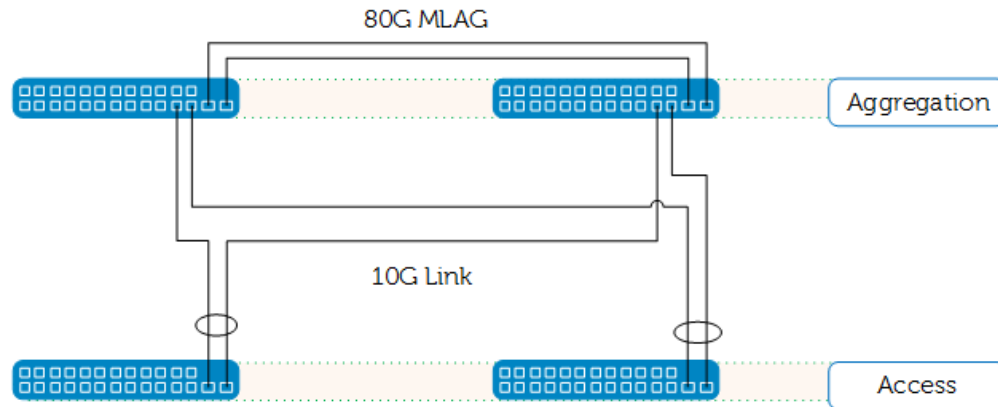


Figure 4 Aggregation and access switches

3.3 Access layer prerequisites

The access switch is the device deployed and managed by HiveManager NG cloud management. This example applies to all Dell Networking switch models and Aerohive access points identified in Section 2. For additional details on the cloud-managed switches, see the [Wired + Wireless Cloud-managed Campus Reference Architecture](#) and [Supported Switches and Access Points](#) at Dell.com.

- Assumptions:
 - All switches 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 port that administrators can configure for management purposes. The Dell N1500 and N2000 series switches only have standard in-band interfaces. For consistency, the deployment steps in this document describe the public cloud management and no-touch deployment through VLAN 1 on in-band interfaces.

3.3.1 Minimum configuration items:

No configuration required; retain or reset to factory defaults.

3.4 Cloud management network

In multilayer networks with redundancy that includes active or dynamic LAG interfaces to the aggregation layer, LAG negotiation can cause temporary loss of connectivity. To ensure constant connectivity, a separate management network is established to facilitate a path from the access switches to the firewall, bypassing the aggregation layer. HiveManager NG must maintain connectivity to the access switches throughout the configuration update process.

- Assumptions:
 - Management network uses VLAN1
- Minimum configuration items:
 - Management switch configuration includes the DHCP server feature for VLAN 1.
 - > A dedicated DHCP server is an acceptable alternative.
 - RSTP-PV

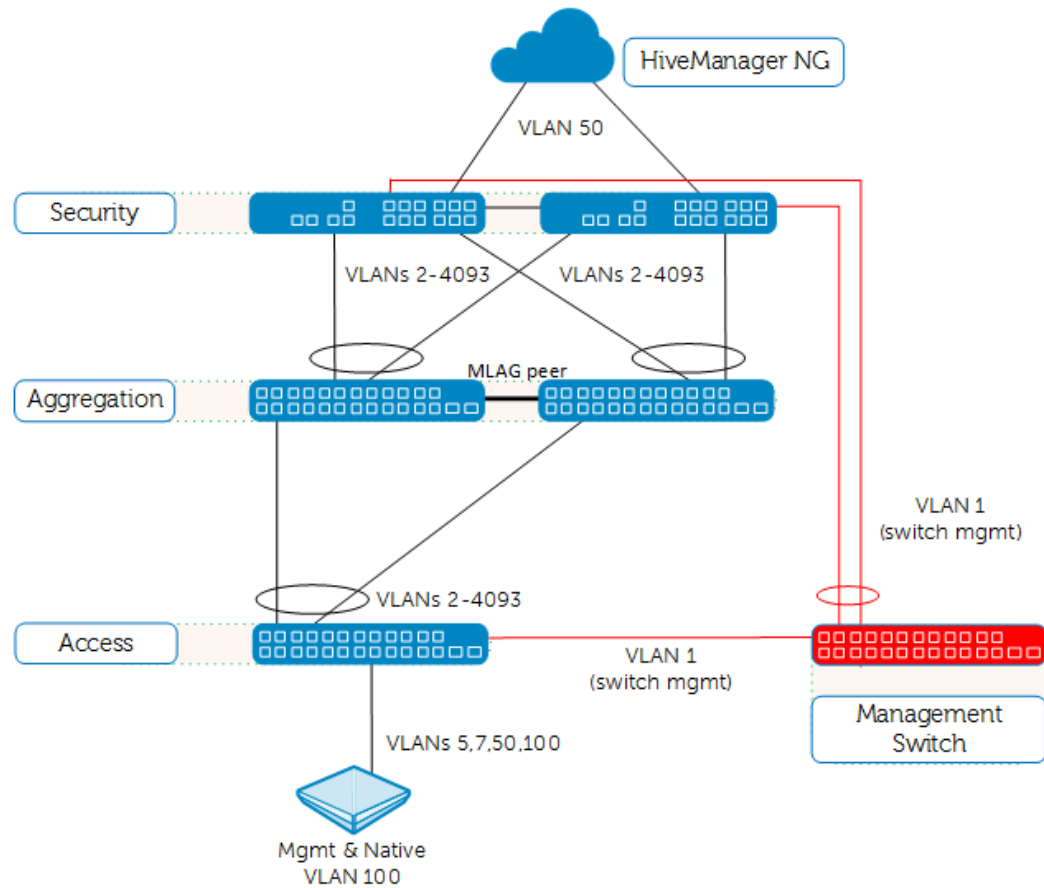


Figure 5 Management network with campus network topology

Note: VLAN 1 is the default management network for HiveManager NG. VLAN 1, with DHCP enabled, is also the factory default interface configuration on Dell N-Series switches. When deploying access switches from HiveManager NG, Dell EMC recommends using the default settings. Dell EMC recommends further configuration for management network security immediately after deployment.

3.5 Recommendations and precautions

HiveManager NG delivers a very powerful management and monitoring tool. When utilized with Dell switches, 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.
 - Interrupted connectivity can cause incomplete updates.
- 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 execute in the appropriate mode or interface.
- Ensure that the script executes properly before remote deployments.
- Complex configurations may require intermediate steps using multiple configuration updates.
- Update only one Device Configuration parameter per device update action.
 - Concurrently updating the Network Policy, Device Template, and Supplemental CLI 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 unsupported 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 Deployment example - Step by step instructions

This section provides detailed deployment steps used in a test environment with the example topology shown in Figure 2. This process is designed for all devices to use the simplest initial configuration necessary to establish a basic campus network.

Note: Best practice is to always perform a proof-of-concept for large scale, remote deployments.

Site Preparation and Standard Deployment

- ☐ Physical installation and cabling
- ☐ Configure firewalls
- ☐ Configure aggregation switches
- ☐ Configure management switch

Cloud Deployment

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

4.1 Firewall initial setup

This example uses two SonicWALL NSA 6600 model firewalls. The interfaces used in actual deployments, including the speed and other capabilities, can differ from the example. The example provides sample interface port numbers to allow the reader to follow the methodology.

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

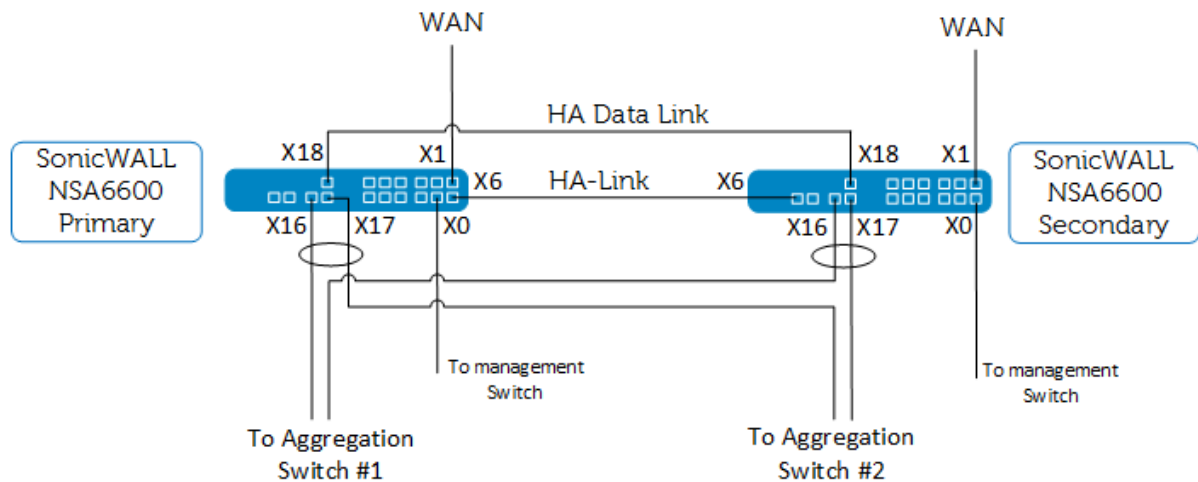


Figure 6 Firewall cabling

The firewall is the path from the internet (WAN) to the access switch (LAN) via the management switch. This example enables the WAN interface to also serve as the firewall management interface.

Configuration steps

Use the following steps to configure the firewall:

1. X1 interface: Assign the public IP address, gateway, and DNS server for the WAN zone on each firewall.
2. X0 interface: Assign an IP address within the VLAN 1 subnet for the management network.
 - a. This address is for management traffic. This example used 10.1.1.254/24.
 - b. See Table 1 in section 4.6 for subnet descriptions.
3. X16 interface: Assign an IP address for the LAN on the Primary firewall.
 - a. This address is the gateway for your private network's traffic to the internet. This example used 10.1.50.254/24.
 - b. Enable link aggregation, and assign the X17 interface as the aggregate port.
4. Configure High Availability
 - a. Set Mode as Active/Standby, enable Stateful Synchronization, and enable Virtual MAC.
 - b. Set HA Control Interface to X6.
 - c. Set HA Data Interface to X18.
 - d. Monitoring – Set a unique IP address for each interface of the Primary and Secondary firewalls.
5. Configure routing policies for each subnet in the LAN.
6. All other settings remain as default.

Connect cables to the aggregation and management switches.

4.2 Aggregation layer initial setup

This example uses two Dell Networking N4064F switches. Deployment and configuration of the aggregation layer is completed independently from the access switches and wireless access points. Access the aggregation layer for management through traditional console access or another network management system, such as Dell Open Manage Network Manager (OMNM). The configuration is identical to the example used in the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#).

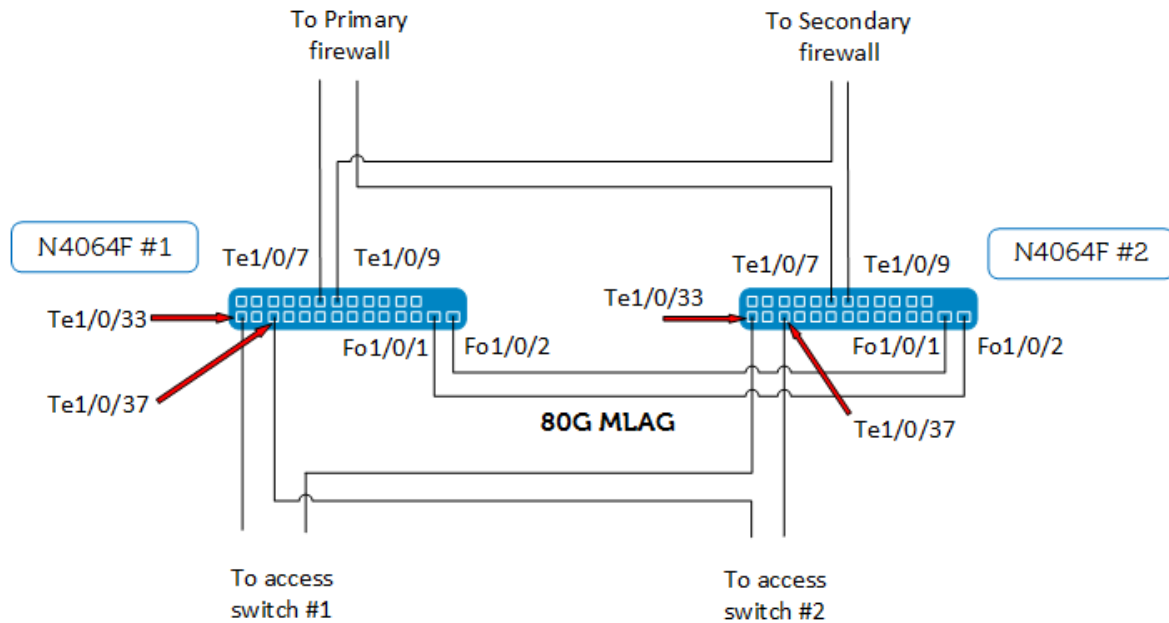


Figure 7 Aggregation cabling

Configuration steps

Use the following steps to configure the aggregation layer:

1. Configure inter-VLAN routing
2. Configure VLANs
 - a. This example uses VLANs designated for employee (5), guest (7), internet (50), and general network use (100).
3. Configure default gateway to internet.
 - a. This example uses VLAN 50, 10.1.50.254/24
 - b. See Table 1 in section 4.6 for subnet descriptions.
4. Configure static LAG interfaces to the firewalls
 - a. This example uses interfaces Te1/0/7 & Te1/0/9, with port channel 7 & 9
5. Configure dynamic LAG interfaces to the access switches
 - a. This example uses interfaces Te1/0/33 & Te1/0/37, with port channel 33 & 37
6. Configure MLAG peer link
 - a. This example uses interfaces Fo1/0/1 & Fo1/0/2, with port channel 1
7. Configure VPC
8. Configure VRRP for each VLAN
9. Configure RSTP-PV

Note: The preceding steps are not intended to be step-by-step. Find details on configuring MLAG peer and partner links in [Using MLAG in Dell Networking N-Series Switches](#). Find other features and example configurations in the *Dell Networking N-Series User's Configuration Guide*, located at [Dell Support](#). The configuration files for the aggregation switches are attached to this document. Filename: *4064F_Aggregation_switch1_config.txt* and *4064F_Aggregation_switch2_config.txt*

4.3 Management switch initial setup

This example uses a N3024 model switch for the management network. The purpose of the management switch is to allow VLAN 1 traffic to reach the access switches without needing to traverse the aggregation layer. The path through the aggregation layer cannot be established until the access switches are onboarded and a complete network policy and Supplemental CLI are pushed.

The diagram in Figure 5 shows the detail for the management switch network. The interface numbers are not significant since each interface retains its default configuration.

Configuration steps

Use the steps below for initial configuration of the management switch:

1. Configure VLAN 1 interface IP address. For this example 10.1.1.10/24 is used.
2. Configure default gateway to firewall. For this example 10.1.1.254 is used
3. Configure DHCP sever (optional if using separate DHCP server)
 - a. The VLAN 1 DHCP server scope should be able to provide for all access switches
4. Configure RSTP-PV

Note: No-touch deployment of the access switches requires DHCP. In this example, the management switch also acts as the VLAN 1 DHCP server. Customers can use a separate DHCP server, which the diagrams do not show. The configuration used during validation for the Management switch is included as an attachment. Filename: *Management switch config.txt*

4.4 Access layer switches initial setup

This example uses a N3000 Series model switch. The example provides sample interface port numbers to allow the reader to follow the methodology. HiveManager NG can also deploy and manage N2000 and N1500 series switches. Configuration and deployment steps are the same and have been validated. The configuration is similar to the example used in the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#).

Note: The Campus Reference Architecture 3.0 utilizes stacks of N-Series switches. At the time of publication, HiveManager NG is not capable of configuring and monitoring switches configured in a stack.

The active path for management traffic to HiveManager NG is through the management switch, as seen in Figure 8.

No configuration is required for the access switches.

Note: Best practice is to have the factory default settings on the access switches during deployment. HiveManager NG cannot import settings from the switch.

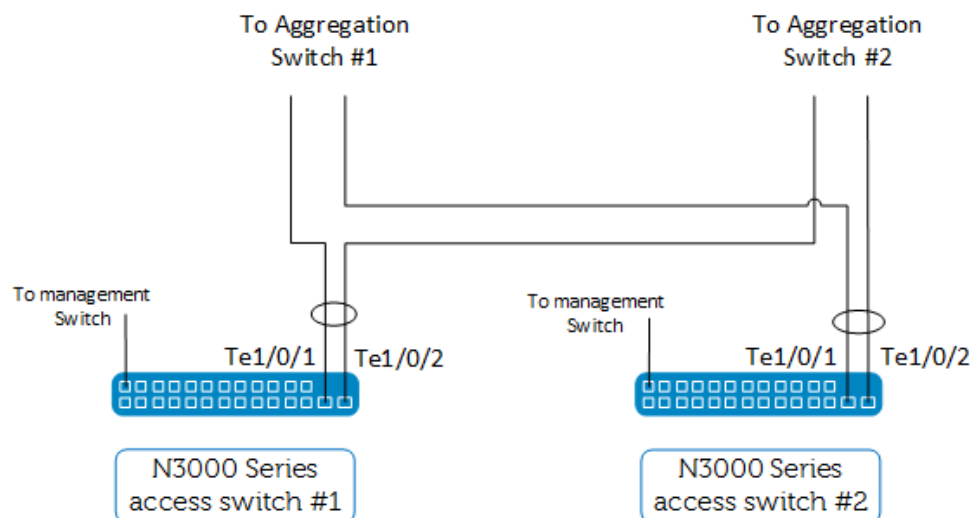


Figure 8 Switch cabling

Setup steps

Use the following steps for initial set up of access layer switches:

1. Connect the cables from the aggregation to the access switch if not already completed
2. From factory default state, power on the switch
3. Let the Dell Easy Setup Wizard timeout (60 seconds)
 - a. (optional) If local CLI access is being monitored, admins can manually decline the wizard.

The factory default behavior for an access switch is to request a DHCP address on VLAN 1. All interfaces have VLAN1 as the default PVID.

The Dell Networking N-Series switches with firmware revision 6.3.0.16 and higher have embedded capability that enables the switch to communicate with HiveManager NG. No configuration is required 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*, located at [Dell Support](#).

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.

After completing the steps in section 4.1 thru 4.4, site preparation and standard deployment is complete.

Site Preparation and Standard Deployment

- ☒ Physical installation and cabling
- ☒ Configure firewalls
- ☒ Configure aggregation switches
- ☒ Configure management switch

4.5 Onboarding Dell Networking N-Series switches to HiveManager NG

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

Dell Networking OS version 6.3.0.16 and higher firmware supports and automatically enables HiveManager NG capability for the Dell N3000, N2000, and N1500 switches. Ensure all switches are upgraded to version 6.3.0.16 prior to onboarding the switches into HiveManager NG.

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 on the **Add** icon on the device table, then click the **Add Real Devices** box

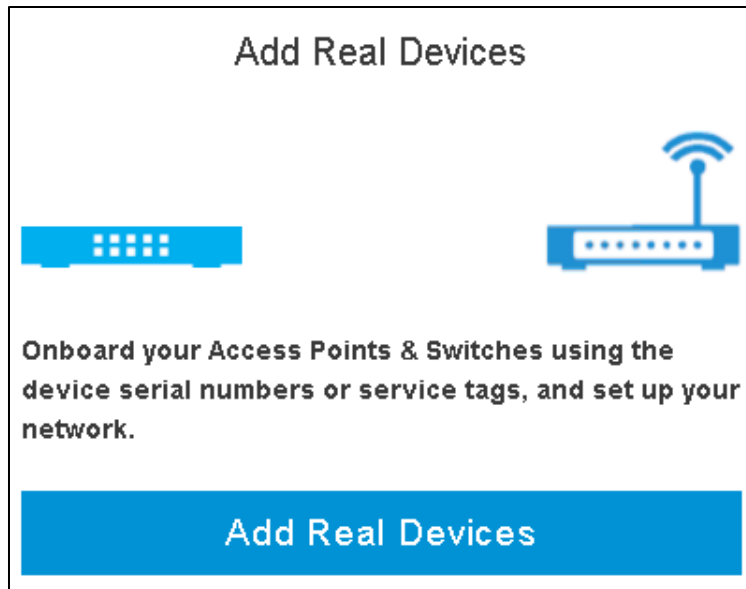


Figure 9 Add devices in HiveManager NG

2. Enter **Dell service tag(s)** for the switches to be onboarded into HiveManager NG, separated by commas, into the field shown in Figure 10 and click **Next**.

The screenshot shows a web interface titled "Add Devices". Below the title is a horizontal line, followed by the heading "Step 1 of 2: Import / Enter Devices".

Under this heading, there are two sections:

- Aerohive section:** It starts with the instruction "Please enter the serial numbers of your Aerohive devices" in orange. Below this is a dashed box containing the text "Choose a file or drag directly here" and a blue "Choose" button. Underneath is a text input field labeled "Aerohive serial numbers" with the placeholder text "Serial Numbers (separated by a comma)". Below the field is an example: "Example: 12345678900000, 12345678900001".
- Dell section:** It starts with the instruction "Please enter the service tags for your Dell devices" in orange. Below this is another dashed box with "Choose a file or drag directly here" and a blue "Choose" button. Underneath is a text input field labeled "Dell service tags" with the placeholder text "ABC123F, ABC123G". Below the field is an example: "Example: 8ZK47M1, 9ZK47M2".

Figure 10 Add Dell service tag(s)

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**, then **Finish**.

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 11 Optional network policy assignment and creation

5. After a short time, each Dell Networking access switch contacts HiveManager NG. After onboarding has completed, the device list should look similar to Figure 12:

<input type="checkbox"/>	Status	Make	Hostname	Model	Firmware Version
<input type="checkbox"/>		Dell	console	N3024F	6.3.0.16
<input type="checkbox"/>		Dell	console	N3048P	6.3.0.16

Figure 12 Device list

This completes the onboarding process for Dell Networking switches.

Cloud Deployment

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

4.6 Network policy configuration

Networking settings reside in the network policy. Generate network policies from the **Configure** tab. You can create network policies before or after onboarding devices.

In HiveManager NG you can create unified wired and wireless policies. Features configured in the network policy through this deployment example include the following:

- Wireless employee access with 802.1x authentication
- Wireless guest access with self-registration and PPSK authentication
- Wired employee access with 802.1x authentication
- Wired access and trunk port interface configurations

Table 1 Purpose of VLANs used in this example

VLAN ID	Purpose
VLAN 1	Access switch management VLAN
VLAN 5	Employee traffic
VLAN 7	Guest traffic
VLAN 50	Route to internet
VLAN 100	Non-user traffic, native and management VLAN for APs

Note: This example 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.

Configuration steps:

Use the following steps to configure a network policy:

1. Log into your HiveManager NG account
2. Navigate to the **CONFIGURE** tab > **Network Policies**
3. Click the ADD NETWORK POLICY icon
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, *Large_Campus_Deployment*.
 - c. Turn on the **Spanning Tree Protocol** by changing the slide button to **ON**, as in Figure 13.

Notes:

1. The slide button enables or disables RSTP.
2. Dell switch configurations contain spanning tree enabled by default (RTSP 802.1w). Administrators must turn on spanning tree within the network policy to keep the default setting enabled when using HiveManager NG. The slide button only appears on the new policy screen. After saving the network policy, the spanning tree settings reside on the Additional Settings tab.

Figure 13 New policy details page

- d. Click **Next**.

Configuring wireless employee access:

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 on the **SSID Broadcast Name** to auto-populate the field with the previous SSID name.

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)

Figure 14 SSID name

- d. Click the **Enterprise** box on the **SSID Authentication** tab, as in Figure 15.

SSID Usage

SSID Authentication | MAC Authentication

Enterprise
WPA / WPA2 802.1X

Personal
WPA / WPA2 PSK

Private Pre-Shared Key

WEP

Open
Unsecured

Key Management
WPA2-(WPA2 Enterprise)-802.1X

Encryption Method
CCMP (AES)

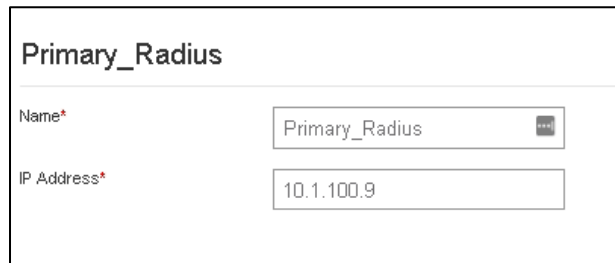
OFF ☒ Enable Captive Web Portal

Enable to display a splash page and configure captive web portal options.

Figure 15 SSID Usage window

- e. Find the **Authentication Settings** section.
- i. Click the **+** icon next to the **Default RADIUS Server Group** table.
 - ii. Enter a Name for a new **RADIUS Server Group** in the **Name** field, for example, *AAA_RADIUS*.
 - iii. Click the **Add** icon at the top of the list.
 - iv. Choose **External RADIUS Server** from the dropdown menu.
 - v. Enter a **Name** for a RADIUS Server in the Name field, for example, *1_RADIUS*.
 - vi. Click the **+** icon next to the **IP Address/Host Name** field and choose the appropriate method, for example, *IP Address*.
 - vii. Enter a **Name** for the RADIUS Server IP Address or Host Name, for example, *Primary_Radius*.

- viii. Enter the **IP Address/Host Name**, for example, *10.1.100.9*, as in Figure 16:



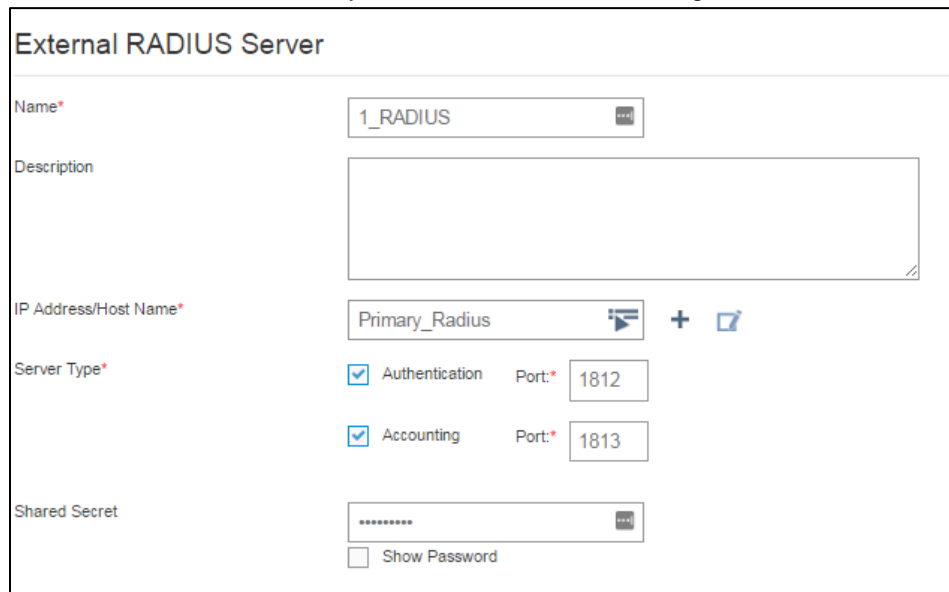
Primary_Radius

Name* Primary_Radius

IP Address* 10.1.100.9

Figure 16 External RADIUS server fields

- ix. Click **Save**.
- x. Enter the **Shared Secret** for your RADIUS server, as in Figure 17:



External RADIUS Server

Name* 1_RADIUS

Description

IP Address/Host Name* Primary_Radius

Server Type*

☒ Authentication Port* 1812

☒ Accounting Port* 1813

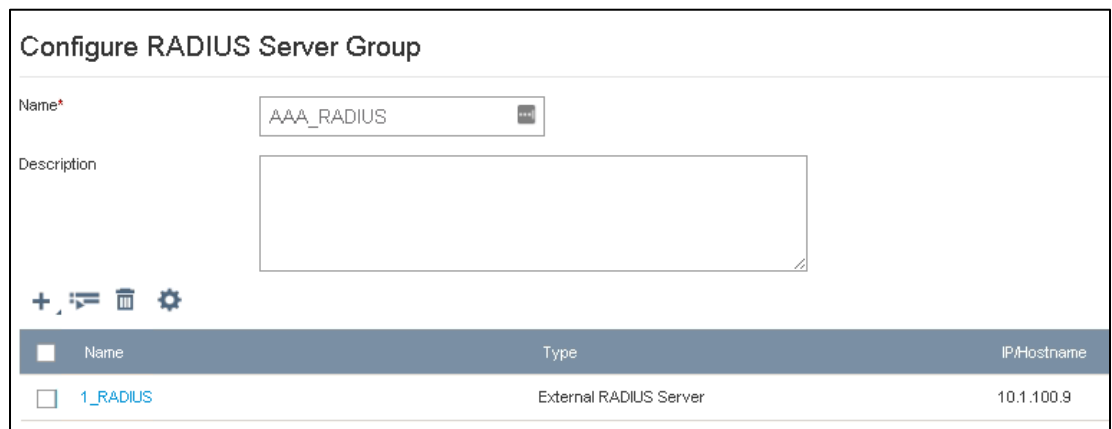
Shared Secret

.....

☐ Show Password

Figure 17 External RADIUS Server fields

- xi. Click **Save**.



Configure RADIUS Server Group

Name* AAA_RADIUS

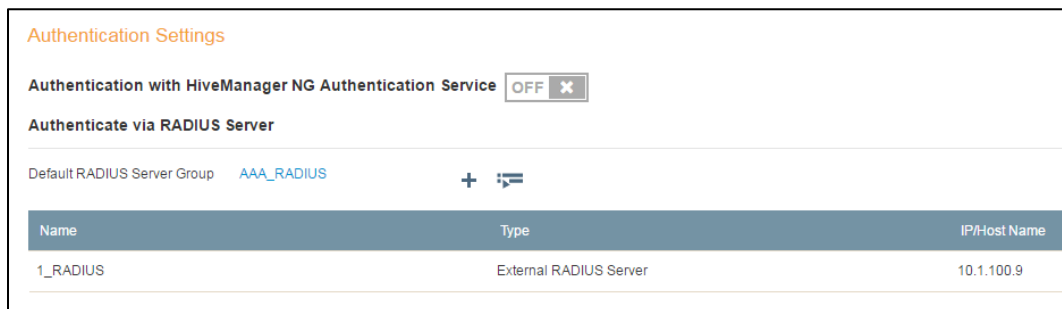
Description

+ - [icon] [icon]

Name	Type	IP/Hostname
<input type="checkbox"/> 1_RADIUS	External RADIUS Server	10.1.100.9

Figure 18 RADIUS Server Group

- xii. Click **Save**.



Authentication Settings

Authentication with HiveManager NG Authentication Service ☐ OFF

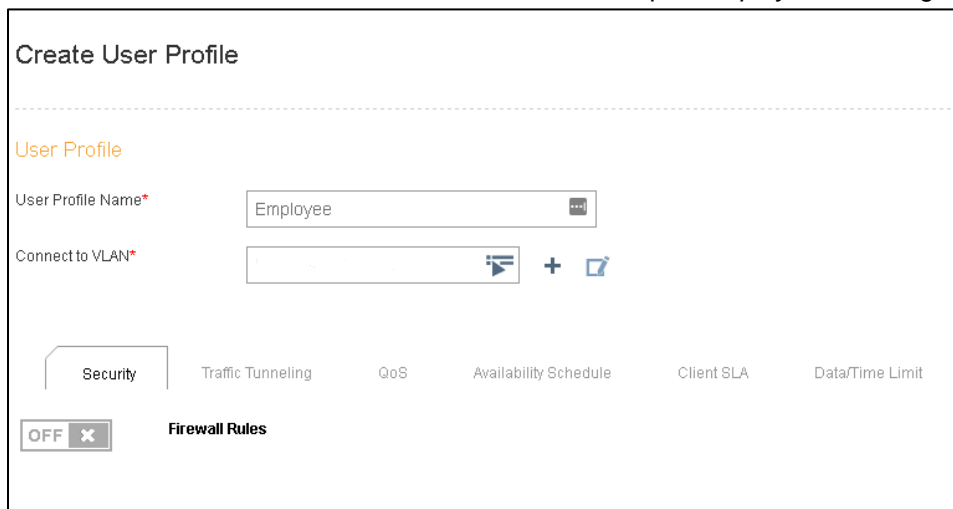
Authenticate via RADIUS Server

Default RADIUS Server Group AAA_RADIUS

Name	Type	IP/Host Name
1_RADIUS	External RADIUS Server	10.1.100.9

Figure 19 Authentication Settings

- f. Find the **User Access Settings** section.
 - i. Create a new **Default User Profile** by clicking on the **+** icon in the section.
 - ii. Enter a name in the **User Profile Name** field, for example, *Employee*, as in Figure 20:



Create User Profile

User Profile

User Profile Name* Employee

Connect to VLAN* [Empty field with + icon]

Security Traffic Tunneling QoS Availability Schedule Client SLA Data/Time Limit

☐ OFF Firewall Rules

Figure 20 Create User Profile fields

- iii. Add a new VLAN by clicking the **+** next to the **Connect to VLAN** field.
- iv. Enter a VLAN name in the **Name** field, for example, *EmployeeVLAN5*.
- v. Enter a VLAN number in the **VLAN ID** field, for example, *5*.



EmployeeVLAN5

Name* EmployeeVLAN5

VLAN ID* 5

☐ Apply VLANs to devices using classification

Figure 21 New VLAN object fields

- vi. Click **Save**.
- vii. **Connect to VLAN** field populates with the new VLAN object.

- viii. Leave other settings as default.
- ix. Click **Save**.
- x. **Default User Profile** populates with the new object created above.
- g. Leave other settings as default.
- h. Click **Save**.

Configuring wireless guest self-registration (2 SSIDs):

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 22.
 - d. Find the **Authentication Type** > **Private PSK** section.
 - i. Choose **Guests can self-register, then sign in**.
 - 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

v 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.

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

☐ Enable employee approval.

*Guest Self-Registration SSID

[Customize Captive Web Portal >](#)

Save **Cancel**

Figure 22 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.

The screenshot shows the 'New Guest Access SSID' configuration interface. On the left, there's a sidebar with a 'Customize Captive Web Portal >' button. The main area is titled 'Customize Captive Web Portal' and includes a note about configuration options. The 'Name' field is set to 'BBB_Guest_web_portal'. Below this, there are tabs for 'LANDING PAGE', 'SUCCESS PAGE', and 'ERROR PAGE'. The 'Colors and Fonts' section shows 'Background Color' as white, 'Font Color' as black, and 'Links Color' as blue. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 23 Guest Captive 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, *GuestVLAN7*.
 2. Enter a VLAN number in the **VLAN ID** field, for example, *7*.
 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.

Pre-Defined Settings >

User Group Settings >

Rename Guest Access Settings

Name* BBB_Guest_Access_profile

VLAN

Connect to VLAN* GuestVLAN7 + -

Firewall Policy Used

Firewall settings have been disabled for this profile.

Save Cancel

Figure 24 Guest User profile settings

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

- iii. Click **Save**.

Figure 25 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.

Wireless SSIDs			
<div> Add <div> <div></div> <div></div> </div> </div>			
	SSID	Guest Access	Access Security
<input type="checkbox"/>	AAA_Employee		WPA / WPA2 802.1X (Enterprise)
<input type="checkbox"/>	BBB_Guests	Edit	Private PSK
<input type="checkbox"/>	BBB_Guest_registration	Edit	Unsecured (Open) Network

Figure 26 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**.

Device Templates				
<div> <div>Add</div> <div></div> <div></div> </div>				
	Device Model	Template	Assignment Rules	Assignment Description
<input checked="" type="checkbox"/>	AP230	<input checked="" type="checkbox"/> AP230_AAA(default)		

Figure 27 Device templates list

Cloud Deployment

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

Configuring wired access switches:

8. **Switch Settings** tab, **Device Templates**
 - a. Click on the **Add** icon above the records table.
 - b. Choose the switch model being deployed, for example, *N3048P*.
 - c. Enter a name in the **Template Name** field, for example, *N3048P_AAA*.
 - d. Click the port 1 (Gi1/0/1) icon to highlight the connection to the management switch.
 - e. Click on **Assign, Create New** with port 1 highlighted.
 - f. Enter a **Name** for the new port type, for example, *to_Mgmt*.
 - g. Ensure **Access Port** on **Port Usage Settings** is selected (default).
 - h. Ensure **VLAN 1** is set for the **VLAN ID** (default).
 - i. Click **Save**.
 - j. Click on 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_AccessPoints*.

- 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. Click the **+** icon next to the **Native VLAN** field
 - ii. Enter a **Name** for native VLAN to be used on the APs, for example, *General100*.
 - iii. Enter the **VLAN ID** number, for example, *100*, as in Figure 28:


The dialog box is titled "Trunk VLANs". It contains two input fields: "Name*" with the value "General100" and "VLAN ID*" with the value "100". Below these fields is a checkbox labeled "Apply VLANs to devices using classification" which is currently unchecked.

Figure 28 Trunk VLANs dialog box: Name/ID

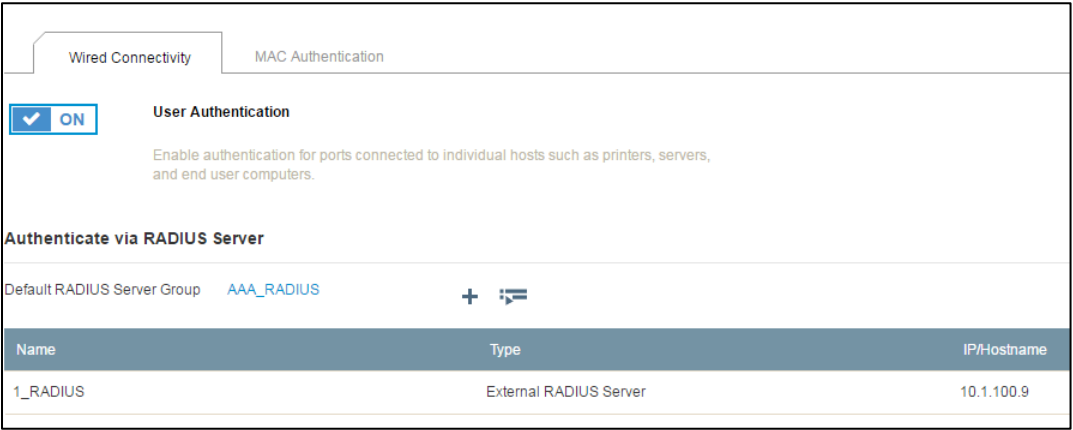
- iv. Click **Save**.
- v. Enter the VLANs required on the APs into the **Allowed VLANs** field, for example, *5, 7, 50, 100*, as in Figure 29:

The dialog box is titled "Trunk VLANs" and has a close button (X) in the top right corner. It contains two input fields: "Native VLAN:" with the value "General100" and a list icon, and "Allowed VLANs:" with the value "5,7,50,100". To the right of the "Native VLAN" field is a "+" icon and a list icon. Below the "Allowed VLANs" field is a note: "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."

Figure 29 Trunk VLANs dialog box: Native/Allowed VLANs

- vi. 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. Turn on **User Authentication** by changing the **Wired Connectivity** tab's User Authentication slide button to **ON**.
- u. Choose the existing **Radius Server Group** by clicking the list icon: , as in Figure 30.
 - i. Select **AAA_RADIUS**, created from the wireless example.

ii. Click **Select**.

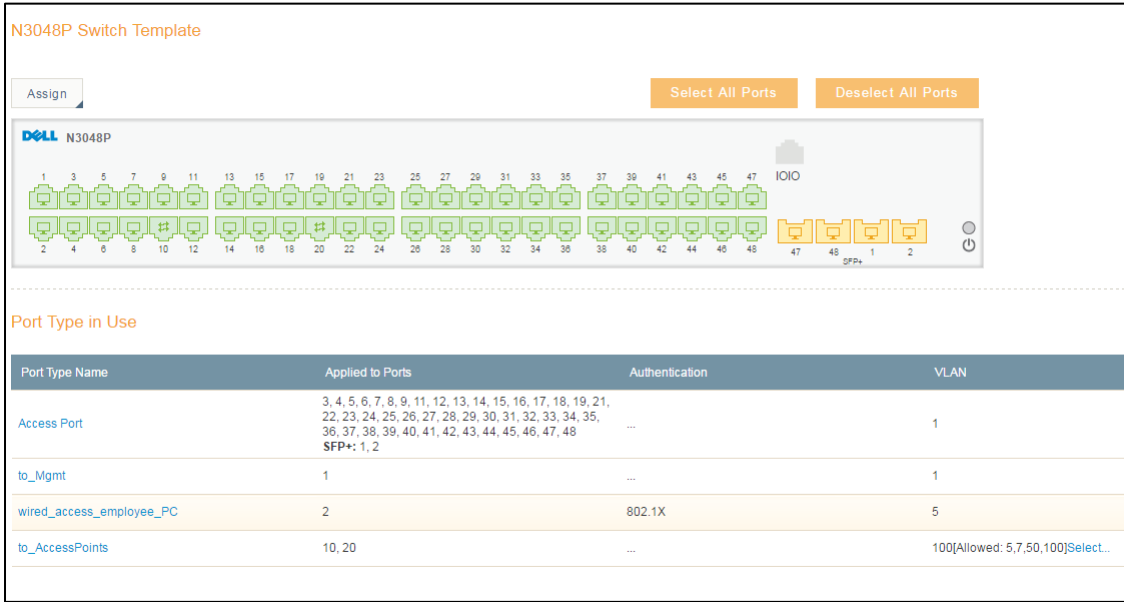


The screenshot shows the 'User Authentication' settings for a switch. It includes a 'Wired Connectivity' tab and a 'MAC Authentication' tab. The 'User Authentication' section has a toggle switch set to 'ON'. Below this, there is a description: 'Enable authentication for ports connected to individual hosts such as printers, servers, and end user computers.' The 'Authenticate via RADIUS Server' section shows the 'Default RADIUS Server Group' as 'AAA_RADIUS'. A table lists the configured RADIUS servers:

Name	Type	IP/Hostname
1_RADIUS	External RADIUS Server	10.1.100.9

Figure 30 User Authentication settings

- v. Find the **VLAN ID** section.
 - i. From the pulldown menu, select the employee VLAN, for example, *EmployeeVLAN5*.
- w. Click **Save** within the **New Port Type** section



The screenshot shows the 'N3048P Switch Template' configuration interface. It includes an 'Assign' button and two orange buttons: 'Select All Ports' and 'Deselect All Ports'. Below these is a diagram of the switch ports, numbered 1 through 48, with a '10/10' label and a power button icon. The 'Port Type in Use' section contains a table with the following data:


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, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48 SFP+: 1, 2	...	1
to_Mgmt	1	...	1
wired_access_employee_PC	2	802.1X	5
to_AccessPoints	10, 20	...	100[Allowed: 5,7,50,100]Select...

Figure 31 Final Template settings

- x. Click **Save**

Notes:


- 1. Each switch model requires a unique device template. The following steps describe adding a switch template for a different model switch.
- 2. Each switch with a unique port and feature configuration requires a unique device template. Multiple templates for the same switch model cannot be deployed under the same network policy. Change device templates for individual switches at the device configuration level.

- y. Add another switch template by clicking on the **Add** icon above the records table.
- z. Choose the switch model being deployed, for example, *N3024F*.
- aa. Enter a name in the **Template Name** field, for example, *N3024F_AAA*.
- bb. Click port 1 (Gi1/0/1) to highlight the connection to the management switch.
- cc. Click **Assign. Choose Existing** with port 1 highlighted.
- dd. Choose the management port type created on the previous switch example, for example, *to_Mgmt*.
 - i. Click **Save**.
- ee. Click port 2 (Gi1/0/2) to highlight a wired access port. Ensure all other ports are not highlighted by clicking on them if necessary.
- ff. Click on **Assign, Create New** with port 2 highlighted.
- gg. Enter a **Name** for the new port type, for example, *to_ApplicationServer*.
- hh. Select **Access Port** on **Port Usage Settings**.
 - ii. VLAN ID section.
 - i. With the list icon () , select the **General100** setting that was configured in the previous steps.
- jj. Click **Save** within the **New Port Type** section.

N3024F Template

Template Name*

N3024F Switch Template

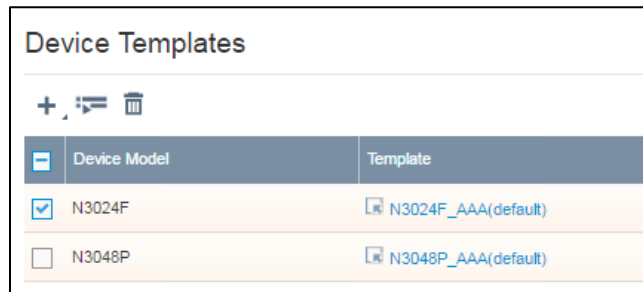


Port Type in Use

Port Type Name	Applied to Ports	Authentication	VLAN
Access Port	3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 SFP+: 1, 2	...	1
to_Mgmt	1	...	1
to_ApplicationServer	2	...	100

Figure 32 Additional template model

- kk. Click **Save** to save the template.





Device Model	Template
<input checked="" type="checkbox"/> N3024F	<input type="checkbox"/> N3024F_AAA(default)
<input type="checkbox"/> N3048P	<input type="checkbox"/> N3048P_AAA(default)

Figure 33 Device template list

- ll. Click **Next**

9. **Additional Settings** tab

- Find the **DNS Server** settings on the left-hand side.
 - Turn off the **DNS Server** using the slide button (this example sets the DNS addresses through DHCP).
 - Click **Save**.
- Find the **NTP Server** settings on the left-hand side.
 - 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.)
 - Click **Save**.
- Find the **Management & Native VLAN** settings on the left-hand side. (This setting only affects APs).
 - For **MGT Interface VLAN**, use the list icon:  to select **General100** that was configured in the previous steps.
 - For **Native (Untagged) VLAN**, use the list icon:  to select **General100** that was configured in the previous steps.
 - Click **Save**.
- This example leaves all other Settings within **Additional Settings** as default.
- Click **Next**.

Cloud Deployment

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

10. Deploy Policy tab

- a. Select the switch device(s) that need to receive the network policy 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.

Notes:

1. This step focuses on deploying the network policy to the switches at this time. Policy deployment to APs is shown later.
2. This document's attachments include access switch configuration files after network policy updates. Their filenames are *3048P_switch_config_after_network_policy_update.txt* and *3024F_switch_config_after_network_policy_update.txt*.

At this point only a partial configuration for the access switches is complete. Use the Supplemental CLI feature within HiveManager NG to complete the configuration of the interfaces for the MLAG partner link to the aggregation layer. Configuration of other features not included in the network policy and templates also occurs at that time.

Cloud Deployment

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

4.7 Supplemental CLI

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

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

11. Click on **Account Details** in the upper right-hand corner of the GUI, as in Figure 34:

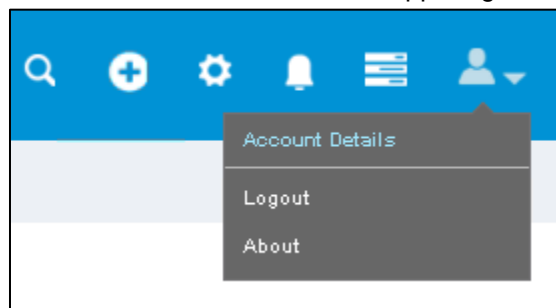


Figure 34 Account Details selection

12. Select **VHM Management** on the left-hand side.
13. Turn on the Supplemental CLI by changing the **Supplemental CLI** slide button to **ON** in the VHM Management section, as in Figure 35:

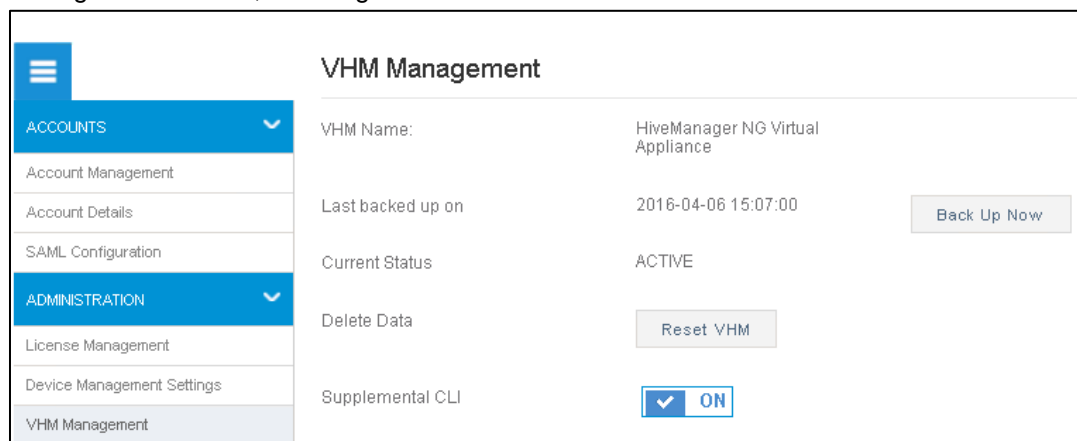



Figure 35 Supplemental CLI – on

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 <http://docs.aerohive.com/dellcloud>.

14. Navigate to the **Monitor** tab > **Devices** list.
 - a. Select the checkbox next to the Dell switch, for example, *N3048P*.
 - b. Click on the **Edit** icon:  near the top of the list to edit the device configuration.

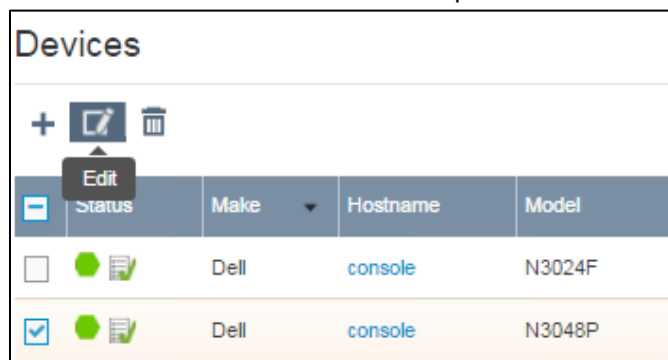


Figure 36 Editing a device configuration

- 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, you can copy/paste the CLI commands below 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 in 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 does not execute.

Enter the following into the CLI Commands text box:

```
enable
configure
interface vlan 5
exit
interface vlan 7
exit
interface vlan 50
exit
interface vlan 100
ip address 10.1.100.67 255.255.255.0
exit
aaa authorization network default radius
radius-server timeout 30
radius-server retransmit 10
radius-server source-ip 10.1.100.67
spanning-tree mode rapid-pvst
spanning-tree vlan 1 max-age 16
spanning-tree vlan 5 max-age 16
spanning-tree vlan 7 max-age 16
spanning-tree vlan 50 max-age 16
spanning-tree vlan 100 max-age 16
interface Gi1/0/2
spanning-tree portfast
exit
interface Te1/0/1
channel-group 1 mode active
exit
interface Te1/0/2
channel-group 1 mode active
exit
interface port-channel 1
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 2-4093
exit
```

The script above is specific to this topology and the example large campus network. The script requires a port channel in the N3048P switch to complete the MLAG partner configuration to the aggregation layer. The management network requires spanning-tree per VLAN (RSTP-PV). The default rapid spanning tree (RSTP) can block links in the management network by using a per-switch spanning-tree protocol.

console: Device Configuration

AAA_CLI

Name*

AAA_CLI

Description

MLAG partner, RSTP-PV, and misc

CLI Commands*

```

enable
configure

interface vlan 5
exit
interface vlan 7
exit
interface vlan 50
exit
interface vlan 100
ip address 10.1.100.67 255.255.255.0

```

Note: 1.You can enter multiple CLI commands, one command per line, not exceeding a maximum total of 8192 characters.
2.You can use CLI Commands that contain IP and VLAN objects: \${ip:ip_object_name} and \${vlan:vlan_object_name}.
3.You must perform a complete configuration update each time commands are appended to device configurations.

Figure 37 Supplemental CLI configuration screen

console: Device Configuration

Device Details

Host Name*

console

Network Details

Network Policy

Large_Campus_Deploym...

Device Template

N3048P_AAA

Supplemental CLI

Supplemental CLI

AAA_CLI

Figure 38 Device Configuration with Supplemental CLI

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

1. Ensure the correct Supplemental CLI name is selected in the dropdown menu.
2. Review the settings for **Network Policy** and **Device Template**.
 - a. The settings pushed according to the Network Policy, Deploy Policy tab should be currently listed and no action is needed.
3. Click Save.
 - a. 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.

Cloud Deployment

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

- b. Navigate back to the **Device** List.
- c. Ensure the checkbox next to the appropriate Dell Switch device is checked.
- d. Click on **Update Devices** in the upper right corner of the list.
- e. Ensure **Update Network Policy and Configuration** is checked.
 - i. Do not check the **Upgrade Dell Switch Images**.
- f. Click **Perform Update**.

Cloud Deployment

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

Create switch-specific Supplemental CLI scripts and apply them to additional switches in the network at this time. The script below is a script used on a Dell Networking N3024F, placed in the example network to show additional devices. To apply this script to the switch, repeat the steps above and ensure that a unique Supplemental CLI name is used.

```

enable

configure

vlan 5
vlan 7
vlan 50

interface vlan 5
exit
interface vlan 7
exit
interface vlan 50
exit
interface vlan 100
exit

spanning-tree mode rapid-pvst
spanning-tree vlan 1 max-age 16
spanning-tree vlan 5 max-age 16
spanning-tree vlan 7 max-age 16
spanning-tree vlan 50 max-age 16
spanning-tree vlan 100 max-age 16

interface Tel1/0/1
channel-group 1 mode active
exit

interface Tel1/0/2
channel-group 1 mode active
exit

interface port-channel 1
switchport mode trunk
switchport trunk native vlan 100
switchport trunk allowed vlan 2-4093
exit

```

The Supplemental CLI scripts have now been applied to the appropriate Dell switches. After updating all access layer switches with the desired Supplemental CLI settings, the access layer switches are now fully deployed per the Campus Reference Architecture 3.0 topology.

Note: The configuration files for the access switches after the Supplemental CLI update are attached to this document. Filename: *3048P_switch_final config.txt* and *3024F_switch_final config.txt*

4.8 Aerohive AP onboarding to HiveManager NG

The onboarding process for Aerohive APs is exactly the same as Dell switches. In the large campus example, the Aerohive APs have a different management VLAN than the Dell switches. In this example, the routing design and communication with the RADIUS server used in our testing requires the APs to be on VLAN 100. Administrators can use any management and native VLAN in their network design. For configuration steps to change the management and native VLAN, refer to the network policy, **Additional Settings**, step 9 on page 36.

Add Aerohive devices in the fields above Dell Networking switches using a serial number.

1. Navigate to **Monitor > Devices**, click on the **Add** icon on the device table and click **Add Real Devices**.
2. Enter the Aerohive serial number(s) into the field shown in Figure 10, separated by commas.
 - a. Click **Next**.
3. Do not assign or create a network policy at this point.
 - a. Click **Next**.
4. Connect the APs to the N3048P switch, ports 10 and 20 in this example.

After a short time, each Aerohive AP contacts HiveManager NG and goes through the onboarding routine. The device list should look similar to Figure 40 after the addition of switches and APs.

Note: If the APs were connected to the access switch during initial installation, they may have received a DHCP address on a VLAN 1 subnet. This example uses a different management VLAN (100). Ensure the APs receive the correct DHCP address on the correct subnet. The AP may require a reboot.









<input type="checkbox"/>	Status	Make	Hostname	Model	Firmware Version
<input type="checkbox"/>	 	Dell	console	N3024F	6.3.0.16
<input type="checkbox"/>	 	Dell	console	N3048P	6.3.0.16
<input type="checkbox"/>	 	Aerohive	AP1	AP230	6.8r1
<input type="checkbox"/>	 	Aerohive	AP2	AP230	6.8r1

Figure 39 Device list with APs

Cloud Deployment

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

After onboarding the APs, update the Network Policy to the APs. Applying the Network Policy is almost identical to applying it to Dell switches.

5. Navigate to **CONFIGURE > Network Policies**
 - a. Click on the network policy, for example, *Large_Campus_Deployment*.
 - b. Click on the **Deploy Policy** tab.
 - c. Select the devices by clicking on the check box next to each AP.
 - d. Click **Upload**.
 - e. Ensure only **Update Network Policy and Configuration** is checked.
 - f. 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.
 - g. Click **Perform Update** and wait for the update to complete.

Cloud Deployment

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

This completes deployment of the large campus topology within the [Dell Networking Campus Switching and Mobility Reference Architecture 3.0](#) using Aerohive APs and HiveManager NG. The basic features for connectivity and management are in-place. Update network policy or apply additional Supplemental CLI scripts for further configuration to implement security, QoS or new routing.

4.9 HiveManager NG Virtual Appliance

The previous sections all utilized the public cloud solution for HiveManager NG. For customers that prefer to administer their own instance of HiveManager NG, there is an on-premises version available in a virtual appliance format.

Customers who purchase entitlement keys for devices for use on HiveManager NG Virtual Appliances receive order information and their entitlement key through email. After following the steps in the email to download the software image, the administrator is ready to deploy HiveManager NG Virtual Appliance.

Note: The [HiveManager NG Virtual Appliance QuickStart Guide](#) provides details for installation of the software image. The guide includes details on minimum server hardware and software requirements in addition to installation configuration steps.

HiveManager NG Virtual Appliance supports all the same features as the cloud instance. The virtual appliance can reside alongside other common network-wide applications within the local or remote data center.

A 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

Dell Networking OS version 6.3.0.16 firmware supports and automatically enables HiveManager NG capability. Ensure administrators update all cloud-managed switches to version 6.3.0.16 prior to onboarding to HiveManager NG.

B Additional resources

The following websites and documents provide further helpful information:

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

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

[DellTechCenter.com](http://delltechcenter.com)

TechCenter is an IT Community where you can connect with Dell EMC Customers and Dell EMC employees for the purpose of sharing knowledge, best practices, and information about Dell EMC 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 EMC 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 – Branch, Small Campus and Distributed Sites
http://en.community.dell.com/techcenter/networking/m/networking_files/20442896

C Support and feedback

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 best practices guide by sending an email to Dell_Networking_Solutions@Dell.com.

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>.