



You make **possible**



# From Prime Infrastructure to Software Defined Network (SDN) Management with Cisco DNA-Center

Soren Dulong Andreasen  
Stefan Leemann

BRKNMS-2573

**CISCO** *Live!*

Barcelona | January 27-31, 2020





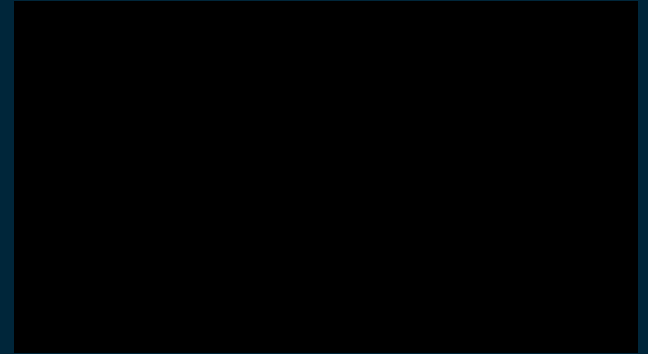
# From Prime Infrastructure to Software Defined Network (SDN) Management with Cisco DNA-Center

Soren Dulong Andreasen  
Stefan Leemann

BRKNMS-2573

**CISCO** *Live!*

Barcelona | January 27-31, 2020



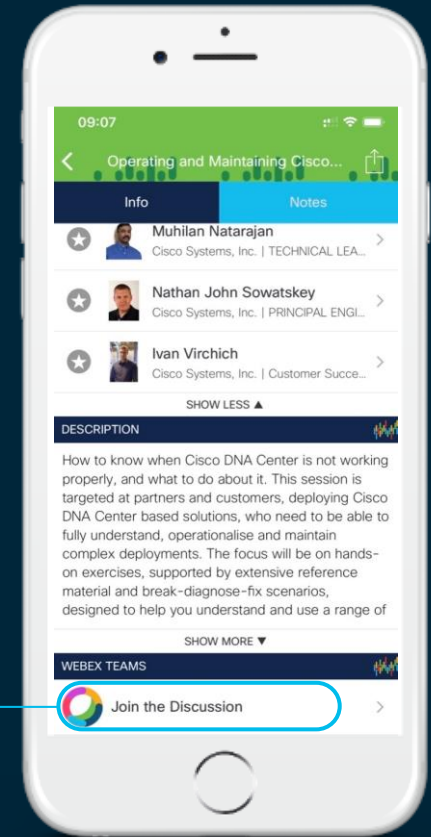
# Cisco Webex Teams

## 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



# CISCO *Live!* IS LIKE A BOX OF CHOCOLATES



The Chocolate on your seat can only be eaten during the official Chocolate Breaks in this session



“Cisco Live Chocolate Breaks”  
invented by Soren and Stefan

# Our Mission statement

*Get all the benefits  
of Cisco DNA-  
Center with  
Co-Existence to  
Prime Infrastructure*



Soren Dulong Andreasen

soren@cisco.com



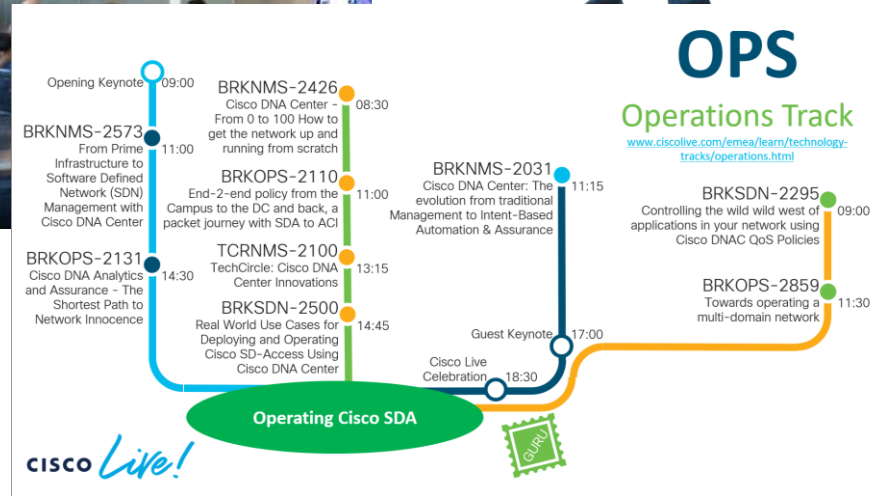
Stefan Leemann

stleeman@cisco.com

# Agenda

1. Introduction
2. Change in Paradigm in Network Management
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

# Introduction



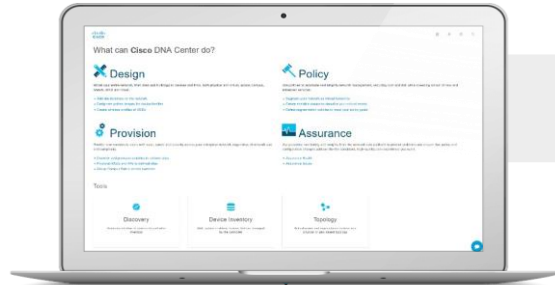
**CISCO Live!**



# Cisco DNA Center

Intent-based controller for the enterprise

Cloud-Enabled



Policy



Provision



Design



Assurance

Cisco DNA Center Appliance



Physical and virtual infrastructure

Cisco and third party



Controller-based automation and analytics



Campus, branch, extended enterprise, wired and wireless



360-degree open platform



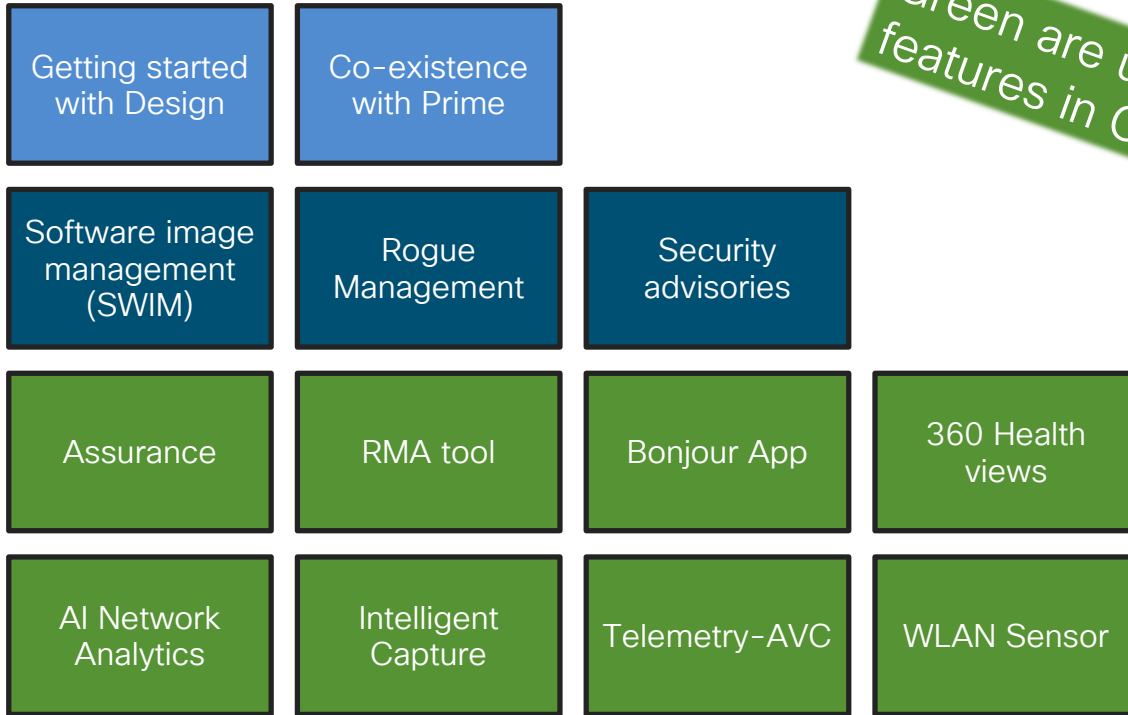
Fully integrated, distributed security



Analytics, machine-learning driven



# What's covered



# Other features unique to Cisco DNA Center

Programmability &  
Integrations

Intent Based  
Application Policy

SD-Access

StealthWatch  
integration

IOS-XE App  
hosting setup

Embedded  
Wireless  
Controller on  
Catalyst AP

License Manager

# Topics covered in the 2018 and 2019 version of BRKNMS-2573

Plug and Play

Wireless  
Automation

Automate  
configuration  
changes

SD-Access,  
provisioning and  
policy control

Service Now  
integration

IPAM integration

North / South  
API's

3<sup>rd</sup> Party support

# Agenda

- 1 Introduction
2. Change in Paradigm in Network Management
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A



## Prime Infrastructure



## Cisco DNA Center



### Traditional Network Management

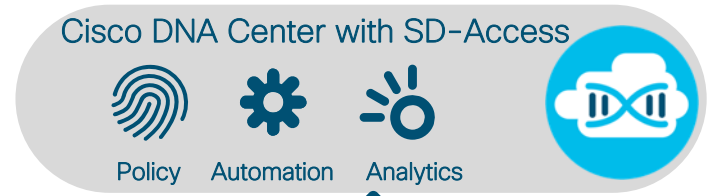
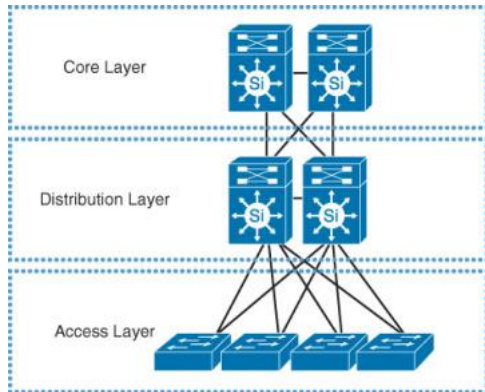
- Software Image Distribution
- Configuration Archive/Backup
- Templating for Automation
- Reporting
- Assurance
- Events
- Tons of data, but not enough insights.
- Semiclosed system with predefined configurations.

### Intent base Network Management

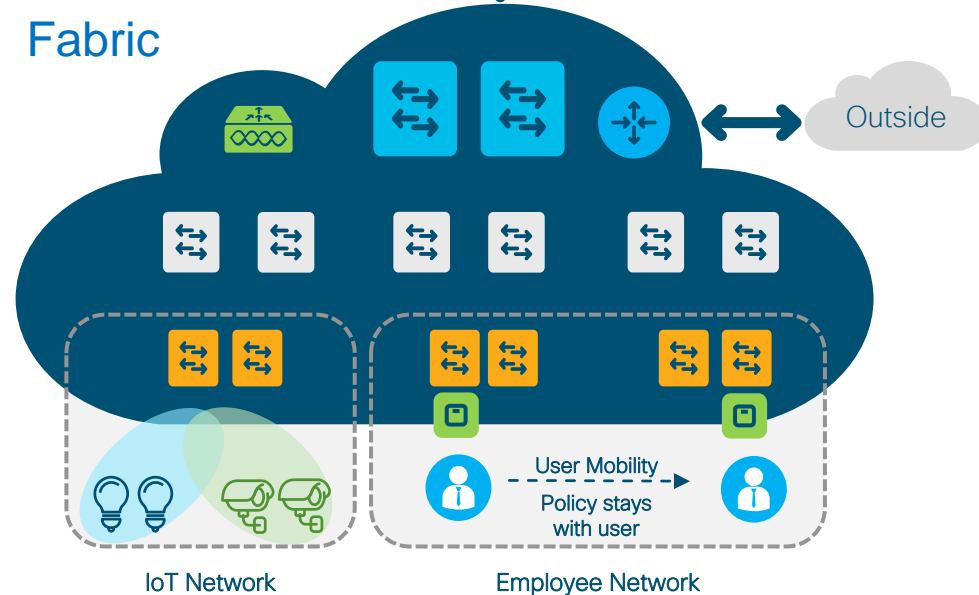
- No events/alarms, but insights and impact analytics with Guided remediation
- Automation, day0, day1, day2
- Policy and segmentation control
- Software update (ITSM, Compliance)
- Network telemetry data collection
- Baselining over time, baseline against others
- No manual configuration required
- API and Business API

# You decide what Cisco DNA-Center will do for you

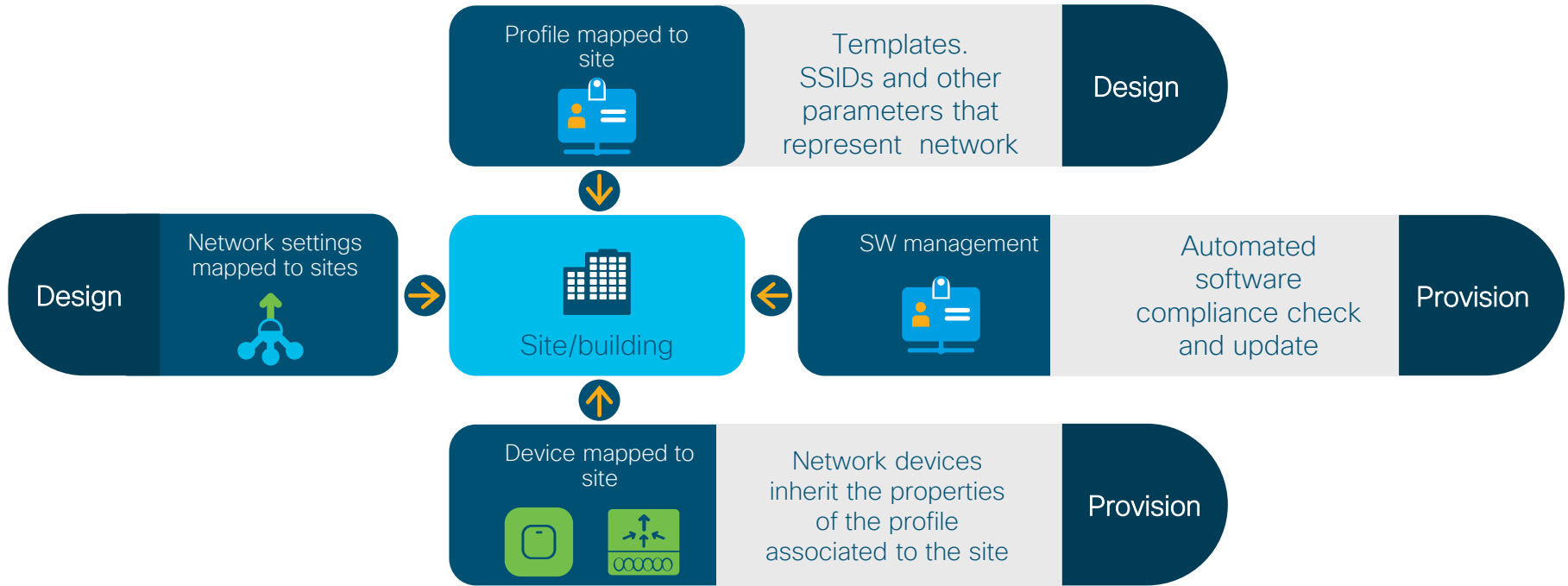
Network Management of classic-Design Enterprise networks



Fabric



# An Intent Based deployment model



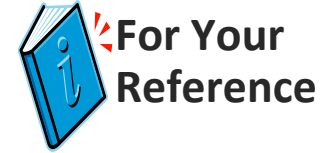
Intent-based workflows

Automated deployment

Cisco best practices



# DNA Center and Prime - Automation

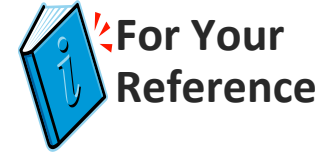


	Prime	DNA Center
Core Functions	Wireless Maps for AP Placements	★
	CMX Integration	MSE Integration
	AP Onboarding	★
	AP Day 2 Changes	Roadmap *
	WLC Configuration - Day 0/N	★
	Brownfield Support (Learning from WLC)	★
	SWIM	★
	Reports	Three reports today (more in roadmap *)
Advanced	Configuration Audit & Compliance	Roadmap *
	Rolling AP Upgrades	
	Bulk Configuration changes on multiple WLC's	
	Position by 2 walls and 3 points	Roadmap *
Differentiators	Auto Placement of AP's using CAD Files	Roadmap *
	Location/IP/Switchport based AP Onboarding	Roadmap *
	Unified configuration flow for all architectures	
	Flex Enhancements for SWIM	Roadmap *

★ Better in DNAC

\* subject to change

# DNA Center and Prime - Assurance



Core Functions

	Prime	DNA Center
Wireless heatmaps for troubleshooting		★
Application Visibility		★
Reporting		Three reports today (more in roadmap *)
Health Dashboards		★
Real Time Client, Network and App Data	SNMP Based	2-90 Sec ★ (Streaming Telemetry)
Rogue Management & Detection		★
wIPS		Roadmap *
*Switch Port Tracing		Roadmap *
*ISE Integration		
WGB Client Support		Roadmap *
CMX Integration for Tracking Clients		
Intelligent Packet Capture		
Proactive Sensor Testing		
iOS Wi-Fi Analytics		
Guided Issue Remediation		
Application Experience		★
Historical Troubleshooting		★
Integration with ITSM (ServiceNow)		

★ Better in DNAC

Differentiators

\* subject to change



# Agenda

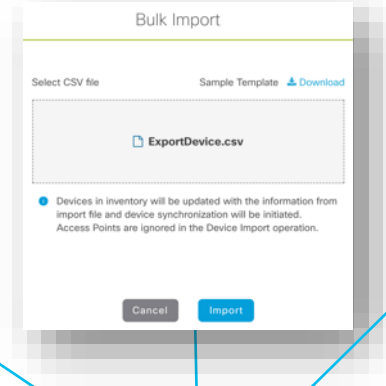
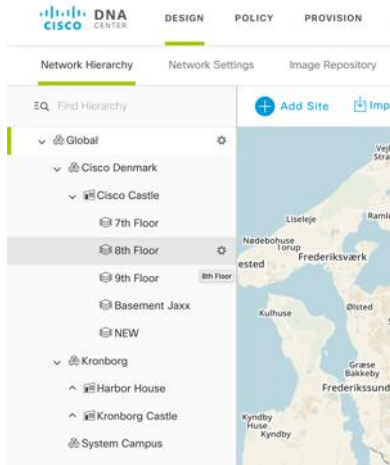
- 1 Introduction
2. Change in Paradigm in Network Management
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

# Getting started with Design

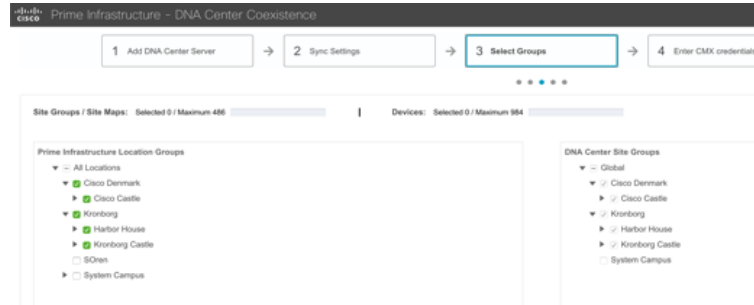
# How to create your design : Site Hierarchy

## 2) Manually Export /Import from Prime

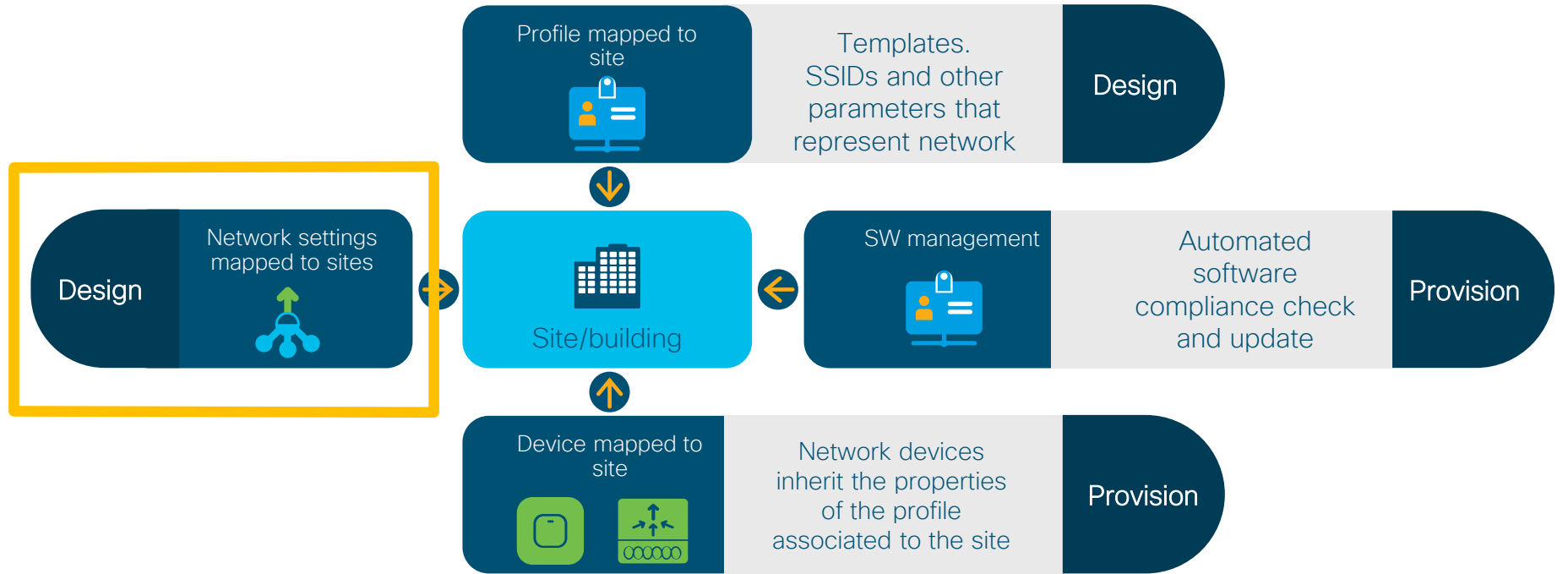
### 1) Manually



### 3) Prime 3.5 Co-existence Tool



# Network settings



Intent-based workflows

Automated deployment

Cisco best practices



# Design -> Network Settings

Be careful! Cisco DNA-Center will configure these settings instantly on all devices based on location etc.

```
sandreas ~ telnet 10.100.0.1 -- 80x24
-- telnet 10.100.0.1
-- bash
ip sla 64427530
icmp-echo 10.100.56.1
owner Cisco IT Realtime Monitoring
Frequency 30
ip sla schedule 64427530 life forever start-time now
logging host 10.101.1.79
logging host 10.101.1.69
logging host 10.101.1.142
!
snmp-server community balocsc!R0
snmp-server community public!R0
snmp-server community Wert432!R0
snmp-server community Public!R0
snmp-server location Soren
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
```



https://10.101.1.141/dna/design/home?site=0c802df1-9d9a-46f3-9c09-1488e68555d6/b5a13f1f...

Most Visited Getting Started Viewing Feed (18) Top 50 IDIOTS ...

DNA CENTER DESIGN POLICY PROVISION ASSURANCE PLATFORM

Network Hierarchy Network Settings Image Repository Network Profiles Auth Template

Find Hierarchy

- Global
- ^ Cisco Denmark
- ^ Kronborg
- System Campus

Network Device Credentials IP Address Pools SP Profiles

Setup network properties like AAA, NTP, Syslog, Trap and NetFlow using the deploy using these settings.

DHCP Server

DHCP 10.99.2.200 +

DNS Server

Domain Name cicolab.dk


Primary 10.99.2.200 +

SYSLOG Server

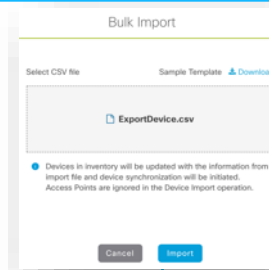
SYSLOG 10.101.1.69 Additional SYSLOG 10.101.1.141

# Getting devices into Cisco DNA-Center

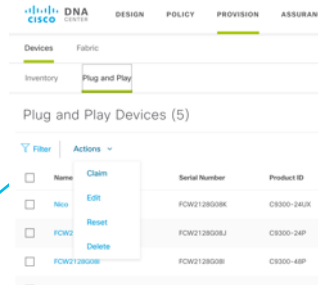
2) Manual add into Inventory



3) Bulk Import via CSV

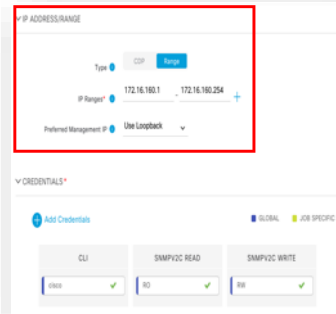


4) Plug and Play

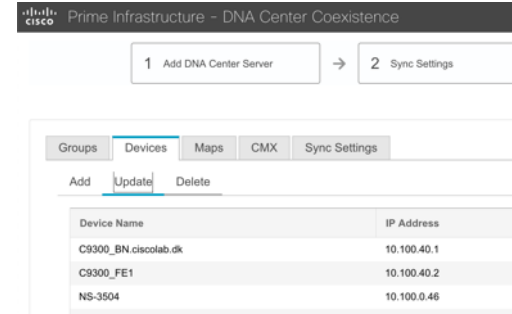


Name	Claim	Serial Number	Product ID
Nico	Edit	FCW2128508K	CS900-240K
FCW2	Reset	FCW2128508J	CS900-24P
FCW2128508	Delete	FCW2128508	CS900-48P

1) Discovery Job



5) Prime -> Co-Existence



Device Name	IP Address
C9300_BN_ciscolab.dk	10.100.40.1
C9300_FE1	10.100.40.2
NS-3504	10.100.0.46



*CISCO Live!*

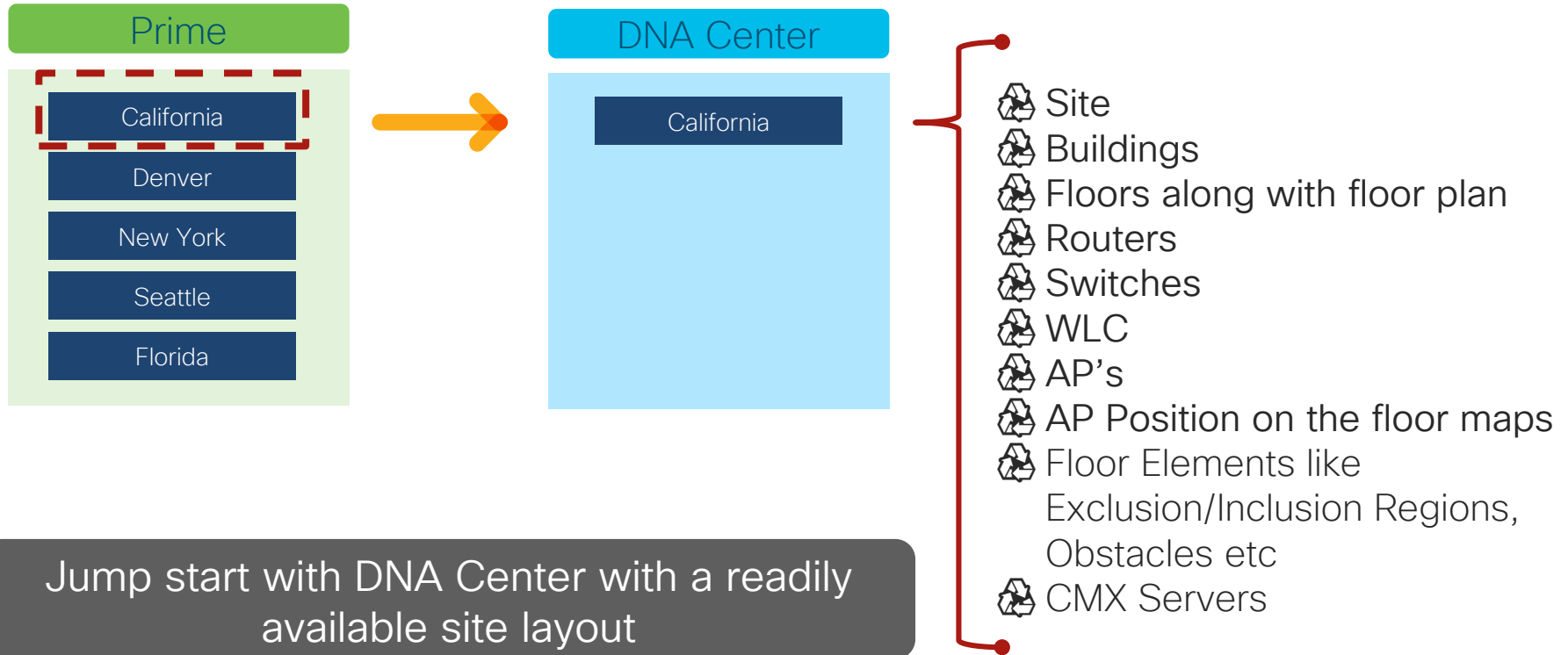


# Co-Existence Tool to assist with Migration

# Co-existence Objectives

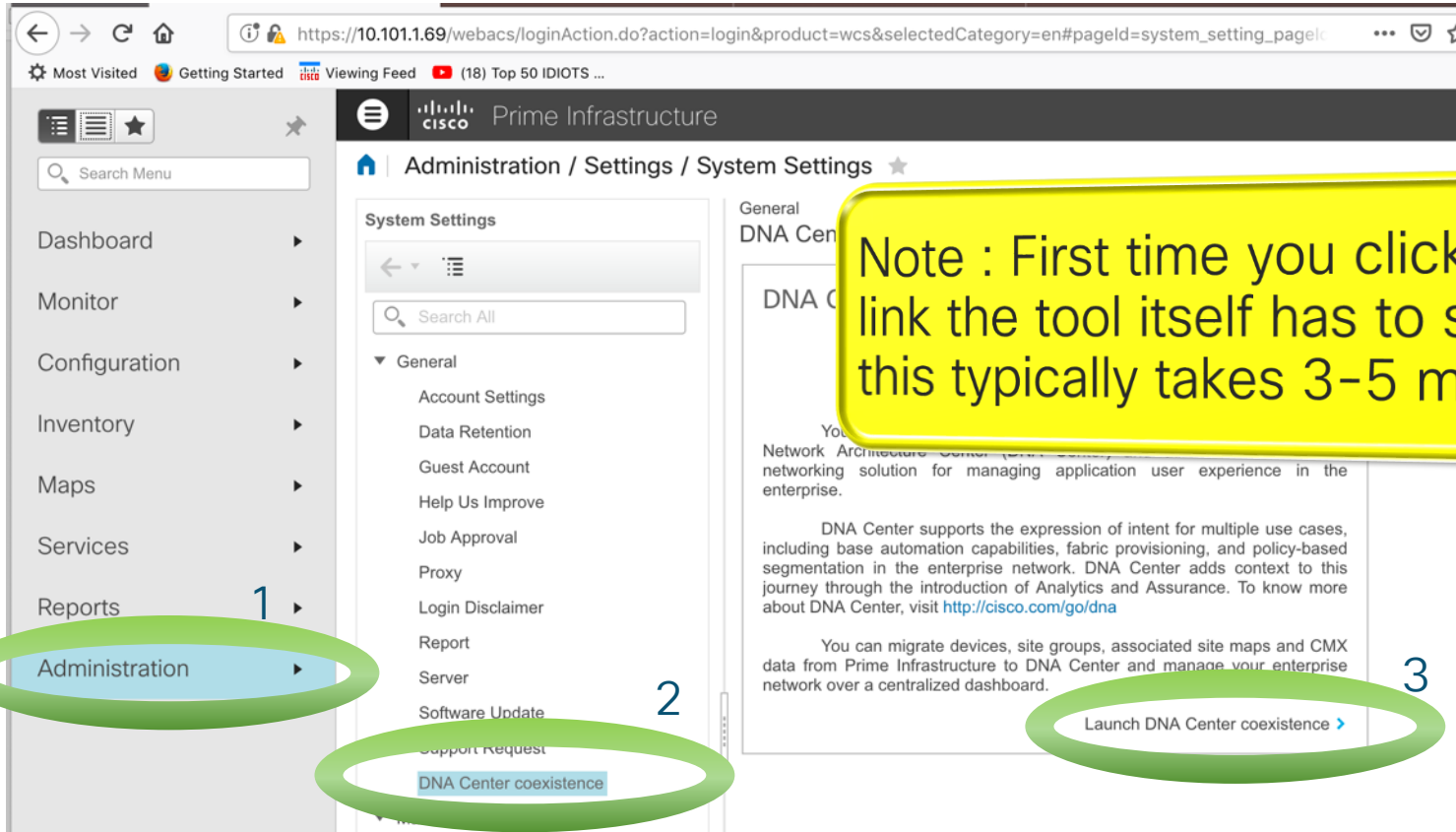
- 1 Start using Cisco DNA Center with minimal efforts for Prime Infrastructure customers
- 2 Migrate Devices, Location Groups, Maps and CMX Servers from Prime Infrastructure to Cisco DNA Center seamlessly using the workflow
- 3 Allow Incremental updates to the migrated dynamically
- 4 Make it easy to run Prime Infrastructure and Cisco DNA-Center in parallel

# Co-existence Overview



Jump start with DNA Center with a readily available site layout

# Start the Cisco DNA-Center Co-existence tool



https://10.101.1.69/webacs/loginAction.do?action=login&product=wcs&selectedCategory=en#pageId=system\_setting\_pageId

Most Visited Getting Started Viewing Feed (18) Top 50 IDIOTS ...

Prime Infrastructure

Administration / Settings / System Settings

System Settings

Search All

General

- Account Settings
- Data Retention
- Guest Account
- Help Us Improve
- Job Approval
- Proxy
- Login Disclaimer
- Report
- Server
- Software Update
- Support Request
- DNA Center coexistence

General DNA Center

DNA C

Note : First time you click the link the tool itself has to start, this typically takes 3-5 minutes

You

Network Architecture Center (NAC) is a

networking solution for managing application user experience in the enterprise.

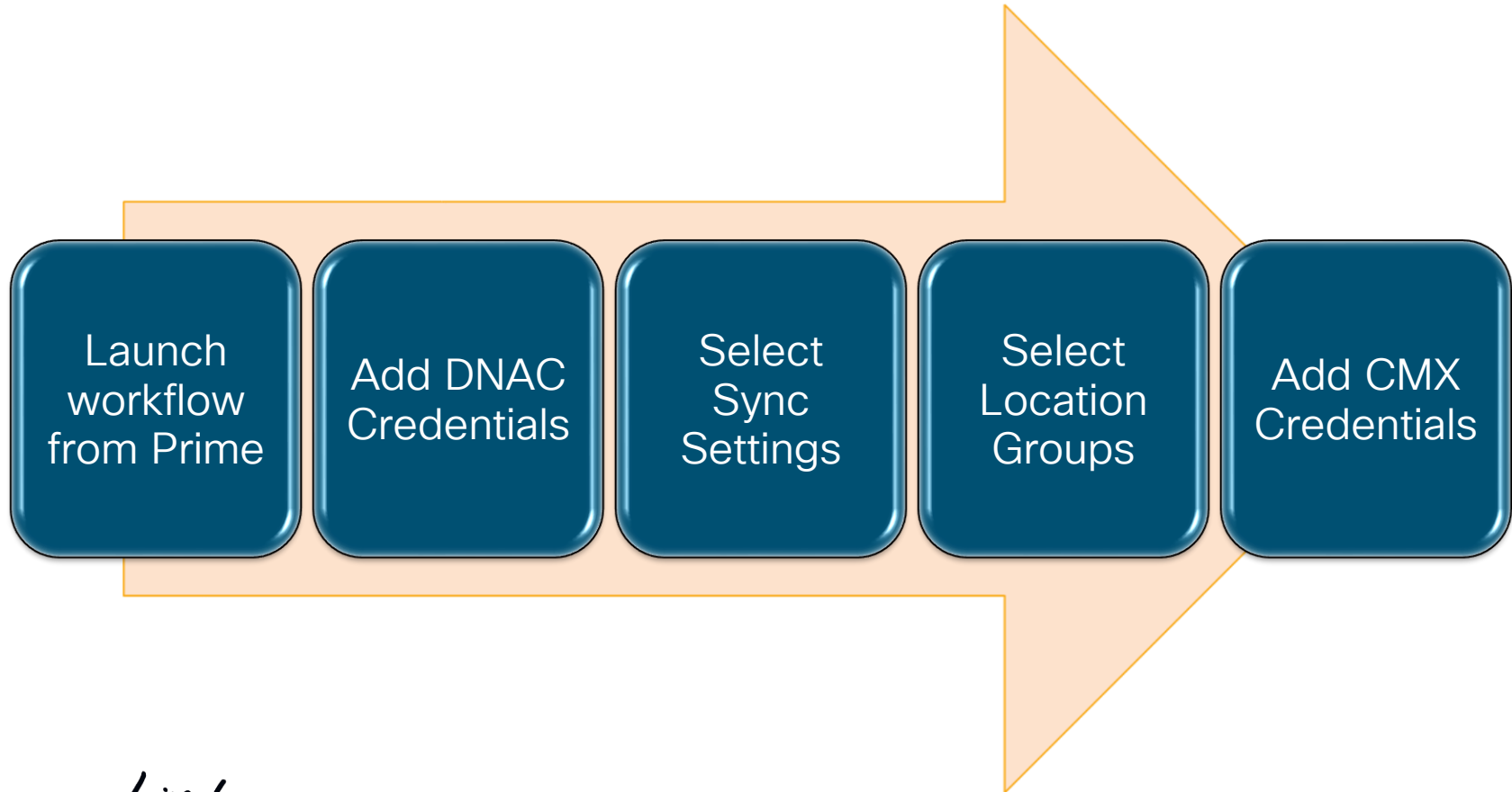
DNA Center supports the expression of intent for multiple use cases, including base automation capabilities, fabric provisioning, and policy-based segmentation in the enterprise network. DNA Center adds context to this journey through the introduction of Analytics and Assurance. To know more about DNA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

# Demo, Prime Co-existence

# Workflow Summary



# Sync Behavior



## Force Sync

- Force sync essentially pushes all data, based on selection of groups, irrespective of the previous data push from PI to DNA Center
- For any setting change to come into effect, a force sync has to be done
- Initial sync from PI to DNAC will always be a force sync

## Auto Sync

- Auto Sync is an incremental, dynamic synchronization of the data from PI to DNAC based on the earlier selection
- Any changes to groups association and device credentials will be synced
- CMX and Maps are not in scope of auto sync and need to be triggered via the Force Sync option
- Auto sync has 2 modes of operation :
  - ✓ Changes to the already synced groups and devices only are pushed to DNAC
  - ✓ Any new groups added as a sub-group to the already selected location groups and its device association are pushed to DNAC

# Some comments on Cisco DNA-Center co-existence tool (1/4)



Supported Prime Infrastructure versus Cisco DNA-Center versions can be found in the Cisco Prime Infrastructure 3.X Administrator Guide (see upcoming slide)

For Catalyst 9800 WLC you will need to manually add Netconf “port” and SSH credentials  
10.5.0 and above versions of CMX is supported  
SNMPv1 not supported in DNA-Center

PI user credentials has to be Root  
Area/Site/floor names has to have be less then 32 characters and not contain “/”

What happens behind the scenes: API calls between the Co-exist tool and Prime Infrastructure and between Co-exist tool and Cisco DNA-Center



# Some comments on Cisco DNA-Center co-existence tool (2/4)



Migration of 500 groups + 1000 devices using force sync will take between 20-30 minutes

Removal of many groups/devices/maps takes more time(hours)

Tip : If you are having issues, try and do it manually to see the error messages. You can also have a look in the logfile on Prime  
“/opt/CSCOlumos/logs/process\_dnac\_migration.log”

Adding an AP or moving and AP on a MAP requires a manual “force sync” from the Co-exist tool

# Some comments on Cisco DNA-Center co-existence tool (3/4) Prime Infrastructure 3.7



Appliance Type	Site Groups/Site Maps	Devices
DN1-HW-APL DN2-HW-APL	500	1000
DN2-HW-APL-L	1000	4000
DN2-HW-APL-XL	2000	5000

Cisco DNA Center Version	Supported/Recommended
1.2.1	Supported
1.2.2	Supported
1.2.3	Supported
1.2.4	Supported
1.2.5	Supported
1.2.6	Supported & Recommended
1.2.8	Supported & Recommended
1.2.10	Supported & Recommended
1.2.10.4	Supported & Recommended
1.2.11	Supported & Recommended
1.2.12	Supported & Recommended
1.3.0	Supported & Recommended
1.3.0.1	Supported
1.3.0.2	Supported
1.3.0.3	Supported & Recommended
1.3.1	Supported & Recommended

# Some comments on Cisco DNA-Center co-existence tool (4/4)



- If your WLC('s) is not assigned to a site(unassigned) or its assigned to the “System Campus”, then it will not be exported to DNA-Center
- Sensor(s) will be deleted from maps if already added in DNA-Center

# Upcoming enhancements in PI 3.7.1/3.8



Error Message enhancement: On failure of DNAC Server integration, error messages have been changed to adhere to exact reason of failure like “Certificate Error, Credential error, unsupported version and Server not reachable

## UI Enhancements:

Allow to select more than 500 records in Group selection screen

Provided “Progress Bar” widget in summary screen tab while the operation is in progress

Ability to guess Country based on Civic address or Geo location

Avoiding stale entries of “Site” from being migrated to DNAC and displaying the stale groups as strike through

Avoid database issues by blocking dynamic updates when Cisco DNA Center is upgraded to unsupported version

# CISCO *Live!* IS LIKE A BOX OF CHOCOLATES



Chocolate  
Break

# RMA tool

# Device Replacement – RMA

Eliminate manual interventions for device replacements



## Unified Workflows

- Common workflows to replace Switch, Router, Access Points\*, Sensors\*, C9800 WLC\*
- Restores Image, Configuration, License
- Like to like device replacement

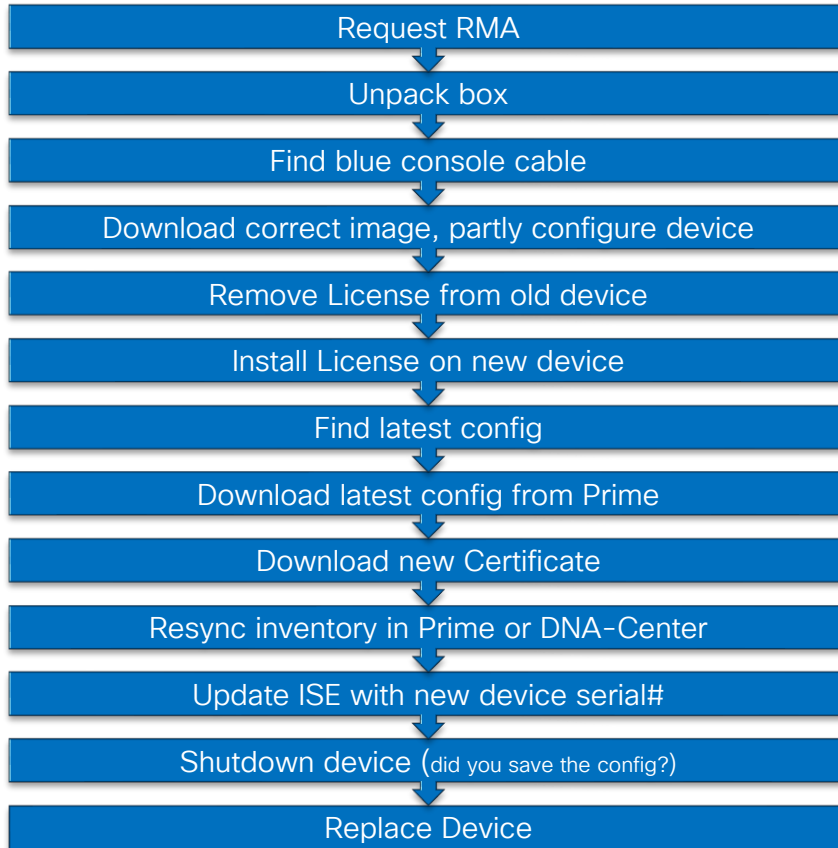


## RMA Operations

- Replace device in ISE
- Replace device in Cert server
- Copy license from old device to new device
- Replace device in DNAC inventory
- Preserve KPI trends for old device

Single workflow for Wired and Wireless hardware replacement

# Why RMA in Cisco DNA Center?



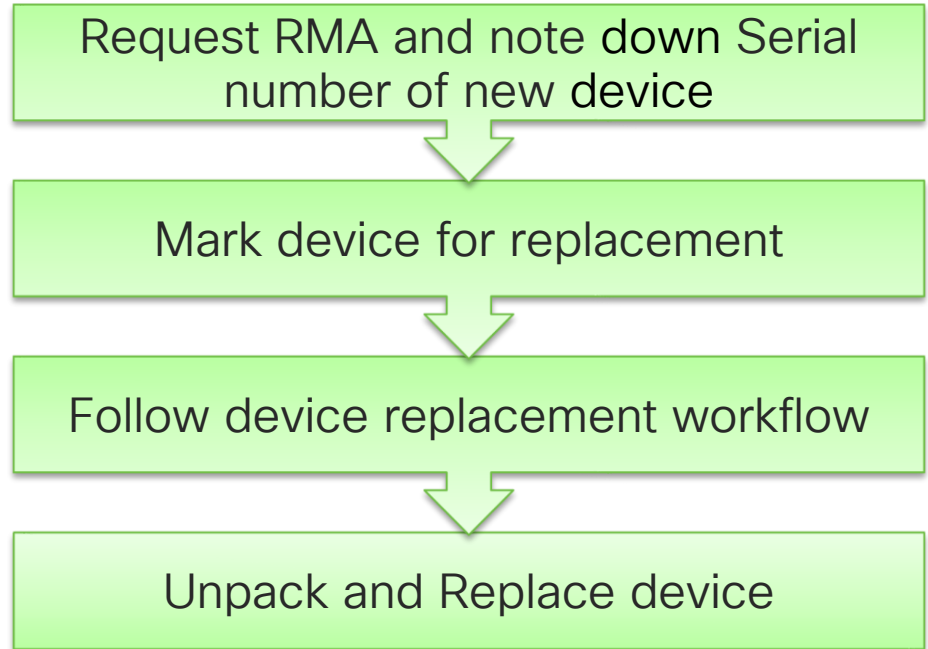
Prime Infrastructure



# Why RMA in Cisco DNA Center?



Cisco DNA-Center



# Wifi AP refresh

**Coming soon to a cinema near you..**

A decorative pattern at the top of the slide consists of numerous vertical bars and circles of varying heights and widths, arranged in a somewhat rhythmic, wave-like sequence across the width of the page. The elements are dark blue, matching the background.

# Demo, RMA tool

# Key Points for RMA from 1.3.1



- Exact PID to PID (C9300L-48UXG-2Q to C9300L-48UXG-2Q)
- Supports SD-Access
- RMA Methods:
  - **Zero-Touch RMA** - Replacement device is connected to Cisco DNA Center via PnP. No manual configuration on device required. (For SD-Access, DHCP should be configured on the “upstream” device)
  - **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
- Unclaimed state
  - Device did PnP and was redirected to DNA-Center
  - Device was added to DNA-Center manually
  - Device was learned from Smart Account PnP portal

# Prerequisites for RMA in 1.3.1



- Any device can be marked for replacement, but replacement workflow can only be done for a device that is unreachable
- Only “Managed” and “Not Provisioned” devices in Inventory and “Unclaimed” devices in Plug and Play are eligible as replacement devices for RMA.
- For Zero-Touch RMA, faulty device should be assigned to site before failure.
  - If it is not assigned to site before failure, it can be recovered only by One-Touch RMA method (via discovery).
- Software image of faulty device should be in repository of Software Image Management (SWIM).
- Replacement device should be connected to neighbor devices on the same port(s) as faulty device in topology. (Well,, Same vlan/subnet is enough)

# Limitations for RMA in 1.3.1



## Not Supported:

- Stack Switch, StackWise Virtual (SVL), SUP(s) in Modular Switches, Nexus Switches
- Access Points, Wireless Sensors and Wireless Controllers (AireOS, C9800 or C9800 Embedded).
- Routers with network modules such as UCS-E\*, SM-X-ES3\*, NIM-SSD, SSD-MSATA-200G
- SDA: Extended node and Fabric-in-a-Box.

## License:

- Support only restoring of DNA/Network Essential and DNA/Network Advantage licenses.
- Restoration of legacy switching licenses (e.g. LAN base, IP base and IP service) and routing licenses (IP base, security and etc.) is not supported. Note that License Manager does not show license info if switches with legacy license are running image prior to 16.8.
- Workaround: Configure legacy licenses manually before triggering replacement in RMA workflow

# Limitations for RMA in 1.3.1



## 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.

## Zero-Touch RMA via PnP

- When new device is claimed via PnP for RMA, if it is reloaded 1<sup>st</sup> time for image activation, DHCP IP on new device may change, which could cause image validation failure in RMA.

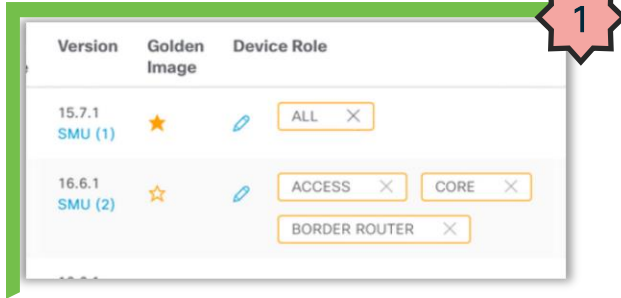
## Certificate

- Support revocation of device certificate on faulty device if it is issued by Cisco DNA Center PKI, but does not support request and installation of device certificate by same CA on new device yet.
- Do not support revocation, request and installation of device certificate if it is issued by any CA outside Cisco DNA Center, e.g. auth certificate on router for DMVPN not issued by Cisco DNA Center PKI.

SWIM

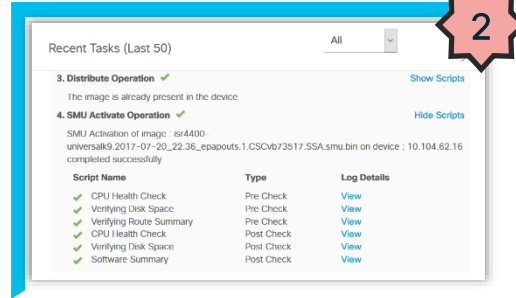


# Core Principles of Software Upgrade with DNA Center



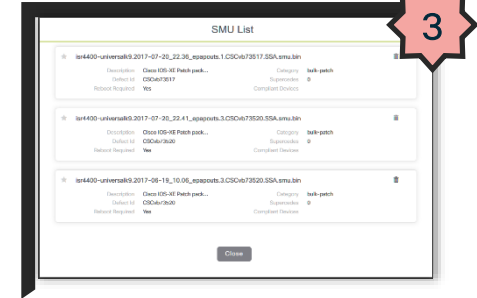
## Intent based Network Upgrades

Standardization of Software by Network device role, device type and location



## Seamless Upgrades

Pre/Post check validations with rollback provide confidence for upgrades



## Reduce Downtime with Patching

Upgrade only what is needed with minimal to zero downtime

# Software Image Management with DNA-Center

Note: Marking a software version as Golden does not update the device automatically

## What can SWIM do for you:

- Upgrade software on switches, routers, WLC's (show recommended image)
- SMU support (patching)
- Rommon upgrade with software upgrade (requires Cisco.com access/credentials)
- Image Update Readiness Check (enough space, enough ram etc)
- Use an approval workflow
- Schedule upgrade and activation

## Software images can be uploaded to DNA-Center:

- Manually using browser or ftp/http
- Directly from Cisco.com (needs cisco.com credentials)

## Software can be marked golden based on:

- Device family type (9300, 9400 etc)
- Role (access, core etc)
- Site (area, building, floor)

# Software Image Management

## Intent Based Network Upgrades



Captures your upgrade intent to automate process and drive consistency

## Streamlined Upgrade Process



Upgrade base image, patches, and other add-ons in one single flow

## Trustworthiness Integration

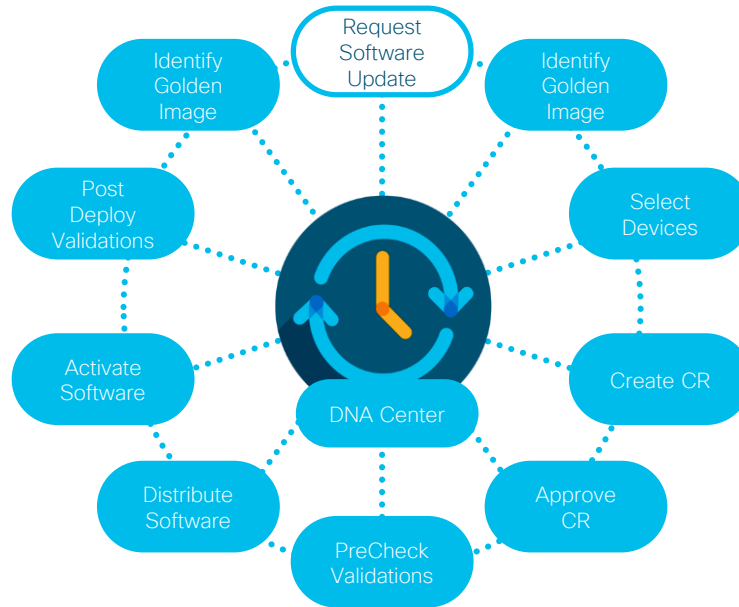


Assures that device images are not compromised in any way.

## Patching Support



Pre/Post check ensures updates do not have adverse effects on network



Automate your software upgrade cycle

# Demo, SWIM

# Rommon upgrade supported on



## Routers

PID	Standalone
ISR 4431	YES
ISR 4221	YES
ISR 4351	YES
ISR 4451-X	YES
ASR 1001-X	YES
ASR 1002-X	YES
ASR 1006-X (RP2)	YES
ASR 1006-X (RP3)	YES
ASR 1009-X (RP2)	YES
ASR 1009-X (RP3)	YES
ASR 1001-HX	YES
ASR 1002-HX	YES

## Switches

PID
C4500-E/X (SUP 7E 7LE 8LE)
C4500-X (SUP 7E 7LE 8LE)
C4507R+E (SUP 7E 7LE 8LE)
C4503/6E (Sup 8E   9E)
C4507R+E (Sup 8E   9E)
C4510R+E (Sup 8E   9E)
C4500X Fixed Chassis
C6503/4/6/9E (Sup 2T 6T)
C6513E (Sup 2T 6T)
C6807-XL (Sup 2T 6T)
C6840-X and C6880-X

Device Controllability is your friend ;-)  
How can I see that a software image is  
downloaded already?

# Cisco DNA Service for Bonjour

# Bonjour Services Use Cases

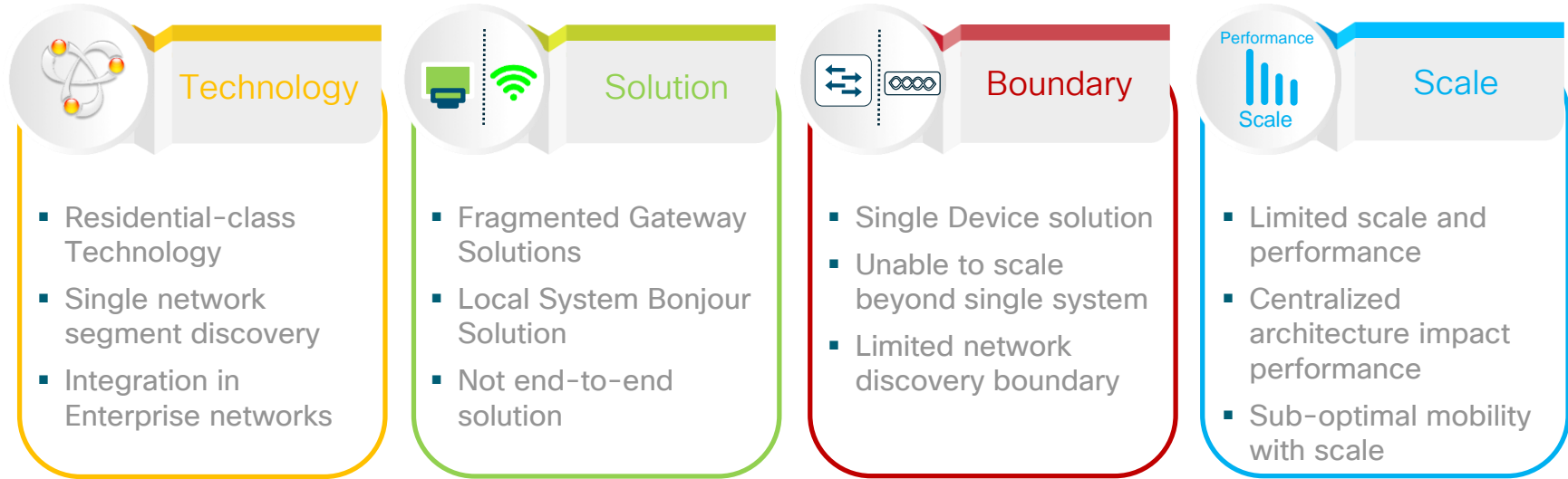


Bonjour enabled devices on the rise!

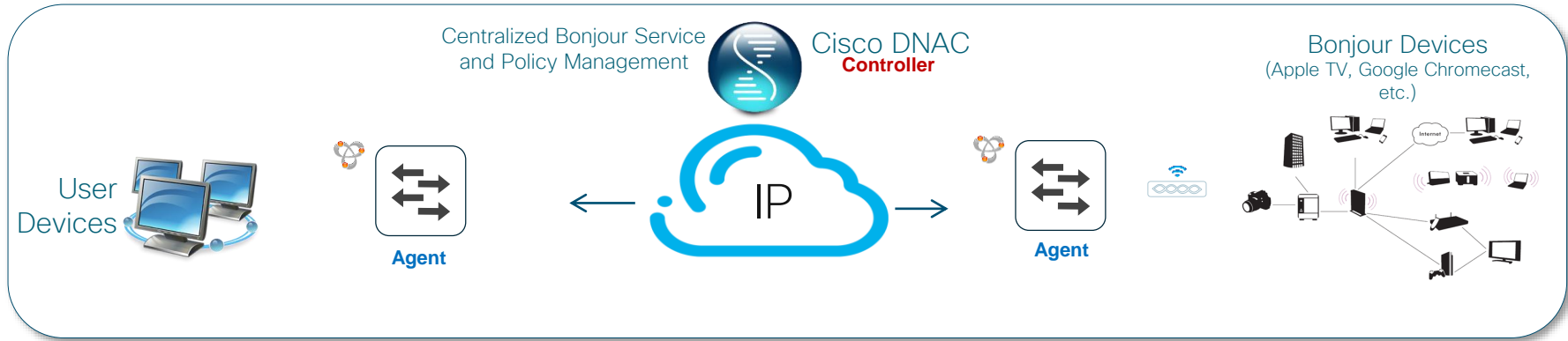




# Current Limitations for Service Discovery



# Bonjour Service Discovery Without Boundaries



## Traditional Bonjour



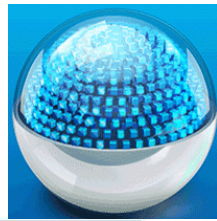
- Single Gateway solution, cannot scale across enterprise
- No access control
- Limited Management capabilities

## Cisco DNA Service for Bonjour



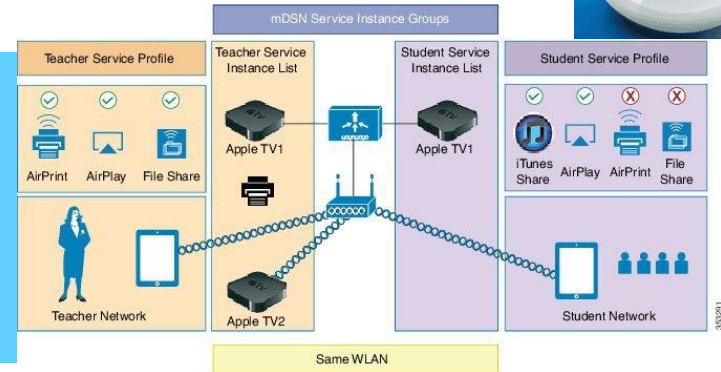
- **Enables** Discovery and service distribution across LAN and WLAN networks
- **Access Controlled**
- **Simplified** Intuitive Controller Based Management

# Bonjour with Prime Infrastructure



## Option 1: Manual mDNS config via CLI templates on WLC

- all manual work
- only on WLC
- only local Area Network



## Option 2: Manual Service Discovery Gateway config via CLI templates on WLC

- all manual work
- WLC & Switches & ISR
- Limited support of IOS-XE



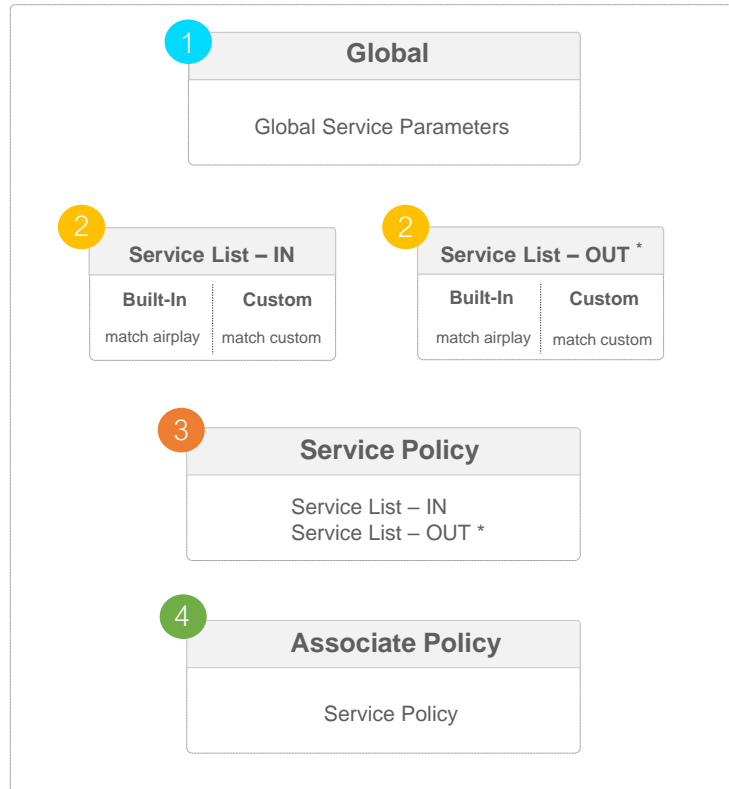


Demo, Bonjour

# Agent – Local Area Bonjour Policy (CLI)



## Local Area Bonjour Policy – LAN and WLAN



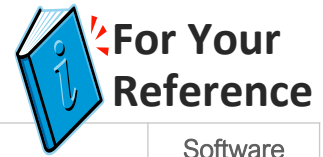
```
!  
Agent(config)# mdns-sd gateway  
!
```

```
!  
Agent(config)# mdns-sd service-list <NAME> < IN | OUT >  
Agent(config-mdns-sl-in)# match airplay  
!
```

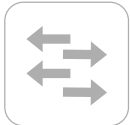
```
!  
Agent(config)# mdns-sd service-policy <NAME>  
Agent(config-mdns-sl-in)# service-list <NAME> < IN | OUT >  
!
```

```
!  
Agent(config)# interface Vlan <ID>  
Agent(config-if)# mdns-sd gateway  
Agent(config-if-mdns-sd)# service-policy <NAME>  
!
```

# SD-Access Network Product Matrix



Cisco  
DNA-Center



Catalyst



WLC \*

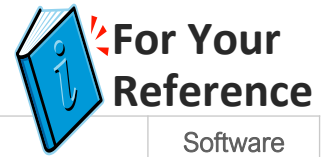
Supported Controller	Hardware	Software
Cisco DNA-Center	DN2-HW-APL-L and DN2-HW-APL-L DN2-HW-APL-XL	v1.3.1.0

Supported SDG Agent	Local Area SDG	Wide Area SDG	Software
Catalyst 9200	DNA Essentials	⊗	17.1.1 *
Catalyst 9300	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9400	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9500 / 9500-H	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9600	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9800 WLC	DNA Essentials	DNA Advantage	Pass-Thru
Cisco 5520/8540 WLC	DNA Essentials	DNA Advantage	Pass-Thru
Catalyst Embedded WLC	DNA Essentials	DNA Advantage	16.11.1

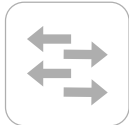
\* Roadmap



# Traditional Network Product Matrix



Cisco  
DNA-Center



Catalyst



ISR



WLC \*

\* Pass-Thru

**CISCO** *Live!*

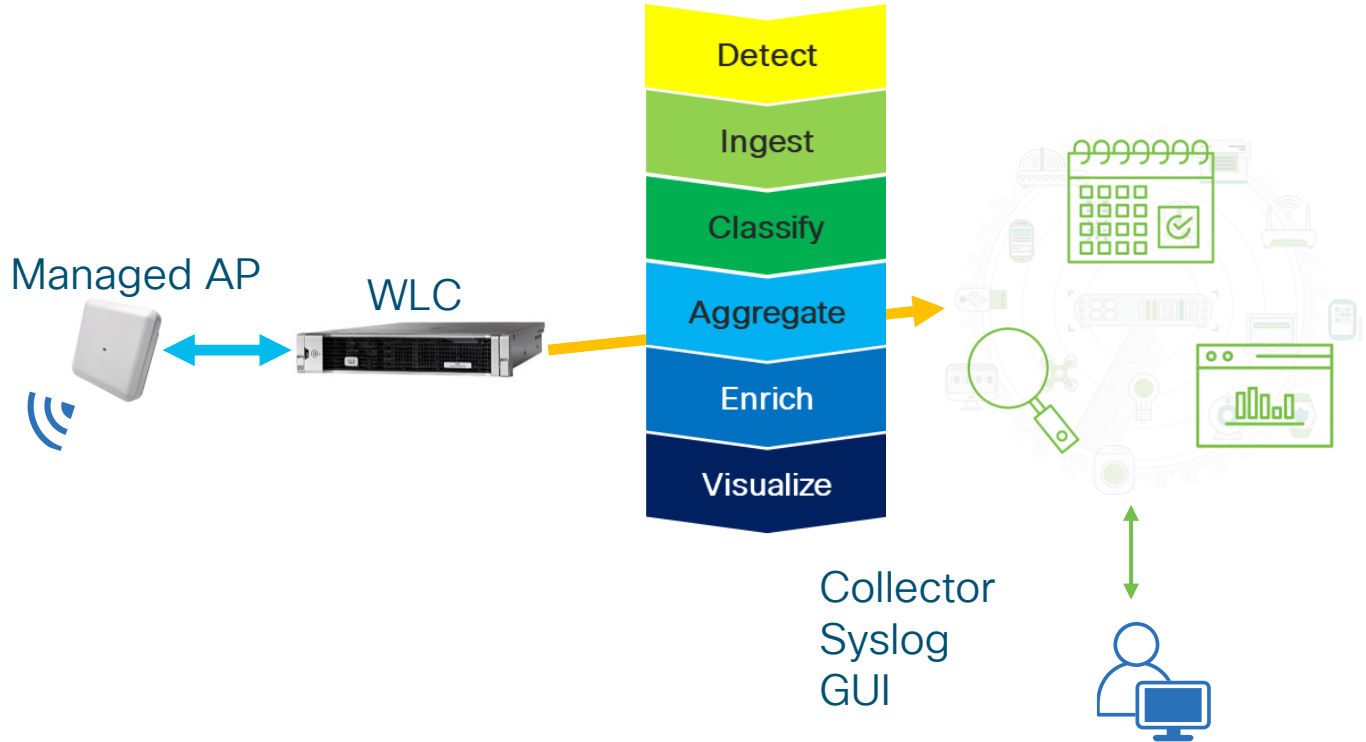
Supported Controller	Hardware	Software
Cisco DNA-Center	DN2-HW-APL-L and DN2-HW-APL-L DN2-HW-APL-XL	v1.3.1.0

Supported SDG Agent	Local Area SDG	Wide Area SDG	Software
Catalyst 9000 (C9300-C9600)	DNA Essentials	DNA Advantage	16.11.1
Catalyst 9200	DNA Essentials	⊗	17.1.1
Catalyst 9200L	⊗	⊗	Pass-Thru
Catalyst 9800 WLC	DNA Essentials	⊗	Pass-Thru
Cisco 5520/8540 WLC	⊗	⊗	Pass-Thru
Catalyst 6800	IP Base	Adv Ent + DNA-Addon	15.5(1)SY4
Catalyst 4500E/X	IP Base	IP Services + DNA-Addon	3.11.0
Catalyst 3850/3650	DNA Essentials	DNA Advantage	16.11.1
Catalyst 2960 X	LAN Base	⊗	15.2.6E2
Catalyst 2960 XR	IPLite	⊗	15.2.6E2
Cisco ISR 4000 Series	IPBase	AppX	16.11.1



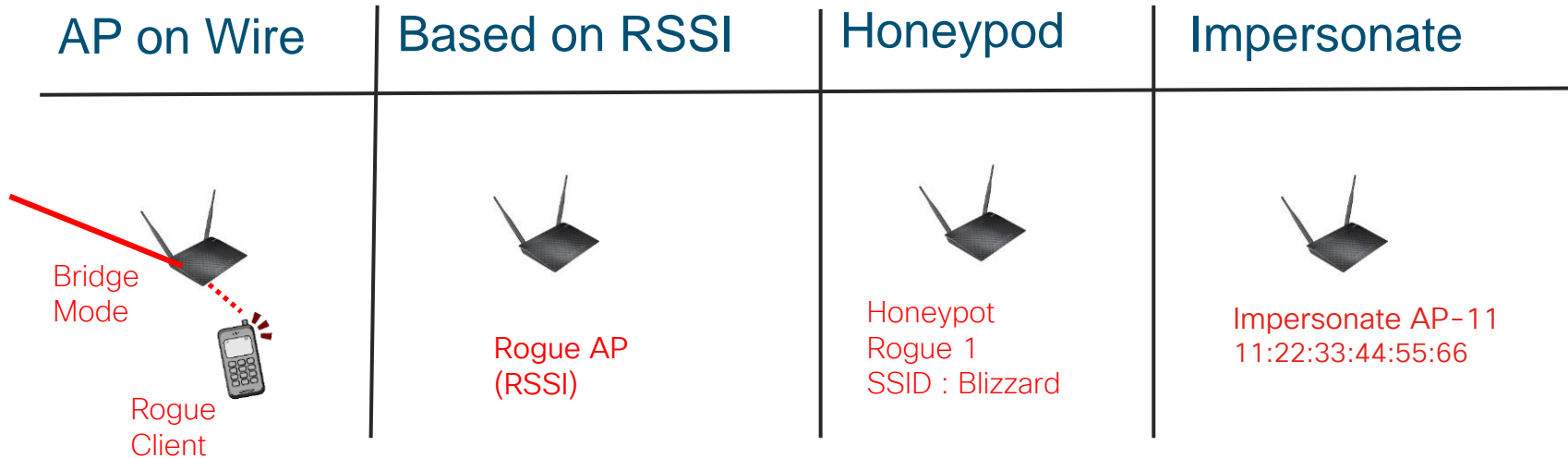
# Cisco DNA Center Rogue Management

# Rogue analytics - overview



# Rogue Classification

A **rogue access point** is a wireless **access point** that has been installed on a secure network, by well-meaning employee or by a malicious attacker.

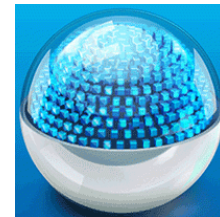


Informational

Potential

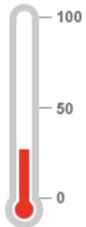
High

# Rogue with Prime Infrastructure



Security Index

Score: 27.12%



### Top Security Issues

[View All](#) | [Devices](#)

- WLAN interface is set to 'management' interface (3)
- Rogue policy to detect and report adhoc networks is disabled on the controller (2)
- 'MFP Client Protection' is set to 'Optional' for WLAN (2)
- "MFP Client Protection" is set to "Disabled" for WLAN (1)
- No user authentication configured for WLAN (1)

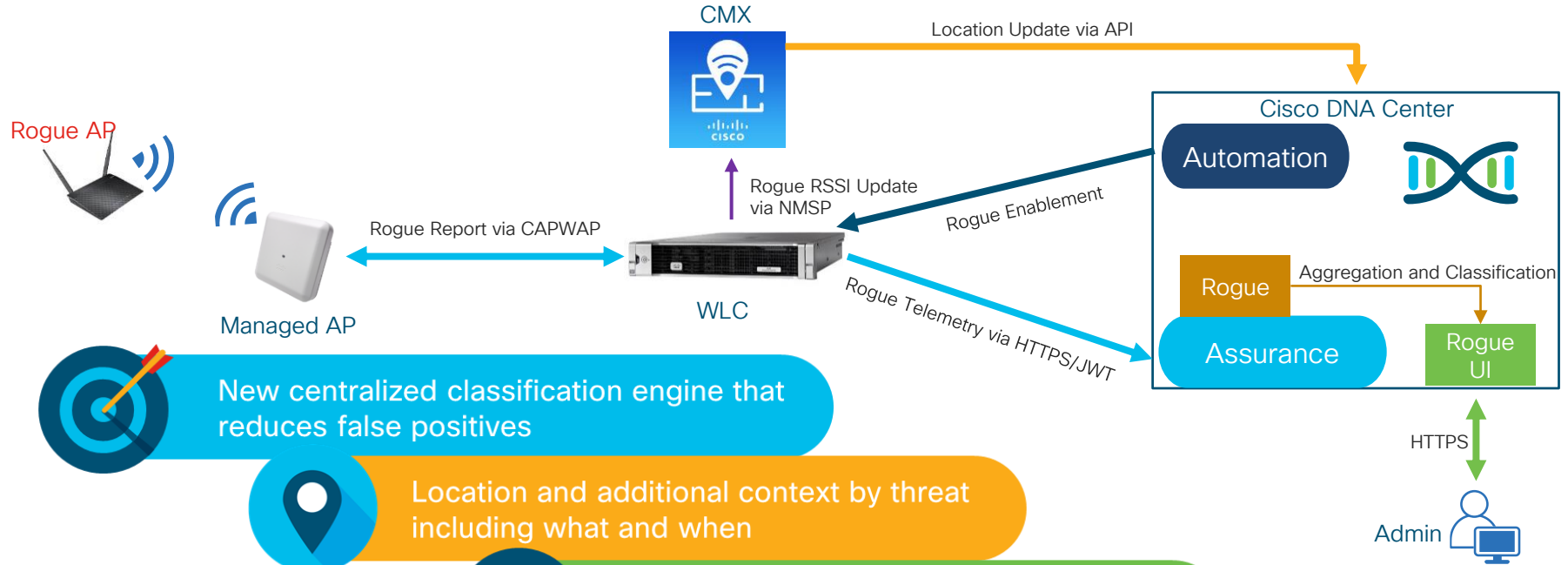
Prime Infrastructure consolidates all of the controllers rogue access point data


Searched By - Category : Rogue AP & Classification Type : Unclassified - [Reset](#)


Rogue Classification


<input type="checkbox"/>	Severity	Rogue MAC ...	Vendor	Classifica...	Radio T...	Strongest ...	No. Of Rogue...	Owner	Timestamp	State	SSID	AP Loc...	Status
<input type="checkbox"/>	Minor	54:67:51:e9:e8...	Compal Br...	Unclassified		-38	0		January 3, 2020 3:32:38 PM...	Alert	UPC...	default I...	No
<input type="checkbox"/>	Minor	1c:24:cd:00:a5...	Askey Com...	Unclassified		-41	0		January 3, 2020 3:32:34 PM...	Alert	Pfaff...	default I...	No
<input type="checkbox"/>	Minor	32:10:b3:af:75...	Unknown	Unclassified	802.11n...	-55	0		January 3, 2020 3:32:12 PM...	Alert	DIR...	default I...	No
<input type="checkbox"/>	Minor	c0:25:06:fe:1f:82	AVM GmbH	Unclassified		-60	0		January 3, 2020 3:28:47 PM...	Alert	FRIT...	default I...	No
<input type="checkbox"/>	Minor	70:3a:cb:76:bc...	Google, Inc.	Unclassified	802.11n...	-43	0		January 3, 2020 3:28:47 PM...	Alert	cape...	default I...	No


# Cisco DNAC - Rogue Management Architecture



 New centralized classification engine that reduces false positives

 Location and additional context by threat including what and when

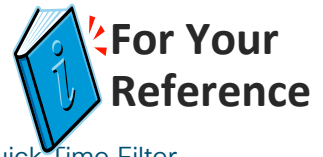
 Curated view to highlight most relevant data and reduce data overload

 Automate action based on Rogue Enablement



# Demo, Rogue

# Rogue Management Dashboard - Overview



For Your Reference

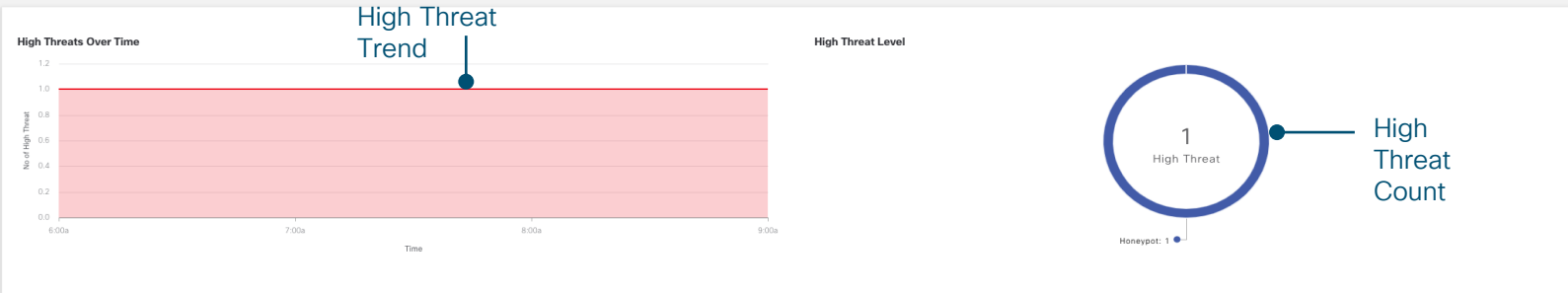
Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Quick Time Filter

## Rogue Management

Time Slider

Nov 7, 2019 9:25 AM Refresh Show Map Last 3 hours



Threats (132) All Threats

Filter

Threat Level	Rogue AP MAC address	Type	Connection	Detecting AP	Detecting AP Site	RSSI	SSID	Last Reported
High	00:2A:10:4C:EB:A0	Honeypot	Wireless	SJC04-F1-AP3	...SJC/SJC04/SJC04-AFP-1	-76	lightning	Nov 07, 2019 09:23 am
Potential	70:79:B3:AD:51:E0	Interferer	Wireless	SJC04-F1-AP2	...SJC/SJC04/SJC04-AFP-1	-58	AS-B1-WLC-3504	Nov 07, 2019 09:23 am
Potential	08:4F:F9:2E:E0:AE	Interferer	Wireless	SJC04-F1-AP3	...SJC/SJC04/SJC04-AFP-1	-36	@CorpSSID	Nov 07, 2019 09:23 am
Potential	08:4F:F9:2F:25:6F	Interferer	Wireless	SJC04-F1-AP1	...SJC/SJC04/SJC04-AFP-1	-51	@CorpSSID_98	Nov 07, 2019 09:23 am



# High Threat - Honeypot Rogue



Threats (108)

Honeypot High Threat

Filter

Threat Level	Rogue AP MAC address	Type	Connection	Detecting AP	Detecting AP Site	RSSI	SSID	Last Reported
High	B0:26:80:D5:03:A0	Honeypot	Wireless	SJ-AP2	Global	-29	lightning	Apr 24, 2019 01:34 pm
High	00:F6:63:14:1D:A0	Honeypot	Wireless	SJ-AP2	Global	-56	lightning	Apr 24, 2019 01:34 pm
Potential	F4:DB:E6:46:28:E0	Interferer	Wireless	SJ-AP2	Global	-57	CiscoAirProvision	Apr 24, 2019 01:34 pm
Potential	EC:BD:1D:AB:0E:50	Interferer	Wireless	SJ-AP3	Global	-46	CiscoLive	Apr 24, 2019 01:34 pm
Potential	38:0E:4D:BB:81:90	Interferer	Wireless	SJ-AP1	Global	-53	Jerry01	Apr 24, 2019 01:34 pm
Potential	EC:BD:1D:B1:DF:B0	Interferer	Wireless	SJ-AP2	Global	-34	MySsid001	Apr 24, 2019 01:34 pm
Potential	EC:C8:82:FB:32:A0	Interferer	Wireless	SJ-AP1	Global	-32	LA-Flex	Apr 24, 2019 01:34 pm
Potential	00:5D:73:9C:91:40	Interferer	Wireless	SJ-AP3	Global	-51	DNAC-WLC-02-SSID	Apr 24, 2019 01:34 pm
Potential	70:F3:5A:80:E3:80	Interferer	Wireless	SJ-AP1	Global	-43	MFG-5GTEST	Apr 24, 2019 01:34 pm

Show 100 entries

Showing 1 - 100 of 108

Previous 1 2 Next



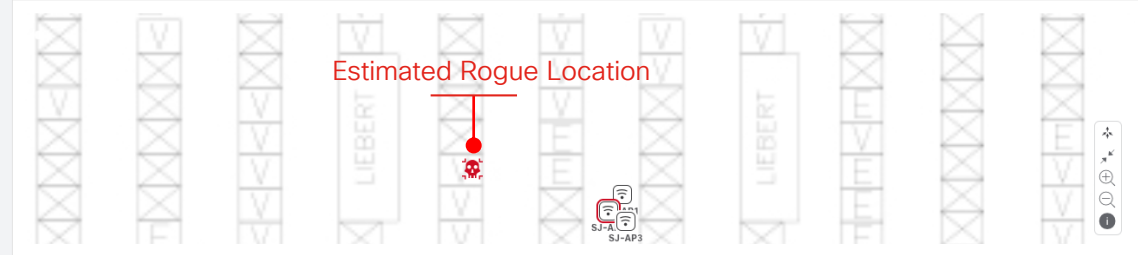
# High Threat – Honeypot 360 View



Threat 360: Mac 00:F6:63:14:1D:A0

Threat Level	Threat Type	Status	Rogue Vendor	Last Reported
High	Honeypot	Active	Cisco Systems, Inc	Apr 24, 2019 04:49 pm

Location: ...San Jose/SJC04/Floor1 [Full Screen](#)



Without CMX, the estimated rogue location is shown based on the detecting AP with strongest RSSI only.

Detecting Access Points (4) Clients (0)

Detecting Access Points (4) [Export](#)

Filter

Detecting AP	AP Domain	Rogue SSID	RSSI	Channels	Radio Type	SNR	State	Last Updated
SJ-AP2	...San Jose/SJC04/Floor1	lightning	-54	11	802.11n (2,4)	26	Active	Apr 24, 2019 04:49 pm
SJ-AP3	...San Jose/SJC04/Floor1	lightning	-60	132	802.11ac	35	Active	Apr 24, 2019 04:44 pm
SJ-AP1	...San Jose/SJC04/Floor1	lightning	-61	132	802.11ac	30	Active	Apr 24, 2019 04:44 pm

Detecting AP with strongest RSSI



# Agenda

- 1 Introduction
2. Change in Paradigm in Network Management
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A



# What is Assurance ?

The guarantee that the infrastructure is doing what you intended it to do



## Continuous Verification

Monitor and alert on operational impact to network after every Configuration Changes

Successful Rollouts, Operational Continuity



## Insights & Visibility

Visibility, Context, Historical Insights, Prediction

Minimize Downtime, User Productivity



## Corrective Actions

Guided Remediation, Automated Updates, System optimization

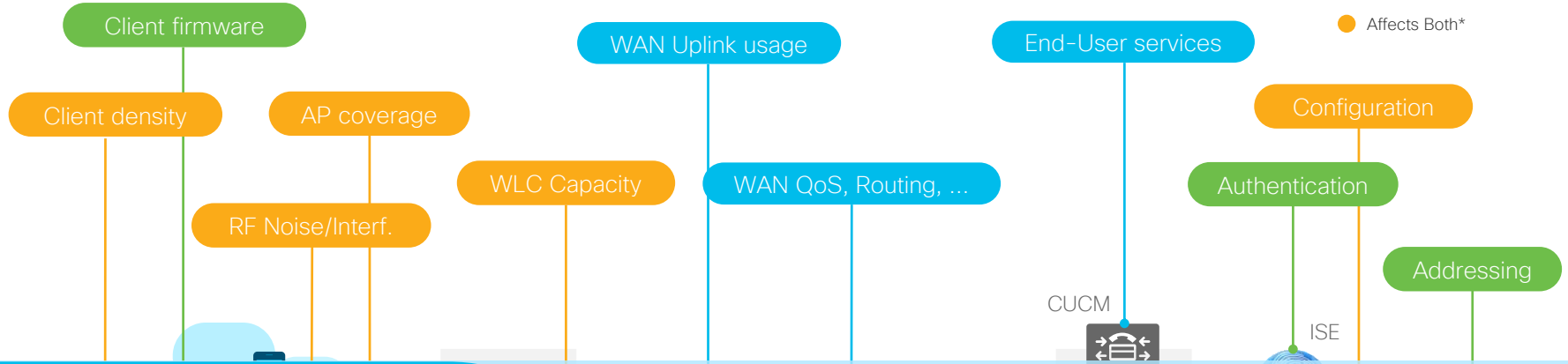
IT Productivity

# Network Quality is a Complex, End-to-End Problem

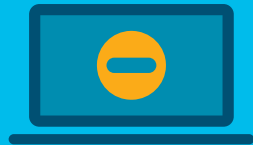


43% of IT Time spent in Troubleshooting

- Affects Join/Roam
- Affects Quality/Throughput
- Affects Both\*



There are 100+ points of failure between user and app



What is the problem?



Where is the problem?

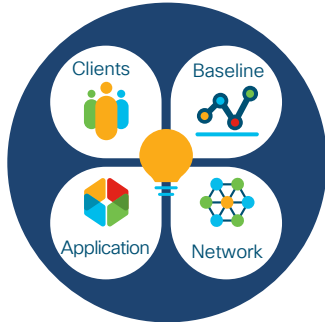
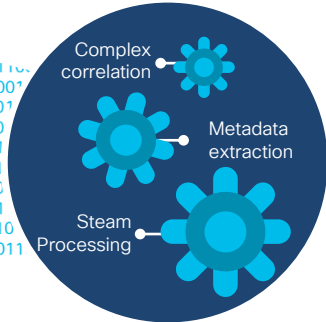
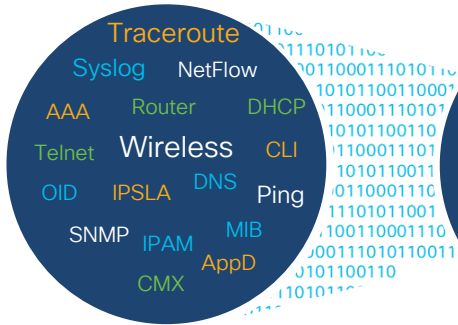


How can I fix the problem fast?

\* Both Join/Roam and quality/throughput

# Cisco DNA Assurance

From network data to business insights

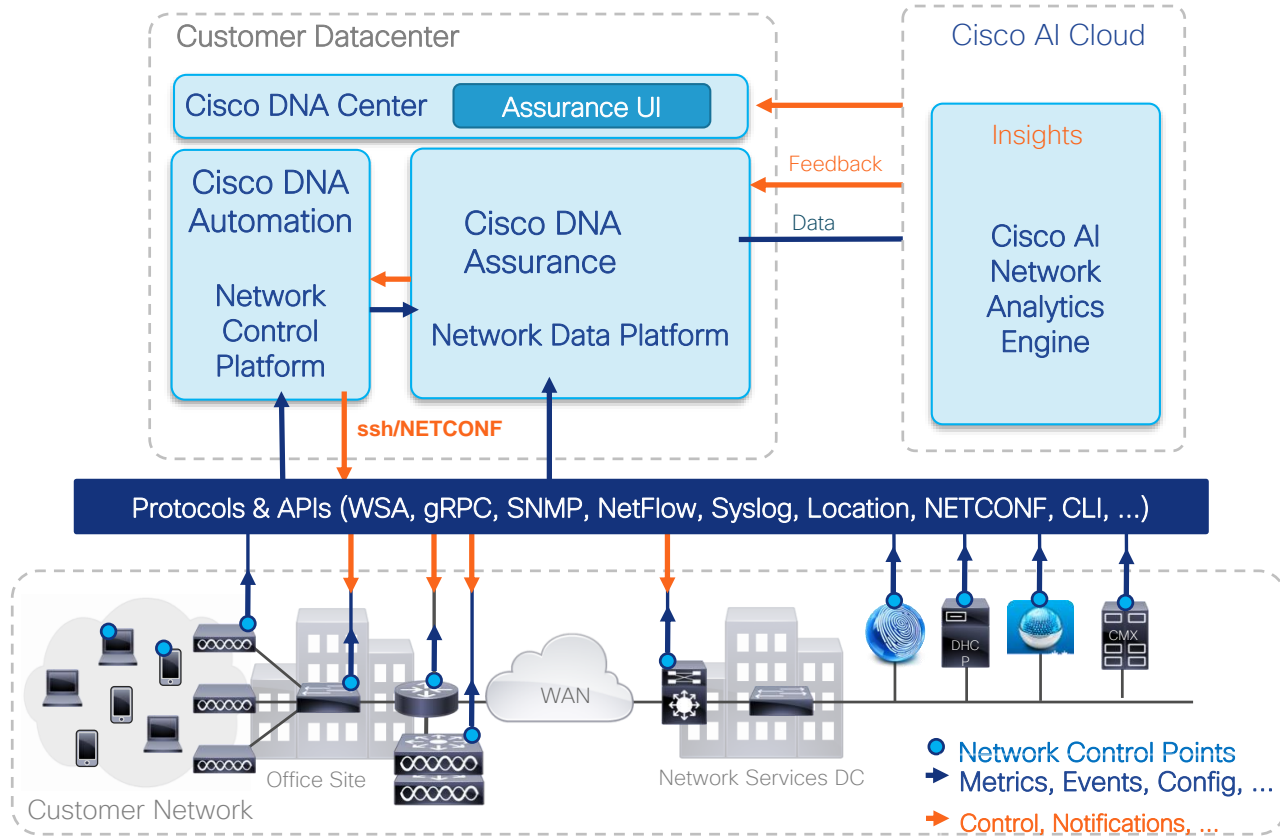


Everything as a sensor

Over 150 actionable insights  
Clients | Applications | Wireless | Switching | Routing



# Cisco DNA Assurance Architecture



# Client / Network / Application 360 views





Demo, 360 Views

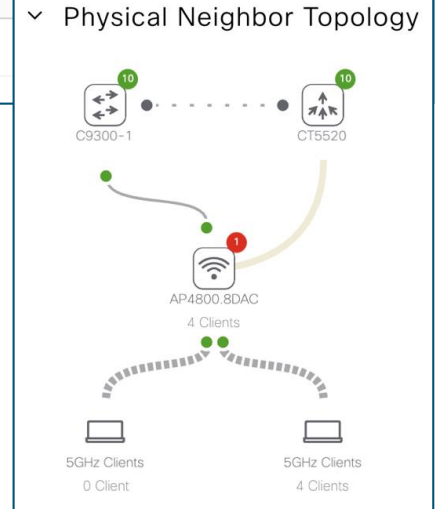
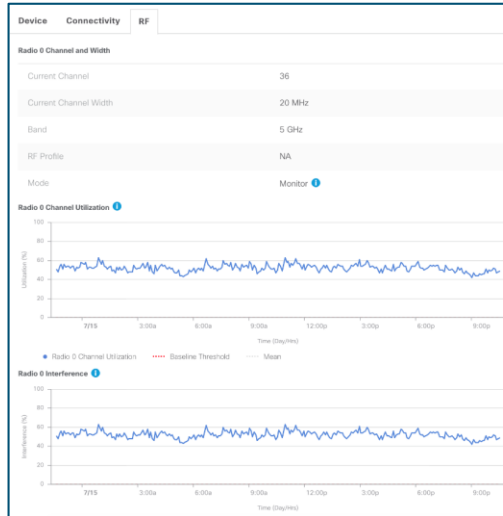
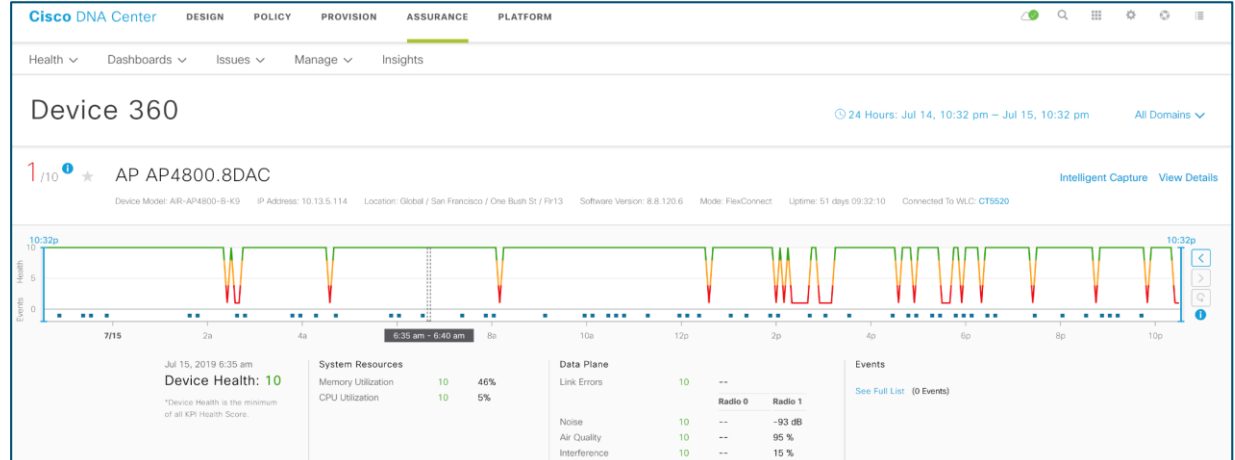


# 360° Visibility – Network Device

Network device Health history, Proactively identify any Issues

Detailed Device health information

Physical Neighbor Topology



# 360° Visibility-Client Device

Network Client Health history, Proactively identify any Issues

Detailed Client health information

Client Onboarding Details

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Health Dashboards Issues Manage Insights

## Client 360

24 Hours: Jul 14, 10:43 pm - Jul 15, 10:43 pm All Domains Intelligent Capture

7/10 User4

Device: Android-Motorola OS: android-dhcp-7.1.1 MAC: 7C:46:85:20:7B:27 IPv4: 10.13.4.186 IPv6: fe80::7e46:85ff:fe20:7b27 VLAN ID: 140 Status: Connected Last seen: Jul 15, 2019 10:42:00 pm Connected Network Device: AP4800.922C

SSID: @CorpSSID Last Known Location: San Francisco/One Bush St/Fir13

Issues Onboarding Event Viewer Path Trace Application Experience Detail Information

Issues (3)

- Onboarding P3 Wireless client failed to connect (SSID: @CorpSSID, AP: AP4800.606E, Band: 2.4 GHz, Site: Global/San Francisco/One Bush St/Fir13) - Failed to authenticate due to Client Timeout Jul 15, 2019 8:10 pm Instance Count: 13
- Onboarding P3 Wireless client failed to connect (SSID: @CorpSSID, AP: AP4800.922C, Band: 2.4 GHz, WLC: CT5520) - AAA Server Rejected Client Jul 15, 2019 7:07 pm Instance Count: 2
- Onboarding P3 Wireless client failed to roam (SSID: @CorpSSID, AP: AP4800.606E, Band: 2.4 GHz, WLC: CT5520) - AAA Server Rejected Client Jul 15, 2019 4:44 pm Instance Count: 1

### Detail Information Jul 15, 2019 10:43 pm

Device Info Connectivity RF

#### Information

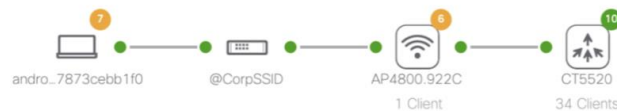
User Name	User4
Host Name	android-2ccc07873cebb1f0
MAC Address	7C:46:85:20:7B:27
IPv4 Address	10.13.4.186
IPv6 Address	fe80::7e46:85ff:fe20:7b27

#### Connection Information

Band	2.4 GHz
Spatial Streams	0
Channel Width	20 MHz
WMM	Supported
U-APSD	Disabled

### Onboarding Jul 15, 2019 10:43 PM

✓ AAA ✓ DHCP



# Application Experience

Client level Application usage visibility per Business relevance category

Per-Application Health Score along with historical trending

Detailed Application level flow metrics – Throughput, Packet loss, Latency, Delay

Application Experience Jan 25, 2018 1:14 pm [Refresh](#)

Business Relevant **Business Irrelevant** Default

Application (5) [Export](#)

[Filter](#) EQ Find

Name	Domain Name	Health		Destination	Average Throughput (Mbps)	Average Bandwidth Utilization (%)	Traffic Class	Packet Loss (%)		Latency (ms)		Application Delay (ms)	
		Most Recent	Last 24 Hours					Max	Average	Max	Average	Max	Average
All Applications				Multiple	2	2							
• cifs	--	1	<a href="#">View</a>	USA/Data Center	1	1	bulk-data	100	2	45944	2292	106	0
• ssh	--	2	<a href="#">View</a>	USA/Data Center	0.49	0.69	ops-admin-mgmt	100	8	184793	2350	3961	6
• cfbix-static	--	--		USA/Data Center	0.08	0.11	multimedia-streaming	0	0	0	0	0	0
• ntp	--	--		USA/Data Center	0	0	ops-admin-mgmt	0	0	0	0	0	0

Business Relevant **Business Irrelevant** Default

Application (3) [Export](#)

[Filter](#) EQ Find

Name	Domain Name	Health		Destination	Average Throughput (Mbps)	Average Bandwidth Utilization (%)	Traffic Class	Packet Loss (%)		Latency (ms)		Application Delay (ms)	
		Most Recent	Last 24 Hours					Max	Average	Max	Average	Max	Average
All Applications				Multiple	0.13	0.18							
• disney-web-portal	www.disney.com	7	<a href="#">View</a>	USA/Data Center	0.09	0.13	transactional-data	100	7	21325	585	6222	40
• espn-browsing	www.espn.com	4	<a href="#">View</a>	USA/Data Center	0.03	0.04	transactional-data	100	2	50363	1700	5761	45
• netflix	www.netflix.com:443	2	<a href="#">View</a>	USA/Data Center	0.01	0.01	multimedia-streaming	100	4	93552	1383	6618	93

# Application Assurance – Per App 360 View

## Application 360

Last 24 hours

10/10 ssh

Business Relevancy: business-relevant Traffic Class: ops-admin-mgmt Category: net-admin

HEALTH

10  
5  
0

10:00a 11:00a 12:00p 1:00p 2:00p 3:00p 4:00p 5:00p 6:00p 7:00p 8:00p 9:00p 10:00p 11:00p 4/21 1:00a 2:00a 3:00a 4:00a 5:00a 6:00a 7:00a

### Application Experience - unknown

Throughput and Bandwidth Utilization

Packet Loss

Latency

Application Delay

Apr 21, 2018 2:02 pm  
Throughput: 0.0145Mbps  
Utilization: 0.0015%

ssh - unknown

#### Clients (2)

Filter EQ Find

Health	Client	MAC Address	Usage	Location	OS
10	192.168.139.173	00:0C:2B:F4:F4:FC	534.74 KB	USA/DC	---
10	192.168.139.201	38:0E:4D:9C:4A:58	1.11 GB	---	---

### Application Experience

Apr 21, 2018 9:39 am Refresh

Filter Export EQ Find

Source Location	Health		Usage	Average Throughput	Average Bandwidth Utilization (%)	DSCP		Packet Loss (%)		Latency		Application De	
	Most Recent	Last 24 Hours				Marking	Preservation	Max	Average	Max	Average	Max	Aver:
USA	4	View	1.8 KB	13 bps	0	CS2	No	100	66	1 ms	0 ms	0 ms	0 ms
unknown	7	View	1.13 GB	20.45 Kbps	0	CS2	No	50	0.91	32 ms	2 ms	999 ms	14 ms

- Application Performance over last 24 hrs
- List of clients who used the App in the given timeframe



# CISCO *Live!* IS LIKE A BOX OF CHOCOLATES



Chocolate  
Break

# Setup Telemetry from Infrastructure to DNA-Center

# Telemetry Configuration

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes 'Cisco DNA Center' and tabs for 'DESIGN', 'POLICY', 'PROVISION', 'ASSURANCE', and 'PLATFORM'. Below this, there are sub-tabs for 'Network Hierarchy', 'Network Settings', 'Image Repository', 'Network Profiles', and 'Authentication Template'. The 'Network Settings' tab is active, and the 'Network' sub-tab is selected. The main content area is titled 'Setup network properties like AAA, NTP, Syslog, Trap and Netflow using the "Add Servers" link. deploy using these settings.' It contains three sections: 'Primary' with an IP address field set to '111.2.2.2' and a note 'Supports both IPv4 and IPv6'; 'SYSLOG Server' with a checked checkbox 'Cisco DNA Center as syslog server' and an 'IP Address' field; and 'SNMP Server' with a checked checkbox 'Cisco DNA Center as snmp server' and an 'IP Address' field. A blue arrow points from the 'SNMP Server' section to a callout box that reads: 'The IP address set here is the destination server for SNMP traps and messages from network devices'. The left sidebar shows a hierarchy starting with 'Global' and sub-items for 'Canada', 'Mexico', 'Netherlands', and 'USA'.

- ❑ Telemetry Configuration
  - SYSLOG Server
  - SNMP Trap Server
  - SNMP Polling
- ❑ Cisco DNA Center is configured as Syslog and SNMP Trap Server by default
- ❑ Telemetry Configuration is pushed while assigning devices to sites
- ❑ Usage of Network Telemetry App is not mandatory and used only to create custom telemetry profile

# Network Telemetry App

The screenshot shows the Cisco DNA Center interface for the Network Telemetry App. The top navigation bar includes 'Cisco DNA Center', 'Network Telemetry', and a yellow button labeled 'Network Telemetry App from Tools'. The main content area is titled 'Network Telemetry Assessment' and has tabs for 'Site View' and 'Profile View'. A blue 'Add Profile' button is visible on the right side of the interface, with a large blue arrow pointing downwards from it. A dark blue text box is overlaid on the center of the screen, containing the following text:

DNA-Center 1.3.1 and newer, for routers and switches when enabling "Maximal Visibility, Netflow/AVC is only enabled for interfaces where the keyword "LAN" is part of the Description. Example : interface GigabitEthernet 0/0 Description This is my LAN interface

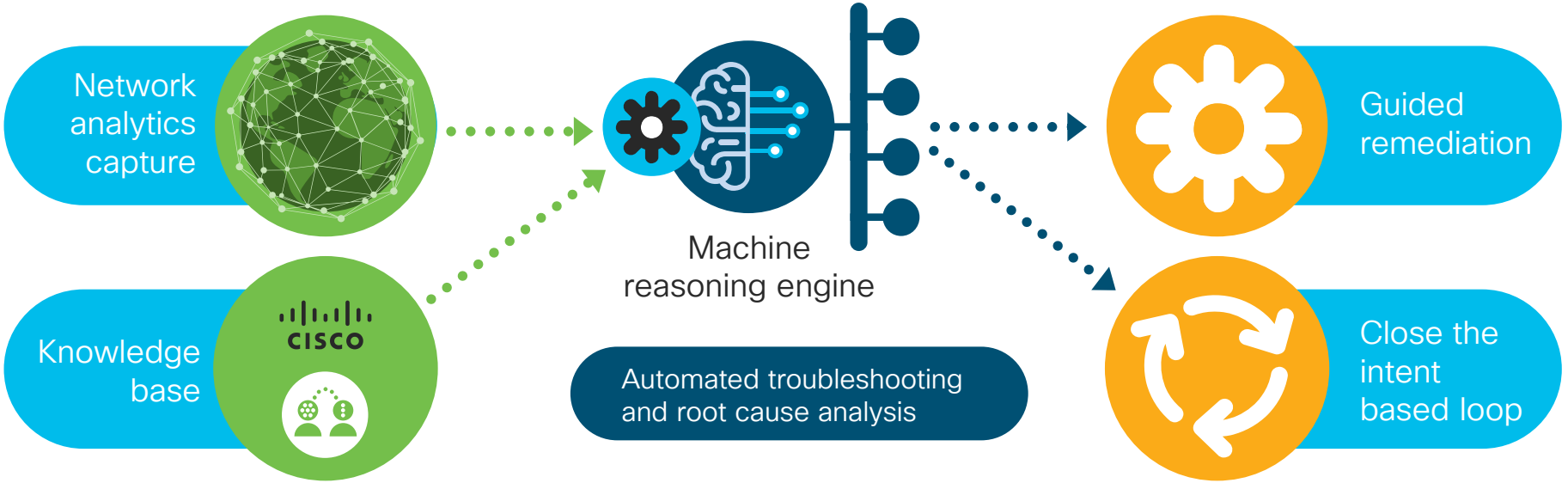
- Maximal Visibility
  - Syslog with severity level "Informational"
  - Application Visibility, NetFlow support on switches, routers and WLC
- Optimal Visibility
  - Syslog with severity level "Informational"
  - No Application Visibility
- Create Custom Telemetry Profile with different Syslog Severity Level if desired

The screenshot shows the 'Syslog Severity Levels' configuration dialog. The dialog has a yellow title bar and a 'Cancel' button. It contains two checked checkboxes: 'Syslog' and 'Application Visibility'. The 'Severity Level' is set to 'Informational', and a dropdown menu is open showing the following options: 'Informational', 'Errors', 'Warnings', 'Notifications', and 'Debugging'. A 'Save' button is located at the bottom right of the dialog.



# Cisco DNA Center AI / ML Network Analytics

# AI Network Analytics Architecture





# Use Case 1: Improve Incident Alert Fidelity

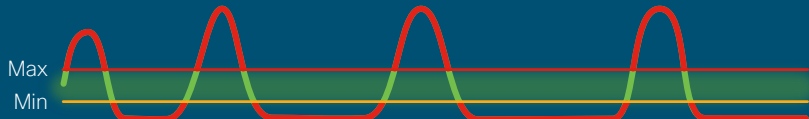
## Personalized Baseline



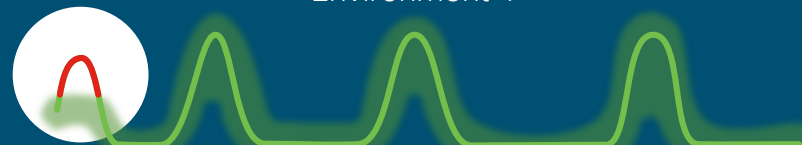
**Before:** Custom thresholds = Alert overload

**AI-driven:** Dynamic baselines = relevant anomalies

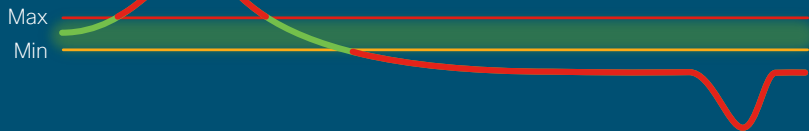
Environment 1



Environment 1



Environment 2



Environment 2



Environment 3



Environment 3



# Use Case 2: Proactive & Predictive Insights

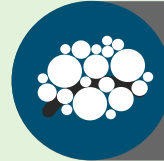
## Intelligent Analysis



Find Issues  
Before Users Do



Proactive Exploration



System Generated  
Insights



Peer-to-peer &  
Site-to-site Comparison



# Demo, AI Network Analytics

# Cisco DNA Center Security advisories

# Security Advisories Overview

The Cisco Product Security Incident Response Team (PSIRT) responds to Cisco product security incidents, regulates the Security Vulnerability Policy, and recommends Cisco Security Advisories and Alerts.

The Security Advisories tool uses these recommended advisories, scans the inventory within Cisco DNA Center, and finds the devices with known vulnerabilities.

ADVISORY	IMPACT	CVE	LAST UPDATED	VERSION
<a href="#">Cisco Data Center Network Manager Authentication Bypass Vulnerabilities</a>	Critical	CVE-2019-15975 CVE-2019-15976 ...	2020 Jan 02	1.2
<a href="#">Cisco Data Center Network Manager SQL Injection Vulnerabilities</a>	High	CVE-2019-15984 CVE-2019-15985	2020 Jan 02	1.0
<a href="#">Cisco Data Center Network Manager Path Traversal Vulnerabilities</a>	High	CVE-2019-15980 CVE-2019-15981 ...	2020 Jan 02	1.0
<a href="#">Cisco Data Center Network Manager Command Injection Vulnerabilities</a>	High	CVE-2019-15978 CVE-2019-15979	2020 Jan 02	1.0
<a href="#">Cisco Data Center Network Manager XML External Entity Read Access Vulnerability</a>	Medium	CVE-2019-15983	2020 Jan 02	1.0
<a href="#">Cisco Data Center Network Manager JBoss EAP Unauthorized</a>	Medium	CVE-2019-15980	2020 Jan 02	1.0

<https://tools.cisco.com/security/center/publicationListing.x>



# Security advisories with Prime Infrastructure



Updates with  
Maintenance  
Releases

Prime Infrastructure

🏠 Reports / Reports / PSIRT and EOX ★

[Schedule Job](#) [View Job Details](#) PAS

[Device PSIRT](#) [Device Hardware EOX](#) [Device Software EOX](#) [Module Hardware EOX](#) [Field Notice](#)

Device PSIRT CSV  Show

Device Name	Device Type	IP Address	OS Type	OS Version	PSIRT Title	Vulnerable	Match Reason	Caveat
berlab6880.cisco.com	Cisco Catalyst 68xx Virtual Switch	10.49.232.151	IOS	15.2(1)SY3	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab3750x-rack2.cisco.com	Cisco 3750 Stackable Switches	10.100.10.145	IOS	15.2(4)E4	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab3750-tg1	Cisco 3750 Stackable Switches	10.100.80.22	IOS	12.2(55)SE12	Cisco IOS and IOS XE Software Internet Key ...	Vulnerable	MATCH:OSTY...	Manual verifi...
berlab6880.cisco.com	Cisco Catalyst 68xx Virtual Switch	10.49.232.151	IOS	15.2(1)SY3	Multiple Cisco Products OSPF LSA Manipulati...	Vulnerable	MATCH:OSTY...	Mapping logi...
berlab3750x-rack2.cisco.com	Cisco 3750 Stackable Switches	10.100.10.145	IOS	15.2(4)E4	Multiple Cisco Products OSPF LSA Manipulati...	Vulnerable	MATCH:OSTY...	Mapping logi...
berlab3750-tg1	Cisco 3750 Stackable Switches	10.100.80.22	IOS	12.2(55)SE12	Cisco IOS and IOS XE Software Cluster Man...	Vulnerable	MATCH:OSTY...	Automation d...

# Security Advisories: Advisories View

## Tools area, click Security Advisories

Cisco DNA Center Security Advisories

Security Advisories Focus: [Advisories](#) Last scanned: Jan 3, 2020 4:54 PM [Scan](#)

Advisories (84)

[Filter](#)

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	13	128	08/29/2019
<a href="#">cisco-sa-20180328-smi2</a>	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2018-0171	6	646	05/04/2018
<a href="#">cisco-sa-20170317-cmp</a>	Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2017-3881	2	1022	04/18/2019
<a href="#">cisco-sa-20180328-xesc</a>	Cisco IOS XE Software Static Credential Vulnerability	9.8	● CRITICAL	CVE-2018-0150	12	646	09/20/2018
<a href="#">cisco-sa-20180328-qos</a>	Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2018-0151	5	646	04/28/2018
<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	2	576	06/08/2018
<a href="#">cisco-sa-20180328-ldp</a>	Cisco IOS, IOS XE, and IOS XR Software Link Layer Discovery Protocol Buffer Overflow Vulnerabilities	8.8	● HIGH	CVE-2018-0175,CVE-2018-0167	3	646	05/02/2018
<a href="#">cisco-sa-20190612-iosxe-csrf</a>	Cisco IOS XE Software Web UI Cross-Site Request Forgery Vulnerability	8.8	● HIGH	CVE-2019-1904	1	205	07/17/2019

# Security Advisories: Device view

Cisco DNA Center Security Advisories 🔍 ☰ ⚙️ 🔄 ☰

Security Advisories Focus: Devices ▾

EQ Find Hierarchy

- ▾ Global
  - Unassigned Devices
  - > 🌐 CANADA
  - > 🏠 Casa Central
  - > 🇺🇸 USA

Devices (28)

Filter | Tag Device

<input type="checkbox"/>	Device Name
<input type="checkbox"/>	TO-ASR1001X-1.corp.local
<input type="checkbox"/>	LA1-3850-CSW-2.corp.local
<input type="checkbox"/>	LA1-ASR1001X-1.corp.local
<input type="checkbox"/>	LA2-3850-ACC-1.corp.local
<input type="checkbox"/>	LA2-3850-CSW-3.corp.local
<input type="checkbox"/>	LA2-3850-ACC-2.corp.local
<input type="checkbox"/>	LA1-ASR1001X-2.corp.local
<input type="checkbox"/>	LA1-3850-CSW-1.corp.local

LA1-3850-CSW-2.corp.local (10.30.255.101) ✕

📶 Reachable 🕒 Uptime: 482 days 17 hours 32 minutes

[Run Commands](#) [View 360](#) Last updated: 4:55 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	128	08/29/2019	
<a href="#">cisco-sa-20180328-qos</a>	Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2018-0151	646	04/28/2018	
<a href="#">cisco-sa-20180328-xesc</a>	Cisco IOS XE Software Static Credential Vulnerability	9.8	● CRITICAL	CVE-2018-0150	646	09/20/2018	
<a href="#">cisco-sa-20180328-smi2</a>	Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability	9.8	● CRITICAL	CVE-2018-0171	646	05/04/2018	
<a href="#">cisco-sa-20180328-xepriv</a>	Cisco IOS XE Software Web UI Remote Access Privilege Escalation Vulnerability	8.8	● HIGH	CVE-2018-0152	646	03/29/2018	

# Security Advisories: Good to know

To use the Security Advisories tool, you must install the Machine Reasoning package

If you log in to Cisco DNA Center as an Observer, you cannot view the **Security Advisories** tool in the home page.

**AUTO UPDATE:** System Settings > Settings > Machine Reasoning.  
Click Import Latest from Cisco, or download the latest available Knowledge Base, and then Import from local. AUTO UPDATE toggle button to subscribe to the automatic update.

If you are launching the **Security Advisories** page for the first time, click **Scan**

**No Hardware EoX in Cisco DNAC**

**No Software EoX in Cisco DNAC**

# Cisco DNA Center Intelligent Capture

# Intelligent Capture overcomes the challenge of replicating Wireless issues

63%

Users assume the wireless network is the problem



Packet capture is a very difficult task over WiFi



Cross Stack Innovation  
AP HW, AireOS, DNAC



Dramatic simplification via single PCAP across multiple APs with zero packet loss during roaming

 **72-hours-**  
**to minutes**

Average Time to resolve user issues with Intelligent Capture



Live Client  
Onboarding State



Anomaly Triggered  
PCAPs



On-Demand  
RF Scanning



Real-time  
Client Location



On-Demand  
Wi-Fi App Analytics

# Real Time Wireless Client Troubleshooting

Start and Stop Full Packet Capture for AP4800

Real-Time Live Mode

Network Time Travel



Real-Time Client Event Viewer

Time	Duration
11:40:20 am	754,271 ms
11:40:08 am	2,511 ms
11:36:49 am	3,988 ms
11:37:23 am	
11:37:13 am	
11:36:53 am	
11:36:53 am	
11:36:49 am	
11:36:49 am	
11:27:05 am	5,093 ms
11:25:58 am	1,016 ms
11:14:34 am	601,172 ms
	2,467 ms
	1 ms
	0,596 ms

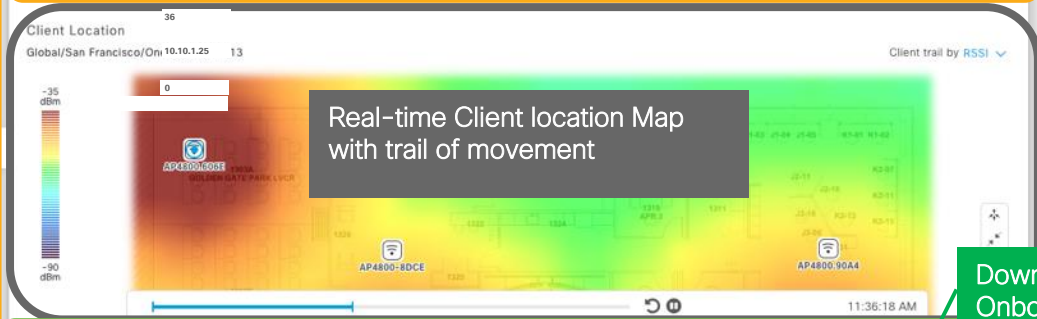
Session Duration

### KeyExchange

Jun 8, 2019, 11:36:53.278 am

Client android-a5d4f6cf958dafef failed to connect due to 4-way handshake timeout

AP MAC:	70:69:5A:51:3F:A0	AP Name:	AP4800.606E
Frequency(GHz):	2.4	WLC Name:	CT5520-MK
WLAN:	@CorpSSID_PSK	Radio:	0



Download Onboard Packet



# Real Time Spectrum Analyzers



- Persistent Fast Fourier Transform
- Swept Spectrogram
- Interferers with impacted BW
- Duty Cycle per Channel
- Available on WiFi5 and WiFi 6 APs
- Support Local/FlexConnect and Monitor mode AP



# Intelligent Capture Three Configuration Step



## Recommended Version

- DNAC 1.3.x
- AireOS 8.8.125/8.10
- IOS-XE 16.12.1s
- AP2800/3800/4800  
AP9120/9130

## Day-1 Config

1. Add WLC to DNAC  
(Discovery or Inventory)
2. (Optional) Hyperlocation
3. (Optional) Add CMX and  
vNAM to DNAC

Cisco DNAC automate all of necessary configs in WLC and AP

# Intelligent Capture Operation and Scale



Operation	Data Type	Concurrent Session
Global or per AP	Anomaly Packet Capture	All APs in the DNAC inventory
	Client RF stats (30 sec)	All Clients connected up to 1000 APs
	AP RF Stats	Up to 1000 APs
On-demand (Live mode) or Scheduled	Real Time Client RF stats (5sec)	Up to 16 Clients
	Real Time Client Onboarding Events from WLC (2sec. Interval)	
	OnBoard PCAP (Mgmt., DHCP/ICMP, EAP, etc.)	
On-Demand	Full Packet Capture	One Client Device
	Spectrogram View	Up to 20 APs

# Cisco DNA Center Wireless Sensor

# Wireless Sensor



1

## On-Boarding Tests

802.11 Association  
802.11 Authentication & Key Exchange  
IP Addressing DHCP (IPv4)



2

## Network tests

DNS (IPv4)  
RADIUS (IPv4)  
First Hop Router/Default gateway (IPv4)  
Intranet Host  
External Host (IPv4)

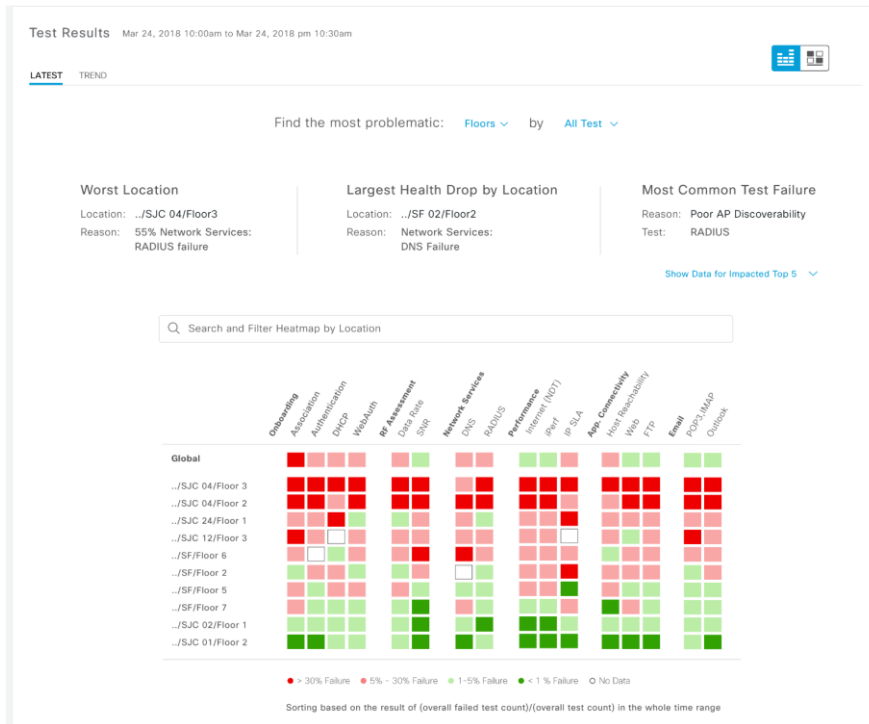


3

## Application tests

Email: POP3, IMAP, Outlook Web Access (IPv4)  
File Transfer: FTP (IPv4), iPerf Test  
Web: HTTP & HTTPS (IPv4)

# Wireless Sensor - Dashboard Heatmap



- Network Time Travel with Sensor Test Result
- Customizable Color grading threshold
- Insight View – Worst Location, Largest Health Drop by Location, Most Common Test Failure with reason code, expandable to top 5 on each category



# Demo, Wireless Sensor

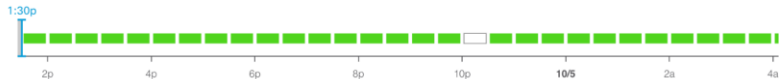
# Wireless Sensor 360

## Network Time Travel

Sensor Dashboard

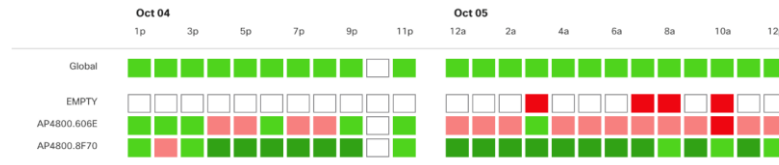
Sensor Sensor-0140

State: **RUNNING** Location: Global/San Francisco/SFO13/Floor13 Ethernet MAC: 70:f3:5a:78:01:40 Base Radio: 70:f3:5a:78:6b:6  
 IP Address: 10.13.5.122 Type: Cisco Aironet 1800S Active Sensor Sensor Uptime: Sep 28, 2019 12:08 pm Template: ST-SFO



## Target AP-based View

Test Type: All Tests



Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

## Performance Trend w/ comparison

Sensor Performance Trend

Test Type: Association



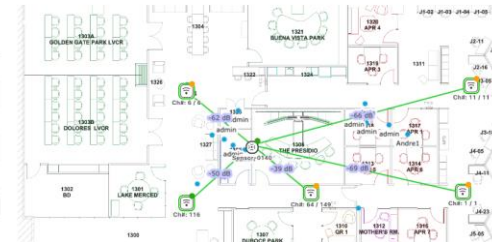
## Visual Neighbor AP Map

Neighbor APs

Band: 2.4 GHz (selected) 5 GHz

Neighbor APs	RSSI
AP4800.606E	-52 dBm
AP4800.8F70	-50 dBm
AP4800.90A4	-39 dBm
SJCAPIF-1.8D4C	-56 dBm
SJCAPIF-2.922C	-69 dBm

Showing 1 - 5 of 5



# Wireless Sensor – Guest Network

Guest Network Test  
Sensor extended Guest SSID  
Test to ISE and ClearPass

Enter SSID Credentials

Specify the SSID details necessary to run the Sensor test.

SSID: Blizz

WPA2 Enterprise

EAP Method: PEAP

User Name: userid@email

Password: \*\*\*\*\*

SSID: Alpha

WPA2 Enterprise

Password: \*\*\*\*\*

SSID: Guest

WPA2 Enterprise

WPA2 Personal

Open with ISE Guest Portal

### Enter ISE Guest Portal or Whitelist Details

ISE Guest Portal  Whitelist sensor Mac Address

Captive Portal Dection URL

Choose the labels that are same as your ISE Guest portals

Username  Passcode (Coupon)  Password

AUP(Acceptable use policy)

Cannot find the labels in above list?  
[Add Your Portal Labels](#)

Label Name	Tag
<input type="text"/>	<input type="text"/>

[Cancel](#) [Apply](#)

Assurance – Manage

Create SCEP Profile

Legacy Test **Setting**

Filter Actions

Profile Name	URL
<input type="checkbox"/> SCEP Profile	
<input checked="" type="checkbox"/> Profile1	cisc
<input checked="" type="checkbox"/> MyProfile	cisc
<input checked="" type="checkbox"/> Cutom8/22	cisc
<input type="checkbox"/> Instance_sdslid	cisc
<input checked="" type="checkbox"/> CAprofile	cisc
<input type="checkbox"/> Profile2	cisc
<input type="checkbox"/> Profile3	cisc
<input type="checkbox"/> 95111profile	cisc
<input type="checkbox"/> Profile4	cisc
<input type="checkbox"/> Profile5	cisc

### Enroll using SCEP

SCEP Profile Name: Profile 1

Content:

URL\*: XXXXXXXXX

State: CA

Locality: XXXXXXXXX

Organization Unit: XXXXXXXXX

Server certificate finge: XXXXXXXXX

Select SCEP Profile

SCEP Profile 1

SCEP Profile 2

Username

Common Name (CN)  Serial Number  Custom

Password

Common Password  One-Time Password  No Password

Password\*

[Manage Your SCEP Profile](#)

Enterprise-grade EAP-TLS provisioning solution  
SCEP (Simple Certificate Enrollment Protocol) Support

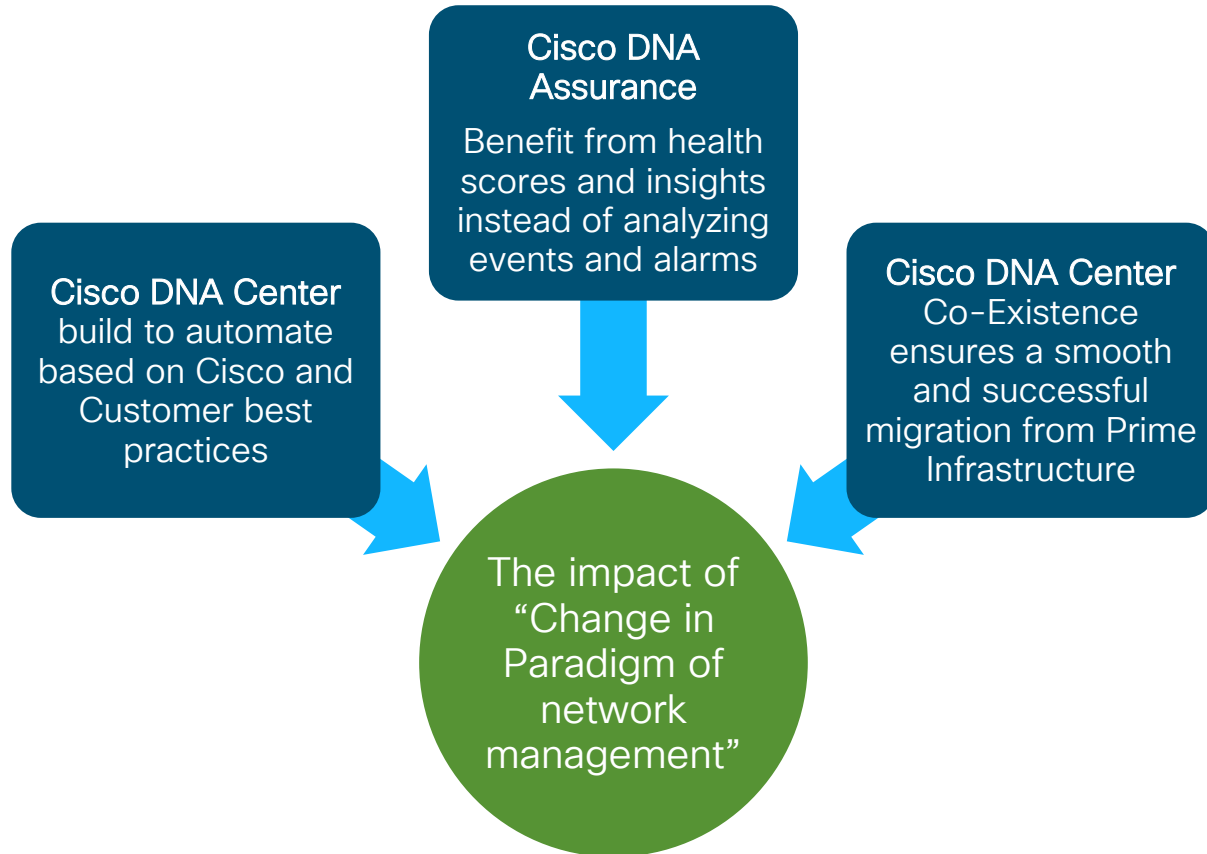
**cisco** *Live!*



# Agenda

- 1 Introduction
2. Change in Paradigm in Network Management
3. Automation with Cisco DNA-Center
4. Assurance with Cisco DNA-Center
5. Key takeaways & Q&A

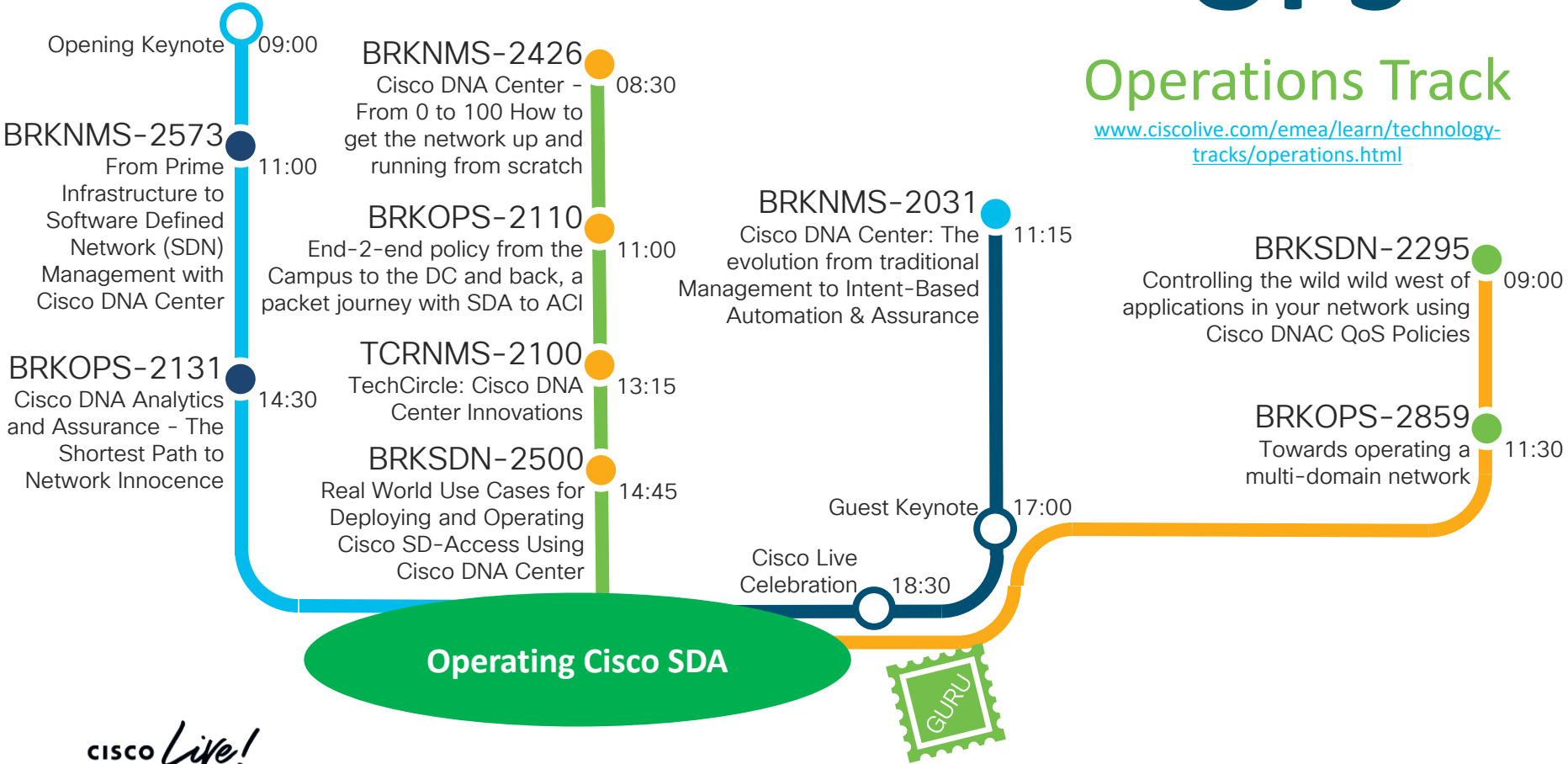
# Key takeaways



# OPS

## Operations Track

[www.ciscolive.com/emea/learn/technology-tracks/operations.html](http://www.ciscolive.com/emea/learn/technology-tracks/operations.html)



Mission statement : Get all the  
benefits of Cisco DNA-Center  
with Co-Existence to Prime  
Infrastructure

Q & A

# 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 campus



Walk-in labs



Meet the engineer  
1:1 meetings



Related sessions



Thank you





You make **possible**