You make **possible**

Onboarding Cisco DNA Center

With Automation Use Cases

Ehsan Lesani & Rahul Gupta, CSS

BRKCRS-2637

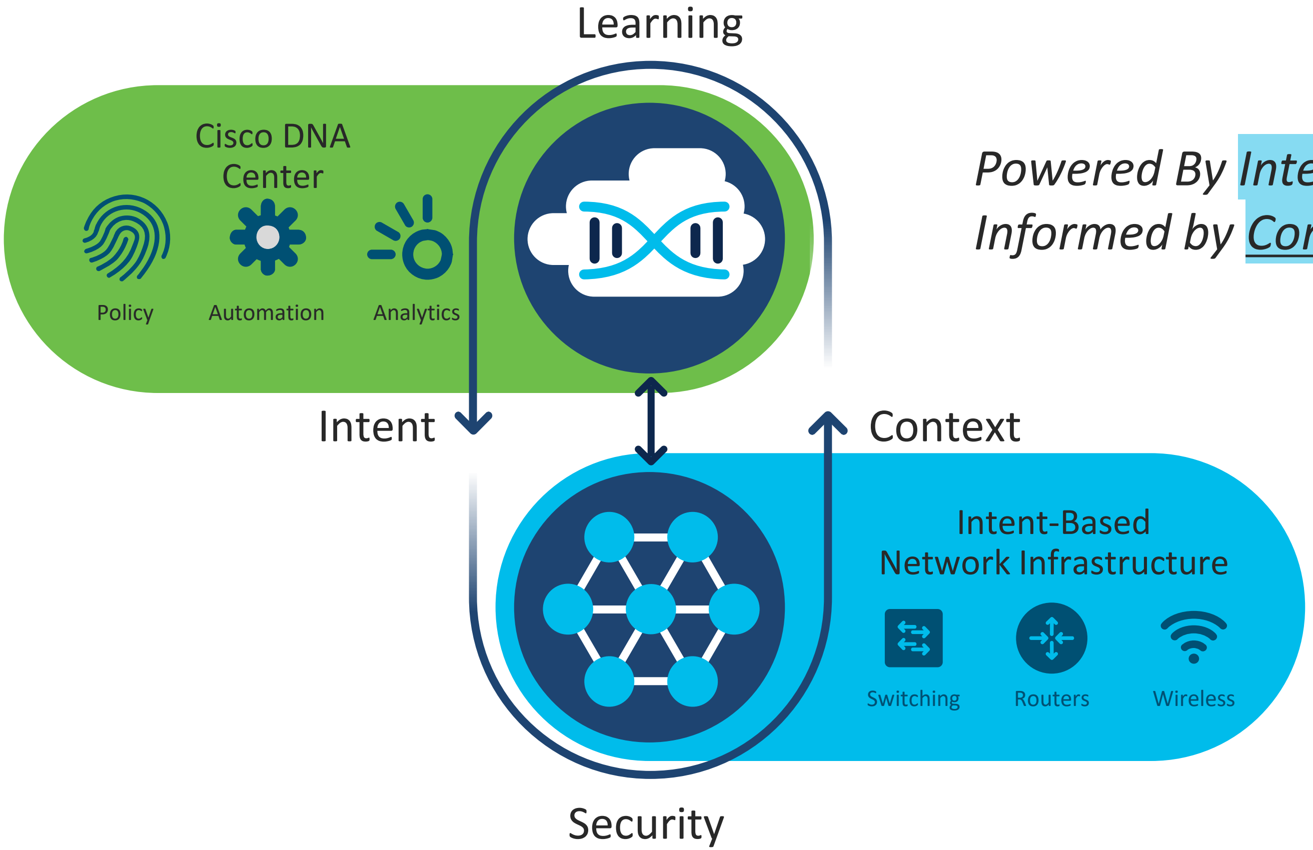
Agenda

- Introduction
- Base Automation
  - Design Hierarchy and Credentials, Discovery, Collectors, Telemetry Profiles
- Software Image Management
- Templates
- Plug and Play

What is Cisco DNA Center

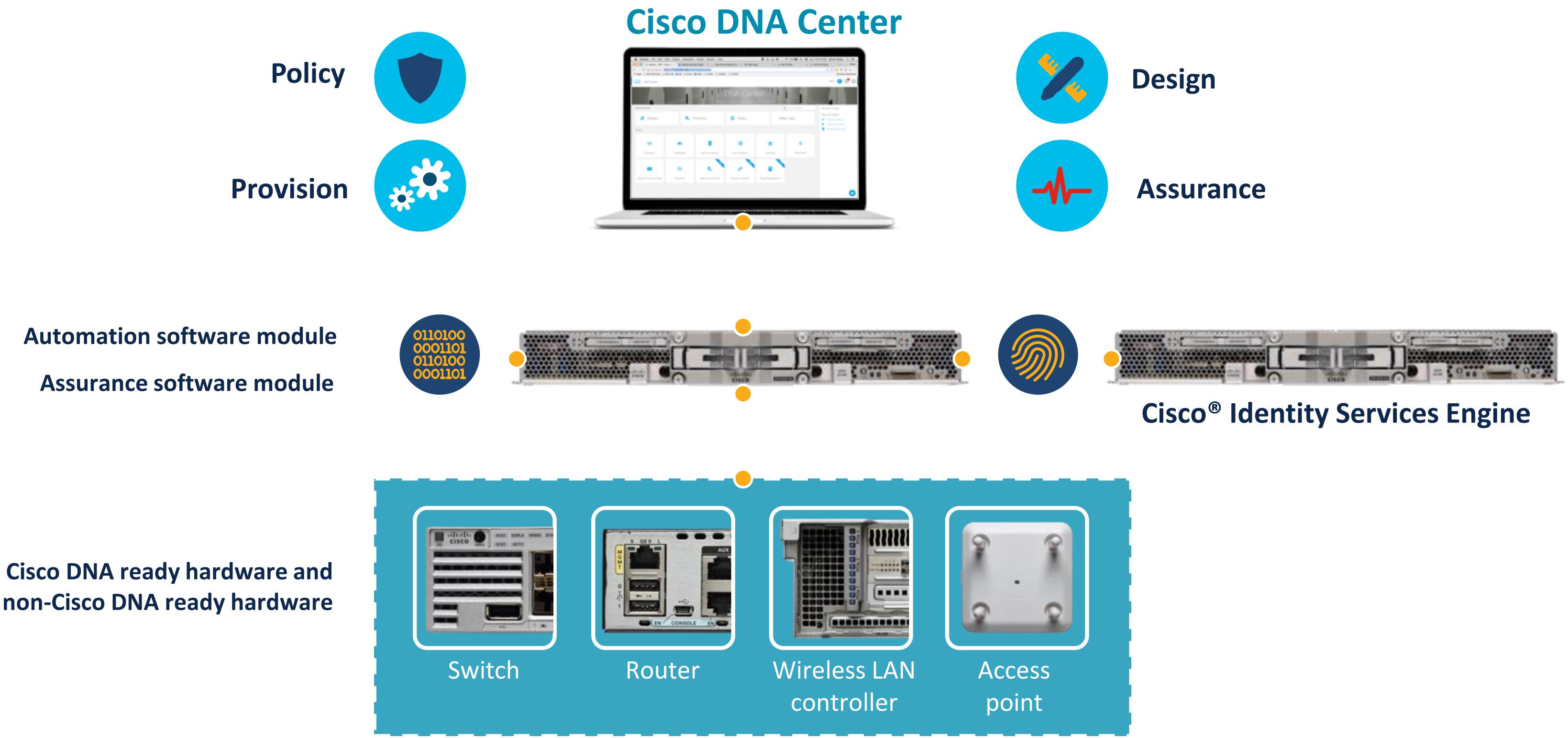
You make the power of data **possible**

Cisco’s intent-based Networking



Powered By Intent
Informed by Context

Intent-based networking – Cisco DNA components



Cisco DNA Center

Policy

Provision

Design

Assurance

Automation software module

Assurance software module

Cisco® Identity Services Engine

Cisco DNA ready hardware and non-Cisco DNA ready hardware

Switch

Router

Wireless LAN controller

Access point

Why Automation?

Automation: The guarantee that automatic infrastructure configurations and updates ensure compliance with pre-defined network standards

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

Continuous Verification

Configurations, Changes, Routing, Security

Services, Compliance, Audits

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

Prerequisites

You make networking **possible**

Base Automation and Assurance Prerequisites

- Global Credentials
  - Global Credentials can be set before discovery. This is optional as Global and discovery specific credentials can be defined during the discovery process. However, these settings will be used to help define and apply missing device credential once discovered.
- Collectors
  - Configure SNMP Collector to allow SNMP MIB walk on network devices. Required for basic device health and analytics to be captured.

Base Automation and Assurance Prerequisites

- Discovery
  - Devices must be in managed state in inventory through discovery or manual addition. Global credentials and SNMP collection configurations applied during this process.
- Site Hierarchy
  - When Devices are associated to a site Network Setting configurations for that site are applied to the device. Devices should also be associated to the correct building or floor before Telemetry is applied to allow correct assurance statistical association and analysis.

Network Discovery

You make security **possible**

What is Discovery?

- Discovery is a process of learning the devices in the given network
- User will have to provide the SNMP and CLI credentials to discover devices on a network
- Once the device is discovered successfully, the device will be added to inventory for inventory data collection

Cisco DNA Center Device Discovery

- For Devices to be managed by Cisco DNA Center they must first be discovered
- The Discovery feature
  - Scans the network
  - Inventories discovered devices
  - Can configure required network settings (if not already present)
- Discovery Prerequisites for network devices
  - SNMP Credential for Cisco DNA Center discovery
  - Exec level privilege SSH Credentials for Cisco DNA Center management

Cisco DNA Center Device Discovery Methods

- Devices can be discovered through the following protocol methods
  - Cisco Discovery Protocol (CDP)
  - Link Layer Discovery Protocol (LLDP)
  - IP address range (ICMP)

- CDP and LLDP Discoveries connect to a seed device and learn next CDP and LLDP next hop devices, and repeat the process with newly discovered hops
- IP Range Discovery scans the designated IP range with ICMP to identify responding devices

Network Device Setup

- What is required to add devices into Cisco DNA Center?
  - Ensure the following ports are open in ACLs/Firewalls between Cisco DNA Center and network devices

Ping	SSH	SNMP Poll	SNMP Trap	Syslog	NetFlow	
ICMP echo and reply	TCP/22	UDP/161	UDP/162	UDP/514	UDP/6007	TCP/443

- Minimal CLI and SNMP details are required for Cisco DNA Center to discover devices
  - SSH/Telnet Login (Privileged / RW)
  - SNMPv2c community (RO)
- More details can be found in the release notes

Device Controllability in Discovery

- When discovery is run with ”Device Controllability” enabled
  - If Cisco DNA Center could not connect to device using any of the SNMP credentials provided, but could connect using the CLI credentials, then Cisco DNA Center will configure the first SNMP credential available in the request
  - If available, the first SNMPV3 credential will be configured instead of SNMPV2
  - If NETCONF support exists in the device and Cisco DNA Center could not connect to the device using NETCONF but could connect to the CLI credentials, then Cisco DNA Center will configure NETCONF on the first port provided in the request
- NETCONF is supported on Polaris images version 16.5 or higher

Configuration Changes on WLCs

```
(Cisco Controller) >transfer download start


Mode........................................... SFTP
Data Type...................................... NA Serv
CA cert
SFTP Server IP.................................
192.168.139.162
SFTP Server Port............................... 22
SFTP Path......................................
/cert/3183c217-de69-4a80-ba7e-bb97211ef951/
SFTP Filename..................................
systemcert.pem
SFTP Username..................................
sftpuser
SFTP Password..................................
*********
```

Install Certificate for Steaming Telemetry

Configuration Changes on WLCs

```
(Cisco Controller) >show network assurance summary


     Server url............................. https://192.168.139.162
     Wsa Service............................ Enabled
     wsa Onchange Mode...................... Enabled
     wsa Sync Interval...................... Fixed
                                                       NAC Data
Publish Status:
        Last Error........................... Fri Feb 16 06:57:12 2018
        Last Success......................... Fri Feb 16 07:38:18
2018
        JWT Token Config..................... JWT Auth Configured
        JWT Last Success..................... Fri Feb 16 06:57:12
2018
        JWT Last Failure..................... None


                                                      Sensor Backhaul
settings:
        Ssid................................. Not Configured
        Authentication....................... Open
                                                      Sensor
provisioning:
        Status............................... Disabled
        Interface Name....................... None
        WLAN ID.............................. None
        SSID................................. None
```

Configure steaming telemetry services (WSA)

#CiscoLiveAPJC

Example: WLC Config Pushed at Discovery

- Pushed from Cisco DNA Center when a supported WLC is discovered

```
(Cisco Controller) > debug aaa tacacs enable
*SNMPTask: Apr 19 19:15:34.667: Log to TACACS server(if online): snmp syscontact
*emWeb: Apr 19 19:16:13.017: Log to TACACS server(if online): transfer download datatype na-serv-ca-cert
*emWeb: Apr 19 19:16:13.056: Log to TACACS server(if online): transfer download mode sftp
*emWeb: Apr 19 19:16:13.056: Log to TACACS server(if online): transfer download port 22
*emWeb: Apr 19 19:16:13.096: Log to TACACS server(if online): transfer download username sftpuser
*emWeb: Apr 19 19:16:13.136: Log to TACACS server(if online): transfer download password <hidden>
*emWeb: Apr 19 19:16:13.176: Log to TACACS server(if online): transfer download path /cert/495d13f4-c030-458a-bf4d-3f99b5279f03/
*emWeb: Apr 19 19:16:13.219: Log to TACACS server(if online): transfer download serverip 192.168.124.152
*emWeb: Apr 19 19:16:13.256: Log to TACACS server(if online): transfer download filename systemcert.pem
*emWeb: Apr 19 19:16:13.296: Log to TACACS server(if online): transfer download port 22
*emWeb: Apr 19 19:16:13.379: Log to TACACS server(if online): transfer download start
*emWeb: Apr 19 19:16:28.980: Log to TACACS server(if online): cloud-services wsa mode Disable
*emWeb: Apr 19 19:16:29.181: Log to TACACS server(if online): network assurance server url  https://192.168.124.152
*emWeb: Apr 19 19:16:30.310: Log to TACACS server(if online): cloud-services wsa mode Enable
```

Device Controllability in Host Tracking

- When device discovery or add is performed with “Device Controllability” enabled
  - The Cisco DNA Center will configure IPDT on discovered devices with a role of “Access”
  - IP Device Tracking keeps track of connected hosts on a device

Configuration Changes (Switches)

There are several changes that Cisco DNA Center automatically makes to switches during discovery

- PKI
- IPDT
- HTTP Server source
- SNMP RO & RW communities
    - (If not already configured)

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl
crypto pki certificate chain DNAC-CA
  <snip>
  quit

device-tracking tracking
!
device-tracking policy IPDT_MAX_10
 limit address-count 10
 no protocol udp
 tracking enable
!
interface <ACCESS-INTERFACES>
 device-tracking attach-policy IPDT_MAX_10

ip http client source-interface Loopback0

snmp-server community <RO-COMMUNITY> RO
snmp-server community <RW-COMMUNITY> RW
```

Configuration Changes (Routers)

There are several changes that Cisco DNA Center automatically makes to routers during discovery

- PKI
- HTTP Server source
- SNMP RO & RW communities
    - (If not already configured)

```
crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl
crypto pki certificate chain DNAC-CA
  <snip>
  quit

ip http client source-interface Loopback0

snmp-server community <RO-COMMUNITY> RO
snmp-server community <RW-COMMUNITY> RW
```

Collectors

You make the power of data **possible**

Cisco DNA Center SNMP Collector

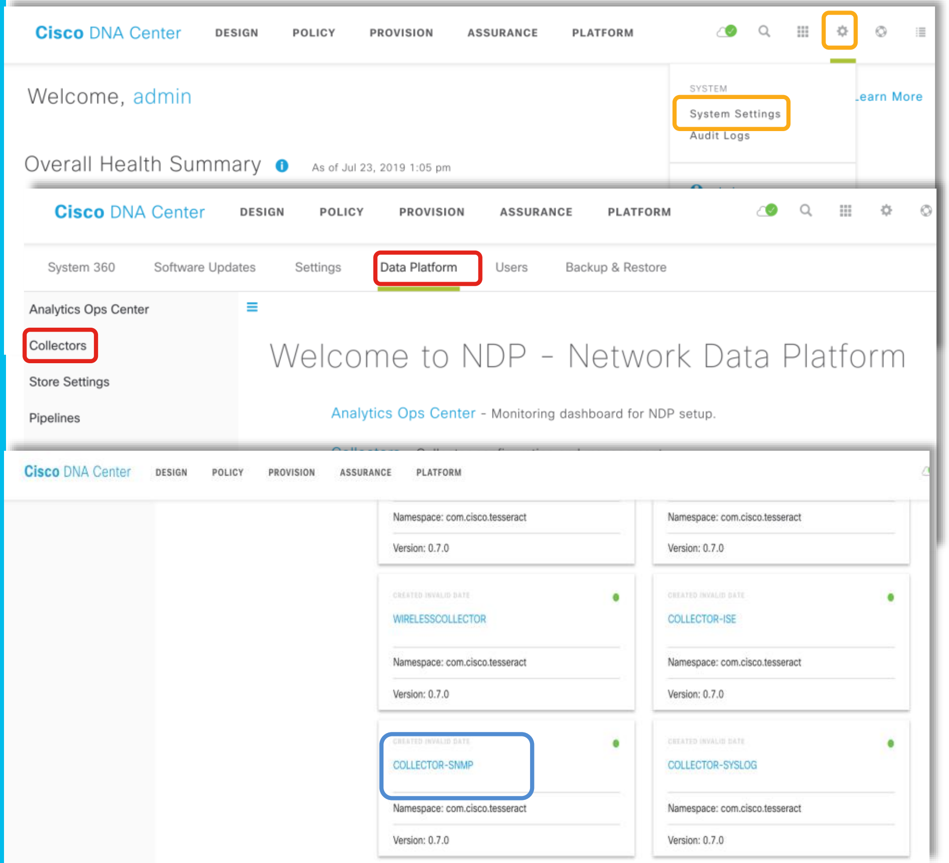
Select the Gear Icon

System Settings

Select Data Platform tab

Collectors Link

Select COLLECTOR-SNMP



Welcome, admin

Overall Health Summary As of Jul 23, 2019 1:05 pm

Welcome to NDP - Network Data Platform

Analytics Ops Center - Monitoring dashboard for NDP setup.

Namespace: com.cisco.tesseract

Version: 0.7.0

Telemetry Profiles

You make multi-cloud **possible**

Assurance Provisioning

- Device Site Assignment Provisioning
  - Assurance requires devices be provisioned with a site assignment in order to push telemetry configuration
- Predefined or Custom Telemetry Profile Creation
  - Two best practice default telemetry profiles exist for use in provisioning assurance configurations.
  - Custom telemetry profiles can also be created in exception use cases where the best practice telemetry profile settings need to be altered.

Assurance Provisioning

- Telemetry Profile Provisioning
  - Assign profiles to specific devices and validate configuration push

- Assurance Telemetry Verification
  - Verify Assurance Dashboards are being populated with expected telemetry data

Example: IOS Config Pushed by Telemetry App

- Pushed from Cisco DNA Center Telemetry App – Custom Profile, Syslog/SNMP enabled (without NetFlow)

```
Pod12-Fusion#
*Apr 20 00:00:04.909: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.201.14.156 port 0 CLI Request Triggered
*Apr 20 00:00:04.913: %HA_EM-6-LOG: catchall: logging host 10.201.14.156 transport udp port 514
*Apr 20 00:00:04.922: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.201.14.156 port 514 started - CLI initiated
*Apr 20 00:00:04.941: %HA_EM-6-LOG: catchall: logging trap 6
*Apr 20 00:00:04.956: %SYS-5-CONFIG_I: Configured from console dy dnac on vty2 (192.168.124.152)
*Apr 20 00:00:04.959: %HA_EM-6-LOG: catchall: exit
*Apr 20 00:00:05.143: %HA_EM-6-LOG: catchall: configure terminal
*Apr 20 00:00:05.202: %HA_EM-6-LOG: catchall: snmp-server enable traps
*Apr 20 00:00:05.534: %HA_EM-6-LOG: catchall: snmp-server host 10.201.14.156 traps versión 2c tesseract-traps udp-port 162
*Apr 20 00:00:05.547: %SYS-5-CONFIG_I: Configured from console by dnac on vty2 (192.168.124.152)
*Apr 20 00:00:05.551: %HA_EM-6-LOG: catchall: exist
Pod12_Fusion#
*Apr 20 00:01:27.184: %HA_EM-6-LOG: catchall: disable
*Apr 20 00:01:27.272: %HA_EM-6-LOG: catchall: logout
Pod12-Fusion#
```

Notes on Cisco DNA Center and NetFlow

- NetFlow is required for Application Health data
- Cisco DNA Center provisioning of NetFlow is only supported on routers running IOS version 16.x or newer
- The current behavior is for NetFlow to be enabled on all interfaces on the routers

```
performance monitor context tesseract profile application-performance
exporter destination <DNAC-IP> source Loopback0 transport udp port 6007
traffic-monitor application-client-server-stats
traffic-monitor application-response-time

interface <ALL-INTERFACES>
 performance monitor context tesseract
```

Telemetry Profiles

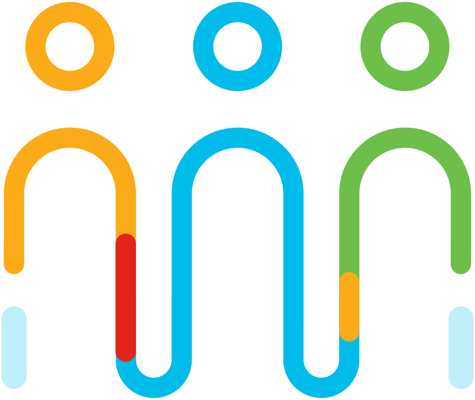
- There are three telemetry profiles defined by default. The Capabilities are as outlined

Profile Name	Syslog Security Level	NetFlow
Maximal	Informational	IPFIX
Optimal	Informational	
Disable		

- Profiles can be assigned at Site and Device level
- Default assigned is Disable Telemetry
- Recommendation is to apply Maximal to Routers and Optimal to switches

Prerequisites Demo

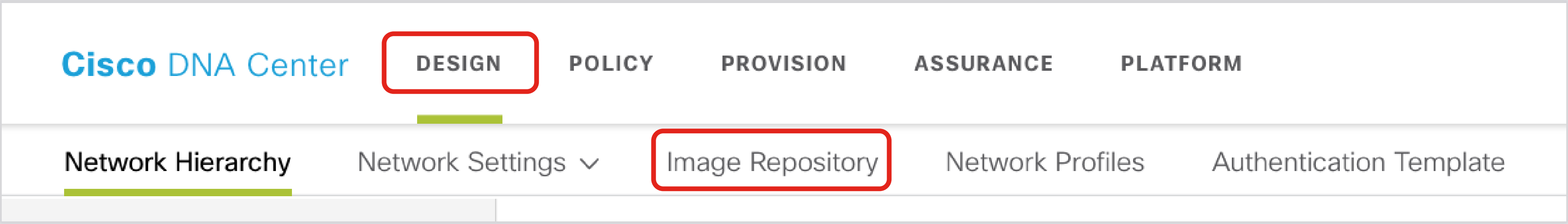
Software Image Management (SWIM)



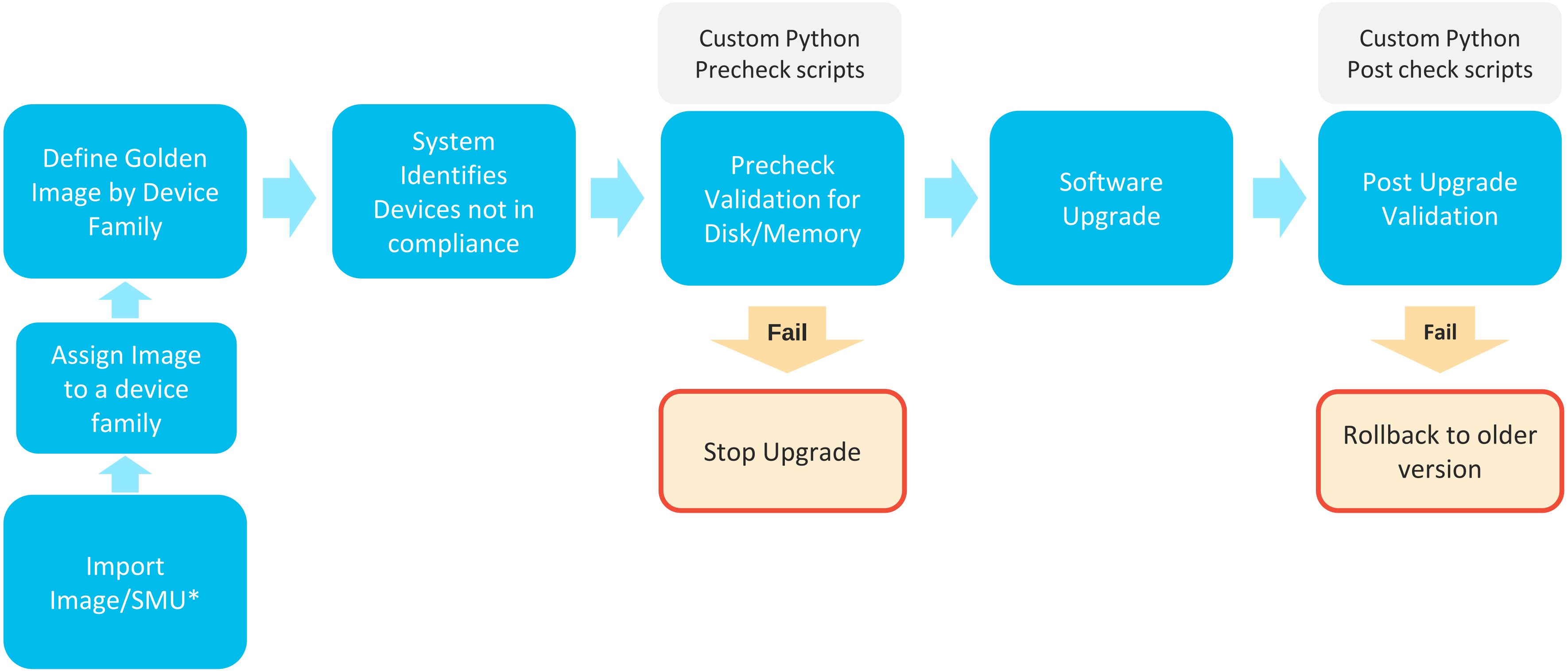
You make customer experience **possible**

Image Repository

- Manages software and VNF images
- Also manages third-party images
- Accessible as a page in Design



Cisco DNA Center – Software Update Workflow



Import Image/SMU*

Assign Image to a device family

Define Golden Image by Device Family

System Identifies Devices not in compliance

Custom Python Precheck scripts

Precheck Validation for Disk/Memory

Fail

Stop Upgrade

Software Upgrade

Custom Python Post check scripts

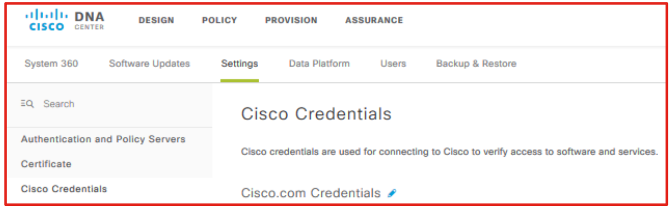
Post Upgrade Validation

Fail

Rollback to older version

**SMU* = Software Maintenance Upgrade

Integration of Image Repository with Cisco



Cisco Credentials

Cisco credentials are used for connecting to Cisco to verify access to software and services.

Cisco.com Credentials

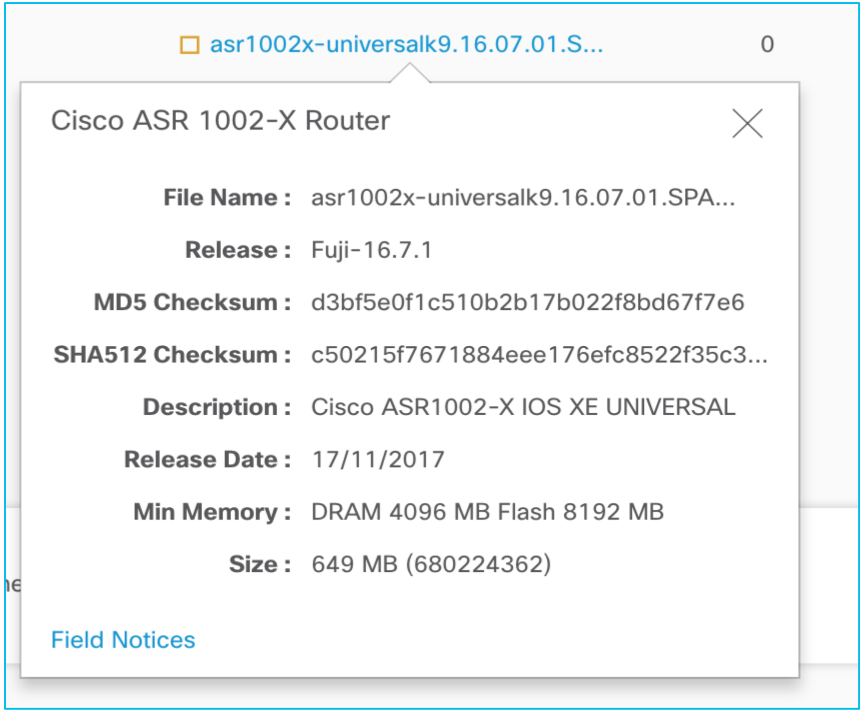
Integrate image repository management with Cisco

Provide your CCO credentials to get started

Accept EULA agreement to unlock further image details:

- Get access to field notices and release notes
- Get Cisco *recommended* image information
- Get Cisco *latest* image information

Image Details – with and without CCO



□ asr1002x-universalk9.16.07.01.S... 0

Cisco ASR 1002-X Router

File Name : asr1002x-universalk9.16.07.01.SPA...

Release : Fuji-16.7.1

MD5 Checksum : d3bf5e0f1c510b2b17b022f8bd67f7e6

SHA512 Checksum : c50215f7671884eee176efc8522f35c3...

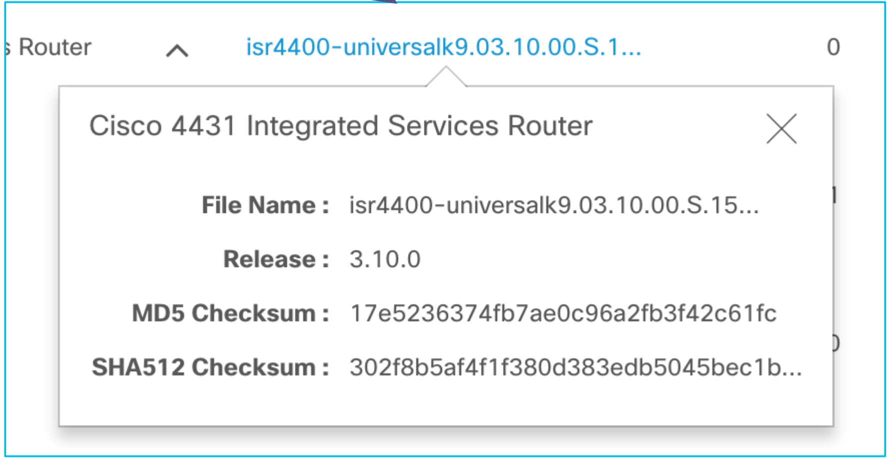
Description : Cisco ASR1002-X IOS XE UNIVERSAL

Release Date : 17/11/2017

Min Memory : DRAM 4096 MB Flash 8192 MB

Size : 649 MB (680224362)

Field Notices



Router isr4400-universalk9.03.10.00.S.1... 0

Cisco 4431 Integrated Services Router

File Name : isr4400-universalk9.03.10.00.S.15...

Release : 3.10.0

MD5 Checksum : 17e5236374fb7ae0c96a2fb3f42c61fc

SHA512 Checksum : 302f8b5af4f1f380d383edb5045bec1b...

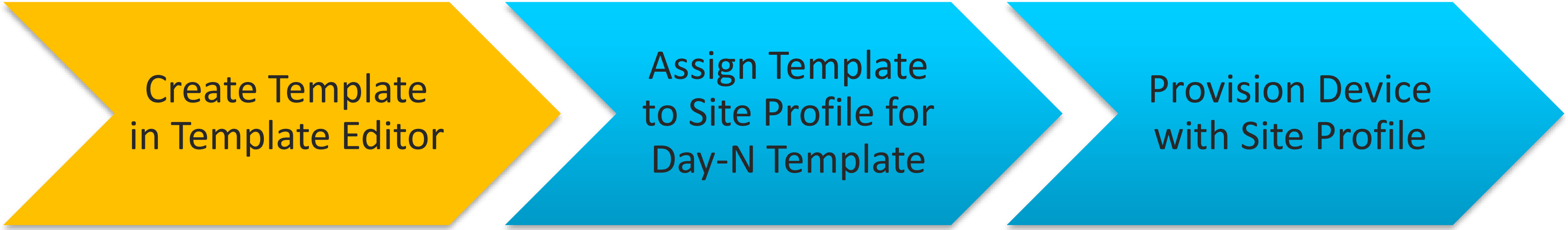
SWIM Demo

Template Editor

You make networking **possible**

Day-N Automation – Router and Switch

- Workflow from Design to Provision Day-N Templates


Create Template in Template Editor

Assign Template to Site Profile for Day-N Template

Provision Device with Site Profile

What is Template Editor?

- CLI Templates allow customers to script their network configurations
  - Project
    - Container for configuration templates
  - Template
    - Resides within a Project
- Cisco's template language, that is broadly a mix of
  - Apache Velocity Template Language for control constructs
  - Cisco CLI for network configuration

What is Template Editor?

- Template Editor aims at providing users with a development environment for…
  - Creating templates
  - Editing templates
  - Deploying templates to real devices

Template Editor Language

- Templates are a composite of Cisco CLI and Apache Velocity Template Language (VTL)
- VTL can be used to write more advanced content in templates through the use of different switches like those exemplified below
  - Variables: $device
  - Properties: $device.Address
  - Methods: $device.getAddress()
  - Directives:

```
<table>#foreach( $device in $deviceList )
<tr><td>$foreach.count</td><td>$device.interface</td></tr>
#end
</table>
```

CLI and Variable Template Commands

- Configure hostname

```
hostname  $name
```

- Configure interface

```
interface  $interfaceName
     description $description
```

- Configure NTP time interval on WLC

```
config time ntp Interval $interval
```

** Note: All the commands executed via templates are always in conf t mode, so there is no need to specify the enable / conf t command explicitly in the template*

Enable Mode Template Commands

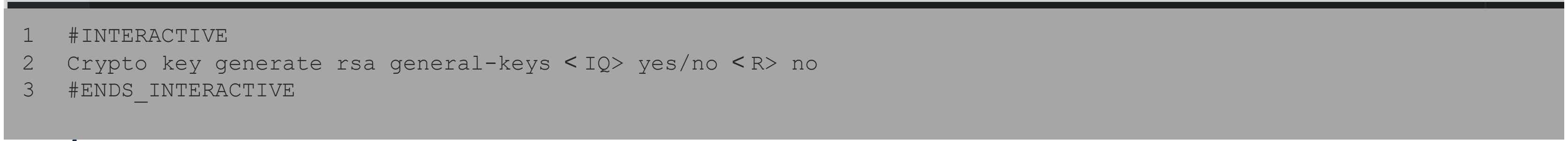
- Adding Enable Mode Commands
  - Use this syntax to add enable mode commands to your CLI templates

```
#MODE_ENABLE
wr  mem
#MODE_END_ENABLE
```

- ** Note: You need to specify #MODE_ENABLE if you want to execute any command outside the configure terminal*

Interactive Template Commands

- Adding Interactive Commands
  - An interactive command contains the input that must be entered following the execution of a command
  - To enter an interactive command in the CLI Content area, use the following syntax
    - CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
    - 2<R>command response 2
  - <IQ> and <R> tags are case-sensitive and must be entered as uppercase



```
#INTERACTIVE
Crypto key generate rsa general-keys < IQ> yes/no < R> no
#ENDS_INTERACTIVE
```

Combining Interactive and Enable Commands

- Combining Interactive Enable Mode Commands
- Use this syntax to combine interactive Enable Mode commands
    - #MODE_ENABLE
    - #INTERACTIVE
    - commands<IQ>interactive question<R>response
    - #ENDS_INTERACTIVE
    - #MODE_END_ENABLE

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ> Create directory filename ? <R>tt12
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

What is Variable Binding?

- Before version 1.2, the user had to provide the value for every variable which was defined in the template. In some cases, values for those variables are already defined in the system (e.g., DHCP Server, DNS, syslog server)
- Variable Binding allows user to bind template variables to existing sources, which are already defined in the system
- Binding is associated to the Attribute of a specific variable

Variable Binding

Network Profile Objects

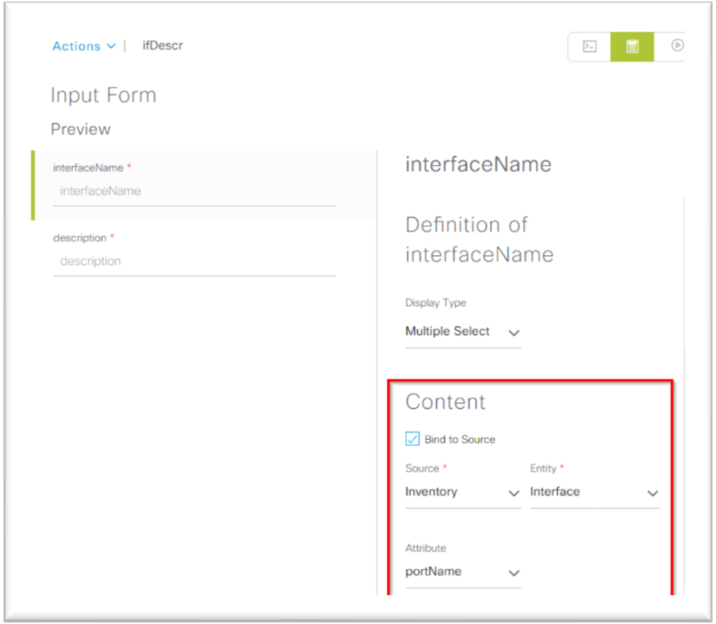
- SSID

Common Settings Objects

- dhcp.server, syslog.server, snmp.trap.receiver, ntp.server, timezone.site, device.banner dns.server, netflow.collector

Inventory Objects

- Device, Interface, AP Group, Flex Group, WLAN, Policy Profile, Flex Profile



Input Form

Preview

interfaceName *
interfaceName

description *
description

interfaceName

Definition of interfaceName

Display Type
Multiple Select

Content

☑ Bind to Source

Source *
Inventory

Entity *
Interface

Attribute
portName

Network Device Onboarding

You make security **possible**

What is Network Plug-n-Play (PnP)?

- An Automation tool that allows devices to be discovered, provisioned and configured automatically at power on
- Can load Image, boot config, startup config and configuration templates (Day-0/Onboarding Templates)
- For Router, Switches, APs

PnP Server Discovery Options

Automated

1 DHCP with option 43
PnP string: 5A1D;B2;K4;I172.19.45.222;J80 added to DHCP Server

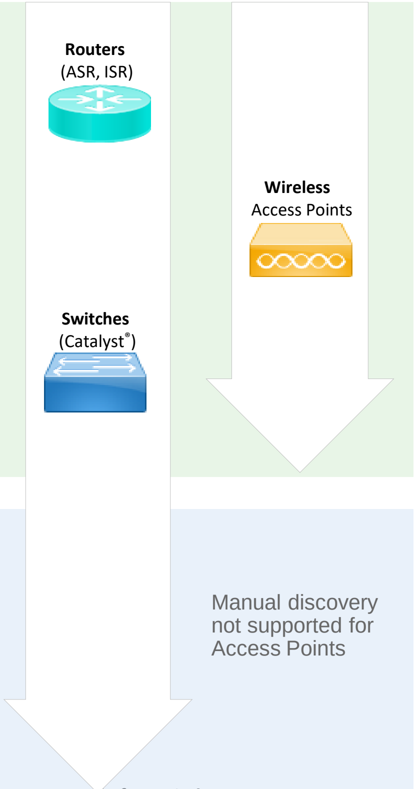
2 DNS lookup
pnpserver.localdomain **resolves to Cisco DNA Center IP Address**

3 Cloud re-direction https://devicehelper.cisco.com/device-helper
Cisco hosted cloud, re-directs to on-prem Cisco DNA Center IP Address

Manual

4 USB-based bootstrapping*
router-confg/router.cfg/ciscortr.cfg

5 Manual - using the Cisco® Installer App**
iPhone, iPad, Android

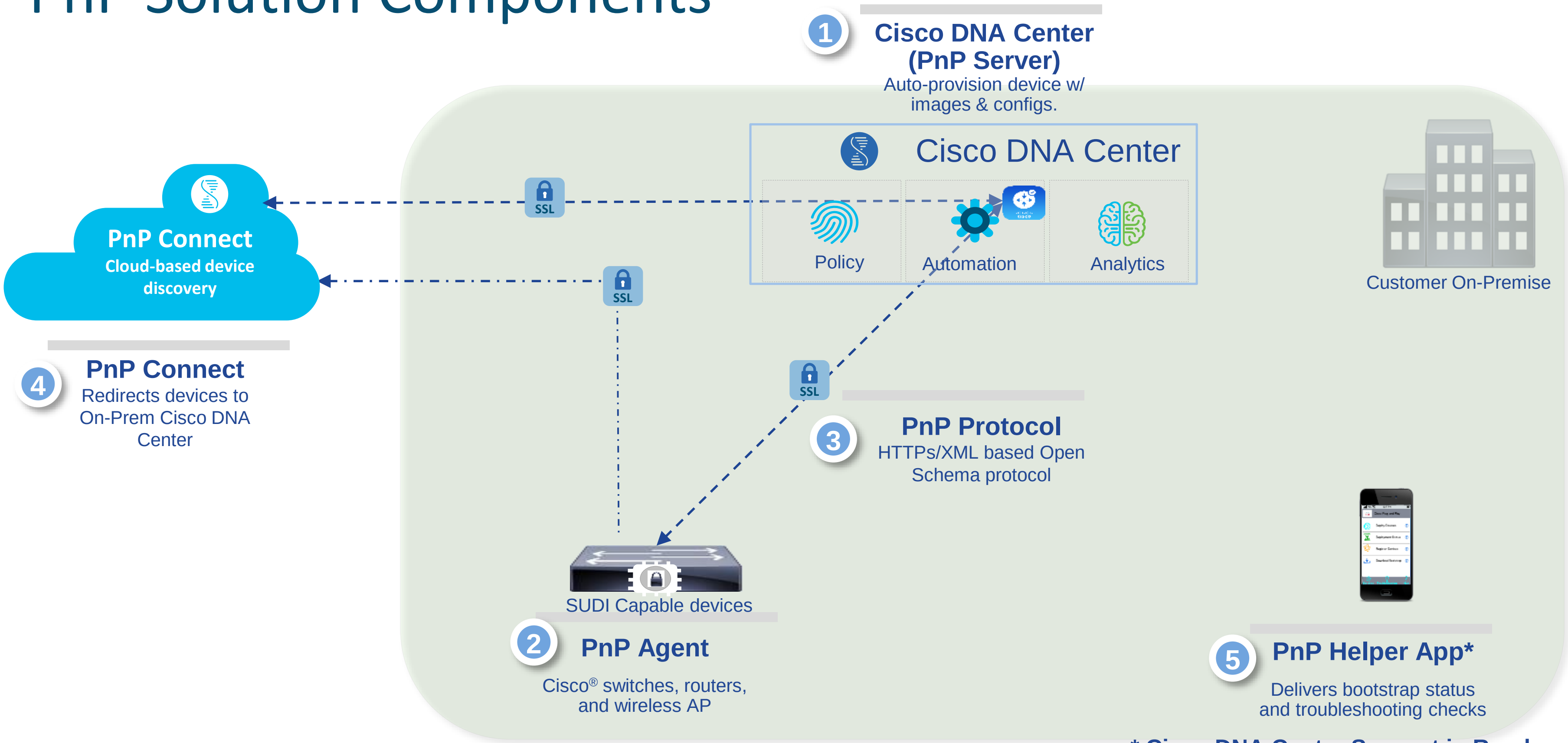


Manual discovery not supported for Access Points

* **Supported on Cat 9K only for switches**

* ***DNA-C Support in Roadmap**

PnP Solution Components



1 **Cisco DNA Center (PnP Server)**
Auto-provision device w/ images & configs.

2 **PnP Agent**
Cisco® switches, routers, and wireless AP

3 **PnP Protocol**
HTTPs/XML based Open Schema protocol

4 **PnP Connect**
Redirects devices to On-Prem Cisco DNA Center

5 **PnP Helper App***
Delivers bootstrap status and troubleshooting checks

*** Cisco DNA Center Support in Roadmap**

Network Device Onboarding Demo

Thank you

You make **possible**

cisco