



You make **possible**



# Cisco DNA Center

The evolution from traditional management  
to Intent Based automation and assurance

Lila Rousseaux – CCIE #6899  
Technical Solutions Architect  
[@lila\\_rousseau](#)

BRKNMS-2031

**CISCO** *Live!*

Barcelona | January 27-31, 2020



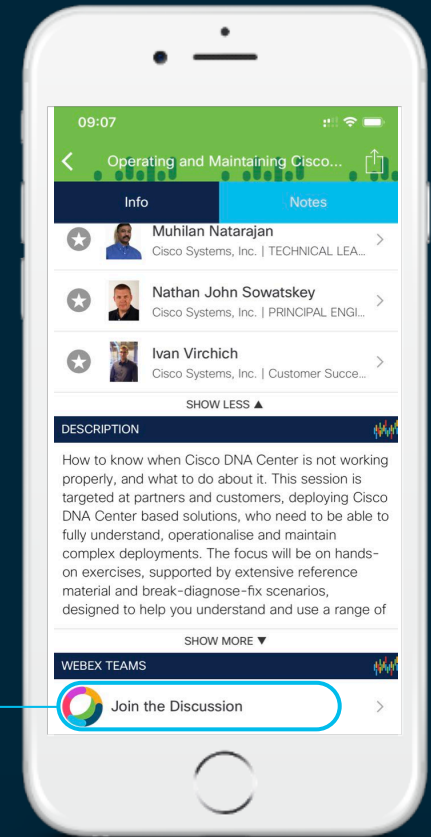
# Cisco Webex Teams

## Questions?

Use Cisco Webex Teams to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



# Agenda

- Why an Intent Based solution
- Traditional Management vs. Intent Based Networking
- What is Cisco DNA Center
- Cisco DNA Center **Automation**- Use Cases **Examples**
  - DAY0: Onboarding new devices using Zero Touch Deployment
  - DAY1: Configurations using Templates
  - DAYN: Security Advisories based on Machine Reasoning Engine
  - DAYN: Simplified Software Management based on Golden Images
  - DAYN: Defective Device Replacement - RMA
- Cisco DNA Center **Assurance**- Use Cases **Examples**
  - Network Health & Device 360
  - Client Health & Client 360
  - Application Health & Application 360
  - Proactive troubleshooting using Sensors
- What about Prime Infrastructure?
- Key Takeaways

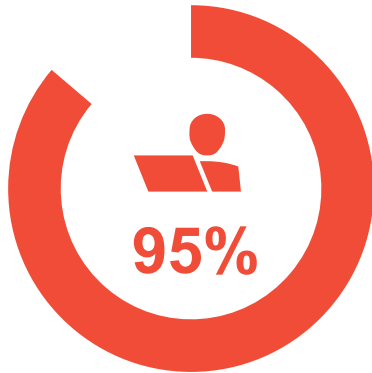


# Why an Intent Based Solution ?

# The Cost of Doing Business in the Digital World

**\$60B** Spent on Network Operations Labor and Tools

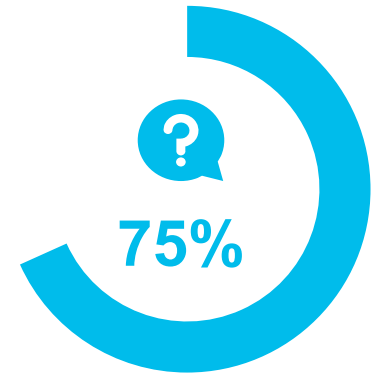
## Why are companies spending so much?



Network Changes Performed Manually



Policy Violations Due to Human Error



OpEx Spent on Network Changes & Troubleshooting

# Traditional Management vs. Intent Based Networking

# What do we mean by Intent Based Networking?

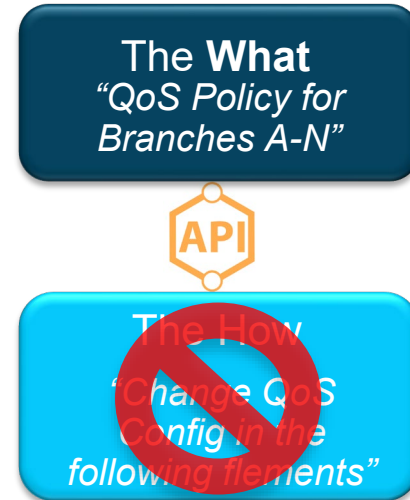
## Manual Policy Deployment

Admin  
Driven



## Intent Based Policy Deployment

Admin  
Driven



# Feature Configuration vs. Intent Based Networking

## FEATURE CONFIGURATION

The screenshot shows the Cisco Prime Infrastructure interface. The main window displays a table of network interfaces with columns for Location, Device Name, Device IP, and Interface Name. Row 11 is selected, corresponding to the modal window. The modal window, titled 'Enable QoS', has two tabs: 'Details' and 'CLI Preview'. Under 'Details', there are checkboxes for 'Enable QoS on Ingress' and 'Enable QoS on Egress', both of which are checked. Below these are classification and scheduling options. For 'Enable QoS on Ingress', the classification is 'Classify based on profile' with a dropdown menu set to 'test101'. For 'Enable QoS on Egress', the classification is 'Classify based on profile' with a dropdown menu set to 'test101'. The scheduling action is 'egress-8-c'. At the bottom of the modal, it states 'You are about to enable QoS on:' followed by 'Devices Total: 1' and 'Interfaces Total: 3'. There are 'Deploy' and 'Cancel' buttons at the bottom right of the modal.

	Location	Device Name	Device IP	Interface
1	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
2	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
3	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
4	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
5	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
6	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
7	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Loop
8	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Tunn
9	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Giga
10	...AMSTERDAM	AMS-ASR1K-INET	10.11.254.2	Tunn
11	...E-LAB/SJ-HQ	ASR1K-CORE1	10.0.2.2	Giga
12	...E-LAB/SJ-HQ	ASR1K-CORE1	10.0.2.2	Tunn

# Feature Configuration vs. Intent Based Networking

INTENT BASED NETWORKING

The screenshot displays the Cisco Intent-Based Networking configuration interface. The main view is for the 'Branch-Policy' application policy, which is configured for 'Wired' devices. The interface shows a list of application sets on the left, including 'Custom\_Video\_Set', 'Authentication-Services', 'Backup-And-Storage', 'Collaboration-Apps', 'Database-Apps', 'Desktop-Virtualization-Apps', and 'Email'. The main area shows the policy configuration for 'Branch-Policy' with a summary of device status: 3 Total devices, 0 Failed devices, 3 Successful devices, and 0 Aborted devices. Below the summary is a table of devices with columns for Device Name, Site, Status, Status Details, Device Type, Network Role, and Device IP Address.

Device Name	Site	Status	Status Details	Device Type	Network Role	Device IP Address
BR-SW1.cisco.com	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco Catalyst 9300 Switch	DISTRIBUTION	10.10.64.2
BR-R1.cisco.local	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco 2921 Integrated Services Router G2	BORDER ROUTER	10.2.252.2
BR-SW2.cisco.com	Global/USA/SJC/Branch	SUCCESS	N / A	Cisco Catalyst 9300 Switch	ACCESS	10.10.64.7

CISCO Live!

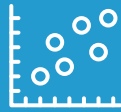
# What is Cisco DNA Center?

# Cisco DNA Center: Design, Policy, Provision, Assurance

## Intent Based Driven Management



**Logical workflow to design,  
provision, set policy**  
Respond to changes faster



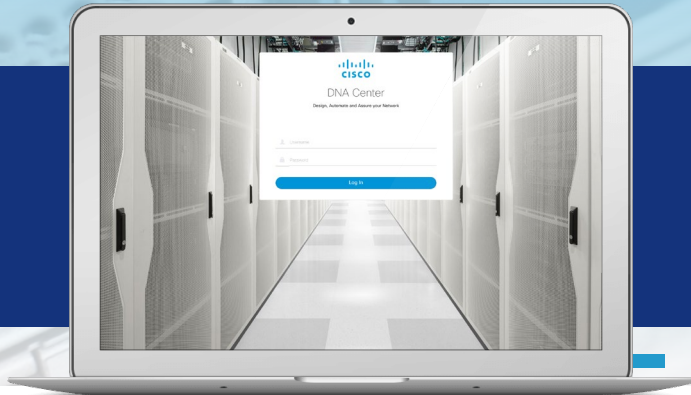
**Monitor end-to-end  
network performance**  
Predict and act on problems  
before they happen



**Pinpoint problems faster**  
Reduce downtime with an  
end-to-end view instead of  
hop by hop



**Manage hardware and  
software lifecycles**  
Keep up to date, meet  
compliance and plan for refresh



**Cisco DNA Center: Design,  
provision, automate policy and  
assure services from one place**



# Pillars of Cisco DNA Center

Covered in this session

## ASSURANCE

- Client Onboarding
- Sensors
- Troubleshooting
- Network Time Travel
- Path Trace
- WLC/AP360
- Application Experience

## AUTOMATION

- Day 0 Automation/PNP
- SWIM
- Wireless Automation
- Routing Automation
- Day 2 Automation
- Application Policy

## SD ACCESS

- SD-Access Overview
- Policy & Segmentation
- Automated Network Fabric
- Insights & Telemetry
- SD-Access Resources
- Tracking Tool

## PLATFORM

- Intent API
- ITSM Integration
- IPAM Integration
- Data & Reporting
- Events & Notifications
- Multi-Vendor SDK

# Pillars of Cisco DNA Center

Might come up in  
Q&A

## ASSURANCE

- Client Onboarding
- Sensors
- Troubleshooting
- Network Time Travel
- Path Trace
- WLC/AP360
- Application Experience

## AUTOMATION

- Day 0 Automation/PNP
- SWIM
- Wireless Automation
- Routing Automation
- Day 2 Automation
- Application Policy

## SD ACCESS

- SD-Access Overview
- Policy & Segmentation
- Automated Network Fabric
- Insights & Telemetry
- SD-Access Resources
- Tracking Tool

## PLATFORM

- Intent API
- ITSM Integration
- IPAM Integration
- Data & Reporting
- Events & Notifications
- Mult-Vendor SDK

# Cisco DNA Center Automation:

Using Cisco DNA  
Center for Base  
Network  
Automation

# DNA Center Automation - Journey Map

## Day 0

### Network On-boarding

- Greenfield switch on-boarding
- WiFi site planning & deployment
- AP Refresh



## Day 1

### Config & Operations

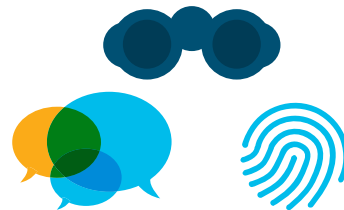
- Device Provisioning
- Wireless Rogue detection\*
- StackWise Virtual (SVL)\*



## Day 2

### Security & Optimization

- MRE based Security Advisory
- Netflow/ETA enablement w/ Stealthwatch



## Day N

### Patching and Maintenance

- Software upgrade using SWIM
- Application Policy
- Bonjour
- RMA



# Automation Use Cases covered in this session

- **Use Case #1-** New device onboarding
- **Use Case #2-** Configurations using Templates
- **Use Case #3-** Security Advisories based on Machine Reasoning Engine
- **Use Case #4-** Software and Image Management
- **Use Case #5-** Defective Device Replacement - RMA

Demo  
&  
Lecture



# Preparing Cisco DNA Center

Demo

# Preparing Cisco DNA Center



For your  
reference

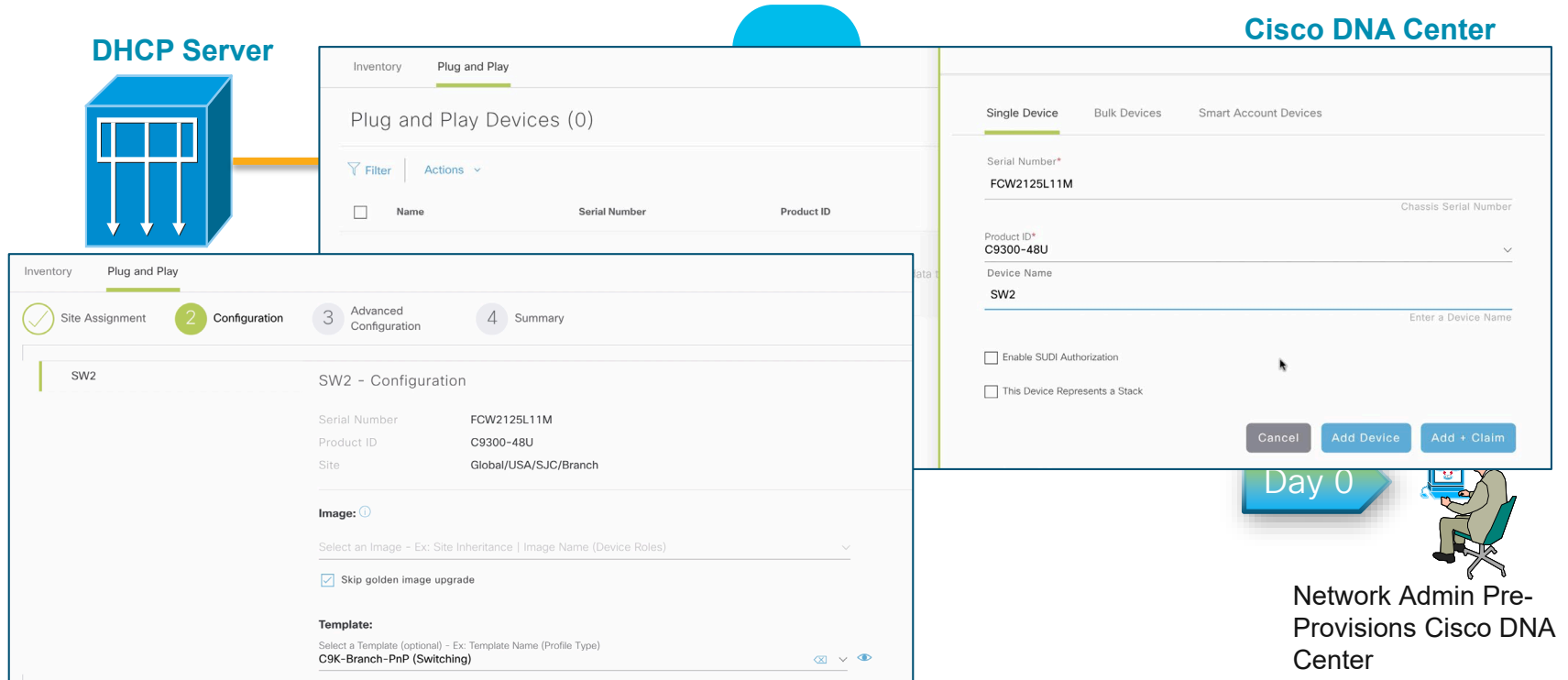
- Step 1 – Define your network hierarchy
- Step 2 – Define Network Settings and Device Credentials
- Step 3 – Discover existing network
- Step 4 – Check Inventory (Devices in Managed State)
- Step 5 – Assign Devices to Sites
- Step 6 (Optional) – Check Topology

# New device onboarding – Network Plug and Play



# Use Case Example

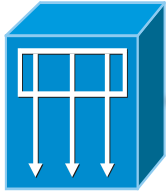
## Device Deployment in Campus



# Use Case Example

## Device Deployment in Campus

DHCP Server



```
<..snip..>  
CISCO_PNP.pnpserver  
"5A;B2;K4;I10.11.11.11;J80"  
<..snip..>
```

Day 1



Installer

cisco *Live!*

Remote Install

- Mount and devices
- Power-on

Status	Time	Details	Info
✓	01/04/2019 12:57:30 UTC	Device added to Site Global/USA/SJC/Branch	Info
✓	01/04/2019 12:57:29 UTC	Device added to Inventory	Info
✓	01/04/2019 12:57:29 UTC	Task: System Backup Config Task Completed	Info
✓	01/04/2019 12:57:28 UTC	Executing Task: System Backup Config Task	Info
✓	01/04/2019 12:57:23 UTC	Task: Site Config Task Completed	Info
✓	01/04/2019 12:57:03 UTC	Executing Task: Site Config Task	Info
✓	01/04/2019 12:56:58 UTC	Task: System Backup Config Task Completed	Info
✓	01/04/2019 12:56:57 UTC	Day 0 Config Generated	Info

Device validates server's location and establishes a communication with the server

(PnP Server)



IP Address  
**10.11.11.11**

Day 1



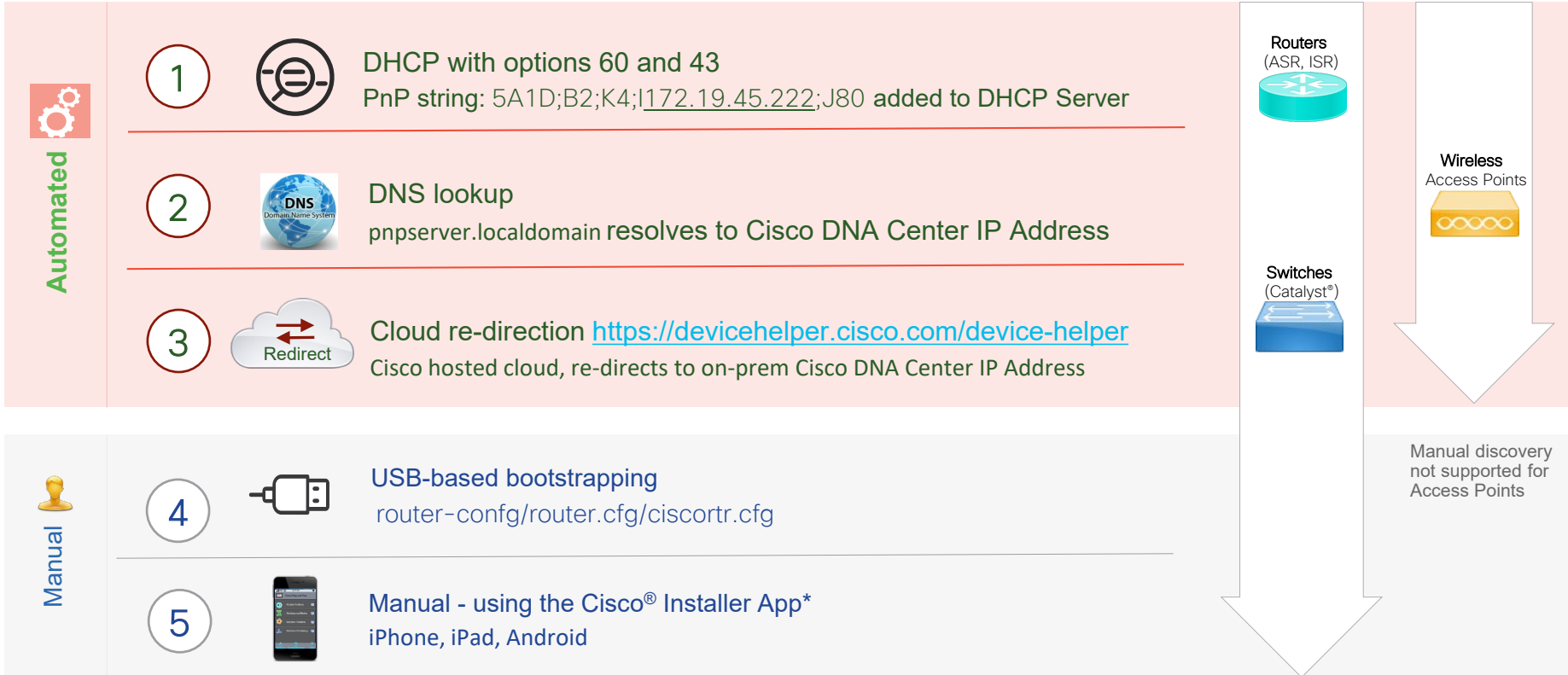
Network Admin remotely monitors status of install while in progress.



# New device onboarding – Network Plug and Play

## Demo

# PnP Server Discovery Options



\* Cisco DNA Center Support in Roadmap

# DHCP Server Configuration



For your  
reference

Microsoft DHCP server to configure  
using option 43.

The screenshot shows the Microsoft DHCP console with the following configuration details:

Option Name	Vendor	Value
003 Router	Standard	10.4.48.1
006 DNS Servers	Standard	10.4.48.10
015		

The 'Scope Options' dialog is open, showing the following configuration:

**Available Options**

Option	Description
<input checked="" type="checkbox"/> 043 Vendor Specific Info	Embedded
<input type="checkbox"/> 044 WINS/NBNS Servers	NBNS Addr
<input type="checkbox"/> 045 NetBIOS over TCP/IP NBDD	NetBIOS ov
<input type="checkbox"/> 046 WINS/NBT Node Type	0x1 = B-nod

**Data entry**

Data:	Binary:	ASCII:
0000	35 41 31 4E 3B 42 32 3B	5A1N;B2;
0008	4B 34 3B 49 31 30 2E 34	K4;I10.4
0010	2E 34 38 2E 32 33 32 3B	.48.232;
0018	4A 38 30	J80

Cisco device acting as a  
DHCP server:

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
5A1N;B2;K4;I10.4.48.232;J80
```

# DHCP Server Configuration

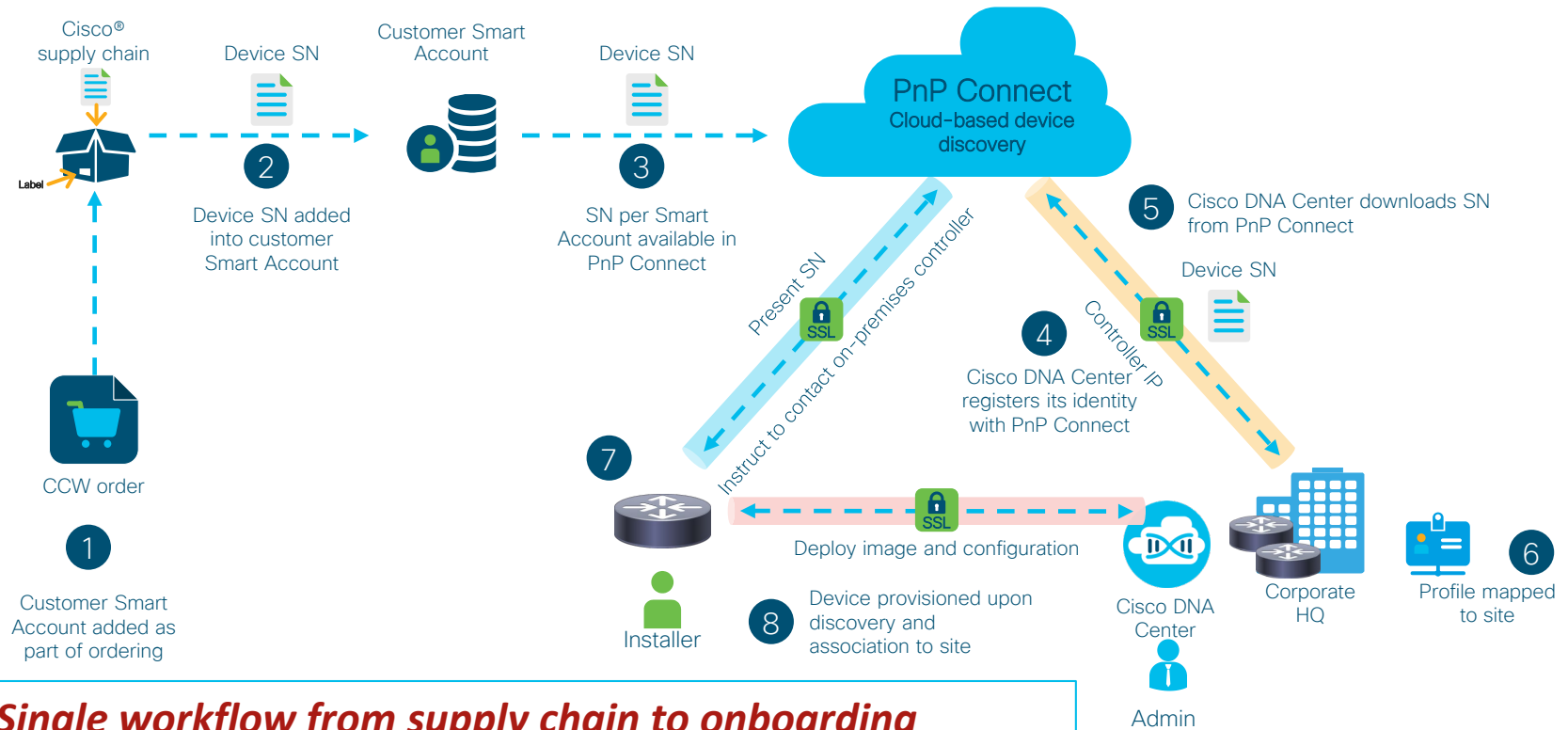


For your  
reference

## Sample Linux DHCP server configuration

```
# Sample /etc/dhcpd.conf
default-lease-time 600;
max-lease-time 7200;
option space CISCO_PNP;
option CISCO_PNP.pnpserver code 43 = string;
option subnet-mask 255.255.255.0;
option broadcast-address 10.30.30.255;
subnet 10.30.30.0 netmask 255.255.255.0 {
    range 10.30.30.1 10.30.30.255;
}
class "ciscopnp" {
    match if option vendor-class-identifier = "ciscopnp"
        option vendor-class-identifier "ciscopnp";
        vendor-option-space CISCO_PNP;
        option CISCO_PNP.pnpserver "5A;B2;K4;I172.19.210.215;J80";
}
```

# Day-0 deployment using PnP Connect



**Single workflow from supply chain to onboarding**

# Plug & Play Stack Support

Full Stack Support in  
“Unclaimed” and  
“Planned” workflow

Cisco DNA Center

DESIGN POLICY

Devices Fabric Services

Plug and Play Devices (9)

Filter Actions

#	Device Name	Serial Number	Product ID
1	TBRANCH-C9200L-2	JAE22501KT6	C9200L-24T-4G
2	TBRANCH-C9K-STACK	FOC2245Z0C2	C9300-24P
3	TBRANCH-C9200L-3	JAE22501JNX	C9200L-24T-4G
4	TRN6-C9200L-TBRANCH	JAE22501JXT	C9200L-24T-4G
5	ExtendedNode	FOC2004W14D	WS-C3560CX-12PD-S

Single Device Bulk Devices Smart Account Devices

Serial Number\*  
JAE22501KT6

Product ID\*  
C9200L-24T-4G

Device Name  
C9200L-TBRANCH-STACK

- Enable SUDI Authorization  
 This Device Represents a Stack



# Plug & Play Stack Support

Select an Image (optional) - Ex: Site Inheritance | Image Name (Device Roles)

cat9k\_iosxe.16.09.02.SPA.bin (access)

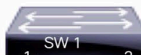
Skip golden image upgrade

### Template:

Select a Template (optional)

C9K-Branch-PnP (Switching)

### Stack Switch Wiring Scheme:



Top of Stack

Software Upgrade to whole stack

## Plug and Play Devices (1)

Filter Actions



Name

Serial Number

Product ID

Source

State

Site

Last Contact



BR-SW2



FOC2245Z0C2

C9300-24P

User

Provisioned

Global/Canada/Ontario/Toronto/TBRANCH

03/09/2019  
00:46:36 UTC

- Auto-Discover Stack Members
- Stack Icon

Last updated: 6:49 pm

Refresh

Add

Find

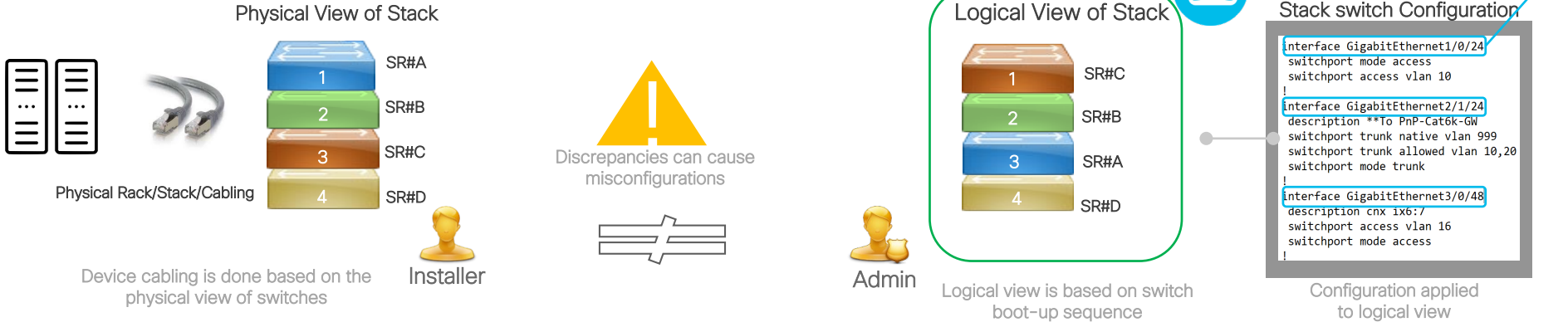
Show 25 entries

Showing 1 - 1 of 1

Previous 1 Next

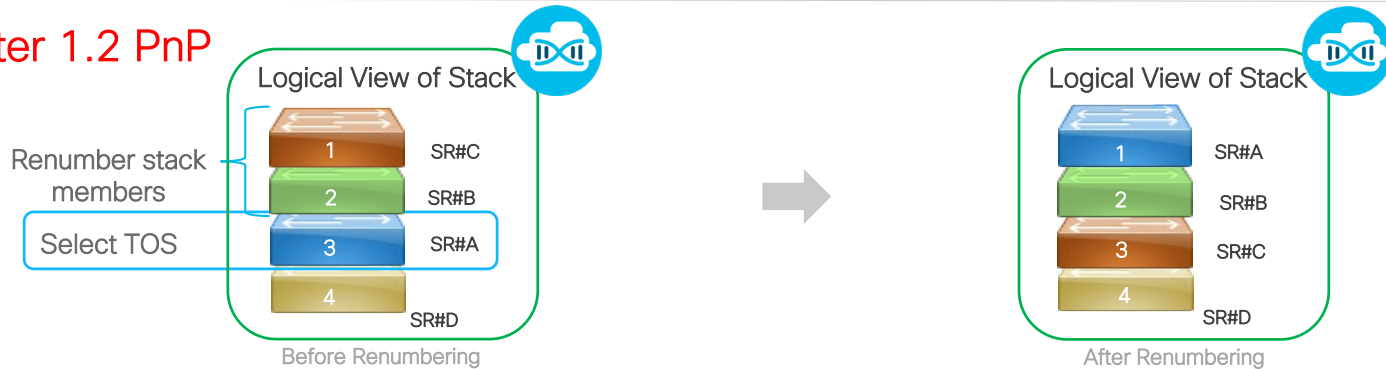
# Stack Switch Numbering Issue

Before



## Cisco DNA Center 1.2 PnP

Provides option to select Top of Stack(TOS) and renumber stack during provisioning



Deterministic stack order with renumbering

# Stack Switch Numbering Issue

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Devices ▾ Fabric Services

1 Site Assignment 2 Configuration 3 Advanced Configuration 4 Summary

To configure a device, click on the Device Name

Filter

#	Device Name	Serial Number	Product ID	Assigned Site
1	Switch	FOC2245Z0C2	C9300-24P	Global/Canada/Ontario

Configuration for device name: Switch

Ex: Site Inheritance | Image Name (Device Roles)

Template: Select a Template (optional)  
C9K-Branch-PnP-New (Switching) Preview

Ex: Template Name (Profile Type)

Supported Stack Switch Wiring Schemes:

1A 1B

Select a Cabling Scheme (required for Top of Stack renumbering)  
1B

Select a Top of Stack Serial Number (optional)  
FCW2152L07D

Select a License Level (optional)

Cancel Save

Enter the Top of Stack SN and Stack License level -> System Level Stack Renumbering

Stack Renumbering triggers an extra reload



# Day N Configuration with Templates

Demo

# How do Variables Work



For your reference

The screenshot illustrates the workflow in Cisco DNA Center. On the left, the 'Template Editor' shows a template named 'PORT\_SECURITY' with a variable `interface $` in a `#foreach` loop. A large blue arrow points from this variable to the right-hand screenshot. The right-hand screenshot shows the 'Provision Devices' step, where the variable is resolved to 'GigabitEthernet1/0/17' in the 'interface' field. The provisioning process is numbered 1 to 4: 1. Assign Site, 2. Configuration, 3. Advanced Configuration, 4. Summary.

**Template Editor**

PORT\_SECURITY × C9K-B

Actions ▾ | Edit ▾ | PORT DES

**Template**

```
1 #foreach ($interface in
2   interface $
3   descrip
4
5   #end
```

**Provision Devices**

DESIGN POLICY **PROVISION** ASSURANCE PLATFORM

Devices Fabric

Inventory Plug and Play

1 Assign Site 2 Configuration 3 **Advanced Configuration** 4 Summary

**Devices**

Select devices to fill out provisioning parameters

Find Show

EQ Device All ▾

PORT DESCRIPTION (1)

TBRANCH-C9K-STACK.cisco.com

**PORT DESCRIPTION**

interface \*

× GigabitEthernet1/0/17 × ▾

description \*

Pushed by DNAC Template

# Velocity Template Language



For your  
reference

## What is It?

Java-based template engine

Allows Cisco DNA-C to expose variables

Allows scripting logic to be included in a template

Greatly expands ability of templates to be used everywhere

## What features do I gain

Source-binding

Manipulation of variables

If-then branches

For-each loops

# Variables & Bind to Source



For your  
reference

Actions ▾ | Edit ▾ | PORT DESCRIPTION



## Template

```
1 #foreach ($interface in $interfaces)
2   interface $interface
3     description $description
4
5   #end|
```

# Variables & Bind to Source



For your reference

The screenshot displays a configuration tool interface for a "PORT DESCRIPTION" entity. It is divided into several sections:

- Template:** A code editor showing a `#foreach` loop for iterating over interfaces.
- Input Form:** A preview of the form with fields for "interface" and "description".
- Content:** A configuration panel for the "interface" field, where "Bind to Source" is checked, and the source is set to "Inventory" and the entity to "Interface". A list of attributes is shown, with "portName" selected.
- Definition of description:** A configuration panel for the "description" field, where "Bind to Source" is checked, and the source is set to "Inventory" and the entity to "Interface". The attribute "portName" is selected, and the display type is set to "Text Field".
- Field Properties:** A panel on the right showing "Field Name" as "interface" and "Required" as checked.

Blue boxes and arrows highlight the "Bind to Source" checkbox and the attribute selection process in the "Content" panels.



# Bind to Source

What information can I access?



### Inventory

Content

Bind to Source

Source \* Entity \*

Inventory Interface

Attribute description

- Interface
- AP Group
- Flex Group
- Wlan
- Policy Profile
- Flex Profile

### Common Settings

Content

Bind to Source

Source \* Entity \*

CommonSettings dhcp.server

Attribute

- dhcp.server
- syslog.server
- snmp.trap.receiver
- ntp.server
- timezone.site
- device.banner

### Network Profile

Content

Bind to Source

Source \* Entity \*

NetworkProfile SSID

Attribute

- SSID

# Flexible Deployment Options



For your  
reference

## Template

```
1 #foreach ($interface in $interfaces)
2   interface $interface
3     switchport port-security
4     switchport port-security maximum $max
5     switchport port-security
6     swi
7     swi
8     swi
9     swi
10 #end
```

## Key-Value Pairs

### Preview

Interface \*

Interface

Maximum Number of IP Addresses \*

1

Aging Time \*

1

Violation Mode \*

Protect

Protect

Restrict

Shutdown

mode

Default	Key	Value
---------	-----	-------

<input checked="" type="radio"/>	Protect	protect
----------------------------------	---------	---------

<input type="radio"/>	Restrict	restrict
-----------------------	----------	----------

<input type="radio"/>	Shutdown	shutdown
-----------------------	----------	----------

# Flexible Deployment Options



For your  
reference

## Template

```
1 #foreach ($interface in $interfaces)
2   interface $interface
3     switchport port-security
4     switchport port-security maximum $max
5     switchport port-security aging time $age
6     switchport port-security
7     switchport port-security
8     switchport
9     switchport
10 #end
```

## Min-Max Values

Maximum Number of IP Addresses \*

1

Aging Time \*

1

Violation Mode \*

Protect

Definition of age

Data Type Integer Display Type Text Field

Content

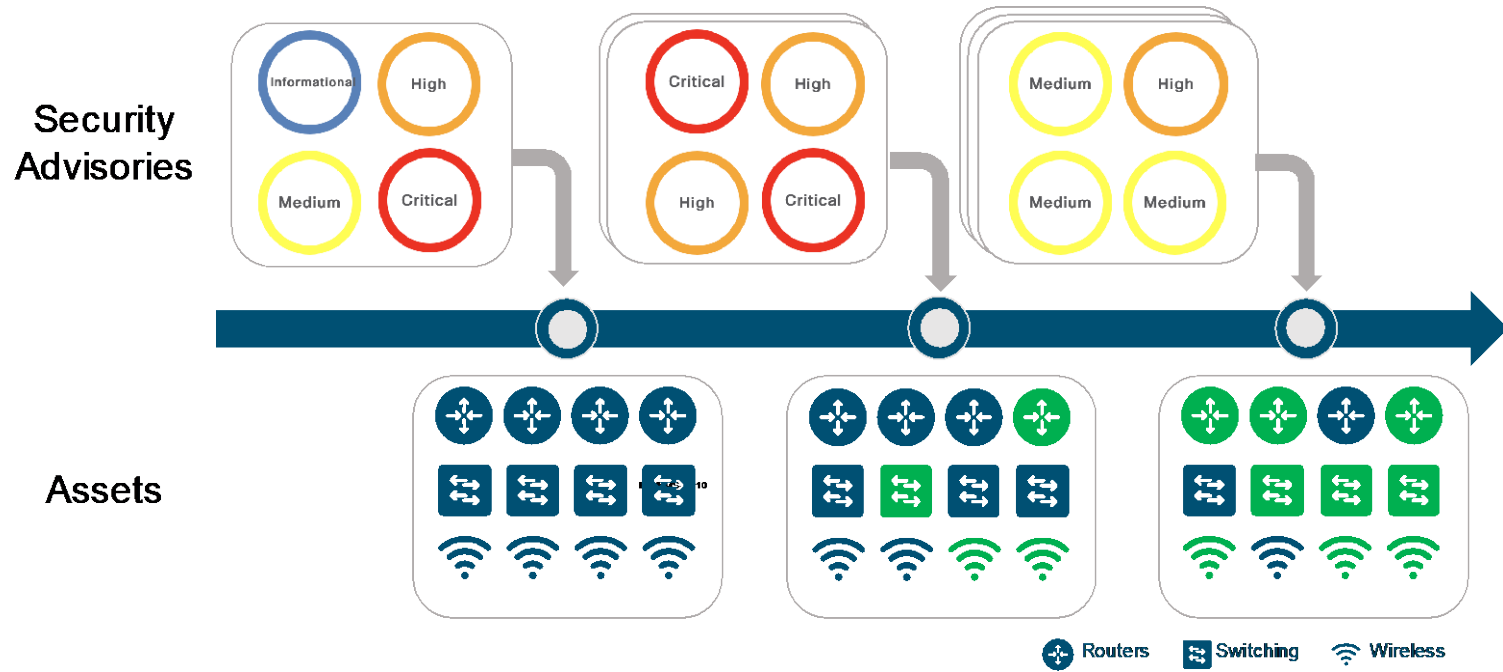
Bind to Source  Manual input

Range

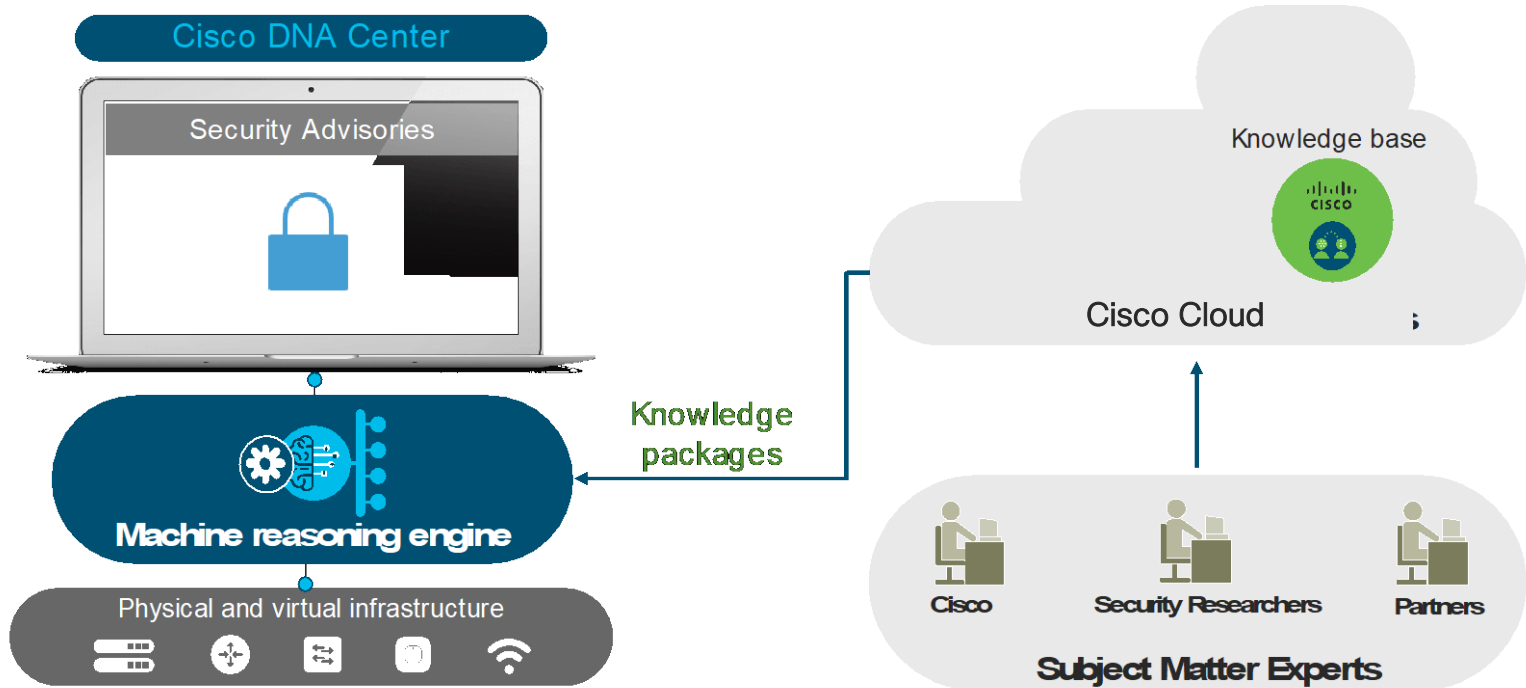
Min 1 Max 1440

# Security Advisories based on Machine Reasoning Engine

# Identifying and fixing vulnerabilities is challenging and ongoing



# Machine Reasoning Engine





# Security Advisories based on Machine Reasoning Engine

Demo

# Security Advisories



For your  
reference

Cisco DNA Center

Security Advisories



This page shows security advisories published by Cisco that may affect devices on your network based on the software image currently installed. At this time, further analysis of the configuration, platform details, or other criteria may be required to determine if a vulnerability is actually present.

**Note:** The information shown here is subject to the [Cisco Security Vulnerability Policy](#).

Security Advisories Focus: [Advisories](#) ▾

Advisories (60)

Filter

The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity.

Scan

Advisory ID	Advisory Title	CVSS Score ▾	Impact	CVE	Devices	Known Since (days)	Last Updated	
<a href="#">cisco-sa-20190828-iosxe-rest-auth-bypass</a>	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	10	● CRITICAL	CVE-2019-12643	18	56	08/28/2019	
<a href="#">cisco-sa-20180328-xesc</a>	Cisco IOS XE Software Static Credential Vulnerability	9.8	● CRITICAL	CVE-2018-0150	7	574	09/19/2018	
<a href="#">cisco-sa-20180606-aaa</a>	Cisco IOS XE Software Authentication, Authorization, and Accounting Login Authentication Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2018-0315	4	504	06/08/2018	
<a href="#">cisco-sa-20190327-xecmd</a>	Cisco IOS XE Software Command Injection Vulnerability	8.8	● HIGH	CVE-2019-1745	7	210	03/27/2019	
<a href="#">cisco-sa-20190327-iosxe-privesc</a>	Cisco IOS XE Software Privilege Escalation Vulnerability	8.8	● HIGH	CVE-2019-1754	4	210	03/27/2019	





# Security Advisories



Security Advisories Focus: **Devices** ▾

Last scanned: Oct 23, 2019 12:32 PM

**Scan**

Find Hierarchy

Devices (10)

Filter | Tag Device

- Global
  - Unassigned Devices (1)
- Canada
  - ALBERTA
  - British Columbia
  - Ontario
    - Toronto
      - TBRANCH
      - TRN6
  - Quebec

<input type="checkbox"/>	Device Name	IP Address	Device Type	Advisories ▾	Image Version	Site	Reachability	⋮
<input type="checkbox"/>	<a href="#">TRN6-TBRANCH-FUSION</a>	10.85.54.51	Routers	51	16.6.2	.../TBRANCH	Reachable	
<input type="checkbox"/>	<a href="#">TRN6-TBRANCH-C3650-S1.cisco.com</a>	10.85.54.53	Switches and Hubs	39	16.8.1a	.../TBRANCH	Reachable	
<input type="checkbox"/>	<a href="#">TRN6-TBRANCH-DIST.cisco.com</a>	10.85.54.17	Switches and Hubs	39	16.8.1a	.../TBRANCH	Reachable	
<input type="checkbox"/>	<a href="#">TBRANCH-C9200L-2.cisco.com</a>	10.85.54.24	Switches and Hubs	9	16.11.1	.../TBRANCH	Reachable	
<input type="checkbox"/>	<a href="#">TRN6-C9200L-TBRANCH.cisco.com</a>	10.85.54.23	Switches and Hubs	9	16.11.1	.../TBRANCH	Reachable	
<input type="checkbox"/>	<a href="#">TBRANCH-C9200L-3</a>	10.85.54.25	Switches and Hubs	9	16.11.1	.../TBRANCH	Reachable	



# Security Advisories



For your reference



This page shows security advisories published by Cisco that may require platform details, or other criteria may be required to determine

**Note:** The information shown here is subject to the [Cisco Security](#)

## Security Advisories Focus: [Devices](#)

Find Hierarchy

- Global
  - Unassigned Devices (1)
- Canada
  - ALBERTA
  - British Columbia
  - Ontario
    - Toronto
      - TBRANCH
      - TRN6
    - Quebec

Devices (10)

Filter | Tag Device

<input type="checkbox"/>	Device Name
<input type="checkbox"/>	TRN6-TBRANCH-
<input type="checkbox"/>	TRN6-TBRANCH-
<input type="checkbox"/>	TRN6-TBRANCH-
<input type="checkbox"/>	TBRANCH-C9200-
<input type="checkbox"/>	TRN6-C9200L-TB-
<input type="checkbox"/>	TBRANCH-C9200-

### TRN6-C9200L-TBRANCH.cisco.com (10.85.54.23)

Reachable Uptime: 4 days 13 hours 16 minutes

[Run Commands](#) | [View 360](#) | Last updated: 3:39 PM [Refresh](#)

Details **Advisories** Configuration Interfaces

Filter

Advisory ID	Advisory Title	CVSS Score	Impact	CVE	Known Since (days)	Last Updated	
<a href="#">cisco-sa-20190828-iosxe-rest-auth-bypass</a>	Cisco REST API Container for IOS XE Software Authentication Bypass Vulnerability	10	● CRITICAL	CVE-2019-12643	56	08/28/2019	
<a href="#">cisco-sa-20190925-webui-cmd-injection</a>	Cisco IOS XE Software Web UI Command Injection Vulnerabilities	7.6	● HIGH	CVE-2019-12650,CVE-2019-12651	28	09/30/2019	
<a href="#">cisco-sa-20170726-aniacp</a>	Cisco IOS and IOS XE Software Autonomic Control Plane Channel Information Disclosure Vulnerability	7.4	● HIGH	CVE-2017-6665	819	07/26/2017	
<a href="#">cisco-sa-20170726-anidos</a>	Cisco IOS and IOS XE Software Autonomic Networking Infrastructure Denial of Service	7.4	● HIGH	CVE-2017-6663	819	07/26/2017	

# Software and Image Management

# But wait! Doesn't PI have Image Management?

How to interpret  
the colors

Indicates ITSM Process Steps

Actions outside of NMS,  
mostly manual

Steps covered in NMS Tool

Steps covered in DNA-C

## General Steps to Update Software Image Update

Plan a  
Image  
Upgrade

Select  
Golden  
Image

Identify  
devices to  
upgrade

Create a  
Change  
Request

Approval  
of CR

Pre-Check  
validations

Distribute  
Image

Activate  
Image

Post  
Upgrade  
Validation

Close CR

## Traditional NMS Software Image Update

Plan a  
Image  
Upgrade

Select  
Golden  
Image

Identify  
devices to  
upgrade

Create a  
Change  
Request

Approval  
of CR

Pre-Check  
validations

Distribute  
Image

Activate  
Image

Post  
Upgrade  
Validation

Close CR

## Cisco DNA Center Software Image Update

Plan a  
Image  
Upgrade

Select  
Golden  
Image

Identify  
devices to  
upgrade

Create a  
Change  
Request

Approval  
of CR

Pre-Check  
validations

Distribute  
Image

Activate  
Image

Post  
Upgrade  
Validation

Close CR

# But wait! Doesn't PI have Image Management?

The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar shows the Cisco logo, the text "Prime Infrastructure", and a notification bell with "16" alerts. The breadcrumb path is "/ ... / Network Devices / Device Groups / All Devices / PAR-3850-1". Below this, there are tabs for "Device Details", "Configuration", "Applied/Scheduled Templates", "Configuration Archive", and "Image".

The main content area is titled "Images Applied" and contains a detailed view of an applied image:

- File Name:** cat3k\_caa-universalk9.SPA.03.06.01.E.152-2.E1.bin
- Image Name:** CAT3K\_CAA-UNIVERSALK9-M
- Image Family:** CAT3K\_CAA
- Image Version:** 03.06.01.E
- File Size:** 277.4 MB (290830104 bytes)
- Checksum:** 55938f1c79fa09b7619c566744f49dc3
- Minimum RAM (MB):** undefined
- IMAGE MINIMUMFLASH:** undefined

Below this, there is a section for "Recommended Images" with "Import" and "Distribute" buttons. A search filter "SYSTEM\_SW" is applied. A table lists recommended images:

Name	Features	Version	Size	In Repository
<input type="checkbox"/> cat3k_caa-universalk9.SPA.03.03.05.SE.150-1.EZ5(1).bin	IP[SLA] IPV6 S-IS FIREWALL PLUS QoS H...	03.03.05SE	245.7 MB (257651868 bytes)	Yes

# Selecting Golden Image

Network Hierarchy   Network Settings ▾   **Image Repository**   Network Profiles   Authentication Template

EQ Find Hierarchy

Update Devices | Show Tasks

Physical   Virtual

Filter | Refresh   Last updated: 2:27 PM

Family	Image Name	Using Image	Version	Golden Image	Device Role
> Cisco 4331 Integrated Servi...	isr4300-universalk9.16.06...	1	16.6.4 Add On (1)	★	
> Cisco Catalyst 9200L Switch...	cat9k_lite_iosxe.16.12.01.... ✔ Verified	0	16.12.1 (Latest) Add On (N/A)	★	ALL ★
> Cisco 4321 Integrated Servi...	isr4300-universalk9.16.06...	1	16.6.2 Add On (1)	★	
> Cisco Catalyst 3650 Switch ...	cat3k_caa-universalk9.16.... ✔ Verified	0	16.6.3 Add On (N/A)	☆	DISTRIBUTION ★

# Identify Devices to Upgrade

The screenshot displays the Cisco DNA Center interface for identifying devices to upgrade. The main view shows a list of 10 devices under the 'Global' location, filtered by 'Software Images'. A red box highlights the 'Software Image' column, which includes the image name and a 'Needs Update' status. The table below summarizes the data shown in the interface.

Device Name	IP Address	Device Family	Site	Reachability	Software Image	Image Version
TBRANCH-C9200L-2	10.85.54.24	Switches and Hubs	.../Toronto/TBRANCH	Reachable	cat9k_lite_iosxe.16.12.0... Needs Update	16.12.1
TBRANCH-C9200L-3	10.85.54.25	Switches and Hubs	.../Toronto/TBRANCH	Reachable	cat9k_lite_iosxe.16.12.0... Needs Update	16.12.1
TRN6-SDA-CAMPUS-B1.cirrus.cloud	10.85.62.102	Switches and Hubs	.../TRN6/TRN6-28-SELab	Reachable	cat9k_iosxe.16.09.02s.S... Needs Update	16.9.2s
TRN6-SDA-CAMPUS-B2.cirrus.cloud	10.85.62.103	Switches and Hubs	.../TRN6/TRN6-28-SELab	Reachable	cat9k_iosxe.16.09.02s.S... Needs Update	16.9.2s
TRN6-SDA-CAMPUS-E1.cirrus.cloud FabricEdge	10.85.62.106	Switches and Hubs	.../TRN6/TRN6-28-SELab	Reachable	cat9k_iosxe.16.09.02s.S... Needs Update	16.9.2s
TRN6-SDA-CAMPUS-E2.cirrus.cloud FabricEdge	10.85.62.107	Switches and Hubs	.../TRN6/TRN6-28-SELab	Reachable	cat9k_iosxe.16.09.02s.S... Needs Update	16.9.2s

# Image Update Readiness Checks

## Image Update Readiness Check ✕

Running Image : cat9k\_lite\_iosxe.16.12.01.SPA.bin  
 Golden Image : cat9k\_lite\_iosxe.16.11.01.SPA.bin  
 Reboot Required **Yes**

[Export](#) [Recheck](#)

Check Type	Description	Status <span style="font-size: 0.8em;">!</span>	Last Checked
Startup config check	Startup configuration exist for this device	✔	Tue Nov 26 2019 05:54:30
Config register check	Config-register verified successfully	✔	Tue Nov 26 2019 05:54:30
Flash check	Image Size is larger than free space Expected : 730 MB Available Free space is: 491 MB [Install mode needs free space to 2.2 times of Image size] Actual : flash: 491 MB Action :Please Clean the Flash location And then Resync the device. However flow can proceed, auto flash clean up will be attempted for this device.	⚠	Tue Nov 26 2019 05:54:30
File Transfer Check	HTTPS/SCP is reachable :10.85.52.203	✔	Tue Nov 26 2019 05:54:30
Service Entitlement Check	Unable to validate license for Device. Not enough information to validate. Action :Ensure CCO is reachable and inventory updated with license	⚠	Tue Nov 26 2019 05:54:28

a > Ontario > Toronto > TBRANCH Take a Tour ☰

Last updated: 10:56 AM 🔄

All Reachable Unreachable

Reachability	Software Image	Image Version	Update Status
Reachable	N/A	8.8.111.0	NA
Reachable	N/A	8.8.111.0	NA
Reachable	cat9k_iosxe.16.12.02.SPA	16.12.02	Activation Success
Reachable	cat9k_lite_iosxe.16.12.0... <span style="font-size: 0.8em;">Needs Update</span>	16.12.1	Distribution Pending
Reachable	cat9k_lite_iosxe.16.12.0... <span style="font-size: 0.8em;">Needs Update</span>	16.12.1	Distribution Pending
Reachable	cat9k_lite_iosxe.16.12.0... <span style="font-size: 0.8em;">Needs Update</span>	16.12.1	Distribution Pending
Reachable	Cisco Controller <span style="font-size: 0.8em;">Needs Update</span>	8.8.111.0	Distribution Failure



# Out of box Pre-Checks and Post-Checks

The screenshot displays the Cisco Prime Network Manager interface. On the left, the 'Devices' section shows a hierarchy of devices, including 'TBRANCH' and 'TRN6'. The main panel shows a list of 10 devices under the 'Inventory' focus, with columns for 'Device Name' and 'IP Address'. The 'Recent Tasks (Last 50)' panel on the right shows a task titled 'Image Upgrade for 10.85.54.54' which is 'Successful'. The task details include 'Distribute Operation' and 'Activate Operation'. A red box highlights the 'Show Scripts' section of the 'Activate Operation', which lists various pre-checks and post-checks.

Device Name	IP Address
TBranch_NonFabric_AP1	10.85.54.30
TBranch_NonFabric_AP2	10.85.54.26
TBRANCH-C9K-STACK	10.85.54.54
TBRANCH-C9200-1.cisco.com	10.85.54.23
TBRANCH-C9200L-2.cisco.com	10.85.54.24
TBRANCH-C9200L-3.cisco.com	10.85.54.25

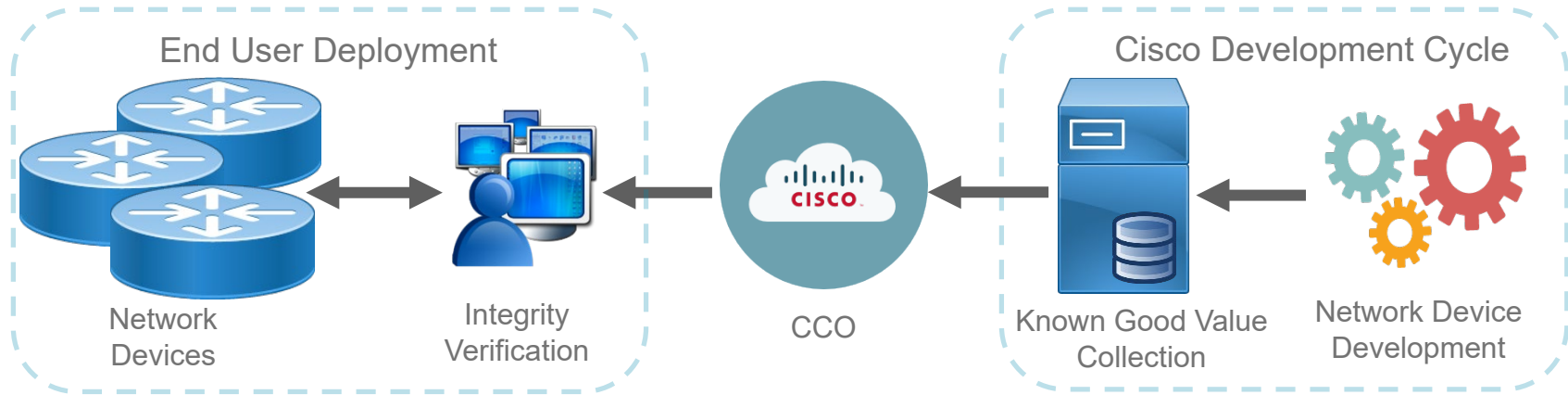
**Recent Tasks (Last 50)** Refresh Last updated: 10:54 AM

**Image Upgrade for 10.85.54.54**  
cat9k\_iosxe.16.12.02.SPA.bin  
Duration : 0h: 24m: 15s Start Time : Nov 25 2019 15:21:58 Successful

- Distribute Operation** Duration : 0h: 8m: 9s [Show Scripts](#)  
Distribution of image: cat9k\_iosxe.16.12.02.SPA.bin on device: 10.85.54.54 with protocol: SCP completed successfully
- Activate Operation** Duration : 0h: 16m: 6s [Hide Scripts](#)  
Activation of image: cat9k\_iosxe.16.12.02.SPA.bin on device: 10.85.54.54 completed successfully.

Show Scripts	Type	Details
Spanning Tree Summary Check	Pre Check	<a href="#">View</a>
Running Config Check	Pre Check	<a href="#">View</a>
CDP neighbors Check	Pre Check	<a href="#">View</a>
Interface Check	Pre Check	<a href="#">View</a>
Config register check	Pre Check	<a href="#">View</a>
Startup config check	Pre Check	<a href="#">View</a>
Spanning Tree Summary Check	Post Check	<a href="#">View</a>
Running Config Check	Post Check	<a href="#">View</a>
CDP neighbors Check	Post Check	<a href="#">View</a>
Interface Check	Post Check	<a href="#">View</a>
Startup config check	Post Check	<a href="#">View</a>


















# Software Upgrade – Integrity Verification



**Software** Is the software used by the device authentic? Includes checks of the software files (Known Good Value) and in-memory (Imprint Value) contents. Also includes shell access attempts (Event Occurrence)

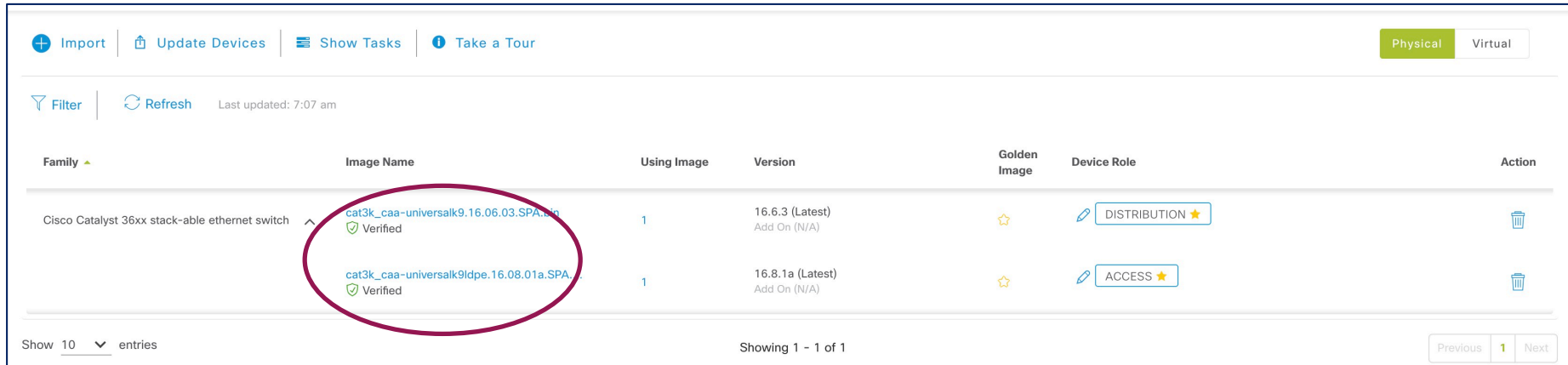
# Software Upgrade – Integrity Verification

- To provide a level of security integrity devices must run authentic and valid software
- Cisco DNA Center Integrity Verification uses a system to compare collected image integrity data to Known Good Values (KGV) for Cisco software.
- The MD5 or SHA values of the images are validated against KGV's.

Family 	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco Catalyst 36xx stack-able ethernet switch	<a href="#">cat3k_caa-universalk9.16.06.03.SPA.bin</a>  Unable to verify	2	16.6.3 (Latest) Add On (N/A)		+ DISTRIBUTION 	
	<a href="#">cat3k_caa-universalk9ldpe.16.03.06.SPA.bin</a>	0	Denali-16.3.6 (Suggested, Latest) Add On (N/A)		+	
	<a href="#">cat3k_caa-universalk9ldpe.SPA.03.06.08.E.152-2...</a>	0	3.6.8E (Suggested, Latest) Add On (N/A)		+	
	<a href="#">cat3k_caa-universalk9.SPA.03.06.08.E.152-2.E8....</a>	0	3.6.8E (Suggested, Latest) Add On (N/A)		+	
	<a href="#">cat3k_caa-universalk9.16.03.06.SPA.bin</a>	0	Denali-16.3.6 (Suggested, Latest) Add On (N/A)		+	
	<a href="#">cat3k_caa-universalk9.16.08.01a.SPA.bin</a>  Unable to verify	0	16.8.1a (Latest) Add On (N/A)		+ Importing 	

# Software Upgrade – Integrity Verification

- To provide a level of security integrity devices must run authentic and valid software
- Cisco DNA Center Integrity Verification uses a system to compare collected image integrity data to Known Good Values (KGV) for Cisco software.
- The MD5 or SHA values of the images are validated against KGV's.



The screenshot displays the Cisco DNA Center software management interface. At the top, there are navigation links: Import, Update Devices, Show Tasks, and Take a Tour. On the right, there are tabs for Physical and Virtual. Below the navigation, there are Filter and Refresh buttons, and a timestamp indicating the last update at 7:07 am. The main content is a table with the following columns: Family, Image Name, Using Image, Version, Golden Image, Device Role, and Action. The table contains two entries for Cisco Catalyst 36xx stack-able ethernet switch. The first entry is for version 16.6.3 (Latest) with a 'DISTRIBUTION' role. The second entry is for version 16.8.1a (Latest) with an 'ACCESS' role. Both entries have a 'Verified' status, which is highlighted by a red circle. The bottom of the interface shows 'Showing 1 - 1 of 1' and navigation buttons for Previous, 1, and Next.

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco Catalyst 36xx stack-able ethernet switch	cat3k_caa-universalk9.16.06.03.SPA... Verified	1	16.6.3 (Latest) Add On (N/A)	☆	DISTRIBUTION ☆	🗑️
	cat3k_caa-universalk9ldpe.16.08.01a.SPA... Verified	1	16.8.1a (Latest) Add On (N/A)	☆	ACCESS ☆	🗑️



# Software and Image Management

Demo

# What you need to know ...

- Both BUNDLE mode and INSTALL mode are supported
- We don't support BUNDLE/INSTALL mode conversion
- INSTALL mode doesn't allow to import image directly from the device
- To upgrade image during PnP the device has to be in INSTALL mode

The screenshot displays the software image management interface for a Cisco Catalyst 9300 Switch. The interface shows a list of software images with their respective modes. A blue dashed line connects the 'cat9k\_iosxe.16.06.03.SPA...' image to the 'Bundle Mode' callout, and another blue dashed line connects the 'cat9k\_iosxe.16.06.04a.SP...' image to the 'Install Mode' callout.

Image Name	Count	Version	Mode	Actions
cat9k_iosxe.16.06.03.SPA... Verified	1	16.6.3 Add On (0)	DISTRIBUTION ★	✖
cat9k_iosxe.16.08.01a.SP... Verified	0	16.8.1a Add On (0)	ACCESS ★	✖
cat9k_iosxe.16.06.02.SPA... Verified	0	16.6.2 Add On (0)	✪	✏ ✖
cat9k_iosxe.16.06.05.SPA... Verified	0	Everest-16.6.5 (Latest) Add On (0)	✪	✏ ✖
cat9k_iosxeldpe.16.09.02.... Verified	0	Fuji-16.9.2 (Latest) Add On (0)	✪	✏ ✖
cat9k_iosxe.16.06.04a.SP... Verified	0	16.6.4a (Latest) Add On (0)	✪	✏ ✖
cat9k_iosxe.16.06.01.SPA... Verified	0	16.6.1 Add On (0)	✪	✏ ✖
Install Mode (16.8.1a)	1	16.8.1a Add On (0)	✖ ✖	✏ ✖

# N+1 rolling AP upgrades

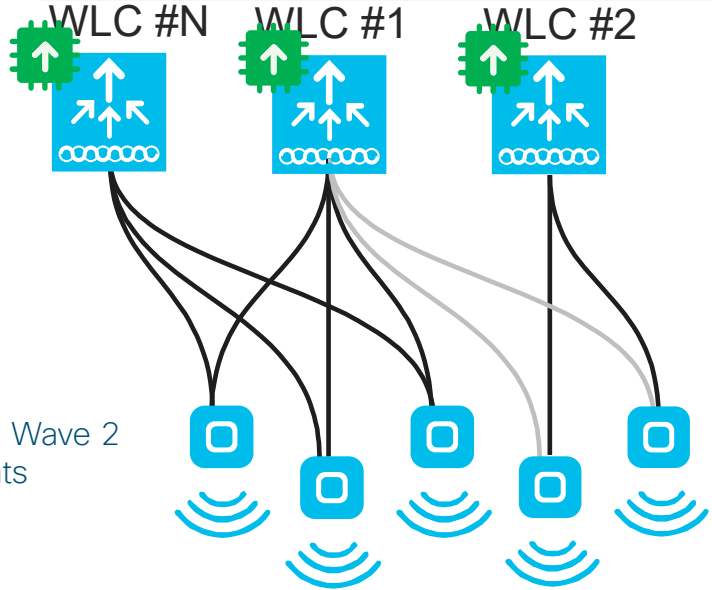
## Zero client downtime during image upgrades



Unified management with Cisco DNA Center



N+1 Cisco® Catalyst® 9800 Series Wireless Controllers

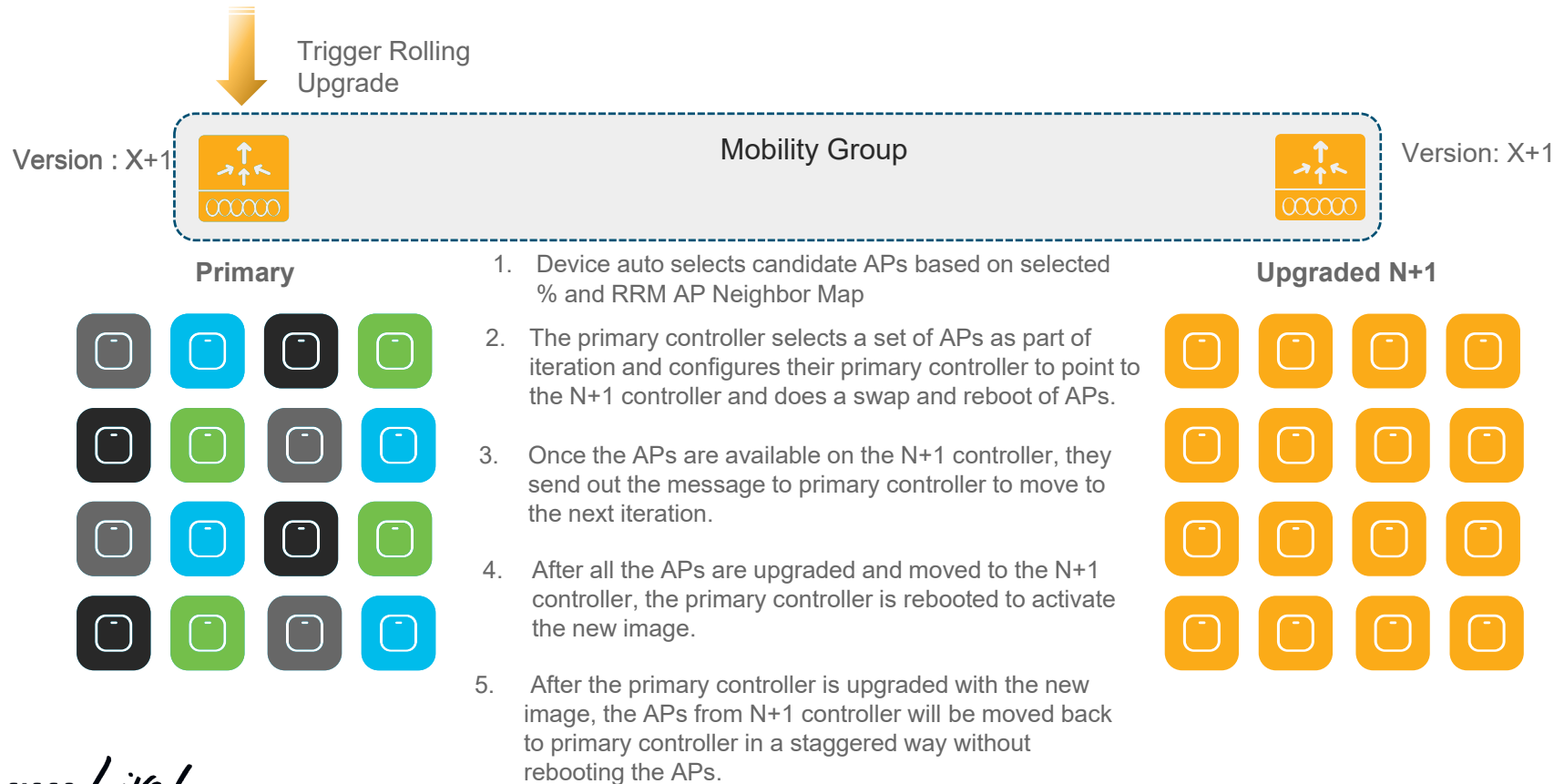


Wave 1 and Wave 2 access points

### Key highlights

- ✓ Automated group creation with Radio Resource Management for N+1 rolling AP upgrades
- ✓ No more manual intervention to create groups in Cisco Prime® Infrastructure
- ✓ Manage all your software updates and upgrades through Cisco DNA Center

# N+1 Rolling AP Upgrade - Process





# N+1 Rolling AP Upgrade

## What you need to know ...



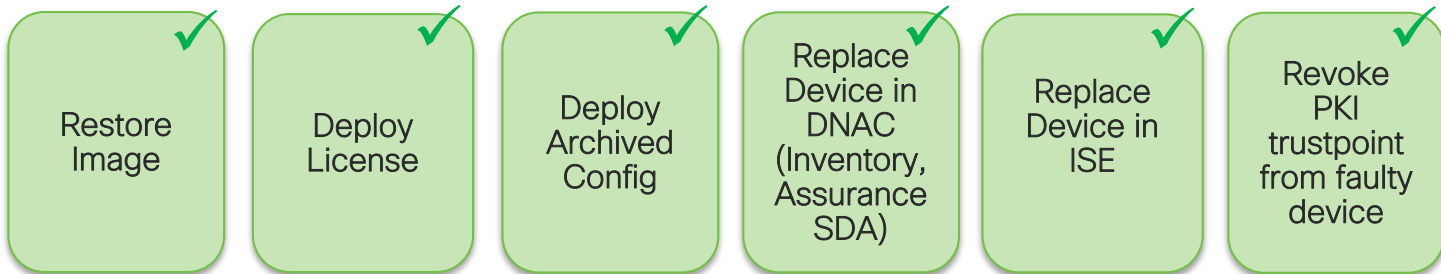
For your  
reference

- An N+1 HA controller is required to perform the Rolling AP upgrade
- The N+1 controller is already running the Golden image
- N+1 controller should be running the same configuration as the Primary WLC (WLANs and policies)
- The N+1 controller is reachable and in Managed state in Cisco DNA Center.
- **Mobility Tunnel Up between Primary & N+1:** The Primary WLC and N+1 WLC should be part of same Mobility Group and the Mobility Tunnel should be UP between the two before initiating the Rolling AP upgrade process.
- The AP upgrade information between the Primary and N+1 controllers are exchanged through the **mobility tunnel**.

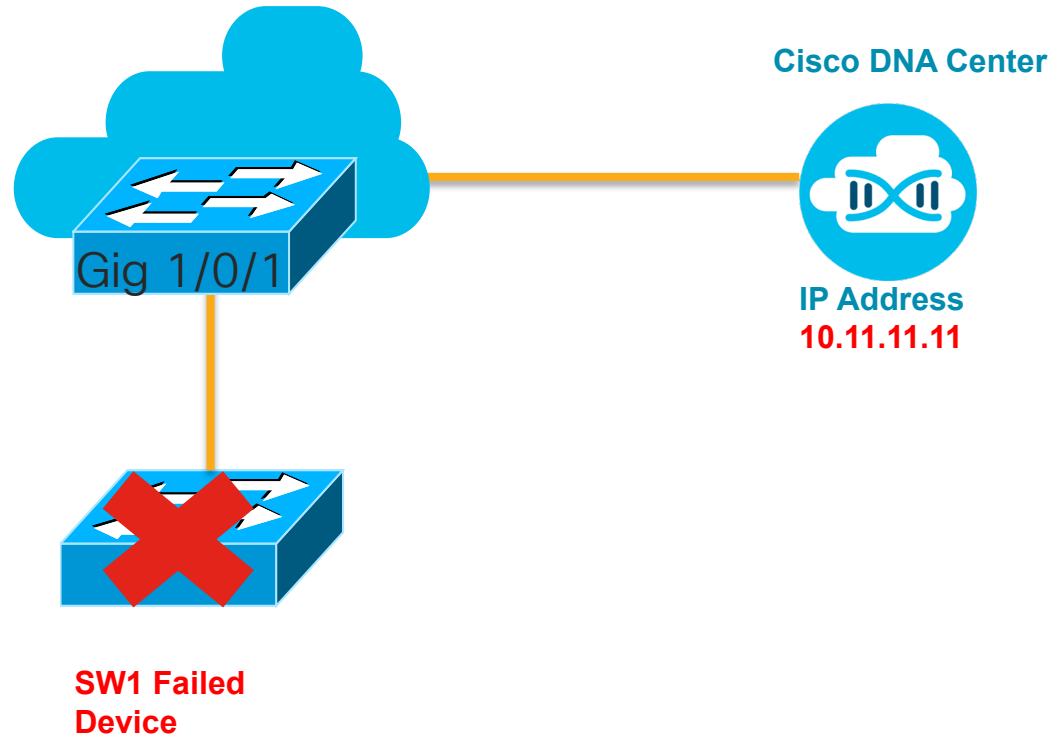
# Defective Device Replacement - RMA

# Why Defective device replacement (RMA) in Cisco DNA Center?

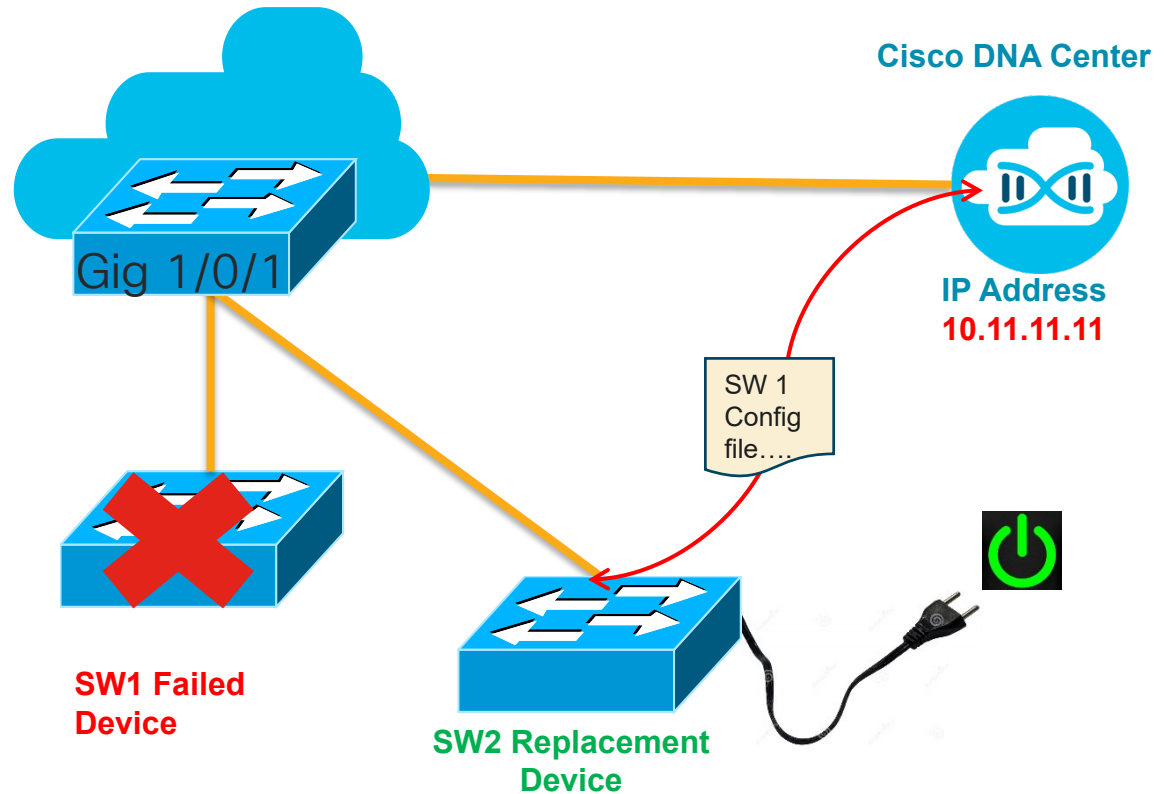
- RMA is a critical part of device lifecycle management.
- Existing RMA procedure is manual and time consuming.
- RMA in Cisco DNA Center provides users the ease of automation to recover failed device quickly, thus improving productivity and reducing Opex.



# Return Material Authorization (RMA) workflow



# Return Material Authorization (RMA) workflow



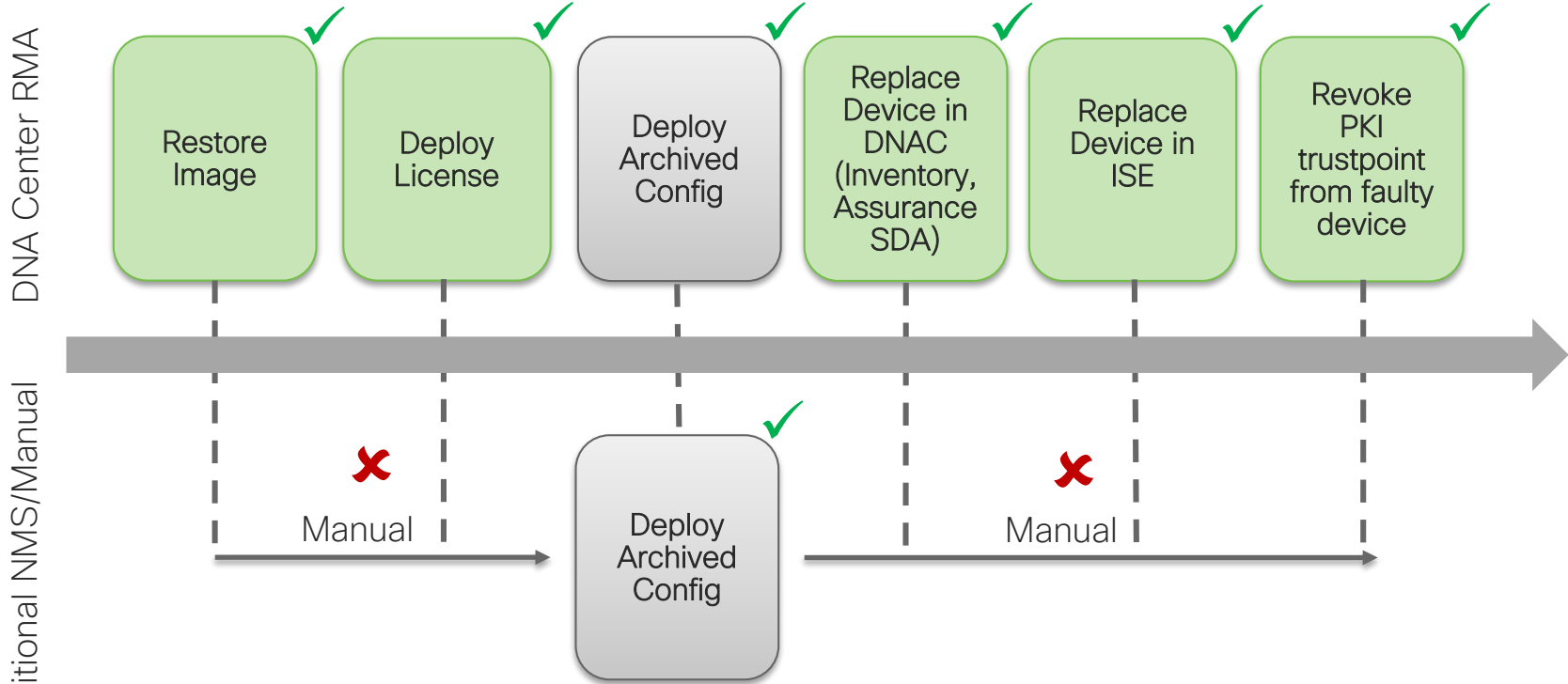
Replacement switch is racked and all the connections are moved from the RMA device to the replacement switch



Installer

cisco *Live!*

# Benefits of DNA Center RMA Workflow





# Defective Device Replacement – RMA

Demo

# Cisco DNA Center 1.3.1: RMA

## What you need to know ...



For your  
reference

- Only like-to-like replacement is supported.
- Supports both fabric (SDA) and no-fabric devices. SDA supports One-Touch RMA only
- RMA Methods:
  - **Zero-Touch RMA** - Replacement device is connected to Cisco DNA Center via PnP. No manual configuration on device required. Not yet supported for devices in fabric (SDA).
  - **One-Touch RMA** - Replacement device is manually configured via console with basic IP and mgmt. credentials first so it can be discovered by Cisco DNA Center
- Supported platforms: Routers and Switches.
- It is two-reboot process if image upgrade is required, 1st reboot for image upgrade and 2nd reboot for configuration, licensing and etc.
- Configuration:
  - The running config is archived only at initial discovery of device and at 23:00 daily.
  - vlan.dat on switch is archived same way as the running config.



# Checklist before proceeding with RMA in production



For your  
reference

- Cisco DNA Center release is 1.3.1 is or above.
- Faulty switch that needs to be replaced must be in UNREACHABLE state.
- The replacement switch has the same exact SKU as the RMA device (faulty)
- Replacement switch is racked and all the connections are moved from the RMA device to the replacement switch
- Replacement switch is powered up
- Replacement switch onboarded using PnP and is available as an unclaimed device in the PnP inventory.
- For devices with legacy licensing, the license on the replacement device should match the license on the faulty device to be replaced.
- Replacement switch boot mode is INSTALL mode (as opposed to BUNDLE mode)

# Cisco DNA Center Assurance:

Gaining Deep Insights  
with Cisco DNA Center  
Assurance and Analytics

# Cisco DNA Center Assurance

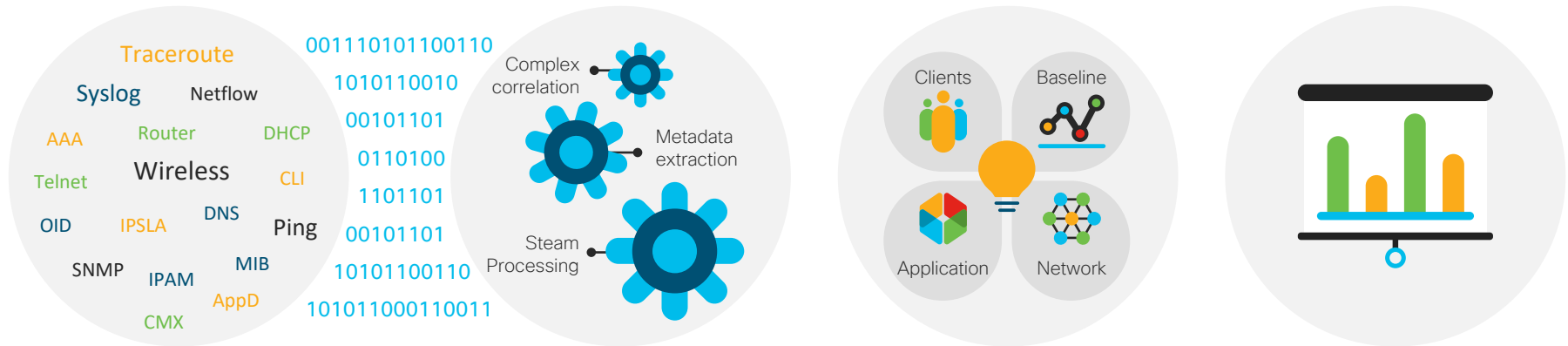
From Network Data to Business Insights

Network Telemetry  
Contextual Data

Complex Event  
Processing

Correlated Insights

Guided  
Remediation



Everything as a Sensor

170+ Actionable Insights

Client | Applications | Wireless | Switching | Routing

# Assurance Use Cases covered in this session

- **Use Case #1-** Overall Health Dashboard
- **Use Case #2-** Network Health & Device 360
- **Use Case #3-** Client Health & Client 360
- **Use Case #4-** Application Health & Application 360
- **Use Case #5-** Sensors



Demo



# Assurance & Analytics

## Demo

cisco *Live!*

# What about Prime Infrastructure?

# Deployment with Prime and Cisco DNA Center

## DNA Center Managed Network

- DNA Center is used for Day 0 and Day 2.
- One time migration from Prime to DNA Center

## Prime and DNA Center Managed Network

- Run DNA-C and Prime together in the network
- DNA Center is used for Automation or Assurance or both for parts of the network

There is only one system that will make changes to the network

# Migration Scenarios

- Full Migration from Prime to DNAC
- Prime and DNAC Co-existence

1 DNAC on Assurance Mode

PI = R/W, DNAC = RO

2 DNAC on Automation + Assurance Mode

PI = RO, DNAC = R/W

3 DNAC on Automation Mode

PI = RO, DNAC = R/W

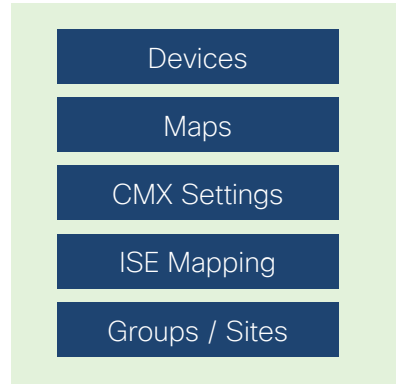
There is only one system that will make changes to the network



# Assurance in Cisco DNA Center and Config in Prime

1

## Prime

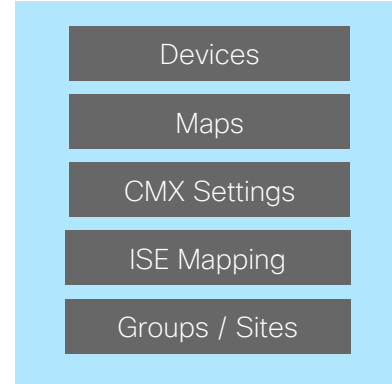


Select WLC  
- Migrate to  
DNAC



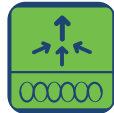
Identify the  
Sites  
Managed  
by WLC

## DNA Center



## WLC is RO in DNAC

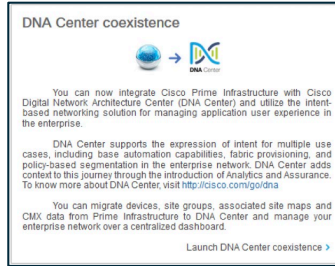
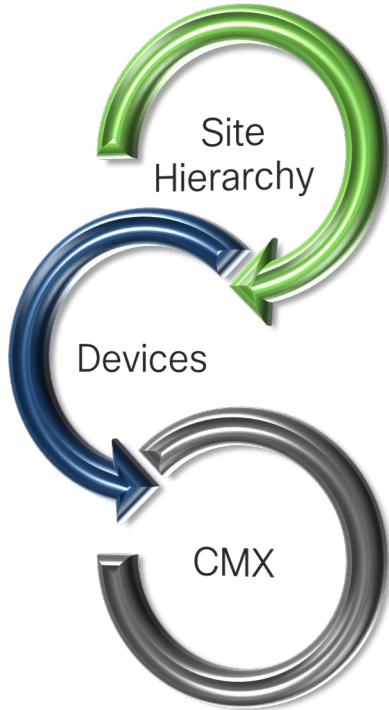
- Reports
- Configuration of WLC
- Update of Maps
- Rogue
- Compliance



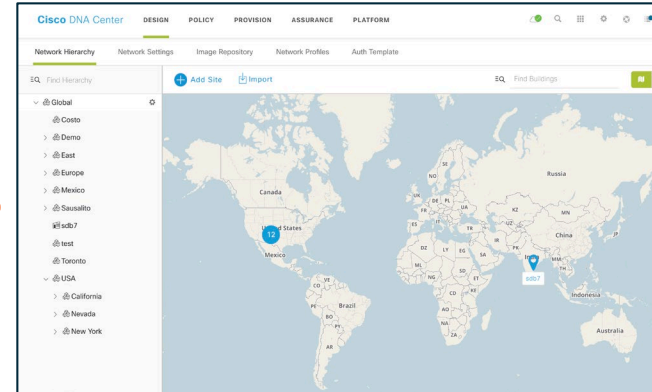
- Maps **synced** from Prime for selected sites
- Issues and resolution in DNAC
- Sensor & Proactive troubleshooting

# Co-Existence Overview

- Sites
- Buildings
- Floors with floor plan
- Floor elements – Inclusion/Exclusion Areas, Obstacles etc
- WLCs
- APs
- Routers
- Switches
  
- CMX Servers



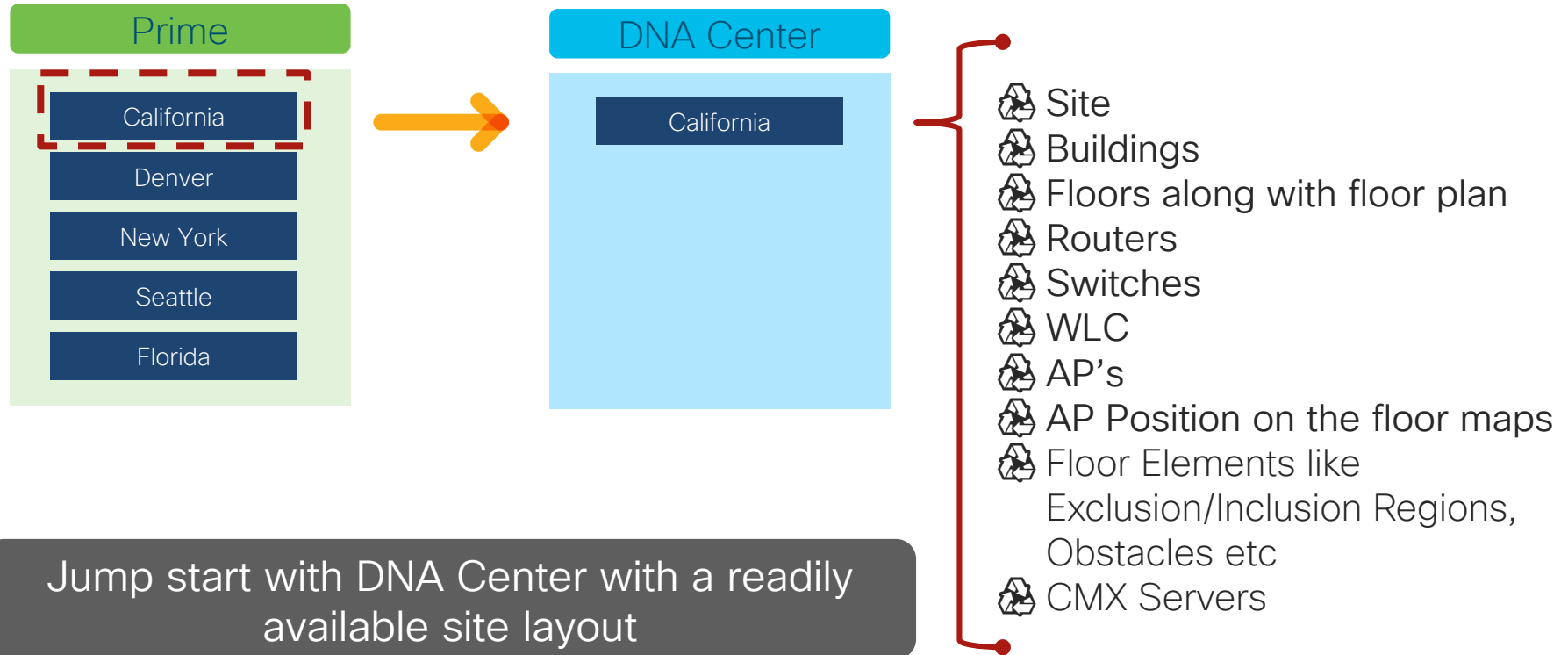
Prime Infrastructure  
3.5 Update 2



Cisco DNA Center –  
1.2.6, 1.2.8, 1.2.10, 1.3

Jump start with DNA Center with a readily available site layout

# Co-existence Overview



# Co-existence Workflow

The screenshot displays the Cisco Prime Infrastructure Administration / Settings / System Settings interface. The left sidebar shows the 'System Settings' menu with 'DNA Center coexistence' highlighted. The main content area is titled 'General DNA Center coexistence' and contains the following text:

**DNA Center coexistence**



You can now integrate Cisco Prime Infrastructure with Cisco Digital Network Architecture Center (DNA Center) and utilize the intent-based networking solution for managing application user experience in the enterprise.

DNA Center supports the expression of intent for multiple use cases, including base automation capabilities, fabric provisioning, and policy-based segmentation in the enterprise network. DNA Center adds context to this journey through the introduction of Analytics and Assurance. To know more about DNA Center, visit <http://cisco.com/go/dna>

You can migrate devices, site groups, associated site maps and CMX data from Prime Infrastructure to DNA Center and manage your enterprise network over a centralized dashboard.

[Launch DNA Center coexistence >](#)

# Co-existence Workflow

Prime Infrastructure - DNA Center Coexistence Logout

1 Add DNA Center Server → 2 Sync Settings → 3 Select Groups → 4 Enter CMX credentials → 5 Summary

### DNA Center Server

Prime Infrastructure supports integration of DNA Center 1.2.1 and above. You can integrate only one DNA Center server at a time.

- \*Server IP or Hostname:  ✓
- \*Username:
- \*Password:
- \*Confirm Password:

Success  
DNA Center Server added successfully.

# Co-existence Workflow

Prime Infrastructure - DNA Center Coexistence Logout

1 Add DNA Center Server → **2 Sync Settings** → 3 Select Groups → 4 Enter CMX credentials → 5 Summary

Enables automatic synchronization of data integrated with DNA Center ?

Include newly added data during dynamic synchronization ?

Supported / Available Limits

	Recommended Scale	Available
Site Groups / Site Maps	500	490
Devices	1000	978

Ensure that you don't exceed the recommended scale.

**Enabling auto sync will move modifications of already migrated data from Prime Infrastructure to DNA Center automatically right after modification**

Previous Next

# Co-existence Workflow

Prime Infrastructure - DNA Center Coexistence Logout

1 Add DNA Center Server → 2 Sync Settings → **3 Select Groups** → 4 Enter CMX credentials → 5 Summary

Site Groups / Site Maps: Selected 3 / Maximum 493 | Devices: Selected 3 / Maximum 981

**Prime Infrastructure Location Groups**


- All Locations
- Chennai
  - SDB Tower7
    - Ground Floor
  - System Campus

**DNA Center Site Groups**

- Global
- Bangalore
- Chennai
  - Sholinganallur
  - SDB Tower7 - *New!*
    - Ground Floor - *New!*
  - Fabric

[Previous](#) [Next](#)

# Co-existence Workflow

 Prime Infrastructure - DNA Center Coexistence Logout

1 Add DNA Center Server → 2 Sync Settings → 3 Select Groups → **4 Enter CMX credentials** → 5 Summary

•••••

### CMX Servers

You can integrate CMX server with DNA Center. Once integrated, the CMX for the selected site maps will not be managed by Prime Infrastructure.

Credential Status	Server IP	Server Name	Username	Owner	SSH Username	SSH Password	
<input type="text" value="true"/>	<input type="text" value="10.197.71.48"/>	<input type="text" value="admin"/>	<input type="text" value="admin"/>	<input type="text" value="admin"/>	<input type="text" value="cmxadmin"/>	<input type="password" value="....."/>	

**Save | Cancel**



# Co-existence Workflow

**Prime Infrastructure - DNA Center Coexistence** Logout

1 Add DNA Center Server → 2 Sync Settings → 3 Select Groups → 4 Enter CMX credentials → 5 Summary

● ● ● ● ●

Groups | Devices | Maps | CMX | Sync Settings

Add | Update | Delete

Group Hierarchy	Group Name
Location/All Locations	langtest
Location/All Locations/langtest	langbuild
Location/All Locations/langtest/langbuild	langfloor

**Note :** Based on the group selection above groups will get added / updated / deleted accordingly into DNA Center

**Status :** Force Sync Completed on Wed Oct 24 06:40:00 UTC 2018

Previous **Force Sync**

# Cisco DNAC vs Prime - Lifecycle Mgmt for IOS-XE Based Infrastructure



For your reference

	Cisco DNAC	Prime	Comments	
Day 0	Discovery/Inventory/Sites/Topology	✓	✓	
	Device Onboarding/PnP	✓	✓	
	Sensor Onboarding	✓	✗	
Day 1	StealthWatch/ETA Integration	✓	✗	
	App Policy	✓	✗	
	Rolling AP Upgrades	✓	✓	PI: limited support (AireOS only)
Day N	Rogue Detection	✓	✓	1.3.1: 1 <sup>st</sup> phase
	Proactive Insights w/ Sensors	✓	✗	
	Intelligent Capture	✓	✗	
	Application policy support	✓	✗	1.3.1: Configure and deploy application policies on Catalyst 9800 WLC
	Compliance	✗	✓	
	Reports	✓	✓	1.3.1: Client, Inventory, SWIM Roadmap: other reports

# Cisco DNAC vs Prime - Lifecycle Mgmt for IOS-XE Based Infrastructure



Day N

	Cisco DNAC	Prime	Comments
Defective device replacement	✓	✗	
Security advisories	✓	✓	Requires Machine Reasoning package
Browser-Based Configuration Wizard	✓	✗	
Application hosting	✓	✗	Docker applications on Catalyst 9300 series switches
Telemetry profile enhancements	✓	✗	1.3.1: support for the Application Visibility profile
ACI groups in Cisco DNA Center	✓	✗	
Wide Area Bonjour application	✓	✗	Provides you with centralized access control and monitoring capabilities for large-scale Bonjour services
Stealthwatch Security Analytics Service	✓	✗	1.3.1: 1 <sup>st</sup> phase
AI: Network Analytics	✓	✗	
AI: Trends, Insights, Comparative Analytics	✓	✗	
Data Rate KPI (wireless clients)	✓	✗	
Ekahau Integration	✓	✓	
Embedded Wireless Support: Fabric Edge	✓	✗	Support for Cisco Catalyst 9300/9400/9500 Series

# Key Takeaways

# Key Takeaways

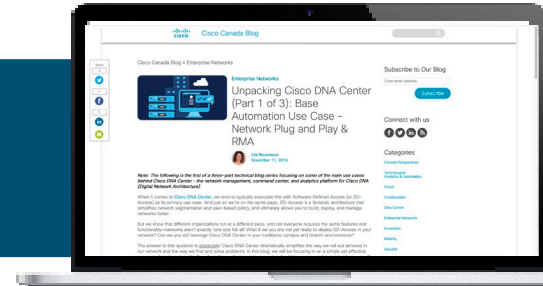
- Traditional NMS solutions are insufficient for managing TODAY's networks
- “Network Profiles” help deliver Business Intent for Automation - Day 0 to Day N
- Downtime is expensive. Leverage Cisco DNA Center Assurance to address issues faster to dramatically minimize downtime and increase productivity.
- DNA Center is real and ready for production deployments today, both greenfield and brownfield

# Check out my blogs

1

## Blog #1: Network Plug and Play & RMA

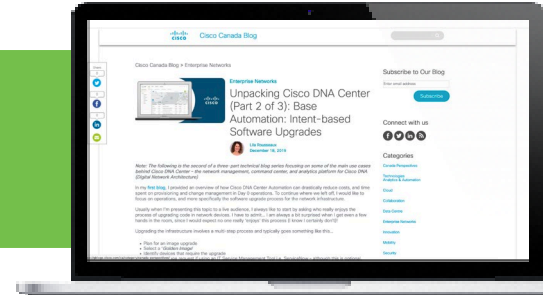
<https://gblogs.cisco.com/ca/2019/11/11/unpacking-cisco-dna-center-part-1-of-3-base-automation-use-case-network-plug-and-play-rma/>



2

## Blog #2: Intent-based Software Upgrades

<https://gblogs.cisco.com/ca/2019/12/18/unpacking-cisco-dna-center-part-2-of-3-base-automation-intent-based-software-upgrades/>



# Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on [ciscolive.com/emea](https://ciscolive.com/emea).

Cisco Live sessions will be available for viewing on demand after the event at [ciscolive.com](https://ciscolive.com).

# Continue your education



Demos in the  
Cisco Showcase



Walk-In Labs



Meet the Engineer  
1:1 meetings



Related sessions





Thank you





You make **possible**

# Reference Slides

Cisco DNA Center Scale  
and device support

# DNA Appliance – Scale and Hardware Spec

## DN2 – Entry

- ✓ 44 Core M5
- ✓ 1000 Switches and Routers
- ✓ 4000 APs
- ✓ 25K Clients (75K transient)
- ✓ 1.2.8 Release

## DN2 – Mid Size

- ✓ 56 Core M5
- ✓ 2000 Switches/Routers
- ✓ 6000 AP
- ✓ 40,000 Clients (120K transient)
- ✓ 1.3 Release

## DN2 – Large

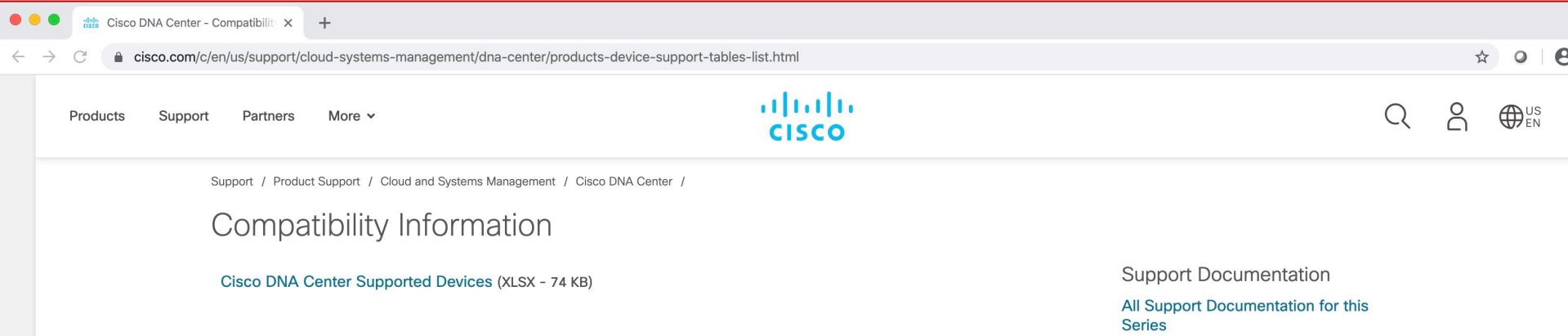
- ✓ 112 Core M5
- ✓ 5K switches/routers
- ✓ 13K AP
- ✓ 100,000 Clients (40/60KWLAN)  
(250K transient)
- ✓ 1.3 Release



Automation HA available with all models  
Cluster members must be of the same  
appliance type  
Including (DN2-Entry with DN1)



# Cisco DNA Center 1.3.3 Supported Devices



The screenshot shows a web browser window with the URL <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html>. The page features the Cisco logo and navigation links for Products, Support, Partners, and More. The main content area displays the title "Compatibility Information" and a link to "Cisco DNA Center Supported Devices (XLSX - 74 KB)". On the right side, there is a "Support Documentation" section with a link to "All Support Documentation for this Series".

<https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-device-support-tables-list.html>

Reference Slides

Sensor Tests

# Cisco DNA Center Sensor Tests

## Network Tests

- **Wireless Onboard Tests:** Connects to the SSID with credentials and gets the IP address through DHCP. It then verifies the gateway and DNS server received through DHCP.
- **RF Assessment Test:** Cisco DNA Center collects various RF performance measurements like Tx/Rx Data rate and SNR during the active sensor testing and assesses the quality of the RF environment during that sensor test.
- **DNS Tests:** Resolves IP address for the domain name.
- **Host Reachability Tests:** Verifies reachability using the Internet Control Message Protocol (ICMP) echo request.
- **RADIUS Tests:** The sensor acts as a RADIUS authenticator and authenticates through wireless. Sensors can test RADIUS Server using Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).  
\*if the network administrator is already using the Wi-Fi Onboarding test that includes 802.1x/EAP Authentication, then this RADIUS test is essentially already covered as part of the onboarding test.

# Cisco DNA Center Sensor Tests

## Performance Tests

- **Speed Test:** Performs tests against NDT servers in the internet to obtain to the downlink & uplink throughput and latency. Here is test sequence
  - Sensor will send http query to M-Lab Server to get nearest M-lab Server info.
  - Then Sensor will use returned NDT server cluster info
  - Sensor will access NDT server using TCP Port 3001
- **IP SLA Test:** Sensor sends an UDP probe to the AP that acts as a responder to determine the Jitter, Latency, Packet Loss and Round Trip time of the last hop



# Cisco DNA Center Sensor Tests

## Application Tests

- **Email Tests** includes the following:
  - **Internet Message Access Protocol (IMAP)** - Connects to IMAP server TCP port (143).
  - **Post Office Protocol3 (POP3)** - Connects to POP3 server TCP port (110).
  - **Outlook Web Server (OWS)** - Logs into the OWS (with On-Premise Exchange Server) and verifies access.
- **File Transfer Tests:** Tests for upload or download file operation using FTP protocol
- **Web Tests (http, https):** Tests for access to the provided URL and verifies the response data.

Reference Slides

Prime and DNAC  
Migration Scenarios

# Migration Scenarios



For your  
reference

- Full Migration from Prime to DNAC

- Prime and DNAC Co-existence

- 1 DNAC on Assurance Mode

PI = R/W,      DNAC = RO

- 2 DNAC on Automation + Assurance Mode

PI = RO,      DNAC = R/W

- 3 DNAC on Automation Mode

PI = RO,      DNAC = R/W

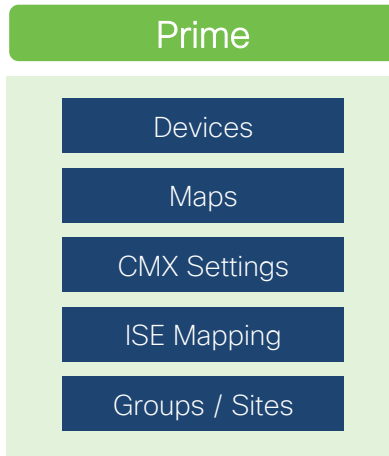
There is only one system that will make changes to the network

# Scenario 1

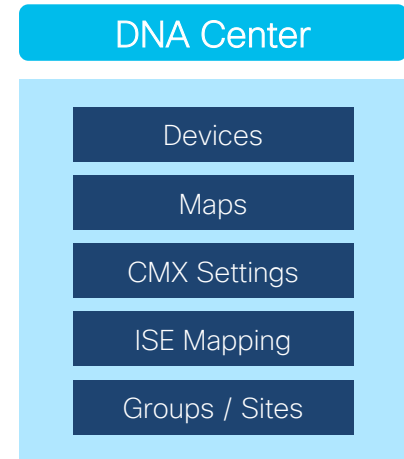
## Full Migration: Prime to DNA Center



For your reference



One-time migration to  
DNA Center



# Co-Existence: Scenario - 1

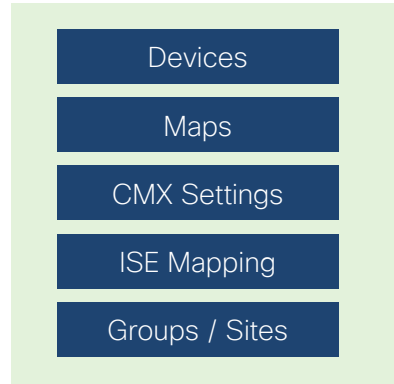
## Assurance in DNA Center and Config in Prime



For your reference

1

### Prime

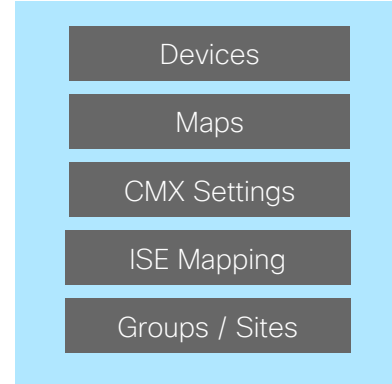


Select WLC  
- Migrate to  
DNAC



Identify the  
Sites  
Managed  
by WLC

### DNA Center



### WLC is RO in DNAC



- Reports
- Configuration of WLC
- Update of Maps
- Rogue
- Compliance



- Maps **synced** from Prime for selected sites
- Issues and resolution in DNAC
- Sensor & Proactive troubleshooting

# Co-Existence: Scenario - 2

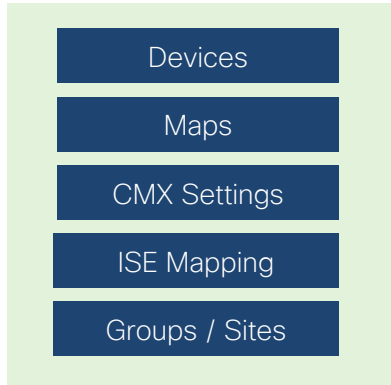
## Assurance and Automation in DNA Center



For your reference

2

### Prime



### WLC is RO in Prime

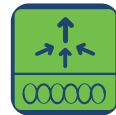
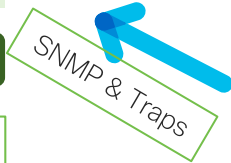
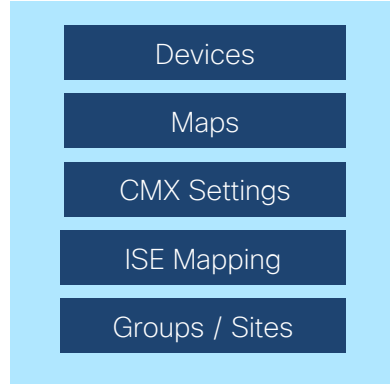
- Reports
- Rogue
- Maps **synced** from DNAC for migrated sites
- Cannot push changes to WLC or AP's managed by DNAC

Select WLC  
- Migrate to  
DNAC



Identify the  
Sites  
Managed  
by WLC

### DNA Center



- Automated Deployment
- Issues and resolution in DNAC
- Sensor & Proactive troubleshooting
- Maps and AP Placement

# Co-Existence: Scenario - 3

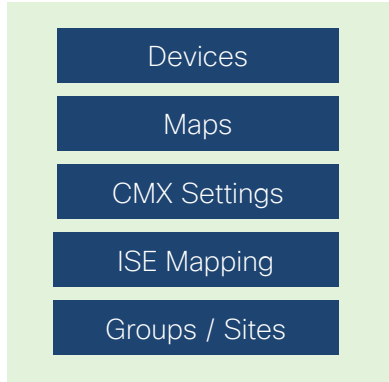
## Automation in DNA Center and Monitoring with Prime



For your reference

3

### Prime



### WLC is RO in Prime

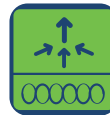
- Reports
- Rogue
- Maps **synced** from DNAC for migrated sites
- Troubleshooting from Prime

Select WLC  
- Migrate to  
DNAC

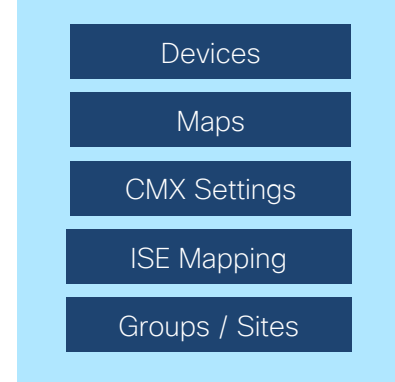


Identify the  
Sites  
Managed  
by WLC

SNMP & Traps



### DNA Center



- Automated Deployment
- Software Update
- Day 2 Changes
- Maps and AP Placement



You make **possible**