Extreme
Connect Beyond the Network

WING 5.X Deployment Guide

Centralized Deployments

Published: April 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

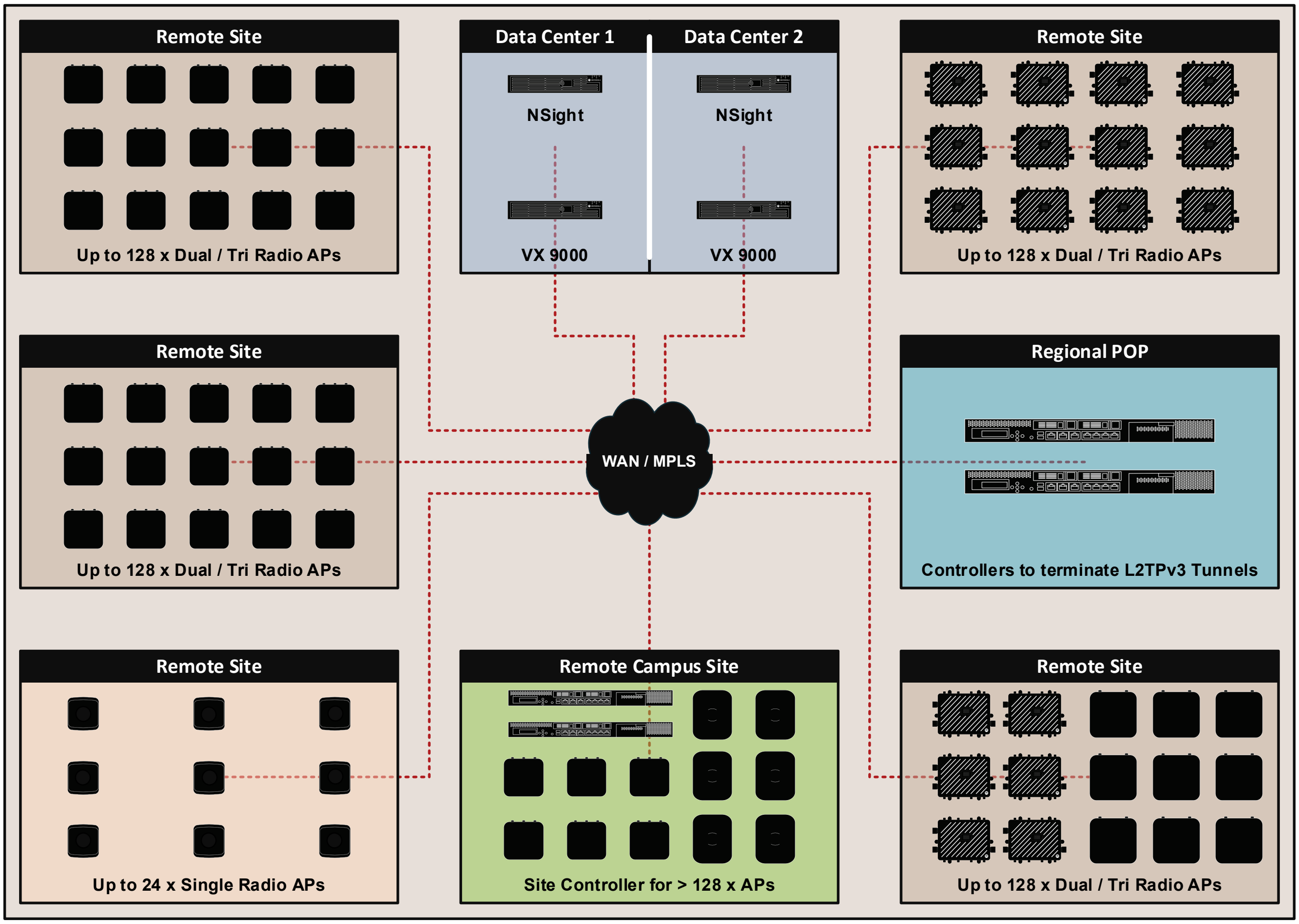
www.extremenetworks.com

P/N XXXXX-XX

Contents

Introduction

WING 5 centralized deployment model provides a highly scalable centrally managed Wireless LAN solution that is intended for customers deploying Wireless LAN services at remote branch sites. The centralized model differs from a typical campus deployment as all the configuration and management is performed centrally on Wireless Controllers located in a data center rather than Wireless Controllers deployed locally at each site. Wireless user traffic can be bridged locally within the remote site eliminating unnecessary overhead on the WAN and potential Wireless Controller bottlenecks, as well as it can be tunneled back to Wireless Controllers via respective RF Domain Manager.


Remote Site
Up to 128 x Dual / Tri Radio APs
Data Center 1
Data Center 2
NSight
NSight
VX 9000
VX 9000
Remote Site
Up to 128 x Dual / Tri Radio APs
Remote Site
Up to 128 x Dual / Tri Radio APs
WAN / MPLS
Regional POP
Controllers to terminate L2TPv3 Tunnels
Remote Site
Up to 24 x Single Radio APs
Remote Campus Site
Site Controller for > 128 x APs
Remote Site
Up to 128 x Dual / Tri Radio APs

The centralized model can be scaled to support up to 10,240 remote sites and as of WING 5.5 each remote site can support up to 128 x Dual or Tri Radio Access Points or 24 x Single Radio Access Points. For sites with more than 128 x Access Points, site controller can be deployed to account for AP capacity of the site.

Access Points at each remote site communicate with the Wireless Controllers in the data center over a private or public WAN. To further optimize WAN bandwidth one elected Access Point at each site (the RF Domain Manager) maintains communications with the centralized Wireless Controllers. The RF Domain Manager is responsible for distributing firmware images, aggregating statistics and performing SMART RF calculations for the site.

Availability is also provided with the centralized solution at a number of different levels. Access Points can be deployed to provide full site survivability in the event of a WAN outage. Each Access Point is fully capable of providing AAA, DHCP, Firewall, WIPS and WIDS services for the site. Unlike competing Wireless LAN solutions a WAN outage will not restrict the Wireless services or security capabilities of the remote site.

Key Concepts

MINT Protocol

WING 5 devices use Medium Independent Network Transport protocol (MINT) as the primary means of communication between the WING 5 devices. The MINT protocol is used for WING 5 device discovery, management / control, clustering and user data encapsulation. The MINT protocol differs from previous generations of Wireless LAN protocols as MINT completely decouples the management / control and data planes in addition to allowing WING 5 devices to dynamically discover and establish MINT links with other WING 5 devices on the network.

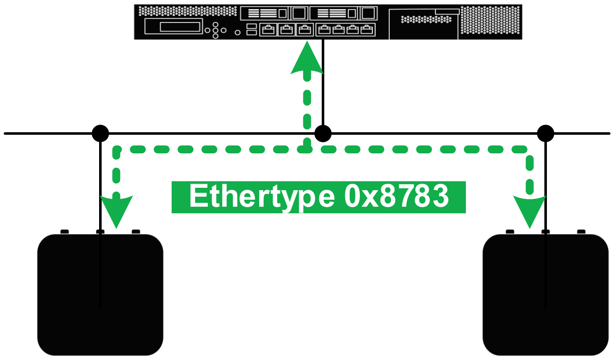
Previous generations of Wireless LAN protocols such as CAPWAP, LWAPP, TAPA and WiSPe use a single IPv4 tunnel between the Access Points (APs) to the Wireless LAN Controller for all management / control and user data encapsulation. With the MINT protocol the management / control traffic is completely decoupled from the encapsulated user traffic providing a much more flexible and scalable architecture. While the management / control traffic is tunneled to a Wireless LAN Controller, the encapsulated user traffic can be forwarded to a separate WING 5 device on the network. The WING 5 device that forwards the traffic onto the wired network is automatically elected allowing the WING 5 devices to form a logical network irrespective of the underlying transport type and connection.

The MINT protocol is also unique in that it is medium independent. Traditional Wireless LAN protocols can only operate over an IP network and as such are limited to the physical mediums that support IP protocols. In contrast the MINT protocol can operate at Layer 2 in addition to over IPv4 or IPv6 networks. A WING 5 device can be adopted and managed over a Layer 2 network such as Ethernet, Fabric, layer 2 tunnel or Wireless Mesh in addition to any physical medium that supports IPv4 and IPv6 protocols. MINT traffic can also be secured in IPsec permitting deployments over public or high-security private networks.

VLAN Based MINT Links

VLAN based MINT links use EtherType 0x8783 and can be established MINT links between two or more WING 5 devices over Ethernet, Mesh, MeshConnex™ or layer 2 tunnels. VLAN based MINT links are point-to-multipoint and use two packet types:

- Multicast – Using the destination MAC address 01:A0:F8:00:00:00 to exchange hello packets for device discovery and reachability.
- Unicast Packets – Using the destination MAC address of the WING 5 host for management / control and Wi-Fi user data encapsulation.



In a Centralized deployment VLAN based MINT links used in Access Point (AP) only sites to allow the APs at a site to discover themselves and elect an RF Domain Manager (RFDM) for the site. The VLAN based MINT links are automatically established by defining a Control-VLAN to each RF Domain for the AP only sites.

VLAN based MINT links are also used in AP only sites for encapsulating user data between the APs when traffic is being tunneled to the data center either via Level 2 MINT links or L2TPv3. The Wi-Fi user traffic is encapsulated and forwarded from non-RFDMs to the elected RFDM over the Control-VLAN and is then re-encapsulated and forwarded to the Active Centralized Controller or L2TPv3 Concentrator in the data center.

For Site Controller / AP only sites, VLAN based MINT links can be used to allow the Site Controllers to adopt and manage the APs at the site as well as encapsulate user traffic between the Site Controllers and APs if tunneling is enabled in one or more Wireless LANs. The APs can automatically discover the Site Controllers over one or more VLANs and adopt with no network addressing being required.

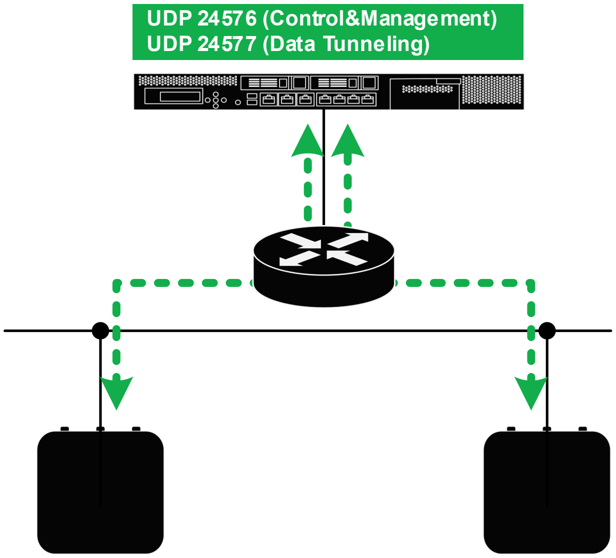
VLAN based MINT links are established over a VLAN if one or more of the following is true:

1. A Site Controller and AP are connected to a common VLAN. The AP will automatically discover the Site Controller over the VLAN and establish a MINT link for adoption and management. A VLAN based MINT link is preferred for adoption over an IP based MINT link.
2. APs are adopted and managed over VLAN based MINT links and tunneling is enabled on one or more Wireless LANs.
3. A Control-VLAN has been defined in the RF Domain assigned to a site.
4. A Controller VLAN has been defined in a Profile or Device.
5. A VLAN based MINT link has been manually defined in a Profile or Device.

IP Based MINT Links

Internet Protocol (IP) based MINT links use UDP and can be established between WING 5 devices over any medium that supports the IPv4 or IPv6 protocols. IP based MINT links are unicast based (point-to-point) and use the following UDP ports:

- UDP 24576 – Used for management / control, clustering and the exchange of hello packets for reachability.
- UDP 24577 – Used for encapsulating Wi-Fi user traffic.



In a Centralized deployment IP based MINT links are used for clustering, the adoption and management of Site Controllers and Access Points (APs) and encapsulating Wi-Fi user traffic between Site Controllers and APs if tunneling has been enabled in one or more Wireless LANs. IP based MINT links are also used to encapsulate Wi-Fi user traffic from an elected RF Domain Manager (RFDM) at a remote site to the Centralized Controllers when tunneling over Level 2 MINT links is enabled.

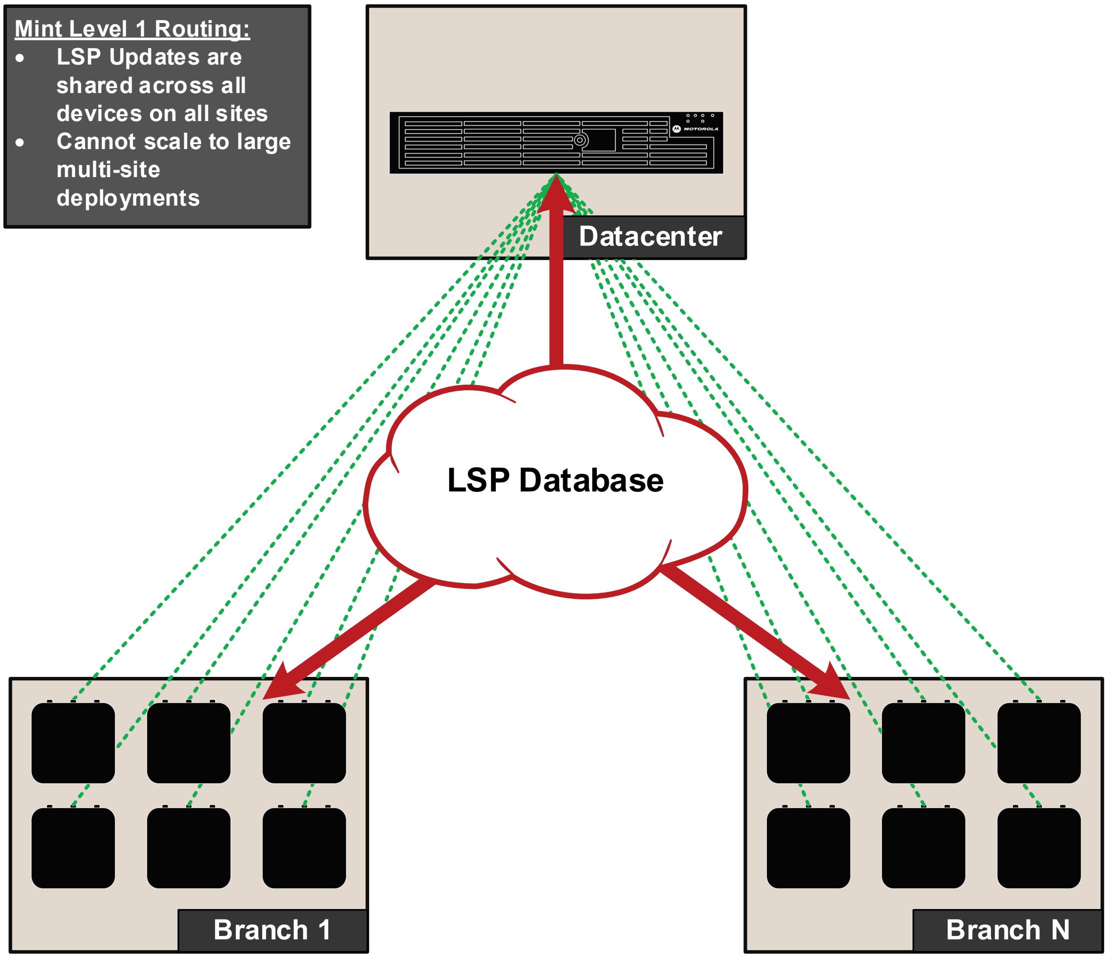
IP Based MINT links will be established between two WING 5 devices if one or more of the following is true:

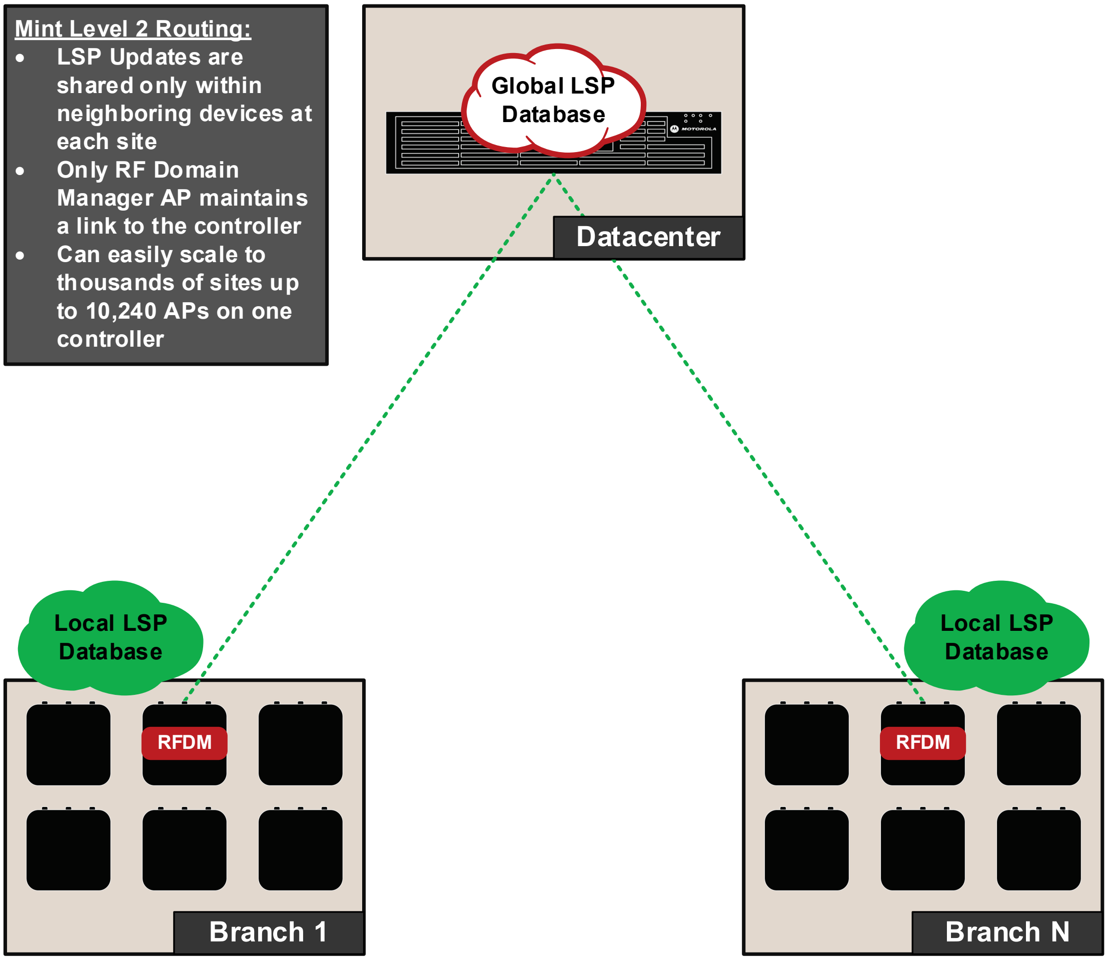
1. Clustering is enabled between two or more controllers.
2. Controller Hostname, DHCP Options or DNS resolution is used by an AP or Site Controller to discover an adopter.
3. An IP based MINT link has been manually defined in a Profile or Device.

Routing Levels

When MINT links are established between two or more WING 5 devices, the WING 5 devices exchange link state packets (LSPs) which contains each WING 5 devices MINT ID and hostname and number of adjacent MINT neighbors. This information is used by each WING 5 device for routing MINT packets when management / control traffic is exchanged or user traffic that is encapsulated and forwarded between two WING 5 devices.

MINT links can be established using Level 1 or Level 2 routing levels depending on the MINT link type. The MINT routing level for each link determines the LSP information that is exchanged between the WING 5 devices over the established MINT link. VLAN based MINT links only support MINT routing Level 1 where IP based MINT links can support MINT routing Level of 1 or Level 2.


Mint Level 1 Routing:
LSP Updates are shared across all devices on all sites
Cannot scale to large multi-site deployments
Datacenter
LSP Database
Branch 1
Branch N


Mint Level 2 Routing:
LSP Updates are shared only within neighboring devices at each site
Only RF Domain Manager AP maintains a link to the controller
Can easily scale to thousands of sites up to 10,240 APs on one controller
Global LSP Database
Datacenter
Local LSP Database
RFDM
Branch 1
Local LSP Database
RFDM
Branch N

The MINT routing level used for Centralized deployments is very important as it determines the number of WING 5 devices the Centralized Controllers, Site Controllers and Access Points (APs) learn about in the system. If all the MINT links used Level 1 routing, all the WING 5 devices would share a common LSP database containing all the WING 5 devices in the system. As one system can support up to 10,240 x WING 5 devices, using Level 1 based MINT links cannot scale as the LSP database on each WING 5 device would be too large.

To provide scaling, Centralized deployments use Level 2 MINT routing by using IP based Level 2 MINT links between the elected RF Domain Manager (RFDM) at each remote site to the Active Centralized Controller in the data center. With Level 2 MINT links the WING 5 devices at each site only learn about the Active Centralized Controller in the data center and the other WING 5 devices at the site. The LSP database for each device will not contain any other WING 5 device in the system. The Centralized Controller however will know about all WING 5 device in the ONEVIEW system.

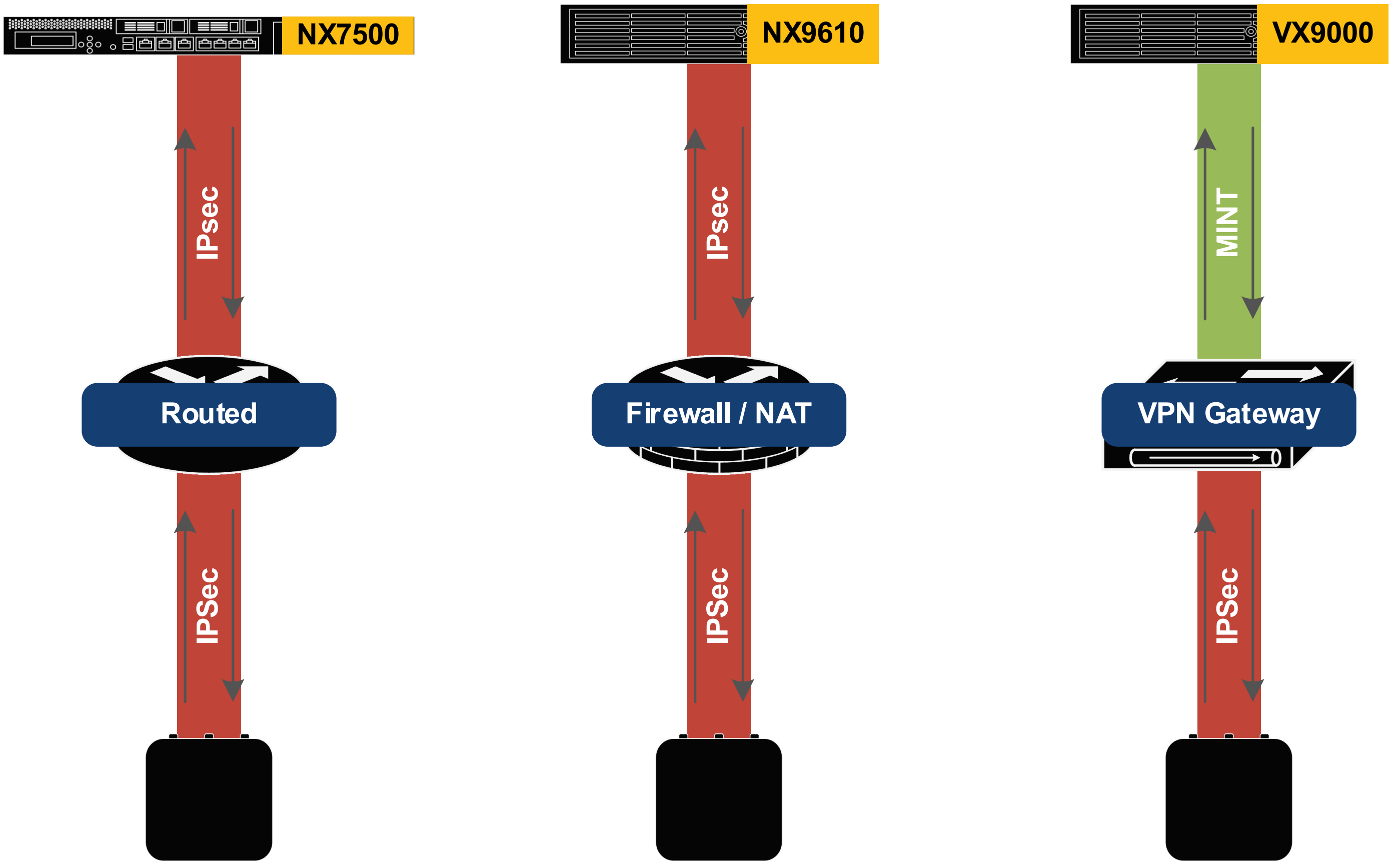
MINT communications between the WING 5 devices within a remote site use Level 1 based MINT links. For AP only sites the Level 1 MINT links are VLAN based and are established by defining a Control-VLAN in the RF Domain. For Site Controller / AP only sites, the Level 1 MINT links can be VLAN or IP based depending on how the APs are adopted and managed by the Site Controllers. All MINT communications to the remote site occurs via the Level 2 MINT link established by the elected RFDM who routes the MINT packets to the destination WING 5 device.

IPsec

WING 5 devices in a Centralized system can be connected to the public Internet or high-secure network where it is desirable to secure the management / control and encapsulated user data. Each WING 5 device supports IPsec VPN which can be employed to secure management / control and encapsulated user traffic exchanged over Level 1 or Level 2 IP based MINT links.

Auto IPsec Secure

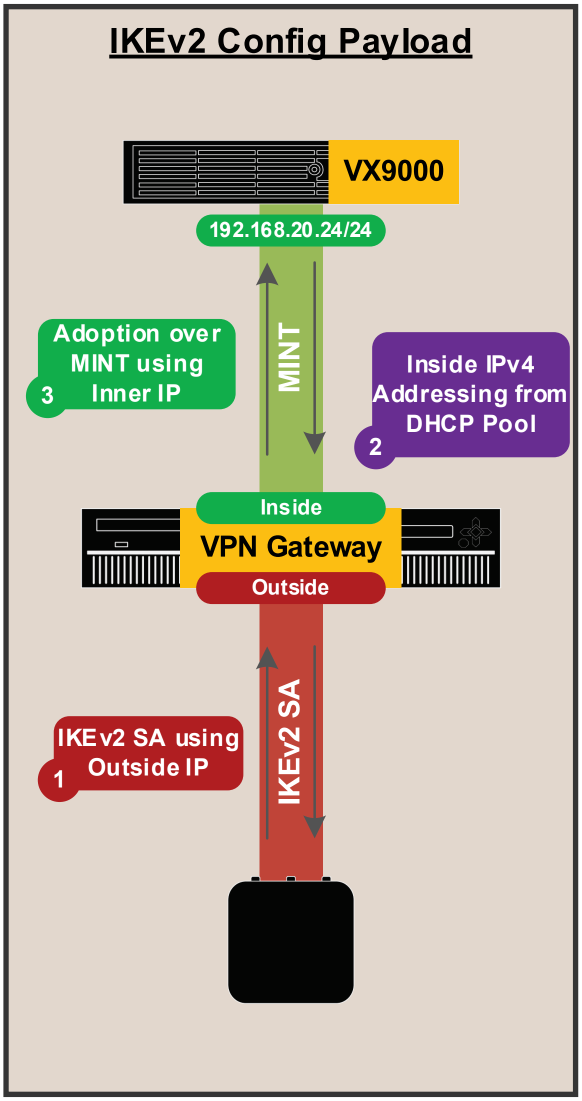
Auto IPsec Secure is supported on all models of RF Switches (RFS), Network Services Platforms (NX) and Access Points (APs). Auto IPsec Secure establishes a host-to-host IPsec VPN tunnel between WING 5 devices with minimum configuration being required. The Auto IPsec Secure tunnel can be initiated by DHCP options or Controller Hostnames defined on the adopting device and authentication can be performed by using pre-shared keys or RSA certificates.



Auto IPsec Secure tunnels are standards based using IKEv1 or IKEv2 (default) protocols. Each IPsec tunnel can be established between two WING 5 devices or a WING 5 device and a third-party VPN gateway providing complete deployment flexibility. The IPsec implementation is also NAT aware allowing remote Site Controllers and APs to be deployed behind a NAT device.

IPsec VPN Client

WING 5 supports an integrated IPsec VPN client which is supported on all models of RF Switches RFS, NX and APs. The IPsec VPN client uses the IKEv2 configuration payload to assign an inside IPv4 address to the remote WING 5 device which is used for device management as well as the exchange of MINT management / control and encapsulated user traffic. The inside IPv4 address can be assigned from an internal pool of addresses defined on the VPN gateway or from an external DHCP server.


IKEv2 Config Payload
VX9000
192.168.20.24/24
Adoption over MINT using Inner IP
3
MINT
Inside IPv4 Addressing from DHCP Pool
2
Inside
VPN Gateway
Outside
IKEv2 SA using Outside IP
1
IKEv2 SA

As with Auto IPsec Secure the IPsec VPN tunnel can be established with minimum configuration being required on the remote WING 5 device. The VPN client tunnel can be initiated by DHCP options or Controller Hostnames defined on the adopting device and authentication can be performed using pre-shared keys or RSA certificates.

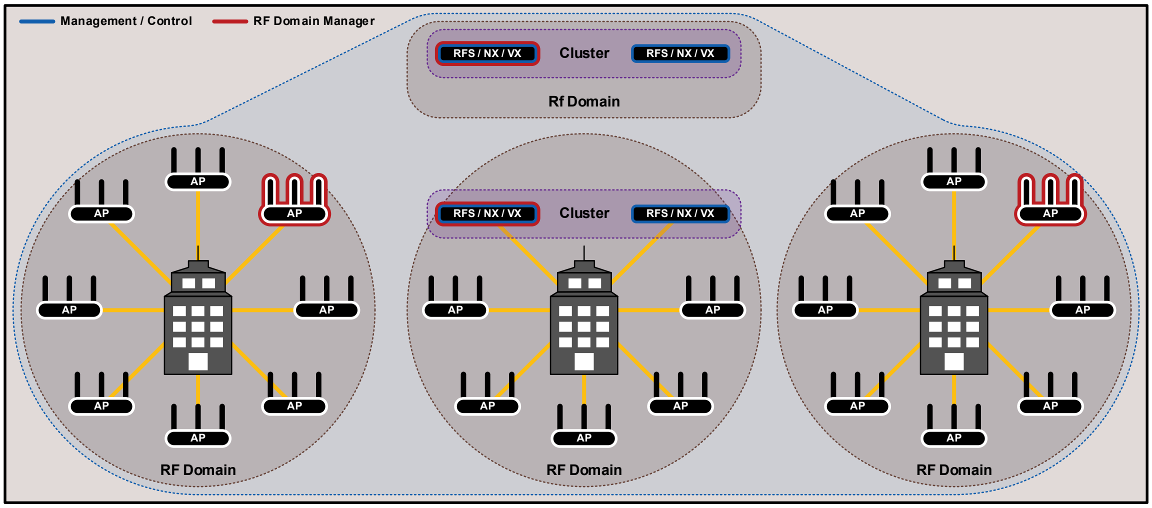
Each IPsec tunnel can be established between two WING 5 devices or a WING 5 device and a third-party VPN gateway providing complete deployment flexibility. The IPsec implementation is also NAT aware allowing remote Site Controllers and APs to be deployed behind a NAT device.

RF Domains

Each Centralized deployment will consist of multiple RF Domains (one per site) where the WING 5 devices at each remote site are assigned to a common RF Domain which is named to reflect the physical location or id of the site. RF Domains are important top-level configuration objects in WING 5 as they are used to organize WING 5 devices for management and visualization on the Active Centralized Controller in addition to determining the country code, time zone, policies and overrides applied to each site.

Each RF Domain will have an automatically elected RF Domain Manager (RFDM) which has specific responsibilities within the RF Domain and the WING 5 device that is elected for this role will depend on the WING 5 devices deployed at the remote site:

- Access Point (AP) only Sites – By default the most powerful AP with the lowest MINT ID will be elected.
- Site Controller / AP Sites – By default the RFS or NX with the lowest MINT ID will be elected.



Each elected RFDM maintains the IP based Level 2 MINT link to the Active Centralized Controller in the data center. The Level 2 MINT link is used to forward all the MINT management / control traffic and encapsulated user traffic exchanged between the data center and remote site. The RFDM also has additional responsibilities within the RF Domain which includes:

1. If enabled provides the Smart RF control logic for the RF Domain. APs report Smart RF data to their elected RFDM which makes the Smart RF decisions for the RF Domain.
2. Collects and aggregates wireless and domain statistics for the RF Domain. All WING 5 devices in the RF Domain report summary statistics to their elected RFDM. When wireless or domain statistics are requested by an administrator using the CLI or Web-UI, the Active Centralized Controller retrieves the requested statistics from the RFDM and displays them.
3. Distributes firmware updates for the RF Domain when AP Upgrade or Device Upgrade is initiated. The RFDM is responsible for downloading and distributing the firmware for each model of WING 5 device within the RF Domain. The RFDM will upgrade its device type and itself last. The RFDM is also responsible for forwarding the update status to the Active Centralized Controller and rebooting the devices (if selected) once the firmware upgrade has been completed.
4. If enabled perform WIPS blacklist management. If an AP in the RF Domain blacklists a client due to violations, the AP forwards the blacklisted clients MAC address to its elected RFDM which propagates the blacklisted MAC address to all other APs in the RF Domain.
5. If enabled maintains a consolidate list of Rogue APs. Each AP in the RF Domain reports unknown BSSIDs to their elected RFDM.
6. If enabled collects and aggregates wireless and domain statistics for the RF Domain to later send it to the NSight analytics platform.

RFDM election is an automatic process that occurs in run-time between all the WING 5 devices within an RF Domain. When all the devices in the RF Domain are operational, one device will be become the elected RFDM for the site. If the elected RFDM fails or is taken off-line, another WING 5 device is automatically elected and assumes the RFDM role. The RFDM election process takes into account a number of factors including:

1. If RFDM election has been specifically disabled on a WING 5 device. Devices that are configured as no rf-domain-manager capable will be excluded from the RFDM election process.
2. The user defined RFDM priority (1-255) assigned to each WING 5 device. The WING 5 device with the highest priority will be elected.
3. The type WING 5 devices in the RF Domain. The most powerful device in the RF Domain will be automatically elected (example NX 5500 -> AP 7532 -> AP 6521 etc.). If multiple WING 5 devices of the same model reside in the RF Domain, the WING 5 device with the lowest MINT ID will be elected.
4. If the AP is connected to the wired network. An AP connected to the wired network will always receive a higher priority than an AP connected via MeshConnex™.
5. If the WING 5 device has an IPv4 address assigned. A WING 5 device with an IPv4 address will always receive a higher priority than a WING 5 device without an IPv4 address.

> Note
>
> As a general best practice each remote site is a separate RF Domain. If two RF Domains are required for an AP only site, the APs in each RF Domain must be deployed on separate VLANs so that two RFDMs are elected. Multiple RF Domains are not supported in Site Controller / AP sites.

Device Adoption and Provisioning

Each Site Controller and Access Point in a centralized system controller is added to the master-configuration that resides on the Centralized Controllers in the data center. The master-configuration includes all the top level objects (TLOs) such as Wireless LANs, Policies, Profiles and RF Domains in addition to the device configurations for each managed WING 5 device in the system.

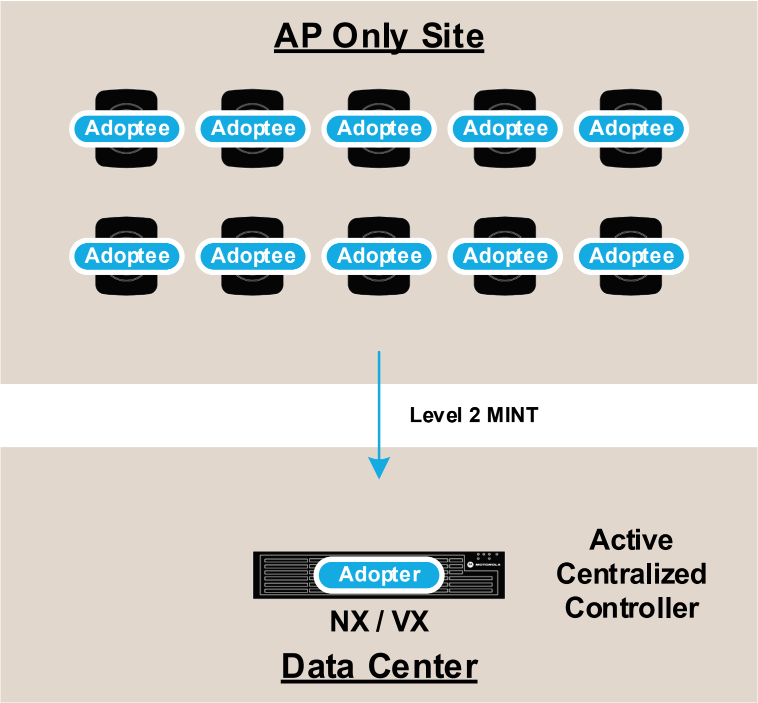
The adoption and management of remote Site Controllers and APs consists of three phases:

- Discovery – How the Site Controllers and APs discover their adopter. WING 5 supports both layer 2 and layer 3 discovery options.
- Provisioning – Profile and RF Domain Assignments. WING 5 supports statically and dynamically assigned Profiles and RF Domains.
- Configuration – Once a Profile and RF Domain has been assigned, the configuration is applied to the adopting device. This includes any Wireless LANs and Policies referenced by the assigned Profile and RF Domain.

Controller Discovery

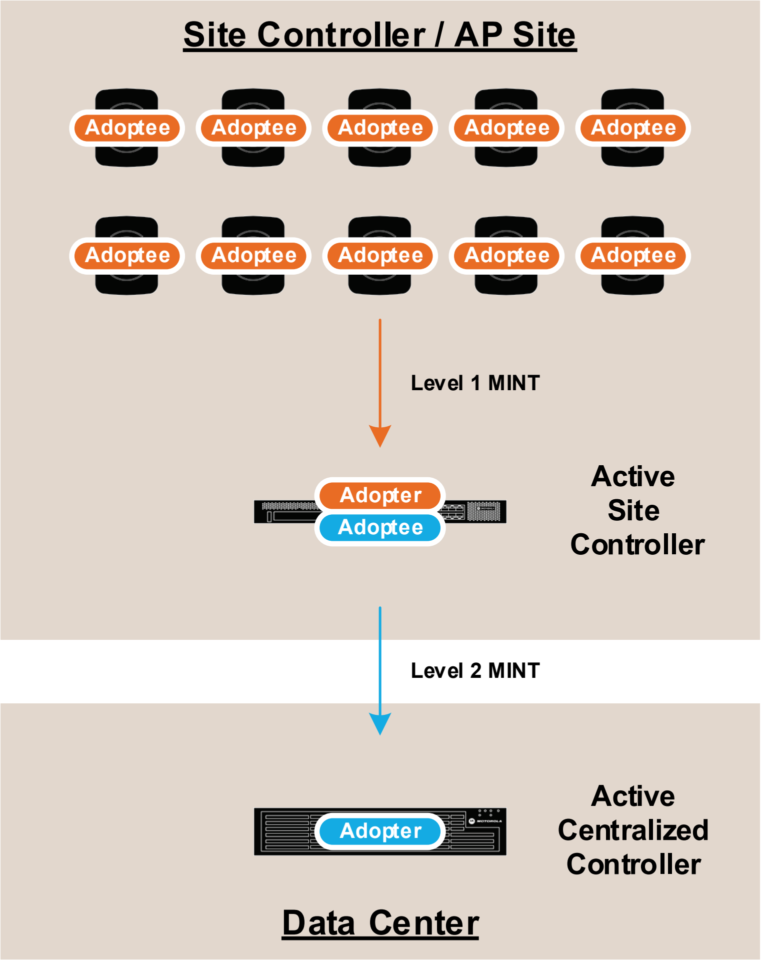
The provisioning of a remote Site Controller or Access Point (AP) cannot be performed unless the remote Site Controller or AP has first discovered its adopter. Site Controllers and APs use the MINT Link Control Protocol (MLCP) as the mechanism to discover adopters and establish Level 1 or Level 2 MINT links. Once a MINT link has been established, the device can be adopted and managed by the adopter and the configuration applied.

For AP only sites, each AP is adopted and managed by the Active Centralized Controller in the data center using IP based Level 2 MINT links. Each remote AP uses Controller Hostnames, DNS or DHCP discovery to discover the Active Centralized Controller and establish a Level 2 MINT link. The Active Centralized Controller being the adopter for each remote AP.



Once the Level 2 MINT link has been established, the remote APs are assigned their Profile and RF Domain and their configuration applied. The APs then discover all the other APs at the site via the Control-VLAN and elect an RF Domain Manager (RFDM) for the site. All but the elected RFDM will transition their Level 2 MINT links into an un-used state.

For Site Controller / AP sites, each Site Controller is adopted and managed by the Active Centralized Controller in the data center using IP based Level 2 MINT links. Each remote Site Controller uses Controller Hostnames, DNS or DHCP discovery to discover the Active Centralized Controller and establish a Level 2 MINT link. The Active Centralized Controller being the adopter for each remote Site Controller.



Once the Level 2 MINT links have been established, each remote Site Controller is assigned a Profile and RF Domain and its configuration is applied. The Site Controllers will then establish the cluster and elect an RF Domain Manager (RFDM) for the site. All but the elected RFDM would transition their Level 2 MINT links into an un-used state.

The APs are adopted directly by the Site Controllers and must discover the Site Controllers within the site. The APs use Layer 2, Controller Hostnames, DNS or DHCP discovery to locate an Active Site Controller and establish a Level 1 MINT link. The Site Controllers being the adopter for each AP within the site. Once a Level 1 MINT link has been established, the APs are assigned a Profile and RF Domain and their configuration applied.

Layer 2 Adoption

WING 5 APs support Layer 2 discovery allowing a remote AP to discover a Site Controller and establish a VLAN based Level 1 MINT link. Layer 2 discovery is only supported for remote sites with Site Controllers managing APs and cannot be used for APs only sites.

Layer 2 discovery works by forwarding MINT Link Control Packet (MLCP) discovery frames out the APs GE port on each defined VLAN. The MLCP discovery frames use EtherType 0x8783 and are multicast based with the destination multicast MAC address set to 01:A0:F8:00:00:00. This allows the MLCP discovery frames to be flooded to each device on each connected VLAN.

Site Controllers that reside on one or more VLANs will respond to the MLCP Discover with a MLCP Offer. The MLCP offer indicating if the Site Controller already has a MINT link established for the VLAN and its load. The

APs will forward a MLCP Reply confirming an Offer. When there are multiple MLCP Offers to choose from the AP will adopt to:

1. Active Site Controller (assuming Active / Standby cluster).
2. Active Site Controller that does not already have a VLAN link.
3. First Site Controller that responds.

It is important to note that Layer 2 discovery is used to establish VLAN based Level 1 MINT links which are point-to-multipoint in nature. When a VLAN based MINT link is established at the site, all the Site Controllers and APs share the same MINT link and form adjacencies. This can cause scaling issues for larger AP deployments especially if multiple VLANs are extended between the Site Controllers and APs. As a best practice it is always recommended to use IP based Level 1 MINT links to adopt and managed APs whenever possible.

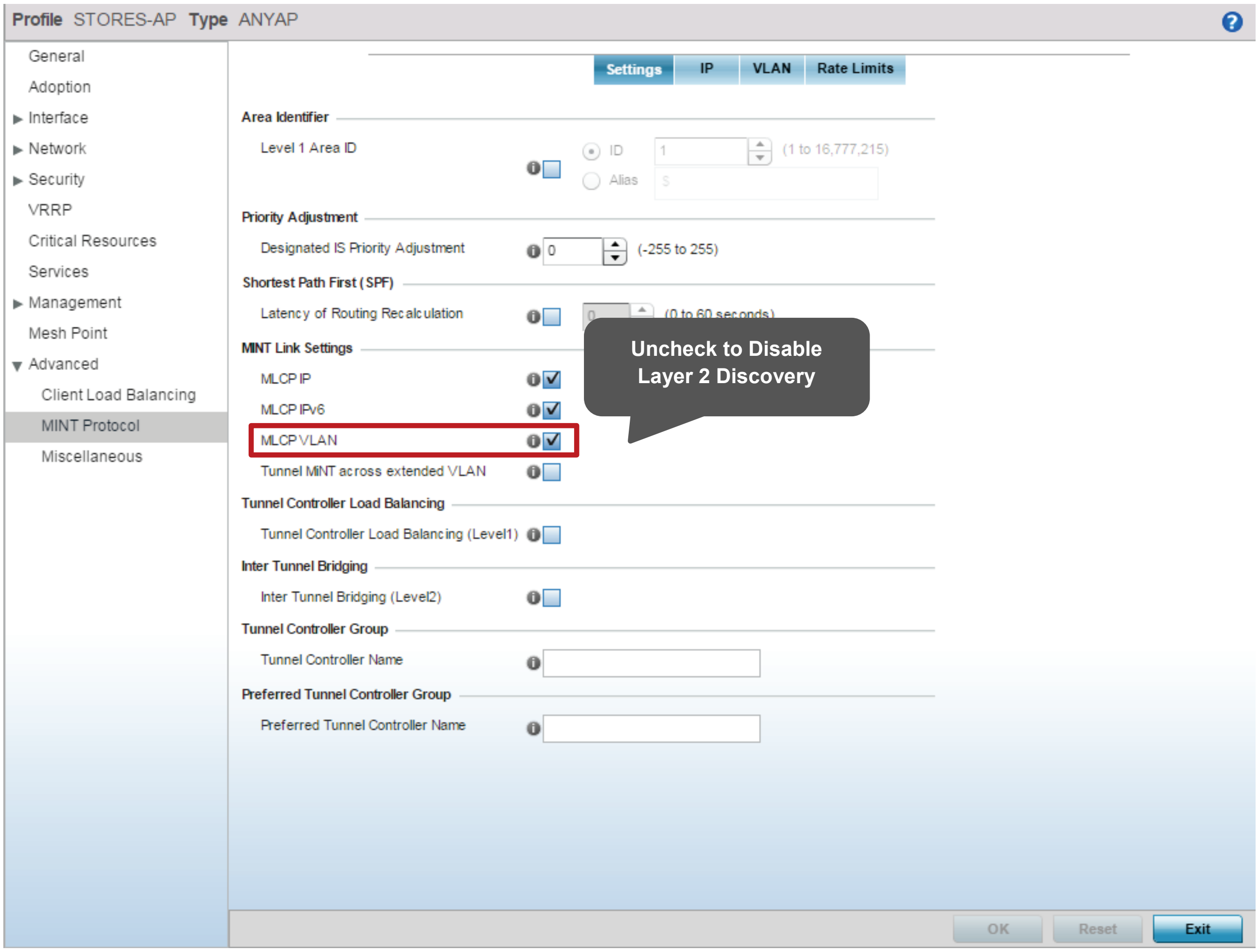
Note

For scaling Layer 2 discovery can support a maximum 128 x Dual / Tri radio APs or 64 x APs if any Single radio APs are present at the site.

You can optionally disable Layer 2 discovery for APs at remote sites by disabling the MLCP VLAN parameter under the AP Profile. This is recommended if the Site Controllers and APs at remote sites are visible at Layer 2 but you wish to force Layer 3 adoption. Unless Layer 2 discovery is disabled, the APs will discover and adopt to the Site Controllers at Layer 2 even if layer 3 discovery (Static, DNS or DHCP) is enabled for the site.

The following example demonstrates how to disable Layer 2 discovery in an AP Profile named STORES-AP using the Web-UI and CLI:

Path: Configuraiton -> Profiles -> <profile-name> -> Advanced -> MINT Protocol



Profile STORES-AP **Type** ANYAP

Area Identifier

Level 1 Area ID □ ● ID 1 (1 to 16,777,215) ○ Alias $

Priority Adjustment

Designated IS Priority Adjustment 0 (-255 to 255)

Shortest Path First (SPF)

Latency of Routing Recalculation □ 0 (0 to 60 seconds)

MINT Link Settings

MLCP IP ☑

MLCP IPv6 ☑

MLCP VLAN ☑

Tunnel MiNT across extended VLAN □

Tunnel Controller Load Balancing

Tunnel Controller Load Balancing (Level1) □

Inter Tunnel Bridging

Inter Tunnel Bridging (Level2) □

Tunnel Controller Group

Tunnel Controller Name

Preferred Tunnel Controller Group

Preferred Tunnel Controller Name

Uncheck to Disable Layer 2 Discovery

CLI Example:

```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile anyap STORES-AP
NX9500-ACTIVE(config-profile-STORES-AP)# no mint mlcp vlan
NX9500-ACTIVE(config-profile-STORES-AP)# commit write
```

Layer 3 Adoption

Static – Controller Hostnames

Site Controllers and Access Points support static layer 3 discovery using Controller Hostnames defined in the Site Controller or AP Profiles. Controller Hostnames are typically used for deployments when remote Site Controllers and APs are assigned static network addressing or where DNS or DHCP services are not deployed. Controller Hostnames can also be used for deployments where DNS based discovery is used to automatically discover the Centralized Controllers and establish IP based Level 1 MINT links but Level 2 MINT links are required.

Note

It is important to note that zero-touch deployments are not possible when static IPv4 or IPv6 addresses are assigned to Site Controllers or APs as pre-staging is required to pre-define the Controller Hostname parameters required by Site Controllers and APs to discover their adopters.

Each Controller Hostname parameter includes the IP Address or FQDN of the adopter in addition to the Pool and MINT Routing Level. Each Site Controller or AP is typically assigned two Controller Hostname parameters where Pool 1 defines the preferred adopter and Pool 2 the less preferred adopter. The MINT routing level must be set to Level 2 for Site Controllers and APs adopting to a Centralized Controller and Level 1 for APs adopting to Site Controllers.

The following table provides a summary of the basic Controller Hostname parameters which can be defined in the Site Controller and AP Profiles:

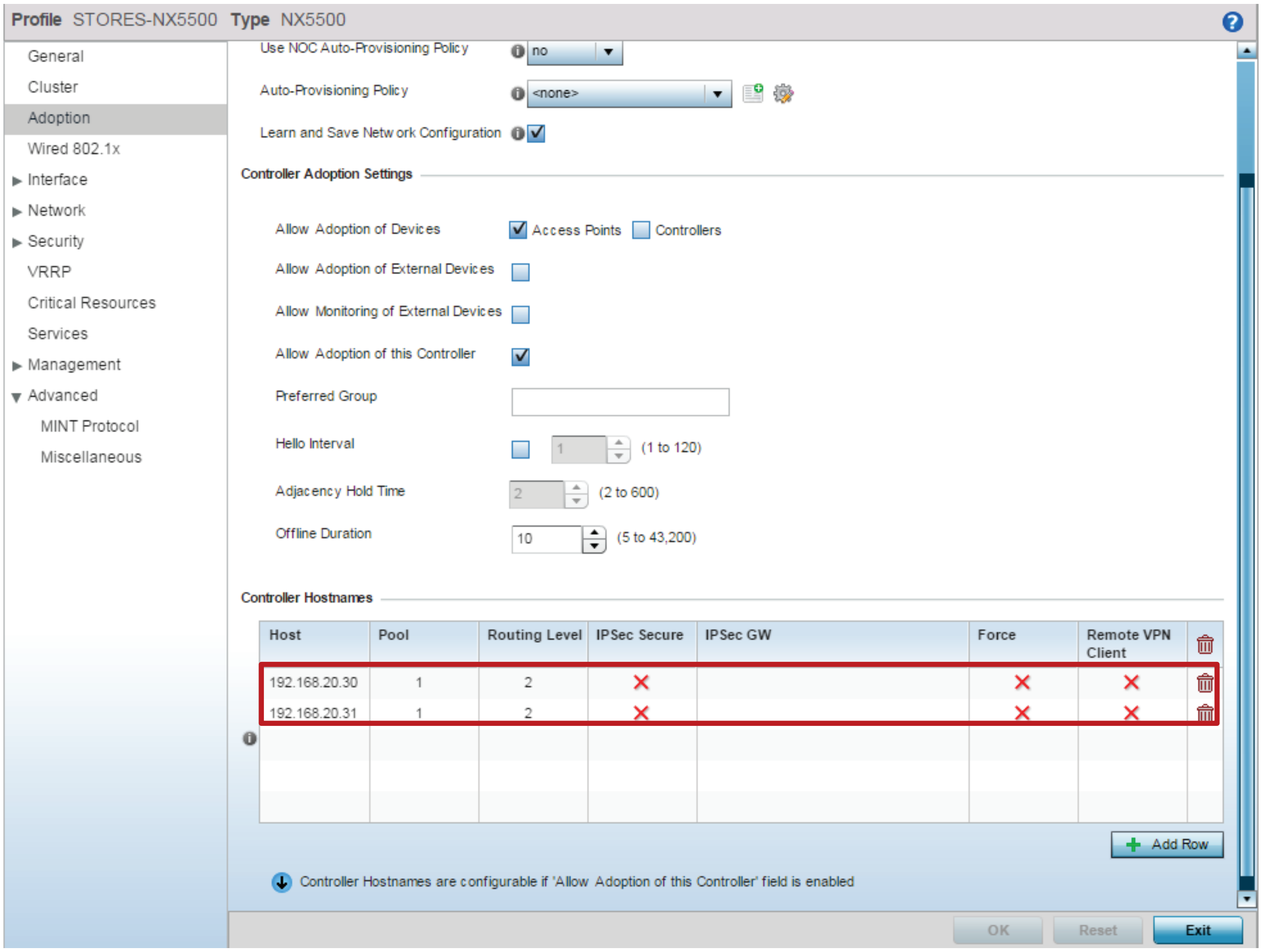
Parameter	Value	Description
Host	IP Address/FQDN	Host IP Address / FQDN The IPv4 / IPv6 address or FQDN of the adopter
Pool	1 or 2	Pool 1 or 2 The Controller Pool the adopter belongs to: • If both Controller Host entries are set to Pool 1, MLCP will attempt discovery against both IP Addresses / Hostnames, only Active controller will send an MLCP reply though. • If the Controller Host entries are set to Pool 1 and Pool 2, MLCP will only attempt to discover the IP Address / Hostname of Pool 2 if the IP Address / Hostname for Pool 1 is unreachable. Useful to achieve geographical redundancy with multiple controller clusters
Routing Level	1 or 2	Routing Level 1 or 2 The MINT link level to be established.

Note

The Controller Hostname parameter can also be used to initiate an Auto-IPsec Secure or a Remote VPN Connection between the adoptee and adopter if the management / control and tunneled user traffic needs to be secured.

The following example demonstrates how to define Controller Hostnames in an NX 5500 Profile named STORES-NX5500 using the Web-UI and CLI. In this example the remote NX 5500 Site Controllers use the Controller Hostname parameters to discover and adopt to the Active Centralized Controllers using IPv4 based Level 2 MINT links:

Path: **Configuraiton** -> **Profiles** -> **<profile-name>** -> **Advanced** -> **MINT Protocol**



Use NOC Auto-Provisioning Policy: no

Auto-Provisioning Policy: <none>

Learn and Save Network Configuration ☑

Controller Adoption Settings

Allow Adoption of Devices ☑ Access Points □ Controllers

Allow Adoption of External Devices □

Allow Monitoring of External Devices □

Allow Adoption of this Controller ☑

Preferred Group

Hello Interval □ 1 (1 to 120)

Adjacency Hold Time 2 (2 to 600)

Offline Duration 10 (5 to 43,200)

Controller Hostnames

Host	Pool	Routing Level	IPSec Secure	IPSec GW	Force	Remote VPN Client
192.168.20.30	1	2	✗		✗	✗
192.168.20.31	1	2	✗		✗	✗

Controller Hostnames are configurable if 'Allow Adoption of this Controller' field is enabled

CLI Example:

```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile nx5500 STORES-NX5500
NX9500-ACTIVE(config-profile-STORES-NX5500)# controller host 192.168.20.30 pool 1 level 2
NX9500-ACTIVE(config-profile-STORES-NX5500)# controller host 192.168.20.31 pool 1 level 2
NX9500-ACTIVE(config-profile-STORES-NX5500)# commit write
```

Dynamic – DHCP Discovery

Site Controllers and Access Points support dynamic layer 3 discovery using Dynamic Host Control Protocol (DHCP). DHCP can be used to assign network addressing to the remote Site Controllers and APs in addition to sending WING vendor-specific DHCP options. In WING two vendor-specific DHCP options are supported for discovery and adoption:

- Option 191 – Can be supplied to APs with a DHCP offer for discovery and adoption.
- Option 192 – Can be supplied to Site Controllers with a DHCP offer for discovery and adoption.

DHCP options 191 and 192 are supplied as ASCII / strings in the DHCP offer to the adoptee and each string can include the IP Addresses / FQDN and Pool of the adopters in addition to the MINT Routing Level. DHCP options can also be used to communicate advanced parameters such as the UDP port, MINT timers and if Auto IPsec Secure or VPN client should be initiated to secure the MINT link.

Each Site Controller or AP is typically assigned two IP addresses / FQDNs in the DHCP offer where Pool 1 defines the preferred adopter and Pool 2 the less preferred adopter. The MINT routing level must be set to Level 2 for Site Controllers and APs adopting to a Centralized Controller and Level 1 for APs adopting to Site Controllers.

Table below provides a summary of the basic DHCP option 192 / 192 parameters which can be supplied by DHCP servers to Site Controllers and APs in a DHCP offer:

Option	Format	Example
191 / 192	ASCII / String	`pool1=<ip-fqdn>;pool2=<ip-fqdn>;level=<1|2>`

Option	Format	Example
pool1 | pool2	1 or 2	The Controller Pool the adopter belongs to: • If both Controller Host entries are set to Pool 1, MLCP will attempt discovery against both IP Addresses / Hostnames. • If the Controller Host entries are set to Pool 1 and Pool 2, MLCP will only attempt to discover the IP Address / Hostname of Pool 2 if the IP Address / Hostname for Pool 1 is unreachable.
IP / FQDN	IP Address / FQDN	IP / FQDN IP Address / FQDN The IPv4 / IPv6 Address or FQDN of the adopter. IPv4 addresses are defined in dotted quad notation while IPv6 addresses are contained in [ ] brackets.
Routing Level	1 or 2	Routing Level 1 or 2 The MINT link level to be established.

Note

If FQDNs are defined, DHCP must also supply the Site Controllers and APs with the domain-name and the IP address of at least one domain-name server.

In WING 5 each RFS / NX / VX and AP also includes the IETF standard Class Identifier (option 60) in the DHCP discover and ACKs which can be optionally used by the DHCP server to supply specific DHCP options to Site Controllers and APs based on their model type. Class identifiers can be especially useful as it allows DHCP administrators to define option 191 and 192 values globally rather than per DHCP scope in addition to solving challenges when other DHCP clients support the same options but require different values.

Table below provides a summary of Class Identifiers supported by each model of RFS, NX and AP:

Model	Class Identifier	Model	Class Identifier
RFS 4000	WingRFS.RFS4000	AP 621	WingAP.AP621
RFS 6000	WingRFS.RFS6000	AP 622	WingAP.AP622
RFS 7000	WingRFS.RFS7000	AP 650	WingAP.AP650
NX 4500	WingNX.NX4500	AP 6511	WingAP.AP6511
NX 4524	WingNX.NX4524	AP 6521	WingAP.AP6521
NX 5500	WingNX.NX5500	AP 622	WingAP.AP622
NX 6500	WingNX.NX6500	AP 6522	WingAP.AP6522
NX 6524	WingNX.NX6524	AP 6562	WingAP.AP6562
NX 7500	WingNX.NX7500	AP 6532	WingAP.AP6532
NX 9XXX	WingNX.NX9XXX	AP 7131	WingAP.AP7131
		AP 7161	WingAP.AP7161
		AP 7181	WingAP.AP7181
		AP 7502	WingAP.AP7502
		AP 7522	WingAP.AP7522
		AP 7532	WingAP.AP7532
		AP 7562	WingAP.AP7562
		AP 8122	WingAP.AP8122
		AP 8132	WingAP.AP8132
		AP 8222	WingAP.AP8222
		AP 8232	WingAP.AP8232
		AP 8432	WingAP.AP8432
		AP 8533	WingAP.AP8533

Dynamic – DNS Discovery

Site Controllers and Access Points (APs) support dynamic layer 3 discovery using Domain Name System (DNS) resolution. DNS discovery allows Site Controllers and APs to dynamically discover the IP addresses of the Centralized Controllers in the data center by attempting to resolve the `wing-wlc` hostname at each domain level. The DNS server can respond with one or more IPv4 or IPv6 addresses of the Centralized Controllers depending on how many A records have been defined on the assigned DNS name servers. APs can also use DNS to discover local Site Controllers if desired.

Site Controllers and Access Points (APs) will only attempt DNS discovery if network addressing and DNS parameters have been statically defined or dynamically assigned from a Dynamic Host Control Protocol (DHCP) server. DNS discovery will also not be attempted if Controller Hostnames are defined or DHCP options 191 or 192 are assigned from the DHCP server.

It is important to note that DNS discovery can only be used to establish Level 1 IP based MINT links with the Active Centralized Controller and cannot be used to establish Level 2 IP based MINT links. If Level 2 links are required, you must define Controller Hostnames in the Site Controller and AP Profiles to transition the MINT routing level to Level 2. The Remote Site Controllers and APs will then use DNS for the initial discovery and adoption and then once configured will then use the Controller Hostnames in their assigned Profiles for future discovery and re-adoptions.

The following example demonstrates the results from a nameserver lookup (nslookup) command line tool from a Windows host querying the wing-wlc.tmelabs.local hostname. In this example the name server has two A records defined and responds to the query with two IPv4 addresses:

```
C:\> nslookup wing-wlc.tmelabs.local
Server:  linux-server1.tmelabs.local
Address:  192.168.10.6

Name:    wing-wlc.tmelabs.local
Addresses:  192.168.20.50 192.168.20.51
```

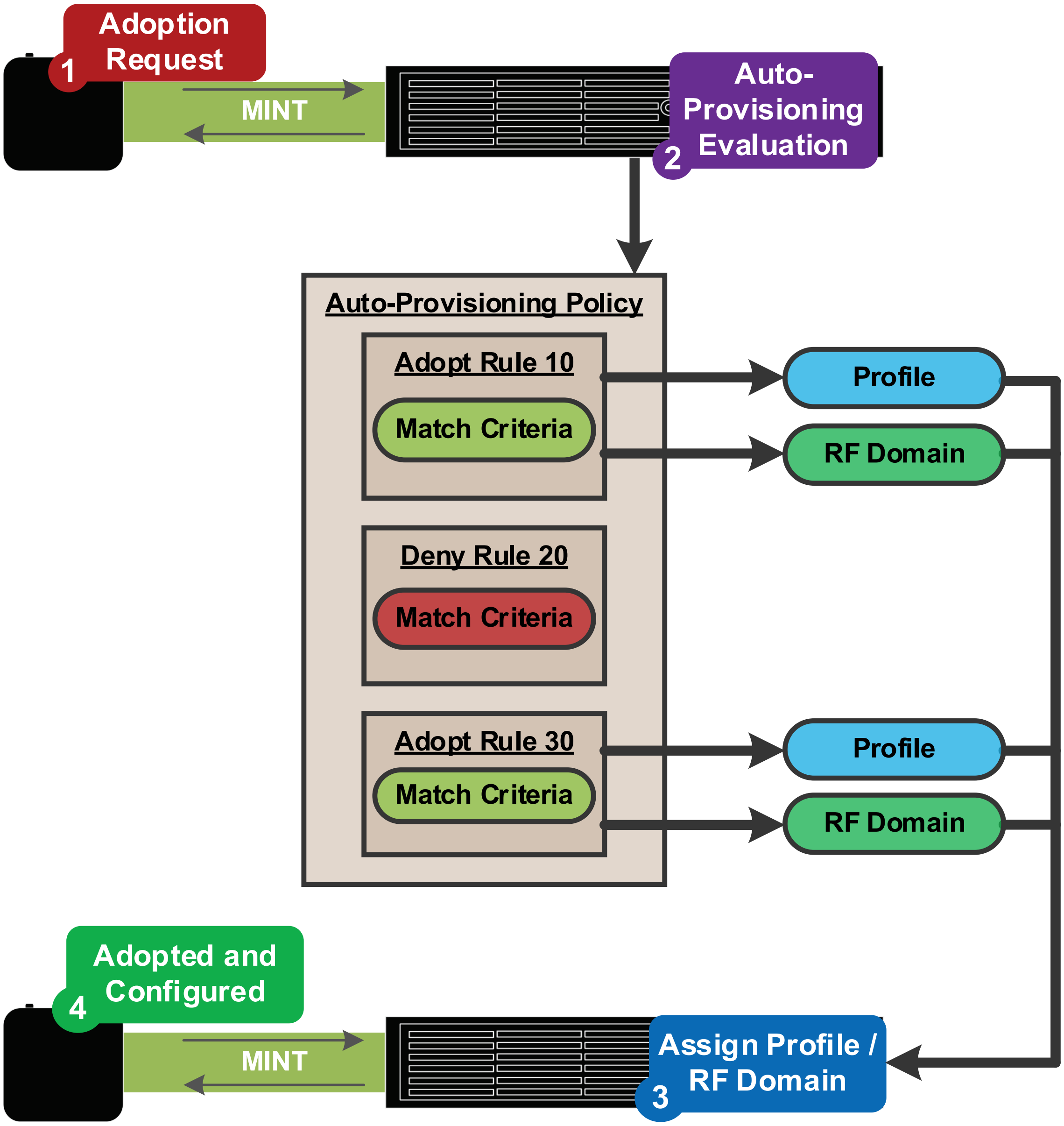
Note

Site Controllers and APs will attempt to resolve **wing-wlc** at each level in the domain. For example, if the device is assigned the domain name suffix store1.example.local, MLCP will first attempt to resolve wing-wlc.store1.example.local. If no A record exists it will then try to resolve wing-wlc.example.local, wing-wlc.local and finally wing-wlc until a response is received.

Auto-Provisioning Policies

When a Site Controller or Access Point AP is initially discovered and managed by a centralized controller, its device configuration is added to the master-configuration on the Centralized Controllers with the devices assigned Profile and RF Domain.

Once a Profile and RF Domain is assigned, the device configuration is applied to the remote Site Controller or AP. The applied configuration includes the Profile and RF Domain in addition to any Wireless LANs and Policies referenced by the assigned Profile and RF Domain. The applied configuration may also include device overrides if they have been learned during adoption or pre-staged in the master-configuration prior to adoption.



By default, a Centralized Controller and Site Controller will assign a default Profile and RF Domain to an adopting device. The default configuration on an RFS and NX includes a default RF Domain and Profile for each supported device in the release. While using a default RF Domain and Profile provides a plug-n-play experience, it is only recommended for standalone site deployments. Centralized deployments require one user defined RF Domain to be defined per site and as a best practice user defined Profiles for each model of Site Controller and AP in the system.

For zero-touch deployments in a centralized scenario, the user defined Profile and RF Domain for each new Site Controller and AP is automatically determined using an Auto-Provisioning Policy assigned to each pool of Centralized Controllers. The Auto-Provisioning Policy includes allow rules which assigns the correct RF Domain and Profile to each new Site Controller and AP based on match conditions defined for each rule.

Note

It is important to note that Auto Provisioning Policies only apply to new devices that are added to the centralized controller. Once a device has been added to the master-configuration and has been provisioned, subsequent adoptions will not use the Auto-Provisioning Policy. The exception to this is if the evaluate-always parameter is enabled in the Auto-Provisioning Policy in which case the Auto-Provisioning Policy rules will be evaluated for every adoption attempt.

Adoption Rules

Each Auto-Provisioning Policy includes an ordered list of rules which operate much like an Access Control List (ACL) where each rule either permits or denies adoption based on a defined match condition and value. For Steering Controllers additional rules are supported in that can redirect adopting devices to their preferred pool of Centralized Controllers or upgrade new devices when a version-mismatch is detected. Each Auto Provisioning Policy can support up to 10,000 rules.

During adoption Site Controllers and Access Points (APs) present information to the adopter such as their MAC address, Serial Number, IP address, hostname and FQDN in addition to information snooped from listening to CDP or LLDP advertisements. When a new device requests adoption, the Active Centralized Controller evaluates the rules in the Auto-Provisioning Policy in order of precedence and if a match is made the new device is assigned its RF Domain and Profile. If no match is made or a deny rule is matched, the new device is placed into a Pending Adoption state and no RF Domain or Profile is assigned.

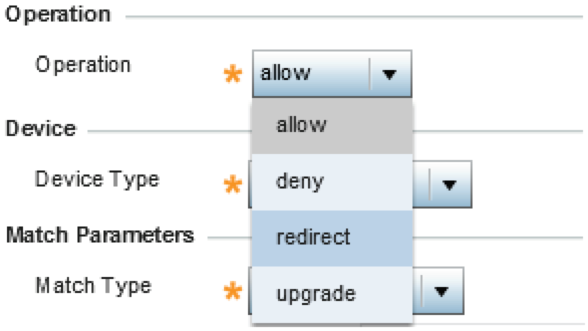
The number of allow rules you define in an Auto-Provisioning Policy will depend on the WING 5 device models you have deployed in the system, the match type you're using and the number of Profiles you have defined for each deployed model type.

Centralized deployments using standard match types such as IP will require one allow rule per remote site. For example, a remote AP only site with both AP 6521s and AP 6532s deployed would require 1 allow rule to be defined per site utilizing anyap profile. If the customer has 1,000 remote sites with both AP 6521s and AP 6532s, the Auto-Provisioning Policy will require 1,000 allow rules.

The Auto-Provisioning Policy rules may also be simplified by implementing wildcards if the Site Controllers and APs use pre-staged hostnames or the remote site uses a unique site identifier which can be captured from the DNS suffix or snooped from CDP or LLDP advertisements. If wildcards are implemented the number of allow rules can be reduced to as few as 1 rule per device and system where one rule assigns the RF Domain and a second rule assigns the Profile.

Operations

Each Auto-Provisioning Policy rule requires that you define an operation that either allows or denies the adoption of the new device. During the initial adoption each allow and deny rule is evaluated in order of precedence until a match is made. If no match is made or a deny rule is matched, an implicit deny is assumed and the device is placed into a pending adoption state.



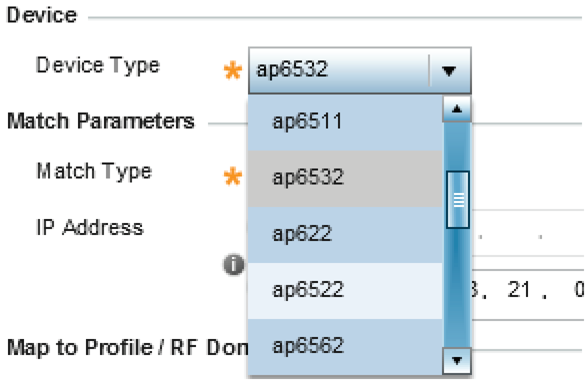
Operation * allow

Table below provides a summary of the operations supported per Auto-Provisioning Policy rule in WING 5:

Operation	Description
Allow	Permits adoption if the match criteria is met.
Deny	Denies adoption if the match criteria is met.
Redirect	Redirects device to another controller (steering-controller operation only)
Upgrade	Upgrades the device before redirecting to adopting controller (steering-controller operation only)

Device Types

Each Auto-Provisioning Policy rule allows to use either device specific profile or anyap profile that would match any device type when evaluating each rule. Each Auto-Provisioning Policy rule requires separate allow rules to be defined for each model of Site Controller and Access Point (AP) deployed on the centralized controller if device specific profiles are used, or a single rule when anyap profiles are utilized.



Device Type * ap6532

The types of devices supported within the Auto-Provisioning Policy is dependent on the model of RFS and NX the Auto-Provisioning Policy is assigned to. Larger platforms such as the NX 7500, VX 9000 and NX 9XX0 support the adoption and management of both Site Controllers and Access Points (APs) while smaller platforms such as the RFS 4000, RFS 6000, NX 5500 only support the adoption of APs. The Auto-Provisioning Policy rules on each platform will therefore only support the device types which the respective platform can support.

The following table provides a summary of supported device types per Auto-Provisioning Policy rule in WING 5 for each model of controller:

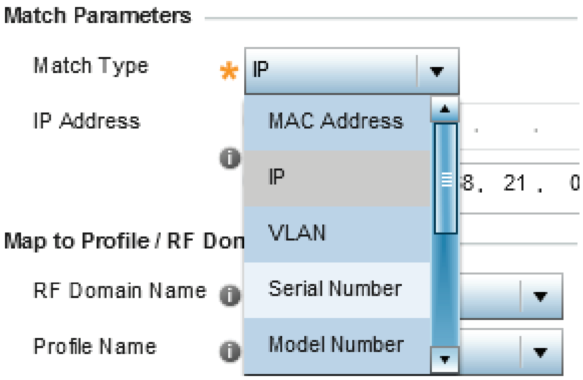
	RFS 4000 RFS 6000	RFS 7000	NX 45XX NX 65XX	NX 5500	NX 7500	VX 9000	NX 95XX	NX 96XX
RFS 4000	✗	✓	✗	✗	✓	✓	✓	✓
RFS 6000	✗	✓	✗	✗	✓	✓	✓	✓
RFS 7000	✗	✓	✗	✗	✓	✓	✓	✓
NX 45 / 65	✗	✗	✗	✗	✓	✓	✓	✓
NX 7500	✗	✗	✗	✗	✓	✓	✓	✓
VX 9000	✗	✗	✗	✗	✗	✓	✓	✓
NX 95X0	✗	✗	✗	✗	✗	✓	✓	✓
NX 96X0	✗	✗	✗	✗	✗	✓	✗	✓
AP 621	✓	✓	✓	✓	✓	✓	✓	✓
AP 622	✓	✓	✓	✓	✓	✓	✓	✓
AP 650	✓	✓	✓	✓	✓	✓	✓	✓
AP 6511	✓	✓	✓	✓	✓	✓	✓	✓
AP 6521	✓	✓	✓	✓	✓	✓	✓	✓
AP 6522	✓	✓	✓	✓	✓	✓	✓	✓
AP 6532	✓	✓	✓	✓	✓	✓	✓	✓
AP 71XX	✓	✓	✓	✓	✓	✓	✓	✓
AP 7502	✓	✓	✓	✓	✓	✓	✓	✓
AP 7522	✓	✓	✓	✓	✓	✓	✓	✓
AP 7532	✓	✓	✓	✓	✓	✓	✓	✓
AP 7562	✓	✓	✓	✓	✓	✓	✓	✓
AP 81XX	✓	✓	✓	✓	✓	✓	✓	✓
AP 82XX	✓	✓	✓	✓	✓	✓	✓	✓
AP 8432	✓	✓	✓	✓	✓	✓	✓	✓
AP 8533	✓	✓	✓	✓	✓	✓	✓	✓
ANY AP	✓	✓	✓	✓	✓	✓	✓	✓

Note

It is recommended that you check the release notes for each WING 5 release for a specific list of devices which can be adopted and managed by each mode of RFS and NX.

Standard Match

Each Auto-Provisioning Policy rule requires that you define a match type and value (argument) which is used in conjunction with the device type when evaluating each rule. Each Auto-Provisioning rule supports a single match type and the match value you enter will depend on the selected match type.



Match Parameters

Match Type * IP

IP Address

Map to Profile / RF Don

RF Domain Name

Profile Name

Following table provides a summary of standard match types supported per Auto-Provisioning Policy rule in WING 5:

Match Type	Description	Example Values
MAC Address	MAC Address Match is made based on the adopting devices MAC address 5C-0E-8B-A4-48-80	5C-0E-8B-A4-48-80
IP	Match is made based on the adopting devices host IP address or IP subnet	192.168.21.100 192.168.21.0/24
VLAN	Match is made based on the VLAN the adopted devices is connected to (used for Layer 2 adoption)	21
Serial Number	Match is made based on the adopting devices Serial Number	11193522200335
Model Number	Match based on the adopting devices Model Number	AP-7532-67030-US
Any	Match any adopting device	Not Applicable

The match type you select will be dependent on the network environment the remote Site Controllers and Access Points are connected to. Most centralized deployments will select a match type and value that is unique per site such as the IP to minimize the number of rules that are defined and managed in the Auto-Provisioning Policy. While device specific match types such as serial number or MAC address are supported, they should be avoided as these match types require a rule to be defined per device adding significant administrative overhead.

The following shows an example Auto-Provisioning Policy which uses the IP match type to assign a Profile and RF Domain to new AP 7532 APs as they are added to the centralized system. In this example one adopt rule is defined per remote site where the match value (argument) is set to the IP subnet the remote APs are connected to. Each rule is used to assign a RF Domain and Profile based on each AP source IP address.

```
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 profile STORES-AP-GUEST rf-domain STORE-1 ip 10.1.10.0/24
 adopt anyap precedence 2 profile STORES-AP-GUEST rf-domain STORE-2 ip 10.2.10.0/24
 adopt anyap precedence 3 profile STORES-AP-NOGUEST rf-domain STORE-3 ip 10.3.10.0/24
 ..
 adopt anyap precedence 100 profile STORES-AP-GUEST rf-domain STORE-100 ip 10.100.10.0/24
!
```

Wildcard Match Types

Wildcard match types provide the ability to assign Profiles and RF Domains to new devices without having to define separate rules for each site or device. Wildcards can significantly reduce the number of adopt rules that are required for centralized deployments by only requiring one wildcard rule for RF Domain assignment and one standard rule (per device type) for Profile assignments.

Unlike standard match types which assign a specific Profile or RF Domain based on a defined value (argument), wildcard rules allow Profiles and RF Domains to be assigned to new devices by partially matching information presented to the adopter by the remote device during the initial adoption. Wildcard rules are defined to match values in pre-defined hostnames, DHCP option string, DNS suffixes or neighbor information obtained from CDP or LLDP snooping which correlate to values in predefined RF Domains and Profiles on the system. The matched values are then used by the adopter to determine the RF Domain name or Profile name that is to be assigned to the new device.

Table 2.5.2.1.4 provides a summary of the wildcard match types supported per Auto-Provisioning Policy rule in WNG 5:

Match Type	Description
$DNS-SUFFIX	Wildcard match based on the adopting devices DNS suffix
$FQDN	Wildcard match based on values within the adopting devices hostname
$CDP	Wildcard match based on CDP neighbor device information snooped by the adopting device
$LLDP	Wildcard match based on LLDP neighbor device information snooped by the adopting device
$DHCP	Wildcard match based on DHCP option 191 string, in particular “rf-domain” tag is being looked at. Example: “pool1=controller1.domain.com,controller2.domain.com;level=2;rf-domain=store-100”

In centralized deployments wildcards are primarily used for RF Domain assignments where a unique site-id is obtained from pre-defined hostnames (FQDN), DNS suffixes or CDP / LLDP snooping. The rules are defined to look for specific characters from the supplied information which are used to match characters in the pre-defined RF Domain. For example, the DNS suffix st1001.us.example.com assigned to a remote site can be used to select and assign the pre-defined RF Domain named STORE-1001 where 1001 is matched by the wildcard rule.

If hostnames are pre-defined on the Site Controllers or Access Points, a FQDN wildcard can be used to assign both RF Domains and Profiles. The pre-defined hostname includes the unique site-id for RF Domain assignment and a separate value which is used to determine the correct Profile assignment. FQDN wildcard matches can be especially useful when a deployment requires different Profiles to be assigned for indoor, outdoor or sensor APs.

The use of wildcards in a centralized system assumes certain prerequisites are met to be successfully implemented. For example, if DNS suffix wildcards are used it is assumed that the devices at each remote site are assigned a DNS suffix which includes a unique site-id that follows a consistent format. The same applies if CDP or LLDP wildcards are used where the access layer switches must be named using a consistent format which includes the site-id. If the formatting differs between remote sites, separate wildcard rules must be defined.

The following provides a list of pre-requisites which must be met to implement wildcards for each match type:

- FQDN – Hostnames are pre-defined on the Site Controllers or APs that include the site-id for RF Domain assignment. If FQDN is used for Profile selection, a function identifier must also be included in the pre-defined hostname. To reduce the number of adopt rules, the pre-defined hostnames should follow the same format.
    - Hostname format example: STXXXYYYZZ where:
    - XXXX = Site-Id used for RF Domain assignment
    - YYY = AP function used for Profile assignment
    - ZZ = Device number
- DNS Suffix – Each remote site has a DNS suffix that includes the site-id for RF Domain assignment. To reduce the number of adopt rules, the DNS suffixes should follow the same format.
    - DNS suffix format example: siteXXXX.us.extremenetworks.com where:
    - XXXX = Site-Id used for RF Domain assignment
- DHCP – DHCP option 191 at the remote site contains "rf-domain" tag identifier with a unique value that includes the site-id for RF Domain assignment. To reduce the number of adopt rules, the DHCP rf-domain tag should follow the same format.
    - RF Domain naming convention format example: siteXXXX where:
    - XXXX = Site-Id provided by DHCP option 191 inside the rf-domain tag for example pool1=controller1.domain.com;level=2;rf-domain=1001
- CDP / LLDP – A unique hostname is assigned to each access layer switch which includes the site-id for RF Domain assignment. To reduce the number of adopt rules, the hostnames should follow the same format.
    - Access layer switch hostname format example: stXXXswYY where:
    - XXX = Site-Id used for RF Domain assignment
    - YY = Device number

Wildcard Example – FQDN Match Type

The following Auto-Provisioning Policy example demonstrates how wildcards can be used to automatically assign RF Domains and Profiles to new APs based on the devices pre-defined hostnames (example ACMEAPST321 or ACMESENST321). The hostnames are pre-defined on the APs prior to deployment and each hostname includes a site-id which is used to determine the RF Domain assignment and a string which is used to determine the Profile assignment:

1. RF Domain – The site-id (200 in this example) is used by the first rule to assign the RF Domain named STORE-200. The site-id in this case is provided by the pre-defined hostname in characters 9 – 11.

2. **Profile** – The AP function (AP or SN in this example) is used by the second rule to assign a Profile named STORE-AP or STORE-SN. The AP function in this case is provided by the pre-defined hostname in characters 5 – 6.

The formatting of the pre-defined hostnames determines the characters which are matched with the $FQDN wildcard. In this example the pre-defined hostnames are 11 characters in length where characters 4 – 6 denotes if the AP is a non-sensor (WAP) or sensor (SEN) for Profile assignment and characters 9 – 11 denotes the site-id for RF Domain assignment.

Predefined AP Hostname Format

A	C	M	E	A	P	S	T	2	0	0
				Chars 5-6				Characters 9 - 11		

```
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 rf-domain STORE-$FQDN[9:11] any
 adopt anyap precedence 2 profile STORE-$FQDN[5:6] any
!
```

Wildcard Example – DNS Suffix Match Type

The following Auto-Provisioning Policy example demonstrates how wildcards can be used to automatically assign RF Domains to new APs based on the DNS suffix assigned to the remote site (example st200.us.acme.local). In this example the DNS suffix for each remote site contains a site-id which is used to determine the RF Domain assignment:

1. **RF Domain** – The site-id (200 in this example) is used by the first adopt rule to assign the RF Domain named STORE-200. The site-id in this case is provided by the DNS suffix for each site in characters 3 – 5.
2. **Profile** – A common Profile named STORE-AP is assigned to all APs by the second adopt rule using the any match type.

The formatting of the DNS suffix determines the characters which are matched with the DNS suffix wildcard. In this example the DNS suffixes are variable in length where characters 3 – 5 denotes the site-id for RF Domain assignment. As there are no characters in the DNS suffix to determine the Profile assignment, the any match type is defined for Profile assignment.

Site DNS Suffix Format

s	t	2	0	0	.	u	s	.	a	c	m	e	.	l	o	c	a	l
		Chars 3-5																

```
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 rf-domain STORE-$DNS-SUFFIX[3:5] any
 adopt anyap precedence 2 profile STORE-AP any
!
```

Wildcard Example – DHCP Match Type

The following Auto-Provisioning Policy example demonstrates how wildcards can be used to automatically assign RF Domains to new APs based on the RF Domain identifier received via DHCP option 191 (example rf-doman=200). In this example the DHCP option 191 contains special “rf-domain” tag with a unique side id value for remote site which is used to determine the RF Domain assignment:

1. RF Domain – The site-id (200 in this example) is used by the first adopt rule to assign the RF Domain named STORE-200. The site-id in this case is provided by the DHCP option 191 via rf-domain tag.
2. Profile – A common Profile named STORE-AP is assigned to all APs by the second adopt rule using the any match type.

The formatting of the DNS suffix determines the characters which are matched with the DNS suffix wildcard. In this example the DNS suffixes are variable in length where characters 3 – 5 denotes the site-id for RF Domain assignment. As there are no characters in the DNS suffix to determine the Profile assignment, the any match type is defined for Profile assignment.

DHCP Option 191 Example:
pool1=192.168.20.30,192.168.20.31;level=2;rf-domain=200

```
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 rf-domain STORE-$DHCP any
 adopt anyap precedence 2 profile STORE-AP any
!
```

Wildcard Example – CDP / LLDP Match Types

The following Auto-Provisioning Policy example demonstrates how wildcards can be used to automatically assign RF Domains to new APs based on the CDP or LLDP neighbor information snooped from CDP / LLDP advertisements. In this example the access layer switches are provisioned with a unique hostname that includes the site-id (example st100cat3700sw1) which is used to determine the RF Domain assignment:

1. RF Domain – The site-id (200 in this example) is used by the first adopt rule to assign the RF Domain named STORE-200. The site-id in this case is provided by the neighboring Ethernet switches hostname advertised by CDP / LLDP in characters 3 – 5.
2. Profile – A common Profile named STORE-AP is assigned to all APs by the second adopt rule using the any match type.

The formatting of the hostname on the access layer switches the APs are connected to determines the characters which are matched with the CDP / LLDP wildcard. In this example the access layer switch hostnames are variable in length where fix characters 3 – 5 denotes the site-id for RF Domain assignment. As there are no characters in the access layer switches hostname to determine the Profile assignment, the any match type is defined for Profile assignment.

CDP / LLDP Neighbor Device ID Format
s t 2 0 0 c a t 3 7 0 0 s w 1
Chars 3-5

```
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 rf-domain STORE-$CDP[3:5] any
 adopt anyap precedence 2 profile STORE-AP any
!
!
auto-provisioning-policy DATACENTER
 adopt anyap precedence 1 rf-domain STORE-$LLDP[3:5] any
 adopt anyap precedence 2 profile STORE-AP any
!
```

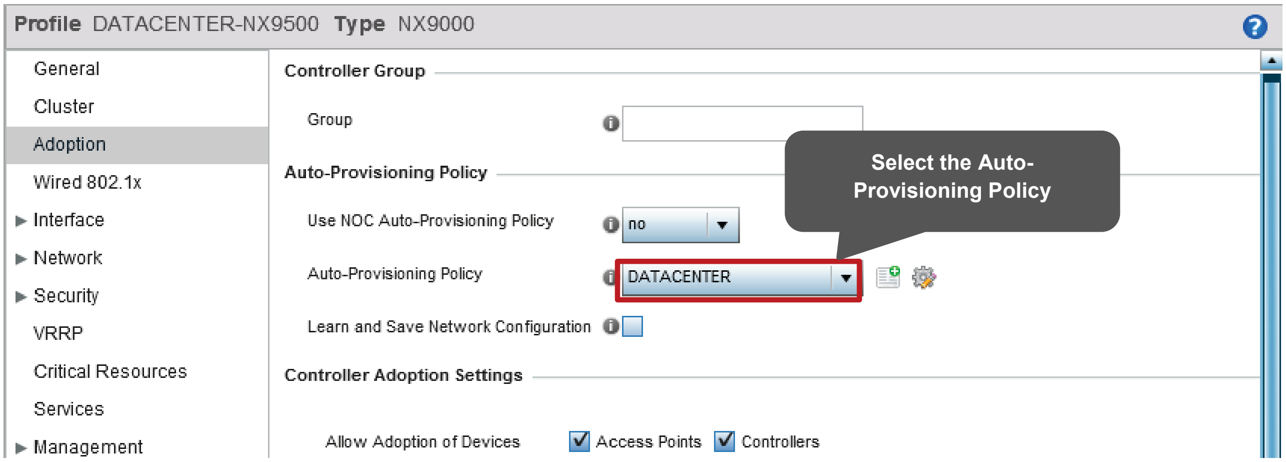
Auto-Provisioning Policy Mappings

The Centralized Controllers can adopt and manage remote Site Controllers and administrators have choice as to where the Auto-Provisioning Policies reside within the centralized system. Administrators can either elect to deploy and manage a single Auto-Provisioning Policy (centralized) that is mapped to the Centralized Controllers or use separate Auto-Provisioning Policies (distributed) which are mapped to both the Centralized Controllers and remote Site Controllers:

- Centralized – One Auto-Provisioning Policy and rules is defined and mapped to the Centralized Controllers in the data center for the whole centralized system. Adopt rules are defined for provisioning remote Access Points (APs) at AP Only Sites, remote Site Controllers and APs managed by the remote Site Controllers.
- Distributed – One Auto-Provisioning Policy and rules is defined and mapped to the Centralized Controllers for provisioning remote APs at AP only sites and remote Site Controllers. Separate Auto-Provisioning Policies and rules are defined and mapped to the Site Controllers for provisioning APs at Site Controller / AP sites.

Auto-Provisioning Policies can be assigned to Centralized Controllers as well as Site Controllers and as a best practice are mapped using Profiles. The following example demonstrates how to map an Auto-Provisioning Policy named DATACENTER to a NX 9000 Profile named DATACENTER-NX9000 using the Web-UI and CLI:

Path: Configuraiton -> Profiles -> DATACENTER-NX9600 -> Adoption



Profile DATACENTER-NX9500 Type NX9000

Controller Group

Group:

Auto-Provisioning Policy

Use NOC Auto-Provisioning Policy: no

Auto-Provisioning Policy: DATACENTER

Learn and Save Network Configuration □

Controller Adoption Settings

Allow Adoption of Devices ☑ Access Points ☑ Controllers

Select the Auto-Provisioning Policy

CLI Example:

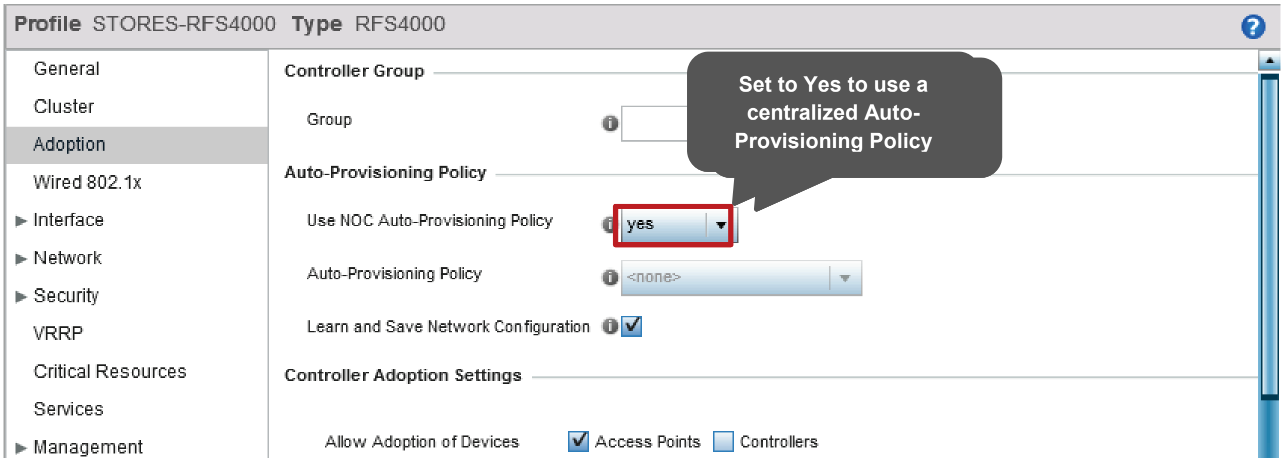
```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile nx9000 DATACENTER-NX9000
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# use auto-provisioning-policy DATACENTER
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# commit write
```

When a centralized Auto-Provisioning Policy is deployed in a centralized system, the remote Site Controllers are explicitly configured use the Auto-Provisioning Policy that is mapped to the Active Centralized Controller in the data center. When enabled, the remote Site Controller will query the Active Centralized Controller via the Level 2 MINT link to determine the RF Domain and Profile name to assign to the new Access Points (APs). The Active Centralized Controller will evaluate the Auto-Provisioning Policy rules in order of precedence to determine the RF Domain and Profile to assign to the remote AP and will respond to the remote Site Controller. If no level 2 MINT link is established from the remote site or no adopt rule is defined, the AP adoption will fail and the AP will be placed into a pending adoption state.

When a centralized Auto-Provisioning Policy is use, the Auto-Provisioning Policy must contain all the necessary adopt rules required to assign RF Domains and Profiles to new devices across the whole centralized system. This includes all the adopt rules required to provision APs for AP only sites in addition to the adopt rules required to provision Site Controllers and APs at Site Controller / AP sites. Failure to define the necessary rules will result in Site Controllers or APs failing to adopt and being placed into a pending adoption state.

The following example demonstrates how to configure a Site Controller Profile named STORES-RFS4000 to use a centralized Auto-Provisioning Policy using the Web-UI and CLI:

Path: Configuraiton -> Profiles -> STORES-RFS4000 -> Adoption



Profile STORES-RFS4000 **Type** RFS4000

Controller Group

Group

Auto-Provisioning Policy

Use NOC Auto-Provisioning Policy: yes

Auto-Provisioning Policy: <none>

Learn and Save Network Configuration: ☑

Controller Adoption Settings

Allow Adoption of Devices: ☑ Access Points ☐ Controllers

Set to Yes to use a centralized Auto-Provisioning Policy

CLI Example:

```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile nx9000 DATACENTER-NX9000
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# use auto-provisioning-policy DATACENTER
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# commit write
```

Note

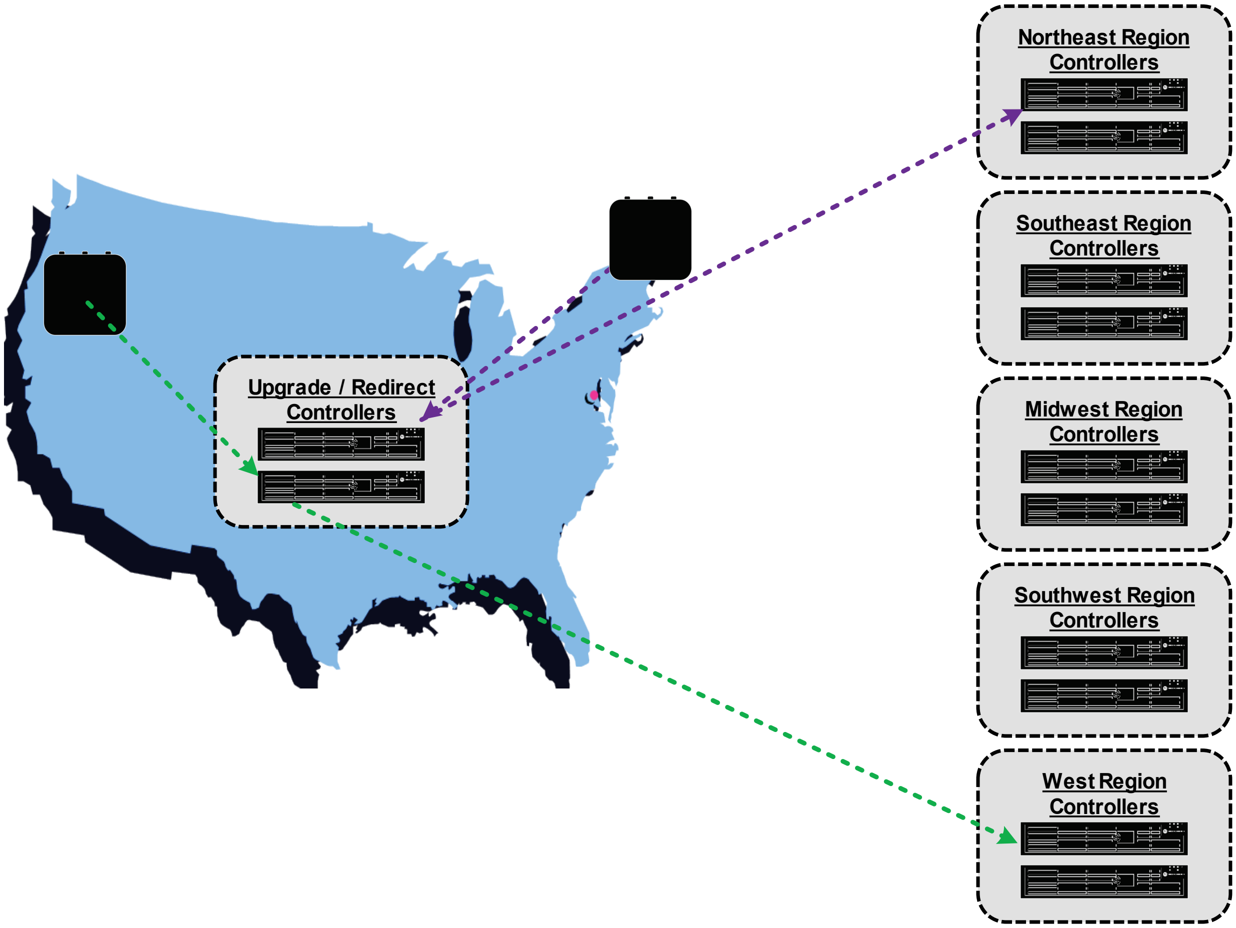
Centralized Auto-Provisioning Policies requires an active Level 2 MINT link to be established between the Active Centralized Controller and remote Site Controller to function. If the backhaul network is unstable or bandwidth constrained, it is recommended that you distribute the Auto-Provisioning Policies between the Centralized Controllers and Site Controllers.

Steering Controllers

Centralized deployments that exceed 10,240 x devices require multiple clusters of NX or VX to be deployed in the customer's datacenters. For these larger deployments customers will typically deploy separate clusters of controllers and distribute the remote sites between the clusters based on the remote sites geography or brand.

When multiple clusters of NXs are deployed in the customer's data center, it can become very challenging to administer as the remote Site Controllers and Access Points need to be directed to their correct pool of Centralized Controllers. This is either achieved managing assigning different Controller Hostnames, DNS A records or DHCP options to each group of devices.

WING 5 attempts to address this challenge by introducing support for Steering Controllers which can be deployed in the customer's data centers to steer adopting devices to their correct pool of Centralized Controllers. All the Site Controllers and APs in the centralized system use Controller Hostnames, DHCP options or DNS to discover the Steering Controllers rather than their assigned pool of Centralized Controllers. The Steering Controllers use an Auto-Provisioning Policy and rules to re-direct the Site Controllers and APs to their correct pool of Centralized Controllers. Redirect rules can also be defined to additionally upgrade the firmware if a version-mismatch is detected.


Northeast Region Controllers
Southeast Region Controllers
Midwest Region Controllers
Southwest Region Controllers
West Region Controllers
Upgrade / Redirect Controllers

The main advantage of using Steering Controllers is that it greatly simplifies the discovery process when multiple pools of Centralized Controllers are deployed in the data center. Site Controllers and APs are provided with a single URL (i.e. IP addresses / FQDNs) of the Steering Controllers rather than the actual IP addresses / FQDNs of their assigned pool of Centralized Controllers. This greatly reduces the administrative back-end overhead of managing a large centralized system.

Steering Controllers also permit the ability to allow administrators to migrate Site Controllers and APs between pools of Centralized Controllers either for re-distributing loads or maintenance purposes. Administrators can migrate devices to a new pool of Centralized Controllers by modifying the Auto-Provisioning Policy rules on the Steering Controllers rather than modifying Profiles or having to submit a change requests to update DNS A records or DHCP options.

Note
For Steering Controllers, the Auto-Provisioning Policy Rules are evaluated for each adoption request.

Redirect and Upgrade Operations

The Auto-Provisioning Policies on Steering Controllers include rules using the redirect and upgrade operations. Administrators can define separate redirect and upgrade rules or combine them into a single rule. If separate redirect and upgrade rules are defined, the upgrade rules must be defined before the redirect rules or the upgrade rules will not be matched prior to redirection. Most centralized deployments will require one redirect rule per device type and remote site using the IP match type, however other match types such as DNS Suffix or CDP / LLDP substrings are also supported.

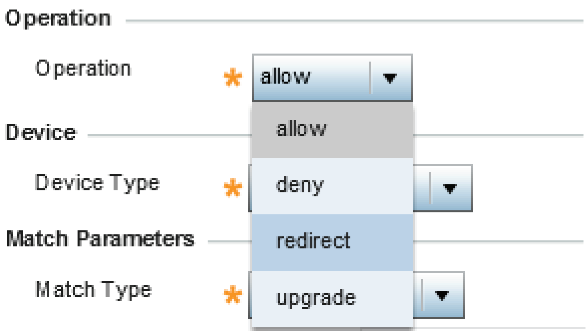


Table below provides a summary of the operations supported per Auto-Provisioning Policy rule in WING 5.5 and above:

Operation	Description
Redirect	Used by Steering Controllers to redirect an adopting device to their assigned pool of Centralized Controllers. Can also be used to optionally upgrade the firmware if a version-mismatch is detected prior to redirection.
Upgrade	Used by Steering Controllers to upgrade the firmware of an adopting device prior to redirection.

Each redirect rule includes the IP address / FQDN of the Active and Standby Centralized Controllers in addition to the pool and MINT Routing Level. Each redirect rule can also upgrade the firmware of the remote device prior to redirection if a version-mismatch is detected. This ensures that the remote Site Controller or AP is running the correct firmware version prior to being redirected.

Remote Site Controllers and Access Points (APs) can either establish Level 1 or Level 2 IP based MINT links to the Steering Controllers prior to being redirected to their designated pool of Centralized Controllers using Level 2 MINT links:

1. When an adoption request is received from a remote Site Controller or AP, the device is placed into a pending adoption state.

2. The Steering Controller evaluates each redirect rule and makes a match:
3. If a version-mismatch is detected the Steering Controller will upgrade the firmware of the remote device. Upon upgrading the remote device will reboot and re-establish a MINT link to the Steering Controller where the redirect rule re-evaluation occurs.
4. The Steering respond to the remote device with the IP address / FQDN of their assigned Centralized Controllers with the pool and MINT routing level.
5. The remote Site Controller or AP establishes an IP based Level 2 MINT link to its assigned Active Centralized Controller where Provisioning and Configuration is applied.

> Note
>
> It is important to note that the firmware version comparison is made between the NX / RFS / AP firmware images stored on the Steering Controllers and not the firmware version running on the Steering Controllers themselves.

Redirect Example – IP Match

```
!
auto-provisioning-policy STEERING-CONTROLLER
 upgrade anyap precedence 1 any
 redirect anyap precedence 2 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 1 level 2 ip
192.168.50.0/24
!
```

Redirect Example – CDP Match

```
!
auto-provisioning-policy STEERING-CONTROLLER
 redirect ap7532 precedence 1 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 2 level 2 cdp-
match 1000 upgrade
 redirect ap7532 precedence 2 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 2 level 2 cdp-
match 1001 upgrade
 redirect ap7532 precedence 3 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 2 level 2 cdp-
match 1002 upgrade
 redirect ap7532 precedence 4 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 2 level 2 cdp-
match 1003 upgrade
 redirect ap7532 precedence 5 controller 192.168.20.30 pool 1 controller 192.168.20.31 pool 2 level 2 cdp-
match 1004 upgrade
 redirect ap7532 precedence 6 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1005 upgrade
 redirect ap7532 precedence 7 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1006 upgrade
 redirect ap7532 precedence 8 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1007 upgrade
 redirect ap7532 precedence 9 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1008 upgrade
 redirect ap7532 precedence 10 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1009 upgrade
 redirect ap7532 precedence 11 controller 192.168.20.33 pool 1 controller 192.168.20.34 pool 2 level 2 cdp-
match 1010 upgrade
!
```

Data Pre-Staging

For certain centralized deployments it may be desirable to predefine certain device or network parameters such as network addressing or hostnames on remote Site Controllers and Access Points and have those parameters be automatically learned and added to the master-configuration on the Centralized Controllers during the initial adoption. This is especially important for deployments that utilize static network addressing as it allows the remote Site Controller or AP to maintain their network connectivity upon receiving their configuration from the Centralized Controllers. If the network parameters were not learned, the devices would lose their network connectivity upon receiving their configuration from the Centralized Controllers.

The Centralized Controllers have the ability to learn a number of device and network parameters during the initial adoption from both Site Controllers and APs. Parameters which can be learned include static IP addresses, default gateway, controller hosts and Virtual LANs. For remote Site Controllers the Centralized Controller can also learn cluster configuration parameters.

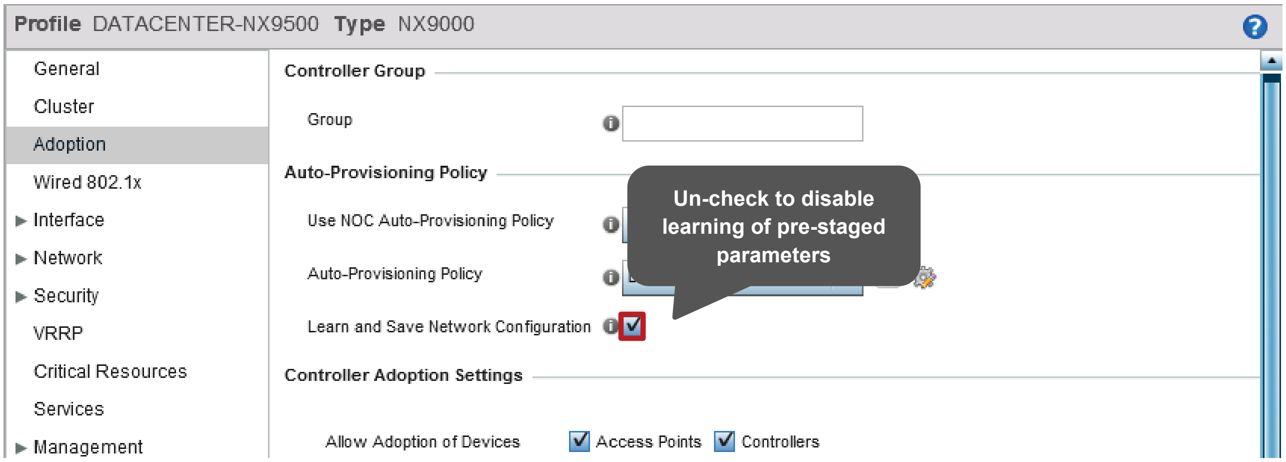
- Allowed VLANs
- Cluster (Site Controllers Only)
- Controller Host
- Default Gateway
- Domain Name
- Hostname
- Name Servers
- Native / Allowed VLANs
- Speed / Duplex
- Static Routes
- Switched Virtual Interfaces

The automatic learning of pre-staged parameters is enabled by default in most RFS and NX Profile. When enabled the Centralized Controller will add the supported pre-defined device level parameters to the master-configuration when the remote Site Controller or AP is adopted for the first time. Automatic learning can also be disabled to prevent the Centralized Controllers from learning any pre-staged parameters which may be desirable if Site Controllers or APs with existing configurations are commonly re-deployed.

The automatic learning of pre-staged configuration parameters only applies to new Site Controllers and Access Points that are added to the centralized system. Once a remote Site Controller or AP has been added to the master-configuration, all subsequent configuration changes must be performed on the Centralized Controller. Once the device or network parameters have been learned, they will remain as overrides for the device in the master-configuration until they are removed.

The following example demonstrates how to disable automatic learning of pre-staged configuration parameters for Site Controllers and APs in a NX 9000 Profile named DATACENTER-NX9000 using the Web-UI and CLI:

Path: Configuraiton -> Profiles -> DATACENTER-NX9600 -> Adoption



Profile DATACENTER-NX9500 Type NX9000

Controller Group

Group

Auto-Provisioning Policy

Use NOC Auto-Provisioning Policy

Auto-Provisioning Policy

Learn and Save Network Configuration ☑

Controller Adoption Settings

Allow Adoption of Devices ☑ Access Points ☑ Controllers

Un-check to disable learning of pre-staged parameters

CLI Example:

```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile nx9000 DATACENTER-NX9000
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# no auto-learn-staging-config
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# commit write
```

Controller Adoption Settings

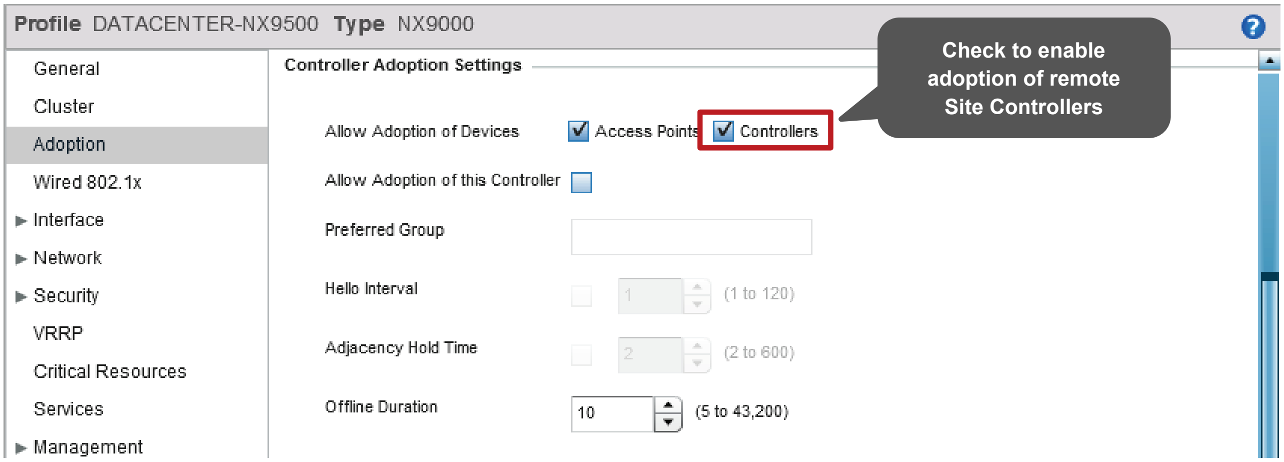
The Centralized Controllers support the adoption and management of both remote Site Controllers and Access Points. New adoption parameters were added to RFS and NX Profiles to allow administrators to determine which devices could be adopted and managed by the Centralized Controllers in the centralized system. Administrators can configure the Centralized Controllers to adopt and manage APs only (default) or adopt and manage both remote APs and Site Controllers.

Centralized Controllers

Administrators can control which devices can be adopted and managed by a Centralized Controller using the **Allow Adoption of Devices** parameter in the Profile. By default, the Centralized Controllers only support the adoption and management of remote Access Points (APs). The adoption and management of remote Site Controllers must be explicitly enabled before the remote Site Controllers can be adopted and managed by the centralized controllers.

The following example demonstrates how to enable the adoption and management of remote Site Controllers in a NX 9000 Profile named DATACENTER-NX9000 using the Web-UI and CLI:

Path: **Configuraiton -> Profiles -> DATACENTER-NX9600 -> Adoption**



Profile DATACENTER-NX9500 **Type** NX9000

Controller Adoption Settings

Allow Adoption of Devices ☑ Access Points ☑ Controllers

Allow Adoption of this Controller □

Preferred Group

Hello Interval □ 1 (1 to 120)

Adjacency Hold Time □ 2 (2 to 600)

Offline Duration 10 (5 to 43,200)

Check to enable adoption of remote Site Controllers

CLI Example:

```
NX9000-ACTIVE# configure terminal
NX9500-ACTIVE(config)# profile nx9000 DATACENTER-NX9000
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# controller adopted-devices aps controllers
NX9500-ACTIVE(config-profile-DATACENTER-NX9000)# commit write
```

If the Allow Adoption of Devices – Controllers parameter is disabled in the Centralized Controllers Profile, this will be captured and displayed when you issue the show adoption adopter log command on the Active Centralized Controller. The log message will state that the MLCP discover message from the remote Site Controller is ignored as controller adoption is not enabled:

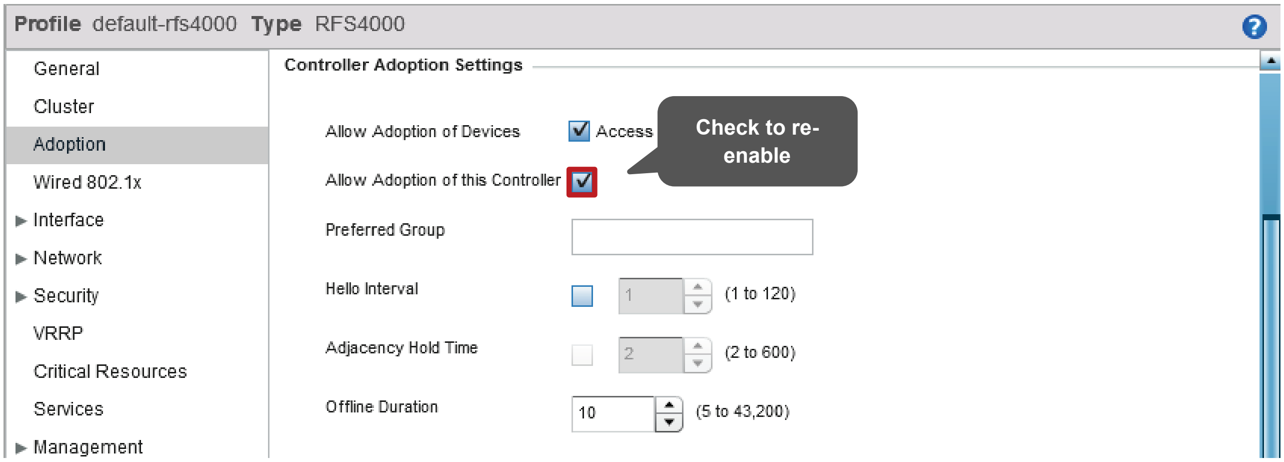
```
NX9500-ACTIVE# show adoption log adopter
2014-05-16 13:00:01:Ignoring MLCP Discover from controller 0B.1A.FE.A0: controller adoption not enabled
2014-05-16 12:59:56:Ignoring MLCP Discover from controller 0B.1A.FE.A0: controller adoption not enabled
2014-05-16 12:59:51:Ignoring MLCP Discover from controller 0B.1A.FE.A0: controller adoption not enabled
```

Site Controllers

Administrators can also control if the remote Site Controller is able to be managed and adopted by the Centralized Controller using the Allow Adoption of this Controller parameter which is enabled by default in each RFS and NX Profile. The Mint Link Control Protocol (MLCP) discovery process on the remote Site Controller will only initiate if the Allow Adoption of this Controller parameter is enabled. If the parameter has been disabled, it must be re-enabled prior to adoption to the Active Centralized Controller.

The following example demonstrates how to re-enable the Allow Adoption of this Controller parameter in a RFS 4000 Profile named default-rfs4000 using the Web-UI and CLI:

Path: Configuraiton -> Profiles -> default-rfs4000 -> Adoption



Profile default-rfs4000 **Type** RFS4000

Controller Adoption Settings

Allow Adoption of Devices ☑ Access

Allow Adoption of this Controller ☑

Preferred Group

Hello Interval □ 1 (1 to 120)

Adjacency Hold Time □ 2 (2 to 600)

Offline Duration 10 (5 to 43,200)

CLI Example:

```
S100ACME4K1# configure terminal
S100ACME4K1(config)# profile rfs4000 default-rfs4000
S100ACME4K1(config-profile-default-rfs4000)# controller adoption
S100ACME4K1(config-profile-default-rfs4000)# commit write
```

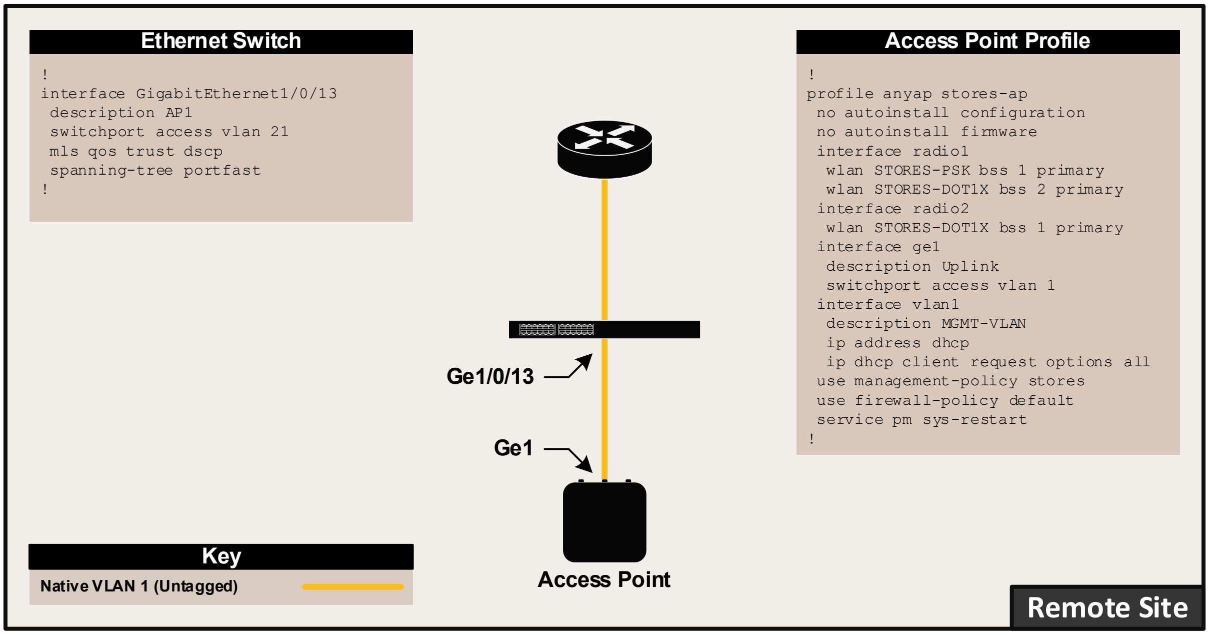
If the Allow Adoption of this Controller parameter is disabled in the Site Controllers Profile, this will be captured and displayed when you issue the show adoption adoptee command on the remote Site Controller. The log message will state that adoption is disabled due to configuration:

```
rfs4000-1AFEA0# show adoption log adoptee
2014-05-16 20:26:30:Adoption state change: 'No adopters found' to 'Disabled'
2014-05-16 20:26:30:Adoption disabled due to configuration
```

Data Forwarding

Local Bridging

Access Points deployed at remote sites forward traffic locally within the site or tunnel traffic to the Wireless Controllers in the data center. If the wireless user traffic at the remote site is mapped to a single VLAN, a single untagged Native VLAN can be deployed at the site and 802.1Q tagging does not need to be enabled. If an untagged Native VLAN id other than 1 is deployed at the remote site, we can safely leave it as VLAN 1 on the AP profile, no matter which VLAN will be actually configured as Native on wired switches (unless VLAN 1 is used in production).



Ethernet Switch

```
!
interface GigabitEthernet1/0/13
 description AP1
 switchport access vlan 21
 mls qos trust dscp
 spanning-tree portfast
!
```

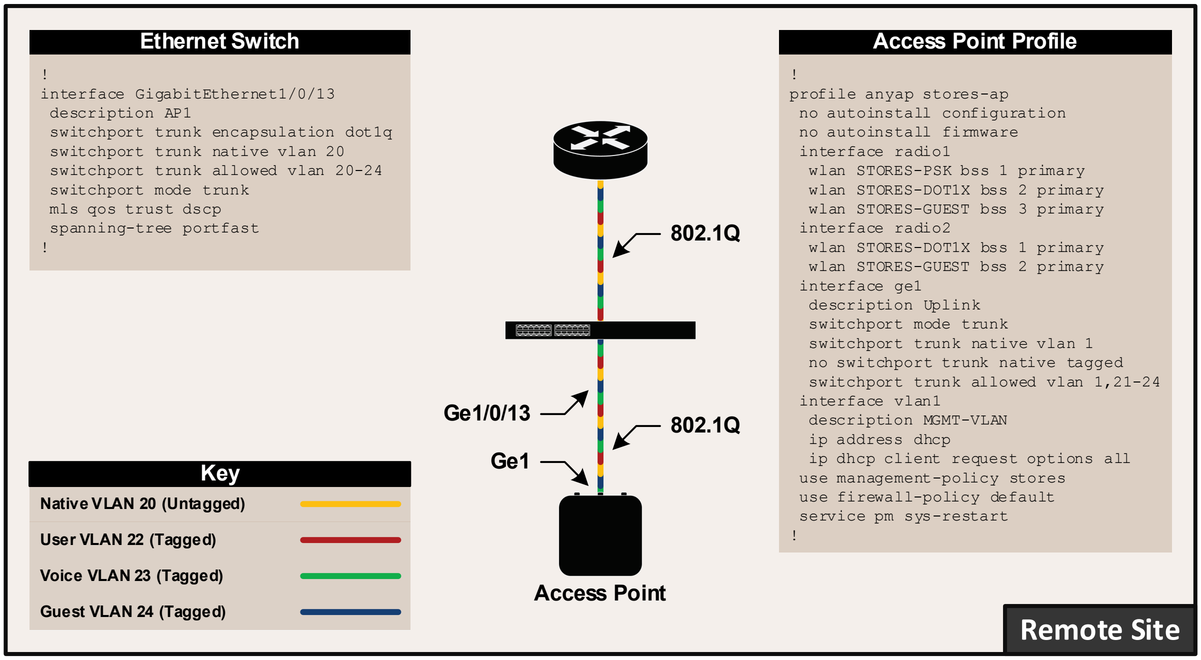
Access Point Profile

```
!
profile anyap stores-ap
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
  wlan STORES-PSK bss 1 primary
  wlan STORES-DOT1X bss 2 primary
 interface radio2
  wlan STORES-DOT1X bss 1 primary
 interface ge1
  description Uplink
  switchport access vlan 1
 interface vlan1
  description MGMT-VLAN
  ip address dhcp
  ip dhcp client request options all
 use management-policy stores
 use firewall-policy default
 service pm sys-restart
!
```

If wireless users are mapped to multiple different VLANs at the site, 802.1Q VLAN tagging must be enabled on both the Access Points Ge1 ports as well as the Ethernet switch ports the Access Points are connected to. The Allowed VLANs on both the Ethernet switch ports and the Access Points Ge1 ports must match or wireless user traffic maybe be dropped.

For plug-n-play Access Point deployments it recommended that the Access Points Native VLAN id at each remote site be configured as untagged. New Access Points deployed at a site will automatically obtain network addressing over their default VLAN 1. If the Ethernet switch port is configured to tag the Native VLAN and drop untagged frames, new Access Points will be unable to communicate with the network and discover the Wireless Controllers in the data center to receive their configuration.

Configuring the Native VLAN as untagged permits Controller discovery and will allow a new Access Point to adopt and receive its configuration in a zero touch manner. A new Access Point will obtain network addressing over VLAN 1, discover the Wireless Controllers in the data center using DHCP option 191, adopt and receive their configuration which includes the new Native VLAN id. Once received the Access Point will switch to the new Native VLAN id and obtain network addressing using the new Virtual IP interface and re-establish communications with the Wireless Controllers in the data center.



```
!
interface GigabitEthernet1/0/13
 description AP1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 20
 switchport trunk allowed vlan 20-24
 switchport mode trunk
 mls qos trust dscp
 spanning-tree portfast
!
```

```
!
profile anyap stores-ap
 no autoinstall configuration
 no autoinstall firmware
 interface radio1
  wlan STORES-PSK bss 1 primary
  wlan STORES-DOT1X bss 2 primary
  wlan STORES-GUEST bss 3 primary
 interface radio2
  wlan STORES-DOT1X bss 1 primary
  wlan STORES-GUEST bss 2 primary
 interface ge1
  description Uplink
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1,21-24
 interface vlan1
  description MGMT-VLAN
  ip address dhcp
  ip dhcp client request options all
 use management-policy stores
 use firewall-policy default
 service pm sys-restart
!
```

Tunneling

For certain centralized deployments it may be desirable to encapsulate and forward (i.e. tunnel) certain traffic from remote sites over a WAN / MPLS network to the data center. A common application requiring tunneling is guest or visitor access where all the guest / visitor traffic is inspected and filtered in the data center prior to being forwarded to the public Internet. Another common is to separate sensitive traffic or remediated hosts from other wired or wireless hosts at the remote site.

A centralized system supports two tunneling protocols which can be implemented to tunnel Wi-Fi user traffic from a remote site to the data center:

- Tunneling over Level 2 MINT – Used to encapsulate and forward Wi-Fi user traffic over selected VLANs to the data center when RFS 7000s, NX 5500s NX 7500s, NX 9510 or NX 9610s are deployed as Centralized Controllers.
- Tunneling over L2TPv3 – Used to encapsulate and forward Wi-Fi user traffic over selected VLANs to the data center when NX 9500s or VX9000s are deployed as Centralized Controllers.

The selection as to which tunneling protocol to implement will mainly depend on the hardware you deploy as the Centralized Controllers in the data center. Centralized Controllers such as RFS 7000s, NX 7500s or NX 9510s support traffic switching allowing tunneling over Level 2 MINT to be implemented where the Active Centralized Controller performs the management / configuration of the remote Site Controllers and Access Points in addition to terminating and forwarding the tunneled traffic. The NX 9500s or VX9000s offers no traffic switching support and therefore L2TPv3 must be implemented if tunneling is required where the L2TPv3 tunnels are terminated on separate pools of RFS 7000s, NX 5500s, NX 7500s or NX 9X10s that reside in points of presence (POPs) or the data center.

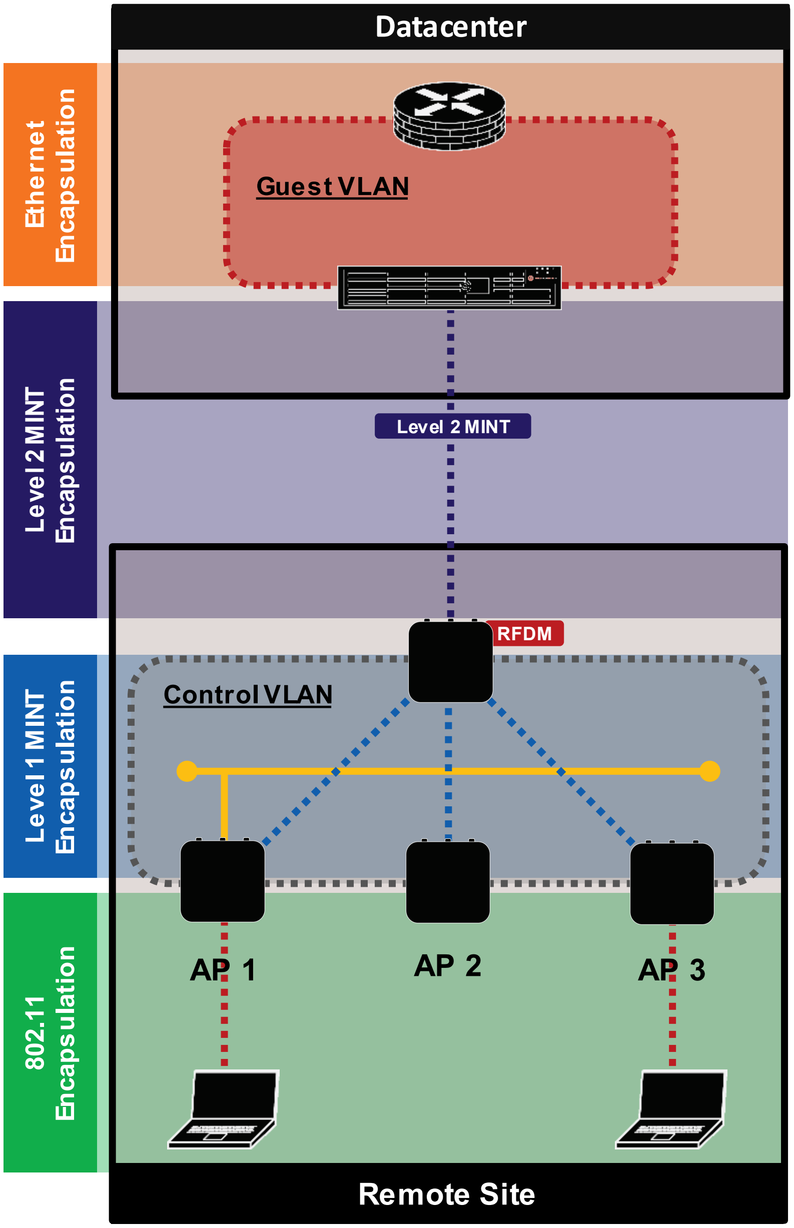
Note

Both Level 2 MINT links and L2TPv3 tunnels can optionally be secured between the remote site and the data center using IPsec VPN tunnels. Both tunneling protocols can be secured using either Auto IPsec Secure or the IPsec VPN client.

Tunneling over Level 2 MINT

Medium Independent Network Transport (MINT) is the proprietary protocol used for management / configuration and data encapsulation between WING 5 devices. WING 5 natively supports encapsulating and forwarding multiprotocol layer 2 communications from remote sites to the Active Centralized Controller over IP based Level 2 MINT links.

Tunneling over Level 2 MINT can be implemented when VLANs from remote sites need to be tunneled to the data center when RFS 7000, NX 7500 or NX 9X10 appliances are deployed as Centralized Controllers. Unlike L2TPv3 where the tunnels can terminate on separate appliances, tunneling over Level 2 MINT links require the tunneled VLANs be terminated on the Active Centralized Controller that is managing the remote Site Controllers and Access Points (APs). The Active Centralized Controller is not only responsible for management / configuration of all the remote devices within the centralized system but is also responsible for switching the tunneled user traffic from the remote sites onto the wired network.



The tunneling of VLANs between the remote sites and the Active Centralized Controller leverages both Level 1 and Level 2 MINT links:

- **Level 1 MINT Links (VLAN or IP based)** – Transports the user VLAN(s) between the elected RF Domain Manager (RFDM) and non-RFDMs within each remote site
- **Level 2 MINT Links (IP based)** – Transports the user VLAN(s) between the elected RFDM and the Active Centralized Controller in the data center.

Wi-Fi user traffic is mapped to one or more VLAN IDs which are tunneled using Level 1 MINT links between the WING 5 devices at the remote site. The tunneled VLANs are not assigned to the GE ports on the Site Controllers or APs to provide layer 2 separation and prevent loops. The elected RDFM maintains the Level 2 MINT link and bridges the traffic between the Level 1 MINT and Level 2 MINT links.

The default gateway and DHCP services for each tunneled VLAN is provided in the data center where the Active Centralized Controller resides. Routing and DHCP services can either be provided internally by the Active Centralized Controller or externally on separate appliances deployed behind the Active Centralized Controller.

> Note
>
> Wi-Fi user traffic that is encapsulated in Level 2 MINT uses User Datagram Protocol (UDP) with the destination port 24577.

Tunneling – Broadcast Domains

Tunneling over Level 2 MINT links or L2TPv3 uses multiprotocol layer 2 encapsulation which effectively extends the broadcast domain for each tunneled VLAN from the remote sites to the Active Centralized Controller or preferred L2TPv3 concentrator that's terminating the tunneled traffic. If all the remote sites tunnel a common VLAN ID, the IPv4 subnet for the tunneled VLAN will be shared between all the remote sites.

Fortunately WING 5 provides several mechanisms which can be implemented to minimize the impact of deploying large broadcast domains between the remote sites:

1. By default, tunnel-to-tunnel traffic is not permitted by the Active Centralized Controller or preferred L2TPv3 Concentrator. This prevents site-to-site communications via the data center, POP or DMZ.
2. Default IP and MAC ACLs are pre-defined in WING 5 which can be applied to Wireless LANs to drop unnecessary broadcast and multicast traffic before it is tunneled. While unicast and ARP traffic is still forwarded, all other traffic will be dropped at the edge of the network.
3. VLAN Pooling can be implemented to break large broadcast domains into smaller broadcast domains.

AAA Redundancy

For remote Access Point deployments RADIUS AAA services are typically provided centrally within the data center where multiple redundant RADIUS AAA servers are deployed. However, RADIUS AAA servers may also be deployed locally at each remote site using physical servers or on network infrastructure such as Routers or a WING 5.X device that supports commonly used EAP methods like PEAP-MSCHAPv2 and EAP-TLS.

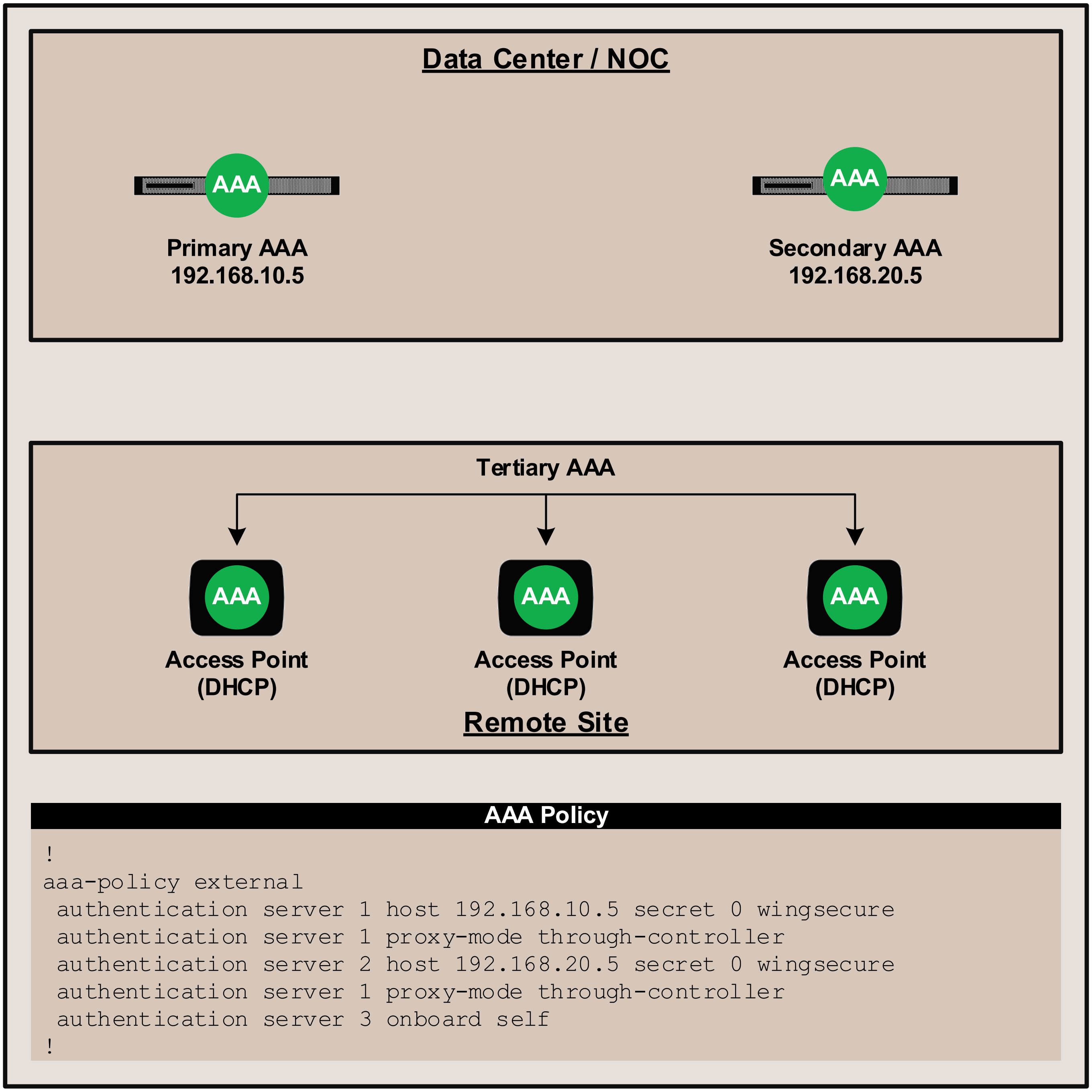
The RADIUS AAA servers used to authenticate wireless users is defined in AAA Policies which are assigned to individual Wireless LANs or Captive Portal Policies. Each AAA Policy can include up to six RADIUS Authentication and Accounting server entries which can be load-balanced (round-robin) or provide fail-over. Each Authentication or Accounting server entry supports three different Server Types:

- Host – RADIUS server is hosted on an external host.
- Onboard Self – RADIUS server is hosted locally on the Access Point.
- Onboard Controller – RADIUS server is hosted on the Wireless Controller adopting the Access Point.
- Onboard Centralized Controller – RADIUS server is hosted on the top Wireless Controller managing the whole network.

For each Server Type WING 5.X also supports a Proxy Request Mode which determines how RADIUS Authentication and Accounting requests are forwarded. RADIUS Authentication and Accounting requests can be forwarded directly from the Access Points to the RADIUS server, proxied through the elected RF Domain Manager at the remote site, proxied through a particular MINT Host or be forwarded through the Wireless Controllers in the data center.

If no RADIUS servers are available at a remote site, existing authenticated users will continue to operate with no interruption as by default user credentials are cached by the Access Points for up to 24 hours. However new users connected to Wireless LANs that require authentication will require an available RADIUS server before being permitted access to the network.

RADIUS Authentication redundancy can be provided in a number of different ways. During normal operation RADIUS Authentication and Accounting requests can be forwarded to a primary RADIUS server in the data center which is backed up by a second RADIUS server either located in the same data center or an alternate data center. If data center communications are disrupted, RADIUS Authentication can be provided locally at the remote site either using a locally deployed RADIUS server, RADIUS service running on a Router or locally on each Independent Access Point.



AAA Policy

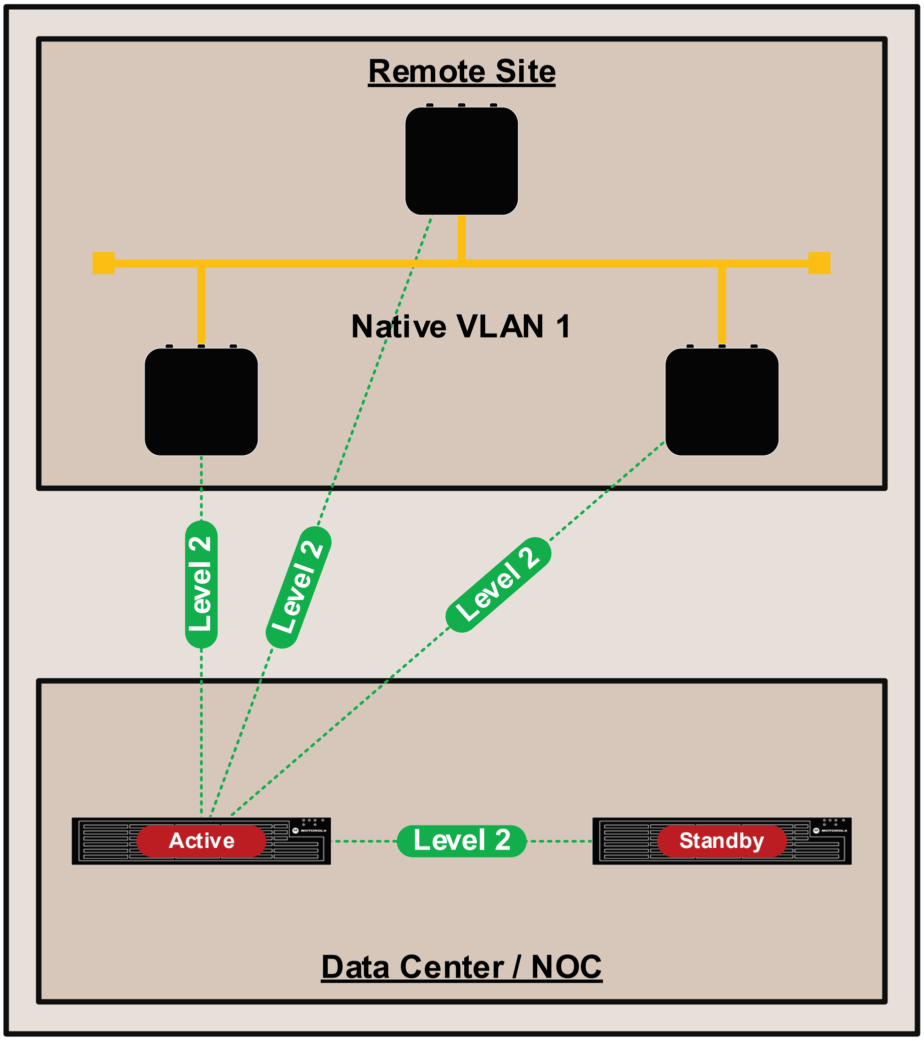
```
!
aaa-policy external
 authentication server 1 host 192.168.10.5 secret 0 wingsecure
 authentication server 1 proxy-mode through-controller
 authentication server 2 host 192.168.20.5 secret 0 wingsecure
 authentication server 1 proxy-mode through-controller
 authentication server 3 onboard self
!
```

When backup RADIUS services are provided locally on the Independent Access Points at a site, a RADIUS Server Policy will need to be defined and assigned to the Access Point Profile. The RADIUS Server Policy includes the RADIUS Server configuration along with specific User Pools. During a WAN outage, each Independent Access Point will be fully capable of authenticating EAP or Hotspot users locally providing no interruption to Wireless services at the remote site.

Centralized Architecture

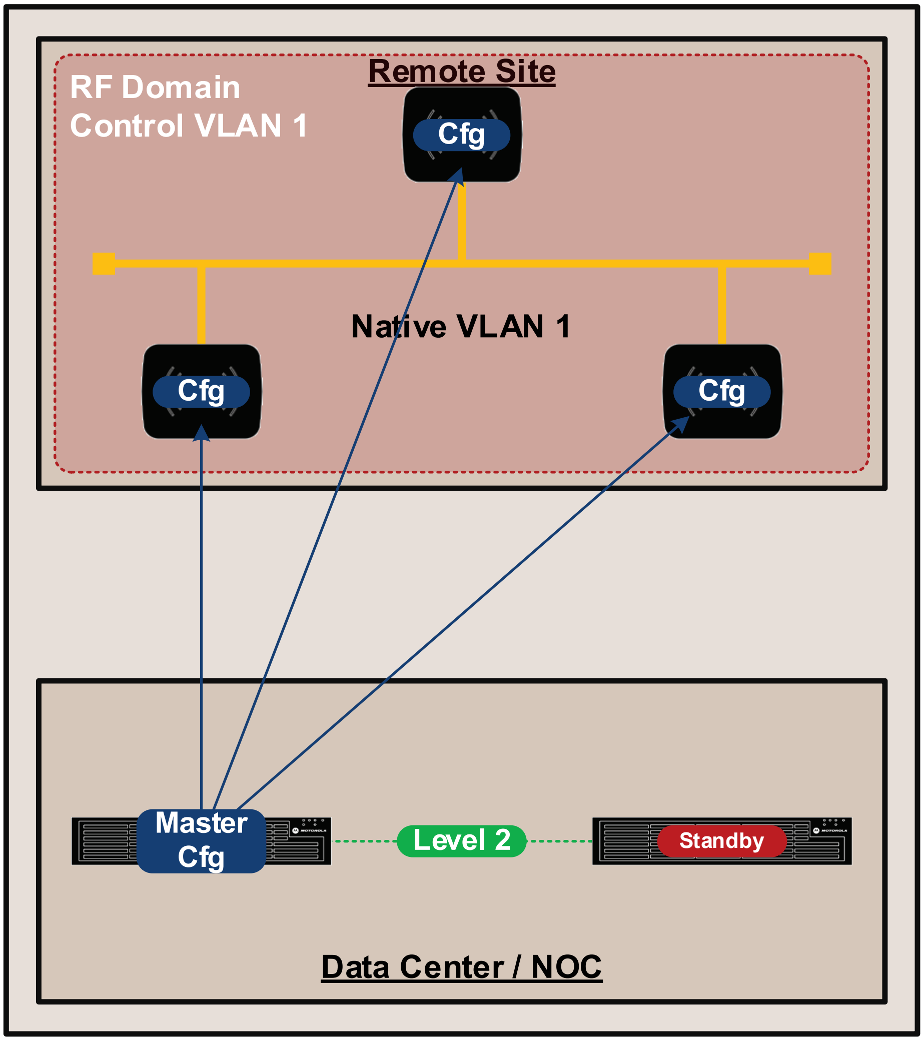
The WING5 centralized deployment model utilizes a cluster of Wireless Controllers in the data center. The cluster is configured using Level 2 IP or VLAN based MINT links rather than Level 1 MINT links typically utilized for campus deployments. Level 2 MINT links must be utilized for these large scale centralized deployments so that the Access Points at each remote site are isolated from Access Points at other sites reducing the MINT routing table size on the Access Points.

The following describes how the Access Points boot and communicate with the centralized model:



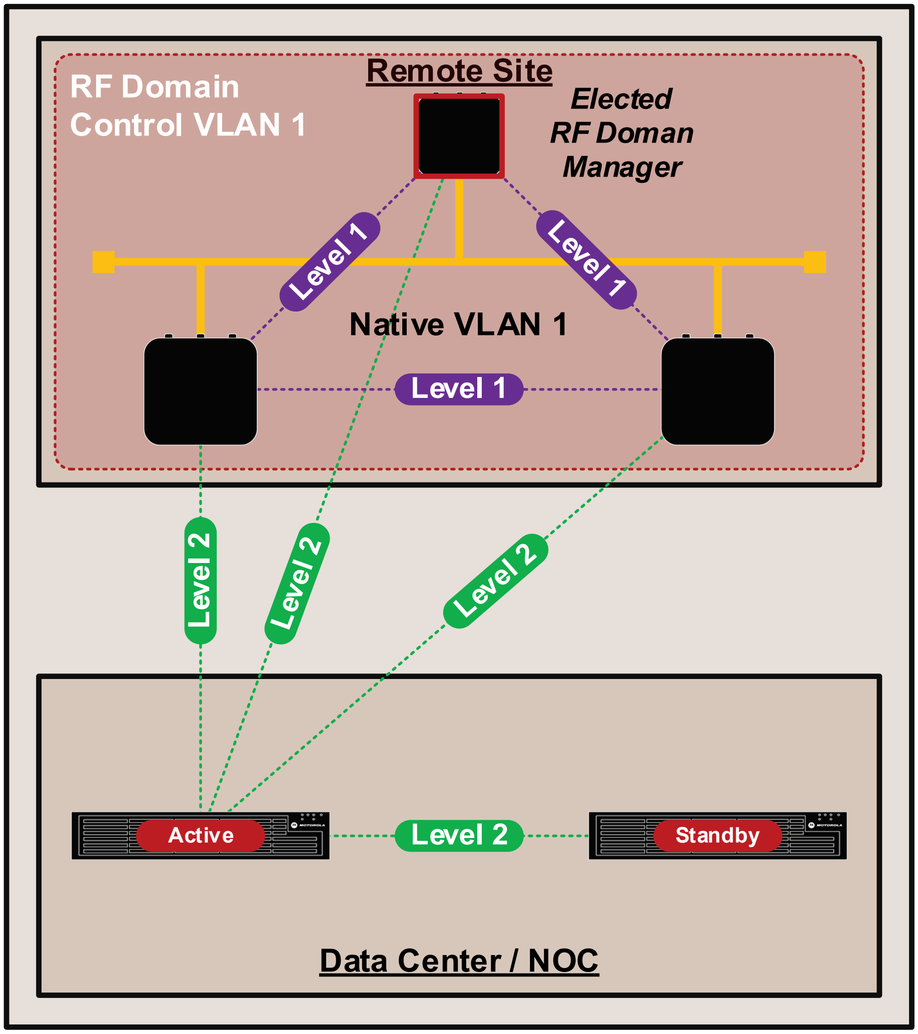
1. The Wireless Access Points at each remote site automatically discover the Wireless Controllers in the data center using DHCP option 191 or manually using static Controller IP addresses / Hostnames defined during staging.

   During initialization the remote Access Points use DHCP option 191 or static configuration to establish a Level 2 IP based MINT link to a Wireless Controller in the data center. The Access Point is adopted by the Active Cluster member.

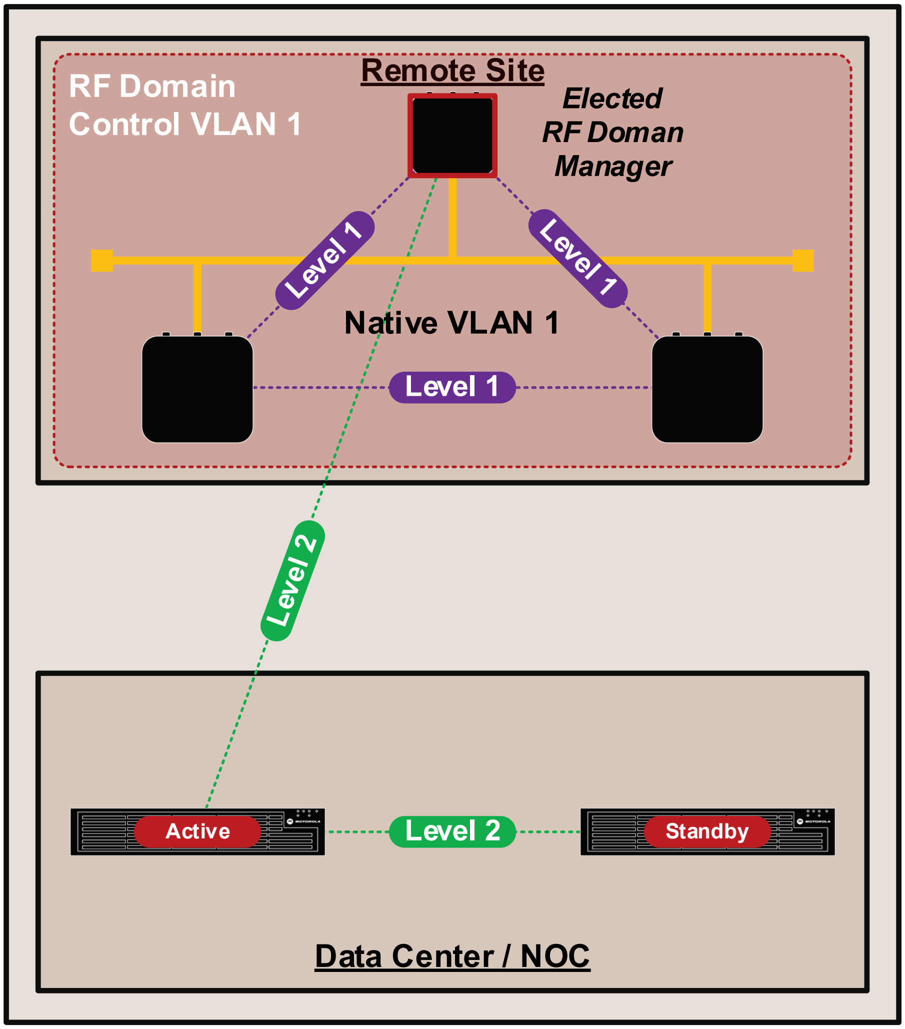


2. Once a Level 2 IP based MINT link to a Wireless Controller has been established, the Access Points receive their configuration which includes its assigned RF Domain and Profile in addition to any Device overrides, Wireless LANs and Policies.

   Each remote site is assigned a unique RF Domain which includes a Control VLAN definition for the remote site. The Control VLAN is typically the Native VLAN that all the Access Points at the remote site are connected to.



3. The Access Points at the remote site use their Control VLAN to establish a Level 1 VLAN based MINT link to discover all the neighboring Access Points at the site. The Access Points then elect one of the Access Points as the RF Domain Manager for the site which is responsible for firmware updated, statistic collection and SMART RF calculations.



4. All the Access Points except the elected RF Domain Manager tear down their Level 2 IP based MINT links to their Wireless Controller at the data center. If the elected RF Domain Manager fails, another Access Point will be automatically elected.

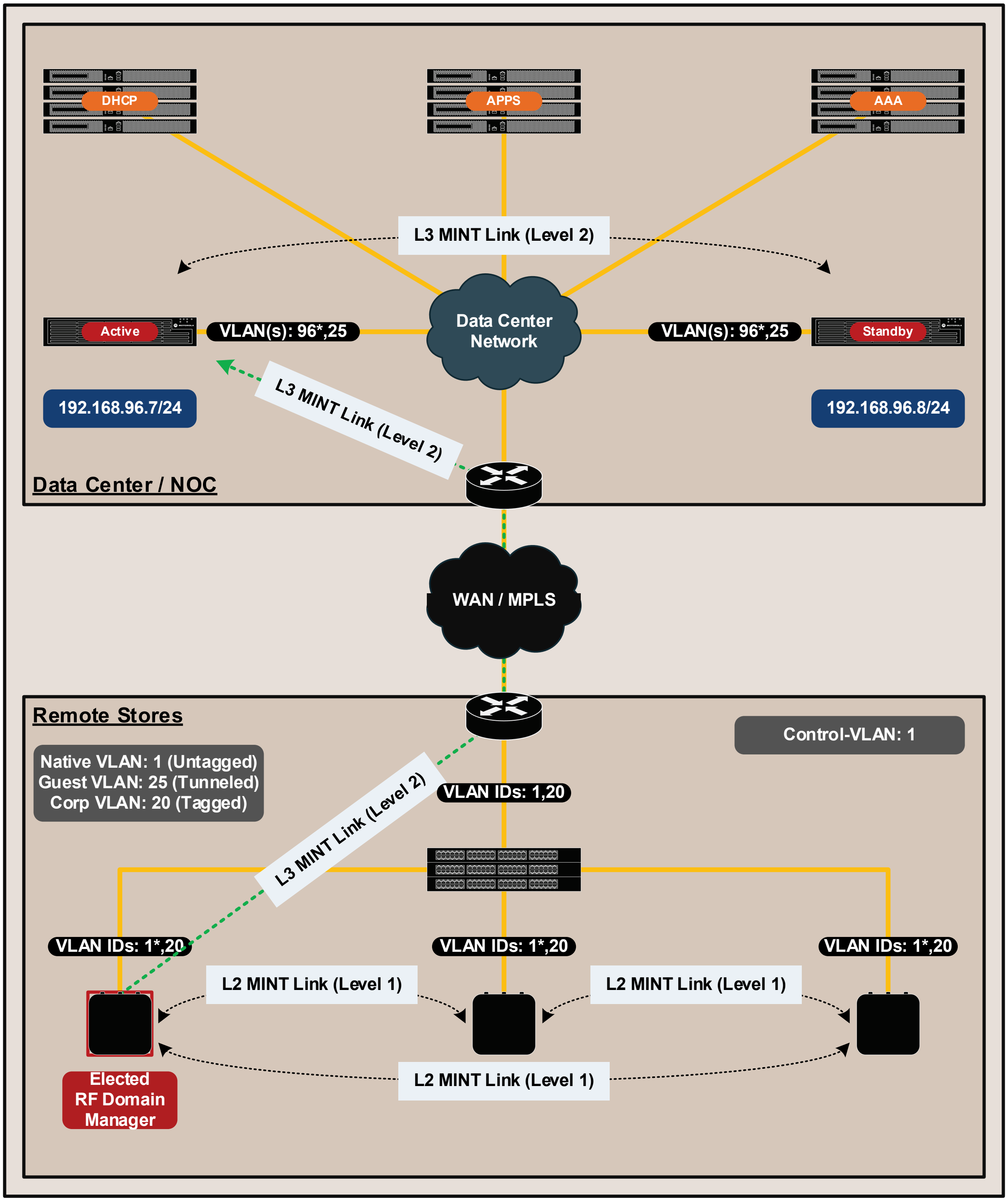
Once the Access Points at the remote site are operational, MINT communications between the data center and remote Access Points occurs through the elected RF Domain Manager for the site. The remote Access Points are managed as if they were connected to the Wireless Controllers over Level 1 MINT links.

Configuration

This section provides the necessary configuration steps required to provision a cluster of Wireless Controllers in a data center to support remote Access Point deployments. In the following configuration example two NX 9610 Wireless Controllers will be configured in the data center as an Active / Standby cluster supporting two remote sites (Store100 and Store101). As the VLANs are common within the data center and each remote site, one user defined Profile will be required for the Wireless Controllers and the remote Access Points:

- One user defined RF Domain will be defined for the data center and each remote site.
- Separate user defined Management Policies will be defined and assigned to the Wireless Controllers in the data center and remote Access Points.
- Common configuration parameters and policies will be assigned to the NX 9610 Wireless Controllers in the data center and remote Access Points using user defined Profiles.
- One 802.11i Wireless LANs for corporate assets will be defined and assigned to AP 8533 Access Point radios using the anyap Profile.
- One Guest Wireless LAN will be defined and assigned to AP radios using AP Profile. Guest user traffic will be tunneled back to the NX9610 controller via Level 2 MINT.
- Static IP addressing and cluster configuration will be assigned to each of the NX 9610 Wireless Controllers as Device overrides.
- An Automatic Provisioning Policy will be defined and assigned to the NX 9610 user defined profile.

Configuration examples will be provided for both CLI and the Web UI Management Interface.



Note

For this configuration example two NX9510 Controllers and AP 8533 Access Points are used. It is important to note that these configuration steps are applicable to other VX / NX series Wireless Controllers as well as other WING5 Access Points.

Configuration – RF Domains

RF Domains allow administrators to assign regional and regulatory, RF and WIPS configuration to devices deployed in a common coverage area such as a remote branch site. Each RF Domain contains mandatory regulatory configuration parameters and optional contact, WIPS and SMART RF configuration.

RF Domains also provide the ability to allow administrators to override certain parameters using a concept of Aliases, as well as directly override Wireless LAN SSID names / PSK values / VLAN assignments for Access Points assigned to the RF Domain. This allows enterprises to deploy common Wireless LANs and Policies across multiple sites while permitting unique parameters for each site.

One RF Domain can be assigned per Wireless Controller and Access Point and by default all devices are assigned to an RF Domain named default. For this configuration example the Wireless Controllers in the data center and the Access Points at each remote site will be assigned to a unique user defined RF Domain. Each user defined RF Domain will define regional and regulatory information as well as location specific parameters.

In addition, the RF Domains for each remote site will include a Control VLAN parameter which will allow the remote Access Points at each site to discover themselves over their Native VLAN and form Level 1 VLAN based MINT links between themselves. For AP-only remote sites the Control VLAN is necessary so that an RF Domain manager can be elected for each site. The RF Domain manager is responsible for aggregating statistics, performing SMART RF calculations and may distribute firmware images for the site. The RF Domain Manager for each remote site is automatically elected, however you can optionally determine which Access Point will become the RF Domain Manager for a site by assigning an RF Domain Manager priority value of 255 as an Override to a specific Access Point. For remote sites with site controllers no Control VLAN is required, as one of the site controllers will automatically become the RF Domain Manager, while local Access Points will adopt to site controllers using Level 1 VLAN or IP based links.

For this configuration step three user defined RF Domains will be created with the following parameters:

1. A user defined RF Domain named noc will be created for the Wireless Controllers in the data center with the following parameters:
    a. The **Country Code** will be set to **DE**
    b. The **Location** will be set to **Frankfurt**
    c. The **Time Zone** will be set to **CET**
2. A user defined RF Domain named store100 will be created for the Access Points in store 100 with the following parameters:
    a. The **Country Code** will be set to **GB**
    b. The **Location** will be set to **London**
    c. The Time Zone will be set to Europe/London
    d. The **Control VLAN** will be set to **1**.
3. A user defined RF Domain named **store101** will be created for the Access Points in store 101 with the following parameters:
    a. The **Country Code** will be set to **CZ**
    b. The **Location** will be set to **Prague**

c. The Time Zone will be set to CET

d. The Control VLAN will be set to 1.

The user defined RF Domain named noc will be manually assigned to each Wireless Controller in the data center using Device configuration. The RF Domains named store100 and store101 will be automatically assigned to Access Points deployed in both sites using Automatic Provisioning Policies.

Note

One unique RF Domain is required per remote site.

Note

The Control VLAN ID must be set to a VLAN ID that is common between all the Access Points at the remote site. In most cases this will be the untagged Native VLAN id the Access Points use to communicate with the Wireless Controllers in the data center.

Note

You can pre-select a specific Access Point as RF Domain Manager for a site by issuing the **rf-domain-manager priority** command as a device Override and assigning a priority value of **255**.

RF Domain Configuration – CLI

Use the following procedure to create a user defined RF Domains for the Wireless Controllers in the data center and the remote Access Points for each store using the Command Line Interface:

1. Create the user defined RF Domain for the Wireless Controllers in the data center named noc and define Country Code, Location, and Time Zone parameters:

```
nx9600-7F34C7(config)# rf-domain noc
nx9600-7F34C7(config-rf-domain-noc)# country-code de
nx9600-7F34C7(config-rf-domain-noc)# location Frankfurt
nx9600-7F34C7(config-rf-domain-noc)# timezone CET
```

2. Verify the changes:

```
nx9600-7F34C7(config-rf-domain-noc)# show context
rf-domain noc
 location Frankfurt
 contact admin@tmelabs.local
 timezone CET
 country-code de
```

3. Exit the RF Domain configuration:

```
nx9600-7F34C7(config-rf-domain-noc)# exit
```

4. Create the user defined RF Domain for the Access Points in store 100 named store100 and define Country Code, Location, Time Zone, and Control VLAN parameters:

```
nx9600-7F34C7(config)# rf-domain store100
nx9600-7F34C7(config-rf-domain-store100)# country-code gb
nx9600-7F34C7(config-rf-domain-store100)# location London
nx9600-7F34C7(config-rf-domain-store100)# timezone Europe/London
nx9600-7F34C7(config-rf-domain-store100)# control-vlan 1
```

5. Verify the changes:

```
nx9600-7F34C7(config-rf-domain-store100)# show context
rf-domain store100
 location London
 timezone Europe/London
 country-code gb
 control-vlan 1
```

6. Exit the RF Domain configuration:

```
nx9600-7F34C7(config-rf-domain-store100)# exit
```

7. Create the user defined RF Domain for the Access Points in store 101 named store101 and define Country Code, Location, Time Zone, and Control VLAN parameters:

```
nx9600-7F34C7(config)# rf-domain store101
nx9600-7F34C7(config-rf-domain-store101)# country-code cz
nx9600-7F34C7(config-rf-domain-store101)# location Prague
nx9600-7F34C7(config-rf-domain-store101)# timezone CET
nx9600-7F34C7(config-rf-domain-store101)# control-vlan 1
```

8. Verify the changes:

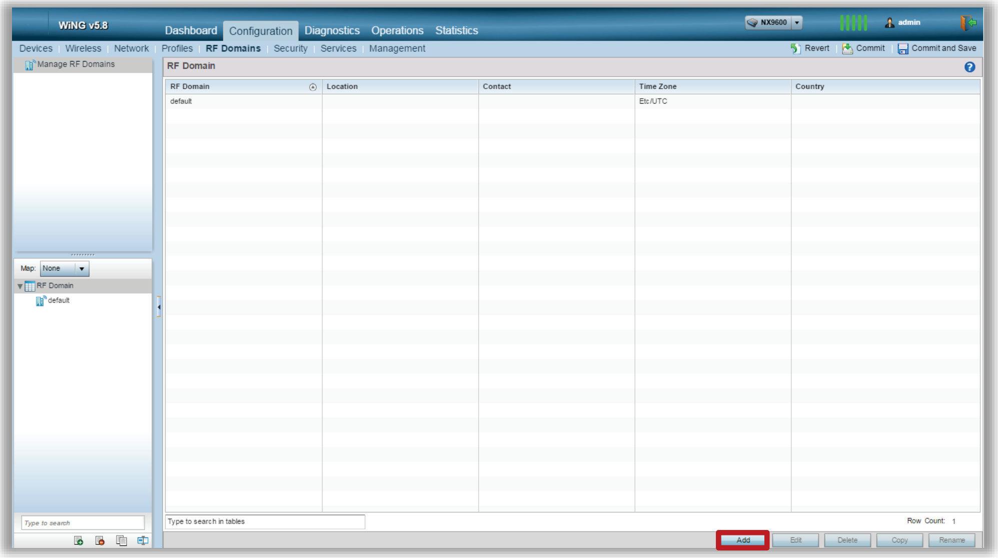
```
nx9600-7F34C7(config-rf-domain-store101)# show context
rf-domain store101
 location Prague
 timezone CET
 country-code cz
 control-vlan 1
```

9. Exit the RF Domain configuration then commit and save the changes:

```
nx9600-7F34C7(config-rf-domain-store101)# exit
nx9600-7F34C7(config)# commit write
[OK]
```

RF Domain Configuration – Web UI

1. Select Configuration -> RF Domains -> Add:

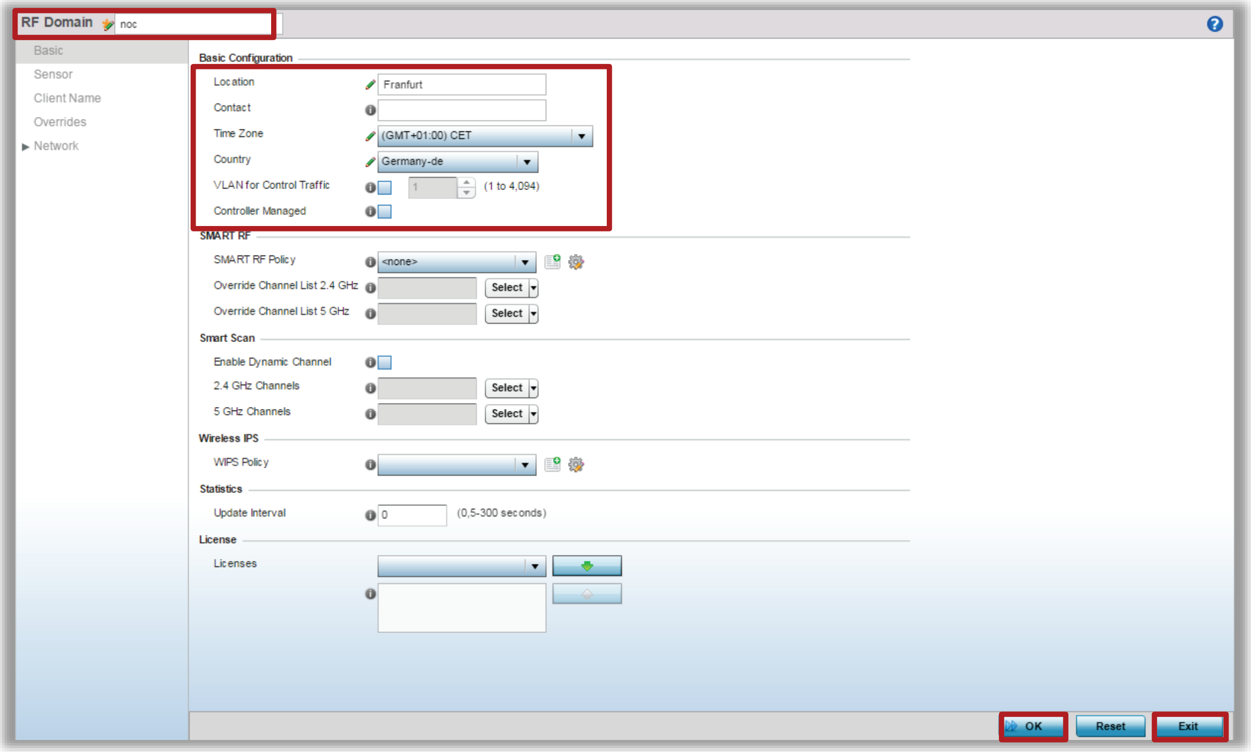


RF Domain

RF Domain	Location	Contact	Time Zone	Country
default			Etc/UTC	

Row Count: 1

2. Enter the RF Domain name noc then enter the Location information. Select a Time Zone and Country Code then click OK and Exit:



RF Domain noc

Basic Configuration

Location: Franfurt
Contact:
Time Zone: (GMT+01:00) CET
Country: Germany-de
VLAN for Control Traffic: □ 1 (1 to 4,094)
Controller Managed: □

SMART RF

SMART RF Policy: <none>
Override Channel List 2.4 GHz: Select
Override Channel List 5 GHz: Select

Smart Scan

Enable Dynamic Channel: □
2.4 GHz Channels: Select
5 GHz Channels: Select

Wireless IPS

WIPS Policy:

Statistics

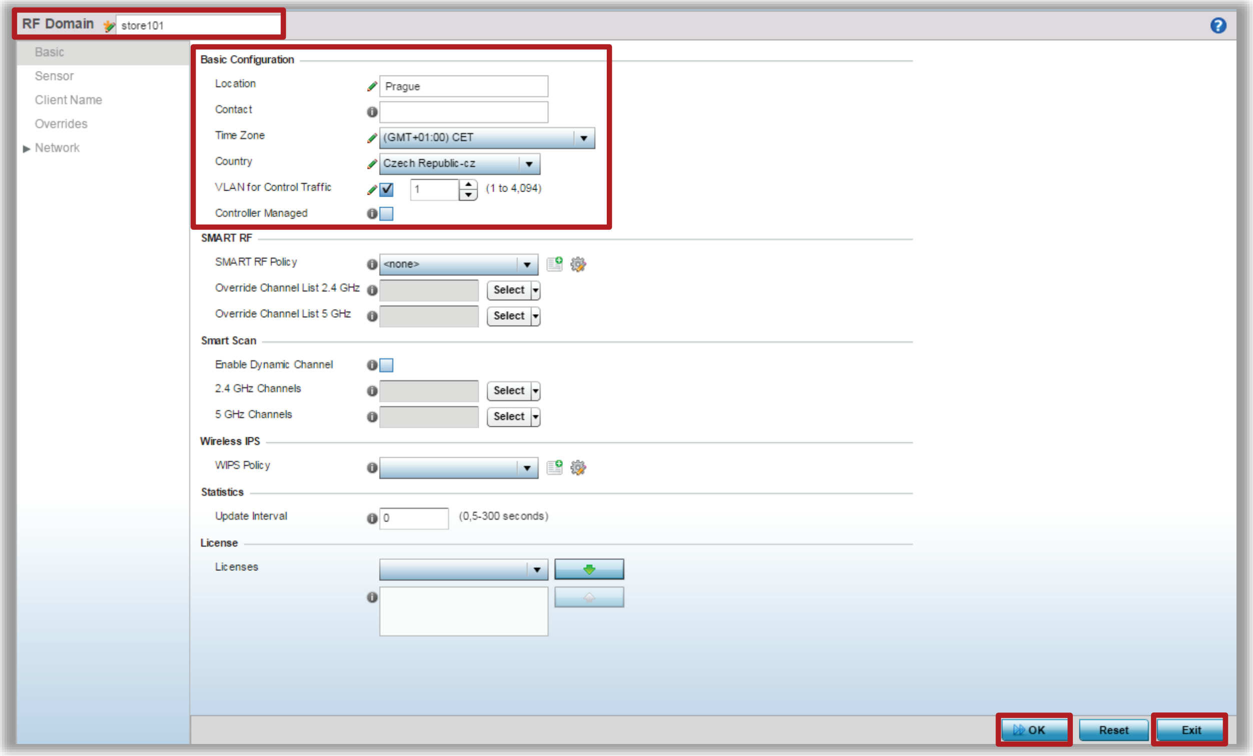
Update Interval: 0 (0,5-300 seconds)

License

Licenses:

3. Click Add to create an RF Domain for store 100. Enter the RF Domain name store100 then enter the Location, and Control VLAN information. Select a Time Zone and Country Code then click OK and Exit. Note in this example the Control VLAN is set to the Access Points untagged Native VLAN ID 1:

4. Click Add to create an RF Domain for store 101. Enter the RF Domain name store101 then enter the Location, and Control VLAN information. Select a Time Zone and Country Code then click OK and Exit. Note in this example the Control VLAN is set to the Access Points untagged Native VLAN ID 1:



RF Domain store101

Basic Configuration

Location: Prague
Contact:
Time Zone: (GMT+01:00) CET
Country: Czech Republic-cz
VLAN for Control Traffic: ☑ 1 (1 to 4,094)
Controller Managed: □

SMART RF

SMART RF Policy: <none>
Override Channel List 2.4 GHz: Select
Override Channel List 5 GHz: Select

Smart Scan

Enable Dynamic Channel: □
2.4 GHz Channels: Select
5 GHz Channels: Select

Wireless IPS

WIPS Policy:

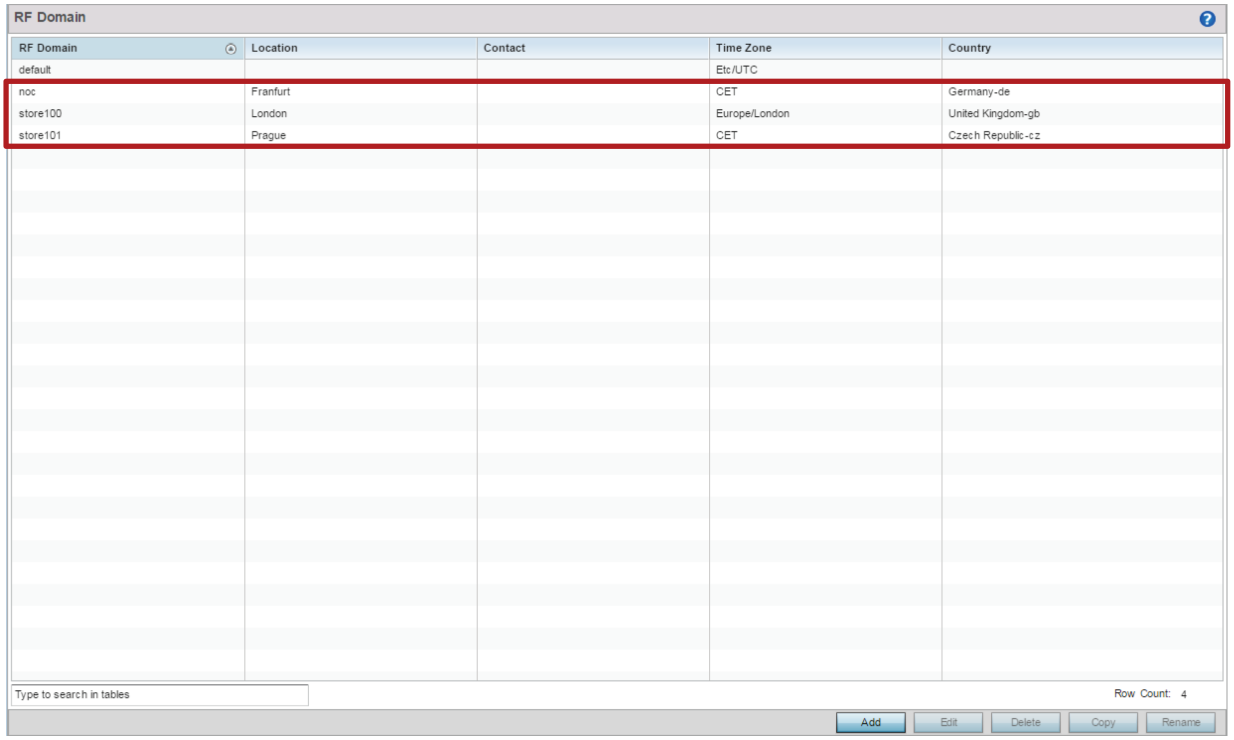
Statistics

Update Interval: 0 (0,5-300 seconds)

License

Licenses:

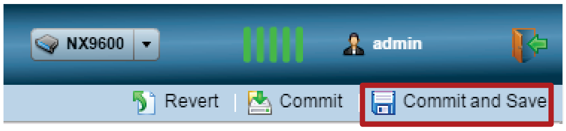
5. User defined RF Domains named noc, store100 and store101 have now been defined:



RF Domain

RF Domain	Location	Contact	Time Zone	Country
default			Etc/UTC	
noc	Franfurt		CET	Germany-de
store100	London		Europe/London	United Kingdom-gb
store101	Prague		CET	Czech Republic-cz

6. Commit then Save the changes:



Configuration Management Policies

Management Policies control administrative access and permissions into WING 5 devices as well as control which management interfaces are enabled. Management Policies can be assigned to groups of devices using Profiles or to individual devices as Overrides.

Device administrators can be authenticated locally by the WING 5 device or centrally on a RADIUS or TACACS+ server. Local authentication requires a username and password in addition to the user's role and access permissions. Remote authentication requires return attributes for the role and access permissions to be provided to the WING 5 device so that the appropriate access is provided to the user.

By default, all devices are automatically assigned to a Management Policy named default. For this configuration example the Wireless Controllers and remote Access Points will be assigned to different Management policies. Depending on the management strategy a single Management Policy can be utilized to manage all the Wireless Controllers or Access Points in the network or separate Management Policies can be deployed for the Wireless Controllers and Access Points. Management Policies may also be defined and assigned for Access Points at each remote site.

For this configuration step two user defined Management Policies will be created with the following parameters:

1. A user defined Management Policy named controllers will be created to manage the Wireless Controllers in the data center with the following parameters:
    a. An administrative user account *admin* with the password *wingsecure* will be created and assigned to the superuser role with permissions to access all management interfaces.
    b. HTTP will be disabled by default, while HTTPS and SSHv2 secure management interfaces will be enabled.
2. A user defined Management Policy named aps will be created to manage all the remote Access Points with the following parameters:
    a. An administrative user account admin with the password wingsecure will be created and assigned to the superuser role with permissions to access the SSHv2 management interface.
    b. HTTPS should be disabled and only the SSHv2 secure management interface will be enabled.
    c. SNMP will be disabled to eliminate ADSP and other management services from directly communicating with the Access Point. SNMP stats can be obtained by querying the Controllers.

The user defined Management Policies will be assigned to the Wireless Controllers and remote Access Points using user defined device Profiles:

Note

As AP 8533 Access Points will be managed by the controller, HTTP management interface will be disabled on Management Policy assigned to the Access Points.

Management Policies – CLI

1. Create the Management Policy for the Wireless Controllers named controllers and define a admin user account and password with an assigned role and access permissions:

```
nx9600-7F34C7(config)# management-policy controllers
nx9600-7F34C7(config-management-policy-controllers)# user admin password wingsecure role superuser access
all
```

2. Verify the changes:

```
nx9600-7F34C7(config-management-policy-controllers)# show context
management-policy controllers
 no telnet
 no http server
 https server
 ssh
 user admin password 1 <encrypted string> role superuser access all
```

3. Exit the Management Policy configuration:

```
nx9600-7F34C7(config-management-policy-controllers)# exit
```

4. Create the user defined Management Policy for all the remote Access Points named stores and define a admin user account and password with an assigned role and access permissions. In addition, disable HTTP, SNMP and enable the secure SSHv2 management interface:

```
nx9600-7F34C7(config)# management-policy aps
nx9600-7F34C7(config-management-policy-aps)# user admin password wingsecure role superuser access all
nx9600-7F34C7(config-management-policy-aps)# no https server
nx9600-7F34C7(config-management-policy-aps)# no snmp-server manager all
```

5. Verify the changes:

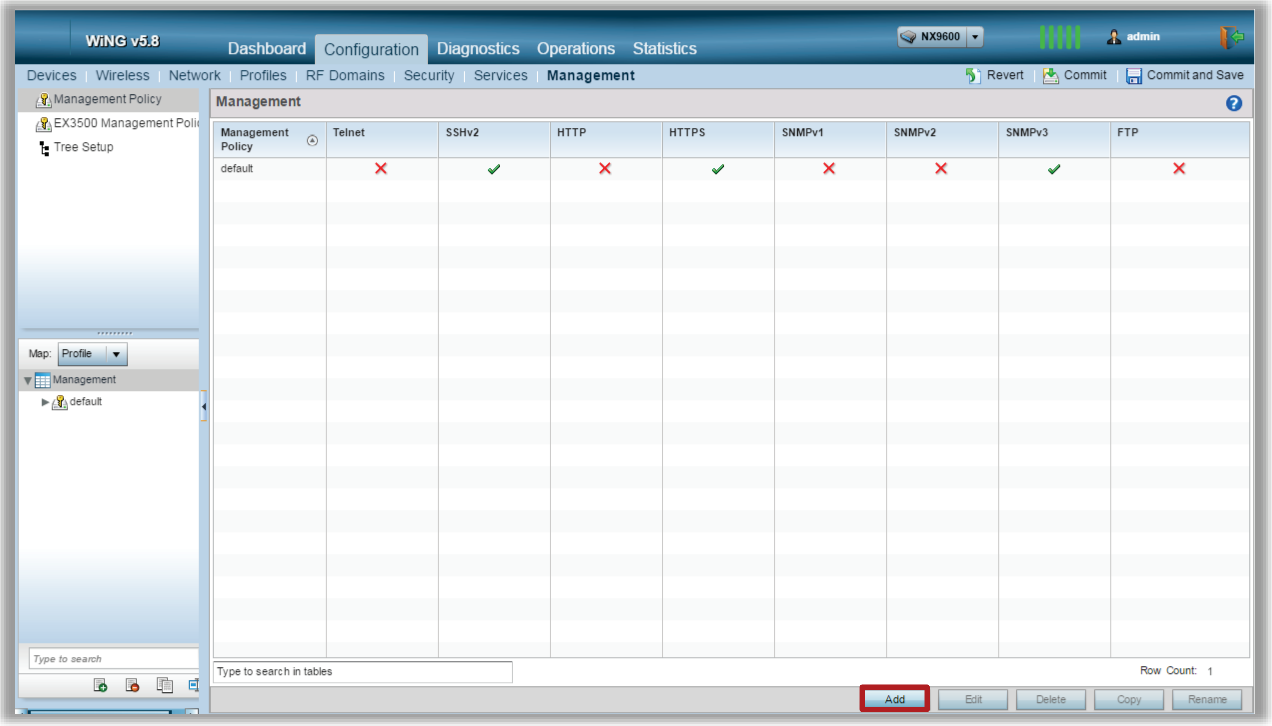
```
nx9600-7F34C7(config-management-policy-stores)# show context
management-policy stores
 no http server
 ssh
 user admin password 1 <encrypted-string> role superuser access all
 no snmp-server manager v3
```

6. Exit the Management Policy configuration then commit and save the changes:

```
nx9600-7F34C7(config-management-policy-aps)# exit
nx9600-7F34C7(config)# commit write
[OK]
```

Management Policies – Web UI

1. Select Configuration -> Management -> Add.

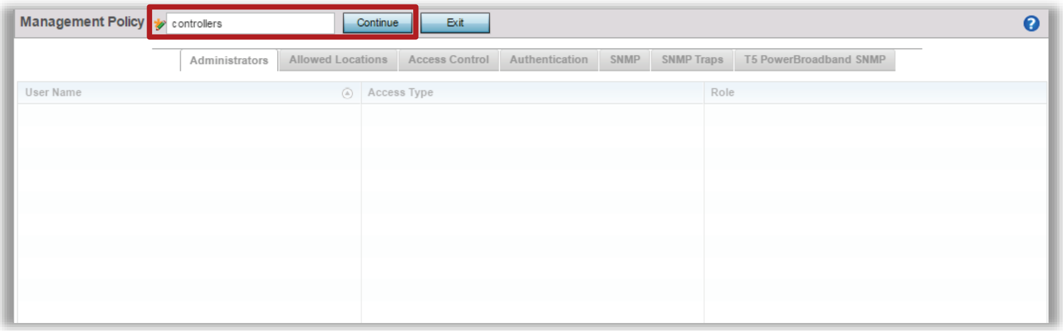


Management

Management Policy	Telnet	SSHv2	HTTP	HTTPS	SNMPv1	SNMPv2	SNMPv3	FTP
default	✗	✓	✗	✓	✗	✗	✓	✗

Row Count: 1

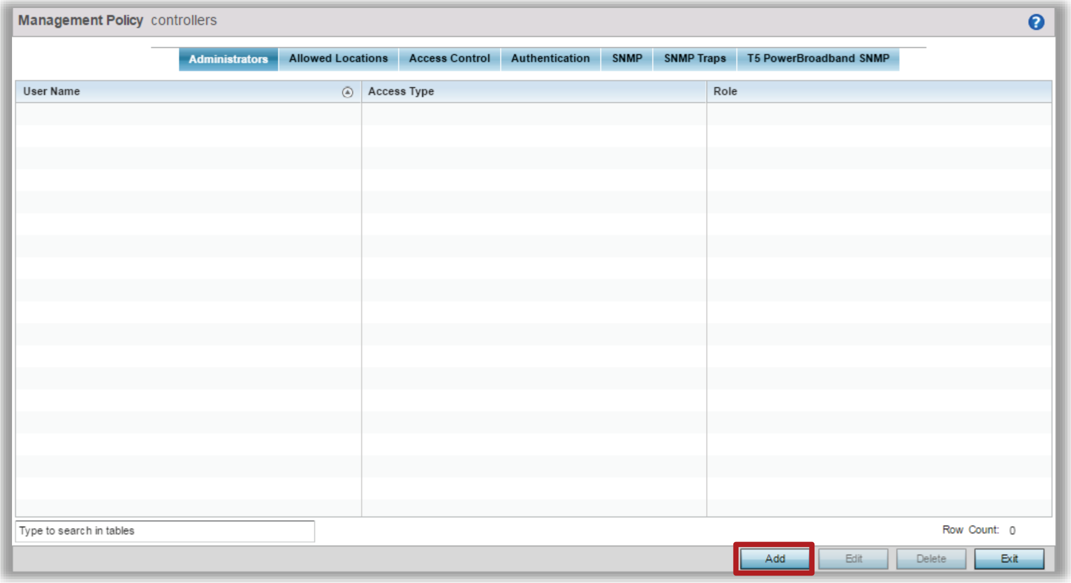
2. Enter the Management Policy name noc then click Continue.



Management Policy: controllers

User Name	Access Type	Role

3. Select Administrators -> Add.

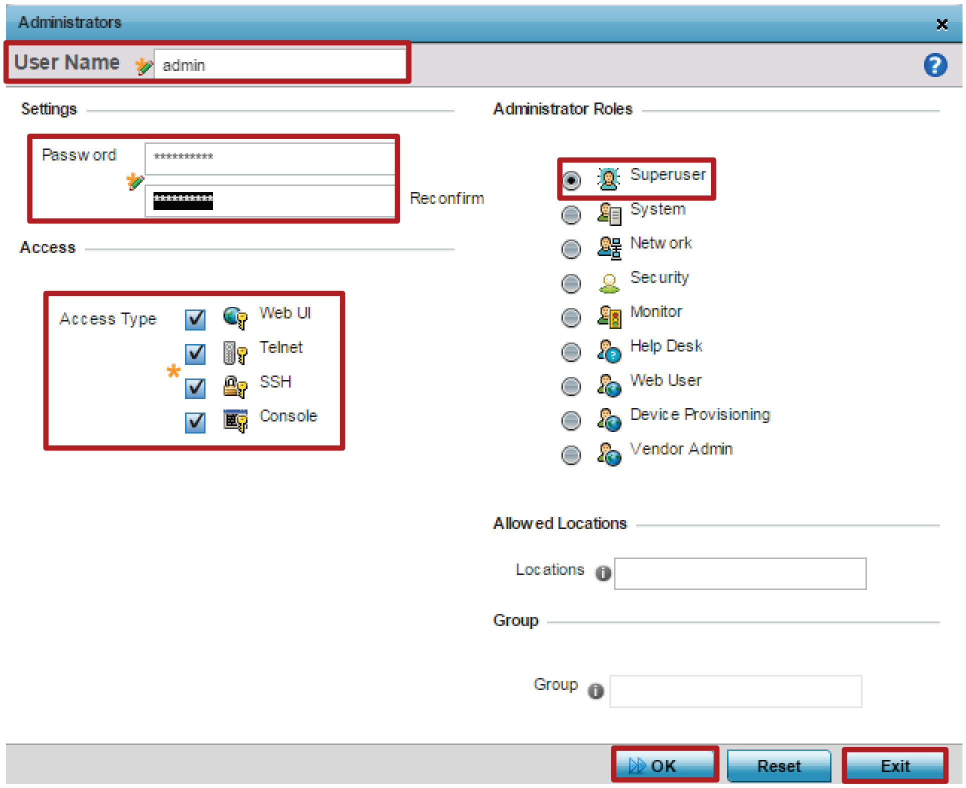


Management Policy controllers

User Name	Access Type	Role

Row Count: 0

4. Enter an admin User Name and Password then select Role named Superuser. Enable All the Access Types then click OK and Exit.



Administrators

User Name: admin

Settings

Password: **********
Reconfirm: **********

Access

Access Type: ☑ Web UI ☑ Telnet ☑ SSH ☑ Console

Administrator Roles

● Superuser
○ System
○ Network
○ Security
○ Monitor
○ Help Desk
○ Web User
○ Device Provisioning
○ Vendor Admin

Allowed Locations

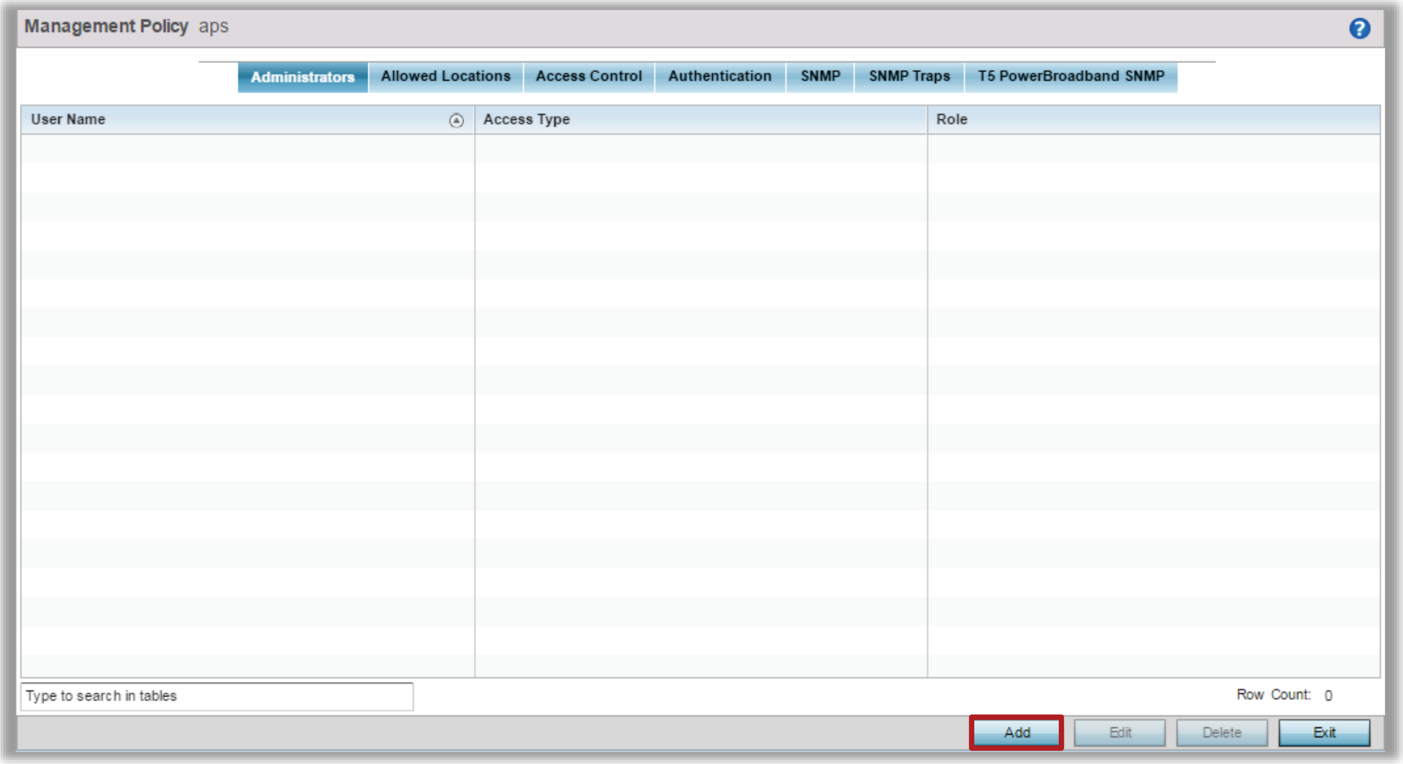
Locations:

Group

Group:

5. Click Add to create a user defined Management Policy for the remote Access Points. Enter the Management Policy name aps then click Continue.

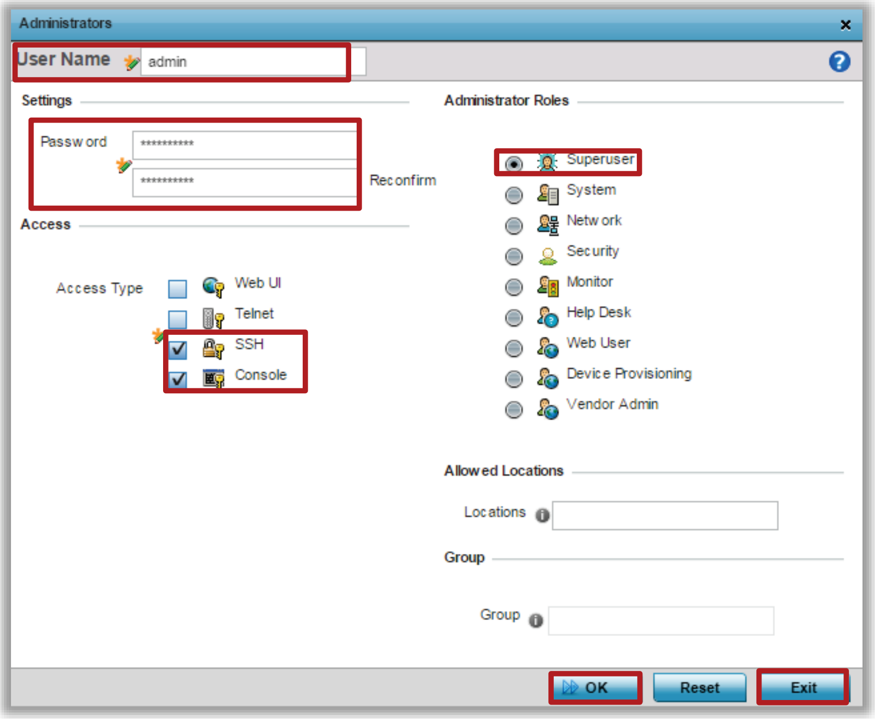
6. Select Administrators -> Add.



User Name	Access Type	Role

Row Count: 0

7. Enter an admin User Name and Password then select Role named Superuser. Under Access Types select SSH and Console then click OK and Exit.



User Name: admin

Password: **********

Reconfirm: **********

Access Type:
- ☐ Web UI
- ☐ Telnet
- ☑ SSH
- ☑ Console

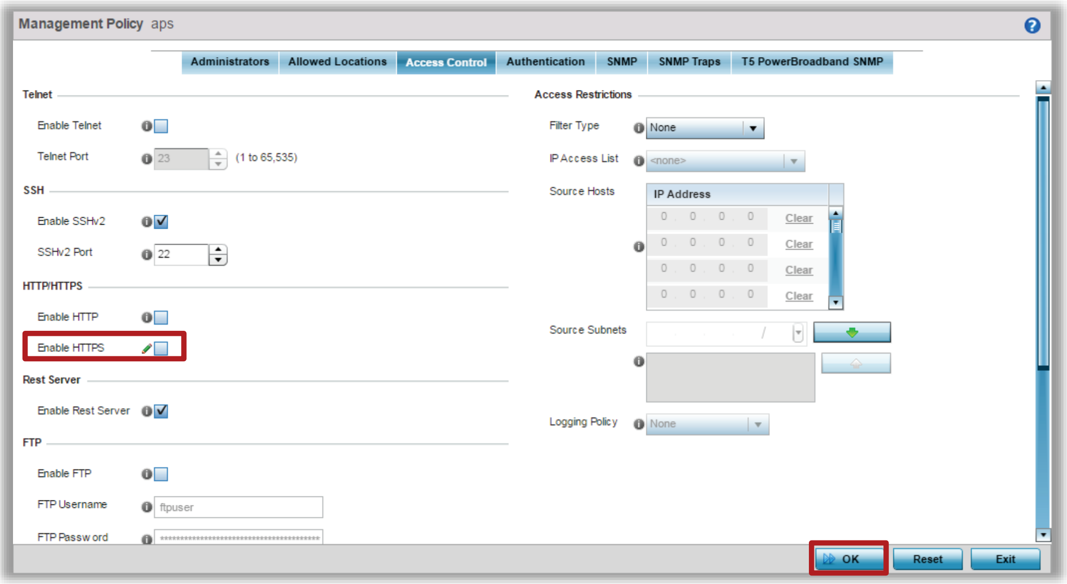
Administrator Roles:
- ● Superuser
- ○ System
- ○ Network
- ○ Security
- ○ Monitor
- ○ Help Desk
- ○ Web User
- ○ Device Provisioning
- ○ Vendor Admin

Locations:

Group

Group:

8. Select the Access Control tab. Disable HTTPS. Click OK.



Management Policy aps

Telnet

- Enable Telnet □
- Telnet Port 23 (1 to 65,535)

SSH

- Enable SSHv2 ☑
- SSHv2 Port 22

HTTP/HTTPS

- Enable HTTP □
- Enable HTTPS □

Rest Server

- Enable Rest Server ☑

FTP

- Enable FTP □
- FTP Username ftpuser
- FTP Password **

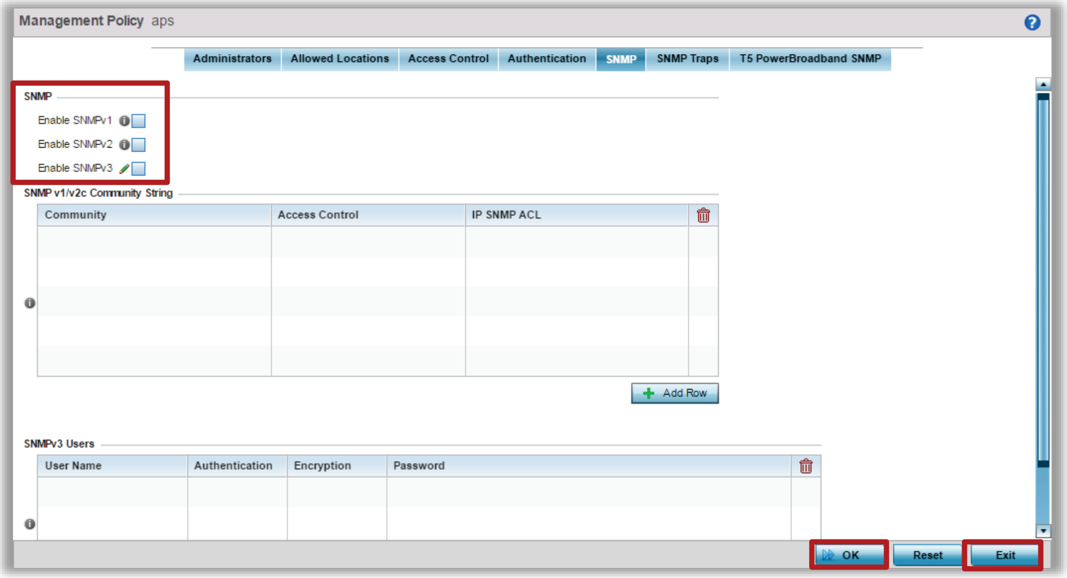
Access Restrictions

- Filter Type None
- IP Access List <none>
- Source Hosts

IP Address
0 0 0 0
0 0 0 0
0 0 0 0
0 0 0 0

- Source Subnets
- Logging Policy None

9. Select the SNMP tab then disable each SNMP service. Click OK then Exit.



Management Policy aps

SNMP

- Enable SNMPv1 □
- Enable SNMPv2 □
- Enable SNMPv3 □

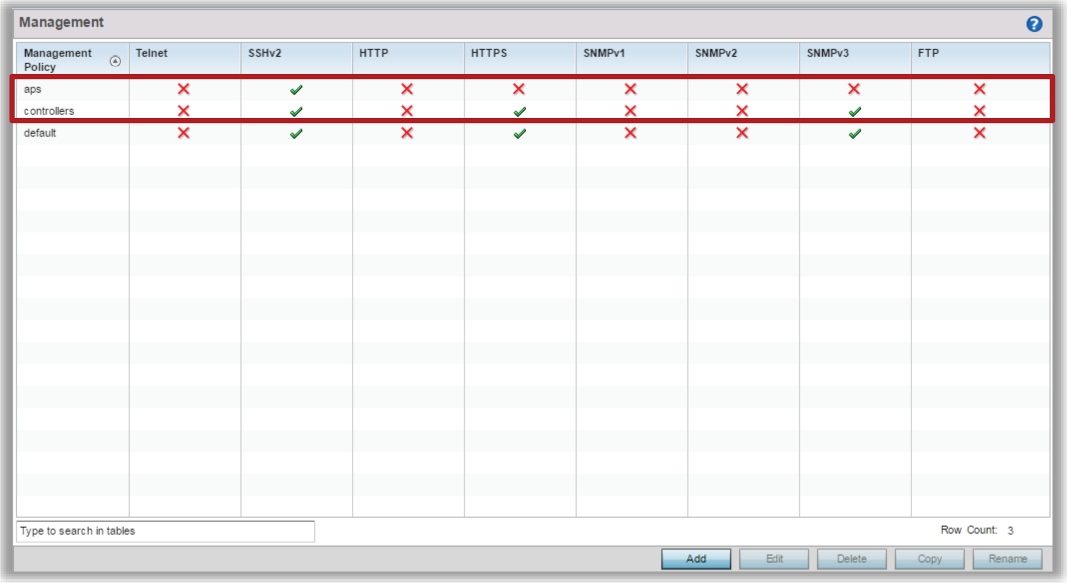
SNMP v1/v2c Community String

Community	Access Control	IP SNMP ACL

SNMPv3 Users

User Name	Authentication	Encryption	Password

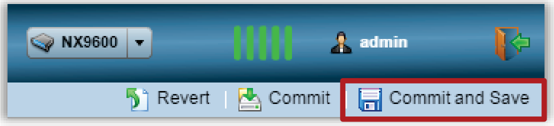
10. User defined Management Policies named controllers and aps have now been defined.



Management

Management Policy	Telnet	SSHv2	HTTP	HTTPS	SNMPv1	SNMPv2	SNMPv3	FTP
aps	✗	✓	✗	✗	✗	✗	✗	✗
controllers	✗	✓	✗	✓	✗	✗	✓	✗
default	✗	✓	✗	✓	✗	✗	✓	✗

11. Commit then Save the changes.



Wireless LANs

Wireless LANs are defined individually within a WING 5 system and can be assigned to groups of Access Point radios using Profiles or to individual Access Point radios as Overrides. Wireless LAN specific parameters such as SSID names and VLAN IDs may also be overridden using Overrides assigned to a RF Domain.

Each Wireless LAN consists of policies and configuration parameters which define the basic operating parameters for the Wireless LAN as well as authentication, encryption, QoS and firewall options. Changes made to a Wireless LANs configuration or assigned policy are automatically inherited by all Access Points serving the Wireless LAN.

No Wireless LANs are pre-defined by default in WING 5.X unless they are created using the Initial Configuration Wizard when first initializing a Wireless Controller or Access Point. Wireless LANs can be assigned to groups of Access Point radios using Profiles or to individual Access Point radios as Overrides. Wireless LANs assigned directly to radios as Overrides will supersede any Wireless LANs inherited from a Profile.

In most deployments each remote sites will be servicing the same Wireless LANs allowing the AP 6532 user defined Profile to be utilized to assign the Wireless LANs to groups of radios. For deployments where the SSID name or VLAN assignments need to be unique per site, the RF Domain assigned to each site can be provisioned to override the SSID name and/or VLAN assignments for Wireless LANs deployed at that site.

For this configuration step two 802.11i Wireless LANs will be created with the following parameters:

1. An AAA Policy named external-aaa will be created using centralized AAA servers deployed in the data center.
2. An 802.11i EAP Wireless LAN named STORES-DOT1X will be created with the following parameters:
    a. EAP authentication with CCMP encryption will be enabled.
    b. The AAA Policy named external-aaa assigned.
    c. Local bridging will be enabled and users assigned to the store VLAN 20.
3. A Guest Wireless LAN named STORES-GUEST with simple device registration be created with the following parameters:
    a. Open authentication with no encryption.
    b. Captive Portal that enables device registration via form.
    c. Tunnel mode will be enabled and users assigned to the extended VLAN 25 terminating on the centralized controllers.

The Wireless LANs named STORES-DOT1X and STORES-GUEST will be assigned to the AP 8533 Access Point radios using the user defined anyap Profile named STORES-AP.

Wireless LANs – CLI

1. Create a AAA policy named external-aaa for the 802.11i EAP Wireless LAN:

```
nx9600-7F34C7(config)# aaa-policy EXTERNAL-AAA
```

2. Create one or more Authentication server entries. In this example centralized Authentication servers 192.168.10.10 and 192.168.10.11 using no proxy have been defined:

```
nx9600-7F34C7(config-aaa-policy-EXTERNAL-AAA)# authentication server 1 host tme-dc-1.wing.com secret
wingsecure
nx9600-7F34C7(config-aaa-policy-EXTERNAL-AAA)# authentication server 2 host tme-dc-2.wing.com secret
wingsecure
```

3. Verify the changes:

```
nx9600-7F34C7(config-aaa-policy-EXTERNAL-AAA)# show context
aaa-policy EXTERNAL-AAA
 authentication server 1 host tme-dc-1.wing.com secret 0 wingsecure
 authentication server 2 host tme-dc-2.wing.com secret 0 wingsecure
```

4. Exit the AAA Policy configuration:

```
nx9600-7F34C7(config-aaa-policy-external-aaa)# exit
```

5. Create an 802.11i EAP Wireless LAN. In this example the 802.11i EAP Wireless LAN will be named STORES-DOT1X:

```
nx9600-7F34C7(config)# wlan STORES-DOT1X
```

6. Set the Encryption to CCMP, Authentication to EAP then assign the AAA Server Policy named external-aaa. Enable local bridging then assign the local VLAN 22:

```
nx9600-7F34C7(config-wlan-STORES-DOT1X)# encryption-type ccmp
nx9600-7F34C7(config-wlan-STORES-DOT1X)# authentication-type eap
nx9600-7F34C7(config-wlan-STORES-DOT1X)# use aaa-policy EXTERNAL-AAA
nx9600-7F34C7(config-wlan-STORES-DOT1X)# bridging-mode local
nx9600-7F34C7(config-wlan-STORES-DOT1X)# vlan 20
```

7. Verify the changes:

```
nx9600-7F34C7(config-wlan-STORES-DOT1X)# show context
wlan STORES-DOT1X
 ssid STORES-DOT1X
 vlan 20
 bridging-mode local
 encryption-type ccmp
 authentication-type eap
 use aaa-policy external-aaa
```

8. Exit the Wireless LAN configuration:

```
nx9600-7F34C7(config-wlan-STORES-DOT1X)# exit
```

9. Create AAA Policy to point to the centralized controllers for Guest User MAC authentication

```
nx9600-7F34C7(config)# aaa-policy ONBOARD-AAA
nx9600-7F34C7(config-aaa-policy-ONBOARD-AAA)# authentication server 1 onboard centralized-controller
```

10. Verify the changes:

```
nx9600-7F34C7(config-aaa-policy-ONBOARD-AAA)# show context
aaa-policy external-aaa
 authentication server 1 onboard centralized-controller
```

11. Exit the AAA Policy configuration:

```
nx9600-7F34C7(config-aaa-policy-ONBOARD-AAA)# exit
```

12. Create a RADIUS Group for the registered Guest Users

```
nx9600-7F34C7(config)# radius-group GUESTS
nx9600-7F34C7(config-radius-group-GUESTS)# guest
nx9600-7F34C7(config-radius-group-GUESTS)# exit
```

13. Create a RADIUS Server policy to enabled onboard RADIUS server on the centralized controllers

```
nx9600-7F34C7(config)# radius-server-policy ONBOARD-RADIUS
nx9600-7F34C7(config-radius-server-policy-ONBOARD-RADIUS)# exit
```

14. Create a Captive Portal Policy for the Guest Users to allow simple registration using a HTML form

```
nx9600-7F34C7(config)# captive-portal REGISTRATION
nx9600-7F34C7(config-captive-portal-REGISTRATION)# access-type registration
nx9600-7F34C7(config-captive-portal-REGISTRATION)# use aaa-policy ONBOARD-AAA
nx9600-7F34C7(config-captive-portal-REGISTRATION)# exit
```

15. Create a Guest Wireless LAN. In this example the Guest Wireless LAN will be named STORES-GUESTS:

```
nx9600-7F34C7(config)# wlan STORES-GUESTS
```

16. Set the Authentication to MAC then assign a AAA Policy. Also assign Captive Portal policy and enable Captive Portal Enforcement. Enable tunnel mode then assign the extended VLAN 25. Enable Device Registration:

```
nx9600-7F34C7(config-wlan-STORES-GUESTS)# use aaa-policy ONBOARD-AAA
nx9600-7F34C7(config-wlan-STORES-GUESTS)# authentication-type mac
nx9600-7F34C7(config-wlan-STORES-GUESTS)# captive-portal-enforcement fall-back
nx9600-7F34C7(config-wlan-STORES-GUESTS)# use captive-portal REGISTRATION
nx9600-7F34C7(config-wlan-STORES-GUESTS)# bridging-mode tunnel
nx9600-7F34C7(config-wlan-STORES-GUESTS)# vlan 25
nx9600-7F34C7(config-wlan-STORES-GUESTS)# registration device group-name GUESTS
```

17. Verify the changes:

```
nx9600-7F34C7(config-wlan-STORES-GUESTS)# show context
wlan STORES-GUESTS
 ssid STORES-GUESTS
 vlan 25
 bridging-mode tunnel
 encryption-type none
 authentication-type mac
 use aaa-policy ONBOARD-AAA
 use captive-portal REGISTRATION
 captive-portal-enforcement fall-back
 registration device group-name GUESTS expiry-time 4320
```

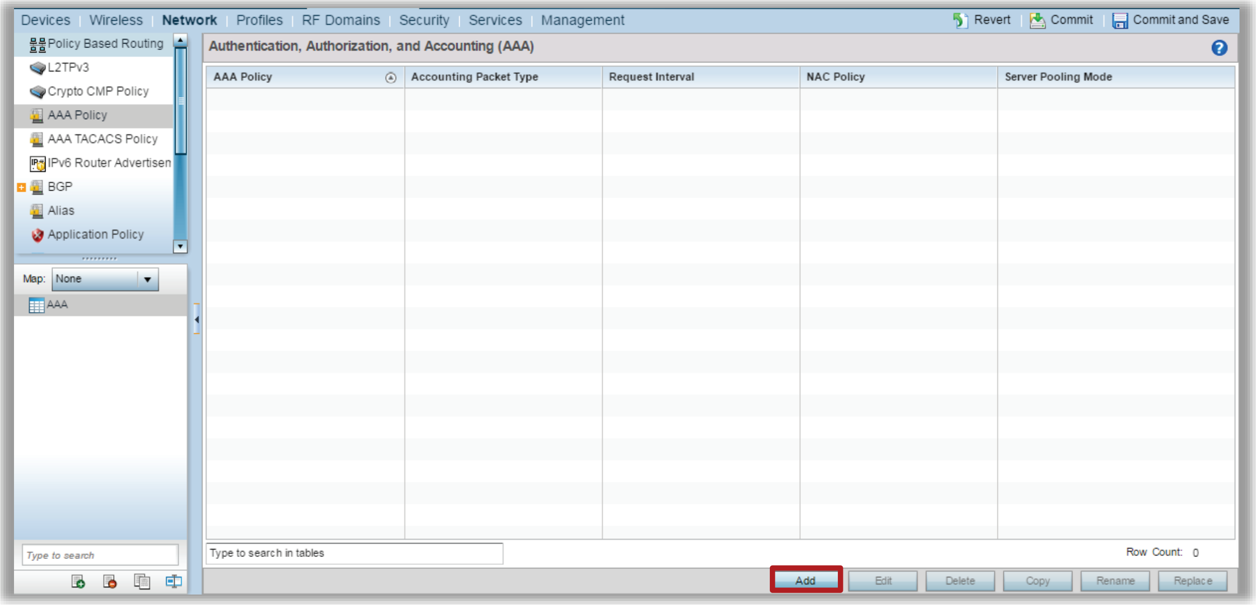
18. Exit the Wireless LAN configuration then commit and save the changes:

```
nx9600-7F34C7(config-wlan-STORES-GUESTS)# exit
nx9600-7F34C7(config)# commit write
[OK]
```

Management User Interface

Use the following procedure to create 802.11i Wireless LANs for each store using the Management User Interface:

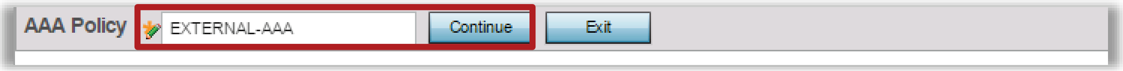
1. Select Configuration -> Wireless -> AAA Policy -> Add.



Authentication, Authorization, and Accounting (AAA)

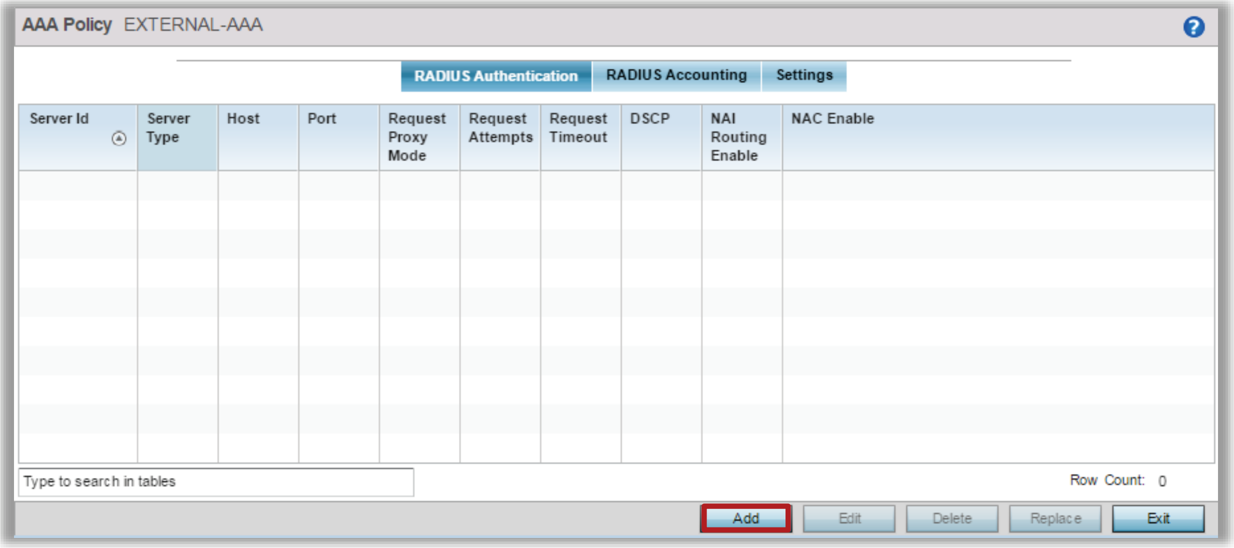
AAA Policy	Accounting Packet Type	Request Interval	NAC Policy	Server Pooling Mode

2. Enter the Management Policy name EXTERNAL-AAA then click Continue.



AAA Policy EXTERNAL-AAA

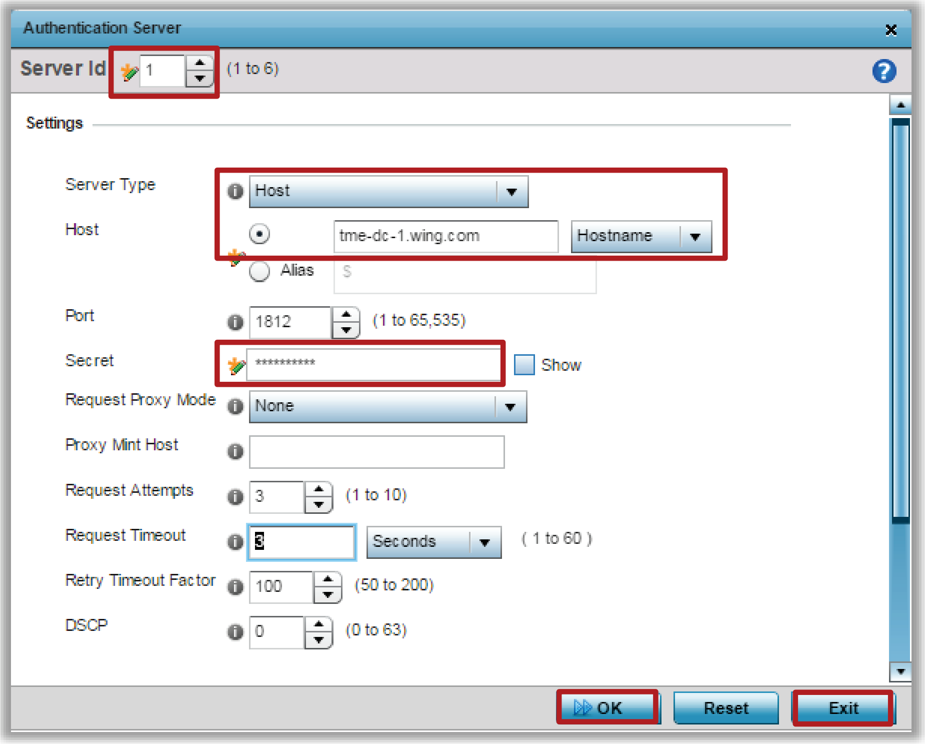
3. Select RADIUS Authentication -> Add.



AAA Policy EXTERNAL-AAA

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable

4. Set the Server Id to 1 then enter the IP Address or Hostname of the primary AAA server. Set the Server Type to Host then enter the RADIUS Shared Secret then click OK and Exit.



Server Id 1 (1 to 6)

Settings

Server Type: Host

Host: ● tme-dc-1.wing.com Hostname

○ Alias $

Port: 1812 (1 to 65,535)

Secret: ********** □ Show

Request Proxy Mode: None

Proxy Mint Host:

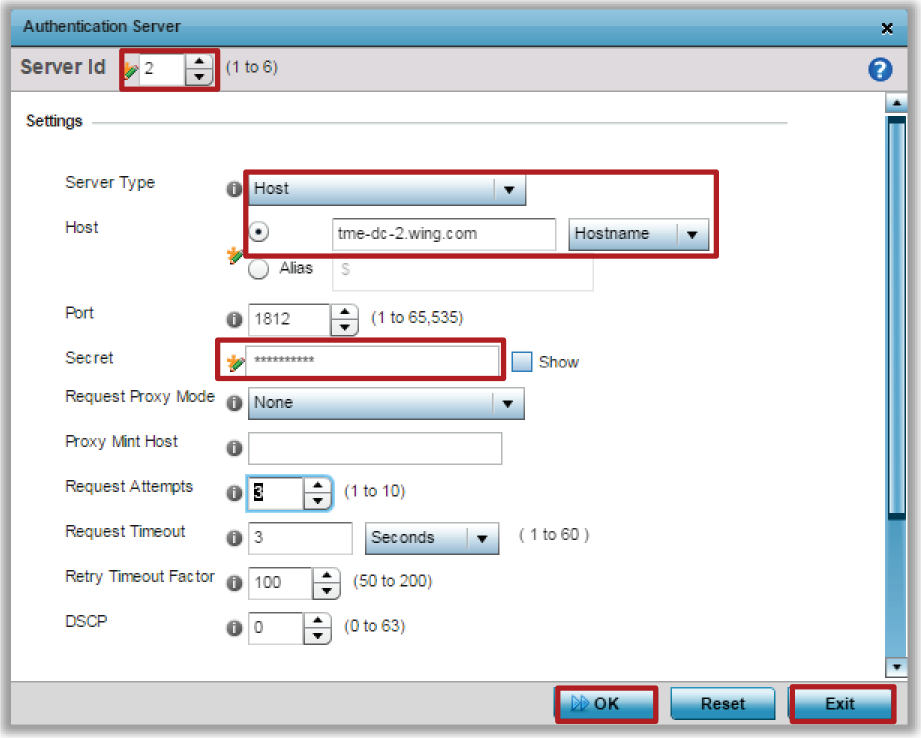
Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

5. Click Add. Set the Server Id to 2 then enter the IP Address or Hostname of the secondary AAA server. Set the Server Type to Host then enter the RADIUS Shared Secret then click OK and Exit.



Server Id 2 (1 to 6)

Settings

Server Type: Host

Host: ● tme-dc-2.wing.com Hostname

○ Alias $

Port: 1812 (1 to 65,535)

Secret: ********** □ Show

Request Proxy Mode: None

Proxy Mint Host:

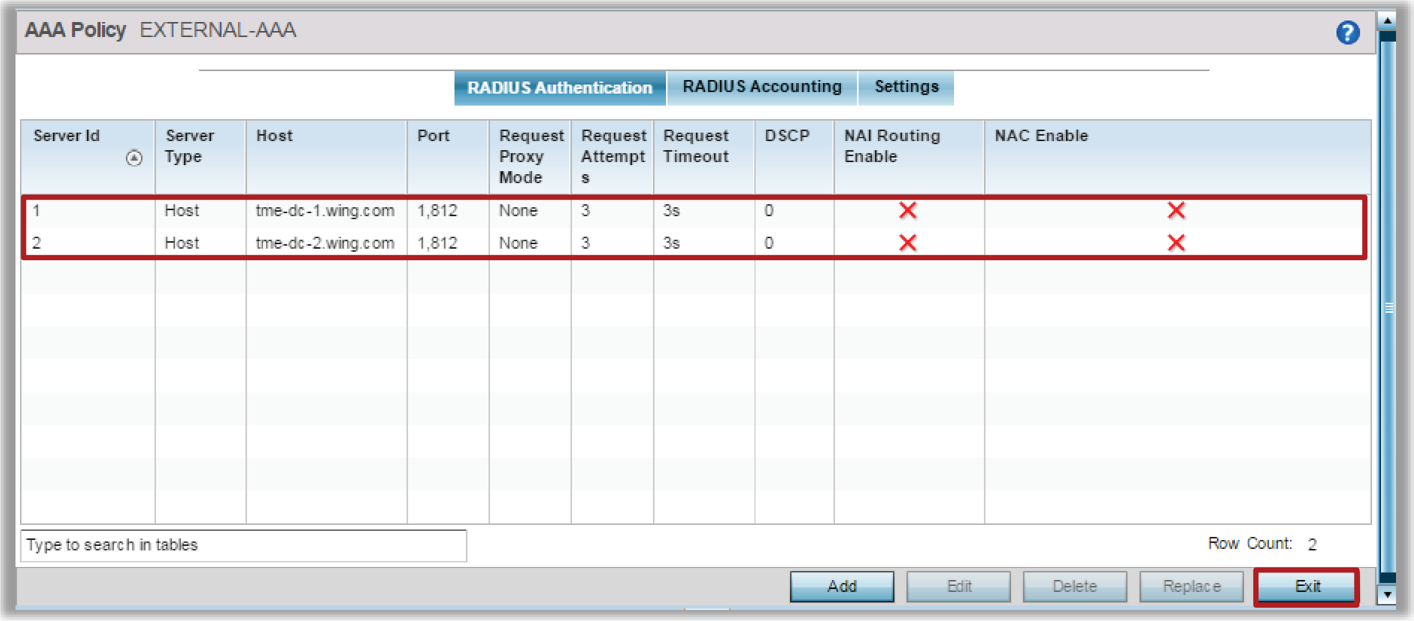
Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

DSCP: 0 (0 to 63)

6. Two RADIUS Authentication server entries have now been defined in the AAA Server Policy named external-aaa. Click Exit.



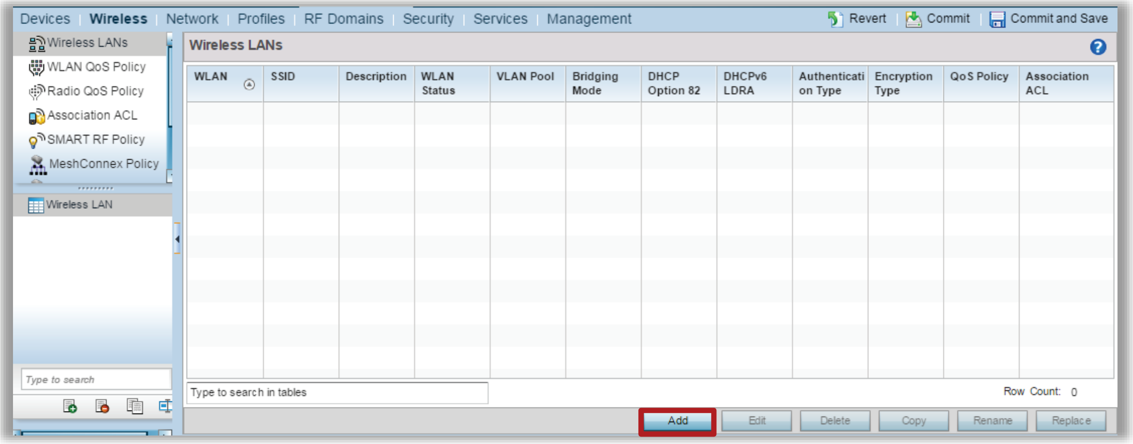
AAA Policy EXTERNAL-AAA

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1	Host	tme-dc-1.wing.com	1,812	None	3	3s	0	✗	✗
2	Host	tme-dc-2.wing.com	1,812	None	3	3s	0	✗	✗

Type to search in tables

Row Count: 2

7. Select Configuration -> Wireless -> Wireless LANs -> Add.



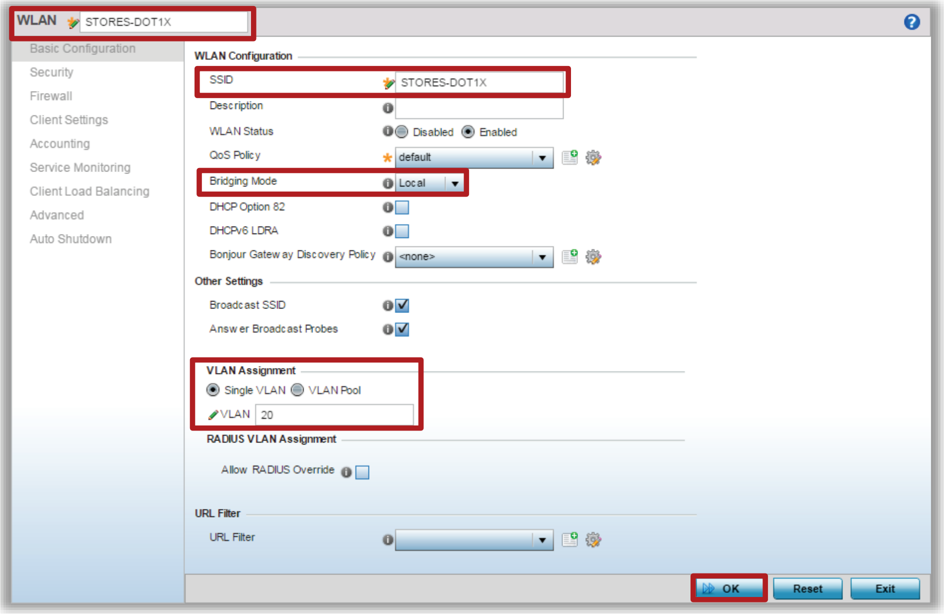
Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL

Type to search in tables

Row Count: 0

8. Enter the WLAN and SSID name then set the Bridging Mode to Local. Enter the local VLAN ID then click OK. In this example the Wireless LAN will be named STORES-DOT1X and the users mapped to the local VLAN 20.



WLAN STORES-DOT1X

WLAN Configuration

SSID: STORES-DOT1X

Description:

WLAN Status: ○ Disabled ● Enabled

QoS Policy: default

Bridging Mode: Local

DHCP Option 82: □

DHCPv6 LDRA: □

Bonjour Gateway Discovery Policy: <none>

Other Settings

Broadcast SSID: ☑

Answer Broadcast Probes: ☑

VLAN Assignment

● Single VLAN ○ VLAN Pool

VLAN: 20

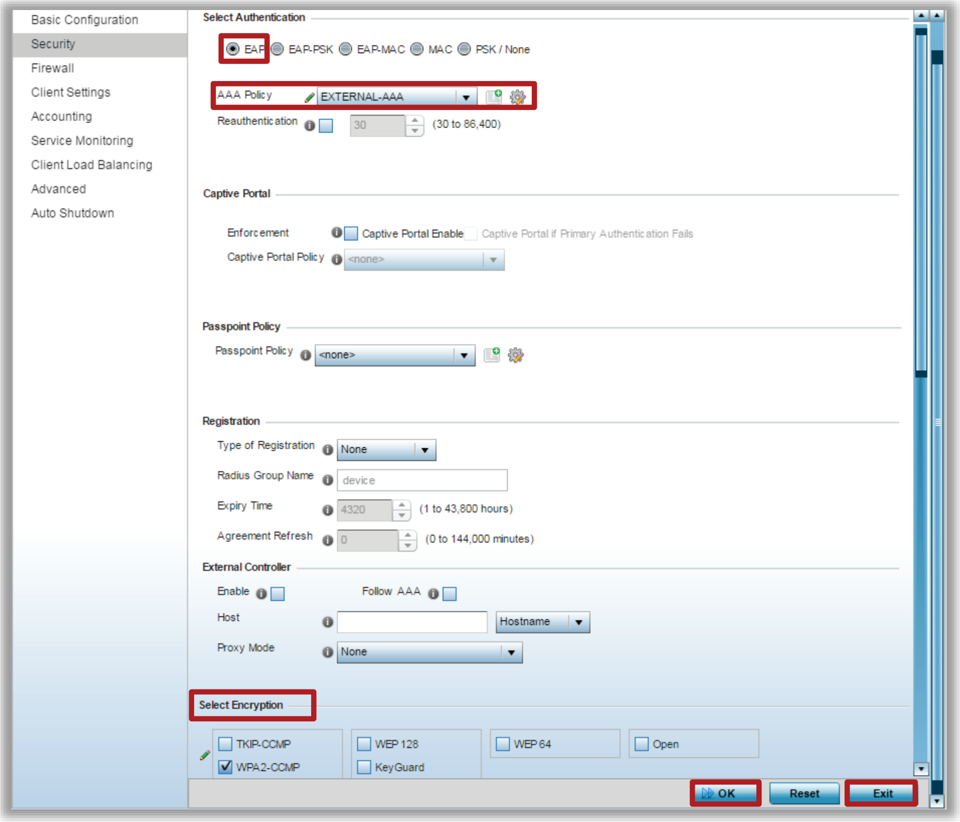
RADIUS VLAN Assignment

Allow RADIUS Override: □

URL Filter

URL Filter:

9. Set the Authentication Type to EAP then assign the AAA Policy named EXTERNAL-AAA. Set the Encryption Type to WPA2-CCMP then click OK and Exit.



Select Authentication

● EAP ○ EAP-PSK ○ EAP-MAC ○ MAC ○ PSK / None

AAA Policy: EXTERNAL-AAA

Reauthentication: □ 30 (30 to 86,400)

Captive Portal

Enforcement: □ Captive Portal Enable □ Captive Portal if Primary Authentication Fails

Captive Portal Policy: <none>

Passpoint Policy

Passpoint Policy: <none>

Registration

Type of Registration: None

Radius Group Name: device

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

External Controller

Enable: □ Follow AAA: □

Host: Hostname

Proxy Mode: None

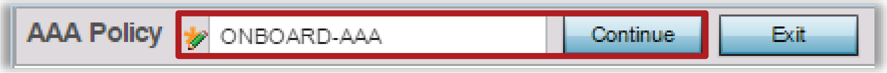
Select Encryption

□ TKIP-CCMP □ WEP 128 □ WEP 64 □ Open

☑ WPA2-CCMP □ KeyGuard

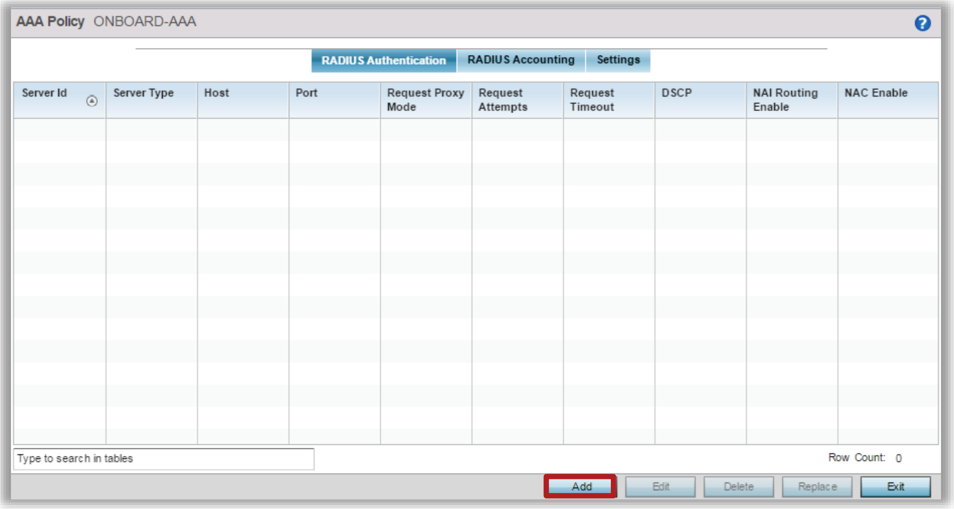
10. Select Configuration -> Network -> AAA Policy -> Add.

11. Enter the AAA Policy name ONBOARD-AAA then click Continue.



AAA Policy: ONBOARD-AAA

12. Select RADIUS Authentication -> Add.

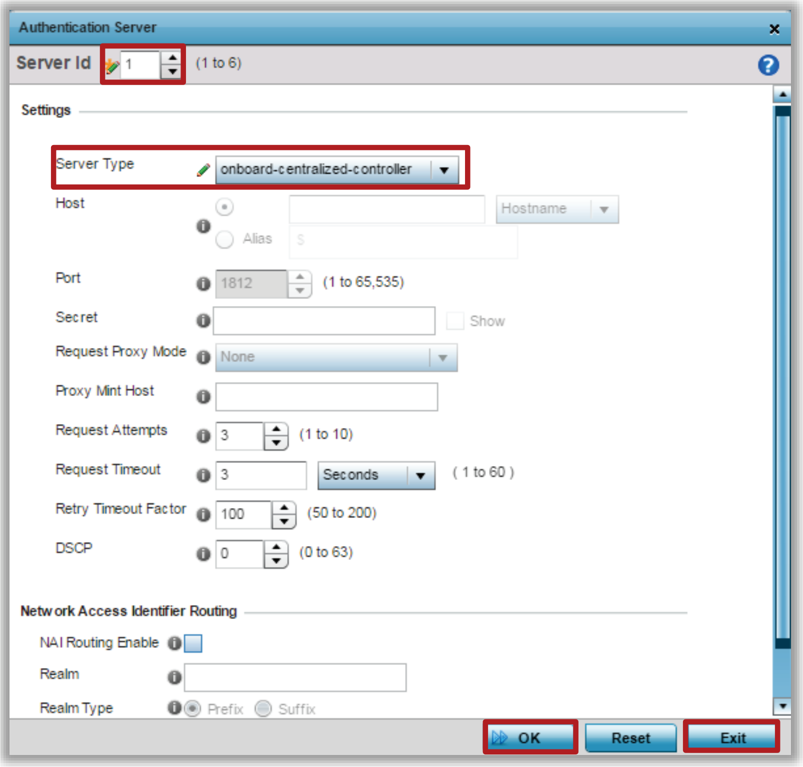


AAA Policy ONBOARD-AAA

Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable

Row Count: 0

13. Set the Server Id to 1 then set server type as Onboard Centralized Controller. Click OK and Exit.



Server Id: 1 (1 to 6)

Server Type: onboard-centralized-controller

Host: ● Hostname ○ Alias $

Port: 1812 (1 to 65,535)

Secret: □ Show

Request Proxy Mode: None

Proxy Mint Host:

Request Attempts: 3 (1 to 10)

Request Timeout: 3 Seconds (1 to 60)

Retry Timeout Factor: 100 (50 to 200)

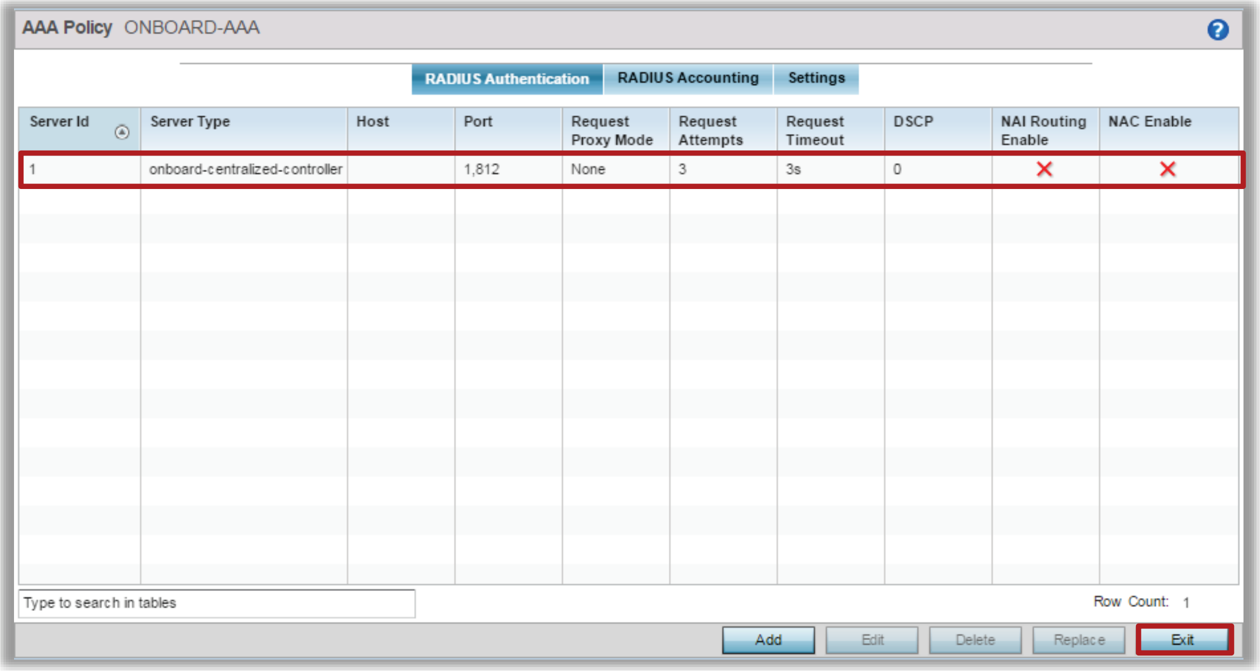
DSCP: 0 (0 to 63)

NAI Routing Enable: □

Realm:

Realm Type: ● Prefix ○ Suffix

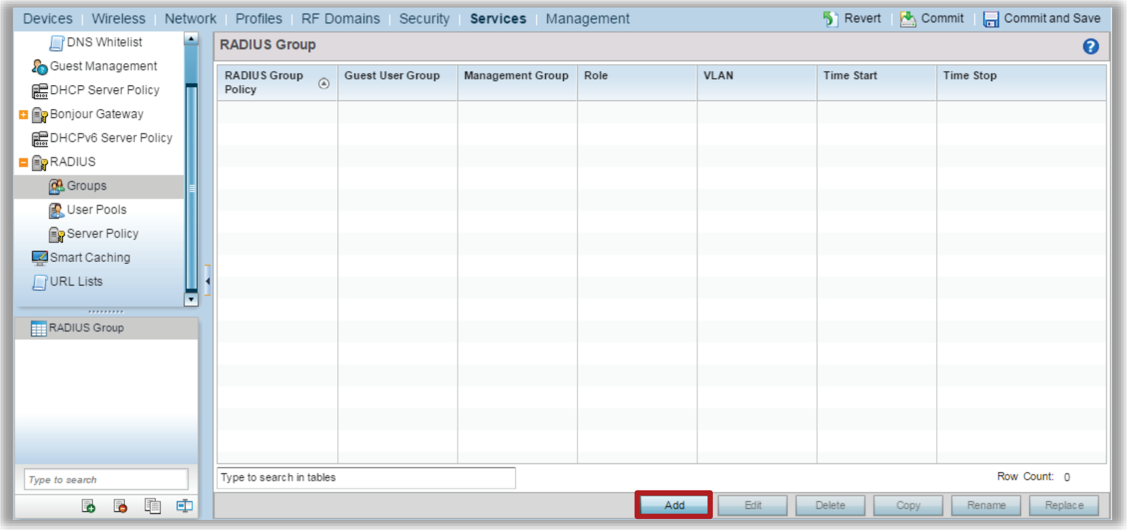
14. One RADIUS Authentication server entry has now been defined in the AAA Server Policy named ONBOARD-AAA. Click Exit.



Server Id	Server Type	Host	Port	Request Proxy Mode	Request Attempts	Request Timeout	DSCP	NAI Routing Enable	NAC Enable
1	onboard-centralized-controller		1,812	None	3	3s	0	✗	✗

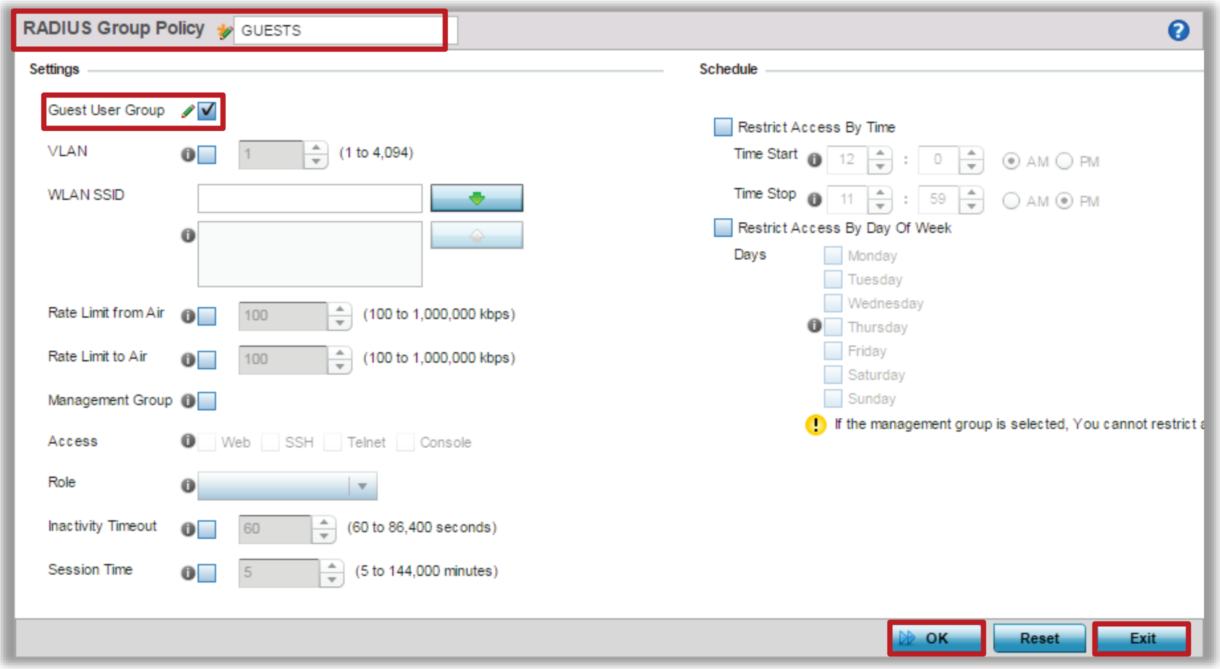
Row Count: 1

15. Select Configuration -> Services ->RADIUS -> Groups -> Add.



RADIUS Group Policy	Guest User Group	Management Group	Role	VLAN	Time Start	Time Stop

Row Count: 0



RADIUS Group Policy: GUESTS

Settings

Guest User Group ☑

VLAN ☐ 1 (1 to 4,094)

WLAN SSID

Rate Limit from Air ☐ 100 (100 to 1,000,000 kbps)

Rate Limit to Air ☐ 100 (100 to 1,000,000 kbps)

Management Group ☐

Access ☐ Web ☐ SSH ☐ Telnet ☐ Console

Role

Inactivity Timeout ☐ 60 (60 to 86,400 seconds)

Session Time ☐ 5 (5 to 144,000 minutes)

Schedule

☐ Restrict Access By Time

Time Start 12 : 0 ● AM ○ PM

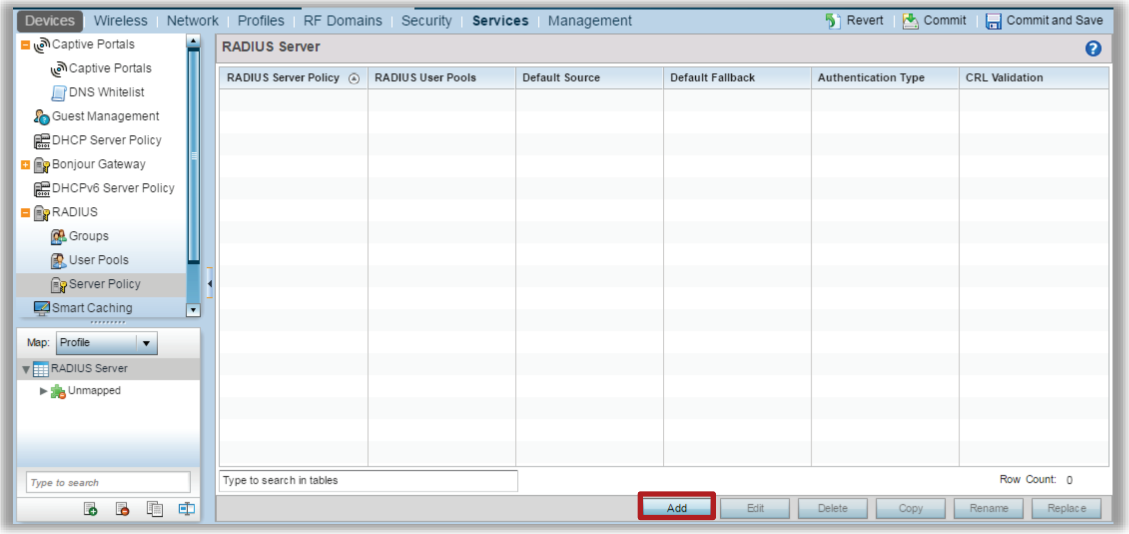
Time Stop 11 : 59 ○ AM ● PM

☐ Restrict Access By Day Of Week

Days ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

If the management group is selected, You cannot restrict a

16. Select Configuration ->Services -> RADIUS -> Server Policy -> Add.

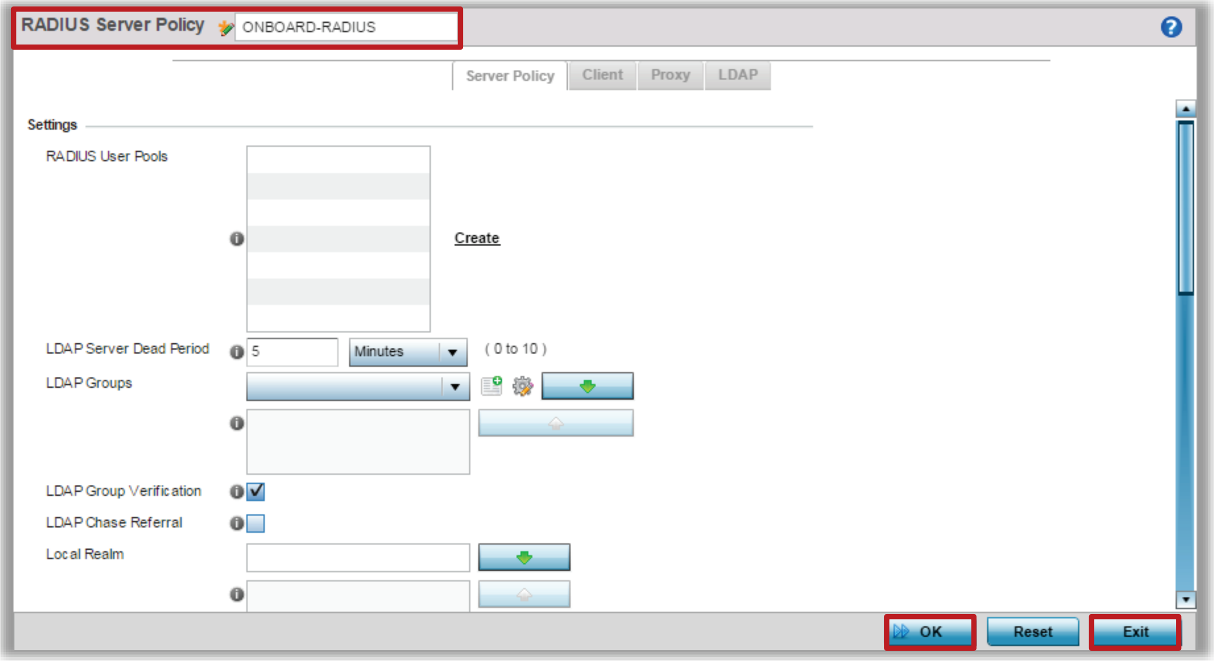


RADIUS Server

RADIUS Server Policy	RADIUS User Pools	Default Source	Default Fallback	Authentication Type	CRL Validation

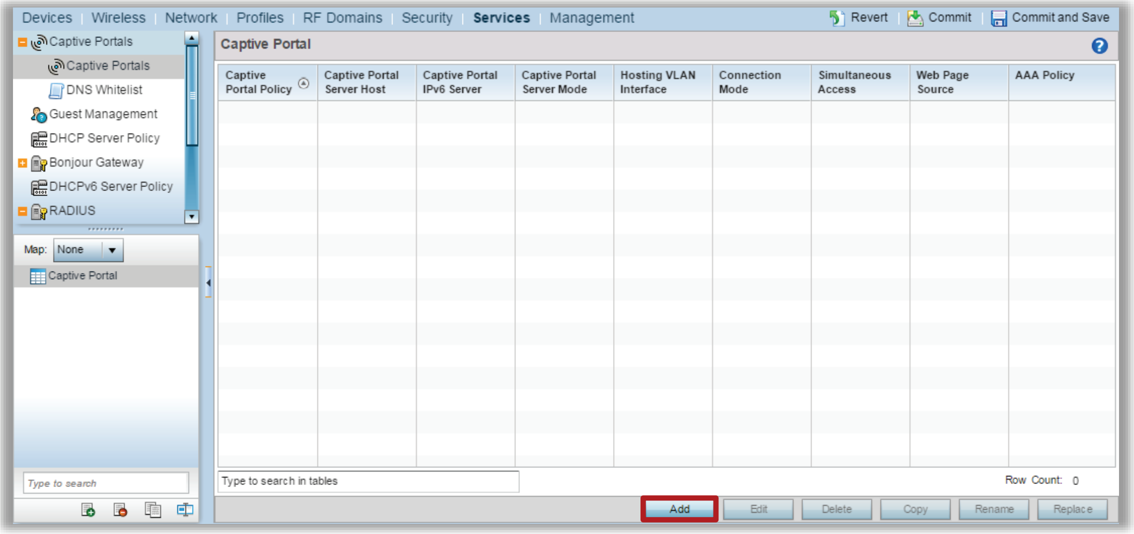
Type to search in tables

Row Count: 0

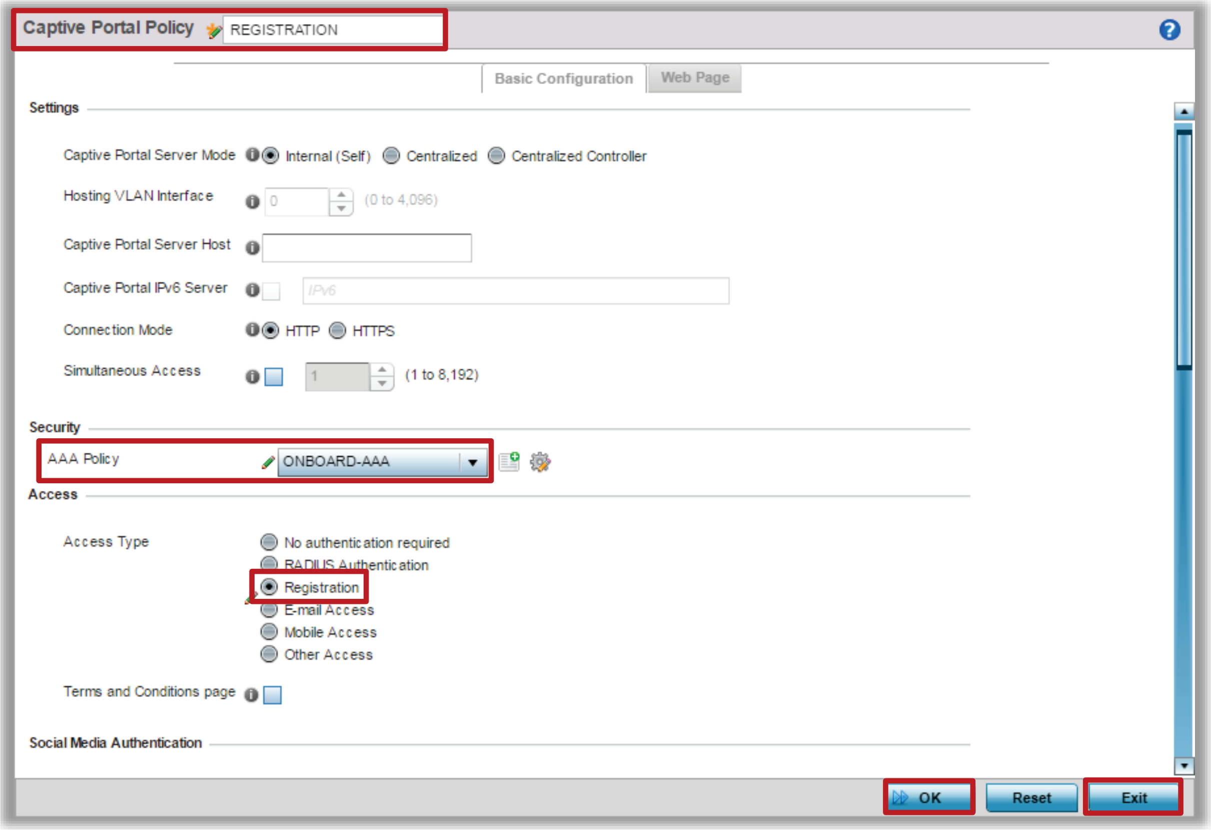


RADIUS Server Policy: ONBOARD-RADIUS

17. Select Configuration -> Services -> Captive Portals -> Add.



Captive Portal Policy	Captive Portal Server Host	Captive Portal IPv6 Server	Captive Portal Server Mode	Hosting VLAN Interface	Connection Mode	Simultaneous Access	Web Page Source	AAA Policy



Captive Portal Policy REGISTRATION

Settings

Captive Portal Server Mode ● Internal (Self) ○ Centralized ○ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server Host

Captive Portal IPv6 Server □ IPv6

Connection Mode ● HTTP ○ HTTPS

Simultaneous Access □ 1 (1 to 8,192)

Security

AAA Policy ONBOARD-AAA

Access

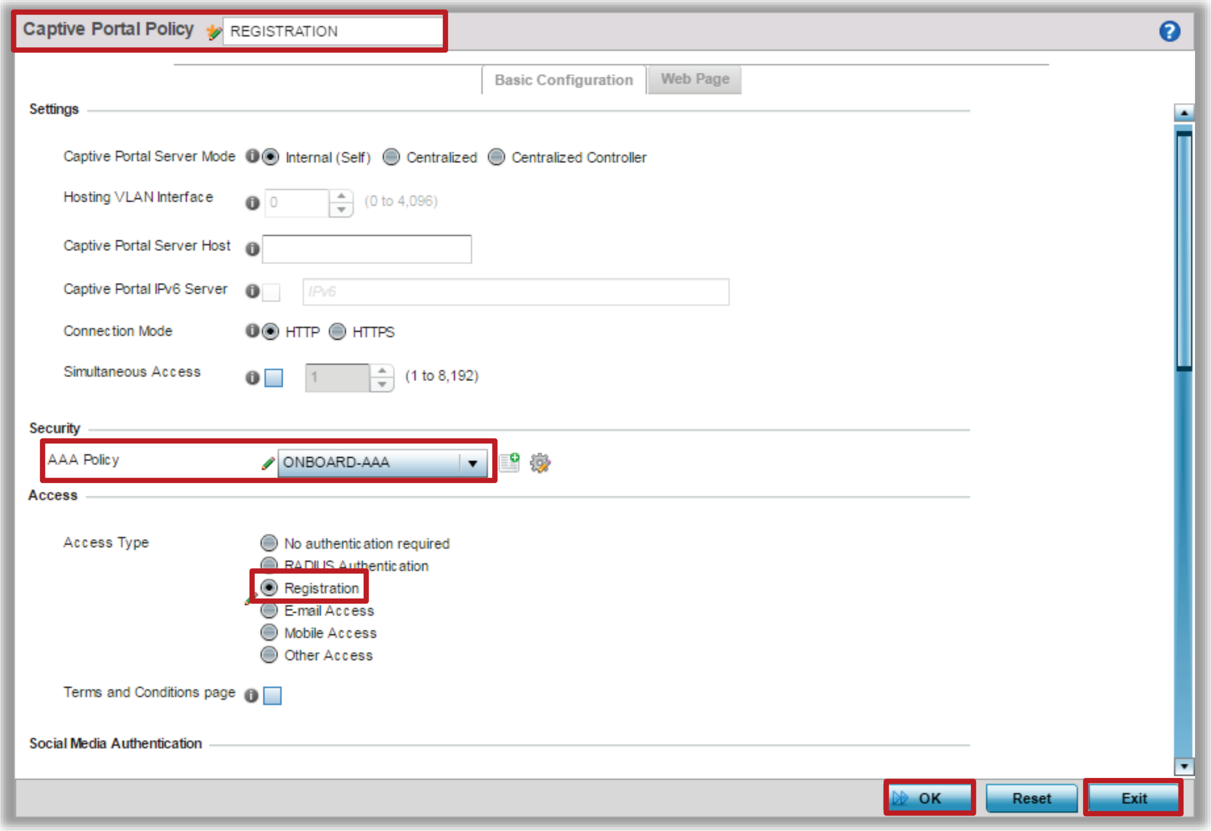
Access Type
○ No authentication required
○ RADIUS Authentication
● Registration
○ E-mail Access
○ Mobile Access
○ Other Access

Terms and Conditions page □

Social Media Authentication

18. Select Configuration -> Wireless -> Wireless LANs -> Add.

19. Enter the WLAN and SSID name then set the Bridging Mode to Tunnel. Enter the VLAN ID 25 then click OK. In this example the Wireless LAN will be named STORES-GUESTS and the users mapped to the extended VLAN 25.



Captive Portal Policy REGISTRATION

Basic Configuration | Web Page

Settings

Captive Portal Server Mode ● Internal (Self) ○ Centralized ○ Centralized Controller

Hosting VLAN Interface 0 (0 to 4,096)

Captive Portal Server Host

Captive Portal IPv6 Server □ IPv6

Connection Mode ● HTTP ○ HTTPS

Simultaneous Access □ 1 (1 to 8,192)

Security

AAA Policy ONBOARD-AAA

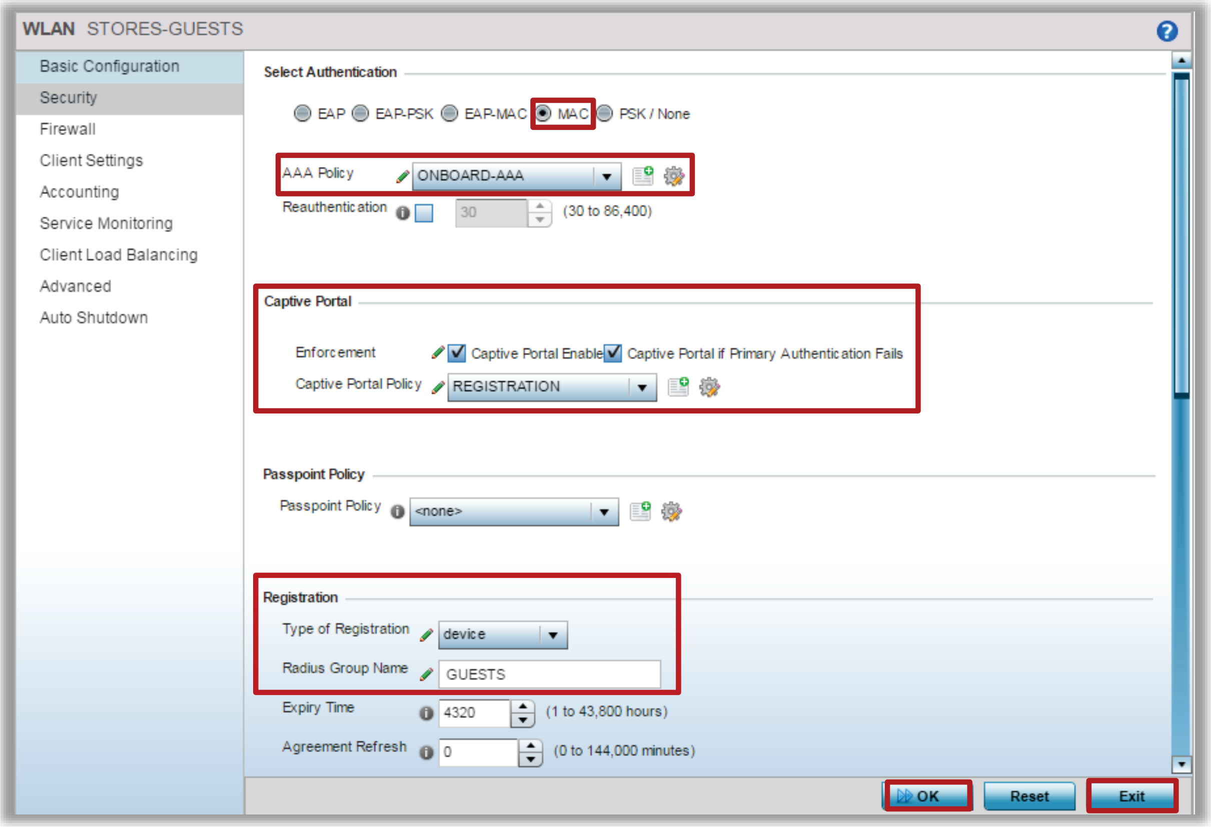
Access

Access Type
○ No authentication required
○ RADIUS Authentication
● Registration
○ E-mail Access
○ Mobile Access
○ Other Access

Terms and Conditions page □

Social Media Authentication

20. Set the Authentication Type to MAC then assign AAA Policy named ONBOARD-AAA. Enable Captive Portal authentication as fallback mechanism, assign Captive Portal Policy named REGISTRATION. Enable Device Registration into the RADIUS Group GUESTS. Click OK and Exit.



WLAN STORES-GUESTS

Select Authentication

○ EAP ○ EAP-PSK ○ EAP-MAC ● MAC ○ PSK / None

AAA Policy: ONBOARD-AAA

Reauthentication □ 30 (30 to 86,400)

Captive Portal

Enforcement ☑ Captive Portal Enable ☑ Captive Portal if Primary Authentication Fails

Captive Portal Policy: REGISTRATION

Passpoint Policy

Passpoint Policy: <none>

Registration

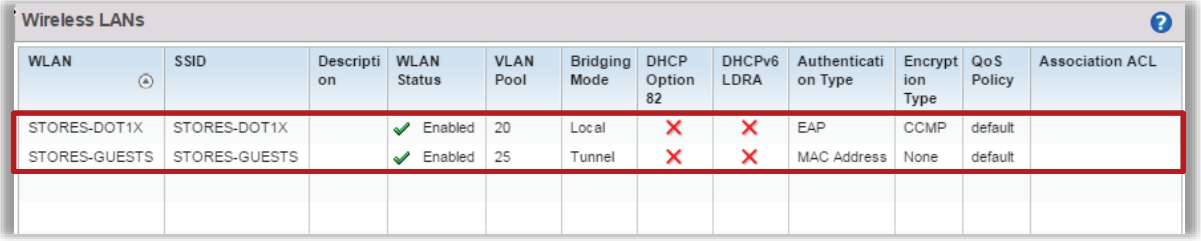
Type of Registration: device

Radius Group Name: GUESTS

Expiry Time: 4320 (1 to 43,800 hours)

Agreement Refresh: 0 (0 to 144,000 minutes)

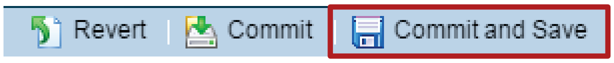
21. Wireless LANs named STORES-DOT1X and STORES-GUESTS have now been defined.



Wireless LANs

WLAN	SSID	Description	WLAN Status	VLAN Pool	Bridging Mode	DHCP Option 82	DHCPv6 LDRA	Authentication Type	Encryption Type	QoS Policy	Association ACL
STORES-DOT1X	STORES-DOT1X		✓ Enabled	20	Local	✗	✗	EAP	CCMP	default	
STORES-GUESTS	STORES-GUESTS		✓ Enabled	25	Tunnel	✗	✗	MAC Address	None	default	

22. Commit and Save the changes.



Configuration – Profiles

Profiles allow common configuration parameters and Policies to be assigned to groups of Controllers and Access Points. Profiles for the Wireless Controllers are hardware model specific, while profiles for the Access Point can be either model specific or can be used with any AP type.

Profiles allow common configuration parameters and policies to be assigned to groups of managed devices such as the Wireless Controllers in the data center or remote Access Points. Changes made to a Profile are automatically inherited by the devices assigned to that profile allowing new services to be quickly deployed in the data center or remote sites.

By default, Controllers and Access Points are automatically assigned to a default device Profile based on their hardware type (example default-nx9000, default-rfs6000, default-ap7532 etc.). Administrators may optionally create user defined profiles which can be manually assigned to existing devices or automatically assigned to new devices using Automatic Provisioning Policies. Each WING 5 device must be assigned to a default or user defined Profile.

In this data center deployment example, the Wireless Controllers and remote Access Points share common configuration parameters such as Management Policies, VLAN port assignments, Wireless LANs, DNS and NTP servers. To assign these common configuration parameters a user defined Profile will be created and manually assigned to the Wireless Controllers in the data center while a user defined Profile will be created and automatically assigned to remote Access Points using Automatic Provisioning Policies.

For this configuration step two user defined Profiles will be created with the following parameters:

1. A user defined NX9600 device Profile named noc-nx9600 will be created for the Wireless Controllers in the data center with the following parameters:
    a. The user defined Management Policy named controllers will be assigned.
    b. The GE1 port will be configured as a Trunk port with the Untagged Native VLAN ID 96 and Tagged VLAN 25 for the Guest Traffic.
    c. The Domain Name will be set to tmelabs.local and the Name Server address 192.168.7.15 defined.
    d. A NTP server time.nist.gov will be assigned.
2. A user defined ANYAP Profile named STORES-AP will be created for the remote Access Points with the following parameters:
    a. The user defined Management Policy named aps will be assigned.
    b. The ge1 port will be configured as a Trunk port with the untagged Native VLAN ID 1 and tagged corporate VLAN ID 20.
    c. Create a Virtual IP Interface for the Native VLAN ID 1 with the DHCP Client enabled.
    d. The Wireless LAN named STORES-DOT1X will be assigned to both radio1 and radio2 while the Wireless LAN named STORES-GUESTS will only be assigned to radio1.
    e. No need to define domain name as it will be received via DHCP
    f. No need to define NTP server, as time is automatically synced with the controller during normal operation.

The user defined Profile named noc-nx9600 will be manually assigned to each NX 9610 Wireless Controller using Device configuration while the user defined Profile named STORES-AP will be automatically assigned to each remote Access Point as they are discovered and adopted using an Automatic Provisioning Policy. The Automatic Provisioning Policy will be assigned to the user defined Profile named noc-nx9600 in a later step.

> Note
>
> As a best practice it is recommended that the Wireless Controllers be connected to the network using 802.1Q tagging which allows additional VLANs to be added in the future without disrupting the Wireless network. As an industry best practice it is also recommended that the Native VLAN is tagged.

> Note
>
> In case VLAN 1 is used in production network at the remote sites it is highly recommended that the Access Points Native VLAN id match the VLAN id of the switch port that the Access Point is connected to at the remote site.

Profiles Configuration – CLI

1. Create a NX 9600 Profile for the Wireless Controllers in the data center named noc-nx9600:

```
nx9600-7F34C7(config)# profile nx9600 noc-nx9600
nx9600-7F34C7(config-profile-noc-nx9600)#
```

2. Assign the user defined Management policy named noc:

```
nx9600-7F34C7(config-profile-noc-nx9600)# use management-policy controllers
```

3. Configure up1 as a Trunk port and assign the tagged Native VLAN 20:

```
nx9600-7F34C7(config-profile-noc-nx9600)# interface ge1
nx9600-7F34C7(config-profile-noc-nx9600-if-ge1)# description Uplink
nx9600-7F34C7(config-profile-noc-nx9600-if-ge1)# switchport mode trunk
nx9600-7F34C7(config-profile-noc-nx9600-if-ge1)# switchport trunk native vlan 96
nx9600-7F34C7(config-profile-noc-nx9600-if-ge1)# switchport trunk allowed vlan 25,96
nx9600-7F34C7(config-profile-noc-nx9600-if-ge1)# exit
```

4. Define an Extended VLAN 25 for the Guest Traffic, enable tunneling over Level 2 MINT and enable Layer 2 Tunnel Broadcast Optimization:

```
nx9600-7F34C7(config-profile-noc-nx9600)# bridge vlan 25
nx9600-7F34C7(config-profile-noc-nx9600-bridge-vlan-25)# bridging-mode tunnel
nx9600-7F34C7(config-profile-noc-nx9600-bridge-vlan-25)# tunnel-over-level2
nx9600-7F34C7(config-profile-noc-nx9600-bridge-vlan-25)# l2-tunnel-broadcast-optimization
nx9600-7F34C7(config-profile-noc-nx9600-bridge-vlan-25)# exit
```

5. Assign a Domain Name, Name Server and NTP Server:

```
nx9600-7F34C7(config-profile-noc-nx9600)# ip domain-name tmelabs.local
nx9600-7F34C7(config-profile-noc-nx9600)# ip name-server 192.168.7.15
nx9600-7F34C7(config-profile-noc-nx9600)# ntp server time.nist.gov
```

6. Assign RADIUS Server Policy to start the RADIUS server:

```
nx9600-7F34C7(config-profile-noc-nx9600)# use radius-server-policy ONBOARD-RADIUS
```

7. Verify the changes:

```
nx9600-7F34C7(config-profile-noc-nx9600)# show context
profile nx9600 noc-nx9600
 bridge vlan 25
  l2-tunnel-broadcast-optimization
  bridging-mode tunnel
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
ip name-server 192.168.7.15
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 use radius-server-policy ONBOARD-RADIUS
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface xge1
 interface xge2
 interface xge3
 interface xge4
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 96
  no switchport trunk native tagged
  switchport trunk allowed vlan 20,96
 interface ge2
 use management-policy controllers
 use firewall-policy default
 ntp server time.nist.gov
 service pm sys-restart
```

8. Exit the Profile configuration:

```
nx9600-7F34C7(config-profile-noc-nx9600)# exit
```

9. Create an ANYAP user defined Profile for the remote Access Points named STORES-AP

```
nx9600-7F34C7(config)# profile anyap STORES-AP
nx9600-7F34C7(config-profile-STORES-AP)#
```

10. Assign the user defined Management policy named aps:

```
nx9600-7F34C7(config-profile-STORES-AP)# use management-policy aps
```

11. Configure ge1 as a Trunk port and assign the untagged Native VLAN 1 and tagged user VLAN 20:

```
nx9600-7F34C7(config-profile-STORES-AP)# interface ge1
nx9600-7F34C7(config-profile-STORES-AP-if-ge1)# description Uplink
nx9600-7F34C7(config-profile-STORES-AP-if-ge1)# switchport mode trunk
nx9600-7F34C7(config-profile-STORES-AP-if-ge1)# switchport trunk allowed vlan 1,20
nx9600-7F34C7(config-profile-STORES-AP-if-ge1)# exit
```

12. Create a Virtual IP interface on the Native VLAN 1 with the DHCP client enabled. This is required so that the Access Points at the site can automatically boot and discover the Wireless Controllers in the data center using DHCP:

```
nx9600-7F34C7(config-profile-STORES-AP)# interface vlan1
nx9600-7F34C7(config-profile-STORES-AP-if-vlan1)# description AP VLAN
nx9600-7F34C7(config-profile-STORES-AP-if-vlan1)# ip address dhcp
nx9600-7F34C7(config-profile-STORES-AP-if-vlan1)# ip dhcp client request options all
nx9600-7F34C7(config-profile-STORES-AP-if-vlan1)# exit
```

13. Define extended VLAN 25 for the Guest Traffic and enable tunneling over Level 2 MINT:

```
nx9600-7F34C7(config-profile-STORES-AP)# bridge vlan 25
nx9600-7F34C7(config-profile-STORES-AP-bridge-vlan-25)# bridging-mode tunnel
nx9600-7F34C7(config-profile-STORES-AP-bridge-vlan-25)# tunnel-over-level2
nx9600-7F34C7(config-profile-STORES-AP-brdige-vlan-25)# exit
```

14. Assign Captive Portal Server Policy to start the hotspot server:

```
nx9600-7F34C7(config-profile-STORES-AP)# use captive-portal server REGISTRATION
```

15. Assign Wireless LANs to the 2.4 GHz radio1. In this example the Wireless LANs named STORES-DOT1X and STORES-GUESTS are assigned to the 2.4 GHz radios:

```
nx9600-7F34C7(config-profile-STORES-AP)# interface radio 1
nx9600-7F34C7(config-profile-STORES-AP-if-radio1)# wlan STORES-DOT1X
nx9600-7F34C7(config-profile-STORES-AP-if-radio1)# wlan STORES-GUESTS
nx9600-7F34C7(config-profile-STORES-AP-if-radio1)# exit
```

16. Assign Wireless LANs to the 5 GHz radio2. In this example only the Wireless LAN named STORES-DOT1X is assigned to the 5 GHz radios:

```
nx9600-7F34C7(config-profile-STORES-AP)# interface radio 2
nx9600-7F34C7(config-profile-STORES-AP-if-radio2)# wlan STORES-DOT1X
nx9600-7F34C7(config-profile-STORES-AP-if-radio2)# exit
```

17. Verify the changes:

```
nx9600-7F34C7(config-profile-STORES-AP)# show context
profile anyap STORES-AP
 bridge vlan 25
  bridging-mode tunnel
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
 no autoinstall configuration
 no autoinstall firmware
 crypto ikev1 policy ikev1-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ikev2 policy ikev2-default
  isakmp-proposal default encryption aes-256 group 2 hash sha
 crypto ipsec transform-set default esp-aes-256 esp-sha-hmac
 crypto ikev1 remote-vpn
 crypto ikev2 remote-vpn
 crypto auto-ipsec-secure
 crypto load-management
 crypto remote-vpn-client
 interface radio1
  wlan STORES-DOT1X bss 1 primary
  wlan STORES-GUESTS bss 2 primary
 interface radio2
  wlan STORES-DOT1X bss 1 primary
 interface radio3
 interface up1
 interface ge1
  description Uplink
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1,20
 interface ge2
 interface fe1
 interface fe2
 interface fe3
 interface fe4
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 interface wwan1
 interface pppoe1
 use management-policy aps
 use firewall-policy default
 use captive-portal server REGISTRATION
 service pm sys-restart
 router ospf
```

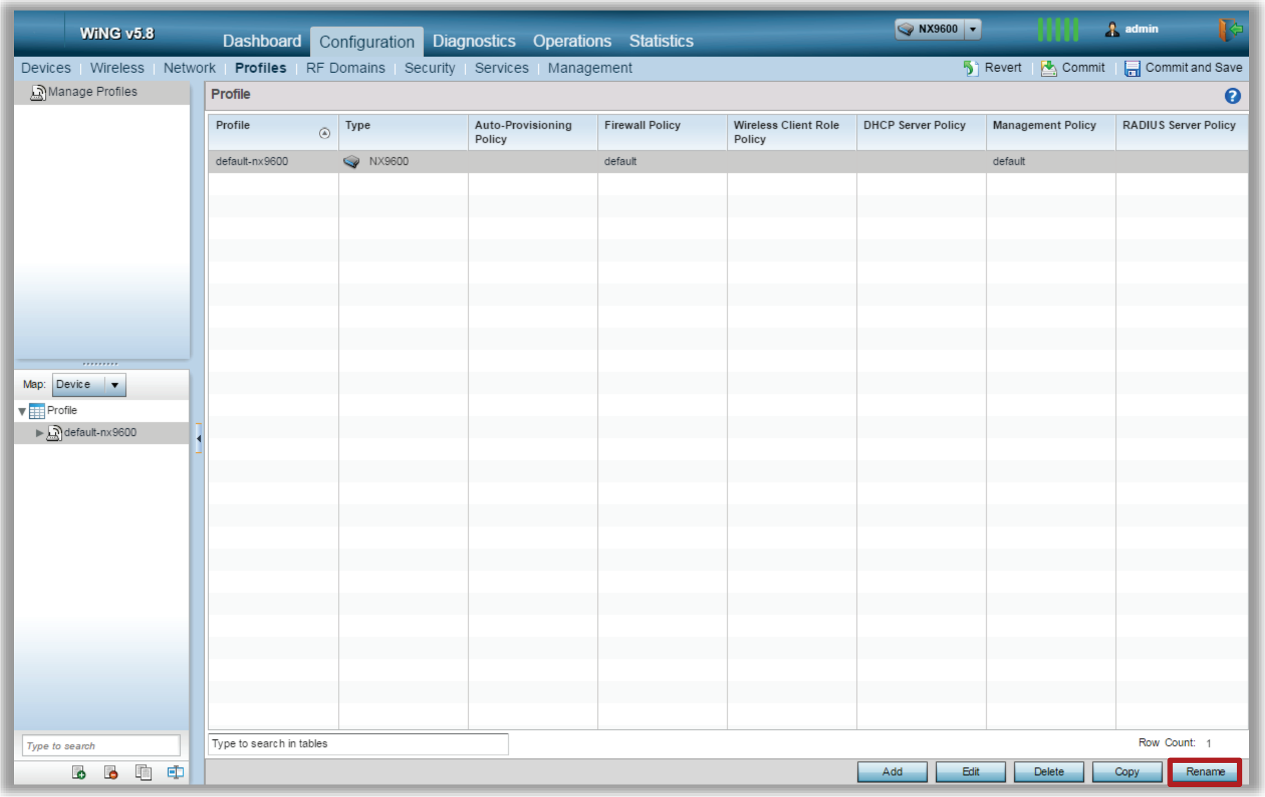
18. Exit the Profile configuration then commit and save the changes:

```
nx9600-7F34C7(config-profile-STORES-AP)# exit
nx9600-7F34C7(config)#commit write
[OK]
```

Profiles Configuration – Web UI

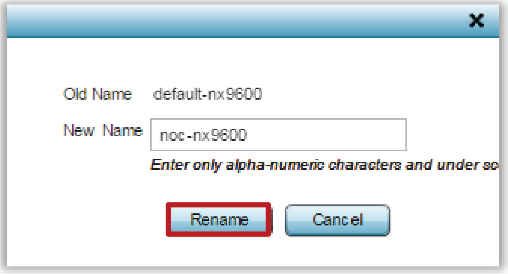
Use the following procedure to create a user defined device Profiles for the Wireless Controllers in the data center and the remote Access Points for each store using the Management User Interface:

1. Select Configuration -> Profiles -> <Select NX9600 default Profile> -> Rename:



Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
default-nx9600	NX9600		default			default	

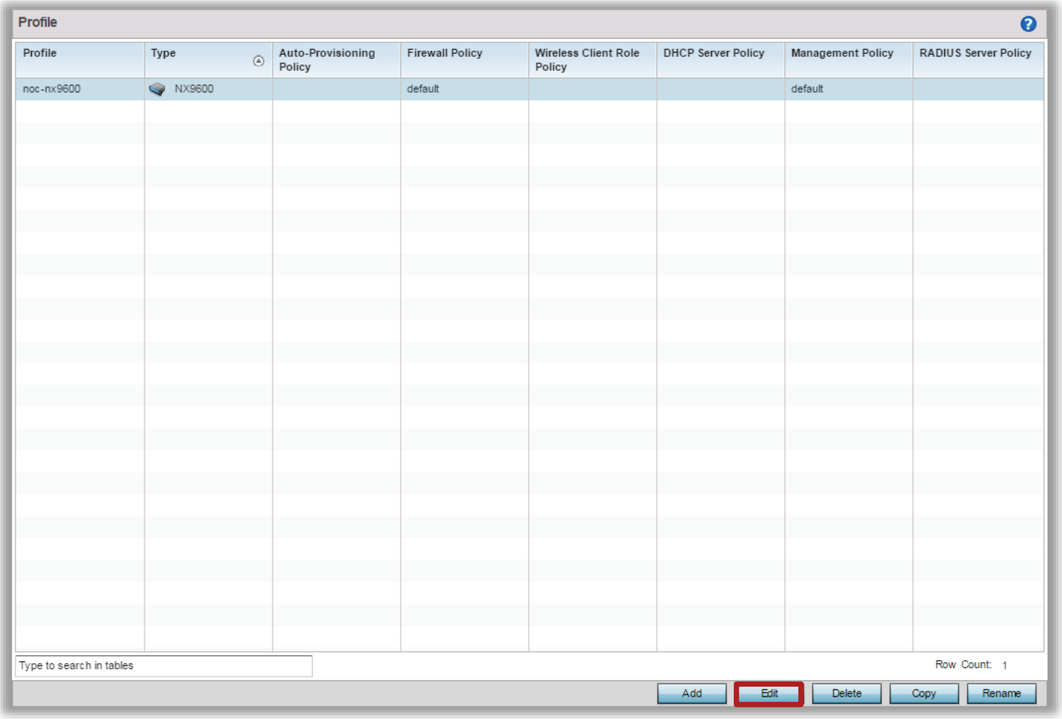


Old Name default-nx9600

New Name noc-nx9600

Enter only alpha-numeric characters and under sc

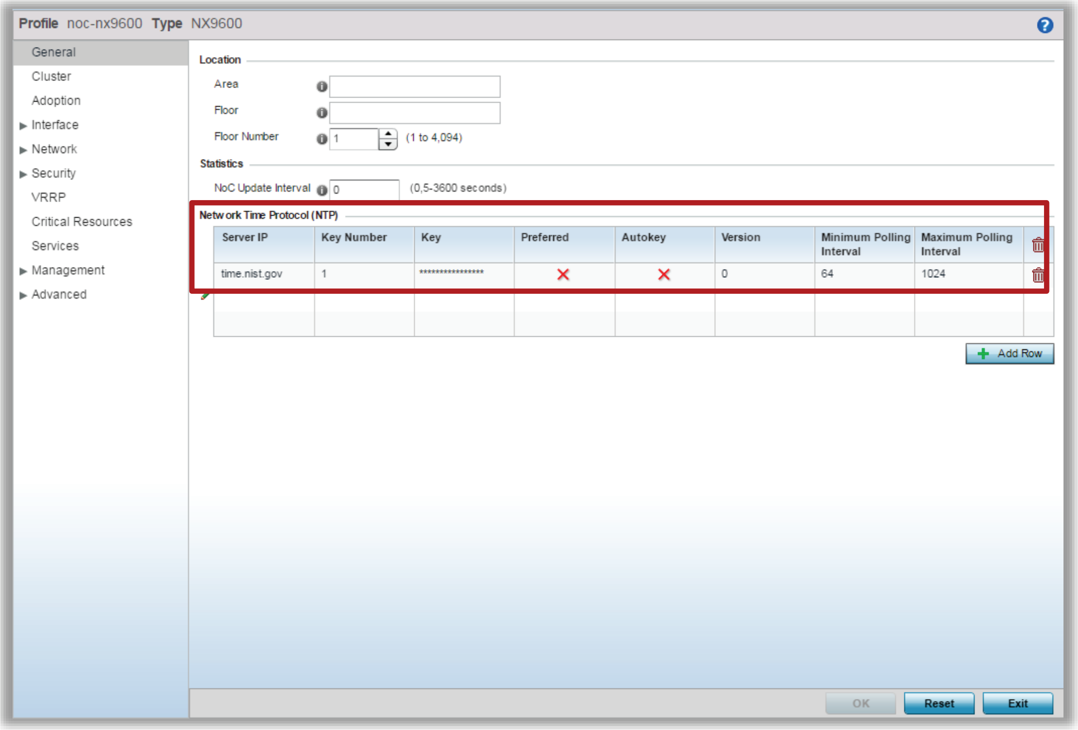
2. Select noc-nx9600 Profile -> Edit:



Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
noc-nx9600	NX9600		default			default	

3. Under Network Time Protocol click Add Row then enter the NTP Server FQDN or IP Address. Click OK:



Profile noc-nx9600 **Type** NX9600

Location

Area

Floor

Floor Number 1 (1 to 4,094)

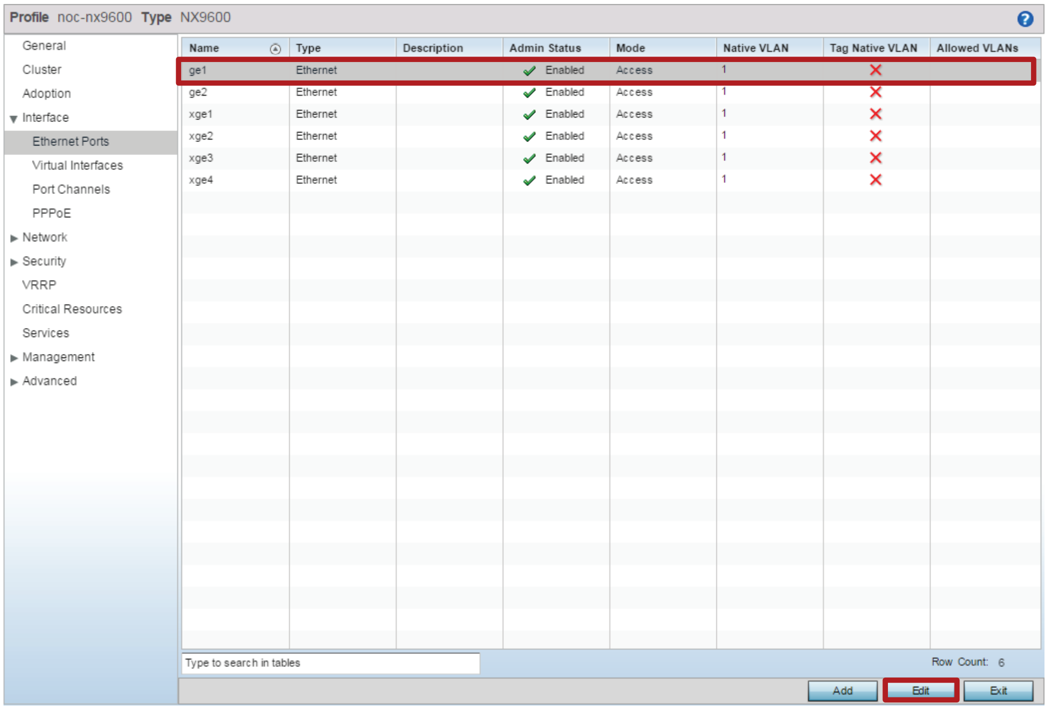
Statistics

NoC Update Interval 0 (0,5-3600 seconds)

Network Time Protocol (NTP)

Server IP	Key Number	Key	Preferred	Autokey	Version	Minimum Polling Interval	Maximum Polling Interval
time.nist.gov	1	****************	✗	✗	0	64	1024

4. Select Interface -> Ethernet Ports -> ge1 -> Edit:

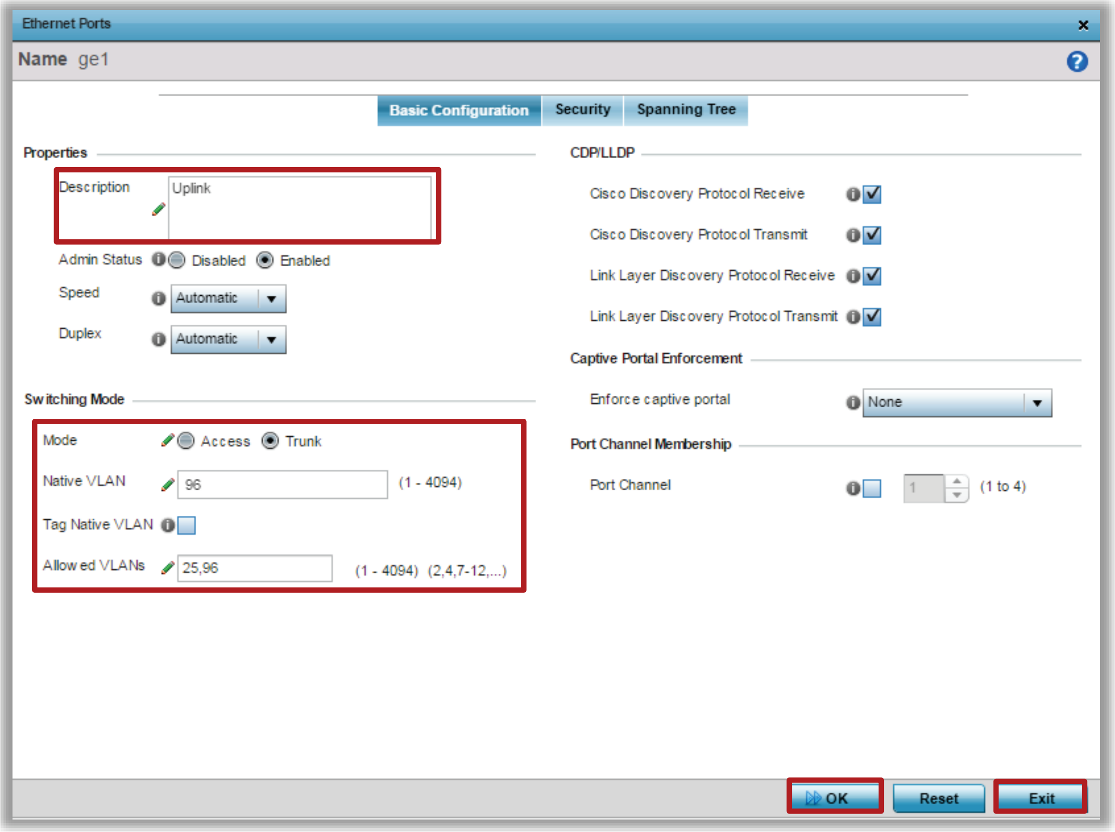


Profile noc-nx9600 **Type** NX9600

Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
ge1	Ethernet		✓ Enabled	Access	1	✗	
ge2	Ethernet		✓ Enabled	Access	1	✗	
xge1	Ethernet		✓ Enabled	Access	1	✗	
xge2	Ethernet		✓ Enabled	Access	1	✗	
xge3	Ethernet		✓ Enabled	Access	1	✗	
xge4	Ethernet		✓ Enabled	Access	1	✗	

Row Count: 6

5. Enter a Description then set the Switching Mode to Trunk. Enter the Native VLAN and Allowed VLANs then click OK and Exit. Note in this example tagged VLAN 25 is deployed in the data center:



Ethernet Ports

Name ge1

Basic Configuration | Security | Spanning Tree

Properties

Description: Uplink

Admin Status ○ Disabled ● Enabled

Speed: Automatic

Duplex: Automatic

Switching Mode

Mode ○ Access ● Trunk

Native VLAN: 96 (1 - 4094)

Tag Native VLAN □

Allowed VLANs: 25,96 (1 - 4094) (2,4,7-12,...)

CDP/LLDP

Cisco Discovery Protocol Receive ☑

Cisco Discovery Protocol Transmit ☑

Link Layer Discovery Protocol Receive ☑

Link Layer Discovery Protocol Transmit ☑

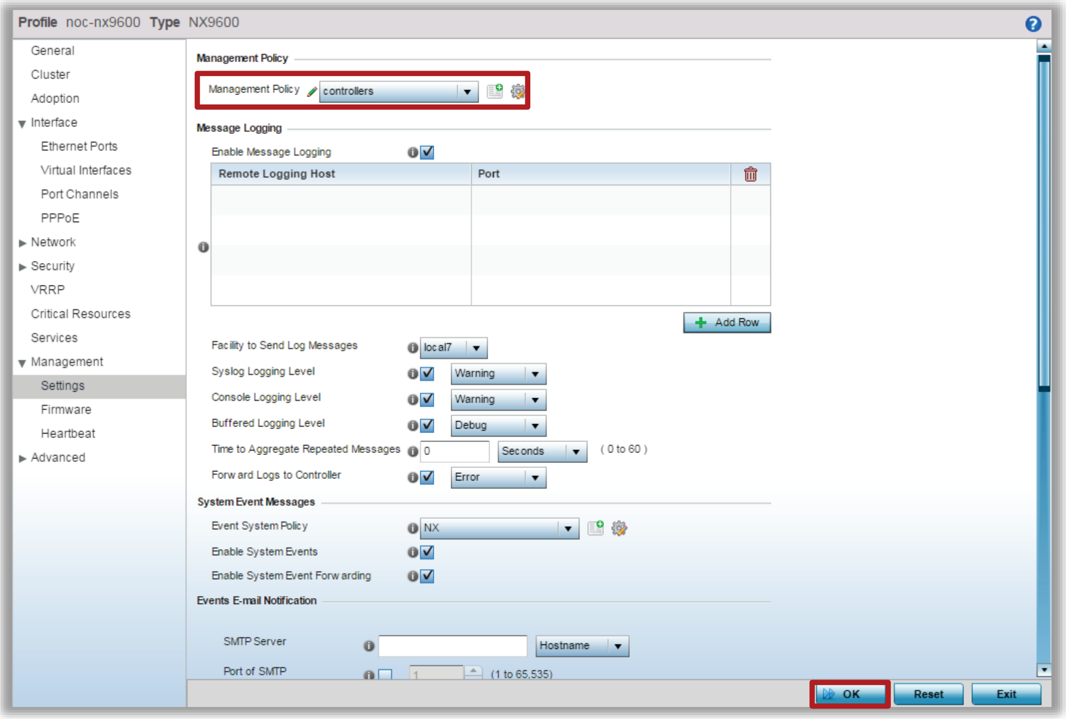
Captive Portal Enforcement

Enforce captive portal: None

Port Channel Membership

Port Channel □ 1 (1 to 4)

6. Select Management -> Settings. Assign the user defined Management Policy named controllers then click OK:



Profile noc-nx9600 **Type** NX9600

Management Policy

Management Policy: controllers

Message Logging

Enable Message Logging ☑

Remote Logging Host	Port

Facility to Send Log Messages: local7
Syslog Logging Level ☑ Warning
Console Logging Level ☑ Warning
Buffered Logging Level ☑ Debug
Time to Aggregate Repeated Messages: 0 Seconds (0 to 60)
Forward Logs to Controller ☑ Error

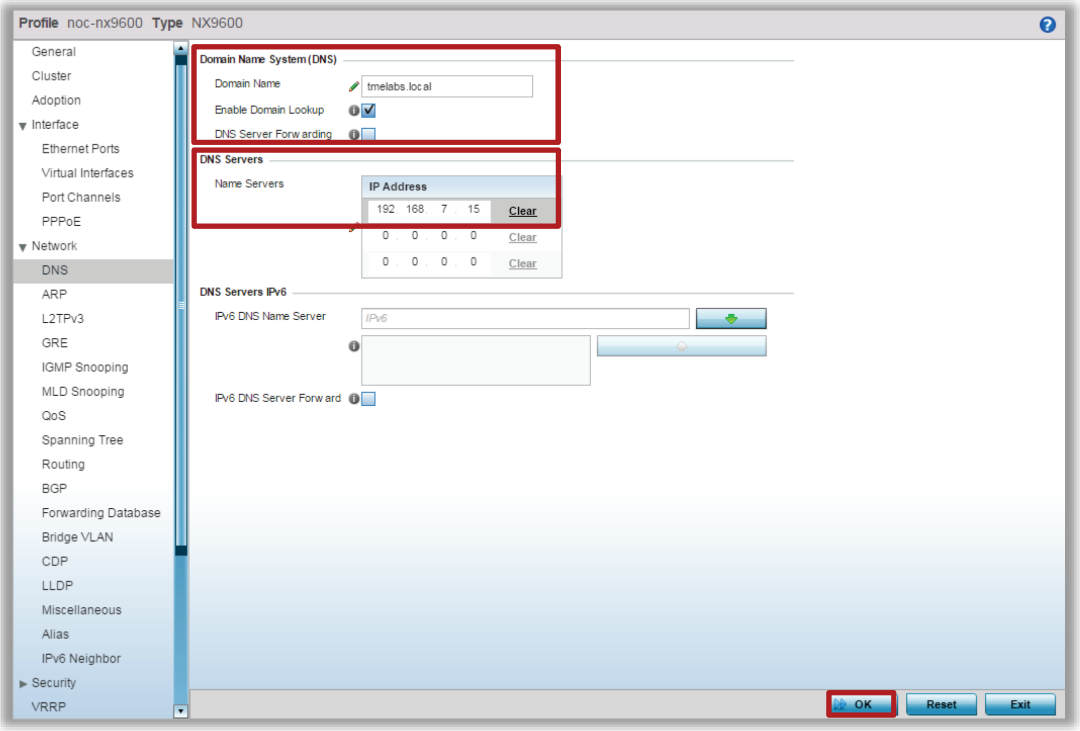
System Event Messages

Event System Policy: NX
Enable System Events ☑
Enable System Event Forwarding ☑

Events E-mail Notification

SMTP Server: Hostname
Port of SMTP □ 1 (1 to 65,535)

7. Select Network -> DNS. Assign the Domain Name then enter the Name Server IP address. Click OK:



Profile noc-nx9600 **Type** NX9600

Domain Name System (DNS)

Domain Name: tmelabs.local
Enable Domain Lookup ☑
DNS Server Forwarding □

DNS Servers

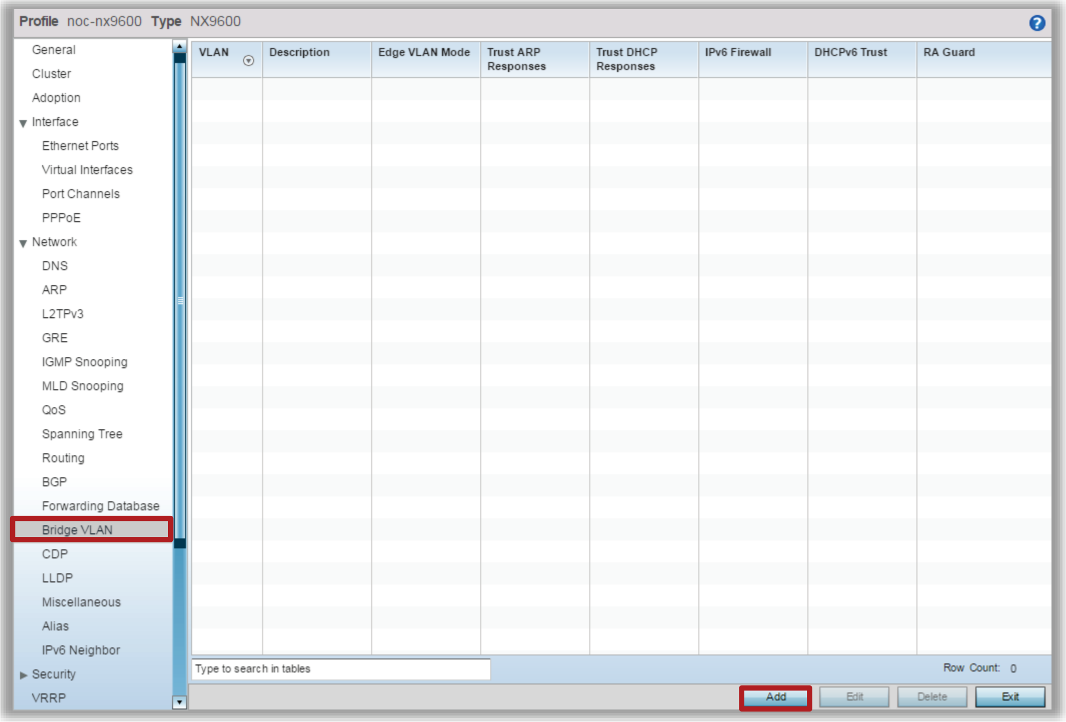
Name Servers

IP Address	
192 . 168 . 7 . 15	Clear
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

DNS Servers IPv6

IPv6 DNS Name Server: IPv6
IPv6 DNS Server Forward □

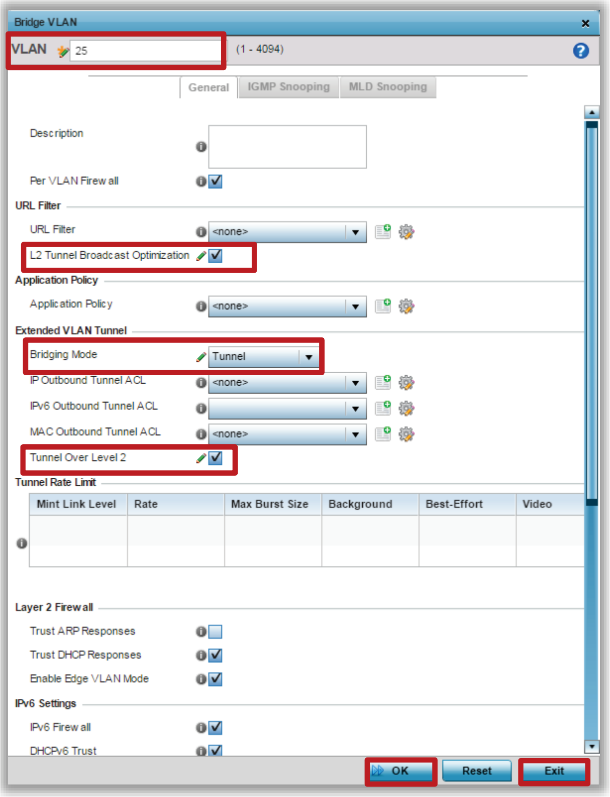
8. Select Bridge VLAN -> Add. Define an Extended VLAN 25 for the Guest Traffic. Enable tunneling over Level 2 MINT and additionally enable Layer 2 Tunnel Broadcast Optimization. Click OK then Exit:



Profile noc-nx9600 Type NX9600

VLAN	Description	Edge VLAN Mode	Trust ARP Responses	Trust DHCP Responses	IPv6 Firewall	DHCPv6 Trust	RA Guard

Row Count: 0



Bridge VLAN

VLAN 25 (1 - 4094)

General | IGMP Snooping | MLD Snooping

Description

Per VLAN Firewall ☑

URL Filter

URL Filter <none>

L2 Tunnel Broadcast Optimization ☑

Application Policy

Application Policy <none>

Extended VLAN Tunnel

Bridging Mode Tunnel

IP Outbound Tunnel ACL <none>

IPv6 Outbound Tunnel ACL

MAC Outbound Tunnel ACL <none>

Tunnel Over Level 2 ☑

Tunnel Rate Limit

Mint Link Level	Rate	Max Burst Size	Background	Best-Effort	Video

Layer 2 Firewall

Trust ARP Responses ☐

Trust DHCP Responses ☑

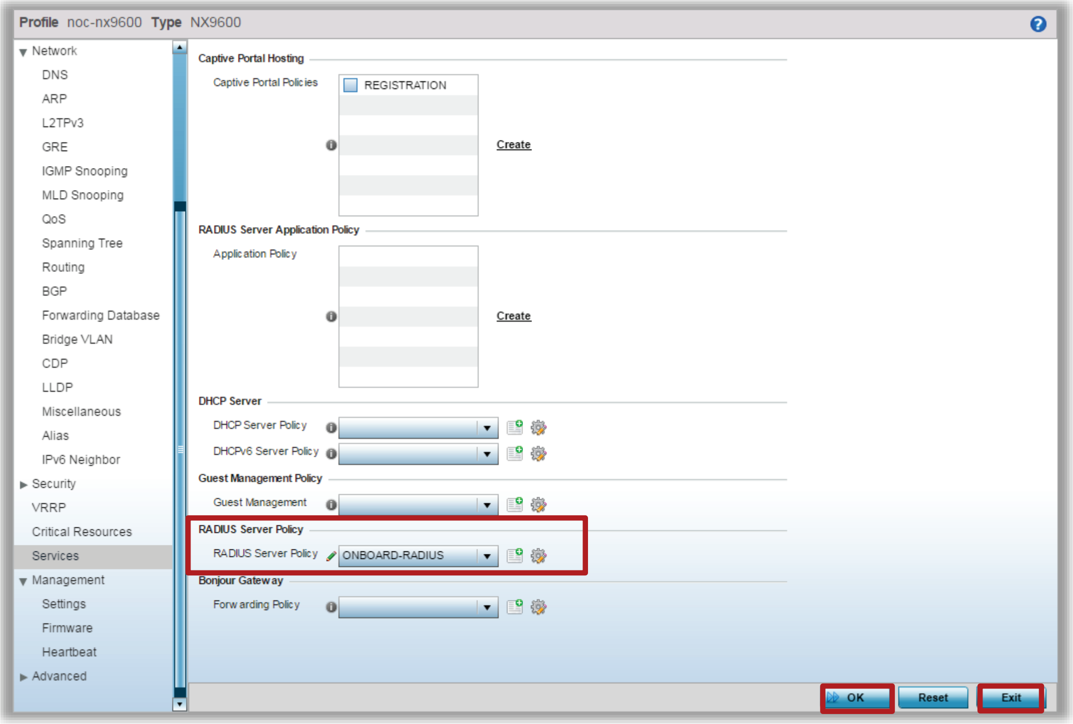
Enable Edge VLAN Mode ☑

IPv6 Settings

IPv6 Firewall ☑

DHCPv6 Trust ☑

9. Select Services. Assign the RADIUS Server Policy then click OK and then Exit:



Profile noc-nx9600 **Type** NX9600

Captive Portal Hosting

Captive Portal Policies: □ REGISTRATION

RADIUS Server Application Policy

Application Policy:

DHCP Server

DHCP Server Policy:

DHCPv6 Server Policy:

Guest Management Policy

Guest Management:

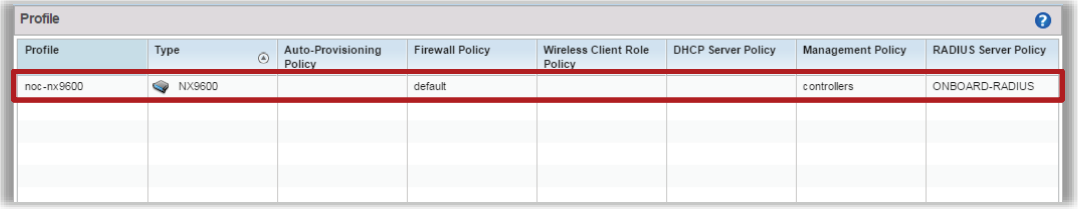
RADIUS Server Policy

RADIUS Server Policy: ONBOARD-RADIUS

Bonjour Gateway

Forwarding Policy:

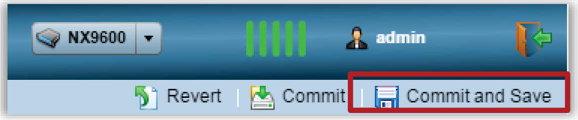
10. A user defined Profile named noc-rfs6000 has now been created:



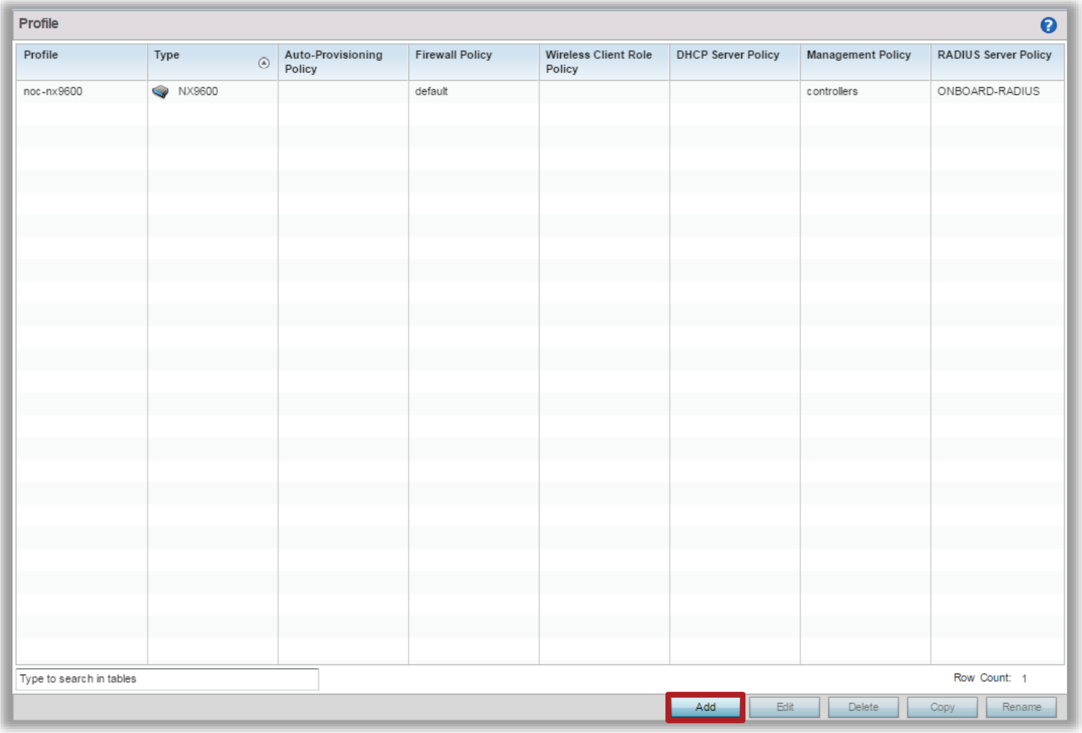
Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
noc-nx9600	NX9600		default			controllers	ONBOARD-RADIUS

11. Commit the changes:



12. Click Add to create a user defined Profile for the remote Access Points:



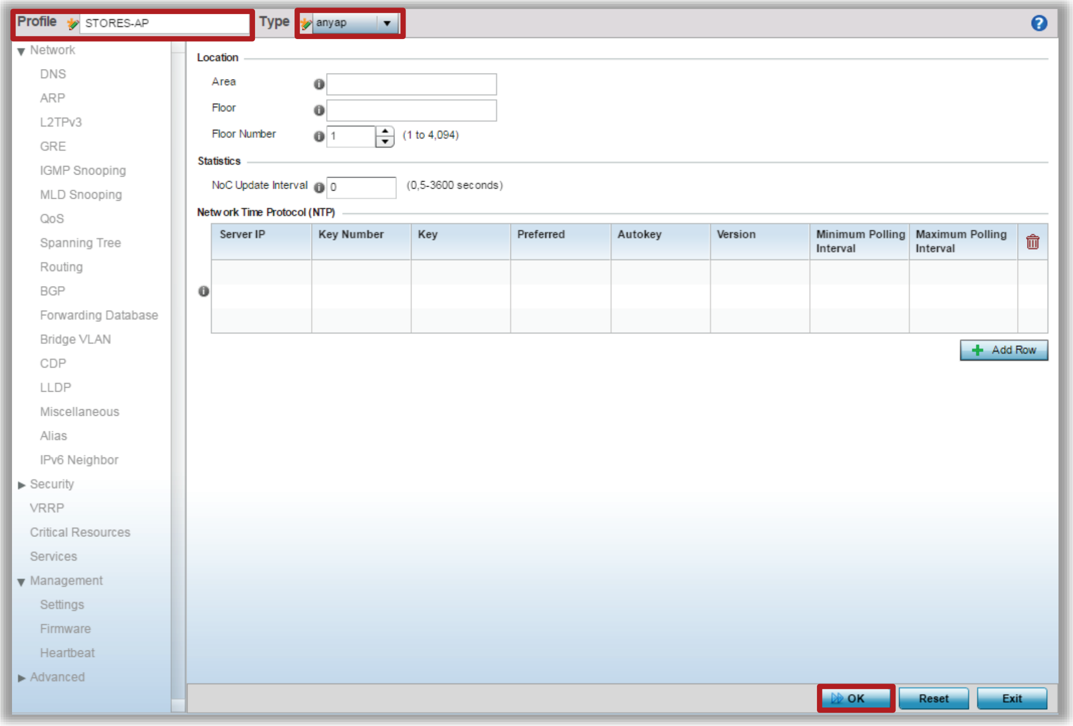
Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
noc-nx9600	NX9600		default			controllers	ONBOARD-RADIUS

Type to search in tables

Row Count: 1

13. Type the Profile name STORES-AP then set the Type to anyap. Click OK:



Profile STORES-AP Type anyap

Location

Area

Floor

Floor Number 1 (1 to 4,094)

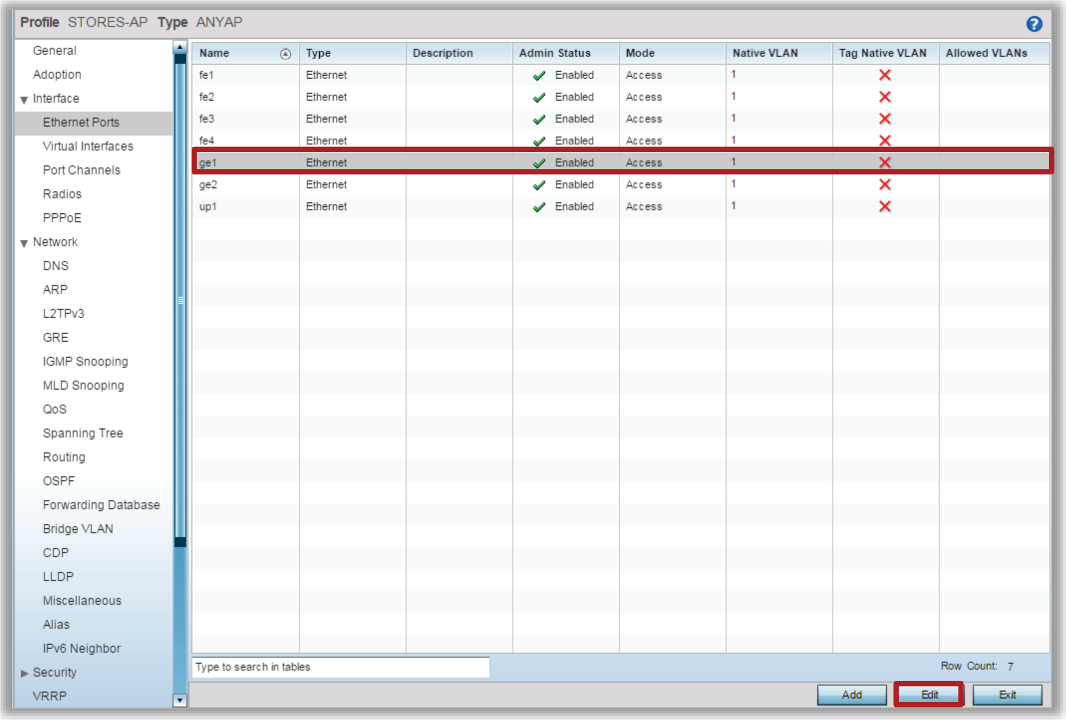
Statistics

NoC Update Interval 0 (0,5-3600 seconds)

Network Time Protocol (NTP)

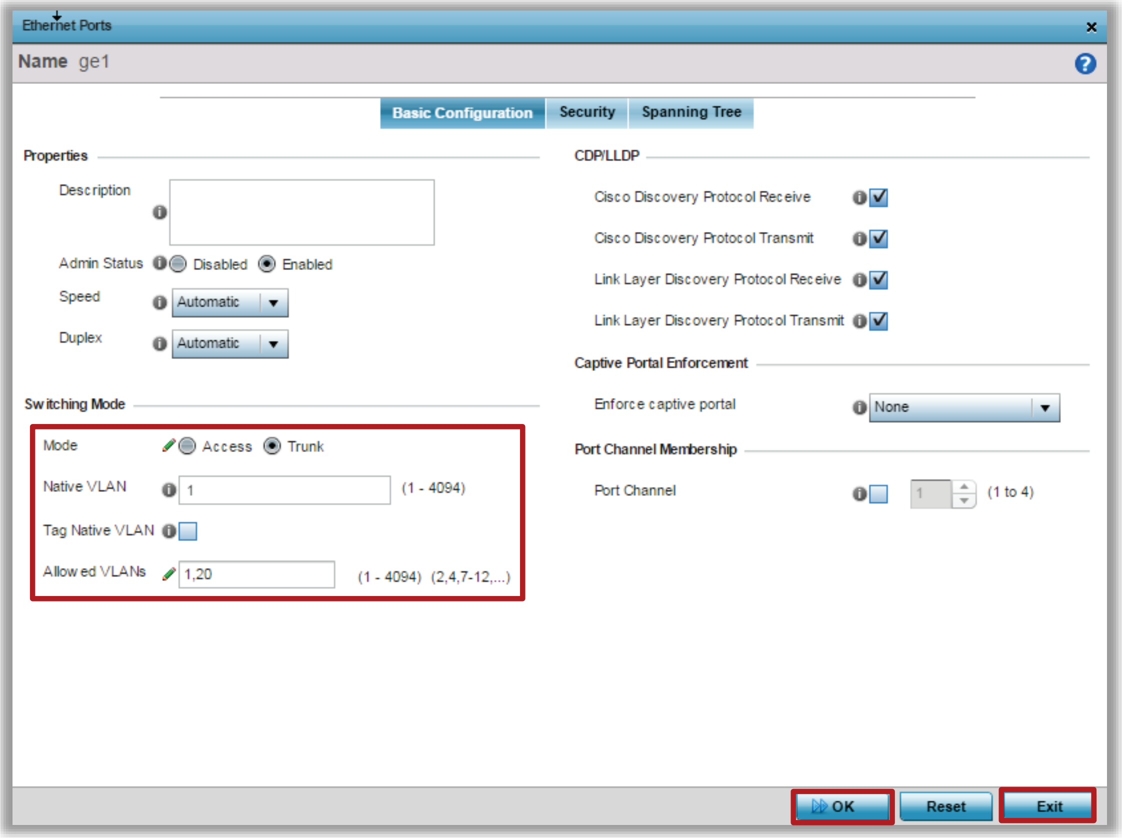
Server IP	Key Number	Key	Preferred	Autokey	Version	Minimum Polling Interval	Maximum Polling Interval

14. Select Interface -> Ethernet Ports -> ge1 -> Edit:



Name	Type	Description	Admin Status	Mode	Native VLAN	Tag Native VLAN	Allowed VLANs
fe1	Ethernet		✓ Enabled	Access	1	✗	
fe2	Ethernet		✓ Enabled	Access	1	✗	
fe3	Ethernet		✓ Enabled	Access	1	✗	
fe4	Ethernet		✓ Enabled	Access	1	✗	
ge1	Ethernet		✓ Enabled	Access	1	✗	
ge2	Ethernet		✓ Enabled	Access	1	✗	
up1	Ethernet		✓ Enabled	Access	1	✗	

15. Enter a Description then set the Switching Mode to Trunk and enter the Allowed VLANs. Click OK and Exit. Note in this example the untagged Native VLAN 1 and tagged user VLAN 20 are deployed in each of the remote stores:



Name ge1

Properties

Description

Admin Status ○ Disabled ● Enabled

Speed Automatic

Duplex Automatic

Switching Mode

Mode ○ Access ● Trunk

Native VLAN 1 (1 - 4094)

Tag Native VLAN □

Allowed VLANs 1,20 (1 - 4094) (2,4,7-12,...)

CDP/LLDP

Cisco Discovery Protocol Receive ☑

Cisco Discovery Protocol Transmit ☑

Link Layer Discovery Protocol Receive ☑

Link Layer Discovery Protocol Transmit ☑

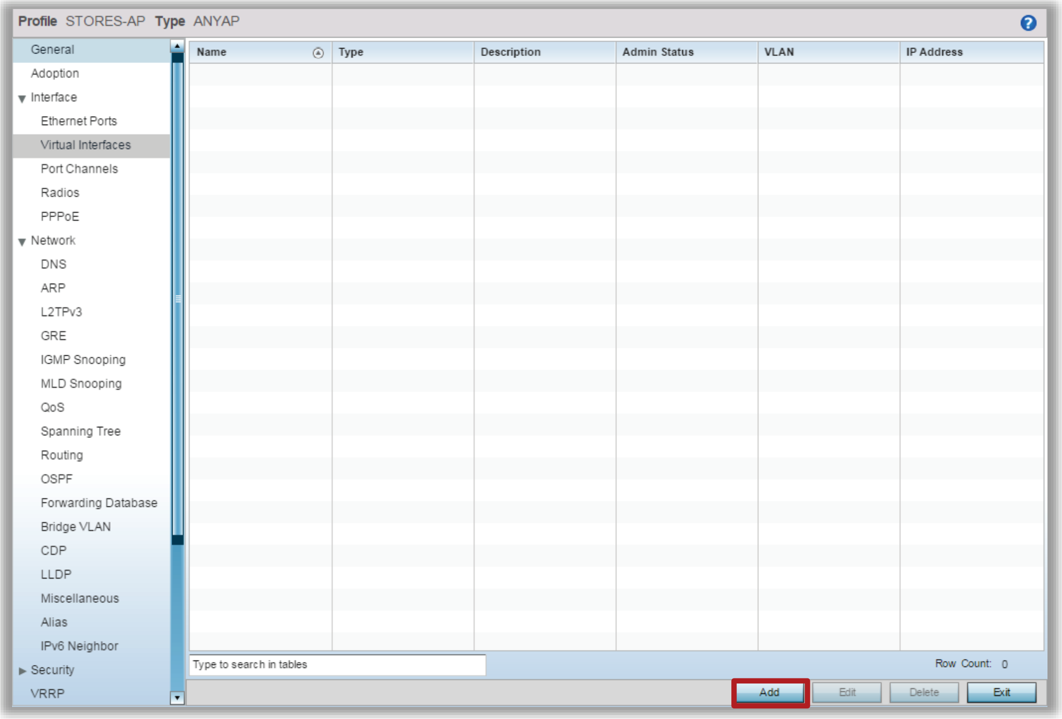
Captive Portal Enforcement

Enforce captive portal None

Port Channel Membership

Port Channel □ 1 (1 to 4)

16. Select Interface -> Virtual Interfaces -> Add:



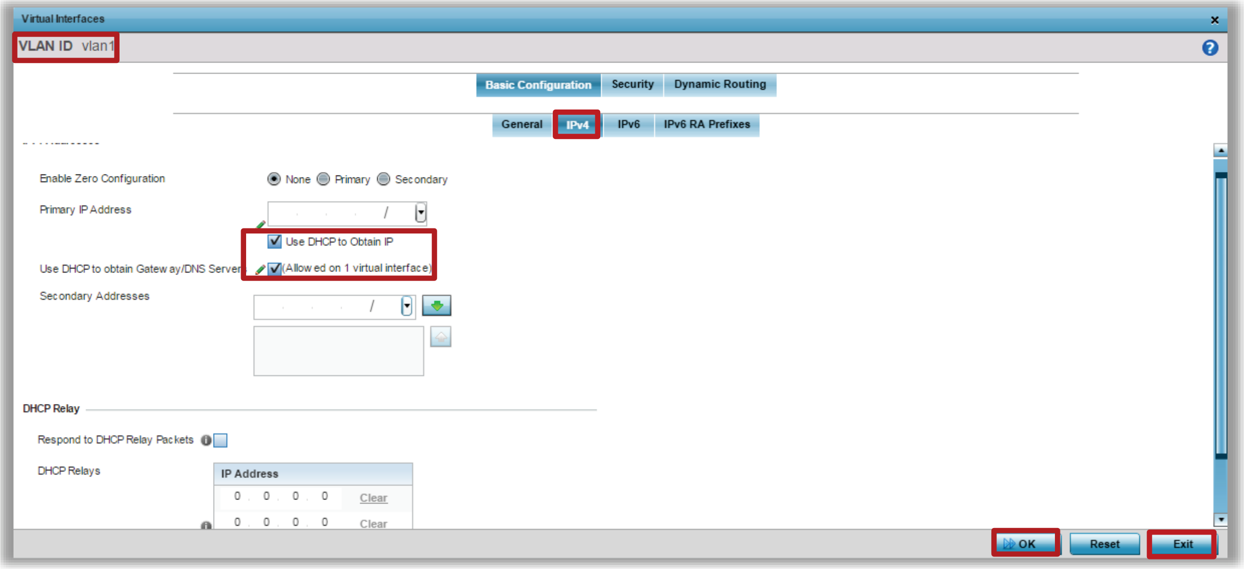
Profile STORES-AP Type ANYAP

Name	Type	Description	Admin Status	VLAN	IP Address

Type to search in tables

Row Count: 0

17. In the VLAN ID field enter the Native VLAN for the stores then select the options Use DHCP to Obtain IP and Use DHCP to obtain Gateway / DNS Servers. Click OK. Note in this example the Native ID for all the remote stores is VLAN 1:



Virtual Interfaces

VLAN ID vlan1

Enable Zero Configuration ● None ○ Primary ○ Secondary

Primary IP Address

☑ Use DHCP to Obtain IP

Use DHCP to obtain Gatew ay/DNS Server ☑ (Allow ed on 1 virtual interface)

Secondary Addresses

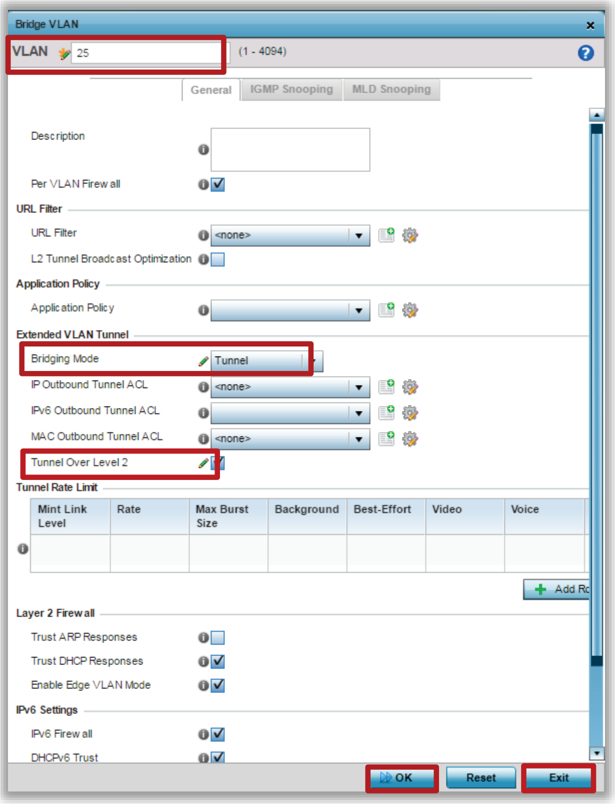
DHCP Relay

Respond to DHCP Relay Packets □

DHCP Relays

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

18. Select Network -> Bridge VLAN -> Add. Define an Extended VLAN 25 for the Guest Traffic. Enable tunnel over Level 2 MINT. Click OK and then Exit:



Bridge VLAN

VLAN 25 (1 - 4094)

General | IGMP Snooping | MLD Snooping

Description

Per VLAN Firewall ☑

URL Filter

URL Filter <none>

L2 Tunnel Broadcast Optimization □

Application Policy

Application Policy

Extended VLAN Tunnel

Bridging Mode Tunnel

IP Outbound Tunnel ACL <none>

IPv6 Outbound Tunnel ACL

MAC Outbound Tunnel ACL <none>

Tunnel Over Level 2 ☑

Tunnel Rate Limit

Mint Link Level	Rate	Max Burst Size	Background	Best-Effort	Video	Voice

Add Ro

Layer 2 Firewall

Trust ARP Responses □

Trust DHCP Responses ☑

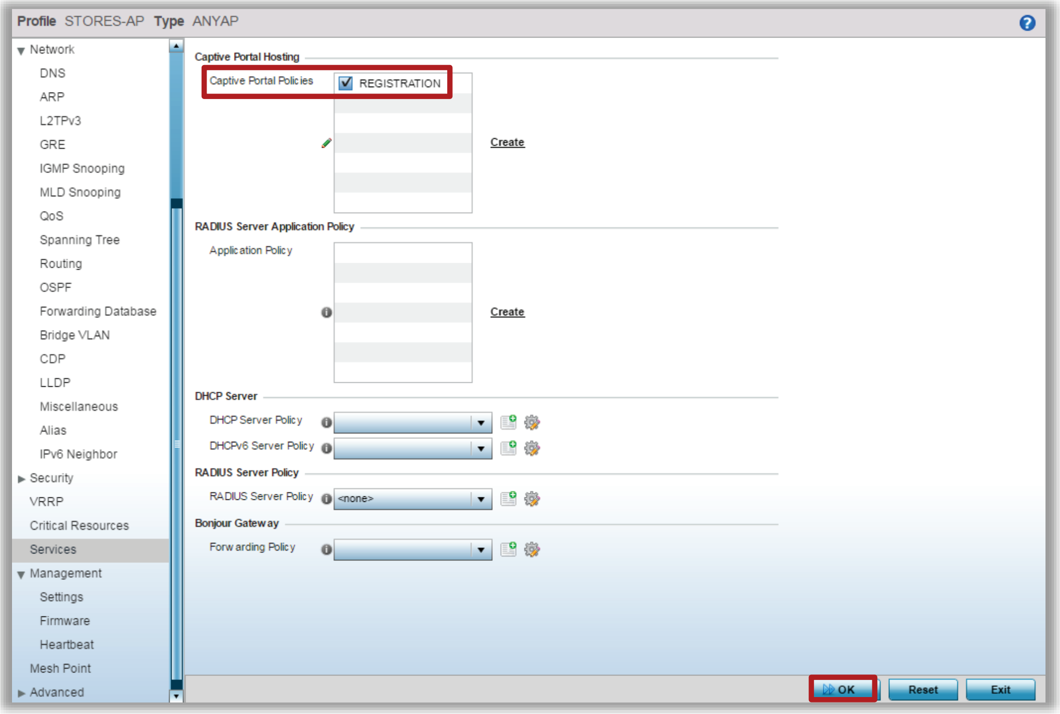
Enable Edge VLAN Mode ☑

IPv6 Settings

IPv6 Firewall ☑

DHCPv6 Trust ☑

19. Select Services. Assign Captive Portal Policy named REGISTRATION to start the hotspot sever. Click OK:



Profile STORES-AP Type ANYAP

Captive Portal Hosting

Captive Portal Policies ☑ REGISTRATION

Create

RADIUS Server Application Policy

Application Policy

Create

DHCP Server

DHCP Server Policy

DHCPv6 Server Policy

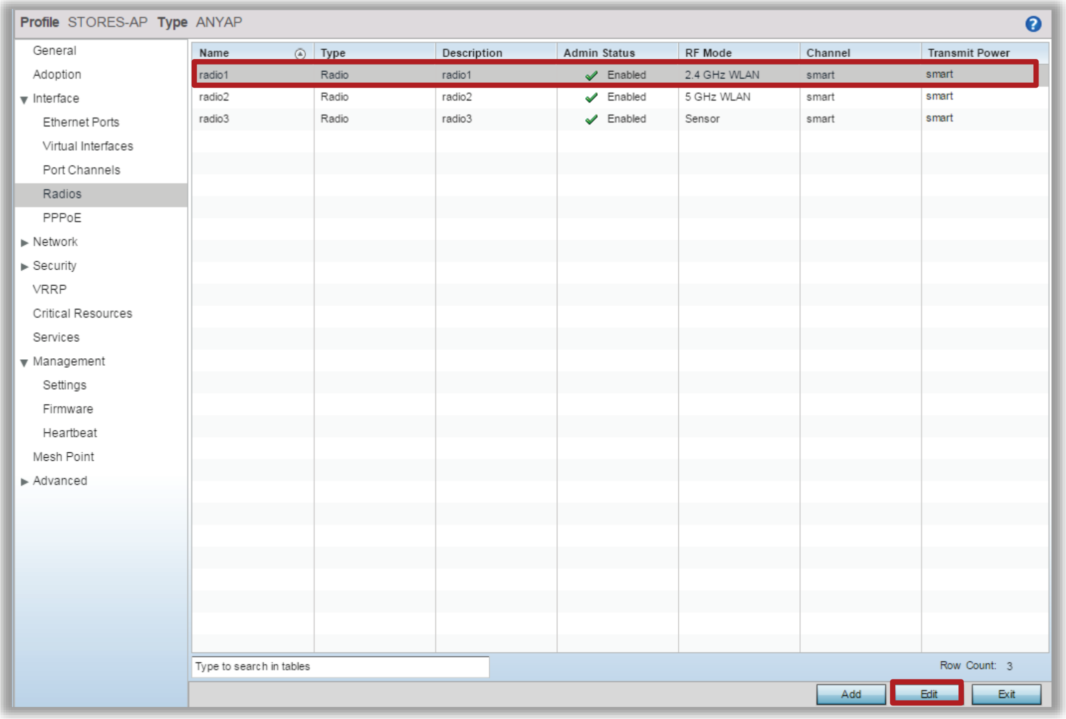
RADIUS Server Policy

RADIUS Server Policy <none>

Bonjour Gateway

Forwarding Policy

20. Select Interface -> Radios -> radio1 -> Edit:

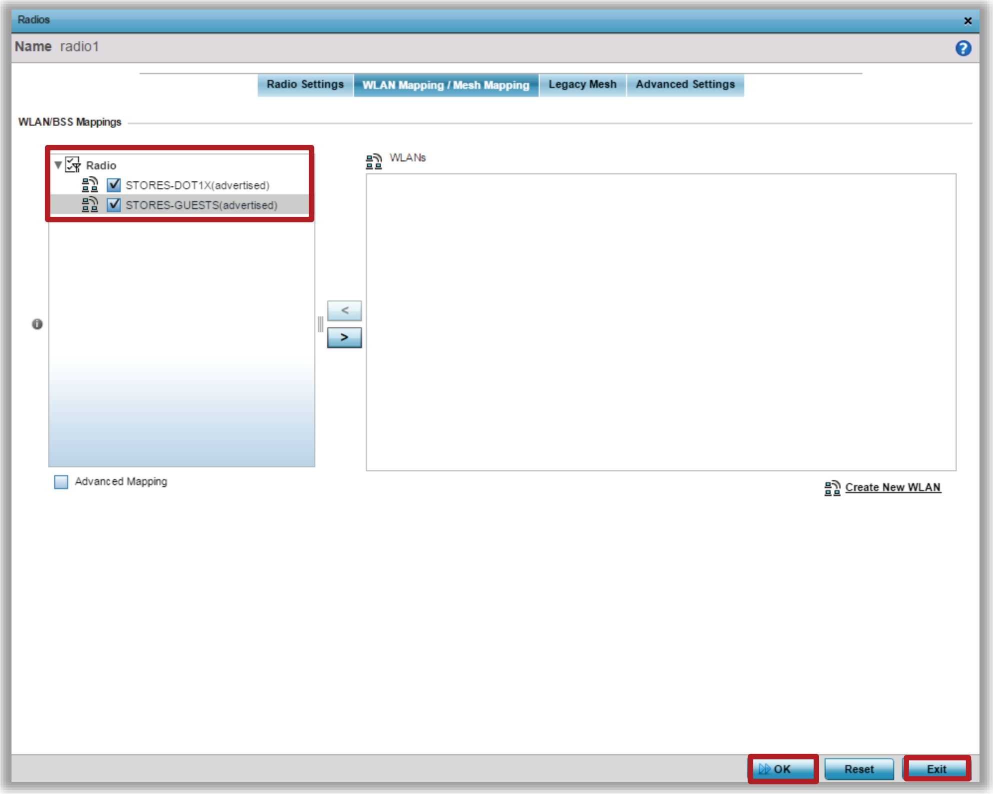


Profile STORES-AP **Type** ANYAP

Name	Type	Description	Admin Status	RF Mode	Channel	Transmit Power
radio1	Radio	radio1	✓ Enabled	2.4 GHz WLAN	smart	smart
radio2	Radio	radio2	✓ Enabled	5 GHz WLAN	smart	smart
radio3	Radio	radio3	✓ Enabled	Sensor	smart	smart

Row Count: 3

21. Select WLAN Mapping then select and Add one or more Wireless LANs to the 2.4 GHz radio. Click OK then Exit. Note in this example the Wireless LANs named STORES-DOT1X and STORES-GUESTS have been assigned to the 2.4 GHz radio:

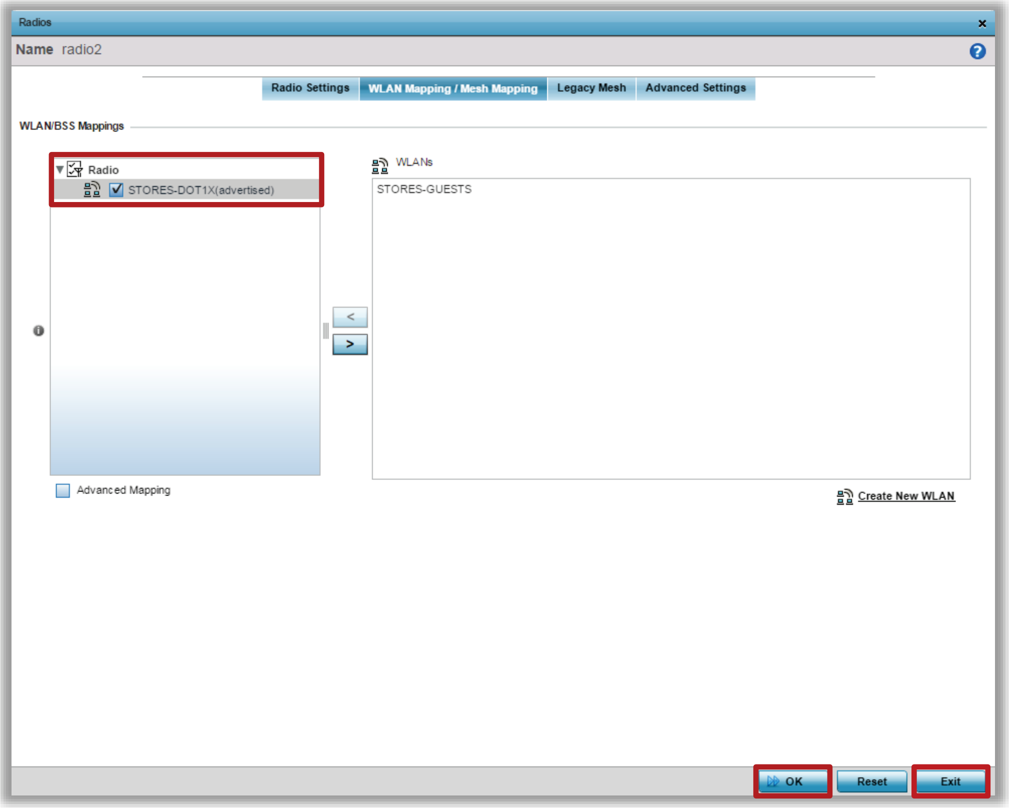


Name radio1

Radio
☑ STORES-DOT1X(advertised)
☑ STORES-GUESTS(advertised)

□ Advanced Mapping

22. Select radio2 then click Edit. Select WLAN Mapping then select and Add one or more Wireless LANs to the 5 GHz radio. Click OK then Exit. Note in this example the Wireless LAN named STORES-DOT1X has been assigned to the 5 GHz radio:



Radios

Name radio2

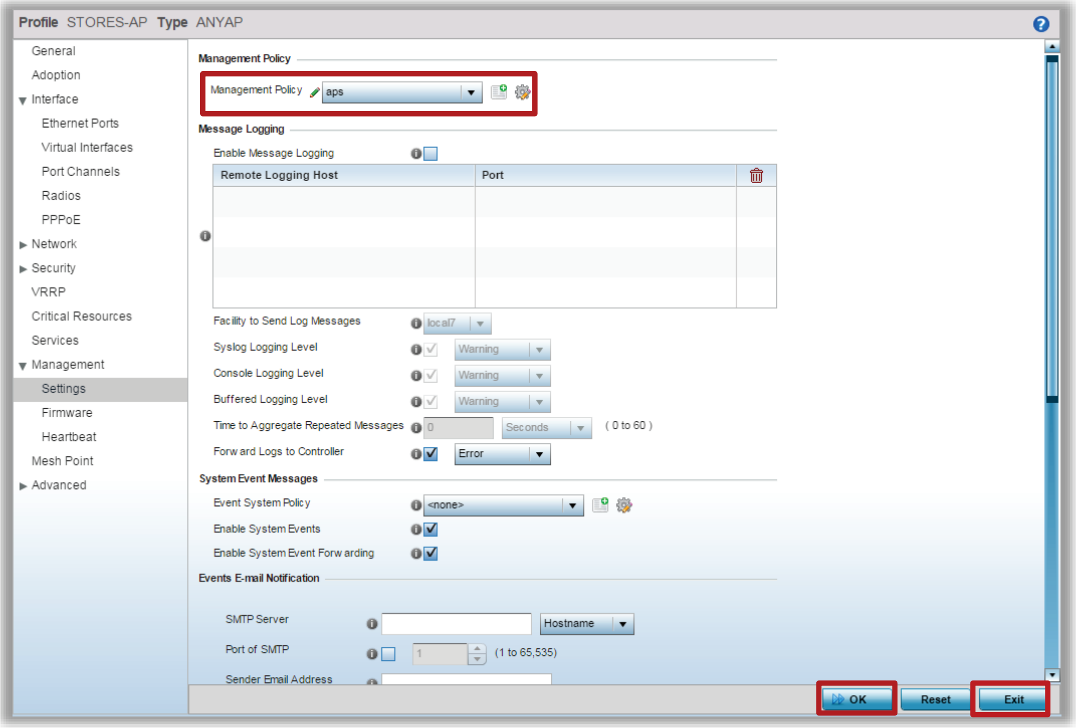
WLAN/BSS Mappings

Radio
- ☑ STORES-DOT1X(advertised)

WLANs
- STORES-GUESTS

□ Advanced Mapping

23. Select Management -> Settings. Assign the user defined Management Policy named aps then click OK then Exit:



Profile STORES-AP Type ANYAP

Management Policy

Management Policy: aps

Message Logging

Enable Message Logging □

Remote Logging Host	Port

Facility to Send Log Messages: local7

Syslog Logging Level ☑ Warning

Console Logging Level ☑ Warning

Buffered Logging Level ☑ Warning

Time to Aggregate Repeated Messages □ 0 Seconds (0 to 60)

Forward Logs to Controller ☑ Error

System Event Messages

Event System Policy: <none>

Enable System Events ☑

Enable System Event Forwarding ☑

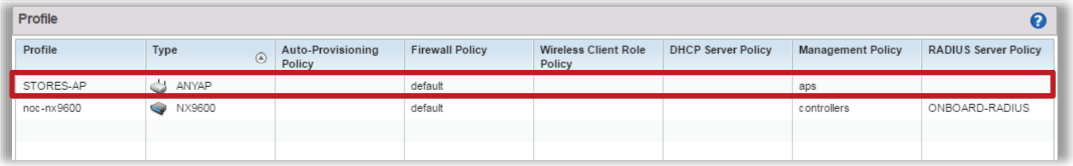
Events E-mail Notification

SMTP Server: Hostname

Port of SMTP □ 1 (1 to 65,535)

Sender Email Address

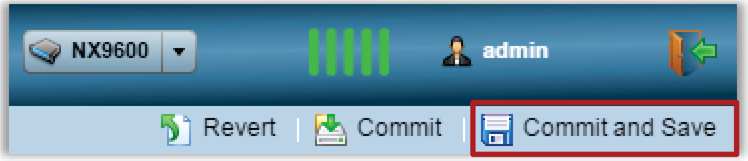
24. A user defined Profile named STORES-AP has now been created:



Profile

Profile	Type	Auto-Provisioning Policy	Firewall Policy	Wireless Client Role Policy	DHCP Server Policy	Management Policy	RADIUS Server Policy
STORES-AP	ANYAP		default			aps	
noc-nx9600	NX9600		default			controllers	ONBOARD-RADIUS

25. Commit then Save the changes:



Configuration – Device Overrides

In the previous step we defined a user defined Profiles which assigned common configuration parameters to the Wireless Controllers in the data center and the remote Access Points. Device configuration allows configuration parameters and Policies to be assigned to individual devices which are referred to as Overrides. Device Overrides allow device specific parameters such as static IP addresses, cluster configuration parameters and hostnames to be assigned to individual devices. In Configuration parameters and Policies can be defined that Override specific configuration parameters and Policies inherited from a Profile.

Cluster Master Configuration

For this configuration step the Wireless Controller that is designated as the Cluster Master will be assigned the following Device Configuration:

1. The default VLAN 1 will be removed (not applicable for the RFS 7000 or NX 9x00).
2. The Profile named noc-nx9000 will be assigned.
3. The RF Domain named noc will be assigned.
4. The Hostname will be set to nx9610-1.
5. A Virtual IP Interface for VLAN 96 will be created and the static IP address 192.168.96.7/24 assigned.
6. A default route pointing to 192.168.96.3 will be defined.
7. The cluster name will be set to NOC-CLUSTER.
8. The cluster priority will be set to 255 (highest value becomes the master).
9. A Level 2 IP MINT Link will be defined pointing to the Cluster Members IP address 192.168.96.8.

Cluster Master Configuration – CLI

Use the following procedure to modify the Device configuration for the Cluster Master controller using the Command Line Interface:

1. Access the Device configuration of the Cluster Master and assign the user defined RF Domain named noc and user defined Profile named noc-nx9600:

```
nx9600-7F34C7# self
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# use profile noc-nx9600
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# use rf-domain noc
```

2. If applicable remove the default Virtual IP Interface for VLAN 1:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# remove-override interface vlan 1
```

3. Define a Hostname for the device. Note in this example the hostname rfs6000-1 is assigned:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# hostname nx9600-1
```

4. Create a Virtual IP Interface for the Native VLAN and assign a static IP address. Note in this example a Virtual IP interface for VLAN 20 has been created and the static IP address 192.168.20.22/24 assigned:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# interface vlan 96
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7-if-vlan96)# description Management
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7-if-vlan96)# ip address 192.168.96.7/24
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7-if-vlan96)# exit
```

5. Assign a default gateway. Note in this example the default gateway for VLAN 20 is 192.168.20.1:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# ip default-gateway 192.168.96.3
```

6. Define a Cluster Name, Cluster Member IP Address and set the Cluster Priority to 255 (Master). Note in this example the Cluster Name is set to NOC-CLUSTER and the Cluster Members IP address is 192.168.96.8. In addition, the MINT link level between the cluster peers is set to Level 2:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# cluster name NOC-CLUSTER
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# cluster member ip 192.168.96.8 level 2
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# cluster master-priority 255
```

7. Verify the changes:

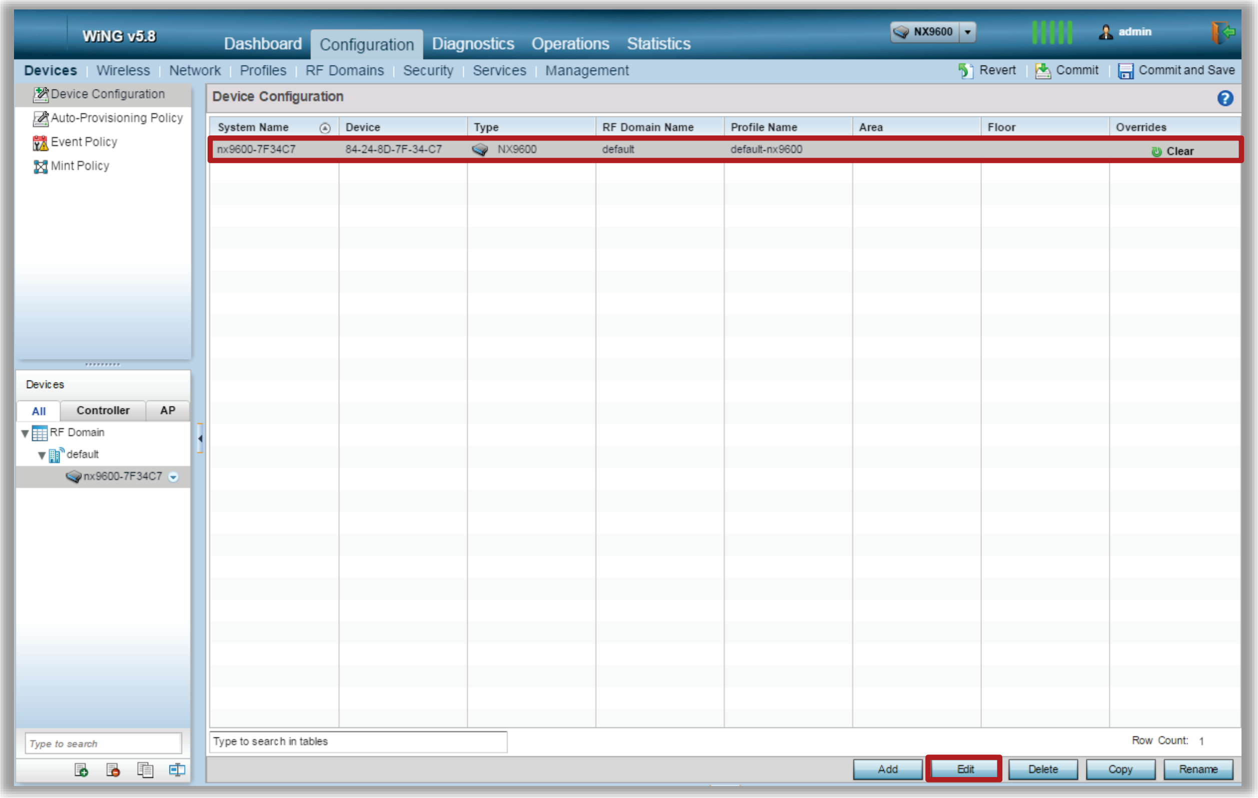
```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# show context
nx9600 84-24-8D-7F-34-C7
 use profile noc-nx9600
 use rf-domain noc
 hostname nx9610-1
 license AAP 8b3a5e5c1875a4482ccafbed015dce11f9203ffa9bbda954407e95e15fe0b347e394ca5fb0f7d813
 license ADSEC 8b3a5e5c1875a4485e0bddf84e41b5fdf9203ffa9bbda9541b80b1d0e2dcffc2ea32ba79ee6faa6f
 ip default-gateway 192.168.96.1
 interface vlan96
  ip address 192.168.96.7/24
 cluster name NOC-CLUSTER
 cluster member ip 192.168.96.8 level 2
 cluster master-priority 255
 logging on
 logging console warnings
 logging buffered debugging
```

8. Exit the Device configuration then commit and save the changes:

```
nx9600-7F34C7(config-device-84-24-8D-7F-34-C7)# exit
nx9600-7F34C7(config)# commit write
```

Cluster Master Configuration – Web UI

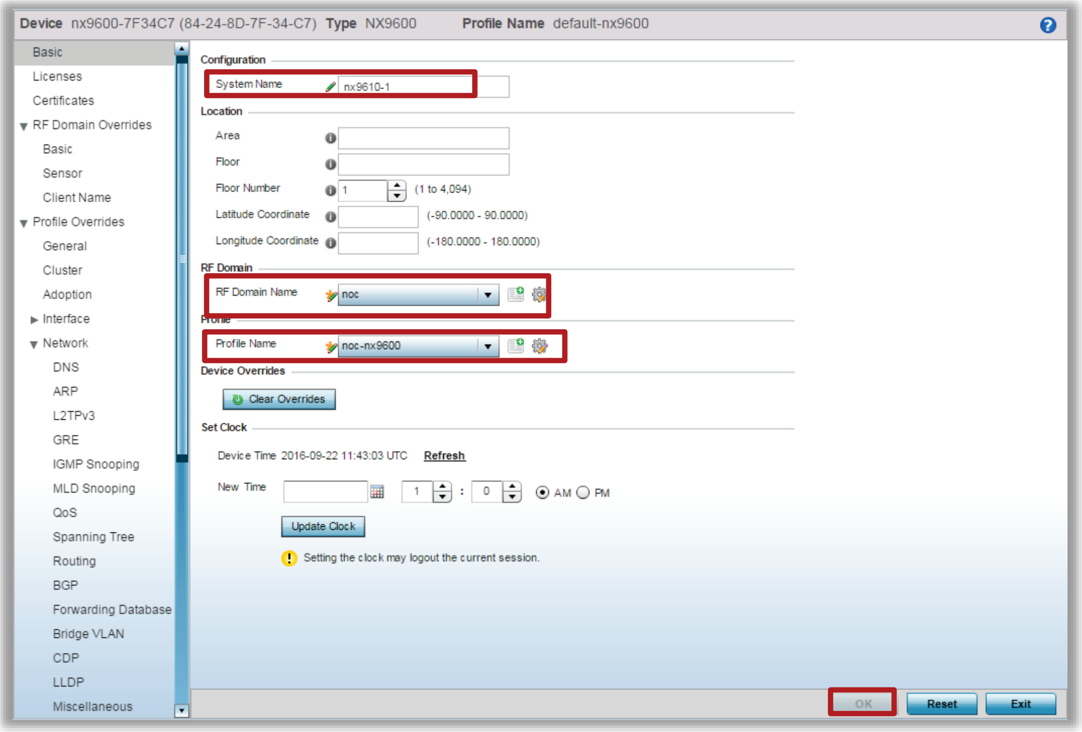
1. Select Configuration -> Devices -> <device> -> Edit:



Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
nx9600-7F34C7	84-24-8D-7F-34-C7	NX9600	default	default-nx9600			Clear

2. Set the System Name to nx9610-1 then assign the user defined RF Domain named noc and the Profile named noc-nx9600. Click OK:



Device nx9600-7F34C7 (84-24-8D-7F-34-C7) Type NX9600 Profile Name default-nx9600

Configuration

System Name: nx9610-1

Location

Area:

Floor:

Floor Number: 1 (1 to 4,094)

Latitude Coordinate: (-90.0000 - 90.0000)

Longitude Coordinate: (-180.0000 - 180.0000)

RF Domain

RF Domain Name: noc

Profile

Profile Name: noc-nx9600

Device Overrides

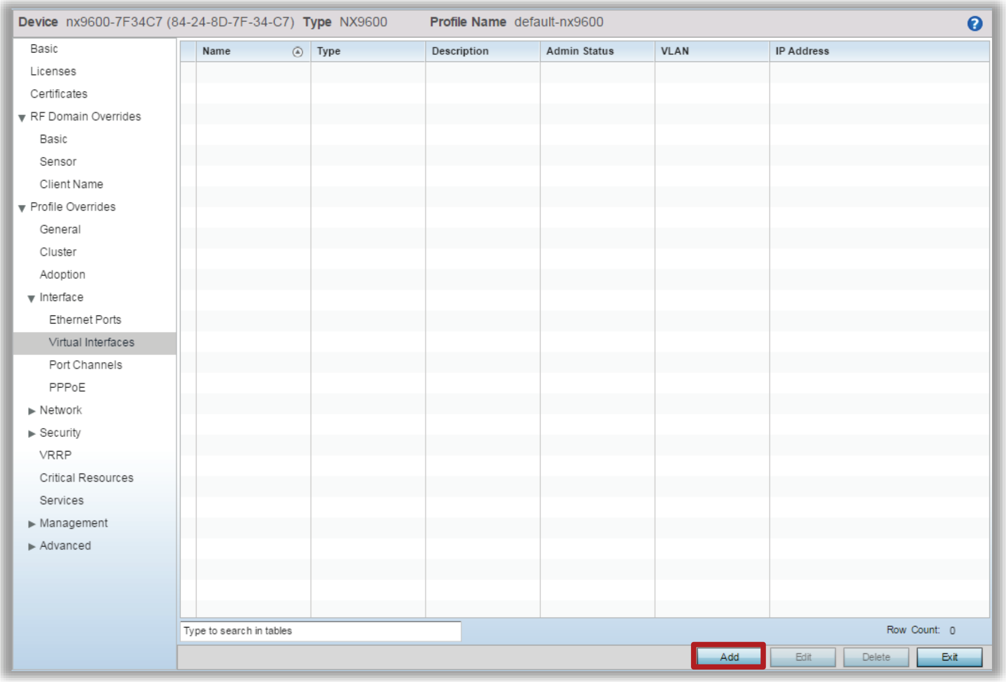
Set Clock

Device Time 2016-09-22 11:43:03 UTC

New Time: 1 : 0 ● AM ○ PM

Setting the clock may logout the current session.

3. Select Profile Overrides -> Interface -> Virtual Interfaces. If present, select vlan1 then click Delete. Click Add to create a new interface for the Native VLAN 96:

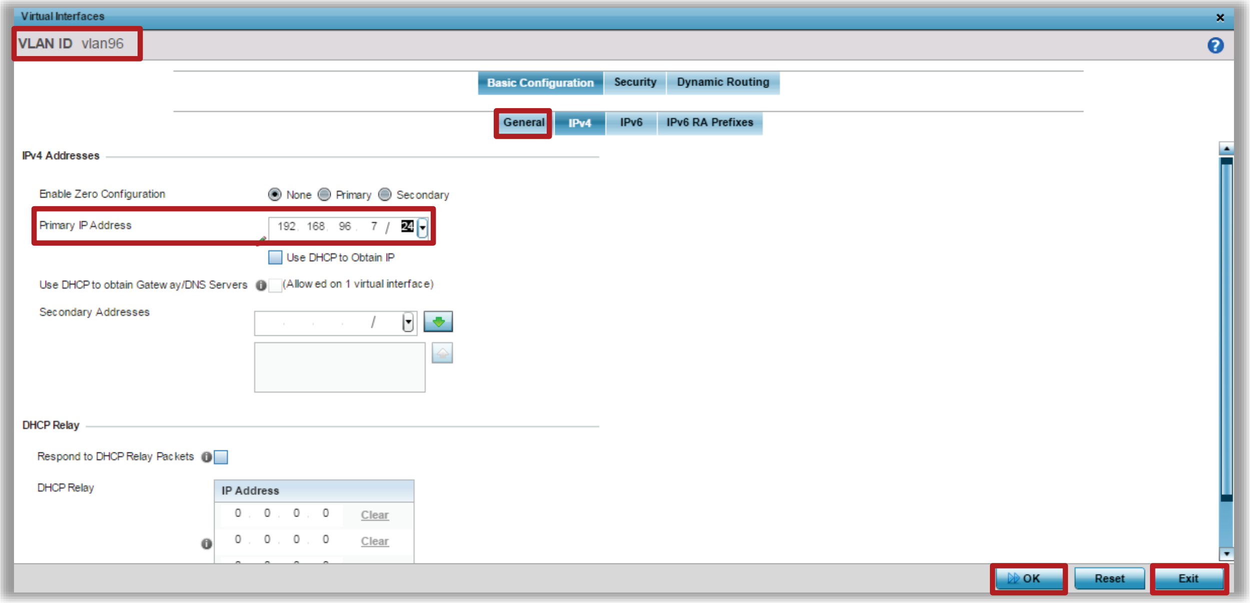


Device nx9600-7F34C7 (84-24-8D-7F-34-C7) Type NX9600 Profile Name default-nx9600

Name	Type	Description	Admin Status	VLAN	IP Address

Row Count: 0

4. Enter a VLAN ID, Description and Primary IP Address then click OK then Exit. Note that in this example the Cluster Masters IP address on VLAN 96 is 192.168.96.7/24:



Virtual Interfaces

VLAN ID vlan96

IPv4 Addresses

Enable Zero Configuration ● None ○ Primary ○ Secondary

Primary IP Address 192 . 168 . 96 . 7 / 24

□ Use DHCP to Obtain IP

Use DHCP to obtain Gateway/DNS Servers □ (Allowed on 1 virtual interface)

Secondary Addresses

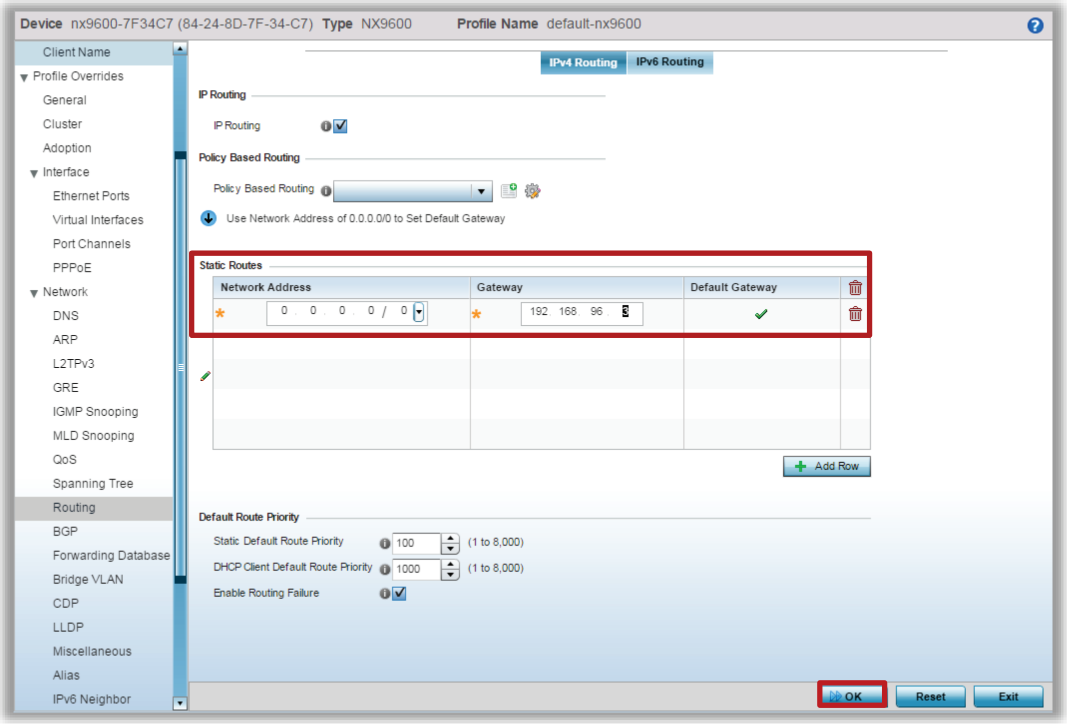
DHCP Relay

Respond to DHCP Relay Packets □

DHCP Relay

IP Address	
0 . 0 . 0 . 0	Clear
0 . 0 . 0 . 0	Clear

5. Select Profile Overrides -> Network -> Routing. Click Add Row and add a default route to 0.0.0.0/0 network:



Device nx9600-7F34C7 (84-24-8D-7F-34-C7) Type NX9600 Profile Name default-nx9600

IP Routing

IP Routing ☑

Policy Based Routing

Policy Based Routing

Use Network Address of 0.0.0.0/0 to Set Default Gateway

Static Routes

Network Address	Gateway	Default Gateway
0 . 0 . 0 . 0 / 0	192 . 168 . 96 . 3	✓

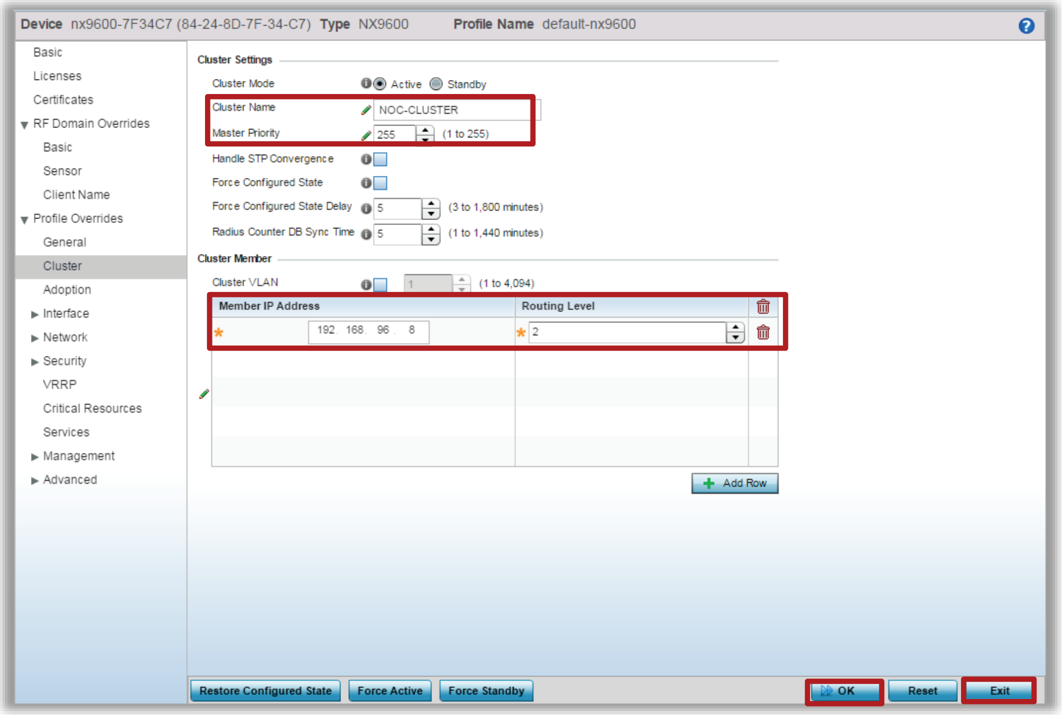
Default Route Priority

Static Default Route Priority 100 (1 to 8,000)

DHCP Client Default Route Priority 1000 (1 to 8,000)

Enable Routing Failure ☑

6. Select Profile Overrides -> Cluster. In the Cluster Name field enter NOC-CLUSTER then set the Master Priority to 255. Under Cluster Member click Add Row. Enter the IP Address assigned to the Cluster Member then set the Routing Level to 2. Note that in this example the Cluster Member is assigned the static IP address 192.168.96.8:



Device nx9600-7F34C7 (84-24-8D-7F-34-C7) **Type** NX9600 **Profile Name** default-nx9600

Cluster Settings

Cluster Mode ● Active ○ Standby

Cluster Name NOC-CLUSTER

Master Priority 255 (1 to 255)

Handle STP Convergence □

Force Configured State □

Force Configured State Delay 5 (3 to 1,800 minutes)

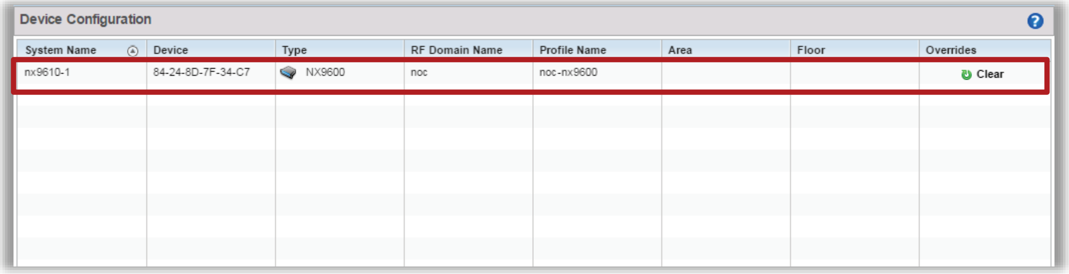
Radius Counter DB Sync Time 5 (1 to 1,440 minutes)

Cluster Member

Cluster VLAN □ 1 (1 to 4,094)

Member IP Address	Routing Level
192 168 96 8	2

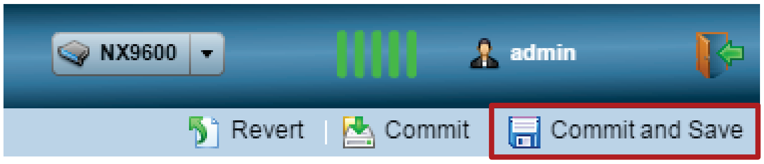
7. The Device configuration for the Cluster Master switch is now completed:



Device Configuration

System Name	Device	Type	RF Domain Name	Profile Name	Area	Floor	Overrides
nx9610-1	84-24-8D-7F-34-C7	NX9600	noc	noc-nx9600			Clear

8. Commit then Save the changes:



Cluster Slave Configuration

For this configuration step the Wireless Controller that is designated as the Cluster Member will be assigned the following Device Configuration. Only minimal networking configuration is required in order to join the secondary controller to cluster:

1. GE1 port configuration would be changed in the default profile to allow VLAN 96 as NATIVE.
2. The **Hostname** will be set to **nx9610-2**.
3. A **Virtual IP Interface** for **VLAN 96** will be created and the IP address **192.168.96.8/24** assigned.
4. A default route pointing to **192.168.96.3** will be defined.

   Automatic Join-Cluster will be initiated to the Cluster Master controller.

Cluster Slave Configuration – CLI Only

Use the following procedure to modify the Device configuration for the Cluster Member using the Command Line Interface:

1. Login to the Secondary Controller and navigate to the default NX9600 profile:

```
nx9600-67C3A1(config)# profile nx9600 default-nx9600
```

2. Change the GE1 configuration to Trunk and set VLAN 96 as NATIVE:

```
nx9600-67C3A1(config-profile-default-nx9600)# interface ge1
nx9600-67C3A1(config-profile-default-nx9600-if-ge1)# switchport mode trunk
nx9600-67C3A1(config-profile-default-nx9600-if-ge1)# switchport native vlan 96
nx9600-67C3A1(config-profile-default-nx9600-if-ge1)# self
```

3. Define a Hostname for the device. Note in this example the hostname nx9610-2 is assigned:

```
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1)# hostname nx9610-2
```

4. Create a Virtual IP Interface for the Native VLAN and assign a static IP address. Note in this example a Virtual IP interface for VLAN 96 has been created and the static IP address 192.168.96.8/24 assigned:

```
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1)# interface vlan 96
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1-if-vlan96)# ip address 192.168.96.8/24
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1-if-vlan96)# exit
```

5. Assign a default gateway. Note in this example the default gateway for VLAN 96 is 192.168.96.3:

```
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1)# ip default-gateway 192.168.96.3
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1)# commit write
nx9600-67C3A1(config-device-84-24-8D-67-C3-A1)# end
```

6. Use join-cluster command to join the Master controller. Use standby mode and Level 2 MINT:

```
nx9610-2#join-cluster 192.168.96.7 user admin password wingsecure mode standby level 2
… connecting to 192.168.96.7
… applying cluster configuration
… committing the changes
… saving the changes
[OK]
```

7. Verify the changes:

```
nx9600-1# show cluster members
------------------------------------------------------------------------------------------
   HOSTNAME    MEMBER-ID            MAC            MASTER OPERATIONAL-STATE    LAST-SEEN
------------------------------------------------------------------------------------------
  nx9610-1    4D.7F.34.C7    84-24-8D-7F-34-C7    True    active              self
  nx9610-2    4D.67.C3.A1    84-24-8D-67-C3-A1    False   standby             00:01:02
------------------------------------------------------------------------------------------
nx9600-1# show cluster status
Cluster Runtime Information
 Protocol version            : 1
 Cluster state               : active
 AP license                  : 0
 AAP license                 : 512
 AP count                    : 0
 AAP count                   : 0
 Max AP adoption capacity    : 10240
 Number of connected member(s): 1
```

Automatic Provisioning Policies

By default, WING 5 devices are assigned to a default RF Domain and device Profile based on their model type. Automatic Provisioning Policies provide a mechanism that allows the Wireless Controllers in the data center to automatically assign a user defined Profile and RF Domain to remote Access Points as they are initially discovered and adopted by a Wireless Controller. Without Automatic Provisioning Policies an administrator would have to manually assign the correct user defined Profile and RF Domain to each individual Access Point.

Automatic Provisioning Policies contain one or more rules for each model of Access Point with match conditions and values that assigns the correct user defined Profile and RF Domain during initial adoption. For data center deployments these rules are typically based on the IP subnet the Access Points are connected too, however matches can also be made based on other values such as a location provided by CDP or LLDP advertisements from the Ethernet infrastructure deployed at the remote site.

For this configuration step an Automatic Provisioning Policy with two rules will be created with the following parameters:

1. An Automatic Provisioning Policy named AUTO-ADOPTION will be created and assigned to the NX 9600 Profile named noc-nx9600.
    a. An anyap rule for store 100 assigning the user defined RF Domain named store100 and user defined Profile named STORES-AP will be defined with a wildcard match based on the CDP snoop from the wired switch. This rule will work for both store100 and store101 or other stores, assuming switch naming convention is the same across stores.

Note
At least one Automatic Provisioning Policy rule will be required for each remote site. As rules can be either Access Point model dependent or can apply for any AP model type.

Note
Web UI does not allow usage of wildcard based auto provisioning rules. In this example only CLI examples will be provided.

Auto Provisioning Policy Configuration – CLI

Use the following procedure to create and assign Automatic Provisioning Policy and rules using the Command Line Interface:

1. Create an Automatic Provisioning Policy named noc with rules. In this example two rules will be defined for AP 6532 Access Points that assigns the user defined Profile named STORES-AP and RF Domain store100 or store101 based on the CDP match of the Ethernet Switch Access Points are connected to:

```
nx9610-1(config)# auto-provisioning-policy AUTO-ADOPTION
nx9610-1(config-auto-provisioning-policy-AUTO-ADOPTION)# adopt anyap precedence 1 profile STORES-AP rf-
domain store$CDP[8:10] any
```

2. Verify the changes:

```
nx9610-1(config-auto-provisioning-policy-AUTO-ADOPTION)# show context
auto-provisioning-policy AUTO-ADOPTION
 adopt anyap precedence 1 profile STORES-AP rf-domain store$CDP[8:10] any
```

3. Exit the Automatic Provisioning Policy configuration:

```
nx9610-1(config-auto-provisioning-policy-AUTO-ADOPTION)# exit
```

4. Access the NX9600 Profile and assign the Automatic Provisioning Policy:

```
nx9610-1(config)# profile nx9600 noc-nx9600
nx9610-1(config-profile-noc-nx9600)# use auto-provisioning-policy AUTO-ADOPTION
```

5. Verify the changes:

```
nx9610-1(config-profile-noc-nx9600)# show context
profile nx9600 noc-nx9600
 bridge vlan 25
  l2-tunnel-broadcast-optimization
  bridging-mode tunnel
  tunnel-over-level2
  ip igmp snooping
  ip igmp snooping querier
  ipv6 mld snooping
  ipv6 mld snooping querier
 no autoinstall configuration
 no autoinstall firmware
 no device-upgrade auto
 use radius-server-policy ONBOARD-RADIUS
 interface xge1
 interface xge2
 interface xge3
 interface xge4
 interface ge1
  description Uplink
  switchport mode trunk
  switchport trunk native vlan 96
  no switchport trunk native tagged
  switchport trunk allowed vlan 25,96
 interface ge2
 use management-policy controllers
 use firewall-policy default
 use auto-provisioning-policy AUTO-ADOPTION
 logging on
 logging buffered debugging
 service pm sys-restart
!
```

6. 6 Exit the Profile configuration then commit and save the changes:

```
nx9610-1(config-profile-noc-nx9600)# exit
nx9610-1(config)# commit write
```

DHCP Services

To support remote plug-n-play Access Point deployments, the Access Points at each remote site will require DHCP services on their Native VLAN for network addressing as well as WING DHCP option 191 parameters and values to discover the Wireless Controllers located in the data center. The DHCP deployment maybe centralized using DHCP services located in the data center or distributed using DHCP services deployed locally at each site.

In a centralized deployment model the remote Access Points use DHCP option 191 to form Level 2 IP based MINT links to the Wireless Controllers in the data center. The WING Option 191 parameters and values provide remote Access Points with the IP Addresses and/or Hostnames of the Wireless Controllers along with the MINT level the Access Points should utilize to communicate with the Wireless Controllers. The option 191 parameters and value can also be utilized to assign advanced parameters such as the UDP port used for MINT encapsulation in addition to timers.

The following table provides some example standard WING DHCP option 191 values which can be utilized for most centralized based deployments:

Standard DHCP Option 191 Values:

```
pool1=192.168.96.7,192.168.96.8;level=2
pool1=nx9610-1.tmelabs.local;nx9610-2.tmelabs.local;level=2
```

Advanced DHCP Option 191 Parameters

WING 5.2.1 and above introduces three new WING DHCP option 191 parameters which can be enabled to address challenges in more advanced deployments. The advanced parameters and values can be utilized to provide remote Access Points with the UDP port used for MINT encapsulation in addition to the timers used to exchange MINT hello packets and how long the Controller waits between hello intervals before determining a remote Access Point is offline:

- udp-port – Defines the UDP port used for MINT encapsulation over IP (default 24576).
- hello-interval – Defines the interval between MINT hello packets exchanged between the data center Controllers and Access Points (default 15).
- adjacency-hold-time – Defines the maximum period since the last MINT hello packet was received before the MINT link is considered down (default 45).
- rf-domain – Defines unique rf-domain tag that can be leveraged to determine the location of the Access Point to assign RF Domain and Profile via Auto Provisioning Policy.

The udp-port parameter must be supplied to the remote Access Points if the default UDP port in the MINT policy assigned on the Controllers has been modified. By default, the Controllers and remote Access Points will utilize UDP port 24576 which is defined in the global MINT policy named global-mint that is assigned to all devices. If the default UDP port is modified, the new DHCP option 191 parameters must be provided to the remote Access Points so that they know how to communicate with the centralized controllers. Failure to provide the UDP port with the DHCP option will result in adoption failures.

The hello-interval and adjacency-hold-time parameters determine the interval between MINT hello packets exchanged between the Controllers and Access Points in addition to the time interval each device waits when no MINT hello packets are received before determining the MINT link is down. By default for IP based MINT links the hello-interval is 15 seconds and the adjacency-hold-time is 45.

Increasing the default hello-interval and adjacency-hold-time parameters may be necessary in certain high-latency or oversubscribed WAN deployments to ensure that Access Points at remote sites stay on-line and are not marked as offline when default MINT timers are exceeded.

When increasing the hello-interval and adjacency-hold-time parameters it is a best practice recommendation that the hello-interval value be set to 1/3rd the adjacency-hold-time value. For example if the adjacency-hold-time value is set to 60 seconds, the hello-interval must be set to 20 seconds. The adjacency-hold-time should always be one or two seconds more than the hello-interval to maintain the MINT link.

Standard DHCP Option 191 Values:

```
pool1=192.168.96.7,192.168.96.8;udp-port=31102;level=2
pool1=nx9610-1.tmelabs.local;nx9610-2.tmelabs.local;level=2;hello-interval=20;adjacency-hold-time=61
```

Note

Any `hello-interval` and `adjacency-hold-time` values assigned from DHCP option 191 will supersede any values assigned to a Profile or directly to a device as override.

DHCP Server Implementation Examples

Cisco IOS Based DHCP Server

Cisco IOS based devices such as Routers and certain Catalyst Switches provide support for integrated DHCP services. An IOS based device at a remote store can be utilized to provide local DHCP services for the site. When an IOS based DHCP server is utilized at a store, the option 191 value must be assigned directly to the DHCP scope providing DHCP services to the Access Points Native VLAN at the store.

Use the following procedure to create a DHCP scope on a Cisco IOS based DHCP server that will assign DHCP option 191 and values from within the scope:

1. For the DHCP scope supporting the Access Points Native VLAN at the site, create a range of excluded addresses:

```
C3725-1(config)# ip dhcp excluded-address 192.168.21.1 192.168.21.99
```

2. Create a DHCP pool for the Access Points Native VLAN and define the required parameters and standard options:

```
C3725-1(config)# ip dhcp pool WINGAPs
C3725-1(dhcp-config)# import all
C3725-1(dhcp-config)# network 192.168.21.0 255.255.255.0
C3725-1(dhcp-config)# domain-name tmelabs.local
C3725-1(dhcp-config)# dns-server 192.168.10.5
C3725-1(dhcp-config)# default-router 192.168.21.1
```

3. Define WING Option 191 as an ASCII string. In this example the Access Points will be provided the Wireless Controller IP addresses 192.168.96.7 and 192.168.96.8 and will establish Level 2 IP based MINT links to the Wireless Controllers:

```
C3725-1(dhcp-config)# option 191 ascii pool1=192.168.96.7,192.168.96.8;level=2
```

4. Exit the DHCP pool then apply the changes:

```
C3725-1(dhcp-config)#  end
C3725-1# write memory
```

Linux ISC DHCP Server

Most Linux distributions provide support for the ISC DHCP server may be deployed centrally in the data center or locally at each store. The Linux DHCP server supports the ability to assign WING Option 191 values directly to each DHCP scope as well as globally across multiple scopes using the Vendor Class Identifier.

Use the following procedure to modify the **dhcpd.conf** configuration file and define an Option Code, Vendor Class and DHCP Scope. The Linux ISC DHCP server that will globally assign WING DHCP option 191 and values to Access Points across multiple DHCP scopes:

1. Define DHCP option code 191 as a String:

```
# Option Code for Wireless Controller Discovery
Option ControllerIPAddress code 191 = string;
```

2. Define the Class for each model of Access Point and assign option 191. In this example a Vendor Class Identifier for an AP 7532 has been defined. AP 7532 Access Points will be provided with the Wireless Controller IP addresses 192.168.96.7 and 192.168.96.8 and will establish Level 2 IP based MINT links to the Wireless Controllers:

```
# Vendor Class for WING 5 AP7532 Access Points
class "WingAP.AP7532" {
   match if substring(option vendor-class-identifier, 0, 17) = "WingAP.AP7532";
   option vendor-class-identifier "WingAP.AP7532";
   option ControllerIPAddress “pool1=192.168.96.7,192.168.96.8;level=2”;
}
```

3. Create a DHCP scope for the Access Points Native VLAN and define the required parameters and standard options:

```
# DHCP Scope for the Access Points Native VLAN
subnet 192.168.21.0 netmask 255.255.255.0 {
   range 192.168.21.100 192.168.21.254;
   default-lease-time 86400;
   max-lease-time 86400;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.21.255;
   option routers 192.168.21.1;
   option domain-name tmelabs.local;
   option domain-name-server 192.168.10.5;
}
```

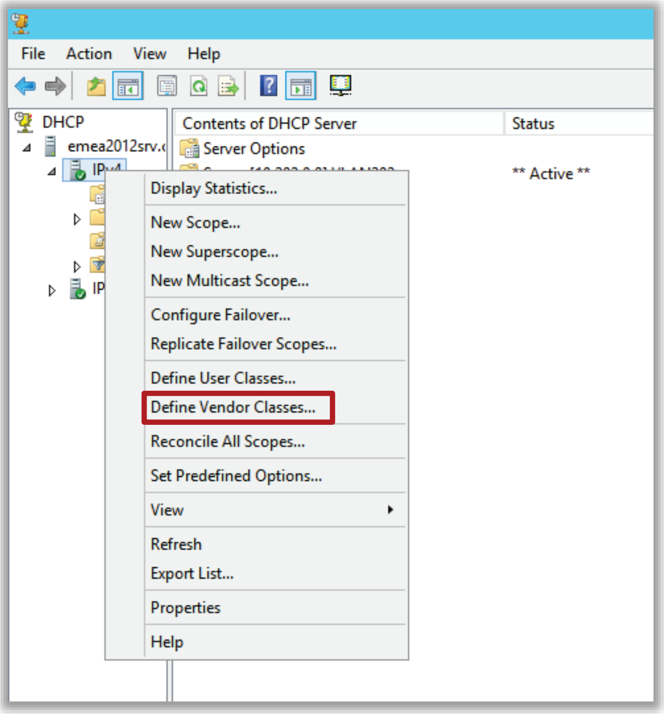
Microsoft Windows DHCP Server

Microsoft Windows Server 2003 / 2008 / 2012 provide integrated DHCP services which may be deployed centrally in the data center or locally at each store. The Microsoft DHCP server supports the ability to assign option 191 values directly to each DHCP scope as well as globally across multiple scopes using the Vendor Class Identifier. When a Microsoft based DHCP server is utilized, the option 191 value must be assigned directly to each DHCP scope providing DHCP services to the Access Points Native VLAN.

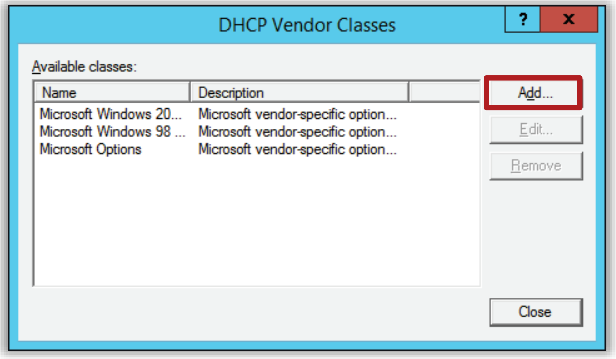
> **Note**
>
> Please reference the relevant Microsoft documentation for assigning DHCP options globally across multiple scopes as this procedure varies by Windows Server version.

Use the following procedure to create a Vendor Class Identifier and Predefined options 191 values on a Microsoft DHCP server that will assign DHCP option 191 and values from a specific DHCP scope:

1. In the DHCP snap-in, right click on the DHCP Server icon then select Define Vendor Classes:



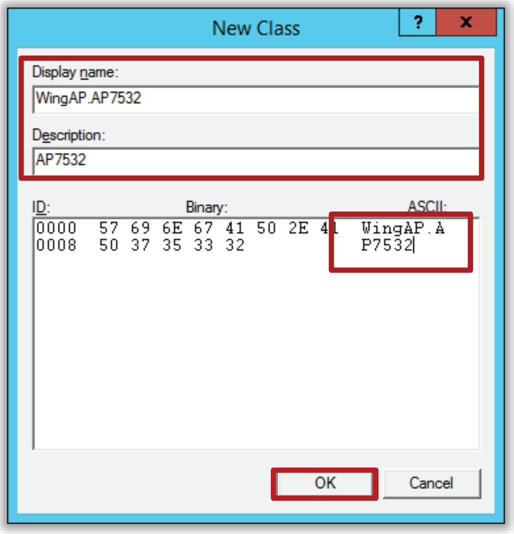
2. Click Add:



Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

3. Enter the Display Name and Description. In the ASCII field type, the Vendor Class Identifier for the Access Point model then click OK. Note in this example the Vendor Class for the AP 7532 Access Points WingAP.AP7532 is defined:

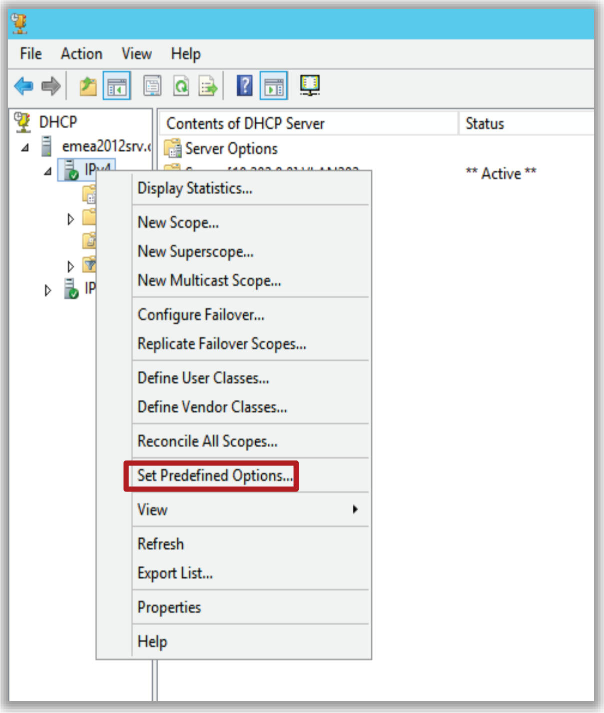


Display name: WingAP.AP7532

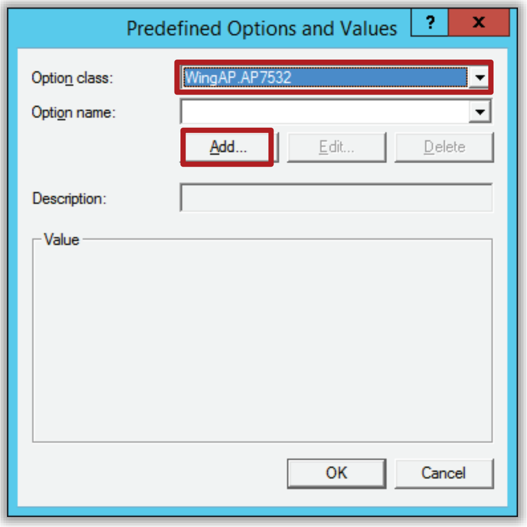
Description: AP7532

```
ID:        Binary:                    ASCII:
0000   57 69 6E 67 41 50 2E 41    WingAP.A
0008   50 37 35 33 32             P7532
```

4. In the DHCP snap-in, right click on the DHCP Server icon then select Set Predefined Options:



5. Select the Option class name created earlier then click Add:

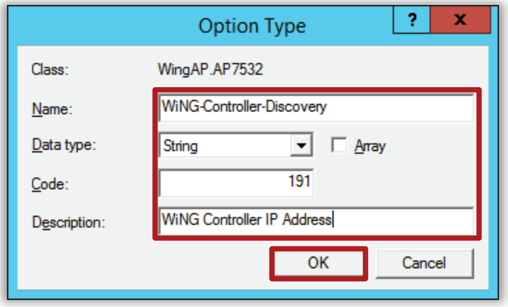


Option class: WingAP.AP7532

Option name:

Description:

6. Enter a Name and Description for the option then set the Data type to String. In the Code field enter 191 then click OK:



Class: WingAP.AP7532

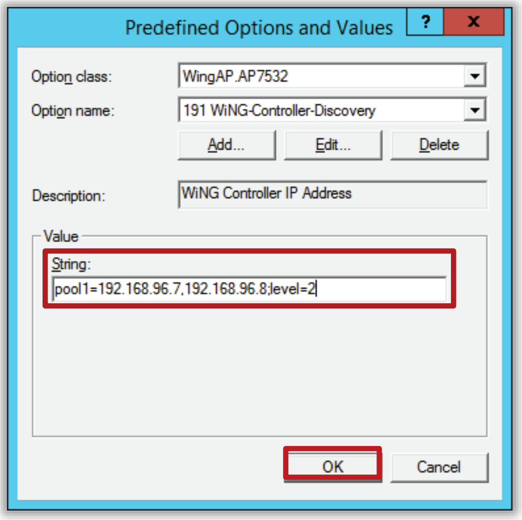
Name: WiNG-Controller-Discovery

Data type: String

Code: 191

Description: WiNG Controller IP Address

7. In the String field enter the value to provide to the WING 5 Access Points. In this example AP 7532 Access Points will be provided the Wireless Controller IP addresses 192.168.96.7 and 192.168.96.8 and will establish Level 2 IP based MINT links to the Wireless Controllers. Click OK:



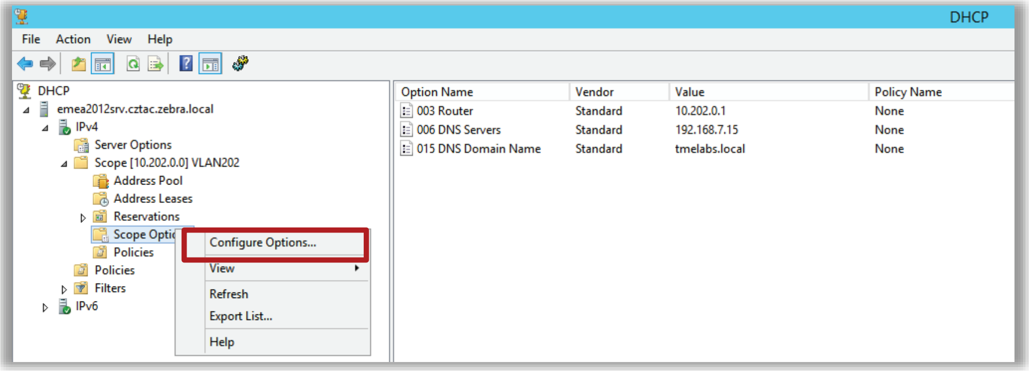
Option class: WingAP.AP7532

Option name: 191 WiNG-Controller-Discovery

Description: WiNG Controller IP Address

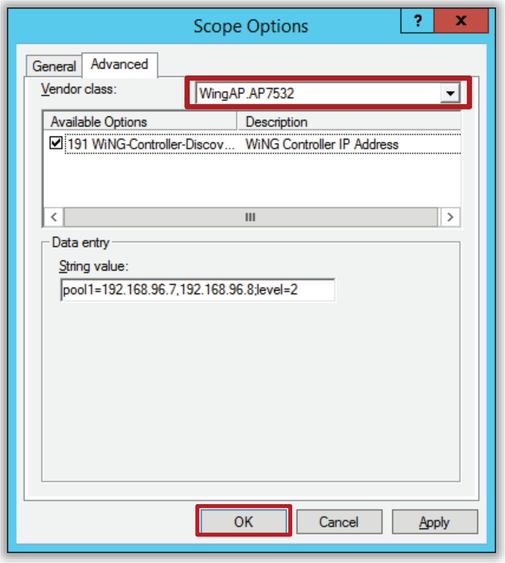
String: pool1=192.168.96.7,192.168.96.8;level=2

8. In the DHCP snap-in, select a DHCP scope then right click on Scope Options then select Configure Options:



Option Name	Vendor	Value	Policy Name
003 Router	Standard	10.202.0.1	None
006 DNS Servers	Standard	192.168.7.15	None
015 DNS Domain Name	Standard	tmelabs.local	None

9. Select the Advanced tab then under Vendor class select the Vendor Class name to assign to the DHCP scope. Click OK:



Vendor class: WingAP.AP7532

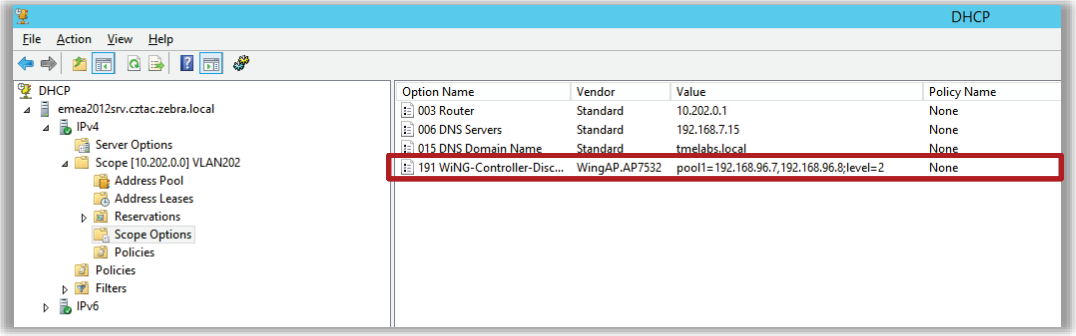
Available Options	Description
☑ 191 WiNG-Controller-Discov...	WiNG Controller IP Address

Data entry

String value:

pool1=192.168.96.7,192.168.96.8;level=2

10. The Vendor Class and Options have now been assigned to a DHCP scope supporting the Access Points Native VLAN at one remote site:



Option Name	Vendor	Value	Policy Name
003 Router	Standard	10.202.0.1	None
006 DNS Servers	Standard	192.168.7.15	None
015 DNS Domain Name	Standard	tmelabs.local	None
191 WiNG-Controller-Disc...	WingAP.AP7532	pool1=192.168.96.7,192.168.96.8;level=2	None

WING 5 DHCP Server

A WING 5 Access Point or Controller can be configured to provide DHCP services for a site. For DHCP services to be provided by WING 5 device, the device providing DHCP services must have a virtual IP interface defined with a static IP address for each VLAN the Access Point is providing DHCP services for. As each remote site will be assigned unique IP addressing, a separate DHCP policy will be required for each remote site.

Use the following procedure to create a DHCP Policy and Pool in WING 5 which can be applied to an individual device as a Device Override:

1. Create a DHCP server policy and define option 191:

```
 (config)# dhcp-server-policy DHCP-SRV
 (config-dhcp-policy-DHCP-SRV)# option ControllerIPAddress 191 ascii
```

2. Create a DHCP pool for the Access Points Native VLAN and define the required parameters and standard options:

```
 (config-dhcp-policy-DHCP-SRV)# dhcp-pool VLAN1
 (config-dhcp-policy-DHCP-SRV-pool-VLAN1)# network 192.168.21.0/24
 (config-dhcp-policy-DHCP-SRV-pool-VLAN1)# address range 192.168.21.100 192.168.21.254
 (config-dhcp-policy-DHCP-SRV-pool-VLAN1)# default-router 192.168.21.1
 (config-dhcp-policy-DHCP-SRV-pool-VLAN1)# option ControllerIPAddress
pool1=192.168.96.7,192.168.96.8;level=2
 (config-dhcp-policy-DHCP-SRV-pool-VLAN1)# exit
 (config-dhcp-policy-DHCP-SRV)# exit
```

3. Assign the DHCP Policy to the WING 5 device as an Override:

```
 (config)# self
 (config-device-5C-0E-8B-33-D3-4C)# use dhcp-server-policy DHCP-SRV
 (config-device-5C-0E-8B-33-D3-4C)# end
```

4. Commit and Write the Changes:

```
 # commit write
```

Pre-Staging Access Points

Use the following procedure to pre-stage an Independent Access Point using the Command Line Interface. Once adopted the Independent Access Points pre-staged configuration will be added to the Access Points Device configuration as Overrides:

1. Login to the Access Point and enter the default credentials admin / admin123. When prompted enter and confirm a new password:

```
ap7532-99B67C login: admin
Password: admin123
System is currently using the factory default login credentials.
Please change the default password to protect from unauthorized access.
Enter new password: wingsecure
Confirm new password: wingsecure
Password for user 'admin' changed successfully.
Please write this password change to memory(write memory) to be persistent
```

2. Access the device configuration and define a hostname for the Access Point. In this example the hostname ap7532-1 is defined:

```
ap7532-99B67C> enable
ap7532-99B67C# self
ap7532-99B67C(config-device-00-23-68-99-B6-7C)# hostname ap7532-1
ap7532-99B67C(config-device-00-23-68-99-B6-7C)# commit
```

3. Access the ge1 interface and assign a Native and Tagged VLANs. In this example the Native VLAN 1 and tagged VLANs 22-25 are defined:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# interface ge 1
ap7532-1(config-device-00-23-68-99-B6-7C-if-ge1)# switchport mode trunk
ap7532-1(config-device-00-23-68-99-B6-7C-if-ge1)# switchport trunk native vlan 1
ap7532-1(config-device-00-23-68-99-B6-7C-if-ge1)# switchport trunk allowed vlan 1,20
ap7532-1(config-device-00-23-68-99-B6-7C-if-ge1)# exit
```

4. Create a Virtual IP interface for the Native VLAN and assign a static IP address and Subnet Mask. In this example the static IP address 192.168.21.50/24 is defined:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# interface vlan 1
ap7532-1(config-device-00-23-68-99-B6-7C-if-vlan1)# ip address 192.168.21.50/24
ap7532-1(config-device-00-23-68-99-B6-7C-if-vlan1)# exit
```

5. Define a Default Gateway. In this example the default gateway for the Native VLAN 192.168.21.1 is defined:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# ip default-gateway 192.168.21.1
```

6. Define static Controller Host entries for the Primary and Secondary Wireless Controllers in the data center. In this example static Level 2 links to 192.168.96.7 and 192.168.96.8 are defined:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# controller host 192.168.96.7 pool 1 level 2
ap7532-1(config-device-00-23-68-99-B6-7C)# controller host 192.168.96.8 pool 1 level 2
```

7. Verify the configuration:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# show context
ap7532 00-23-68-99-B6-7C
 use profile default-ap6532
 use rf-domain default
 hostname ap7532-1
 ip default-gateway 192.168.21.1
 interface ge1
  switchport mode trunk
  switchport trunk native vlan 1
  no switchport trunk native tagged
  switchport trunk allowed vlan 1,20
 interface vlan1
  ip address 192.168.21.50/24
 logging on
 logging console warnings
 logging buffered warnings
 controller host 192.168.96.7 pool 1 level 2
 controller host 192.168.96.8 pool 1 level 2
```

8. Commit and Save the changes:

```
ap7532-1(config-device-00-23-68-99-B6-7C)# commit write
```

9. On the Wireless Controllers in the data center, view the running configuration and verify that the remote Access Point has been discovered and its Device configuration added:

```
nx9610-1# show running-config | begin 00-23-68-99-B6-7C
!
ap7532 00-23-68-99-B6-7C
 use profile STORES-AP
 use rf-domain store101
 hostname ap7532-1
 ip default-gateway 192.168.21.1
 interface vlan21
  ip address 192.168.21.50/24
 controller host 192.168.96.7 pool 1 level 2
 controller host 192.168.96.8 pool 1 level 2
!
```

Device Overrides inherited from the newly discovered AP7532 Access Point from pre-staging. Note that the ge1 interface configuration in this example is not inherited as it matches the ge1 configuration already defined in the assigned AP Profile.

MINT MTU

For certain centrally managed deployments using MPLS or VPN technologies for the wide area network, the default MINT MTU might need to be reduced to accommodate the lower MTU path between the remote Access Points and the Controllers in the Data Center.

By default, the MINT policy assigned to all Controllers and Access Points defines an MTU of 1500 bytes which suffices for most local area network and wide area network deployments. However, when the wide area network leverages MPLS or VPN technologies, the MTU path between the remote sites and the Data Center is often reduced below 1500 bytes. MINT packets that are larger than the MTU path have to be fragmented by the intermediate layer 3 devices to accommodate the lower MTU between the sites.

While the MINT protocol is designed to accommodate IP fragmentation, not all intermediate layer 3 devices fragment packets the same way which can result in various issues. Symptoms of an MTU path issues include remote Access Points not adopting, configuration not being successfully applied to one or more remote Access Points or statistics from remote sites not being received by the Controller. You may also experience Access Point firmware upgrade failures.

To remediate an MTU path issue it is recommended that the MINT MTU be lowered in the MINT policy so that the IP fragmentation is performed by the Controllers and the Access Points rather than by the intermediate layer 3 devices.

Determining the MTU Path

The MTU value you define in the global MINT policy will vary depending on the specific network environment. You can quickly determine the MTU path of the intermediate network by issuing a ping from the Controller to a remote Access Point at various sizes with the **`dont-fragment`** option set. ICMP packets with sizes that receive replies fall within the MTU path while packets that fail to receive replies require fragmentation to be passed and thus fall outside the minimum MTU path.

```
nx9610-1# ping <remote-ap-ip-address> size <value> dont-fragment
```

It is recommended that you start your testing using 1500 byte ICMP packets and reduce the size in increments of 8 (1484, 1476, 1468, 1460 etc.) until you receive a reply. Once you determine the minimum MTU it is recommended to repeat the test using the determined MTU value against Access Points at multiple remote sites to ensure that the MTU path is consistent across all your sites. It is possible that the MTU paths are different between sites especially when multiple service provider networks are utilized.

Note

You can optionally use a Windows based tool such as mtupath.exe to quickly determine the MTU path between the data center and the remote sites. This tool will automatically adjust the MTU on the fly to quickly determine the minimum supported MTU.

Defining the new MTU

You can optionally use a Windows based tool such as mtupath.exe to quickly determine the MTU path between the data center and the remote sites. This tool will automatically adjust the MTU on the fly to quickly determine the minimum supported MTU.

> **Note**
>
> The MTU value you enter MUST be a multiple of 8. If an incorrect value is defined in the CLI, the CLI will automatically round the value to the nearest multiple of 8. However, the Web-UI requires an exact value to be defined.

MINT Policy Configuration Command Line Interface

Use the following procedure to modify the MTU in the MINT Policy named global-default using the Command Line Interface:

1. Access the MINT Policy named default and define a new MTU based on the results of the testing in the previous section:

```
nx9610-1(config)# mint-policy global-default
nx9610-1(config-mint-policy-global-default)# mtu 1372
```

2. Verify the changes:

```
nx9610-1(config-mint-policy-global-default)# show context
mint-policy global-default
 mtu 1372
```

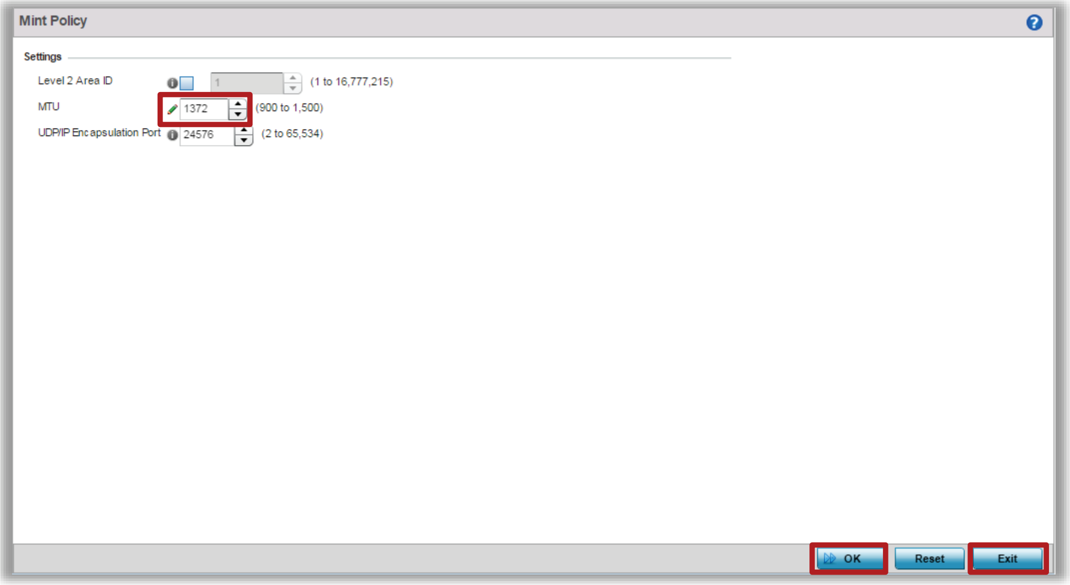
3. Exit the Policy configuration then commit and save the changes:

```
nx9610-1(config-mint-policy-global-default)# exit
nx9610-1(config)# commit write
[OK]
```

MINT Policy Configuration – Web UI

Use the following procedure to modify the MTU in the MINT Policy named global-default using the Management User Interface:

1. Select Configuration -> Devices -> MINT Policy. Enter the new MTU value then click OK and Exit:



Mint Policy

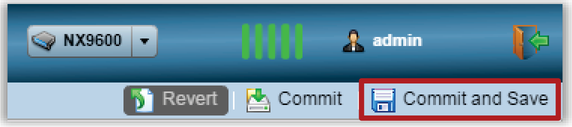
Settings

Level 2 Area ID □ 1 (1 to 16,777,215)

MTU 1372 (900 to 1,500)

UDP/IP Encapsulation Port 24576 (2 to 65,534)

2. Commit then Save the changes:



Verification

Verifying Adoption Status

Issue the show adoption info command to view basic adoption information about the Access Points adopted by the Wireless Controllers in the data center: From the available information you can quickly identify the Total Number of adopted Access Points as well as the Type and Model of each Access Point:

```
nx9610-1# show adoption info

----------------------------------------------------------------------------------------------------
              HOST-NAME                 MAC       TYPE               MODEL           SERIAL-NUMBER
----------------------------------------------------------------------------------------------------
          ap8533-5C4465   74-67-F7-5C-44-65     ap8533   AP-8533-68SB40-EU         16158522200156
          ap8533-5C446F   74-67-F7-5C-44-6F     ap8533   AP-8533-68SB40-EU         16158522200158
          ap8432-5C46E0   74-67-F7-5C-46-E0     ap8432   AP-8432-680B30-EU         16158522200283
          ap8432-5C470D   74-67-F7-5C-47-0D     ap8432   AP-8432-680B30-EU         16158522200292
----------------------------------------------------------------------------------------------------
Total number of devices displayed: 4
```

Note

You can quickly filter the output of a command using grep to look for specific information. For example, issuing the show adoption info | grep store100 command will display all the Access Points adopted from store 100.

Issue the show adoption status command to view detailed adoption information about the Access Points adopted by the Wireless Controllers in the data center. From the available information you can quickly identify which of the Wireless Controllers each Access Point is Adopted By as well as identify each Access Points Configuration State, Uptime and Firmware Version:

```
nx9610-1# show adoption status

-----------------------------------------------------------------------------------------------------------
----
DEVICE-NAME       VERSION         CFG-STAT         MSGS ADOPTED-BY        LAST-ADOPTION
UPTIME
-----------------------------------------------------------------------------------------------------------
----
ap8533-5C4465     5.8.4.0-034R    configured       No   nx9610-1            0 days 00:18:48     0 days
00:20:06
ap8533-5C446F     5.8.4.0-034R    configured       No   nx9610-1            0 days 00:00:38     0 days
00:03:17
ap8432-5C46E0     5.8.4.0-034R    configured       No   nx9610-1            0 days 00:18:03     0 days
00:20:14
ap8432-5C470D     5.8.4.0-034R    configured       No   nx9610-1            0 days 00:17:33     0 days
00:19:50
-----------------------------------------------------------------------------------------------------------
-----
Total number of devices displayed: 4
```

Verifying RF Domains

Issue the show global device-list command to view the Online status of the known Wireless Controllers and Access Points in the Wireless System as well as RF Domain assignments. Each Wireless Controller in the data center should be assigned to a common RF Domain while Access Points should be assigned to one common RF Domain per site:

```
nx9610-1# show global device-list
-----------------------------------------------------------------------------------------------------------
---
               MAC      HOST-NAME       TYPE          CLUSTER       RF-DOMAIN        ADOPTED-BY     ONLINE
-----------------------------------------------------------------------------------------------------------
---
 74-67-F7-5C-44-65    ap8533-5C4465   ap8533                          store101 84-24-8D-7F-34-C7   online
 74-67-F7-5C-44-6F    ap8533-5C446F   ap8533                          store101 84-24-8D-7F-34-C7   online
 74-67-F7-5C-46-E0    ap8432-5C46E0   ap8432                          store100 84-24-8D-7F-34-C7   online
 74-67-F7-5C-47-0D    ap8432-5C470D   ap8432                          store100 84-24-8D-7F-34-C7   online
 84-24-8D-67-C3-A1         nx9610-2   nx9600      NOC-CLUSTER              noc                     online
 84-24-8D-7F-34-C7         nx9610-1   nx9600      NOC-CLUSTER              noc                     online
-----------------------------------------------------------------------------------------------------------
---
Total number of clients displayed: 6
```

Issue the show global domain managers command to view the elected RF Domain Manager for each of the defined RF Domains. One Access Point from each remote site will be elected and displayed. If the elected Access Point fails or is taken off-line, another Access Point at the site will be elected:

```
nx9610-1# show global domain managers
-----------------------------------------------------------------------------------------------------
                      RF-DOMAIN                              MANAGER          HOST-NAME  APS  CLIENTS
-----------------------------------------------------------------------------------------------------
                            noc                    84-24-8D-7F-34-C7           nx9610-1    0        0
                       store100                    74-67-F7-5C-46-E0      ap8432-5C46E0    2        0
                       store101                    74-67-F7-5C-44-65      ap8533-5C4465    2        0
-----------------------------------------------------------------------------------------------------
Total number of RF-domain displayed: 3
```

Note

You can pre-select a specific Access Point as RF Domain Manager for a site by issuing the rf-domain-manager priority command as a device Override and assigning a priority value of 255.

Verifying MINT

Issue the show mint links command on each of the Wireless Controllers in the data center to view the established MINT links. One Level 2 IP based MINT link will be present on each Wireless Controller for the cluster plus one Level 2 MINT link will be present to each RF Domain manager (one per site). In the example below one Level 2 IP based MINT link has been established to nx9610-1 from the elected RF Domain manager at store100 and another Level 2 IP based MINT link has been established from the elected RF Domain manager at store101.

```
nx9610-1# show mint links
3 mint links on 4D.7F.34.C7:
link ip-172.31.2.138:24576 at level 2, 1 adjacencies, (used)
link ip-172.31.3.133:24576 at level 2, 1 adjacencies, (used)
link ip-192.168.96.8:24576 at level 2, 1 adjacencies, forced
```

```
nx9610-1# show mint links on nx9610-2
1 mint links on 68.67.C3.A1:
link ip-192.168.96.7:24576 at level 2, 1 adjacencies, forced
```

Issue the show mint links command on each of the Access Points at a specific site. Each Access Point will have an established Level 1 VLAN based MINT link to its neighboring Access Points over the Control VLAN while only the elected RF Domain manager at the site will display a used Level 2 IP based MINT link to the Wireless Controllers in the data center. Non RF Domain managers will display the Level 2 IP based MINT link but will list it as unused.

```
nx9610-1# show mint links on ap8533-5C4465
2 mint links on 75.5C.44.65:
link vlan-1 at level 1, 1 adjacencies, DIS 75.5C.44.6F
link ip-192.168.96.7:24576 at level 2, 1 adjacencies, (used)
```

```
nx9610-1# show mint links on ap8533-5C446F
2 mint links on 75.5C.44.6F:
link vlan-1 at level 1, 1 adjacencies, DIS 75.5C.44.6F (self)
link ip-192.168.96.7:24576 at level 2, 0 adjacencies, (unused)
```

```
nx9610-1# show mint neighbors on ap8533-5C4465
2 mint neighbors of 75.5C.44.65:
75.5C.44.6F (ap8533-5C446F) at level 1, best adjacency vlan-1
4D.7F.34.C7 (nx9610-1) at level 2, best adjacency ip-192.168.96.7:24576
```

```
nx9610-1# show mint neighbors on ap8533-5C446F
1 mint neighbors of 75.5C.44.6F:
75.5C.44.65 (ap8533-5C4465) at level 1, best adjacency vlan-1
```

```
nx9610-1# show mint neighbors
2 mint neighbors of 4D.7F.34.C7:
75.5C.44.65 (ap8533-5C4465) at level 2, best adjacency ip-172.31.2.138:24576
75.5C.46.E0 (ap8432-5C46E0) at level 2, best adjacency ip-172.31.3.133:24576
```

Issue the mint traceroute <mint-id> command against both the RF Domain Manager and non RF Domain Manager MINT IDs. You will notice that to reach the non RF Domain Manager Access Point at the remote site (forward and reverse), the MINT packets have to go through the elected RF Domain manager at the site.

In the example below for the Wireless Controller can reach the elected RF Domain Manager with the MINT id 75.5C.44.65 directly. However for the Wireless Controllers to reach the non RF Domain Manager with the MINT id 75.5C.44.6F, it has to go through the elected RF Domain Manager with the MINT id 75.5C.44.65:

```
nx9610-1# mint traceroute 75.5C.44.65
DIR MINT-ADDRESS MAC-ADDRESS       L2-gw LEVEL PRODUCT-TYPE RF-DOMAIN    HOSTNAME
--------------------------------------------------------------------------------
F   4D.7F.34.C7  84-24-8D-7F-34-C7 Y     L1/L2 NX9600       noc          nx9610-1
D   75.5C.44.65  74-67-F7-5C-44-65 Y     L1/L2 AP8533       store101     ap8533-5C4465
R   4D.7F.34.C7  84-24-8D-7F-34-C7 Y     L1/L2 NX9600       noc          nx9610-1
```

```
nx9610-1# mint traceroute 75.5C.44.6F
DIR MINT-ADDRESS MAC-ADDRESS       L2-gw LEVEL PRODUCT-TYPE RF-DOMAIN    HOSTNAME
--------------------------------------------------------------------------------
F   4D.7F.34.C7  84-24-8D-7F-34-C7 Y     L1/L2 NX9600       noc          nx9610-1
F   75.5C.44.65  74-67-F7-5C-44-65 Y     L1/L2 AP8533       store101     ap8533-5C4465
D   75.5C.44.6F  74-67-F7-5C-44-6F N     L1/L2 AP8533       store101     ap8533-5C446F
R   75.5C.44.65  74-67-F7-5C-44-65 Y     L1/L2 AP8533       store101     ap8533-5C4465
R   4D.7F.34.C7  84-24-8D-7F-34-C7 Y     L1/L2 NX9600       noc          nx9610-1
```

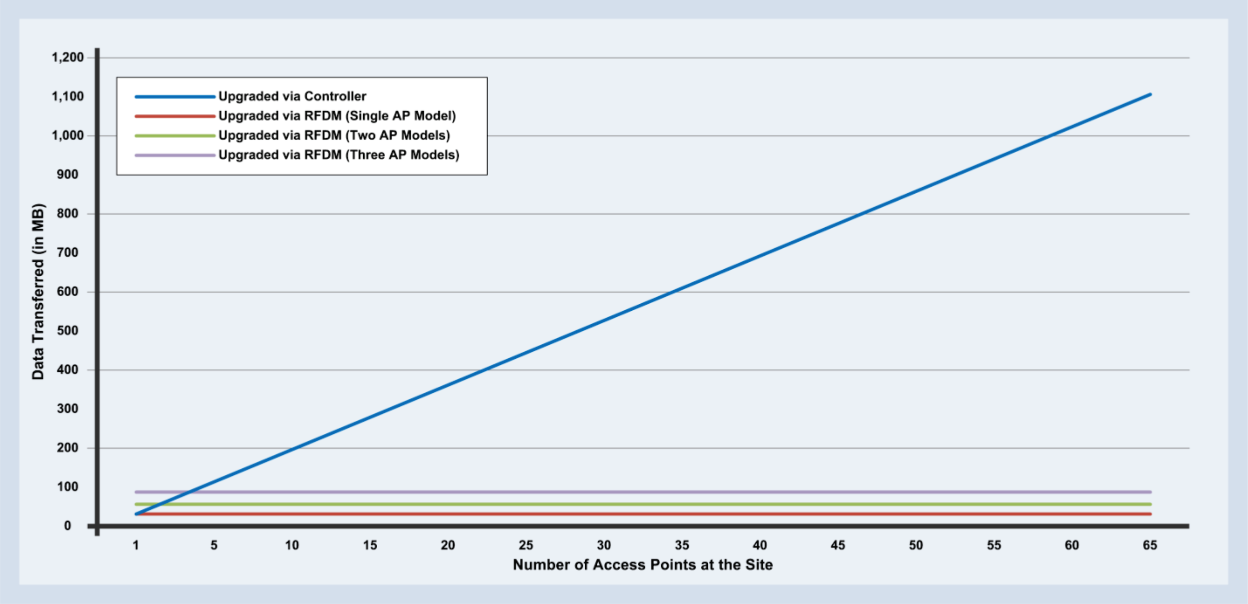
Firmware Image Upgrades

By default, the Controllers in the data center will not automatically upgrade or downgrade Access Points running different firmware releases upon adoption. After upgrading the Controllers in the Data Center to a new WING release, the Access Points running older firmware will re-adopt to the active Controller which will detect the firmware version mismatch and automatically upgrade the Access Points. The default upgrade behavior is fine for campus deployments but is not efficient for large distributed deployments with 100s of sites and 1,000s Access Points.

When working with large distributed Access Point deployments it is recommended that the remote Access Points be upgraded via the elected RF Domain Manager at their site rather than directly from the Controller in the Data Center. Upgrading via the elected RF Domain Manager provides the following benefits:

1. Upgrading via the elected RF Domain Manager is more bandwidth efficient. For each remote site the firmware image for each Access Point / Site Controller model is only sent once over the WAN vs. once for each individual Access Point. This significantly reduces the load over the WAN. For example, if a site has 36 x Access Points (two models), 36MB of data would be transferred over the WAN vs. 648MB if the Access Points were upgraded individually. This is a WAN bandwidth saving of 612MB!
2. Upgrading via the elected RF Domain Manager allows more Access Points to be simultaneously upgraded. Up to 128 remote sites can be upgraded simultaneously from a Controller in the data center vs. 128 individual Access Points at a time. As each remote site contains multiple Access Points, this significantly reduces the amount of time it will take to upgrade the system. For example, up to 16,384 x Access Points (128 sites each with 128 x Access Points) can be simultaneously upgraded vs. 128 x individual Access Points.

The following chart highlights the difference between the amount of data transferred over the WAN per site when using the Controller or RF Domain Managers to perform the Independent Access Point upgrades. This table assumes an average Access Point image size of 18 MB.



Firmware Images

Remote Access Points are upgraded using firmware images stored on the centralized Controllers. The NX 95X0 / VX 9000 / NX 96X0 series of Integrated Services Controllers firmware image includes firmware for all supported Access Points within the release and also the RFS 4000 controller. The RFS X000 series Wireless Controllers however will not include firmware for the AP 6511, AP 7XXX, AP8XXX Access Points. If your deployment includes these Access Point models you will need to download and install the firmware onto the RFS Controllers separately prior to upgrading the remote Access Points.

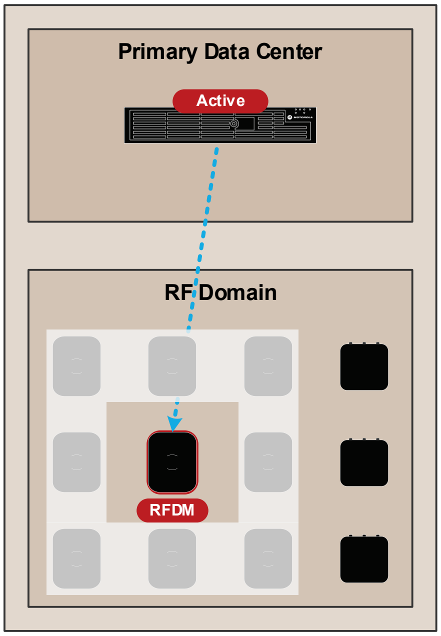
You can verify that the correct Access Point firmware images are installed on the Controllers by issuing the show device-upgrade versions command. If any firmware images are missing, they can be loaded onto the Controllers by issuing the device-upgrade load-image command.

```
nx9610-1# show device-upgrade versions
--------------------------------------------------------------------------------
        CONTROLLER             DEVICE-TYPE                   VERSION
--------------------------------------------------------------------------------
  nx9610-1                ap621                    5.8.4.0-034R
  nx9610-1                ap622                    5.8.4.0-034R
  nx9610-1                ap650                    5.8.4.0-034R
  nx9610-1                ap6511                   5.8.4.0-034R
  nx9610-1                ap6521                   5.8.4.0-034R
  nx9610-1                ap6522                   5.8.4.0-034R
  nx9610-1                ap6532                   5.8.4.0-034R
  nx9610-1                ap6562                   5.8.4.0-034R
  nx9610-1                ap71xx                   5.8.4.0-034R
  nx9610-1                ap7502                   5.8.4.0-034R
  nx9610-1                ap7522                   5.8.4.0-034R
  nx9610-1                ap7532                   5.8.4.0-034R
  nx9610-1                ap7562                   5.8.4.0-034R
  nx9610-1                ap81xx                   5.8.4.0-034R
  nx9610-1                ap82xx                   5.8.4.0-034R
  nx9610-1                ap8432                   5.8.4.0-034R
  nx9610-1                ap8533                   5.8.4.0-034R
  nx9610-1                nx45xx                   none
  nx9610-1                nx5500                   none
  nx9610-1                nx65xx                   none
  nx9610-1                nx75xx                   none
  nx9610-1                nx9000                   none
  nx9610-1                nx9600                   none
  nx9610-1                rfs4000                  5.8.4.0-034R
  nx9610-1                rfs6000                  none
  nx9610-1                rfs7000                  none
--------------------------------------------------------------------------------
```

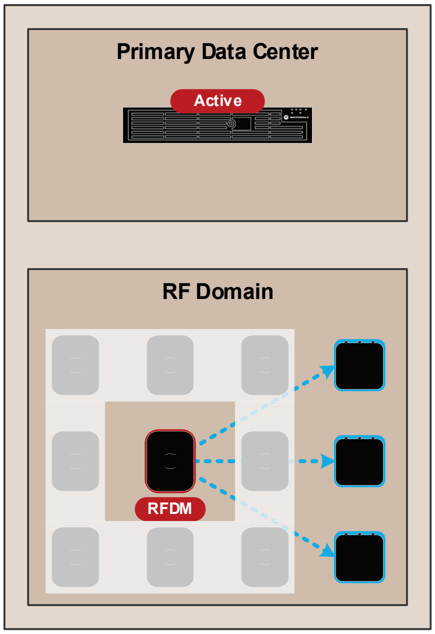
Firmware Upgrade Process

AP Only Sites

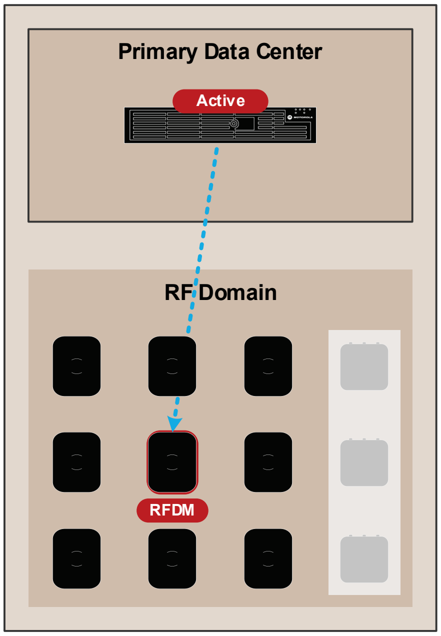
The following describes the upgrade process when upgrading remote sites using the elected RF Domain Managers (RFDM) for each site. This example demonstrates the upgrade process for a remote site with multiple models of Access Points. It is important to note that an RFDM can upgrade multiple models of WING 5 Access Points. If different models of Access Points reside at a site, the RFDM will upgrade the non-like Access Point models first, upgrade like Access Point models next and itself last:



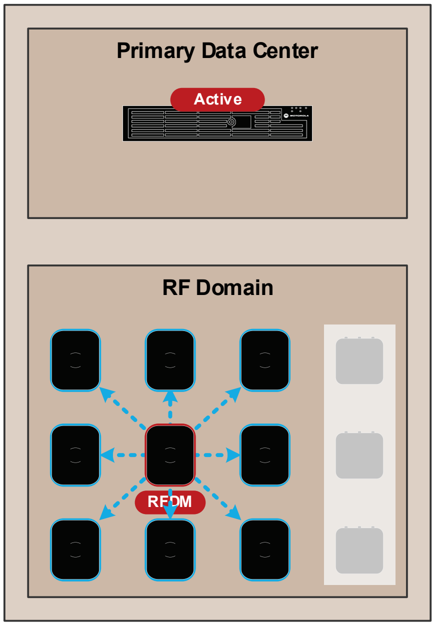
1. When a remote site has been queued for an upgrade, the firmware image for the first Access Point model is transferred to the RF Domain Manager (RFDM) at the site. In this example the site contains both AP 8533 and AP 7532 Independent Access Points and the RFDM is an AP 8533. The firmware image for the AP 7532 Access Points is transferred first.



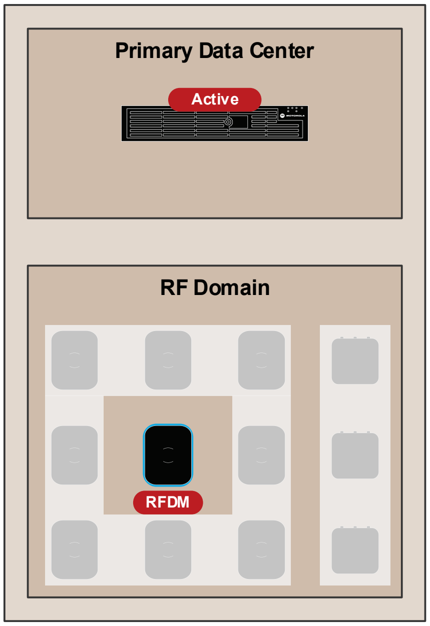
2. The RFDM will distribute the firmware to each of the AP 7532 Access Points at the site. By default, the RFDM will upgrade up to 10 x Access Points simultaneously. If more than 10 x Access Points of the model reside at the site, they will be added to a queue and upgraded after the upgrade for the first 10 Access Points has completed.



3. The firmware image for the second model of Access Point will be transferred to the RFDM at the site. In this example the firmware for the AP 8533 Independent Access Points will be transferred.



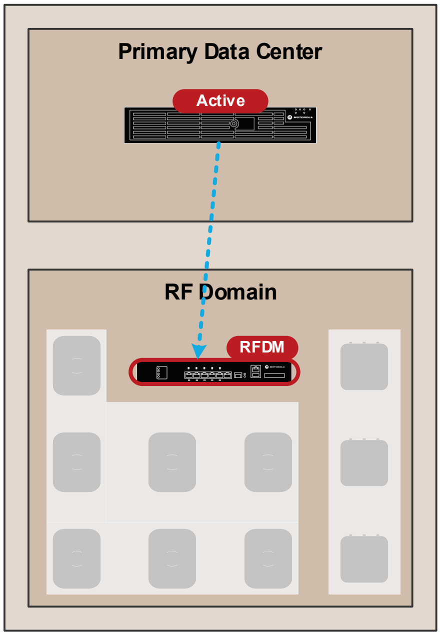
4. The RFDM will distribute the firmware to each of the AP 8533 Access Points at the site. By default, the RFDM will upgrade up to 10 x Access Points simultaneously. If more than 10 x Access Points of the model reside at the site, they will be added to a queue and upgraded after the upgrade for the first 10 Access Points has completed.



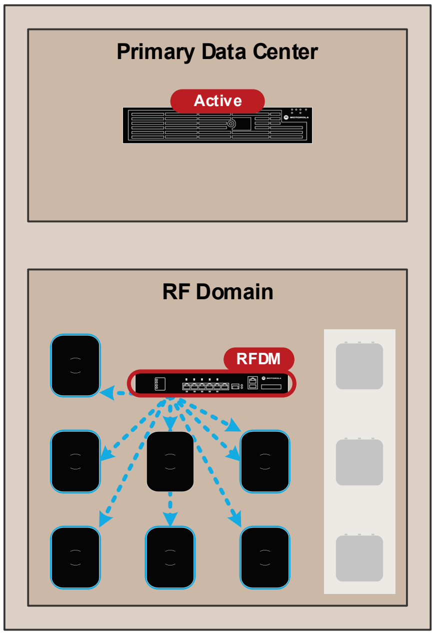
5. Once all of the Access Points at the site have been upgraded, the RFDM will upgrade itself last. Upon upgrading the RFDM will either reboot the Access Points at the site (all or staggered) or will manually require a reset at a later date and time. If no reboot is selected, the upgrade is completed.

Site Controller Sites

The following describes the upgrade process when upgrading remote sites using one of the site controllers elected as an RF Domain Manager (RFDM). This example demonstrates the upgrade process for a remote site with multiple models of Access Points and a single site controller. It is important to note that unlike with AP only sites, Site Controllers will be updated first before updating local Access Points. If different models of Access Points reside at a site, the site controller will upgrade the top grade Access Point models first, upgrade lower grade Access Point models next and so on. Site Controllers can also cache firmware images received from the centralized controller to persist them across reboots to further increase WAN efficiency:

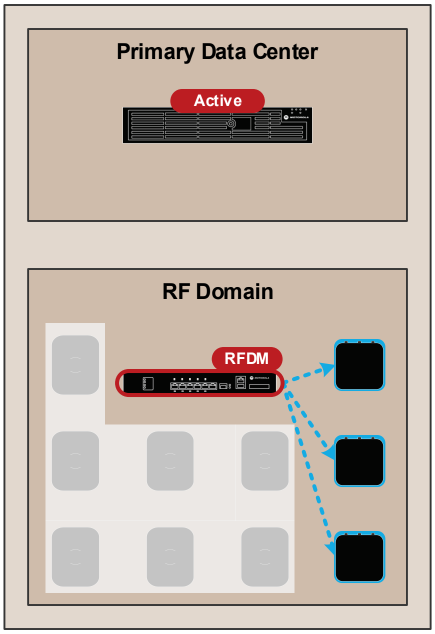


1. When a remote site with Site Controllers has been queued for an upgrade, the firmware image for the Site Controller is transferred first. In clustered environment the standby controller will be updated first, following by the active one. Both Site Controllers will reboot, while all local APs will unadopt during the downtime window.



2. Once the Site Controller is back online and APs re-adopt, it will receive the image for the APs from the active centralized controller (in case no images are available in cache), starting from highest grade AP models, in this example AP 8533.

   By default, the Site Controller will upgrade up to 10 x Access Points simultaneously. If more than 10 x Access Points of the model reside at the site, they will be added to a queue and upgraded after the upgrade for the first 10 Access Points has completed.



3. The firmware image for the second model of Access Point will be transferred to the Site Controller at the site. After that the Site Controller will distribute the firmware to all APs at the site. In this example the firmware for the AP 7532 Access Points will be transferred.

Note

In order to cache received firmware images and save them across reboots device-upgrade persist-images command should be used in the Site Controller Profile.

Firmware Upgrade Procedure

The following section provides a procedure that can be followed to upgrade a centrally managed deployment to a new WING 5 release using the Command Line Interface.

> Note
>
> Please read the release notes for the target release prior to performing any WING 5 upgrades. The release notes will contain details such as upgrade path information as well as a list of any known issues or restrictions for the target release.

Step 1 – Backup the Current Configuration

Prior to upgrading Controller to a new release it is recommended that the current startup-configuration be exported to an external TFTP or FTP server. This provides a backup of the current configuration incase the system needs to be rolled back to the old release at a later date.

For clustered environments only the startup-config from the cluster master needs to be archived as the configuration is shared between the primary and standby Controllers. You can identify the cluster master by issuing the show cluster member command. It is important to note that all pending changes need to be committed and saved to the Controller(s) prior to exporting the startup-config. Failure to commit and save changes may result in an incomplete configuration.

The following demonstrates how to export the startup-config from a Controller using the CLI to an external TFTP server:

Command Syntax:

```
copy startup-config tftp://<tftp-server-ip>/<path>/<filename>
```

CLI Example:

```
nx9000-1# copy startup-config tftp://192.168.10.6/Configs/nx9000-52-current.cfg
```

The following demonstrates how to export the startup-config from a Controller using the CLI to an external FTP server:

Command Syntax:

```
copy startup-config ftp://<user>:<password>@<ftp-server-ip>/<path>/<filename>
```

CLI Example:

```
nx9000-1# copy startup-config ftp://ftpuser:wingsecure@192.168.10.6/Configs/nx9000-52-current.cfg
```

> Note
>
> Please ensure all changes are committed and saved on the Controller(s) prior to exporting the startup-configuration.

> Note
>
> For clustered environments please ensure the cluster is up and operation prior to exporting the startup-config. If the cluster is separated it is recommended that you export the startup-config from both Controllers in the cluster.

Step 2 - Upgrading the Controller Firmware

Each WING 5 device supports a Primary and Secondary firmware image slot allowing two separate firmware images to be installed. When the Controllers are upgraded to a new release, the new firmware will be installed into either the Primary or Secondary image slot depending on which slot the Controller is currently booting from. You can identify which slot is active on each device by issuing the show boot command.

The show boot command will display the firmware version installed in the Primary and Secondary image slots as well as display current version and next version to be loaded. The Current Boot field identifies the firmware version the device is currently operating while the Next Boot field identifies the firmware version that will be loaded upon the next device reset.

```
nx9000-1# show boot
--------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
--------------------------------------------------------------------------------
  Primary       07/16/2016 06:29:11     08/04/2016 09:12:33     5.8.4.0-034R
  Secondary     07/08/2016 18:40:02     07/11/2016 11:36:16     5.8.4.0-032R
--------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
VM support         : Not present
```

The following demonstrates how to upgrade a Controller to WING 5.8.5 using the CLI when the firmware image is located on an external SFTP server:

Command Syntax:

```
upgrade sftp://<user>:<pass>@<sftp-server-address>/<path>/<filename>
```

CLI Example:

```
nx9000-1# upgrade sftp://user:pass@192.168.10.6/Images/NX9600-5.8.5.0-006D.img
Running from partition /dev/sda7
Validating image file header
Removing other partition
Making file system
Extracting files (this may take some
time)...........................................................................................
................................................................................................
................................................................................................
...............................................................
Control C disabled
Version of firmware update file is 5.8.5.0-006D
Removing unneeded files from flash:/crashinfo directory
Removing unneeded files from flash:/var2/log directory
Creating LILO files
Running LILO
Successful
```

After the Controllers in the data center have been upgraded to the new release, the Next Boot parameter will be automatically modified so that the new firmware will be loaded when the Controller is restarted. The Controllers will not load the new firmware until they are restarted.

```
nx9000-1# show boot
--------------------------------------------------------------------------------
     IMAGE            BUILD DATE             INSTALL DATE          VERSION
--------------------------------------------------------------------------------
  Primary       07/16/2016 06:31:58     09/26/2016 17:07:25     5.8.4.0-034R
  Secondary     09/20/2016 12:33:33     09/26/2016 16:28:17     5.8.5.0-006D
--------------------------------------------------------------------------------
Current Boot       : Primary
Next Boot          : Secondary
Software Fallback  : Enabled
VM support         : Not present
Software Fallback  : Enabled
```

Note

For clustered environments both Controllers must be upgraded to the same WING release. A cluster cannot operate when different WING firmware versions are operating on each device.

Step 3 – Disabling Automatic AP Ugrades

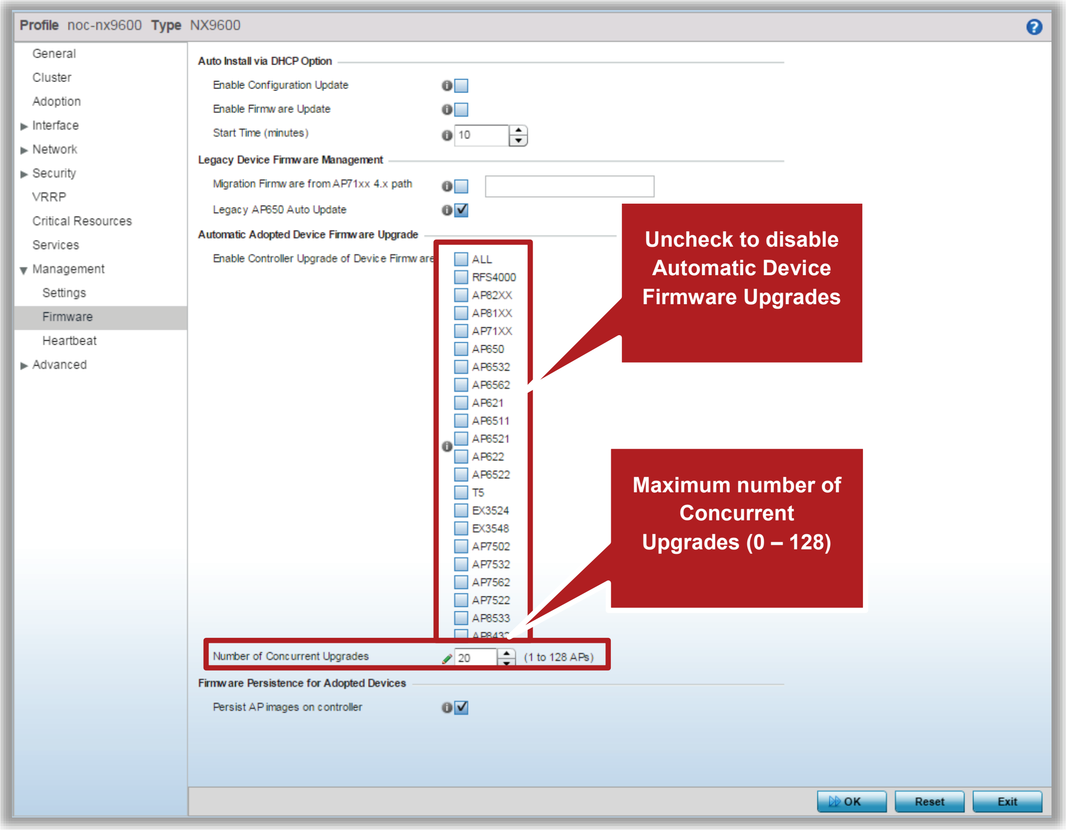
Disabling Automatic Access Point firmware upgrades and specifying the maximum number of concurrent Access Point upgrades can be performed using either the Web-UI or CLI by modifying the profile assigned to the Controllers. By default, Controller profiles includes "device-upgrade auto" parameter which will automatically upgrade all Access Points and support 10 concurrent Access Point upgrades.

The following demonstrates how to disable Auto AP Upgrades and defined the maximum concurrent AP Upgrades in the Controller profile using the CLI. Please ensure that the changes are committed and saved prior to reloading the Controllers with the new WING release:

```
nx9000-1(config)# profile <device-type> <profile-name>
!
profile nx9000 DATACENTER-NX9000
 ip name-server 192.168.10.6
 ip domain-name tmelabs.local
 no autoinstall configuration
 no autoinstall firmware
 no device-upgrade auto
 device-upgrade count 20
 !
 ! Configuration Removed for Brevity
 !
!
```

The following demonstrates how to disable Auto AP Upgrades and defined the maximum concurrent device Upgrades in the Controller profile using the Web-UI. Please ensure that the changes are committed and saved prior to reloading the Controllers with the new WING release:

Configuration -> Profiles -> <profile-name> -> Management -> Firmware



Profile noc-nx9600 **Type** NX9600

Auto Install via DHCP Option

Enable Configuration Update □

Enable Firmw are Update □

Start Time (minutes) 10

Legacy Device Firmware Management

Migration Firmw are from AP71xx 4.x path □

Legacy AP650 Auto Update ☑

Automatic Adopted Device Firmware Upgrade

Enable Controller Upgrade of Device Firmw are

□ ALL
□ RFS4000
□ AP82XX
□ AP81XX
□ AP71XX
□ AP650
□ AP6532
□ AP6562
□ AP621
□ AP6511
□ AP6521
□ AP622
□ AP6522
□ T5
□ EX3524
□ EX3548
□ AP7502
□ AP7532
□ AP7562
□ AP7522
□ AP8533
□ AP843

Number of Concurrent Upgrades 20 (1 to 128 APs)

Firmware Persistence for Adopted Devices

Persist AP images on controller ☑

Uncheck to disable Automatic Device Firmware Upgrades

Maximum number of Concurrent Upgrades (0 – 128)

Step 4 – Reloading the Controllers

The Controllers in the Data Center can now be safely restarted. As the Controller reset is impacting for certain configurations, it is recommended that reset be scheduled during an appropriate maintenance window. For example, if RADIUS traffic is proxied through the Controllers, remote users will be unable to authenticate when the Controllers are offline.

For clustered environments it is recommended that both Controllers be reset at the same time as there is no real advantage to staggering the reboots. Resetting both Controllers ensures that when the cluster re-establishes that both Controllers are running the same firmware version and are in the same active / standby state prior to the upgrade.

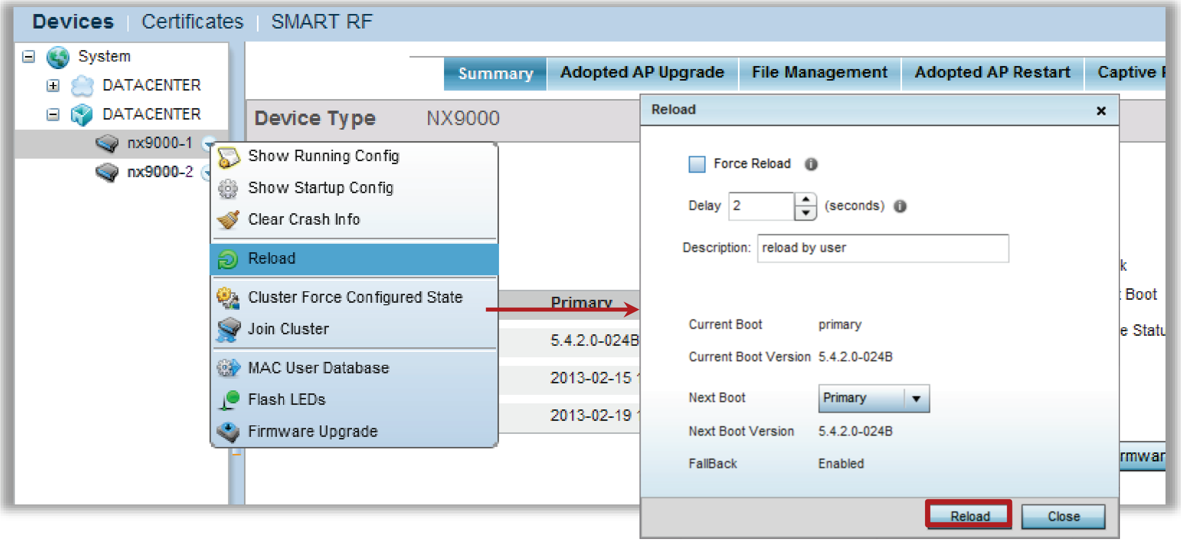
The following demonstrates how to reboot the Controllers using the CLI. Please note that you must connect to the console of both Controllers to issue the **reload** command:

```
nx9610-1# reload
The system will be rebooted, do you want to continue? (y/n): y
Nov 01 13:43:31 2012: %DAEMON-6-INFO: init: The system is going down NOW!
Nov 01 13:43:31 2012: %DAEMON-5-NOTICE: ntpd[2221]: ntpd exiting on signal 15
Nov 01 13:43:31 2012: %AUTH-6-INFO: sshd[2053]: Received signal 15; terminating.
```

```
nx9610-2# reload
The system will be rebooted, do you want to continue? (y/n): y
Nov 01 13:43:35 2012: %DAEMON-6-INFO: init: The system is going down NOW!
Nov 01 13:43:35 2012: %DAEMON-5-NOTICE: ntpd[2221]: ntpd exiting on signal 15
Nov 01 13:43:35 2012: %AUTH-6-INFO: sshd[2053]: Received signal 15; terminating.
```

The following demonstrates how to reboot the Controllers using the Web-UI. Please note that the Web-UI allows you to specify the **Next Boot** option to determine which firmware version to load:

Operations -> **<rf-domain-name>** -> **<hostname>** -> **Reload**



Device Type NX9000

□ Force Reload

Delay 2 (seconds)

Description: reload by user

Current Boot primary

Current Boot Version 5.4.2.0-024B

Next Boot Primary

Next Boot Version 5.4.2.0-024B

FallBack Enabled

Upon rebooting the Controllers will re-establish their cluster and start re-adopting the Access Points. The Access Points will be able to automatically re-establish their MINT links to the active Controller and adopt without having to be reset.

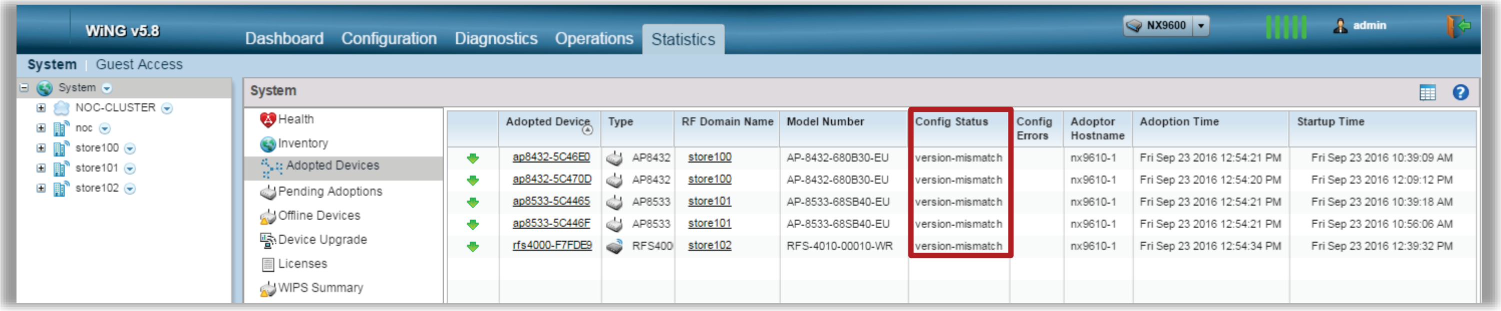
Step 5 – Upgrade the Remote Site

Once the remote Access Points and/or Site Controllers have re-adopted to the active Controller, they can be upgraded on a per site basis to the new WING release.

When the Access Points / Site Controllers adopt they will display a version-mismatch. The Controller will not be able to apply any configuration changes to the Access Points until they are upgraded to the same WING release. Access Points with existing configurations will continue to operate and service clients with no interruption. 802.1X clients will also be able to authenticate when RADIUS is proxied through the Controllers.

```
nx9610-1# show adoption status
-----------------------------------------------------------------------------------------------------------
----
DEVICE-NAME        VERSION          CFG-STAT         MSGS  ADOPTED-BY        LAST-ADOPTION
UPTIME
-----------------------------------------------------------------------------------------------------------
----
ap8533-5C4465      5.8.4.0-034R     version-mismatch No    nx9610-1             0 days 00:00:14     0 days
02:15:17
ap8533-5C446F      5.8.4.0-034R     version-mismatch No    nx9610-1             0 days 00:00:14     0 days
01:58:29
ap8432-5C46E0      5.8.4.0-034R     version-mismatch No    nx9610-1             0 days 00:00:14     0 days
02:15:26
ap8432-5C470D      5.8.4.0-034R     version-mismatch No    nx9610-1             0 days 00:00:15     0 days
00:45:23
rfs4000-F7FDE9     5.8.4.0-034R     version-mismatch No    nx9610-1             0 days 00:00:01     0 days
00:15:03
-----------------------------------------------------------------------------------------------------------
-----
Total number of devices displayed: 5
```

Statistics -> <rf-domain-name> -> <hostname> -> Adoption -> Adopted Devices



	Adopted Device	Type	RF Domain Name	Model Number	Config Status	Config Errors	Adoptor Hostname	Adoption Time	Startup Time
⬇	ap8432-5C46E0	AP8432	store100	AP-8432-680B30-EU	version-mismatch		nx9610-1	Fri Sep 23 2016 12:54:21 PM	Fri Sep 23 2016 10:39:09 AM
⬇	ap8432-5C470D	AP8432	store100	AP-8432-680B30-EU	version-mismatch		nx9610-1	Fri Sep 23 2016 12:54:20 PM	Fri Sep 23 2016 12:09:12 PM
⬇	ap8533-5C4465	AP8533	store101	AP-8533-68SB40-EU	version-mismatch		nx9610-1	Fri Sep 23 2016 12:54:21 PM	Fri Sep 23 2016 10:39:18 AM
⬇	ap8533-5C446F	AP8533	store101	AP-8533-68SB40-EU	version-mismatch		nx9610-1	Fri Sep 23 2016 12:54:21 PM	Fri Sep 23 2016 10:56:06 AM
⬇	rfs4000-F7FDE9	RFS400	store102	RFS-4010-00010-WR	version-mismatch		nx9610-1	Fri Sep 23 2016 12:54:34 PM	Fri Sep 23 2016 12:39:32 PM

Device Upgrade – CLI

Each site is upgraded using the **`device-upgrade`** command which can be issued against multiple sites simultaneously. The **`device-upgrade`** command allows administrators to define which sites are upgraded, which models of Access Points are upgraded, when the upgrades are to be performed and if and when the Access Points are rebooted. It is important to note that an RF Domain Manager can upgrade different Access Point model types.

The following provides an overview of the device-upgrade command syntax and options:

```
device-upgrade <device-scope> <device-model-scope> <options>
<device-scope> - Defines the scope of devices to be upgraded. Can be an individual Access Point, Access
Points of a specific model, Access Points within a specific RF Domain or all Access Points adopted to the
system:
       all - Upgrade all Access Points
       rf-domain <rf-domain-name> - Upgrade all Access Points belonging to an RF Domain
       <device-hostname> - Upgrade an individual Access Point or Site Controller
<device-model-scope> - When upgrading an RF Domain allows you to specify which Access Point model you wish
to upgrade. If not specified, all Access Point and Site Controller models are upgraded:
       ap6521 - Upgrades only AP 6521 Access Points
       ap6522 - Upgrades only AP 6522 Access Points
       ap6532 - Upgrades only AP 6532 Access Points
       ap7532 - Upgrades only AP 7532 Access Points
       ...
<options> - Allows additional options to be specified such as scheduling and how the Access Points are
rebooted:
       no-reboot - Access Points will not be rebooted after the upgrade
       from-controller- The upgrade will not be performed directly via the controller
       staggered-reboot - Reboots the Access Points one at a time
       upgrade-time MM/DD/YYYY-HH:MM - Upgrade the Access Points at a specific Date / Time
       reboot-time MM/DD/YYYY-HH:MM - Reboot the Access Points at a specific Date / Time
```

Note

If the no-reboot parameter is selected, the remote APs can be rebooted at a later time using the reload on <rf-domain> command from the Controller.

Note

To minimize the impact of the upgrade at the remote site, the staggered-reboot option will reboot each Access Point individually.

The device-upgrade command can be issued multiple times allowing multiple RF Domains to be upgraded simultaneously. By default, the Controllers can upgrade 10 x RF Domain Managers (or sites) simultaneously; however, this can be increased to 128 x RF Domain Managers (sites) if desired by increasing the number of concurrent Access Point upgrades to 128 in the Controller profile.

The following demonstrates how to upgrade Access Points in a specific RF Domains using the device-upgrade command:

1. When the device-upgrade command is issued against a specific RF Domain, the RF Domain Manager for the site is added to the upgrade queue:

```
nx9610-1# device-upgrade rf-domain store101 all
-------------------------------------------------------------------------------------
      CONTROLLER       STATUS                         MESSAGE
-------------------------------------------------------------------------------------
  84-24-8D-7F-34-C7   Success   store101(device type(s) ap8533 added for upgrade),
-------------------------------------------------------------------------------------
```

```
nx9000-1# device-upgrade rf-domain store100 all
-------------------------------------------------------------------------------------
      CONTROLLER       STATUS                         MESSAGE
-------------------------------------------------------------------------------------
  84-24-8D-7F-34-C7   Success   store100(device type(s) ap8432 added for upgrade),
-------------------------------------------------------------------------------------
```

```
nx9000-1# device-upgrade rf-domain store102 all
-------------------------------------------------------------------------------------
      CONTROLLER       STATUS                         MESSAGE
-------------------------------------------------------------------------------------
  84-24-8D-7F-34-C7   Success   store100(device type(s) ap8432 added for upgrade),
-------------------------------------------------------------------------------------
```

2. The Controller will download the necessary firmware image to elected RF Domain Manager (RFDM) for each site. If multiple Access Point models exist within the site, the RFDM will upgrade each model of Access Points first and upgrade its model type last:

```
nx9000-1# show device-upgrade status
Number of APs currently being upgraded : 2
Number of APs waiting in queue to be upgraded : 0
Number of APs currently being rebooted : 0
Number of APs waiting in queue to be rebooted : 0
-----------------------------------------------------------------------------------------------------------
     AP           STATE     UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR       UPGRADED BY
-----------------------------------------------------------------------------------------------------------
  ap6532-S1AP3   downloading   immediate    immediate   12       0       -                5C-0E-8B-33-EE-70
  ap6532-S2AP2   downloading   immediate    immediate   11       0       -                5C-0E-8B-33-EE-70
-----------------------------------------------------------------------------------------------------------
```

3. The RF Domain Managers will download the firmware image to the Access Points within the site. By default, each RF Domain Manager can upgrade 10 Access Points simultaneously. If more than 10 Access Points are present at the remote site, the RF Domain Manager will upgrade the first 10 Access Points followed by the next 10 Access Points (and so forth) until all the Access Points at the site have been upgraded:

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
------------------------------------------------------------------------------------------------------------
  DEVICE            STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR    UPGRADED BY
------------------------------------------------------------------------------------------------------------
  ap8432-5C46E0   upgrading-devices   immediate    immediate    0        0       -             ap8432-5C46E0
  ap8432-5C470D   waiting             immediate    immediate    0        0       -             ap8432-5C46E0
  ap8533-5C446F   downloading         immediate    immediate    77       0       -             ap8533-5C4465
  ap8533-5C4465   upgrading-devices   immediate    immediate    0        0       -             ap8533-5C4465
------------------------------------------------------------------------------------------------------------
```

4. Once the firmware has been downloaded to the Access Points they will transition to an updating state. During this time the firmware image is being installed into the Primary or Secondary image slots on the Access Points:

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 2
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 1
Number of devices failed upgrade : 0
------------------------------------------------------------------------------------------------------------
 DEVICE            STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR    UPGRADED BY
------------------------------------------------------------------------------------------------------------
ap8432-5C46E0   upgrading-devices   immediate    immediate    0         0         -             ap8432-5C46E0
  ap8432-5C470D   downloading         immediate    immediate    46       0       -             ap8432-5C46E0
  ap8533-5C446F   wait for reboot     immediate    immediate    0        0       -             ap8533-5C4465
  ap8533-5C4465   updating            immediate    immediate    0        0       -             ap8533-5C4465
------------------------------------------------------------------------------------------------------------
```

5. Once all the Access Points within the site have been upgraded, the RF Domain Manager will update itself last.

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 2
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 1
Number of devices failed upgrade : 0
------------------------------------------------------------------------------------------------------------
DEVICE            STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR    UPGRADED BY
------------------------------------------------------------------------------------------------------------
--------
ap8432-5C46E0   upgrading-devices   immediate    immediate    0         0       -               ap8432-5C46E0
ap8432-5C470D   updating            immediate    immediate    0         0       -               ap8432-5C46E0
ap8533-5C446F   wait for reboot     immediate    immediate    0         0       -               ap8533-5C4465
ap8533-5C4465   updating            immediate    immediate    76        0       -               ap8533-5C4465
------------------------------------------------------------------------------------------------------------
```

6. In this example the Access Points were rebooted upon upgrading. Once the RF Domain Manager has completed its upgrade, it will reboot all the Access Points at the site in addition to itself.

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 2
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----------------------------------------------------------------------------------------------------------
DEVICE            STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR    UPGRADED BY
-----------------------------------------------------------------------------------------------------------
  ap8432-5C46E0   rebooting-devices   immediate    immediate   0        0       -             ap8432-5C46E0
  ap8432-5C470D   rebooting           immediate    immediate   0        0       -             ap8432-5C46E0
  ap8533-5C446F   rebooting           immediate    immediate   0        0       -             ap8533-5C4465
  ap8533-5C4465   rebooting-devices   immediate    immediate   0        0       -             ap8533-5C4465
-----------------------------------------------------------------------------------------------------------
```

7. In this next example the upgrade will be done for the Site Controller RF Domain store102 with RFS 4000 acting as a single site controller. First the Site Controller will receive an image for itself, perform an upgrade before upgrading local APs.

```
nx9610-1# device-upgrade rf-domain store102 all
-------------------------------------------------------------------------------------
      CONTROLLER       STATUS                         MESSAGE
-------------------------------------------------------------------------------------
  84-24-8D-7F-34-C7   Success   store102(device type(s) rfs4000 added for upgrade),
-------------------------------------------------------------------------------------
```

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
-----------------------------------------------------------------------------------------------------------
      DEVICE          STATE     UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR    UPGRADED BY
-----------------------------------------------------------------------------------------------------------
  rfs4000-F7FDE9   downloading   immediate    immediate   63       0       -                 rfs4000-F7FDE9
-----------------------------------------------------------------------------------------------------------
```

```
nx9610-1# show device-upgrade status
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 0
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----------------------------------------------------------------------------------------------------------
      DEVICE        STATE    UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR     UPGRADED BY
-----------------------------------------------------------------------------------------------------------
  rfs4000-F7FDE9   updating   immediate    immediate   54       0       -                 rfs4000-F7FDE9
-----------------------------------------------------------------------------------------------------------
```

8. After upgrade is done Site Controller (s) will reboot to the new firmware version.

```
nx9610-1# show device-upgrade status
nx9610-1#show device-upgrade status
Number of devices currently being upgraded : 0
Number of devices waiting in queue to be upgraded : 0
Number of devices currently being rebooted : 1
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----------------------------------------------------------------------------------------------------------
DEVICE            STATE         UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR     UPGRADED BY
-----------------------------------------------------------------------------------------------------------
rfs4000-F7FDE9   active-sw-rebooting   immediate    immediate   0        0       -           rfs4000-F7FDE9
rfs4000-F7FDE9   rebooting             immediate    immediate   0        0       -           rfs4000-F7FDE9
-----------------------------------------------------------------------------------------------------------
```

10. After Site Controller will come back and re-adopt all local APs, they will receive images for the APs, starting from the top-high model to the lowest one.

```
nx9610-1# show device-upgrade status on store102
Number of devices currently being upgraded : 1
Number of devices waiting in queue to be upgraded : 1
Number of devices currently being rebooted : 2
Number of devices waiting in queue to be rebooted : 0
Number of devices failed upgrade : 0
-----------------------------------------------------------------------------------------------------------
DEVICE             STATE        UPGRADE TIME REBOOT TIME PROGRESS RETRIES LAST UPDATE ERROR     UPGRADED BY
-----------------------------------------------------------------------------------------------------------
ap7502-645A12     waiting-for-image   immediate    immediate   75       0       -            rfs4000-F7FDE9
ap7532-8641A8     downloading         immediate    immediate   79       0       -            rfs4000-F7FDE9
ap8533-07093D     rebooting           immediate    immediate   0        0       -            rfs4000-F7FDE9
ap8533-07081B     rebooting           immediate    immediate   0        0       -            rfs4000-F7FDE9
-----------------------------------------------------------------------------------------------------------
```

Note

Access Point upgrades can be cancelled at any time by issuing the device-upgrade cancel on rf-domain <rf-domain-name> command.

Note

If the Access Points are not rebooted after the upgrade, you will need to connect to one of the remote Access Points at each site to initiate the reboot using the reload on <rf-domain> command.

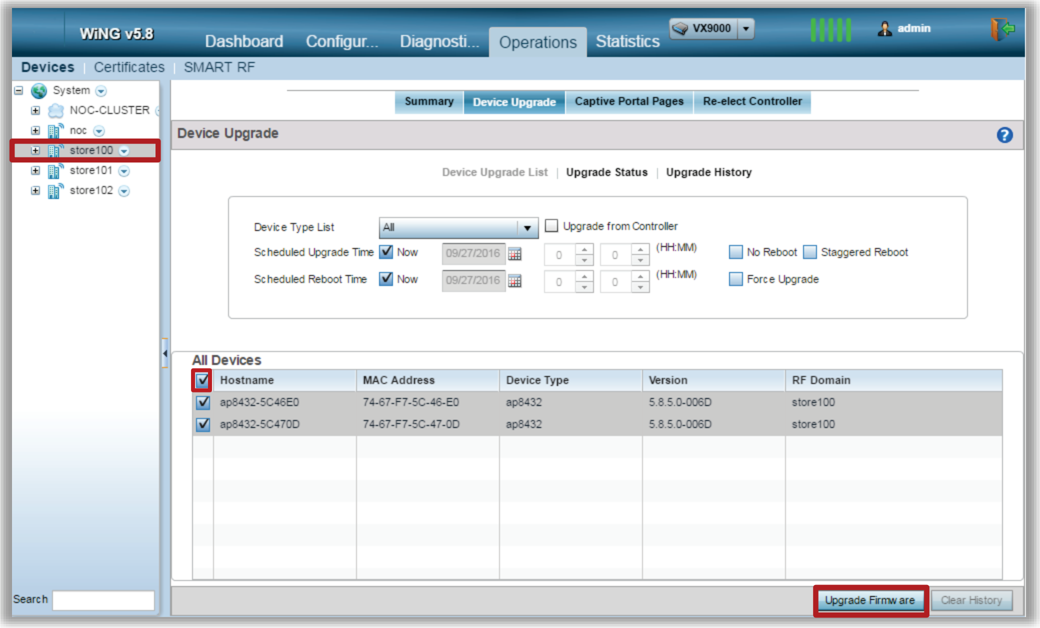
Note

A history of the Access Point upgrades can be viewed by issuing the show device-upgrade history on <rf-domain-name> command.

Device Upgrade – Web UI

The following demonstrates how to upgrade APs in a specific RF Domains using the Web-UI:

1. Select Operations -> <rf-domain-name> -> Device Upgrade List. Select the upgrade and reboot options then select Update Firmware:

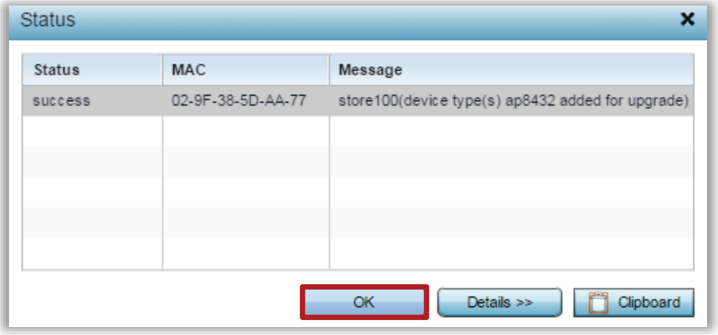


Device Type List: All
☐ Upgrade from Controller
Scheduled Upgrade Time ☑ Now 09/27/2016 0 0 (HH:MM) ☐ No Reboot ☐ Staggered Reboot
Scheduled Reboot Time ☑ Now 09/27/2016 0 0 (HH:MM) ☐ Force Upgrade

All Devices

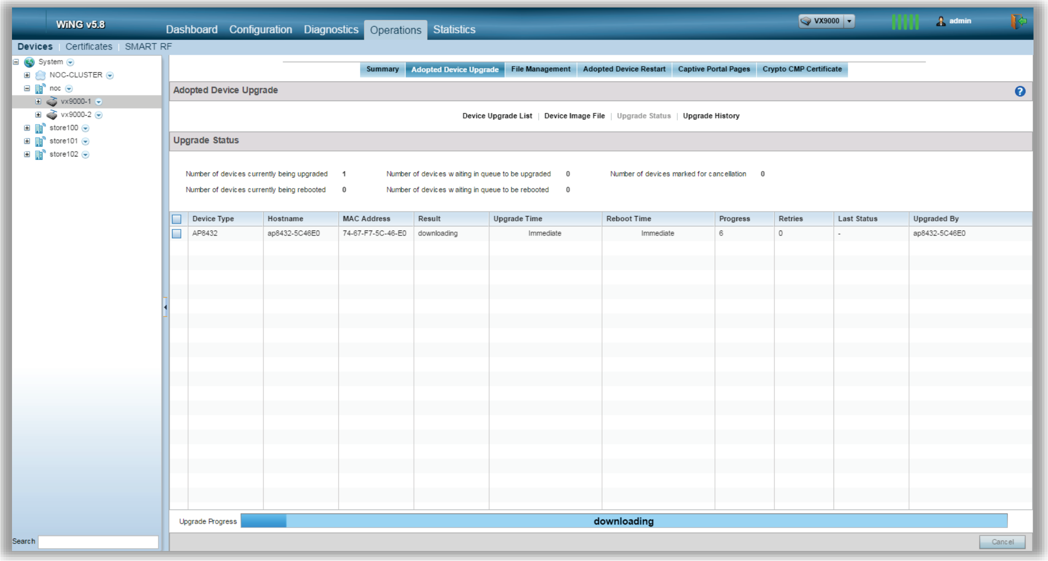
☑	Hostname	MAC Address	Device Type	Version	RF Domain
☑	ap8432-5C46E0	74-67-F7-5C-46-E0	ap8432	5.8.5.0-006D	store100
☑	ap8432-5C470D	74-67-F7-5C-47-0D	ap8432	5.8.5.0-006D	store100

2. Select OK:



Status	MAC	Message
success	02-9F-38-5D-AA-77	store100(device type(s) ap8432 added for upgrade)

3. The firmware image will be downloaded to the RF Domain Manager for the site:



Adopted Device Upgrade

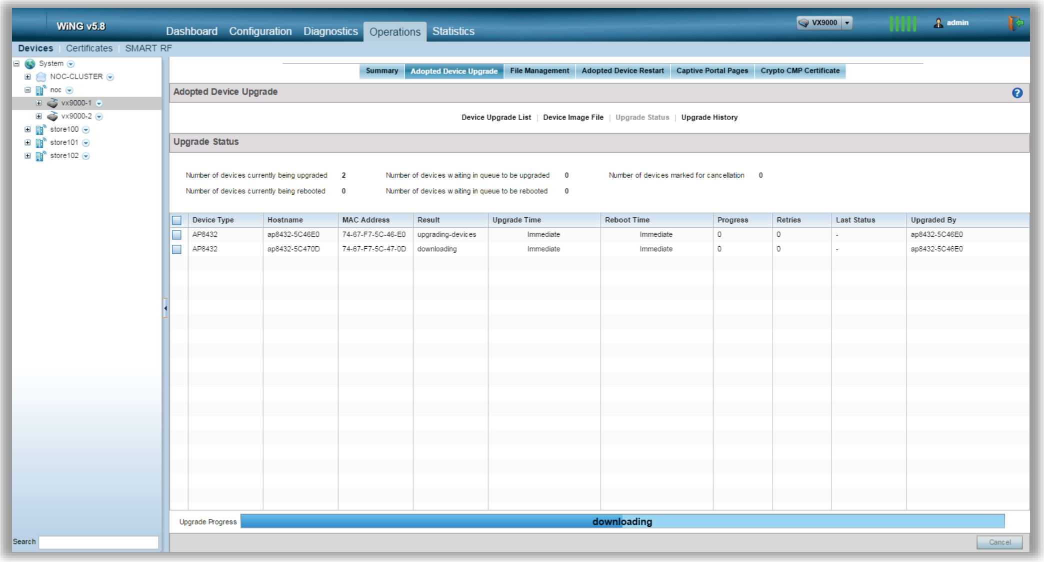
Upgrade Status

Number of devices currently being upgraded 1
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	AP8432	ap8432-5C46E0	74-67-F7-5C-46-E0	downloading	Immediate	Immediate	6	0	-	ap8432-5C46E0

Upgrade Progress downloading

4. The RF Domain Manager will upgrade all the Access Points within the site:



Adopted Device Upgrade

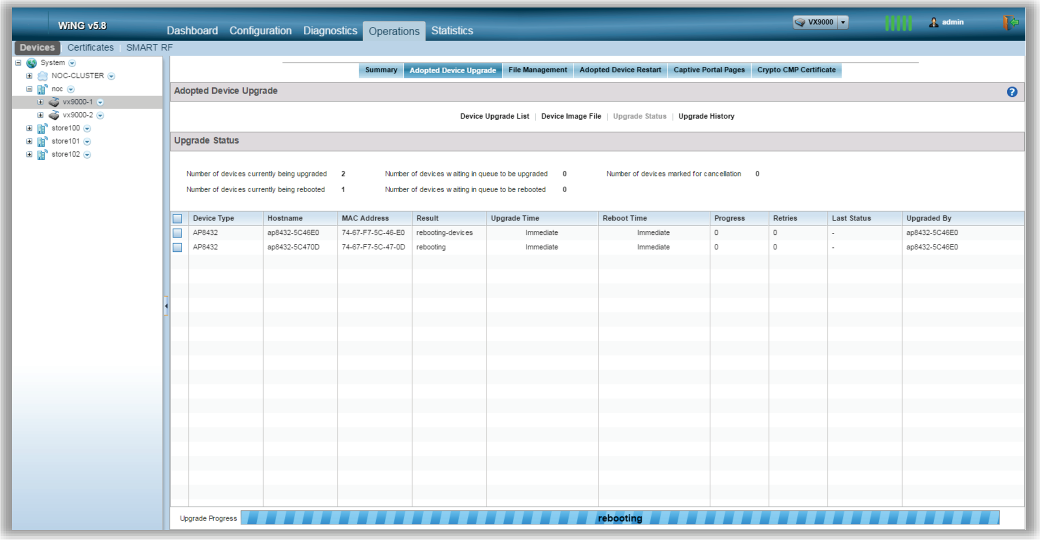
Upgrade Status

Number of devices currently being upgraded 2
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	AP8432	ap8432-5C46E0	74-67-F7-5C-46-E0	upgrading-devices	Immediate	Immediate	0	0	-	ap8432-5C46E0
□	AP8432	ap8432-5C470D	74-67-F7-5C-47-0D	downloading	Immediate	Immediate	0	0	-	ap8432-5C46E0

Upgrade Progress downloading

5. If the Reboot or Staggered Reboot option was selected, the Access Points at the site will be rebooted:



Adopted Device Upgrade

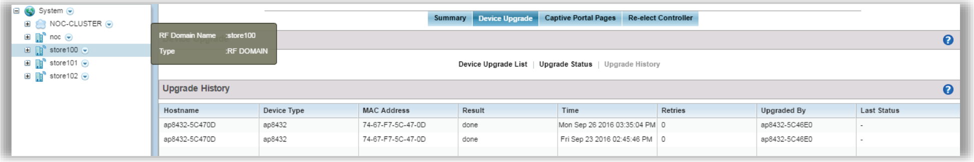
Upgrade Status

Number of devices currently being upgraded 2
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 1
Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	AP8432	ap8432-5C46E0	74-67-F7-5C-46-E0	rebooting-devices	Immediate	Immediate	0	0	-	ap8432-5C46E0
□	AP8432	ap8432-5C470D	74-67-F7-5C-47-0D	rebooting	Immediate	Immediate	0	0	-	ap8432-5C46E0

Upgrade Progress rebooting

6. Once the upgrade has been completed, the results of the upgrade will be displayed in the Upgrade History for the site:



RF Domain Name :store100
Type :RF DOMAIN

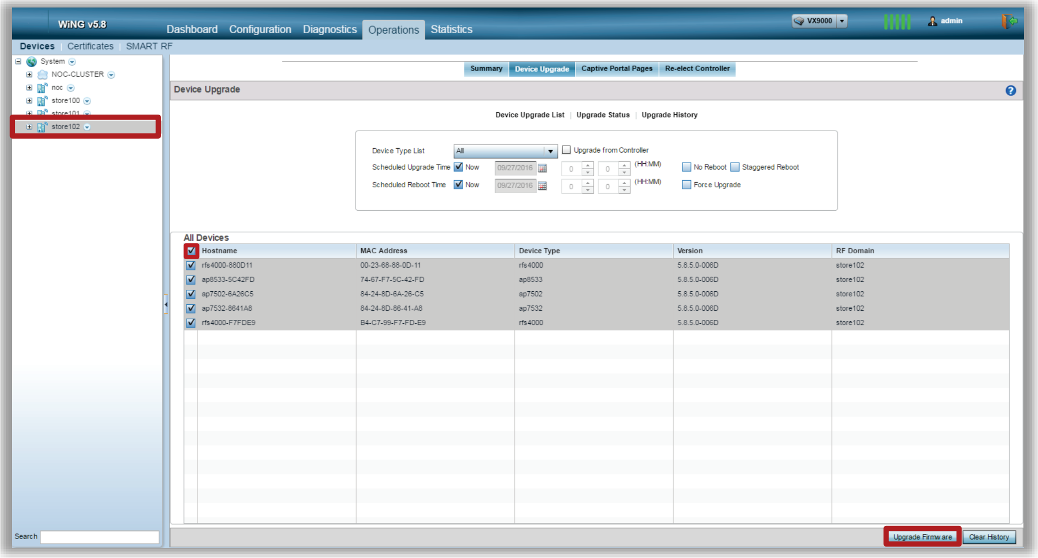
Upgrade History

Hostname	Device Type	MAC Address	Result	Time	Retries	Upgraded By	Last Status
ap8432-5C470D	ap8432	74-67-F7-5C-47-0D	done	Mon Sep 26 2016 03:35:04 PM	0	ap8432-5C46E0	-
ap8432-5C470D	ap8432	74-67-F7-5C-47-0D	done	Fri Sep 23 2016 02:45:46 PM	0	ap8432-5C46E0	-

The following demonstrates how to upgrade APs with Site Controllers in a specific RF Domains using the Web-UI:

1. The following demonstrates how to upgrade APs with Site Controllers in a specific RF Domains using the Web-UI:

   Select Operations -> <rf-domain-name> -> Device Upgrade List. Select the upgrade and reboot options then select Update Firmware:



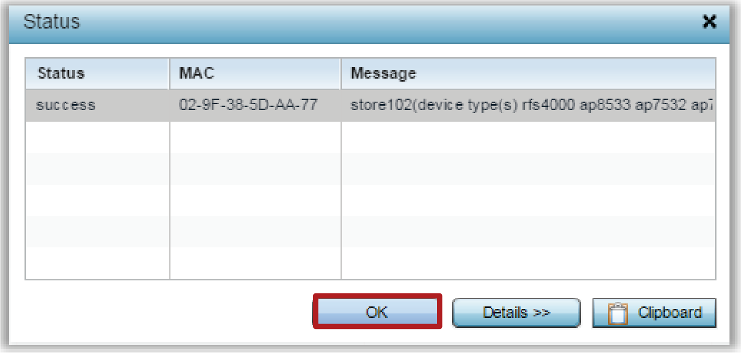
Device Upgrade

Device Type List: All ☐ Upgrade from Controller
Scheduled Upgrade Time ☑ Now 09/27/2016 0 0 (HH:MM) ☐ No Reboot ☐ Staggered Reboot
Scheduled Reboot Time ☑ Now 09/27/2016 0 0 (HH:MM) ☐ Force Upgrade

All Devices

☑	Hostname	MAC Address	Device Type	Version	RF Domain
☑	rfs4000-880D11	00-23-68-88-0D-11	rfs4000	5.8.5.0-006D	store102
☑	ap8533-5C42FD	74-67-F7-5C-42-FD	ap8533	5.8.5.0-006D	store102
☑	ap7502-6A26C5	84-24-8D-6A-26-C5	ap7502	5.8.5.0-006D	store102
☑	ap7532-8641A8	84-24-8D-86-41-A8	ap7532	5.8.5.0-006D	store102
☑	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	rfs4000	5.8.5.0-006D	store102

2. Select OK:

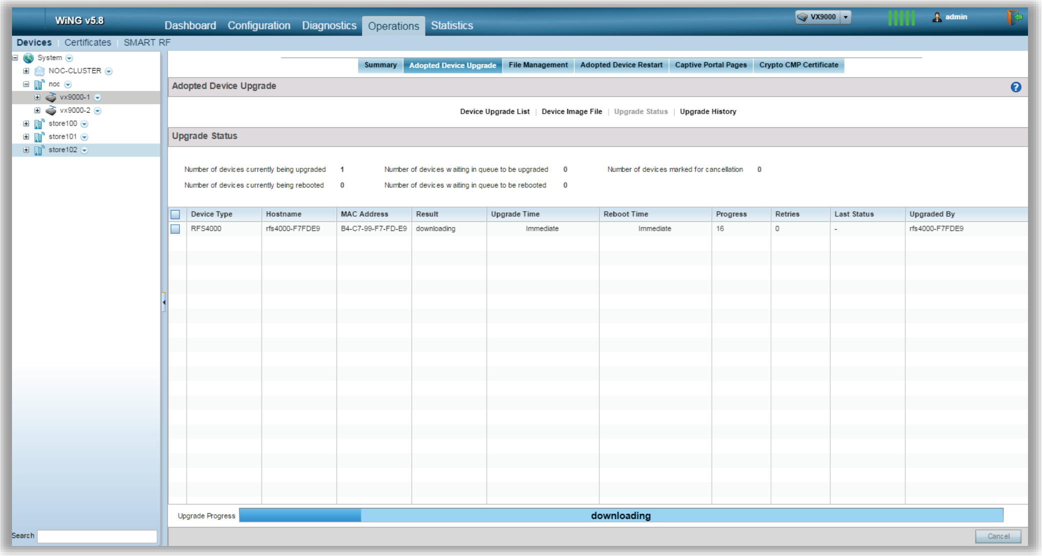


Status	MAC	Message
success	02-9F-38-5D-AA-77	store102(device type(s) rfs4000 ap8533 ap7532 ap7

3. The firmware image will be downloaded to the RF Domain Manager / Cluster Master for the site.

   Standby Site Controller will be upgraded first, followed by the Active Site Controller.

   After both Site Controllers are upgraded, Active member will reboot, while Standby will take over the cluster:



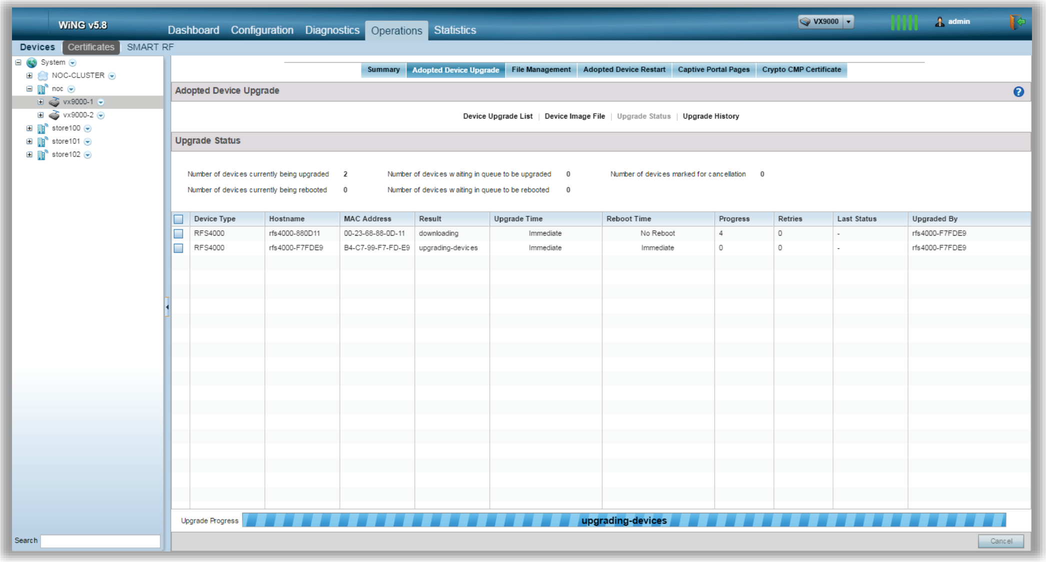
Adopted Device Upgrade

Upgrade Status

Number of devices currently being upgraded 1
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

☐	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
☐	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	downloading	Immediate	Immediate	16	0	-	rfs4000-F7FDE9

Upgrade Progress downloading



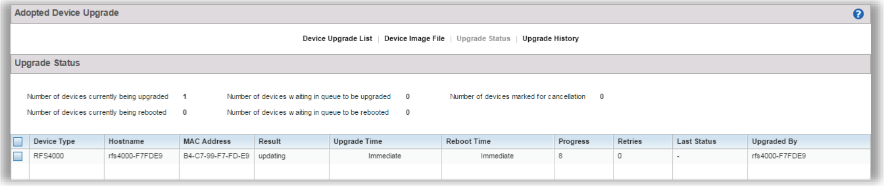
Adopted Device Upgrade

Upgrade Status

Number of devices currently being upgraded 2
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

☐	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
☐	RFS4000	rfs4000-880D11	00-23-68-88-0D-11	downloading	Immediate	No Reboot	4	0	-	rfs4000-F7FDE9
☐	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	upgrading-devices	Immediate	Immediate	0	0	-	rfs4000-F7FDE9

Upgrade Progress upgrading-devices

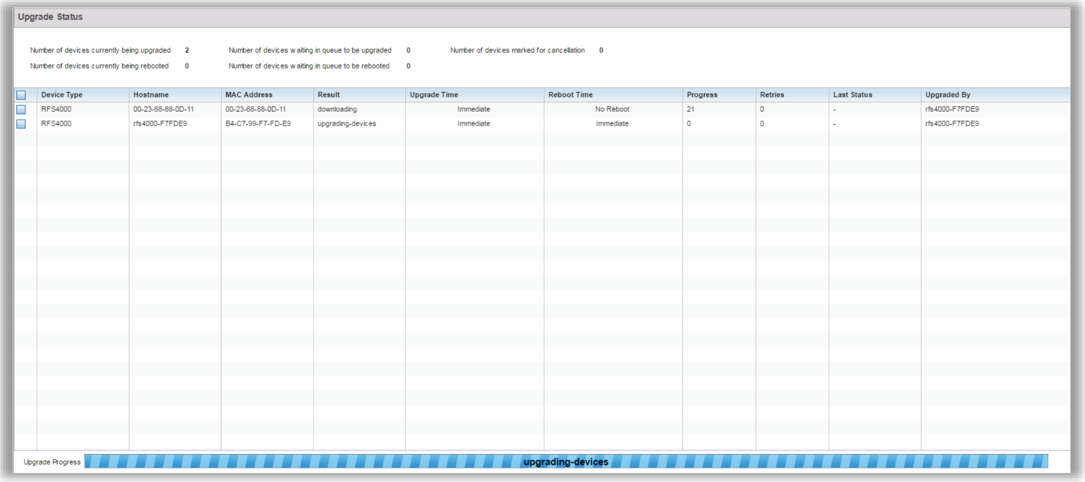


Adopted Device Upgrade

Upgrade Status

Number of devices currently being upgraded 1
Number of devices waiting in queue to be upgraded 0
Number of devices marked for cancellation 0
Number of devices currently being rebooted 0
Number of devices waiting in queue to be rebooted 0

☐	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
☐	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	updating	Immediate	Immediate	8	0	-	rfs4000-F7FDE9



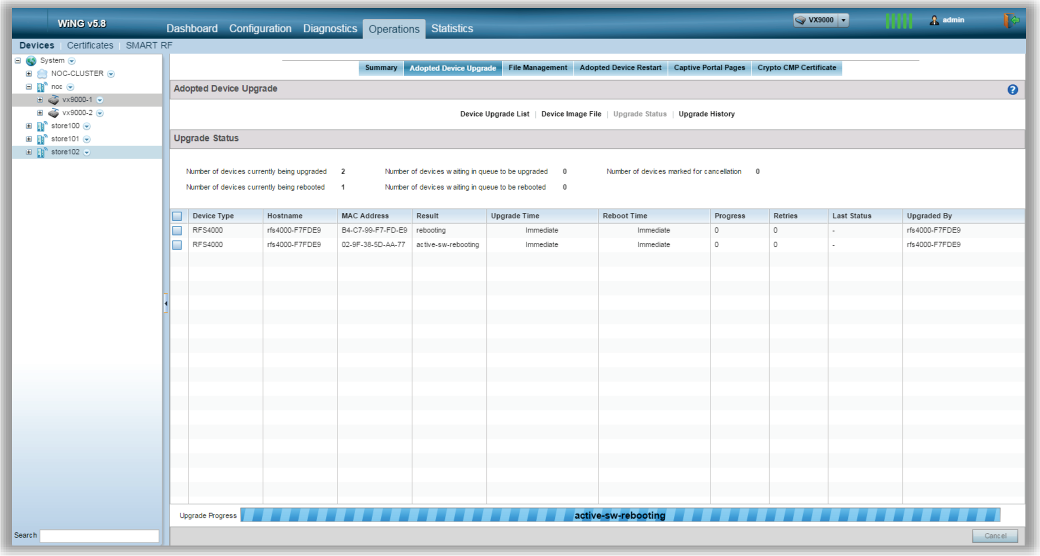
Upgrade Status

Number of devices currently being upgraded 2 | Number of devices waiting in queue to be upgraded 0 | Number of devices marked for cancellation 0

Number of devices currently being rebooted 0 | Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	RFS4000	00-23-68-88-0D-11	00-23-68-88-0D-11	downloading	Immediate	No Reboot	21	0	-	rfs4000-F7FDE9
□	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	upgrading-devices	Immediate	Immediate	0	0	-	rfs4000-F7FDE9

4. The Site Controller(s) will reboot prior to upgrading the local APs:

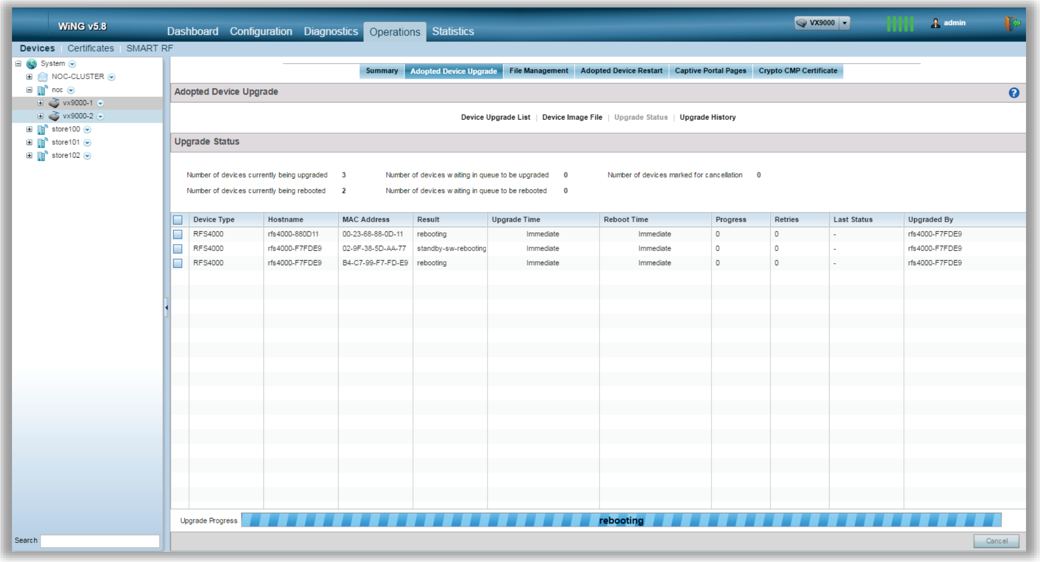


Upgrade Status

Number of devices currently being upgraded 2 | Number of devices waiting in queue to be upgraded 0 | Number of devices marked for cancellation 0

Number of devices currently being rebooted 1 | Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	rebooting	Immediate	Immediate	0	0	-	rfs4000-F7FDE9
□	RFS4000	rfs4000-F7FDE9	02-9F-38-5D-AA-77	active-sw-rebooting	Immediate	Immediate	0	0	-	rfs4000-F7FDE9



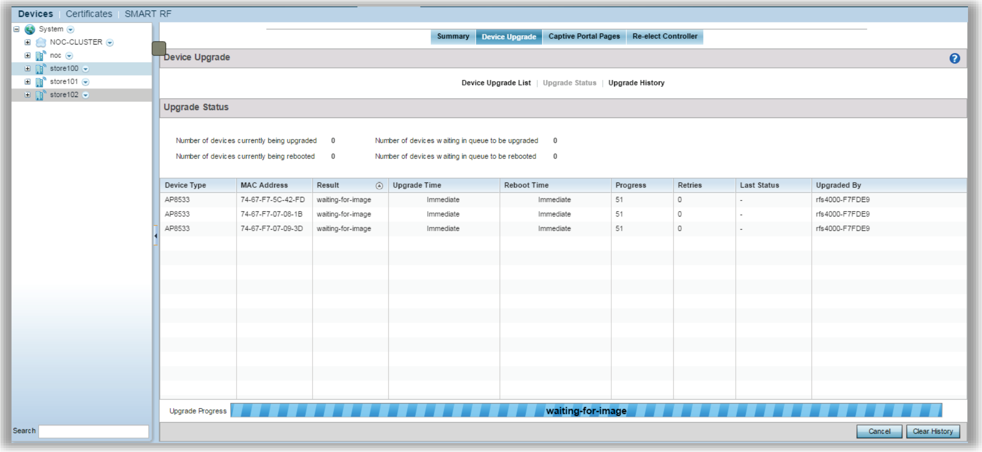
Upgrade Status

Number of devices currently being upgraded 3 | Number of devices waiting in queue to be upgraded 0 | Number of devices marked for cancellation 0

Number of devices currently being rebooted 2 | Number of devices waiting in queue to be rebooted 0

□	Device Type	Hostname	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
□	RFS4000	rfs4000-880D11	00-23-68-88-0D-11	rebooting	Immediate	Immediate	0	0	-	rfs4000-F7FDE9
□	RFS4000	rfs4000-F7FDE9	02-9F-38-5D-AA-77	standby-sw-rebooting	Immediate	Immediate	0	0	-	rfs4000-F7FDE9
□	RFS4000	rfs4000-F7FDE9	B4-C7-99-F7-FD-E9	rebooting	Immediate	Immediate	0	0	-	rfs4000-F7FDE9

5. The Master Site Controller will start upgrading local APs:

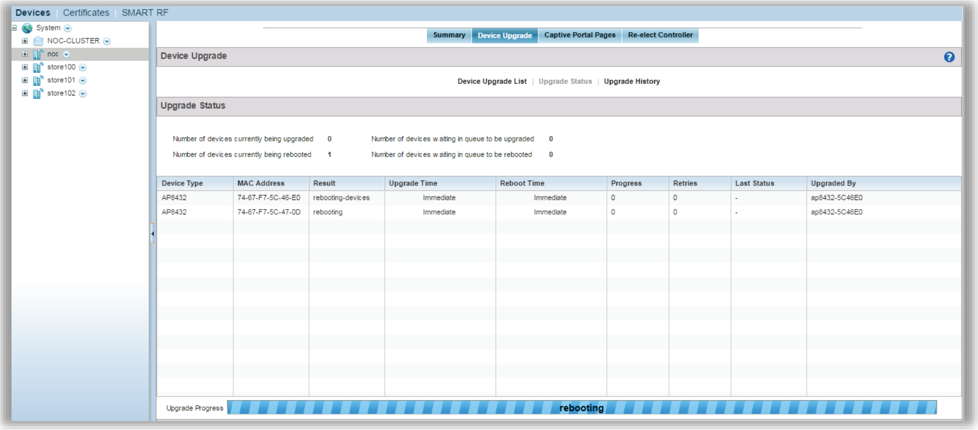


Number of devices currently being upgraded 0 | Number of devices waiting in queue to be upgraded 0

Number of devices currently being rebooted 0 | Number of devices waiting in queue to be rebooted 0

Device Type	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
AP8533	74-67-F7-5C-42-FD	waiting-for-image	Immediate	Immediate	51	0	-	rfs4000-F7FDE9
AP8533	74-67-F7-07-08-1B	waiting-for-image	Immediate	Immediate	51	0	-	rfs4000-F7FDE9
AP8533	74-67-F7-07-09-3D	waiting-for-image	Immediate	Immediate	51	0	-	rfs4000-F7FDE9

6. If the Reboot or Staggered Reboot option was selected, the Access Points at the site will be rebooted:

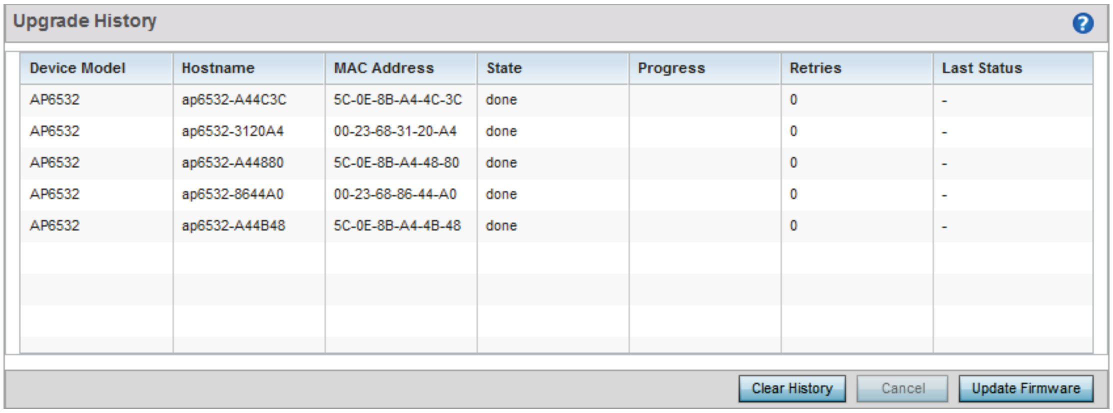


Number of devices currently being upgraded 0 | Number of devices waiting in queue to be upgraded 0

Number of devices currently being rebooted 1 | Number of devices waiting in queue to be rebooted 0

Device Type	MAC Address	Result	Upgrade Time	Reboot Time	Progress	Retries	Last Status	Upgraded By
AP8432	74-67-F7-5C-46-E0	rebooting-devices	Immediate	Immediate	0	0	-	ap8432-5C46E0
AP8432	74-67-F7-5C-47-0D	rebooting	Immediate	Immediate	0	0	-	ap8432-5C46E0

7. Once the upgrade has been completed, the results of the upgrade will be displayed in the Upgrade History for the site:



Device Model	Hostname	MAC Address	State	Progress	Retries	Last Status
AP6532	ap6532-A44C3C	5C-0E-8B-A4-4C-3C	done		0	-
AP6532	ap6532-3120A4	00-23-68-31-20-A4	done		0	-
AP6532	ap6532-A44880	5C-0E-8B-A4-48-80	done		0	-
AP6532	ap6532-8644A0	00-23-68-86-44-A0	done		0	-
AP6532	ap6532-A44B48	5C-0E-8B-A4-4B-48	done		0	-

Appendix

Licensing

Wireless controllers require licensing to determine how many Site Controllers and APs can be adopted and managed in a system as well as enable advanced features or services on a device. Most of the features such as Stateful Packet Inspection Firewall, IP Routing and IPsec VPN are included free of charge as part of the WING 5 operating system with no additional licensing being required. However, feature licenses are required to enable advanced features and services such as the Web Filtering and NSight.

> Note
>
> The acquisition and installation of AP, AAP and feature licenses is out of the scope of this guide.

Access Point Licenses

WING 5 devices support two types of Access Point licenses (AP and AAP):

- AP Licenses – Supported by RFS, AP licenses can be used adopt and manage legacy AP 300 APs as well as newer Independent or Dependent APs. This is a legacy license type and is no longer available for purchase, as AP300 is no longer supported by the current WING 5 firmware.
- AAP Licenses – Supported by RFS / NX / VX, AAP licenses and can be used to adopt and manage WING 5 APs, but not legacy AP 300 APs. For centrally managed deployments AAP license may also be used to adopt and manage remote Site Controllers.

RFS Controllers

RFS can adopt and manage WING 5 APs, while RFS 7000s can also adopt and manage Site Controllers. Each AP and Site Controller that is adopted and managed by a standalone RFS or cluster requires an AP or AAP license.

Each model of RFS supports a specific number of AP and AAP licenses (depending on its hardware capabilities) and the AP / AAP licenses are sold in license packs of varying sizes:

- RFS 4000 – each RFS 4000 includes 6 x AP licenses and supports a total adoption capacity of 144 x Access Points. AAP license packs are available for purchase in increments of 6, 12, 24 and 48 licenses.
- RFS 6000 (legacy) – each RFS 6000 can be purchased with 0, 8, 12, 24 and 48 x AP licenses and supports a total adoption capacity of 256 x Dependent or Independent Access Points. AP license packs are available for purchased in increments of 8 licenses while AAP license packs are available for purchase in increments of 16, 128 or 256 licenses.
- RFS 7000 (legacy) – each RFS 7000 supports a total adoption capacity of 1,024 x Dependent or Independent Access Points and Site Controllers. AP license packs are available for purchase in increments of 16 licenses while AAP license pack are available for purchase in increments of 64, 512 and 1,024 licenses.

Table X provides a summary of the maximum number of AP and AAP licenses supported by each model of RFS:

	RFS 4000	RFS 6000	RFS 7000
Max. AP Licenses	6 (included)	48	256
Max. AAP Licenses	138	256	1,024
Adoption Capacity	144	256	1,024

Network Services Platform

NX controllers can adopt and manage WING 5 AP, while the NX 7500 and NX 9XXX platforms can also adopt and manage Site Controllers. Each AP and Site Controller that is adopted and managed by a standalone NX or cluster requires an AAP license.

Each model of NX supports a specific number of AAP licenses (depending on its hardware capabilities) and the AAP licenses are sold in license packs of varying sizes:

- NX 45XX (legacy) – each NX 4500 / NX 4524 includes 12 x AAP licenses and supports a total adoption capacity of 144 x Access Points.
- NX 65XX (legacy) – each NX 6500 / NX 6524 includes 24 x AAP licenses and supports a total adoption capacity of 264 x Access Points.
- NX 5500 – each NX 5500 includes 0 x AAP licenses and supports a total adoption capacity of 512 x Access Points.
- NX 7500 – each NX 7500 includes 0 x AAP licenses and supports a total adoption capacity of 2,048 x Access Points and Site Controllers.
- NX 9XX0 – each NX 9500 / NX 9510 / NX9600 / NX9610 includes 0 x AAP licenses and supports a total adoption capacity of 10,240 x Access Points and Site Controllers.

The following provides a summary of the maximum number of AAP licenses supported by each model of NX controller:

	NX 45XX	NX 65XX	NX 5500	NX 7500	NX 9XXX
Max. AAP Licenses	144	264	512	2,0418	10,240
Adoption Capacity	144	264	512	2,0418	10,240

VX 9000 (Virtualized WING)

The Virtualized Wireless LAN Controller (VX 9000) can adopt and manage WING 5 APs, as well as Site Controllers. Each AP and Site Controller that is adopted and managed by a standalone VX or cluster requires an AAP license. The VX 9000 can be hosted in the customer’s data center under VMWare ESXi, Citrix XEN or Microsoft Hyper-V or externally hosted in the Amazon EC2 cloud.

Each VX 9000 supports a specific number of AAP licenses (depending on its assigned resources) and the AAP licenses are sold in license packs of varying sizes:

- VX 9000 – each VX 9000 includes 64 x AAP licenses and supports a total adoption capacity of 10,240 x Access Points and Site Controllers.

Tables below provides a summary of the maximum adoption capacity of a VX 9000 based on the allocated resources with and without NSight or Guest Registration Database:

Adoption Capacity	100	500	1,000	2,000	5,000	10,000
vCPU	2	2	4	4	4	8
CPU Clock	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz
Memory	4 GB	4 GB	8 GB	8 GB	16 GB	32 GB
Storage	64 GB	64 GB	64 GB	128 GB	128 GB	256 GB

Adoption Capacity (AP / RF Domain)	100	500 / 100	1,000 / 200	2,000 / 500	5,000 /1000	10,000 / 500
vCPU	8	12	18	24	24	24
CPU Clock	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz	2.5 GHz
Memory (DDR3-L or DDR4)	16 GB	32 GB	40 GB	64 GB	96 GB	128 GB
Storage / Config	500 GB RAID 1+0	500 GB RAID 1+0	500 GB RAID 1+0	500 GB RAID 1+0	4 TB RAID 1+0 4x 800 GB SSD (SLC)	8 TB RAID 1+0 10x 800 GB SSD (SLC)
IOPS	2,000 sustained writes	2,000 sustained writes	3,000 sustained writes	4,000 sustained writes	4,000 sustained writes	4,000 sustained writes

Capacity (User Entries)	1 Million	2 Million
vCPU	6	12
CPU Clock	2.5 GHz	2.5 GHz
Memory (DDR3-L or DDR4)	16 GB	32 GB
Storage / Config	500 GB RAID 1+0	1 TB RAID 1+0

AP / AAP Licensing Strategies

One of the main benefits of the WING 5 is that the architecture supports a large scale centrally managed deployments where up to 10,240 devices can be deployed across hundreds or thousands of remote sites while all being centrally managed from a single cluster of NX 9XX0s or a VX9000.

Each remote site can consist of up to 128 x Access Points (APs) without a Site Controller being present at the site and each adopted and managed AP consumes 1 x AAP license on the Centralized Controllers. Remote sites with greater than 128 x APs require a Site Controller – the selected model being dependent on the type and number of APs at the remote site and the customer's application requirements.

A cluster of Centralized Controllers can now manage remote sites with APs only as well as remote sites with Site Controllers managing APs.

As with APs, each Site Controller that is adopted and managed by a Centralized Controller consumes 1 x AAP license. Therefore, a remote site with a cluster of RFS 6000s will consume 2 x AAP licenses on the Centralized Controllers. However, the APs that are adopted and managed locally by the Site Controllers still require licensing. This is where Hierarchical Management is extremely flexible as the APs can either use the existing AP / AAP licenses installed on their Site Controllers or the Site Controllers can borrow AAP licenses from the Centralized Controllers.

Note

It is important to note that while a Centralized Controller in WING 5 and above can adopt and manage multiple remote Site Controllers, it also maintains configurations for each remote AP that adopted and managed by the remote Site Controllers. As such the number of devices at the remote site (Site Controllers + APs) counts towards the overall adoption capacity of the Centralized Controllers. For example, a centralized cluster of NX 9500s cannot adopt and manage 1,000 remote sites each with clusters of RFS 6000s + 256 x APs (i.e. 268,000 total devices). The cluster would however be able to adopt and manage 39 remote sites each with clusters of RFS 6000s + 256 x APs as this falls below the NX 9500s 10,240 device adoption capacity.

AP / AAP Licensing for Existing Site Controller Deployments

For existing Site Controller deployments, the AP and AAP licenses will already be present and installed on the Site Controllers at each remote site. Each adopted and managed Site Controller will consume 1 x AAP license on the Centralized Controllers while each locally adopted and managed AP will consume 1 x AP or AAP license from the Site Controllers. New AP or AAP licenses will be purchased and applied directly to the Site Controllers.

When calculating the number of AAP licenses for the Centralized Controllers for existing Site Controller deployments, It is important to include AAP licenses for the following devices:

1. Calculate the AAP licenses required to adopt and manage each Independent Access Point for remote sites with fewer than 128 x Access Points.
2. Calculate the AAP licenses required to adopt and manage each remote Site Controller.

Failure to have adequate AAP licenses on the Centralized Controllers will result in Site Controllers or APs failing adopt.

Note

AP and AAP licenses installed on remote Site Controllers cannot be shared between sites. Site Controllers can only obtain leased licenses from the Centralized Controllers.

The following output displays the AAP licenses available on a cluster of NX 9XX0s which are managing a remote site with a cluster of RFS 6000s with 256 x AAP licenses installed. Note that only 2 x AAP licenses have been consumed on the Centralized Controllers to adopt and manage the remote cluster of RFS 6000s. No AAP licenses are consumed on the Centralized Controllers to adopt and manage the local APs at the site as these licenses are applied directly to the Site Controllers:

```
NX9500-DC-1# show licenses
Serial Number : 000C29CC27AE

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 0
  AAP-LICENSE
    String     : <obfuscated string>
    Value      : 10240
  ADVANCED-SECURITY
    String     : <obfuscated string>

Cluster Licenses:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 10240
    Used       : 2

Cluster MAX AP Capacity:
  Value        : 10240
  Used         : 2

Active Members:
-------------------------------------------------------------------------------------------------
 MEMBER             SERIAL               LIC TYPE  VALUE     LENT      TOTAL     NO.APS   NO.AAPS
-------------------------------------------------------------------------------------------------
 00-0C-29-85-09-1D  000C2985091D         AP        0         0         0         0        0
 00-0C-29-85-09-1D  000C2985091D         AAP       0         0         0         -        -
 00-0C-29-CC-27-AE  000C29CC27AE         AP        0         0         0         0        2
 00-0C-29-CC-27-AE  000C29CC27AE         AAP       10240     0         10240     -        -
-------------------------------------------------------------------------------------------------

Total Licenses Including Licenses in Adopted Controllers:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 10240
    Used       : 2
```

The following output displays the AP and AAP licenses available on the remotely managed cluster of RFS 6000s with 256 x AAP licenses installed. This site has 200 x Access Points installed and each Access Point is consuming 1 x AAP license from the RFS 6000 cluster:

```
RFS6K-BRANCH1# show licenses
Serial Number : 10133520400601

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 0
  AAP-LICENSE
    String     : <obfuscated string>
    Value      : 256

Cluster Licenses:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 256
    Used       : 200

Cluster MAX AP Capacity:
  Value        : 256
  Used         : 200

Active Members:
-------------------------------------------------------------------------------------------------
 MEMBER             SERIAL               LIC TYPE  VALUE     BORROWED  TOTAL     NO.APS   NO.AAPS
-------------------------------------------------------------------------------------------------
 00-23-68-64-43-5A  10133520400601       AP        0         0         0         0        200
 00-23-68-64-43-5A  10133520400601       AAP       256       0         256       -        -
 5C-0E-8B-17-E8-F6  10195520400131       AP        0         0         0         0        0
 5C-0E-8B-17-E8-F6  10195520400131       AAP       0         0         0         -        -
-------------------------------------------------------------------------------------------------
```

AAP Licensing for Greenfield Deployments

For new Site Controller deployments, it is recommended that the AAP licenses be purchased and applied directly to the Centralized Controllers. As each Access Point requests adoption to a Site Controller, the Site Controller will borrow 1 x AAP license from the Centralized Controller for each adopted and managed AP at the site. If insufficient AAP licenses are available on the Centralized Controllers, the Site Controller will not permit the adoption of one of more APs.

As with license pooling in clustered environments, leased licenses are persistent between power outages, device resets and network outages. During an extended outage a leased license will remain active on the remote Site Controllers for up to 2,400 hours without communications with the Centralized Controller. Upon re-adoption the Site Controllers will re-request the leased licenses from the Active Centralized Controller. If insufficient AAP licenses are available upon re-adoption, the Site Controller will un-adopt some of its APs based on the number of AAP licenses which were successfully re-borrowed from the Active Centralized Controller.

The following output displays the AAP licenses available on a cluster of NX 9XX0s which are managing a remote site with a cluster of RFS 6000s with zero AP or AAP licenses installed. Note that the cluster of NX 9XX0s has 10,240 x AAP licenses installed where 2 x AAP licenses have been consumed to adopt and manage the cluster of RFS 6000s and 200 x AAP licenses have been lent to the cluster of RFS 6000s to adopt and manage the 200 x APs:

```
NX9000-DC-1#show license
Serial Number : 000C29CC27AE

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 0
  AAP-LICENSE
    String     : <obfuscated string>
    Value      : 10240
  ADVANCED-SECURITY
    String     : <obfuscated string>


Cluster Licenses:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 10040
    Used       : 2

Cluster MAX AP Capacity:
  Value        : 10040
  Used         : 2

Active Members:
-------------------------------------------------------------------------------------------------
 MEMBER             SERIAL               LIC TYPE  VALUE     LENT      TOTAL     NO.APS   NO.AAPS
-------------------------------------------------------------------------------------------------
 00-0C-29-85-09-1D  000C2985091D         AP        0         0         0         0        0
 00-0C-29-85-09-1D  000C2985091D         AAP       0         0         0         -        -
 00-0C-29-CC-27-AE  000C29CC27AE         AP        0         0         0         0        2
 00-0C-29-CC-27-AE  000C29CC27AE         AAP       10240     200       10040     -        -
-------------------------------------------------------------------------------------------------

Total Licenses Including Licenses in Adopted Controllers:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 10240
    Used       : 202
```

The following output displays the AP and AAP licenses available on the remotely managed cluster of RFS 6000s. Note that 200 x AAP licenses have been borrowed from the centralized controllers to adopt and manage the local Dependent Access Points:

```
RFS6K-BRANCH1# show licenses
Serial Number : 10133520400601

Device Licenses:
  AP-LICENSE
    String     :
    Value      : 0
  AAP-LICENSE
    String     :
    Value      : 0

Cluster Licenses:
  AP-LICENSE
    Value      : 0
    Used       : 0
  AAP-LICENSE
    Value      : 3
    Used       : 3

Cluster MAX AP Capacity:
  Value        : 200
  Used         : 200

Active Members:
-------------------------------------------------------------------------------------------------
 MEMBER             SERIAL               LIC TYPE  VALUE     BORROWED  TOTAL     NO.APS   NO.AAPS
-------------------------------------------------------------------------------------------------
 00-23-68-64-43-5A  10133520400601       AP        0         0         0         0        200
 00-23-68-64-43-5A  10133520400601       AAP       0         200       200       -        -
 5C-0E-8B-17-E8-F6  10195520400131       AP        0         0         0         0        0
 5C-0E-8B-17-E8-F6  10195520400131       AAP       0         0         0         -        -
-------------------------------------------------------------------------------------------------
```

When calculating the number of AAP licenses for the Centralized Controllers for new Site Controller deployments, It is important to include AAP licenses for the following devices:

1. Calculate the AAP licenses required to adopt and manage each Access Point for sites with fewer than 128 x APs.
2. Calculate the AAP licenses for each AP which will be leased to the remote Site Controllers.
3. Calculate the AAP licenses required to adopt and manage each remote Site Controller.

Failure to have adequate AAP licenses on the Centralized Controllers will result in Site Controllers or APs failing adopt.

Note

You can issue a clear license lent command on the Centralized Controllers and clear license borrowed command on the remote Site Controller to remove any licenses that have been lent to the Site Controllers.

Feature Licenses

WING 5 supports various advanced features and embedded services which require feature licenses to activate. Feature licenses are platform dependent and support will vary between the different models of RFS and NX controllers. Some feature licenses are included with the purchase of the RFS or NX free of charge while other features require a license to be purchased and installed before activation.

Advanced Security (ADSEC)

Advanced Security Licenses are supported by all RFS, VX and NX platforms to enable the following features:

- Role Based Firewall – Permits IP and MAC firewall rules to be dynamically assigned to Wireless LAN users based on authentication state / type, DHCP fingerprint, encryption type, group membership, LDAP attribute(s) or location. Also permits VLANs to be assigned based on the above.
- IPsec VPN Tunnel Scaling – Increases the number of supported IPsec VPN tunnels from 256 -> 512 (RFS 6000 / NX5500), 512 -> 1,024 (RFS 7000 / NX 7500).

The table below provides summary of the RFS, VX and NX platforms that support the Advanced Feature license:

License	RFS 4000	RFS 6000	NX 45XX	NX 65XX	NX 5500	NX 7500	VX 9000	NX 9XX0
Adv. Security License	Included	Requires License	Requires License	Requires License	Requires License	Requires License	Included	Requires License

An Advanced Security license is included free of charge with the purchase of each RFS 4000 and VX 9000 but must be purchased and installed separately for all other RFS and NX platforms. The Advanced Security license is not shared within a cluster; therefore 1 x Advanced Security License is required for each RFS or NX that is managing Access Points that have Role Policies assigned or require IPsec VPN Tunnel scaling.

Scaling

The Centralized architecture supports up to 10,240 x WING 5 devices, 10,000 remote sites and 400,000 x Wi-Fi clients. Each remote site can support up to 128 x Access Points (APs) without a Site Controller or up to 2,048 x APs with a Site Controller. The total number of WING 5 devices, sites and users is dependent on the model of Centralized Controllers deployed within the customer's data center.

This high scaling is achieved by distributing the management and processing tasks between all the WING 5 devices within the system. The Centralized Controllers provide the main management interface and perform the management, configuration, monitoring and troubleshooting tasks while mobility, packet processing, RF management and policy enforcement is distributed between the WING 5 devices at the remote sites. This approach not only provides industry leading scaling but also site survivability as remote APs can continue to function un-interrupted without communications to the Centralized Controller.

As the functions within the WING 5 system are distributed, the maximum number of APs that can be supported per site is dependent on the types and models of WING 5 devices deployed at each site. For deployment flexibility and investment protection remote sites can be deployed with APs only or Site Controllers managing APs.

Data Center – Centralized Controllers

The model of NX controller you deploy in the Data Center will determine the total number of devices, remote sites and users the system can support. It is important to note that not all models of RFS or NX are supported as Centralized Controllers as not all models of RFS or NX support the adoption and management of Site Controllers.

Table below highlights the supported RFS, VX and NX platforms which can be deployed as Centralized Controllers for small, medium and large centralized deployments:

Model	Managed Devices	Sites	Users
RFS 7000 (legacy)	1,024	1,024	8,192
NX 7500	2,048	2,048	65,536
VX 9000	10,240	10,000	400,000
NX 9XX0	10,240	10,000	400,000

Note
VX 9000 scaling is dependent on the resources assigned to the virtual machine by its host.

Access Point Only Sites

AP only sites can scale to support 128 x APs without a Site Controller being present at the site. The total number of APs that can be deployed is dependent on the AP model that is elected as the RFDM for the site.

Single radio APs have a lower memory footprint than their Dual / Tri Radio counterparts, therefore a Single Radio AP operating as an RFDM can only support a maximum of 24 x APs per site. Remote sites with Dual and/or Tri Radio APs deployed will elect a Dual / Tri Radio AP as the RFDM and can scale higher supporting a maximum of 128 x APs per site.

Remote sites may also be deployed with a combination of Single and Dual / Tri Radio APs. Some mixed AP deployments will include fewer Single Radio APs than Dual / Tri Radio APs ensuring a Dual / Tri Radio AP will always assume the RFDM role. However, it is also possible to deploy site with predominantly Single Radio APs which while supported requires proper planning to ensure an adequate pool of Dual / Tri Radio APs are installed to assume the RFDM role. As a best practice it is recommended that each site include at least two Dual or Tri Radio APs, preferably connected to separate distribution or access layer switches. This ensures that at least one Dual / Tri Radio AP is reachable over the network in the event of a distribution / access layer switch failure. For a mixed site deployment with single radio APs scaling limit is set to 64 x APs per site due to memory constraints on single radio APs.

Additionally, for mixed AP sites it is also a best practice recommendation that you disable the RFDM election capability in the AP Profiles for the Single Radio APs at the site. This ensures that a Single Radio AP cannot be elected as the RFDM in the event that no Dual / Tri Radio APs are available at the site to assume the RFDM role.

Table below highlights the maximum number APs which can be deployed at AP only sites based on the AP models:

AP Types	APs per Site
Single Radio Access Points	24 x Access Points
Mix of Single + Dual + Tri Radio Access Points	64 x Access Points
Dual / Tri Radio Access Points	128 x Access Points
Single Radio Access Points	24 x Access Points

Site Controller / Access Point Sites

Remote sites can be deployed with standalone or a cluster of Site Controllers such as RFS or NX. Remote sites with Site Controllers can scale to support the total adoption capacity of the specific model or RFS or NX deployed at the remote site. The RF Domain Manager (RFDM) role is automatically assumed by the RFS or NX in the cluster with the lowest MINT ID.

While the elected RFDM maintains a Level 2 MINT link to the Active Controller in the data center, it is important to note that APs within the site are adopted and managed by the Site Controllers using Level 1 MINT links. The Site Controllers can either be deployed in an Active / Active or Active / Standby Cluster configuration (Active / Standby is preferred) and the APs can be adopted and managed at Layer 2 or Layer 3 based on scaling requirements.

While Layer 2 adoption is supported, for scaling it is always recommended that you adopt and manage the APs to the Site Controllers at Layer 3. Layer 2 adoption can only scale to support a maximum of 64 x APs if any Single Radio APs are present at the site or 128 x APs if no Single Radio APs are present at the site. If Layer 3 adoption is used, the site can scale to support the adoption capacity of the Site Controllers.

Another consideration when selecting a Site Controller is if tunneling of Wireless LAN traffic is being performed at the site. Each model of RFS / NX supports different hardware architectures and switching capacities and thus can only scale to support a specific number of APs when the APs are encapsulating and forwarding Wireless LAN traffic to the Site Controllers. Legacy platforms such as the RFS 4000, RFS 6000 and RFS 7000 have limited packet switching capacities and can therefore only scale to support a limited number of APs when tunneling is enabled. Next generation platforms such as the NX5500, NX 7500 or NX 9X10 support faster packet processing and backplane to switch or route more traffic and scale higher.

Table 2.3.3 highlights the maximum number of APs which can be deployed at Site Controller / AP only sites based on the Site Controller model:

Model	APs per Site (Local Bridging)	APs per Site (Tunneling)
RFS 4000	144 x Access Points	36 x Access Points
RFS 6000	256 x Access Points	48 x Access Points
RFS 7000	1,024 x Access Points	256 x Access Points
NX 45XX	144 x Access Points	144 x Access Points
NX 65XX	264 x Access Points	264 x Access Points
NX 7500	2,048 x Access Points	1,024 x Access Points
NX 9XX0	2,048 x Access Points	2,048 x Access Points

Bandwidth Requirements

In a centralized deployment remote sites can be connected to the data center using a variety of WAN technologies and services. Most deployments will utilize a private WAN or MPLS service which provide dedicated bandwidth from each remote site. However other deployments may utilize xDSL, DOCSIS or 3G/4G services over the public Internet either for primary WAN connectivity or backup WAN connectivity. Some deployments may utilize a mixture of all technologies depending on which services are available at each site.

The following table provides the recommended minimum bandwidth, latency and MTU recommendations required to support remote Access Points with the centralized model. These values are intended as a basic guideline only as the deployed applications and number of devices at a remote site will ultimately determine the bandwidth and latency requirements for the site:

WAN Characteristic	Minimum
Minimum Bandwidth	256 Kbps
Maximum Latency	< 2,000 ms
Minimum MTU	900 Bytes

Access Point Type	Typical Bandwidth
Access Points	2 - 4 Kbps (Per AP)
Sensor Radio	3 - 5 Kbps (Per Sensor Radio)

By default frequency of RF Domain Manager Controller updates are automatically determined based on the number of remote sites. Typically an RF Domain Manager at a remote site will update the Controllers in the data center once per minute. The update interval can be configured by changing the noc update-interval value <5-3600> in seconds on the Wireless Controllers. A shorter update-interval will result in more WAN bandwidth being required to support each remote site.

When Access Points at remote sites boot and receive their initial configuration they will require a small amount of additional bandwidth while the configuration parameters are pushed from the Controllers to the remote Access Points. Additional bandwidth will also be required when configuration changes are applied to a site. However the additional bandwidth in both these cases is small and inconsequential.

When firmware image updates are applied to a remote site, the firmware is pushed to the elected RF Domain Manager at the sire which co-ordinates the firmware upgrades to Access Points at the site. An RF Domain Manager will upgrade other Access Point models first and will update its own Access Point type as well as itself last.

WING 5.X Protocols and Ports

The following table provides the Protocols and Ports supported by Independent Access Points. If firewalls are deployed between the remote Access Points and Wireless Controllers in the data center, UDP port 24576 must be permitted or adoption will fail. Additional protocols and ports may need to be permitted for AAA and Management depending on each specific deployment requirements:

Protocol	Port	Description
TCP	20-21	FTP File Transfers.
TCP	22	SSHv2 Device Management.
TCP	23	Telnet Device Management.
TCP	49	TACACS+ Authentication.
UDP	53	DNS Name Resolution.
UDP	69	TFTP File Transfers.
TCP	80	HTTP Device Management.
UDP	123	NTP Time Synchronization.
UDP	161	SNMP Device Management.
UDP	162	SNMP Traps.
TCP	389	LDAP / Active Directory Authentication.
TCP	443	HTTPS Device Management / Sensor -> ADSP Communications.
TCP	444	HTTPS Captive Portal Authentication.
TCP	880	HTTP Captive Portal Authentication.
UDP	1,812	RADIUS Authentication.
UDP	1,813	RADIUS Accounting.
TCP	8,443	Sensor -> Controller Communications (Advanced WIPS).
UDP	24,576	Access Point Adoption (Mandatory).