WiNG 5

Auto-Provisioning

Published: April 2017

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

www.extremenetworks.com

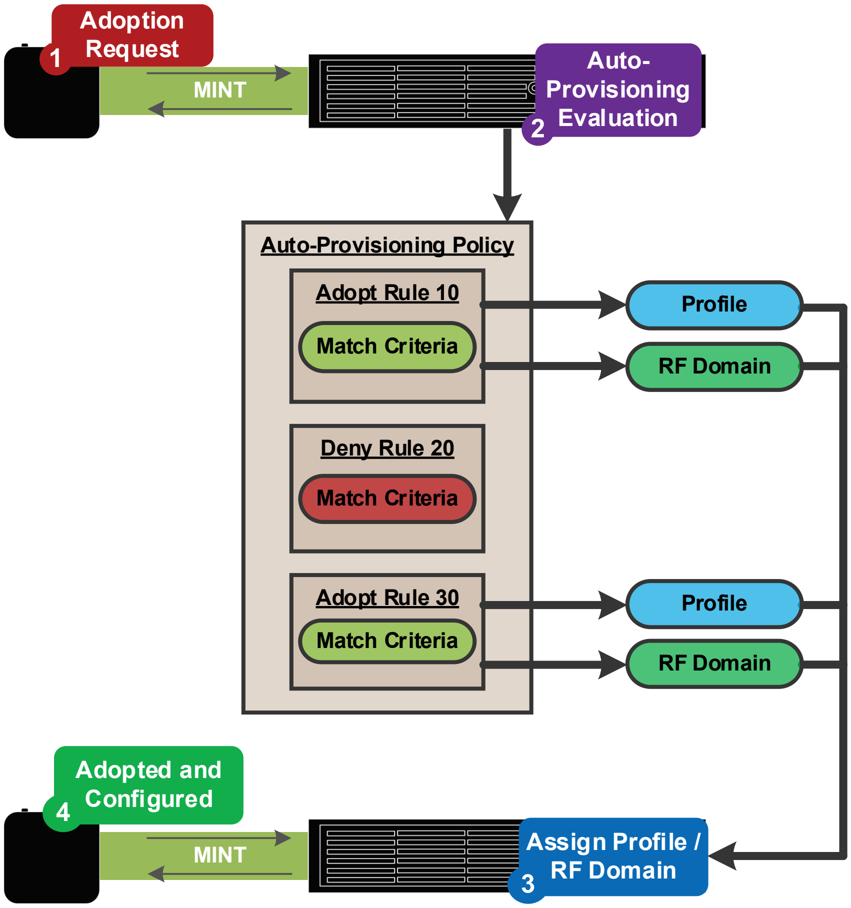
P/N XXXXX-XX

Contents

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's 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.

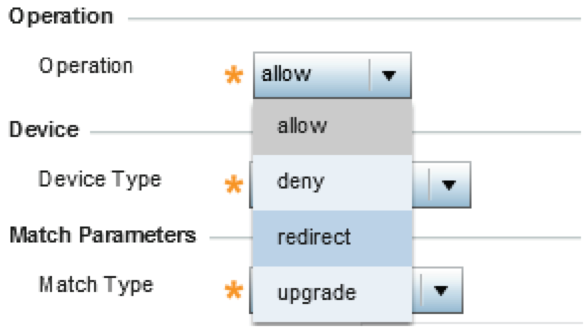
The number of allow rules you define in an Auto-Provisioning Policy will depend on the WiNG 5 device models you have deployed in the system, the match type you're using and the number of Profiles you have defined for each deployed model type.

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

Operation * allow

Device

Device Type *

Match Parameters

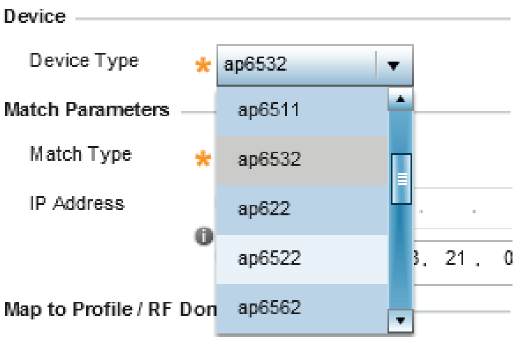
Match Type *

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

Device Type * ap6532

Match Parameters

Match Type *

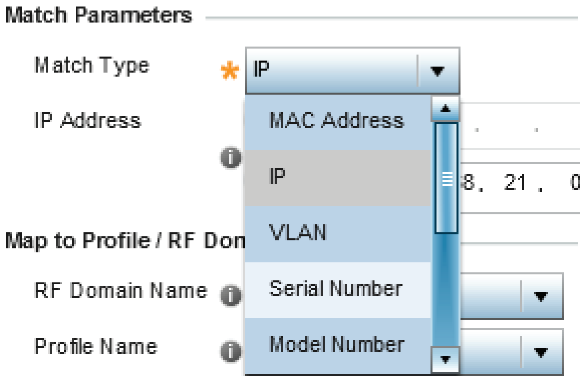
IP Address

Map to Profile / RF Don

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.

Standard Match Types

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	Match is made based on the adopting devices MAC address	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

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.

The table below provides a summary of the wildcard match types supported per Auto-Provisioning Policy rule in WiNG 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.motorolasolutions.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
	Characters 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
!
```