



**CISCO** *Live!*

DevNet Zone



The bridge to possible

# Industrial Automation

From Day0 to Microsegmentation

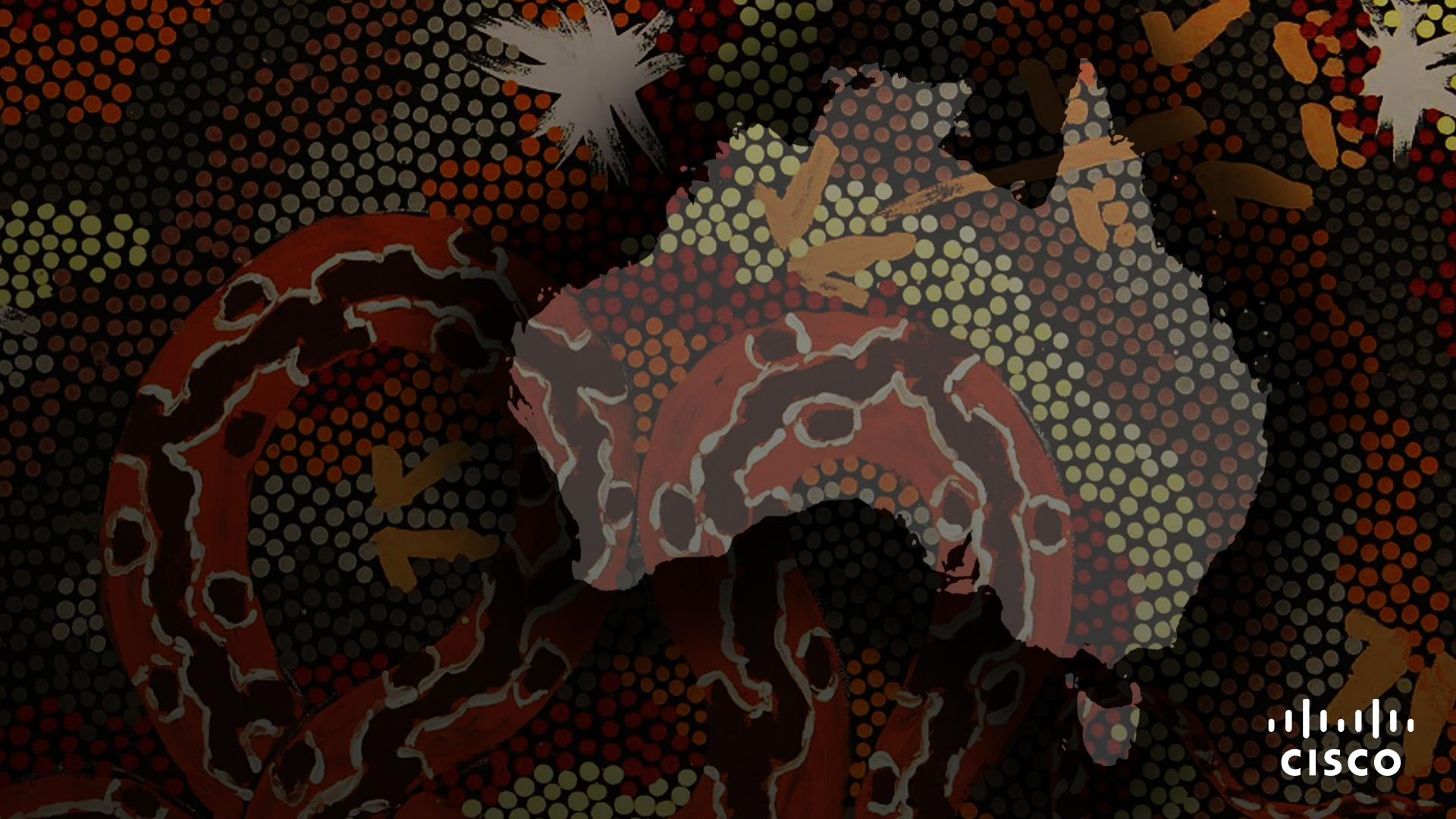
Thomas Kjaer-Olsen

DEVNET-1243



DevNet Zone

#CiscoLiveAPJC



# Cisco Webex App

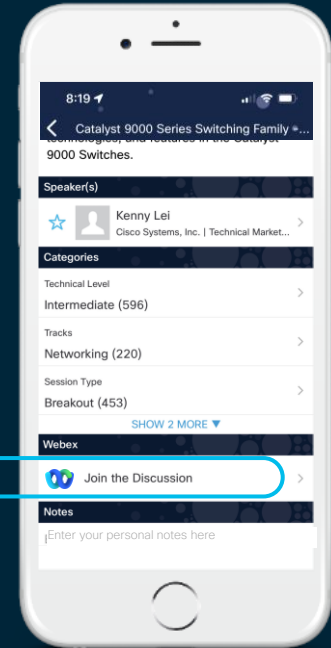
## Questions?

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

## How

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

Webex spaces will be moderated by the speaker until Thursday 22 December, 2022.





# Agenda

- Introduction
- Day0 (PnP) via DNAC
- DayN Templates via DNAC
- Configuration via direct Device Programmability
  - Manual Micro-segmentation example
- Conclusion

Join my



# Industrial Automation – From Day0 to Microsegmentation DEVNET-1243

6th December  
2022 at 4pm

Get the code:

<https://github.com/tkj-scythe/clmel-devnet1243>

# Intro – What

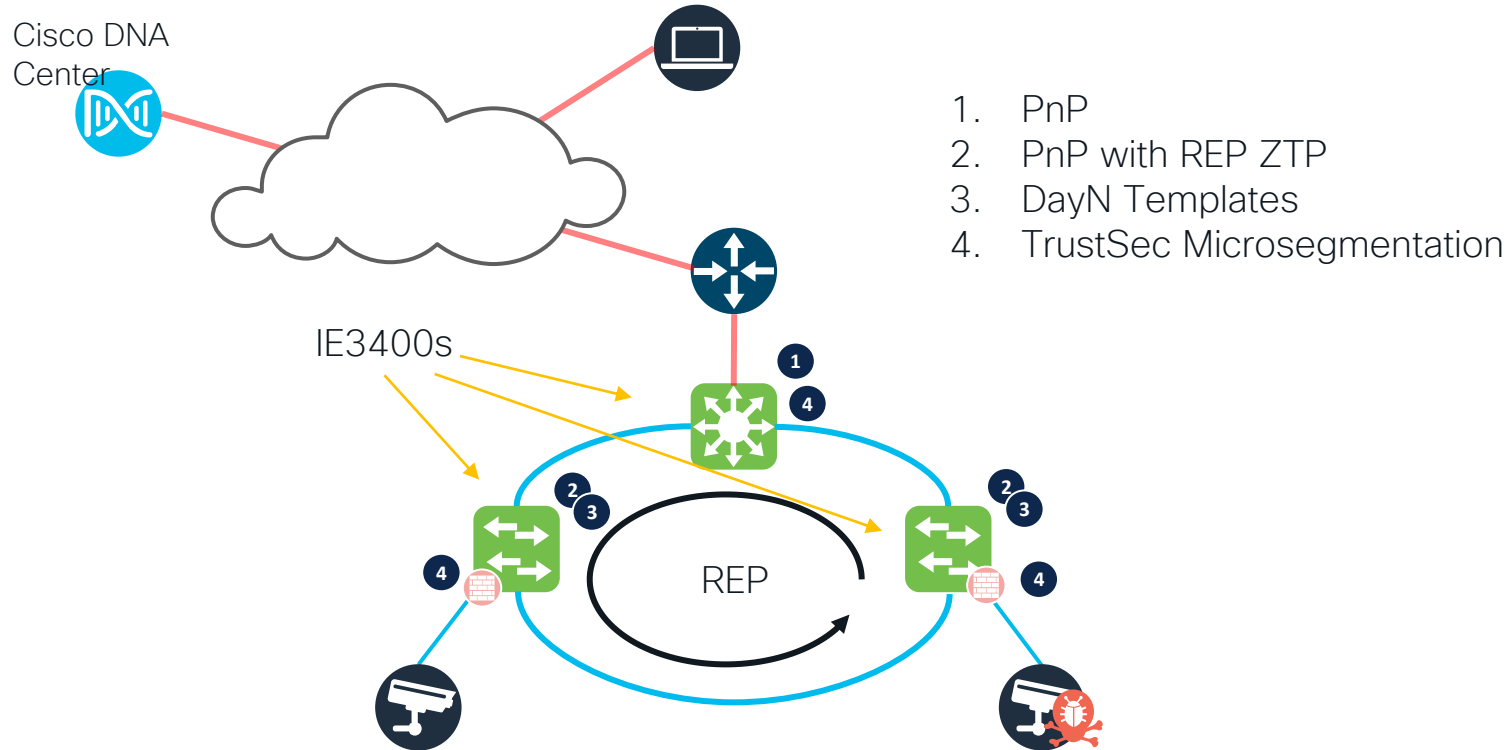
## Intro

- PnP Via DNAC
  - Demo newer Industrial Automation Capabilities
    - REP ZTP
- Driving DNAC PnP via REST API
- DayN Templates
- Pushing config directly via Netconfig-yang
  - Demo Microsegmentation via TrustSec





# Intro - Topology



# Day -1: Network settings

Upstream connectivity:

- PNP Requirements:

1. Configure PnP VLAN
2. Configure DHCP + DNS (or use DHCP Option 43)
3. Add DNS entry for pnpserver

```
UPSTREAM-SWITCH#
```

```
pnp startup-vlan [Vlan number]
```

```
interface Vlan[number]  
  ip address [network] [subnetmask]  
  ip helper-address [DHCP Server IP]
```

```
DHCP-Server#  
ip dhcp pool pnp-dhcp-pool  
  network [network] [subnet mask]  
  default-router [router ip]  
  dns-server [dns server]  
  domain-name [yourdomain]
```

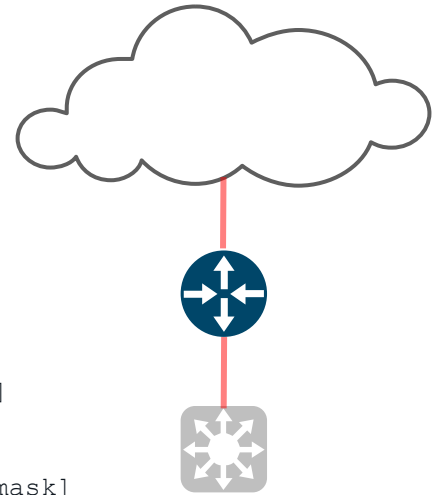
```
ip dhcp excluded-address [router ip]
```



Host (A)

10.66.66.66

static








# Day -1: Cisco DNA Center Setup

DNA-C Requirements:



1. Set up network hierarchy
2. Configure Day0 Templates
3. Create Network Profile
  1. Assign templates to network profile
  2. Assign network profile to network sites

# Day -1: DNAC Setup

 Cisco DNA Center



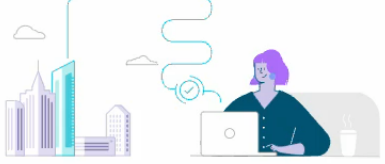
Welcome, [admin](#) [Explore](#)

 Learn about new capabilities in this release on the Cisco DNA Center [YouTube Channel](#). 

Stay up to date with your network and Cisco DNA Center through our insight email

Receive announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email.

[Insights](#)



Assurance Summary

### Health

Healthy as of Nov 7, 2022 11:55 AM

%

%

%

Network Devices

Wireless Clients

Wired Clients

### Critical Issues

Last 24 Hours

0

P1

0

P2

### Trends and Insights

Last 30 Days

AP Performance Advisories

Trend Deviations

**CISCO** *Live!*

DevNet Zone

#CiscoLiveAPJC DEVNET-1243

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

13

# Day -1: Day0 Template Setup

Welcome, **admin**

🖨️ Explore

📺 ⓘ Learn about new capabilities in this release on the Cisco DNA Center [YouTube Channel](#). ✕

Stay up to date with your network and Cisco DNA Center through our insight email

Receive announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email.

Insights



## Assurance Summary

### Health ⓘ

Healthy as of Nov 7, 2022 11:55 AM



### Critical Issues

Last 24 Hours

0

P1

0

P2

### Trends and Insights

Last 30 Days


--





AP Performance

0




Trend Deviations

# Day -1: Network Profile Setup

 Cisco DNA Center

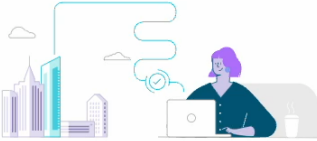
Welcome, **admin** [Explore](#)

  Learn about new capabilities in this release on the Cisco DNA Center [YouTube Channel](#). 


Stay up to date with your network and Cisco DNA Center through our insight email

Receive announcements, network highlights, weekly snapshots, and executive summaries all neatly packaged in a single email.

[Insights](#)



Assurance Summary

Health 

Healthy as of Nov 10, 2022 8:55 PM

— — %

Network Devices

— — %

Wireless Clients

— — %

Wired Clients

[View Details](#)

Critical Issues

Last 24 Hours

0

P1

0

P2

[View Details](#)

Trends and Insights

Last 30 Days

— —

AP Performance Advisories

0

Trend Deviations

[View Details](#)

**CISCO** *Live!*

DevNet Zone

#CiscoLiveAPJC DEVNET-1243

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

23

# Day 0: PnP – via GUI

**Cisco DNA Center**

Welcome, Maglev Admin

Some of your license compliance requirements have not been met. [Learn more.](#)

### Assurance Summary

#### Health

Healthy as of Nov 11, 2022 7:31 PM

84% 100% 96%

Network Devices Wireless Clients Wired Clients

[View Details](#)

#### Critical Issues

Last 24 Hours

2 2

P1 P2

[View Details](#)

#### Trends and Insights

Last 30 Days

0 0

AP Performance Advisories Trend Deviations

[View Details](#)

### Network Snapshot

#### Sites

As of Nov 11, 2022 7:40 PM

53

DNS Servers : 1  
NTP Servers : 1

#### Network Devices

As of Nov 11, 2022 7:40 PM

38

Unclaimed: 2  
Unprovisioned: 7

#### Application QoS Policies

As of Nov 11, 2022 7:40 PM

2

Successful Deploys: 1  
Errored Deploys: 1

```
User Access Verification
Username: admin
Password:
% Login Invalid

Username: admin
Password:
Password OK

000421: Nov 11 09:38:31.250: NCMART_LIC-3-COMM_FAILED: Communications failure with
the Cisco Smart License Utility (CSLU) : Unable to resolve server hostname/domain n
ame
switch#
switch#
```

# Day 0: PnP – via API

Good:

Using templates, single source of truth, work asynchronously with field staff

Bad:

Clicking through GUIs is time consuming at scale  
Still prone to human error

Solution:

Drive PnP via API



# Sidebar: REP ZTP

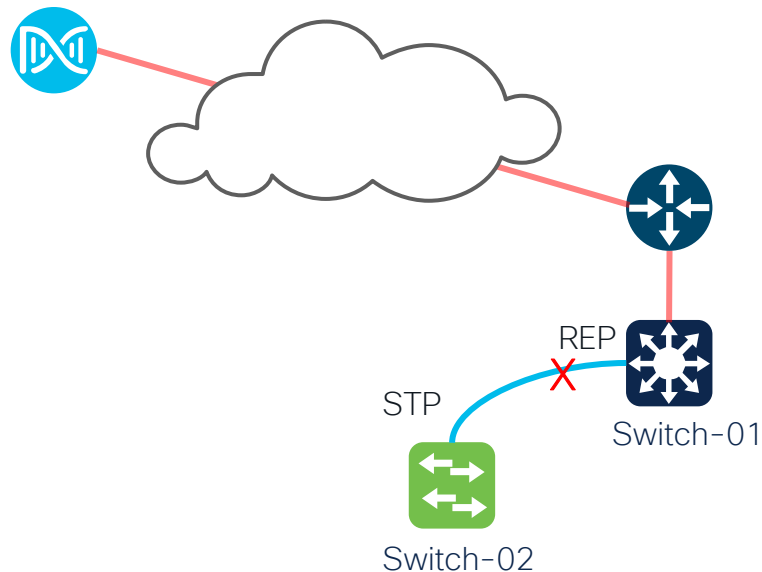
## Next Step: PnP Switch 2

Problem?

Switch 1 is configured for REP  
Switch 2 is factory default with STP  
Switch 1 will block VLANs

Solution?

REP Zero Touch Provisioning (ZTP)



# Sidebar: REP ZTP

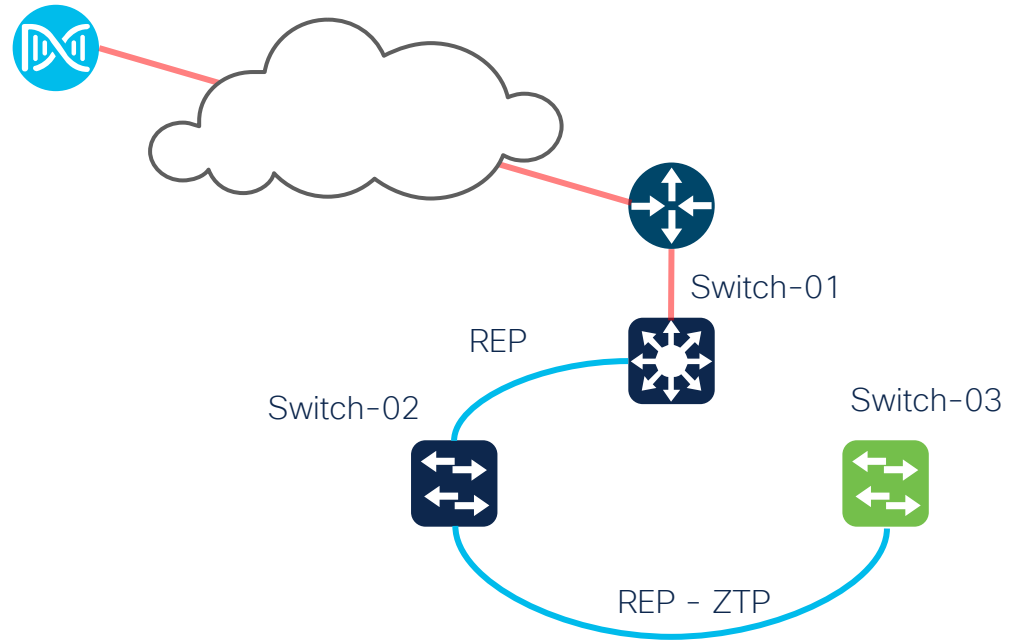
Steps:

1. Switch 1 configured with REP – Sends REP LSL Hello pkts
2. Switch 2 boots with no config – transmits LSL with new TLV
3. Switch 1 receives TLV and puts PNP startup VLAN in FWD mode (all other VLANs blocked)
4. Switch 2 does DHCP/PnP via startup VLAN
5. Switch 2 gets REP config via PnP – REP now forwarding as normal



# Sidebar: REP ZTP

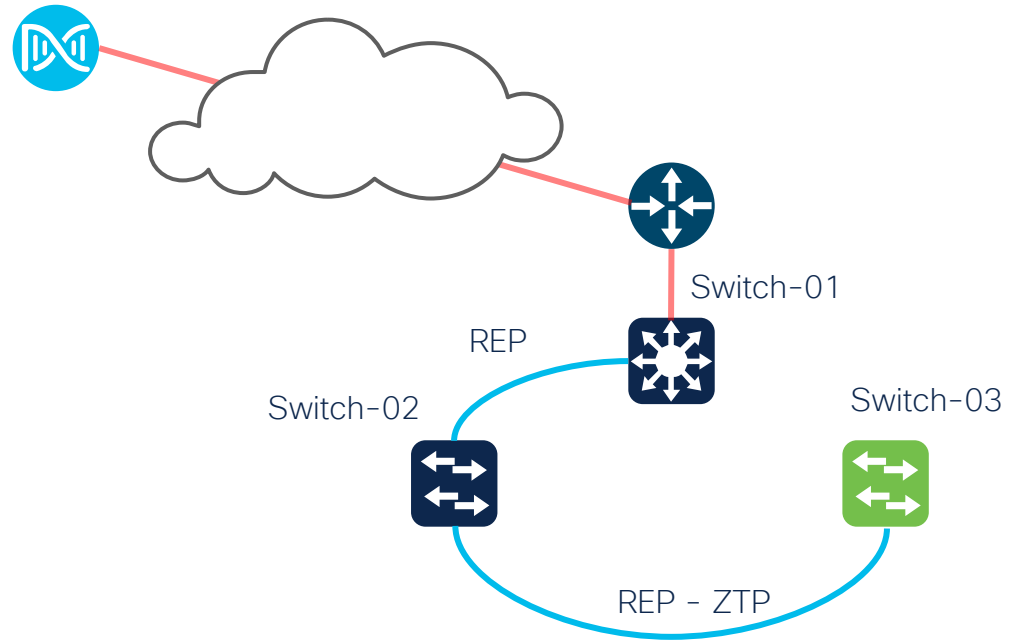
And for the next switch..  
etc



# Sidebar: REP ZTP

Configuration:

```
Switch-01#  
interface Gi1/1  
    rep ztp-enable
```



# Exploring the APIs:

Platform -> Developer Toolkit

← → ↻ ⚠ Not Secure | https://10.66.238.118/dna/platform/app/consumer-portal/developer-toolkit/apis

☰ Cisco DNA Center Platform / Develo

APIs Integration Flows Event Notifications

Check out our API capabilities and try them out for yourself

Explore our developer documentation or test different APIs in your network environment to build, connect, and leverage rich capabilities of Cisco DNA Center.

🔍 Search

Authentication ▾

- Cisco DNA Center System ▾
  - Health and Performance
  - Licenses
  - Platform
  - User and Roles
- Connectivity ▾
  - Fabric Wireless
  - SDA

## Authentication

Authentication APIs provide an authorized token for acc  
**\*Prerequisite\*:** Add the request header 'x-auth-token' successful API response.

Method	Name	
POST	importCertificate	1
POST	importCertificateP12	1 f

# Example: Driving Cisco DNA-Center PnP via APIs

Process:

1. Authenticate (get token via username/password)
2. Add device (by serial) – before it has connected via PnP
3. Wait for device to connect to DNA-C
4. Gather device information: DeviceID, TemplateID, SiteID, IOS-ID
5. Claim device to site

Demo via Postman

# Postman Collection



# Setup Postman Environment Variables

<

:/

POST 4.0 CI

POST 2.0

GET teler

GET 3.0

CLMEL

GET 3.1 Get

GET 3.2

GET 3.3 Ge


CME

>

+


...



CMEL2022-DEVNET-1243



CMEL2022-DEVNET-1243

Fork 0 Save Share ...



	VARIABLE	TYPE ⓘ	INITIAL VALUE ⓘ	CURRENT VALUE ⓘ	...	Persist All	Reset All	
<input checked="" type="checkbox"/>	device_id	default ▾		636eead32c9582000bf5d723				
<input checked="" type="checkbox"/>	serial	default ▾	FOC2351V0XH	FOC2351V0XH				
<input checked="" type="checkbox"/>	dnac	default ▾	10.66.238.118	10.66.238.118				
<input checked="" type="checkbox"/>	token	default ▾		eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIi...				
<input checked="" type="checkbox"/>	device_serial	default ▾	FOC2351V0XH	FOC2351V0XH				
<input checked="" type="checkbox"/>	pid	default ▾	IE-3400-8T2S	IE-3400-8T2S				
<input checked="" type="checkbox"/>	image_id	default ▾		c0760a8c-c0fd-474a-a642-e493b7dc2a34				
<input checked="" type="checkbox"/>	template_id	default ▾		7343d271-3153-4667-a02c-4862641272a8				
<input checked="" type="checkbox"/>	site_id	default ▾		468f08fe-c274-41c7-a651-30492440ff66				
<input checked="" type="checkbox"/>	port	default ▾	443	443				
<input checked="" type="checkbox"/>	password	default ▾	Cisco12345	Cisco12345				
	Add a new variable							



# Day 0: PnP – via API

## 1.1. Get Token

POST

https://{{dnac}}:{{port}}/api/system/v1/auth/token

Send

Params

Authorization ●

Headers (12)

Body

Pre-request Script

Tests ●

Settings

Cookies

Type

Basic Auth

The authorization header will be automatically generated when you send the request. Learn more about [authorization](#) ↗

Username

Username

Password

Password

☒ Show Password

## 1.2. Save Token

POST

https://{{dnac}}:{{port}}/api/system/v1/auth/token

Params

Authorization ●

Headers (12)

Body

Pre-request Script

Tests ●

Settings

```
1 var data = JSON.parse(responseBody);
2 postman.setEnvironmentVariable("token", data.Token);
```

# Day 0: PnP – via API

## 2. Add Device

POST

https://{{dnac}}:{{port}}/dna/intent/api/v1/onboarding/pnp-device

Send

Params

Authorization

Headers (12)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

JSON

```
1 {
2   "deviceInfo": {
3     "hostname": "FJORM-IE3400-01",
4     "serialNumber": "{{device_serial}}"
5   }
6 }
```

Devices (3) Focus: Default

Auto-refresh: 30 s

Search Table

0 Selected Actions Add Devices

As of: Nov 12, 2022 6:57 PM Refresh

	#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site	Last
<input type="checkbox"/>	1	TKO-QUASAR-FAIB-C9300-01	FCW2228G0UL	C9300-24T	10.66.235.197	Network	Unclaimed	<div><div></div></div> 40%	NA	No
<input type="checkbox"/>	2	FJORM-IE3400-01	FOC2351V0XH	Unavailable	Unavailable	User	Unclaimed	<div><div></div></div> 0%	NA	No

# Day 0: PnP – via API

## 3. Wait for device to connect

Device Status

Unclaimed (3)

Error (0)

Provisioned (12)

All (15)

Devices (3)

Focus: Default

Auto-refresh: 30 s

Search Table

0 Selected

Actions

+ Add Devices

As of: Nov 12, 2022 6:59 PM

Refresh

	#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site
<input type="checkbox"/>	1	TKO-QUASAR-FAIB-C9300-01	FCW2228G0UL	C9300-24T	10.66.235.197	Network	Unclaimed	<div><div></div></div> 40%	NA
<input type="checkbox"/>	2	FJORM-IE3400-01	FOC2351V0XH	IE-3400-8T2S	10.66.235.166	User	Unclaimed	<div><div></div></div> 40%	NA

# Day 0: PnP – via API

## 4. Gather device details:

GET

https://{{dnac}}:{{port}}/dna/intent/api/v1/onboarding/pnp-device?serialNumber={{device\_serial}}

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

any

1

var data = JSON.parse(responseBody);

2

postman.setEnvironmentVariable("device\_id", data[0].id);

3

postman.setEnvironmentVariable("pid", data[0].deviceInfo.pid)

GET

https://{{dnac}}:{{port}}/dna/intent/api/v1/image/importation?family=ie3x00&version=17.09.02

Params

Authorization

Headers (10)

Body

Pre-request Script

Tests

Settings

1

var data = JSON.parse(responseBody);

2

postman.setEnvironmentVariable("image\_id", data.response[0].imageUuid);

# Day 0: PnP – via API

## 4. Continue gathering device details:

GET

▼

https://{{{dnac}}}{{{port}}}/dna/intent/api/v2/template-programmer/template?name=IE-Automation-PnP-IE3400-Stubbs-Jinja\_7101221235110

Params ● Authorization Headers (10) Body Pre-request Script Tests ● Settings

```
1 var data = JSON.parse(responseBody);
2 postman.setEnvironmentVariable("template_id", data.response[0].id);
```

GET

▼

https://{{{dnac}}}{{{port}}}/dna/intent/api/v1/site?name=global/Niflheim/Hvergelmir/River+Level

Params ● Authorization Headers (10) Body Pre-request Script Tests ● Settings

```
1 var data = JSON.parse(responseBody);
2 postman.setEnvironmentVariable("site_id", data.response[0].id);
```

# Day 0: PnP – via API

## 5. Claim device:

POST

https://{{dnac}}:{{port}}/dna/intent/api/v1/onboarding/pnp-device/site-claim?=

Send

Params

Authorization

Headers (11)

Body

Pre-request Script

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

JSON


Cookies


Beautify

```
1 {
2   ... "deviceId": "{{device_id}}",
3   ... "siteId": "{{site_id}}",
4   ... "type": "Default",
5   ... "imageInfo": {
6     ... "imageId": "{{image_id}}",
7     ... "skip": false
8   },
9   ... "configInfo": {
10     ... "configId": "{{template_id}}",
11     ... "configParameters": [
12       ... {
13         ... "key": "mgmt_ipaddress_input",
14         ... "value": "10.1.2.1 255.255.255.0"
15       }
16     ]
17   }
18 }
19 }
```

# Day 0: PnP – via API

## 5. Claim device:

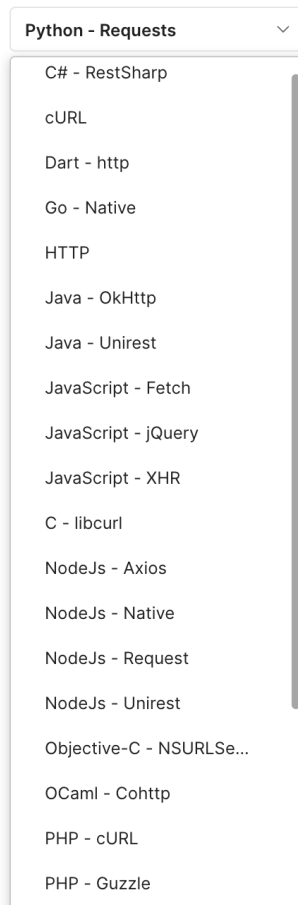
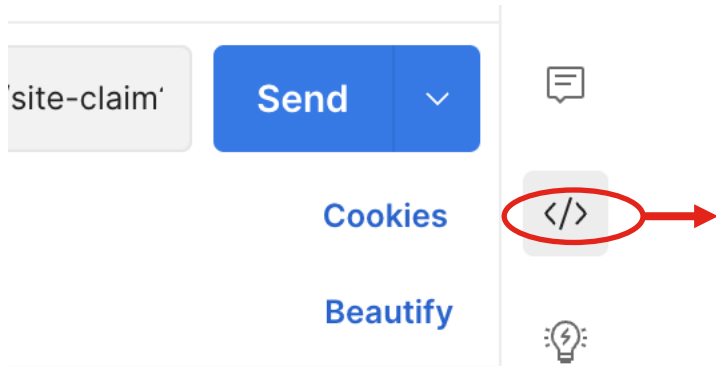
Devices (3) Focus: [Default](#) Auto-refresh: 30 s 



0 Selected [Actions](#) [+ Add Devices](#) As of: Nov 12, 2022 7:04 PM [Refresh](#)

<input type="checkbox"/>	#	Device Name	Serial Number	Product ID	IP Address	Source	State	Onboarding Progress	Site
<input type="checkbox"/>	1	<a href="#">TKO-QUASAR-FAIB-C9300-01</a>	FCW2228G0UL	C9300-24T	10.66.235.197	Network	Unclaimed	<div><div></div></div> 40%	NA
<input type="checkbox"/>	2	<a href="#">FJORM-IE3400-01</a>	FOC2351V0XH	IE-3400-8T2S	10.66.235.166	User	Planned	<div><div></div></div> 40%	Global/Ni

# That was still via a GUI...?





# How did that REP ZTP go?

The screenshot shows the Cisco Provisioning Portal interface. On the left, a sidebar displays a hierarchy starting with 'Global', followed by 'Galacticus', 'Niflheim' (highlighted), 'Queensland', 'SCUH', 'South Park', 'USC', and 'USQ'. A search bar labeled 'Search Hierarchy' is at the top of the sidebar. The main content area is titled 'Provision / Inventory' and shows a list of devices. The 'Niflheim' hierarchy is expanded to show detail. The device list has columns for 'Device Name', 'IP Address', 'Device Family', and 'MAC Address'. The first device is 'FJORM-IE3400-01.bne.ciscolabs.com' with IP '10.66.235.164' and MAC '6c:71:0d:14:74:80'. The second device is 'SVOL-IE3400-01.bne.ciscolabs.com' with IP '10.66.235.165' and MAC 'a8:ab:34:04:14:c0'. The interface includes filters for 'All', 'Routers', 'Switches', 'Wireless Controllers', 'Access Points', and 'Sensors'. There are also links for 'Go to old page', 'Take a tour', and 'Export'.

Search Hierarchy

Search Help

Global

- Galacticus
- Niflheim
- Queensland
- SCUH
- South Park
- USC
- USQ

Provision / Inventory

Expand to see detail.

All Routers Switches Wireless Controllers Access Points Sensors

Devices (2) Focus: Select

Go to old page Take a tour Export

Filter devices

0 Selected + Add Device Tag Actions

As of: Nov 12, 2022 7:

	Device Name	IP Address	Device Family	MAC Address
<input type="checkbox"/>	FJORM-IE3400-01.bne.ciscolabs.com	10.66.235.164	Switches and Hubs	6c:71:0d:14:74:80
<input type="checkbox"/>	SVOL-IE3400-01.bne.ciscolabs.com	10.66.235.165	Switches and Hubs	a8:ab:34:04:14:c0

It worked didn't it? 😊

# How did that REP ZTP go?

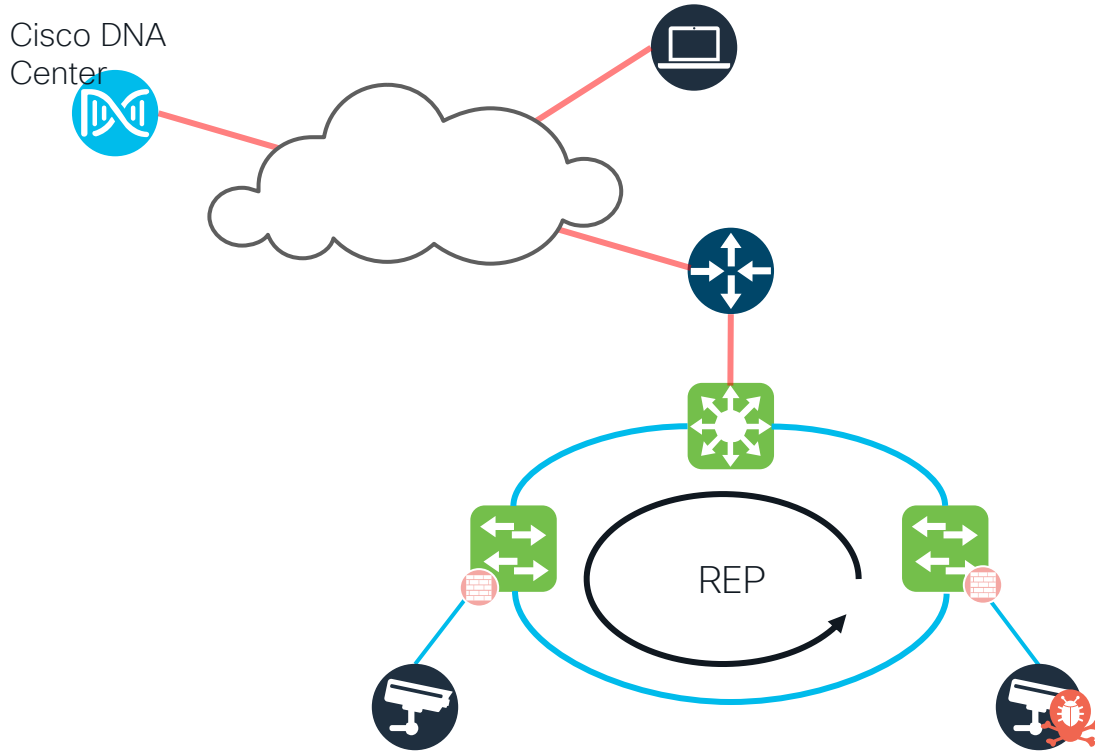
## Upstream debugs:

```
SVOL-IE3400-01#debug rep lslsm
REP debug lsl sm debugging is on
003051: Nov 12 19:34:10.429:      rep_lsl_rx Gi1/1: during state INIT_DOWN, got event 1(phy_link_down)
003052: Nov 12 19:34:10.429: @@@ rep_lsl_rx Gi1/1: INIT_DOWN -> INIT_DOWN
003053: Nov 12 19:34:10.430:      rep_lsl_tx Gi1/1: during state DOWN, got event 1(phy_link_down)
003054: Nov 12 19:34:10.430: @@@ rep_lsl_tx Gi1/1: DOWN -> DOWN
003055: Nov 12 2022 19:34:12.453: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state to up
003056: Nov 12 19:34:13.433:      rep_lsl_rx Gi1/1: during state INIT_DOWN, got event 0(phy_link_up)
003057: Nov 12 19:34:13.433: @@@ rep_lsl_rx Gi1/1: INIT_DOWN -> WAIT
003058: Nov 12 19:34:13.433:      rep_lsl_tx Gi1/1: during state DOWN, got event 0(phy_link_up)
003059: Nov 12 19:34:13.433: @@@ rep_lsl_tx Gi1/1: DOWN -> IDLE
003060: Nov 12 2022 19:34:14.436: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/1, changed state to up
003062: Nov 12 19:34:23.431:      rep_lsl_rx Gi1/1: during state WAIT, got event 6(age_timeout)
003063: Nov 12 19:34:23.431: @@@ rep_lsl_rx Gi1/1: WAIT -> NO_NEIGHBOR
003074: Nov 12 19:34:26.872:      rep_lsl_rx Gi1/1: during state NO_NEIGHBOR, got event 13(rep_ztp_enable)
003075: Nov 12 19:34:26.872: @@@ rep_lsl_rx Gi1/1: NO_NEIGHBOR -> NO_NEIGHBOR
003076: Nov 12 2022 19:34:26.873: %REP-6-ZTPPORTFWD: Interface GigabitEthernet1/1 moved to forwarding on ZTP notification
003077: Nov 12 2022 19:34:27.431: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
```

# Sidebar: TrustSEC / SGTs / SGACLs speedrun

- What are SGTs
  - Tags assigned to traffic at the ingress port – identify the source of the traffic without relying on IP and DNS
  - How? dot1x, manually ...
- How are they carried
  - Carried in the packet header at layer 2
- What are SGACLs
  - Like ACLs – but based on source and destination IP

# Sidebar: Microsegmentation



# DayN Templates

1. Create template
2. Add template to Network Profile
3. Provision device

# DayN Templates

## Interface Template Update:

```
1 template IP_CAMERA_INTERFACE_TEMPLATE
2 spanning-tree portfast
3 spanning-tree bpduguard enable
4 switchport access vlan 40
5 switchport mode access
6 switchport block unicast
7 switchport port-security
```

## Update Access Interfaces:

```
1
2
3
4 {% for interface in interfaces %}
5
6     interface {{ interface }}
7         no switchport access vlan
8         no shutdown
9         source template IP_CAMERA_INTERFACE_TEMPLATE
10        description CCTV ACCESS PORT
11
12 {% endfor %}
13
```

## Interface Template Update with TrustSec:

### Template

```
1 template IP_CAMERA_INTERFACE_TEMPLATE
2 spanning-tree portfast
3 spanning-tree bpduguard enable
4 switchport access vlan 40
5 switchport mode access
6 switchport block unicast
7 switchport port-security
8 device-tracking attach-policy IPDT_POLICY
9 cts manual
10 policy static sgt 40
11 no propagate sgt
```

# Day N: Templates

OnBoarding Template(s)

Day-N Template(s)

Attach Templates

+

Add Template

Cards

Table

IE-IE3400-Interfa...

View Device Type(s)

View Device Tag(s)

IE-3400-Update- ...

View Device Type(s)

View Device Tag(s)

IE-IE3400-Interfa...

View Device Type(s)

# Day N: Templates

OnBoarding Template(s) **Day-N Template(s)**



Attach Templates + Add Template

**Cards** Table

IE-IE3400-Interfa...



[View Device Type\(s\)](#)

[View Device Tag\(s\)](#)



IE- **No-Trustsec** ...

[View Device Tag\(s\)](#)

IE-IE3400-Interfa...

[View Device Type\(s\)](#)



# Day N: Templates

The screenshot displays the Cisco DevNet templates management interface. At the top, there are two tabs: "OnBoarding Template(s)" and "Day-N Template(s)". Below the tabs, the text "Attach Templates" is visible. To the right, there is a blue button with a plus icon and the text "Add Template". Below this, there are two buttons: "Cards" (which is highlighted in blue) and "Table". The main content area shows three template cards. The first card is titled "IE-IE3400-Interfa..." and has a blue callout box with the text "TrustSec" and "fa...". Below the title, it says "View Device Type(s)" and "View Device Tag(s)". The second card is titled "IE-3400-Update-..." and also has "View Device Type(s)" and "View Device Tag(s)" links. The third card is titled "IE-IE3400-Interfa..." and has "View Device Type(s)" link. Each card has a horizontal line at the bottom with a pencil icon and a trash icon.

# Day N: Templates

Tag devices:

Filter devices

2 Selected + Add Device Tag Actions 1

As of: Nov 12, 2022 9:11 PM

Device Name	Family	MAC Address	Compliance
FJORM-IE3400-01.bne	es and Hubs	6c:71:0d:14:74:80	Compli
SVOL-IE3400-01.bne.c	es and Hubs	e8:eb:34:04:14:c0	Compli

TrustS

☐ EnableTrustSec

☒ No-Trustsec

☐ TrustSec

Create new tag (TrustS)

Manage Tags

Apply

# Day N: Templates

Provision Devices:

The screenshot shows the 'Devices' page in the Cisco DevNet Center. At the top, it says 'Devices (2)' with a 'Focus: Select' dropdown. There are links for 'Go to old page', 'Take a tour', 'Export', and a settings icon. A search bar labeled 'Filter devices' is present. Below the search bar, it says '2 Selected' and 'Add Device'. There are tabs for 'Tag' and 'Actions'. The 'Actions' dropdown menu is open, showing options: 'Inventory', 'Software Image', 'Provision', 'Telemetry', 'Device Replacement', 'Compliance', and 'More'. The 'Provision' option is highlighted, and its sub-menu is open, showing options: 'Assign Device to Site', 'Provision Device', 'LAN Automation', 'LAN Automation Status', 'Configure WLC HA', 'Configure WLC Mobility', and 'Manage LED Flash Status'. The 'Provision Device' option is highlighted in the sub-menu. The table below shows two devices: 'FJORM-IE3400-01.bne.ciscola TrustSec' and 'SVOL-IE3400-01.bne.ciscola TrustSec'. Both devices have a 'Provision' icon (orange square) and a 'Compliance' status (green checkmark). The table columns are 'Device Name', 'Device Family', 'MAC Address', and 'Compliance'.

Device Name	Device Family	MAC Address	Compliance
FJORM-IE3400-01.bne.ciscola TrustSec	Switches and Hubs	00:71:0d:14:74:80	Comp
SVOL-IE3400-01.bne.ciscola TrustSec	Switches and Hubs	34:04:14:c0	Comp

# Day N: Templates

Confirm config:

```
SVOL-IE3400-01#show run | s template
template IP_CAMERA_INTERFACE_TEMPLATE
spanning-tree portfast
spanning-tree bpduguard enable
switchport access vlan 40
switchport mode access
switchport block unicast
switchport port-security
```

```
SVOL-IE3400-01#show run int gi1/3
interface GigabitEthernet1/3
description CCTV ACCESS PORT
switchport mode access
source template IP_CAMERA_INTERFACE_TEMPLATE
spanning-tree portfast
```

# Day N: Templates

Update template

1. Re-tag device
2. Re-provision device with new template

# Day N: Templates

Update tag:

Devices (2) Focus: **Select** [Go to top](#)

Q Filter devices

2 Selected [+ Add Device](#) Tag Actions [①](#)

<input checked="" type="checkbox"/>	Device Name	Fam
<input checked="" type="checkbox"/>	FJORM-IE3400-01.bne No-Trustsec	nes
<input checked="" type="checkbox"/>	SVOL-IE3400-01.bne.c No-Trustsec	nes

Trust

☐ No-Trustsec

☐ EnableTrustSec

☒ TrustSec

Create new tag (Trust)

Manage Tags

Apply

## Provision Devices

Network Devices / Provision Devices

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

### Devices

Select devices to fill out provisioning parameters

Find Show

≡ Q Device All [v](#)

[v](#) IE-IE3400-Interface-Templates-Up...  
✓ FJORM-IE3400-01.bne.ciscola...  
✓ SVOL-IE3400-01.bne.ciscolabs...

[v](#) IE-IE3400-Interface-Templates-wit...  
✓ FJORM-IE3400-01.bne.ciscola...  
✓ SVOL-IE3400-01.bne.ciscolabs...

☐ Provision these templates even if they have been deployed before

☒ Copy running config to startup config

IE-IE3400-Interface-Templates-with-SGT

No variables found in template

# Check config:

```
SVOL-IE3400-01#show run | s role
ip access-list role-based allow-all
  10 permit ip
ip access-list role-based allow-ping-only
  10 permit icmp
  20 deny ip
ip access-list role-based allow-ssh-only
  10 permit tcp dst eq 22
  20 deny ip
ip access-list role-based deny-all
  10 deny ip
cts role-based enforcement
SVOL-IE3400-01#show run | s template
template IP_CAMERA_INTERFACE_TEMPLATE
  cts manual
  policy static sgt 40
  no propagate sgt
spanning-tree portfast
spanning-tree bpduguard enable
switchport access vlan 40
switchport mode access
switchport block unicast
switchport port-security
device-tracking attach-policy IPDT_POLICY
```

# Check config:

```
SVOL-IE3400-01#show cts interface
Global Dot1x feature is Disabled
Interface GigabitEthernet1/3:
  CTS is enabled, mode:      MANUAL
  IFC state:                 OPEN
  Interface Active for 10:04:02.876
  Authentication Status:    NOT APPLICABLE
    Peer identity:          "unknown"
    Peer's advertised capabilities: ""
  Authorization Status:     SUCCEEDED
    Peer SGT:               40
    Peer SGT assignment:    Untrusted
  SAP Status:               NOT APPLICABLE
  Propagate SGT:            Disabled
  Cache Info:
    Expiration              : N/A
    Cache applied to link  : NONE
[config snipped]..
```



# Direct Device Programmability

Netconf:

Network Configuration Protocol (NETCONF)

Operates on SSH, port 830 by default

Has a series of base commands:

- get, get-config, edit-config, copy-config etc

RFC: <https://www.rfc-editor.org/rfc/rfc6241>

Yang:

Data modelling language

RFC: <https://www.rfc-editor.org/rfc/rfc7950>

Netconf/yang:

More reading: <https://community.cisco.com/t5/networking-blogs/getting-started-with-netconf-yang-part-1/ba-p/3661241>



# Device Programmability

Turning it on:

```
SVOL-IE3400-01 (config) #netconf-yang
```

That's it

```
SVOL-IE3400-01#show netconf-yang status
netconf-yang: enabled
netconf-yang candidate-datastore: disabled
netconf-yang side-effect-sync: enabled
netconf-yang ssh port: 830
netconf-yang turbocli: disabled
```

# Device Programmability

Python module: ncclient

Repo: <https://github.com/ncclient/ncclient>

# Device Programmability – getting example yang xml

```
import sys
import logging
from ncclient import manager

def iosxe_connect(host, port, user, password):
    return manager.connect(host=host,
                           port=port,
                           username=user,
                           password=password,
                           device_params={'name': "iosxe"},
                           timeout=30,
                           hostkey_verify=False
    )

def export_config(host, user, password):
    with iosxe_connect(host, port=830, user=user, password=password) as m:
        config = m.get_config(source='running')
    with open("output.xml", "w") as f:
        f.write(config.xml)

if __name__ == '__main__':
    export_config(sys.argv[1], sys.argv[2], sys.argv[3])
```

# Device Programmability – getting example yang xml

```
python3 main.py 10.66.235.165 cisco cisco12345 get_config
```

```
▼<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="urn:uuid:9ca9a8a7-1df8-4181-9dda-e02c6f4239d8">
  ▼<data>
    ▼<native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
      <version>17.9</version>
      ▼<memory>
        ▼<free>
          ▼<low-watermark>
            <processor>63466</processor>
            </low-watermark>
          </free>
        </memory>
      </native>
      ▼<call-home>
        <contact-email-addr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-call-home">sch-smart-licensing@cisco.com</contact-email-addr>
        ▼<tac-profile xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-call-home">
          ▼<profile>
            ▼<CiscoTAC-1>
              <active>true</active>
              ▼<destination>
                <transport-method>http</transport-method>
                </destination>
              </CiscoTAC-1>
            </profile>
          </tac-profile>
        </call-home>
      </service>
      <password-encryption/>
      ▼<timestamps>
        ▼<debug-config>
          ▼<datetime>
            <msec/>
            <localtime/>
          </datetime>
        </debug-config>
      </timestamps>
    </data>
  </rpc-reply>
```

etc...



# Device Programmability – updating an SGACLs

```
import sys
import logging
from ncclient import manager

UPDATE_RBACL = """
<config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <native xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-native">
    <cts>
      <role-based xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-cts">
        <permissions>
          <from>
            <range>
              <range >{src_sgt}</range>
              <to>
                <range>
                  <range >{dst_sgt}</range>
                  <ACL-name-new >{acl_name}</ACL-name-new>
                  <ACL-name>{acl_name}</ACL-name>
                  <name>{acl_name}</name>
                </range>
              </to>
            </range>
          </from>
        </permissions>
      </role-based>
    </cts>
  </native>
</config>
"""
```

# Device Programmability – updating an SGACLs

```
import sys
import logging
from ncclient import manager

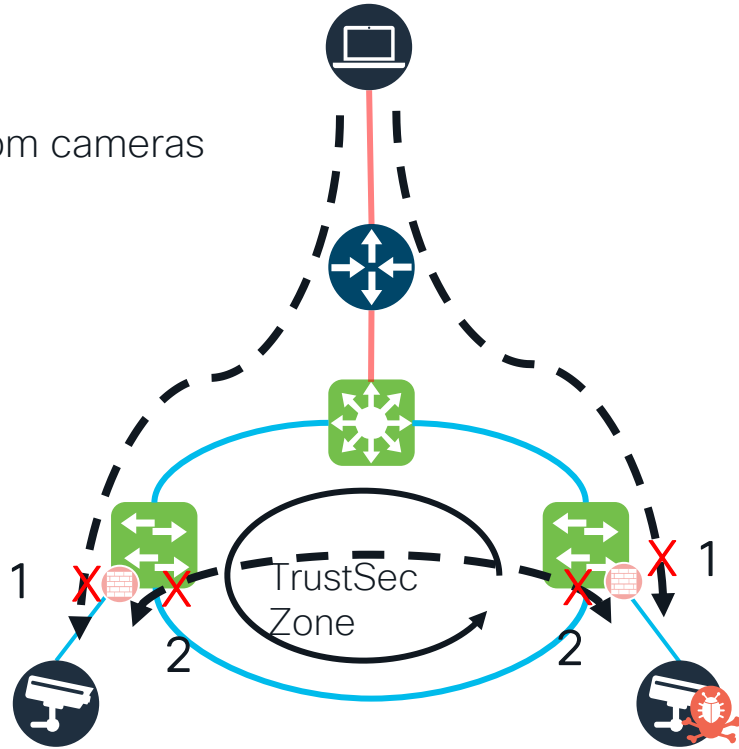
def update_rbac(host, user, password, acl_name, src_sgt, dst_sgt):
    confstr = UPDATE_RBACL.format(acl_name = acl_name, src_sgt = src_sgt, dst_sgt = dst_sgt)
    with iosxe_connect(host, port=830, user=user, password=password) as m:
        m.edit_config(target='running', config=confstr)

if __name__ == '__main__':
    update_rbac(sys.argv[1], sys.argv[2], sys.argv[3], sys.argv[4], sys.argv[5], sys.argv[6])
```

# Device Programmability in action:

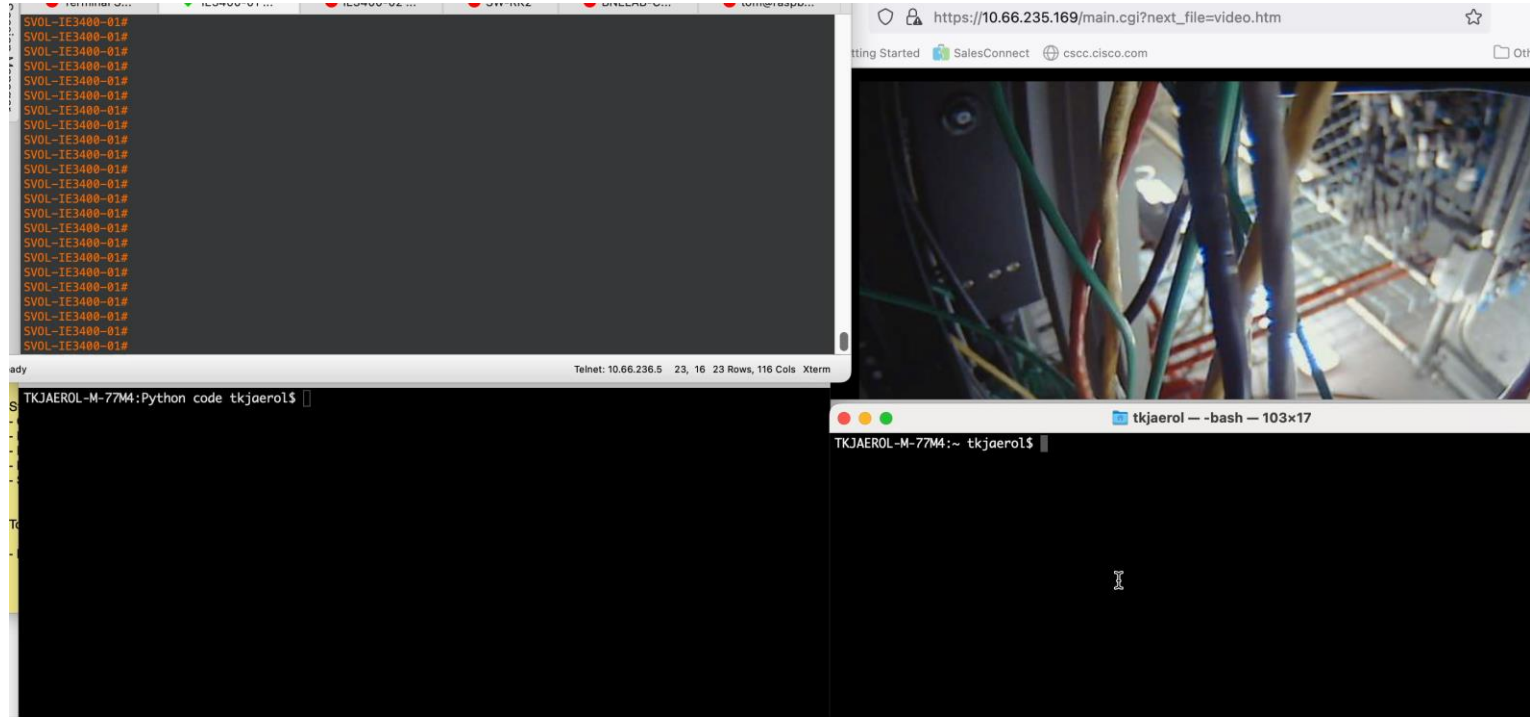
Using ncclient we will:

1. Block external access/unknown devices from cameras (Except SSH)
2. Block east/west traffic flows





# Device Programmability in action pt1:



# Device Programmability in action pt2:



The screenshot shows a terminal window with a yellow background. The prompt is `tom@raspberrypi:~ $`. The terminal is mostly empty, with a mouse cursor visible. Below the terminal window, there is a status bar showing `ssh2: AES-256-CTR 1, 21 23 Rows, 116 Cols Xterm`. Below the status bar, there is a black terminal window with a prompt `TKJAEROL-M-77M4:Python code tkjaerol$`. The bottom of the image shows a date and time stamp: `13 November 2022 at 10:42 pm`.

# Speedrun Recap

- Setting up DNA-C for PnP
- Day0 PnP via DNAC
  - Drive via GUI or RESTAPI
  - Utilise REP ZTP
- DayN template
  - Using tags
- Direct device programmability
  - ncclient for netconf/yang
- Using TrustSec for microsegmentation at the edge

# Questions?

Demo code all here:

<https://github.com/tkj-scythe/clmel-devnet1243>

# Session Surveys

We would love to know your feedback on this session!

- Complete the session surveys in the Cisco Events mobile app. You'll earn some points in the Cisco Live Game and potentially win a prize.
- Complete a minimum of four session and the overall event surveys to claim a Cisco Live cable bag.

# Continue your education



Visit the Cisco Showcase for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs



Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](https://www.CiscoLive.com/on-demand)

# Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. [www.cisco.com/go/certs](http://www.cisco.com/go/certs)

## Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



## Learn

### Cisco U.

IT learning hub that guides teams and learners toward their goals

### Cisco Digital Learning

Subscription-based product, technology, and certification training

### Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

### Cisco Learning Network

Resource community portal for certifications and learning



## Train

### Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

### Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

### Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



## Certify

### Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

### Cisco Guided Study Groups

180-day certification prep program with learning and support

### Cisco Continuing Education Program

Recertification training options for Cisco certified individuals





The bridge to possible

# Thank you

**CISCO** *Live!*

DevNet Zone

#CiscoLiveAPJC



CISCO *Live!*

ALL IN

#CiscoLiveAPJC