

# Simplifying workspace design with zero touch provisioning

**cisco** Live !

Paulo Jorge Correia  
Principal Solutions Engineer, @paucorre

# Cisco Webex App

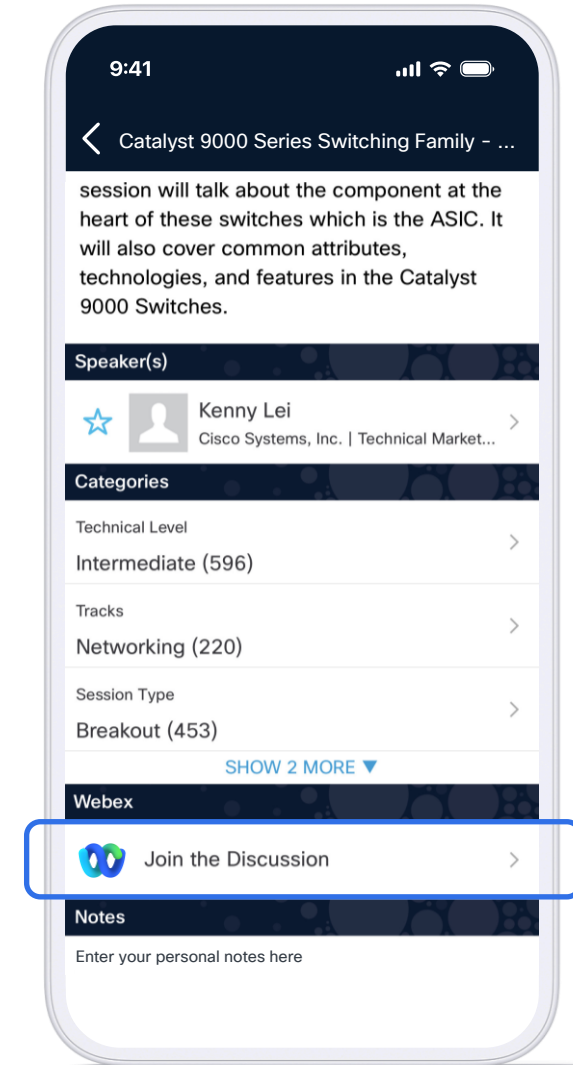
## Questions?

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 14 November 2025.**



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKCOL-2562>

# Agenda

- 01 Introduction
- 02 AVoIP for room accessories
- 03 Zero Touch Network Onboarding  
In a Zero Trust Architecture
- 04 Zero Trust Provision
- 05 Zero Touch Activation
- 06 Bringing it all up together with  
ISE and Webex CH
- 07 Key takeaways

# Introduction

# Why do we need Zero Touch Provisioning (ZTP) ?

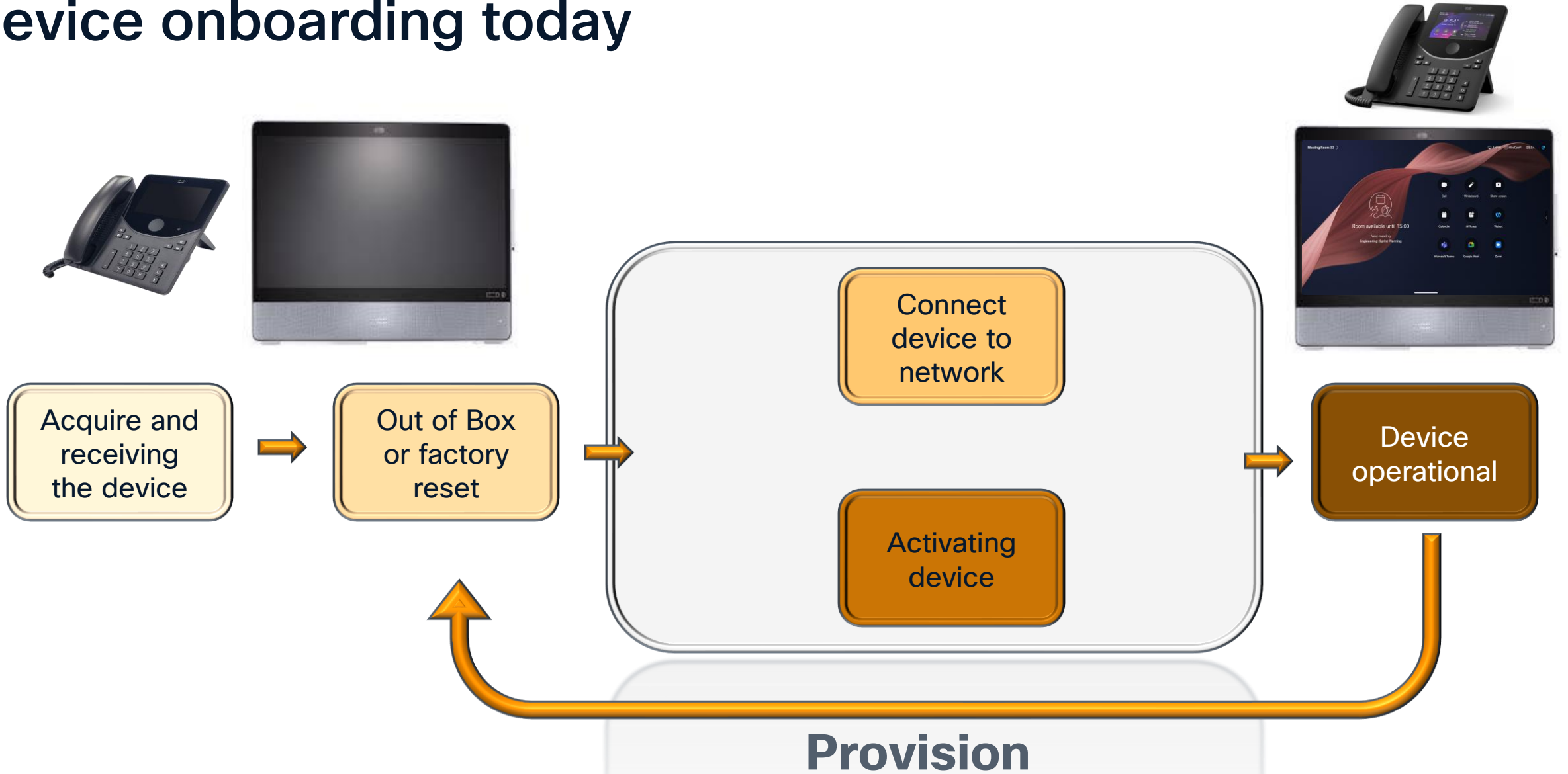


Simply plug in the device(s) to get onboarded to a functional state.

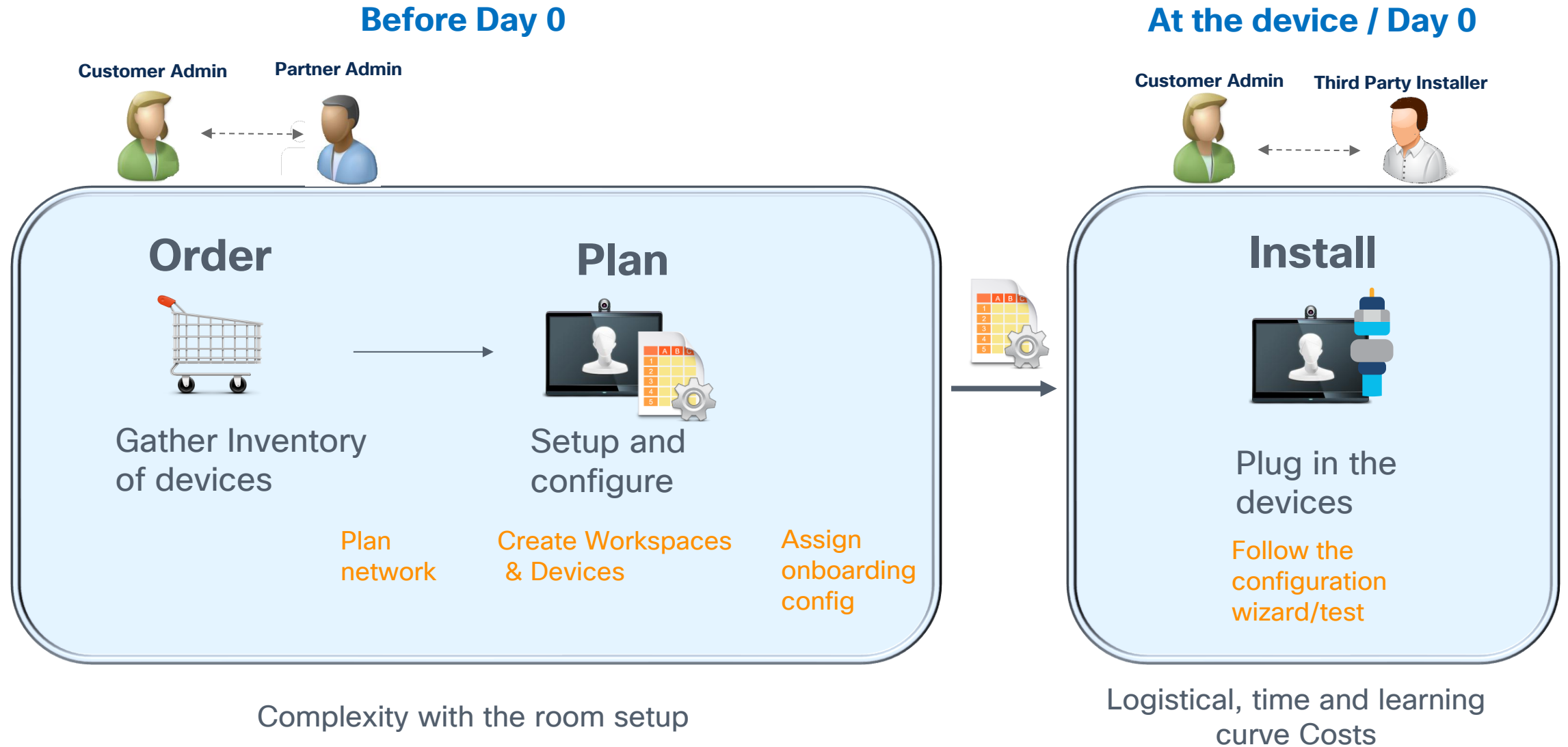
- Done in **Bulk and Automated** where possible
- Preconfigure: **minimal manual interaction** at the device
- **No need for tech savvy installer** (Audio/Video or/and Network) in the process



# Device onboarding today



# Challenges of provisioning at scale



# How we deal with AVoIP accessories

Cisco collab devices have traditionally used a local network to isolate locally deployed accessories from the corporate network.

These accessories can be from Cisco, an OEM to Cisco or other 3<sup>rd</sup> party products and to not necessarily offer the level of network security that is required for deployment on a corporate network like proper API authentication and media encryption.

Examples for such accessories are:

- Cameras (control via eth, media via HDMI)
- Cameras with video-over-IP
- Touch controller
- Microphones (AES67)

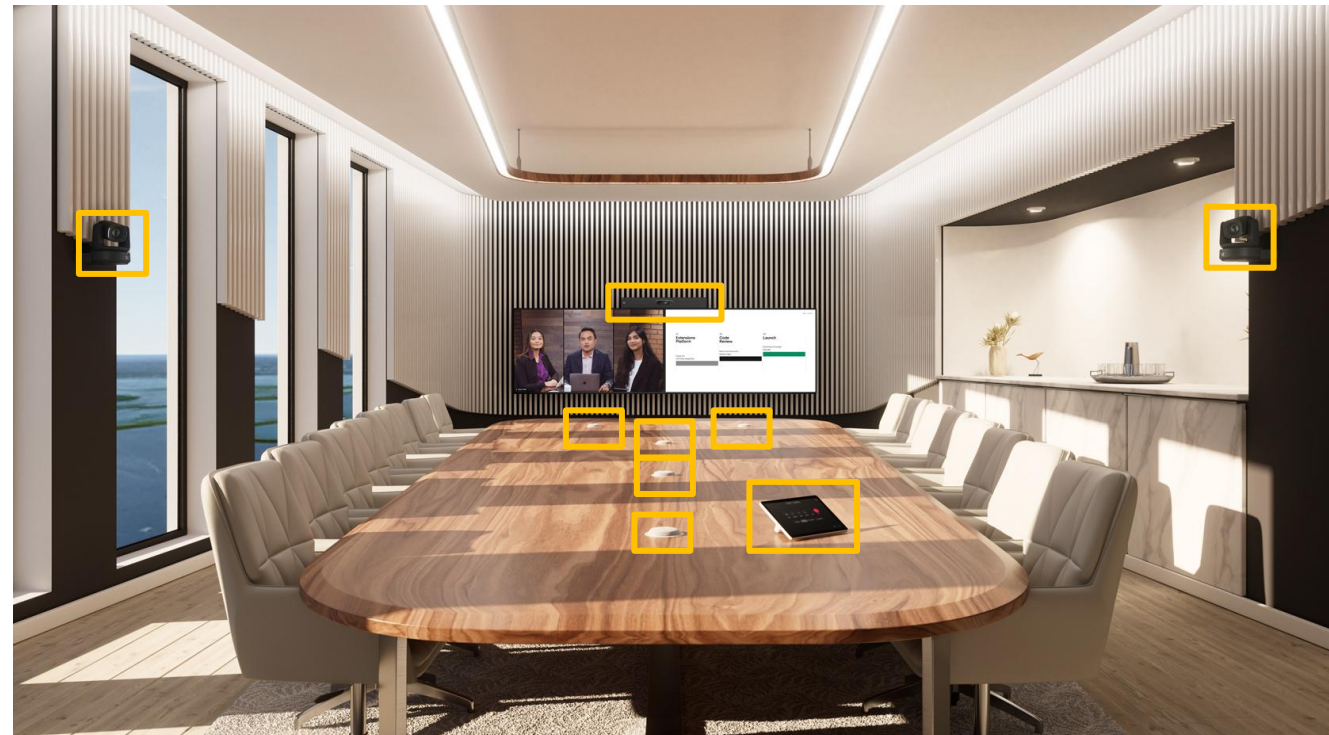


# What is the problem today ?

The market is changing from dedicated AV cables to Ethernet, Cisco is changing with the market and now we have deployments with more than 4 “private” ethernet interfaces.

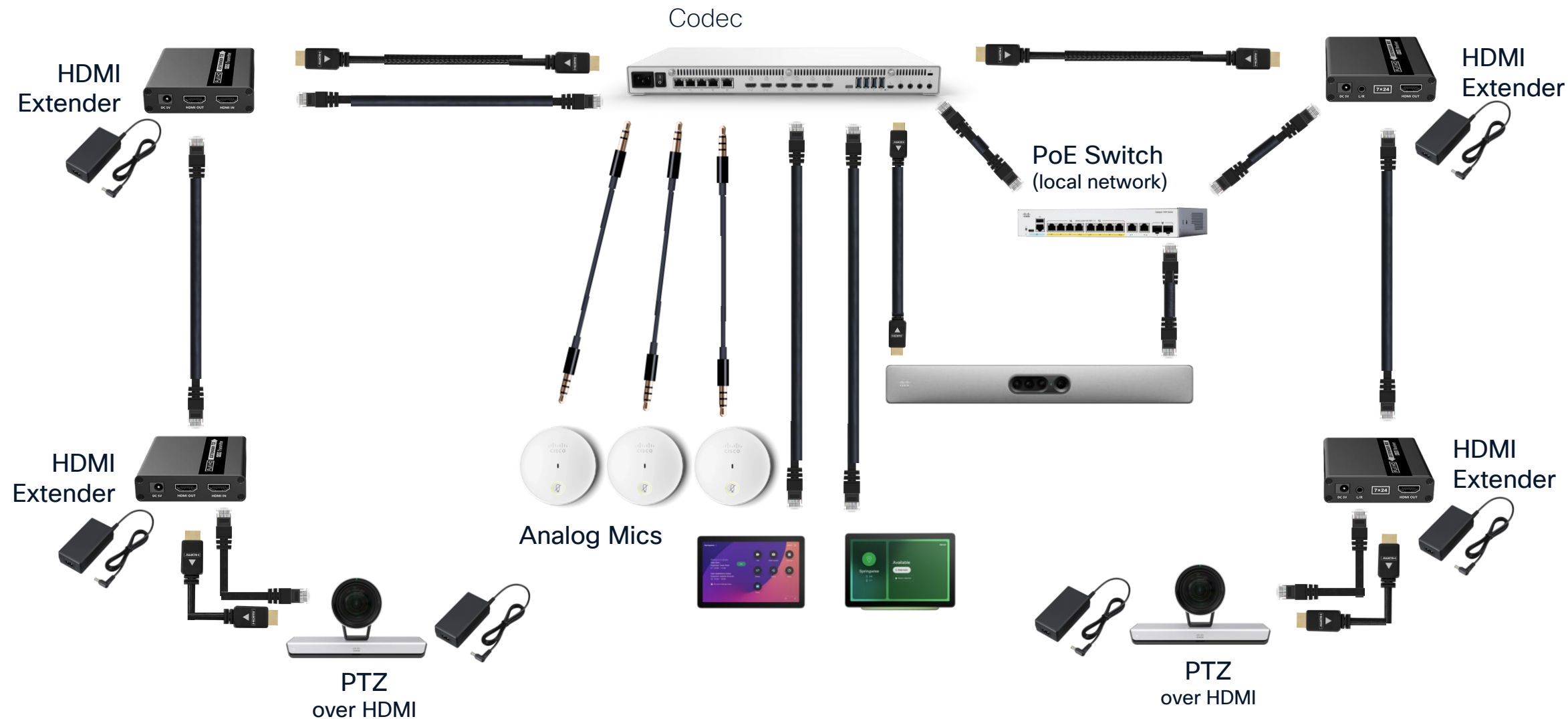
Example of a today deployable room system accessories:

- 5 Mic Pro
- 1 Table Navigator
- 1 Outside Navigator
- 1 Main Camera
- 2 lateral cameras
- 10 “private” Ethernet devices



# **AVoIP for room accessories**

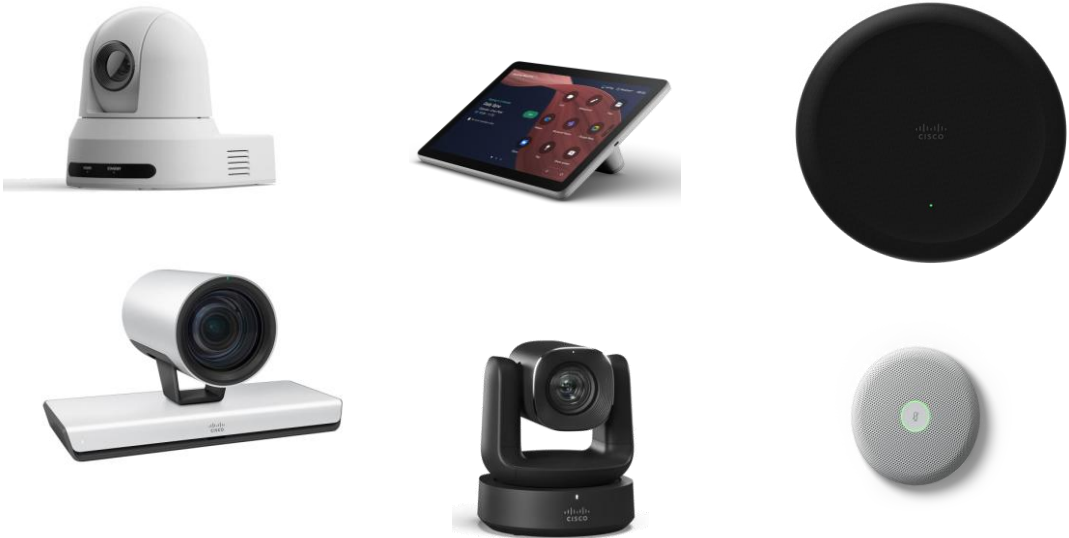
# Traditional AV Approach



# What kind of accessories are Room Devices are we talking about ?

## Ethernet Connected Accessories

|                 |                                                                           |
|-----------------|---------------------------------------------------------------------------|
| Control Only    | Navigator (Table & Wall), Precision 60 Camera, Quad Camera, PTZ 4K Camera |
| Control + AVoIP | Table Microphone Pro, Ceiling Microphone Pro, Room Vision PTZ             |

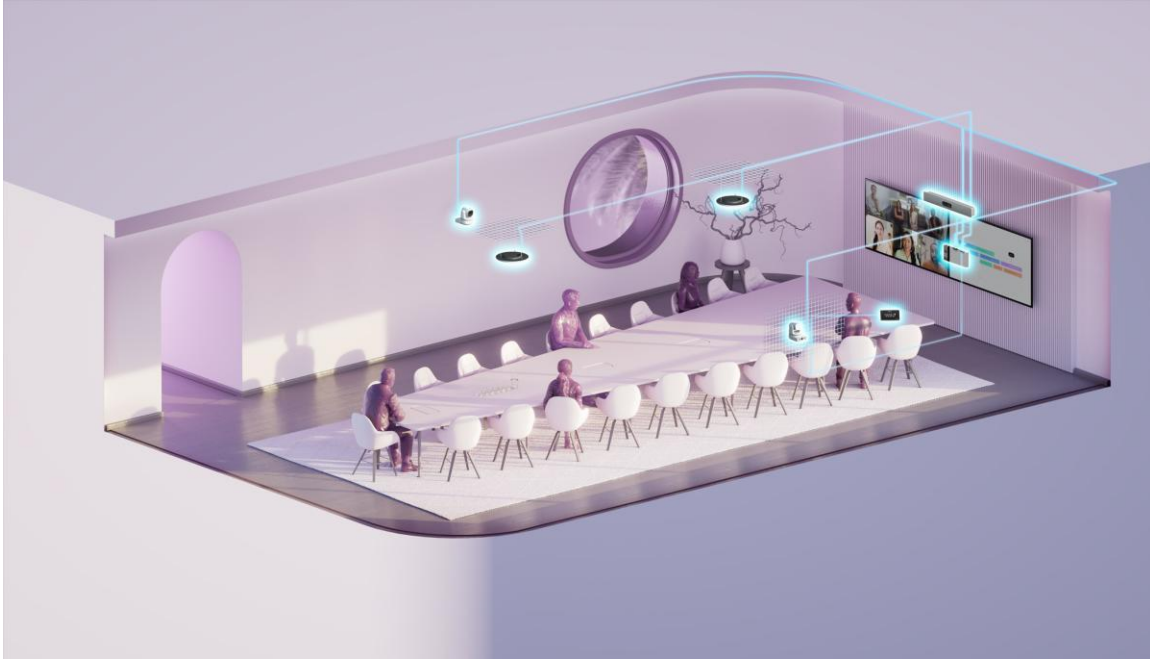


## Room Devices that supports Cisco AvoIP Accessories

| Bars         | Boards       | Integrated Systems | Integrator Codecs |
|--------------|--------------|--------------------|-------------------|
| Room Bar     | Board Pro G1 | Room Kit EQX       | Codec EQ          |
| Room Bar Pro | Board Pro G2 | Room Kit Panorama  | Codec Pro         |



# Assumptions



- Customer **network management and security team don't allow "rogue" devices** to deployed in their premises.
- Customer want to leverage additional network feature to optimize IP traffic from accessories to the codecs
- Customer want **warranties of network performance** for video devices IP accessories
- Customer would like support and maintenance guarantees from single vendor

# Scale and manage your meeting spaces over the network

Extend your AV accessories and simplify deployment over the enterprise network with  
**IP-connected collaboration devices and managed network switches from Cisco**

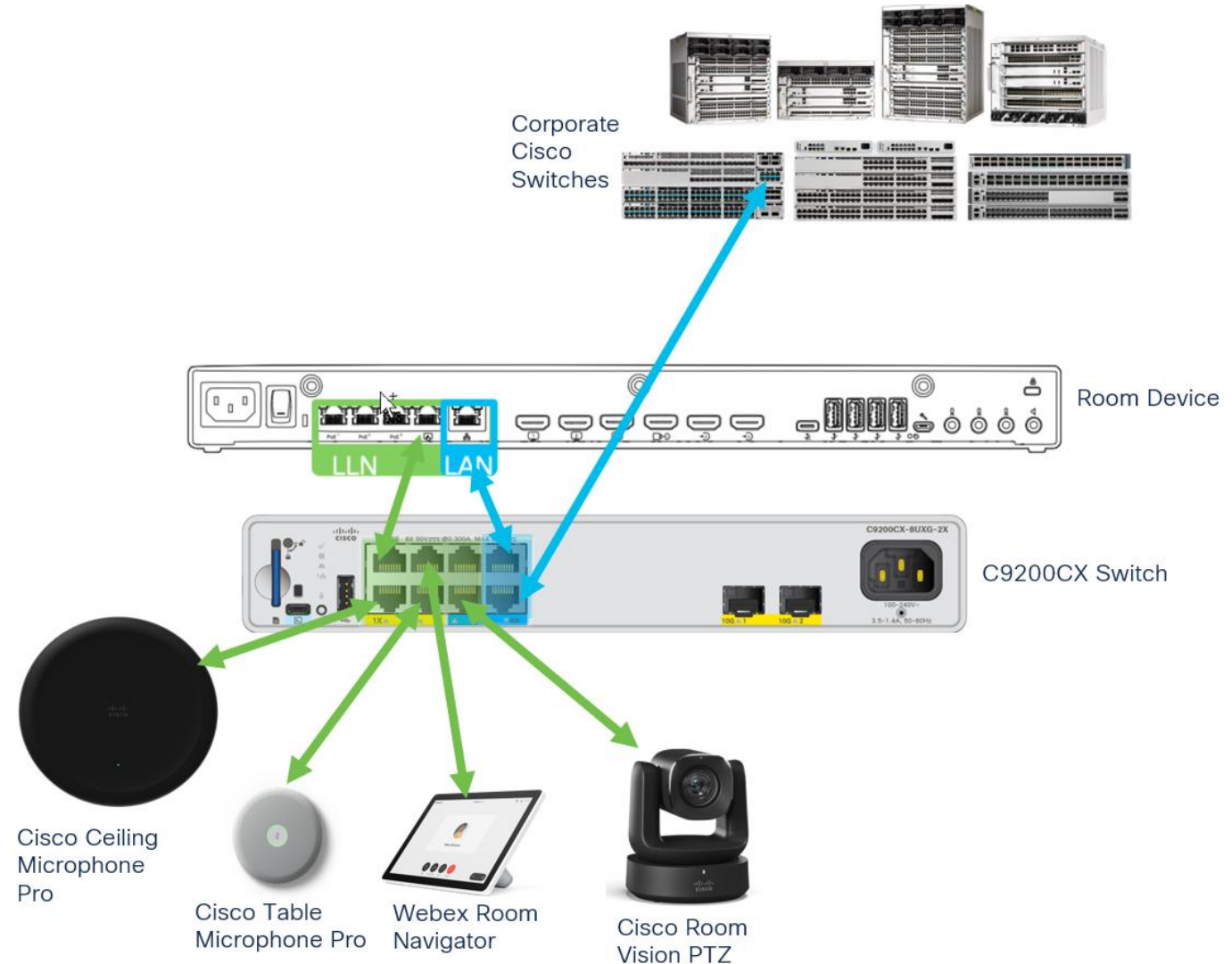


**NETWORK ACCESSIBILITY | SWITCH VISIBILITY IN CONTROL HUB  
SIMPLE AV DEPLOYMENT | ENHANCED SECURITY | REMOTE MONITORING**

# Better story between Video device and Cisco switches

Single ethernet cable to the room with C9200CX managed switch

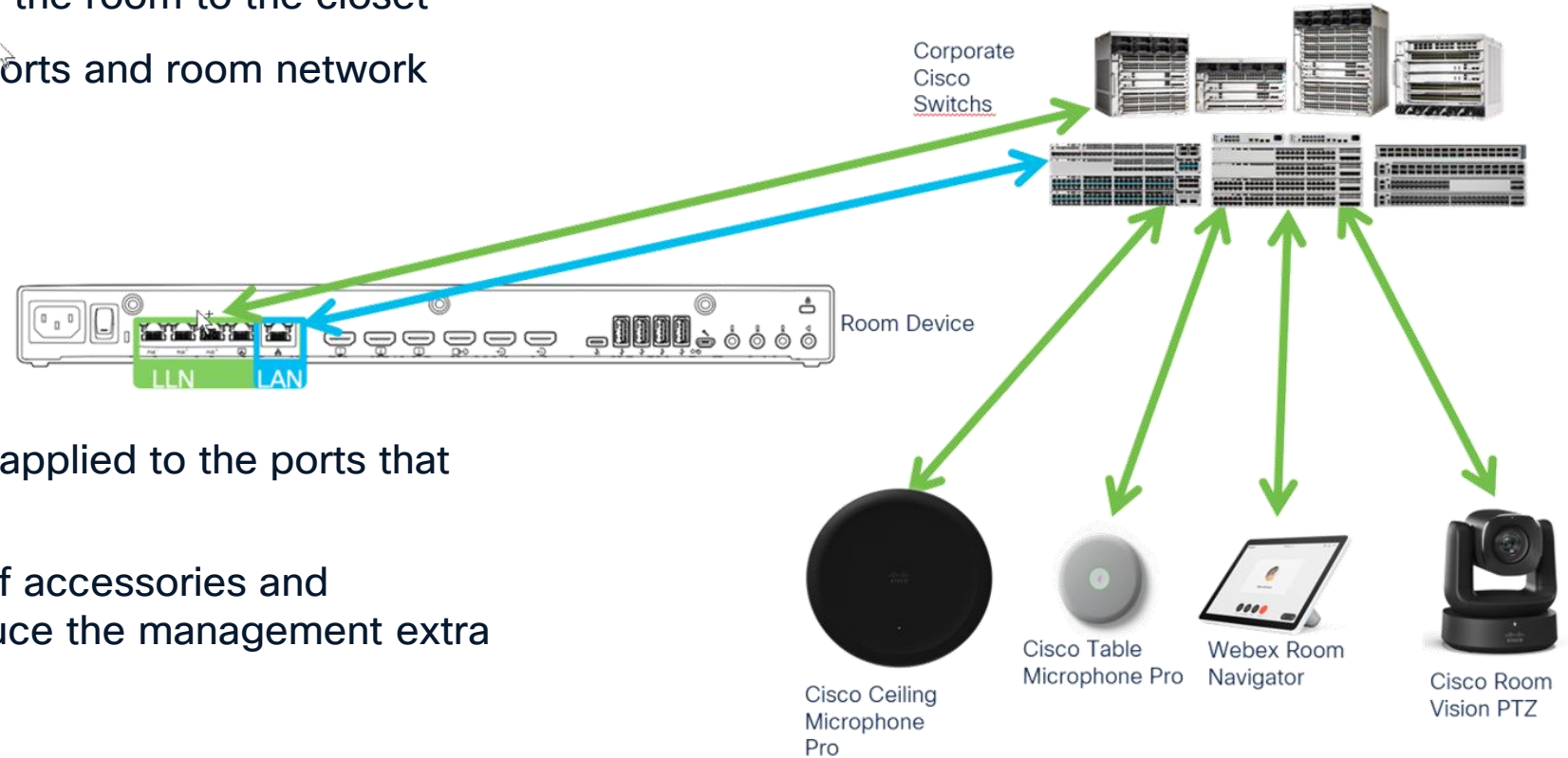
- All switch are managed by Catalyst Center, Merak dashboard or 3<sup>rd</sup> party management platform
- Switch will be configured from the management platform according to the recommended configuration shared in the CVD
- LLN (Link-Local Network) is an isolated VLAN that is not passed to the Corporate network.
- Accessories can use either LLN (Link-Local Network) ports in the Codec or in the switch.



# Better story between Video device and Cisco switches

All cables to the distribution switch

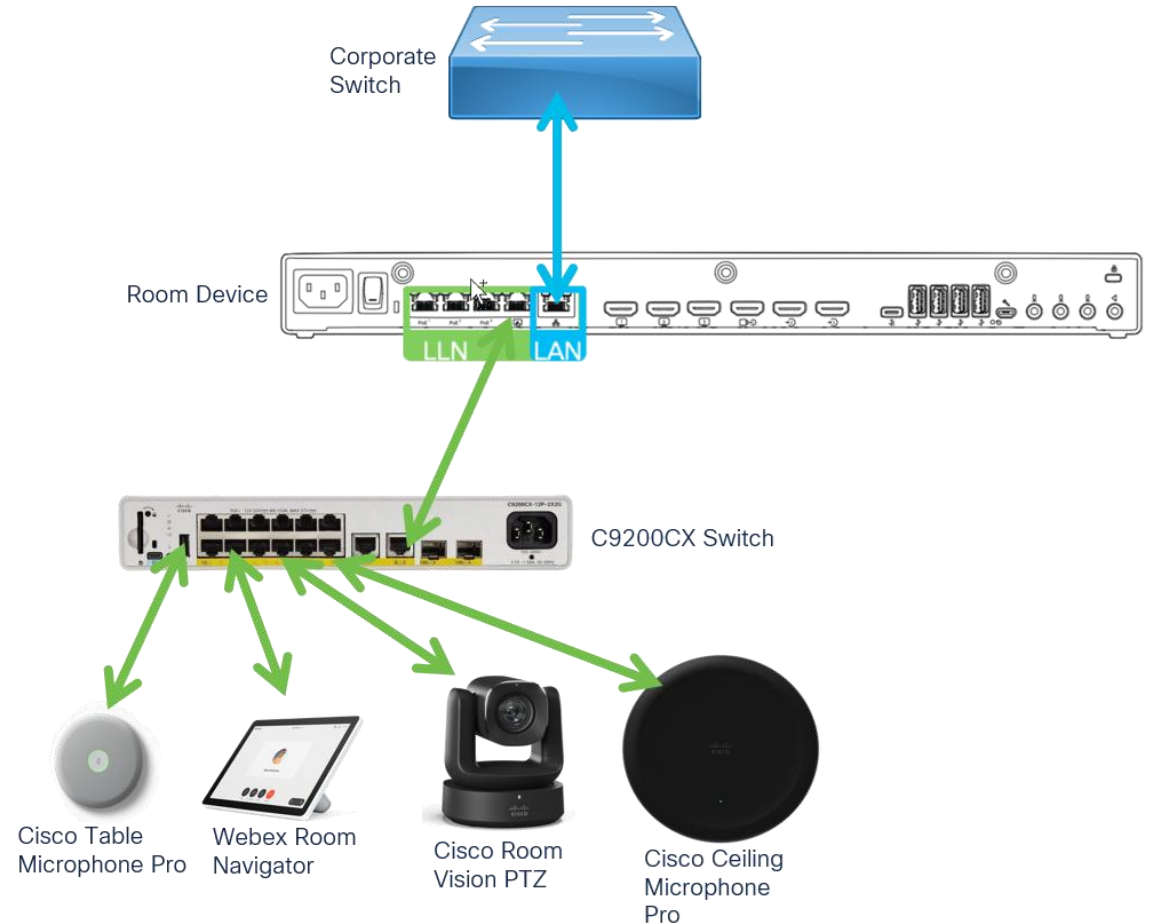
- Requires many network ports from the room to the closet
- Manual mapping between closet ports and room network plug
- Configuration templates would be applied to the ports that are allocated to an accessory
- In the future automatic detection of accessories and automatic configuration might reduce the management extra work



# Better story between Video device and Cisco switches

## Unmanaged switch (Option 1)

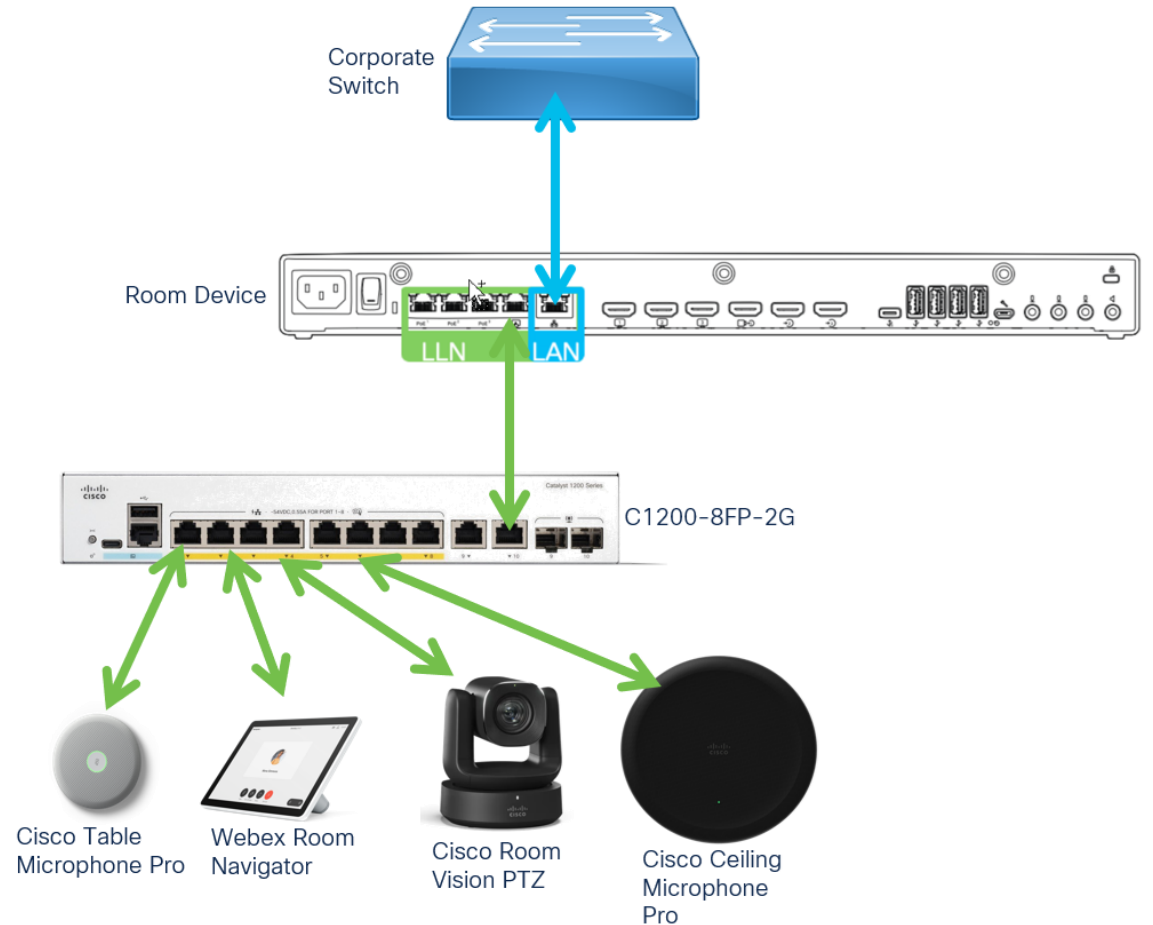
- Typical scenario for customers where there is some freedom and basic network knowledge for the AV team.
- Switch would not be visible from the network, it would join and be hidden behind the LLN in the codec.
- Only room Accessories would be able to have IP services
- **In the future** automatic detection of accessories and automatic configuration might reduce the management extra work and any kind of network knowledge from AV team.



# Better story between Video device and Cisco switches

## Unmanaged switch (Option 2)

- Typical scenario for customers where there is some freedom for the AV team.
  - Switch would not be visible from the network, it would join and be hidden behind the LLN in the codec.
  - Only room Accessories would be able to have IP services
- 
- No switch management, security fixes, or any kind of software upgrades would be possible without manual Intervention from network teams
  - Very cheap network solution



# Catalyst 9200CX Family

## PoE+ and Data Models

### C9200CX-12P-2X2G



- 12 x 1G PoE+
- 2 x 1G copper and 2 x SFP+ uplinks
- Internal AC power supply
- 240W PoE power budget

### C9200CX-8P-2X2G



- 8 x 1G PoE+
- 2 x 1G copper and 2 x SFP+ uplinks
- Internal AC power supply
- 240W PoE power budget

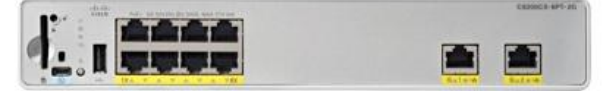
### C9200CX-12T-2X2G



- 12 x 1G data
- 3 x 1G copper and 2 x SFP+ uplinks
- External power adapter (80W)
- 802.3bt Class 6 powered (60W)

## Pass-through Model

### C9200CX-8PT-2G



- 8 x 1G PoE+
- 2 x 1G copper & UPOE+ uplinks
- External power adapter (80W/150W) [LVDC support] & 802.3bt UPOE+ ULs
- 240W Max PoE power budget

## mGig/UPOE

### C9200CX-8UXG-2X



- 4x mGig/10G + 4 x 1G (802.3bt Type 3 Class 6 60W all ports)
- 2x 1/10G SFP+
- Internal AC power supply
- 240W PoE power budget

### C9200CX-12P-2X2GH



- 12 x 1G PoE+
- 2 x 1G copper and 2 x SFP+ uplinks
- Internal HVDC power supply
- 240W PoE power budget

### C9200CX-8P-2X2GH



- 8 x 1G PoE+
- 2 x 1G copper and 2 x SFP+ uplinks
- Internal HVDC power supply
- 240W PoE power budget

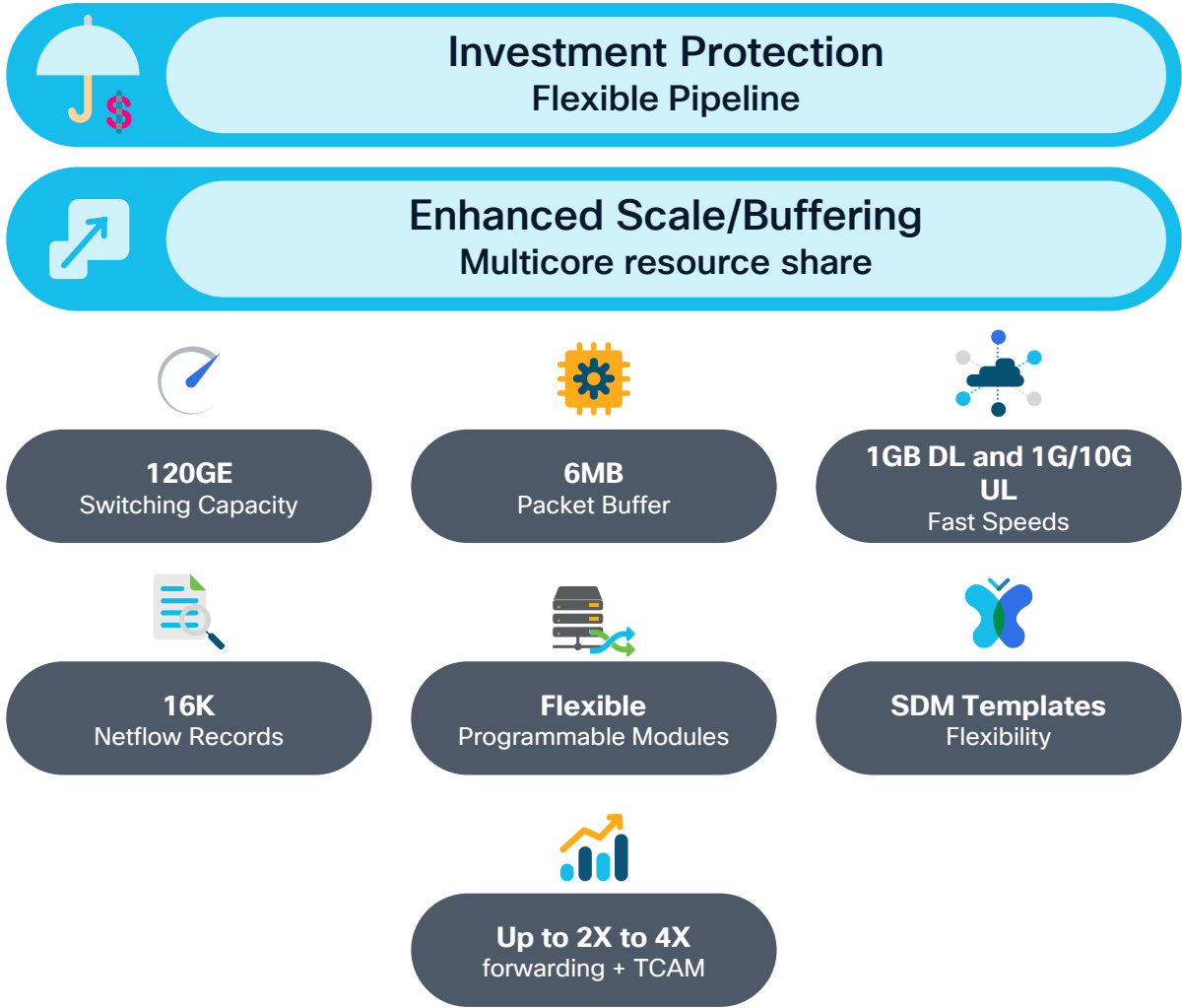
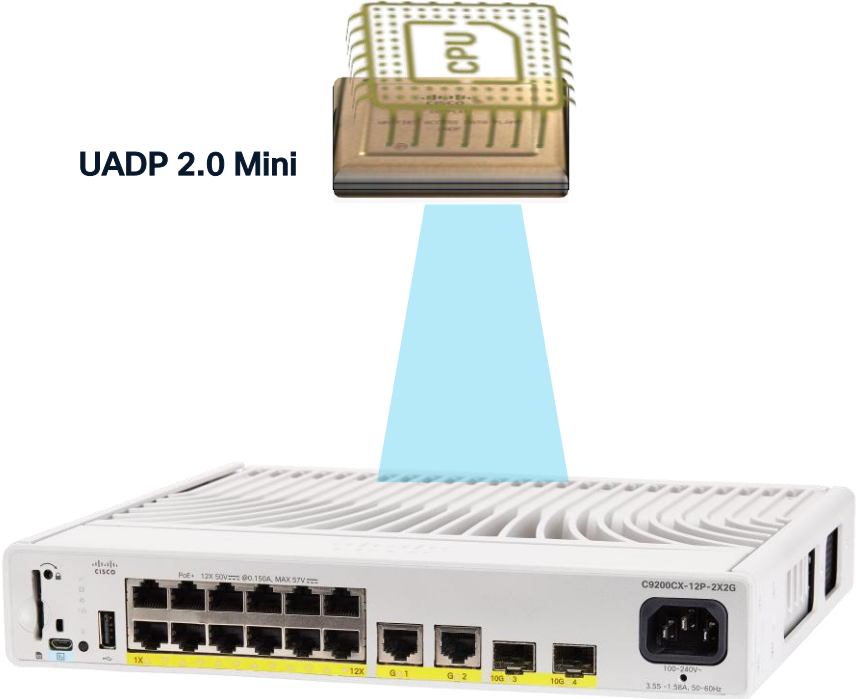
### C9200CX-8UXG-2XH



- 4x mGig/10G + 4 x 1G (802.3bt Type 3 Class 6 60W all ports)
- 2x 1/10G SFP+
- Internal HVDC power supply
- 240W PoE power budget

## HVDC Models

# Architectural simplicity with powerful innovations



# Network discovering Cisco collaboration devices

- Cisco Discovery Protocol (CDP) is link layer protocol to discover network device identities, capabilities and neighbours on local area network
- The Link Layer Discovery Protocol (LLDP) is a vendor-neutral, Layer 2 protocol used by network devices to advertise their identity, capabilities, and neighboring devices on a local area network (LAN). It is formally specified by the IEEE as 802.1AB.



```
C9200-Home#sh lldp neighbors Gig 1/0/2 detail
-----
Local Intf: Gi1/0/2
Local Intf service instance: -
Chassis id: 198.18.9.11
Port id: 845A3EC25CA4:P1
Port Description: SW PORT
System Name: SEP845A3EC25CA4.dcloud.cisco.com

System Description:
Cisco IP Phone 9871, V1, PHONEOS.3-4-1-0002-50

Time remaining: 139 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses:
  IP: 198.18.9.11
Auto Negotiation - supported, enabled
Physical media capabilities:
  1000baseT(FD)
  100base-TX(FD)
  100base-TX(HD)
  10base-T(FD)
  10base-T(HD)
Media Attachment Unit type: 30
Vlan ID: - not advertised
Peer Source MAC: 845a.3ec2.5ca4

MED Information:

  MED Codes:
    (NP) Network Policy, (LI) Location Identification
    (PS) Power Source Entity, (PD) Power Device
    (IN) Inventory

  H/W revision: 1
  F/W revision: sb2-9861 71.EM-01-009
  S/W revision: PHONEOS.3-4-1-0002-50
  Serial number: FVH28242JYF
  Manufacturer: Cisco Systems, Inc.
  Model: DP-9871
  Capabilities: NP, PD, IN
  Device type: Endpoint Class III
  Network Policy(Voice): VLAN 320, tagged, Layer-2 priority: 5, DSCP: 46
  Network Policy(Voice Signal): VLAN 320, tagged, Layer-2 priority: 3, DSCP:
6
  PD device, Power source: PSE, Power Priority: Unknown, Wattage: 12.5
  Location - not advertised

Total entries displayed: 1
```

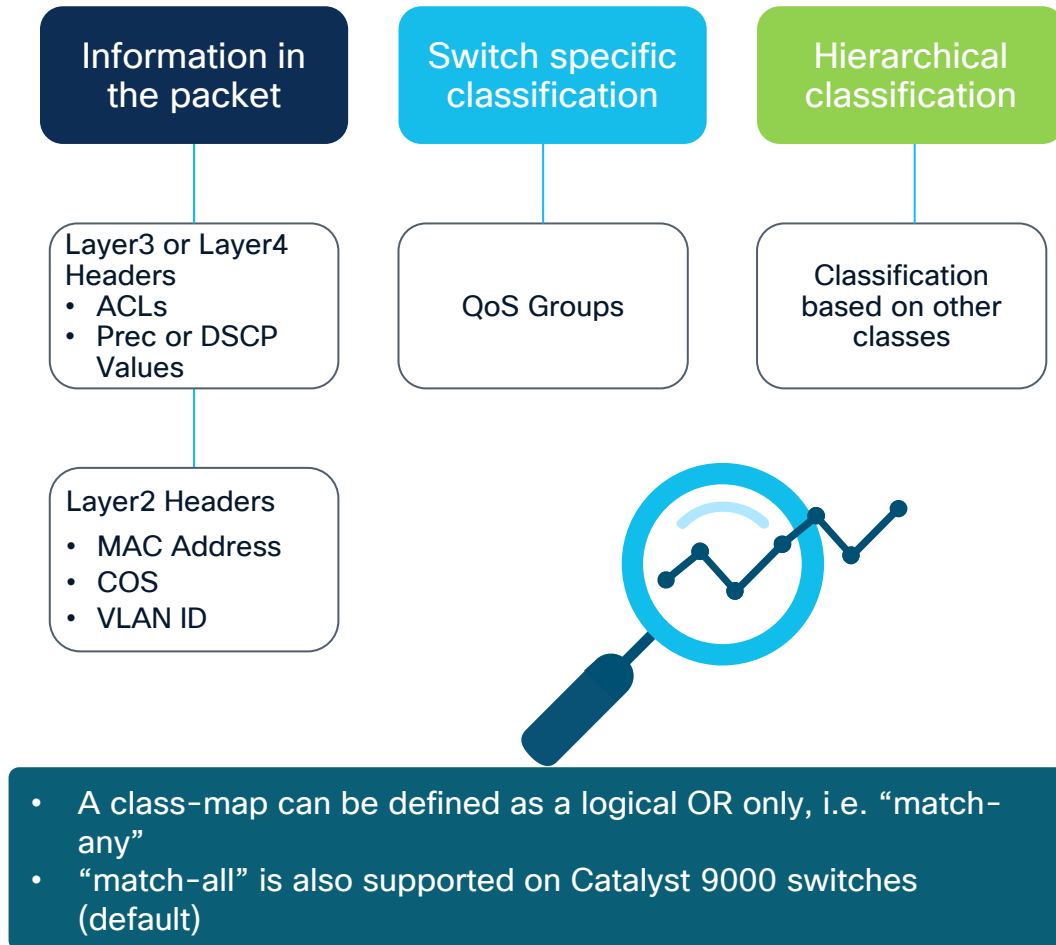
```
C9200-Home#sh cdp neighbors Gig 1/0/2 detail
-----
Device ID: SEP845A3EC25CA4
Entry address(es):
  IP address: 198.18.9.11
Platform: Cisco IP Phone 9871, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): Port 1
Holdtime : 171 sec
Second Port Status: Down

Version :
PHONEOS.3-4-1-0002-50

advertisement version: 2
Peer Source MAC: 845a.3ec2.5ca4
Duplex: full
Power drawn: 13.398 Watts
Power request id: 42078, Power management id: 4
Power request levels are:13398 0 0 0 0

Total cdp entries displayed : 1
```

# QoS Packet classification



```
switch(config-cmap)# class-map match-any VOICE
switch(config-cmap)#match ?
access-group  Access group
any           Any packets
class-map     Class map
cos           IEEE 802.1Q/ISL class of service/user priority values
dscp          Match DSCP in IPv4 and IPv6 packets
group-object  Match object-group
ip            IP specific values
mpls          Multi Protocol Label Switching specific values
non-client-nrt Match non-client NRT
precedence    Match Precedence in IPv4 and IPv6 packets
protocol      Protocol
qos-group     Qos-group
vlan          VLANs to match
wlan          802.11-specific values
```

# QoS Marking



Conditional  
Policer  
based marking



Unconditional  
Explicit marking



Table Map  
based marking

Marking with 'set'  
Marking with Table Maps

```
Catalyst9200CX(config-pmap-c)#set ?
cos      Set IEEE 802.1Q/ISL class of service/user priority
dscp     Set DSCP in IP(v4) and IPv6 packets
ip       Set IP specific values
precedence Set precedence in IP(v4) and IPv6 packets
qos-group Set QoS Group
wlan     Set WLAN
```

[class-maps omitted for brevity]

```
policy-map MARKING-POLICY
class VOIP
  set dscp ef
class MULTIMEDIA-CONFERENCING
  set dscp af41
class SIGNALING
  set dscp cs3
class TRANSACTIONAL-DATA
  set dscp af21
class BULK-DATA
  set dscp af11
class SCAVENGER
  set dscp cs1
class default
  set dscp dscp table COS2DSCP
```

```
table-map COS2DSCP
map from 5 to 46
default copy
```

# Cisco innovations in PoE deliver a robust low voltage infrastructure

## 2-event classification

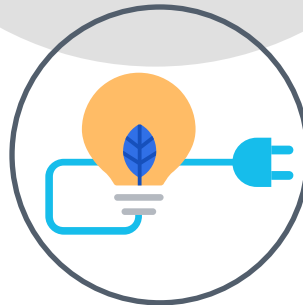
- Fast power negotiation without LLDP
- Physical layer negotiation < 1s

## Perpetual PoE

- Uninterrupted PoE power during control plane reboot

## Fast PoE

- Bypasses IOS control plane boot
- Restores power to PD within 30 sec of power resumption



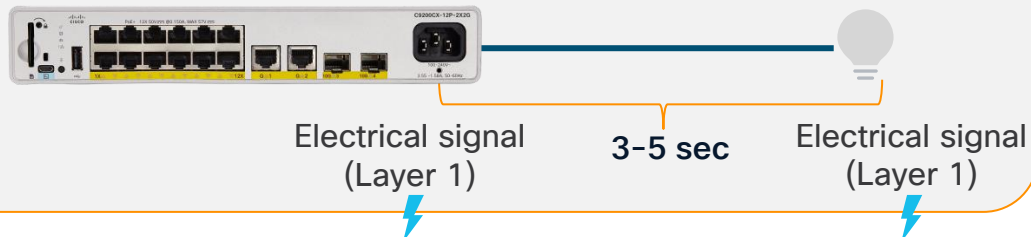
# 2-Event classification



## Without 2-Event Classification



## With 2-Event Classification (Hardware Based)

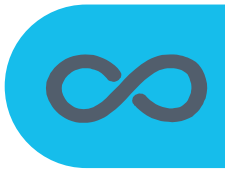
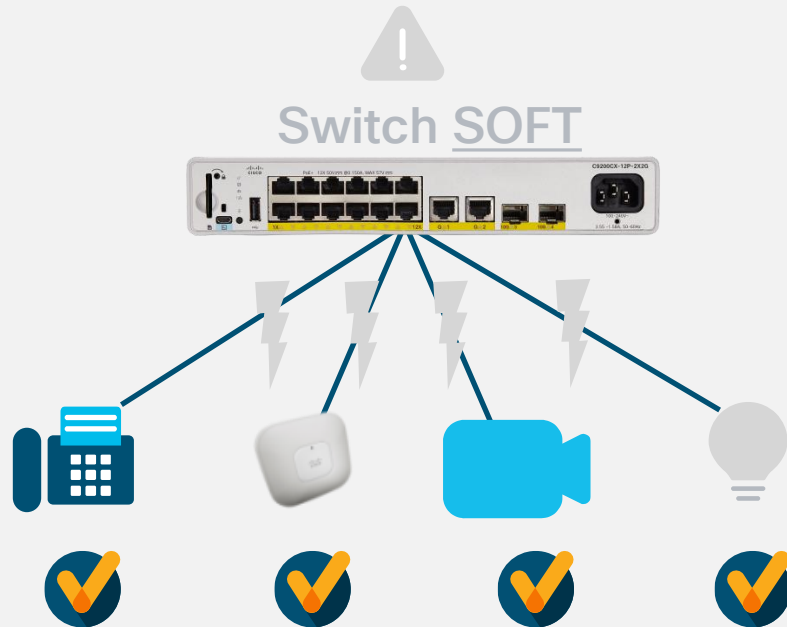


```
Switch> enable
Switch# configure terminal
Switch(config)# interface
gigabitethernet1/0/1
Switch(config-if)#
power inline port 2-event
Switch(config-if)# end
```

- Class 4 PD gets 30W even before the link comes up, otherwise 15.4W
- Type-2 PSE sends classification voltage (2<sup>nd</sup> Handshake) pulse to Class 4 PD (PoE+, 12.96-25.5 W) confirming it is a high-power capable PSE
- 30W of power is allocated for PD (PD draws up to 25.5W)
- Both PSE and PD need to support 2-Event
- No waiting for CDP/LLDP exchange for PoE+ power levels

# Perpetual PoE

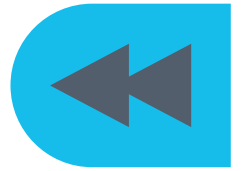
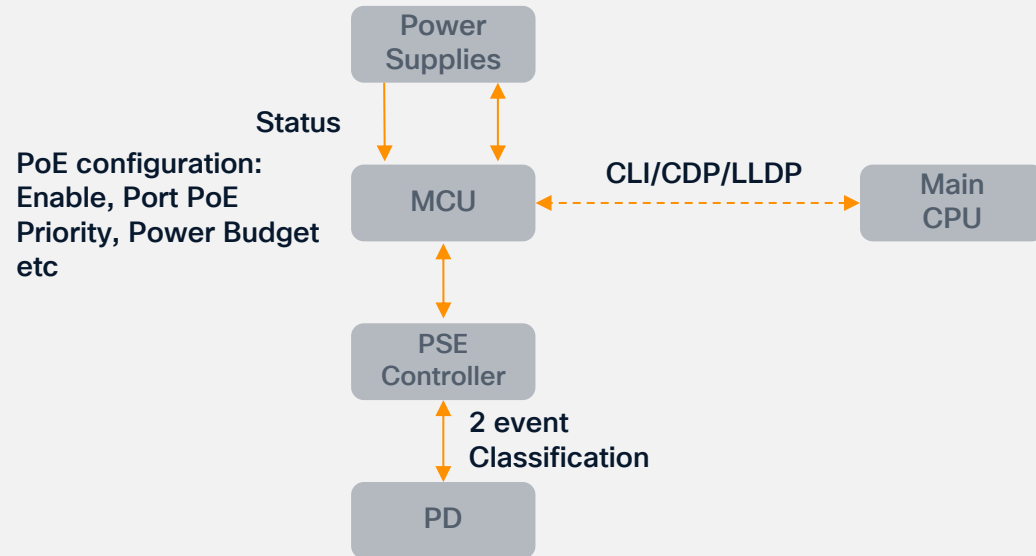
PoE devices connected to switch stay powered even on Switch Reload!



```
Switch> enable
Switch# configure terminal
Switch(config)# interface
gigabitethernet1/0/1
Switch(config-if)#
power inline port perpetual-poe-ha
Switch(config-if)# end
```

- PoE devices continue to get Last Negotiated Power
- Applicable to “Soft” Reload – image upgrade, software crash, manual reboot
- Not applicable during power outage to switch/FEP removed
- Not applicable when switch is in hibernation mode

# Fast PoE



```
Switch> enable
Switch# configure terminal
Switch(config)# interface
gigabitethernet1/0/1
Switch(config-if)#power inline port
perpetual-poe-ha
Switch(config-if)#power inline port poe-ha
Switch(config-if)# end
```

- Restores power to PD in less than 30 seconds post restoration of power
- Works even before IOS comes up
- Allocates last power (stored in NVRAM) drawn from PDs

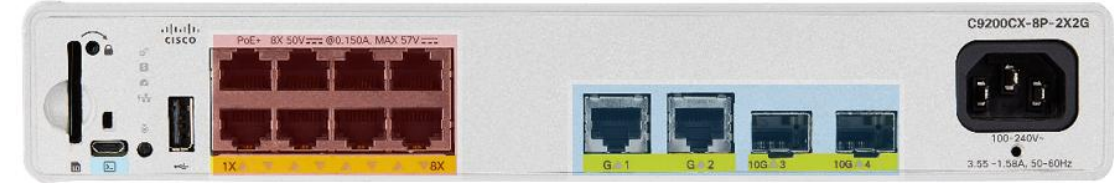
# Cisco C9200CX switches needs for AVoIP accessories

- With the recommended configuration we require 2 ethernet ports that are not on the (Link-Local Network), that can be done with regular ports or with SFP+ ports
- The ports in the LLN network should have POE except the one that connect to the LLN network in the codec.

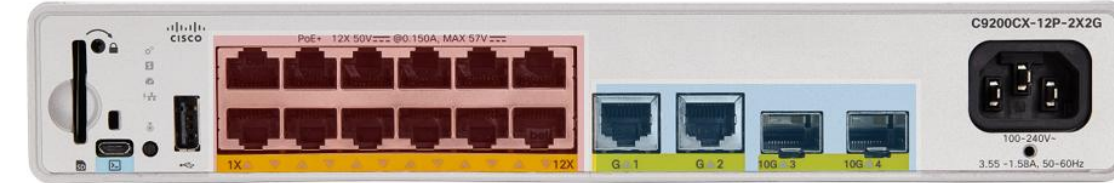


- Today we only require 1Gb POE ports for the AVoIP accessories and 1gb the LLN codec connection.

C9200CX-8P-2X2G



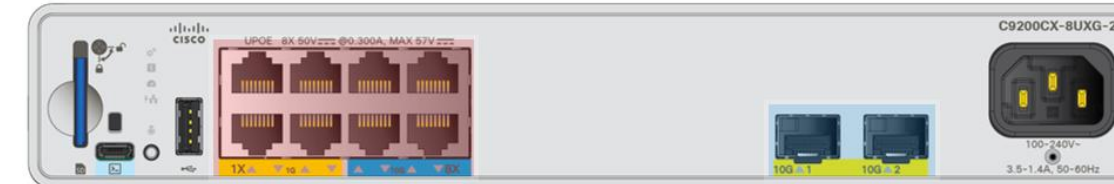
C9200CX-12P-2X2G



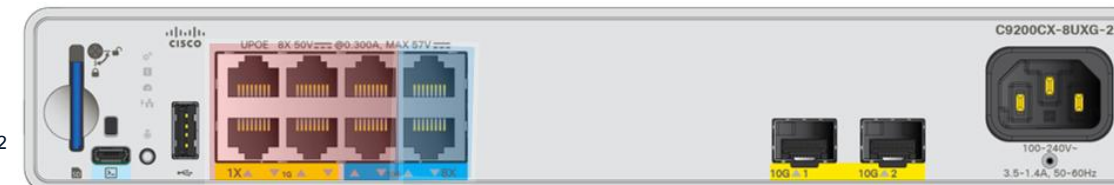
C9200CX-8PT-2G



C9200CX-8UXG-2X



OR



# Global configuration for the AVoIP accessories switch

- We need to enable LLDP for some accessories that don't have CDP
- The Switch should be configured for the VLAN trunking Protocol (VTP) to be in transparent mode.
- There should be a vlan that is not propagated to other switches, to create the LLN network outside the Codec.
- In the upstream port, make sure to block the AVoIP Accessories VLAN

```
! Enable LLDP for accessories
```

```
lldp run
```

```
! Don't pass the AVoIP accessories VLAN to the infrastructure
```

```
vtp mode transparent
```

```
! Vlan for AVoIP Accessories
```

```
vlan 100
```

```
name AVoIP_Accessories
```

```
! Make sure that the VLAN for Accessories is not passs to tother switches
```

```
interface GigabitEthernet1/1/1
```

```
description Connect to distribution switch
```

```
switchport trunk pruning vlan 100
```

```
switchport mode trunk
```

# QoS configuration for the AVoIP accessories

Create a custom QoS Policy map the the AVoIP accessories, with the follow rules:

- Priority 1 queue put PTP traffic
- Priority 2 queue put Audio traffic
- Allocated 65% of the remaining bandwidth, using a weighted fair queuing, to provide guaranteed bandwidth for video traffic.
- Allocated 35% of the remain bandwidth, serving all other traffic not matched by the above classes.

```
! Class-map to identify PTP traffic
class-map match-any vPTP
  match dscp ef

! Class-map to identify Audio traffic
class-map match-any Audio
  match dscp af41

! Class-map to identify Video traffic
class-map match-any Video
  match dscp af42
! Policy-map to assign the traffic to the right switching queues

policy-map AVoIPAccessories

! Priority 1 queue for PTP
class vPTP
  priority level 1

! Priority 2 queue for Audio
class Audio
  priority level 2

class Video
  bandwidth remaining percent 65

class class-default
  bandwidth remaining percent 35
```

# Switch Port Configuration

- We need one Port to extend the LLN from the Codec to the Switch, that port doesn't need PoE and should have the QoS policy created in the previous slide.
- We need a Port to connect to the Codec network interface, that port will get network in the Voice VLAN and will have a QoS policy for a video device, there is no need for PoE

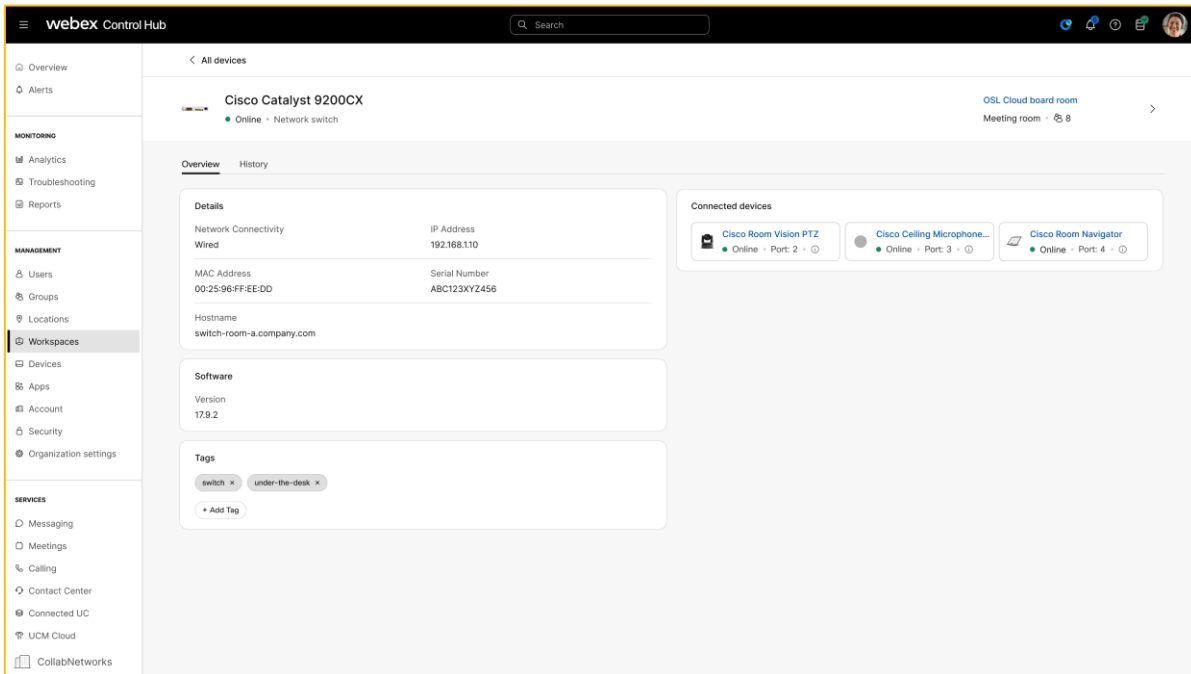
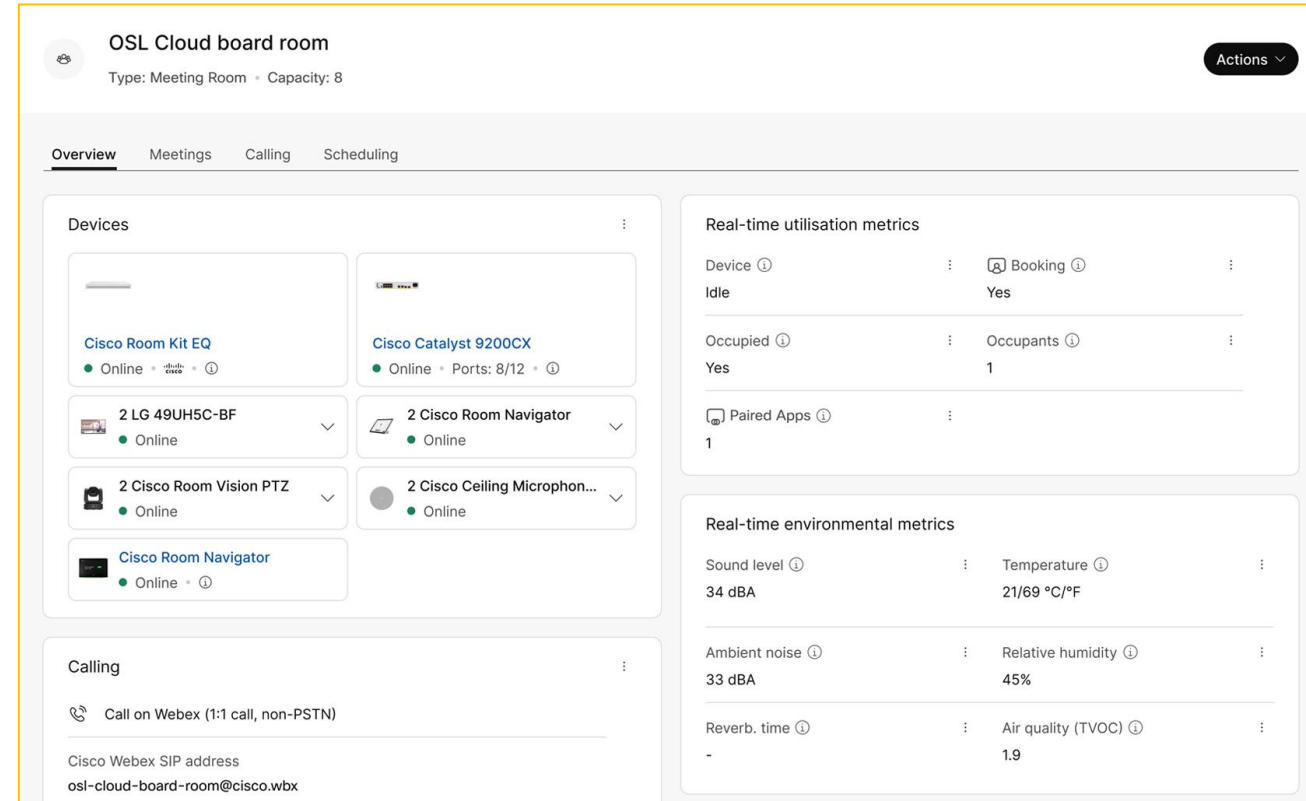
```
! Ports for AVoIP accessories
interface range GigabitEthernet1/0/2 - <6-12>
description AVoIP Accessory
switchport access vlan <AVoIP VLAN>
power inline port perpetual-poe-ha
power inline port poe-ha
service-policy output AVoIPAccessories
spanning-tree portfast
```

```
! Port for the link local interface of the Room Device
interface GigabitEthernet1/0/1
description Codec Link_Local interface
switchport access vlan <AVoIP VLAN>
service-policy output AVoIPAccessories
spanning-tree portfast
!
! Port for the Room Device to connect to the corporate VLAN for
voice/video traffic
interface TenGigabitEthernet1/0/7
description Codec network interface
switchport mode access
switchport voice vlan <VoiceVLAN>
auto qos video cts
spanning-tree portfast
```

All the AVoIP accessories will need to go the VLAN create for that propose and will need perpetual and fast PoE

# Rendering C9200CX switch information in Webex CH

C9200CX switch will be detected by the Codec through CDP and the information will be rendered in Webex CH, just like any other Accessory



In Webex CH there will be a page for the Switch that brings basic information (IOS version, MAC, IP address, AVoIP Accessories port location)

# Zero Touch Network Onboarding In a Zero Trust Architecture

# What is ZTP ?



Acquire and  
receiving  
the device

Out of Box  
or factory  
reset

Connect  
device to  
network

Activating  
device

Device  
operational

Provision

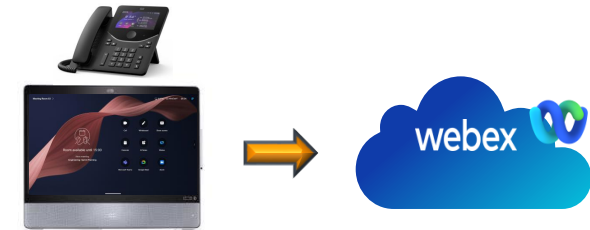
# What are the ZTP challenges ?



Connect  
device to  
network

## Zero Trust Provision (ZTP)

- No passwords, which is a trust dependency on people to secure and not share the secret.
- **Authorized devices only** – network admins choose which devices can join the network.



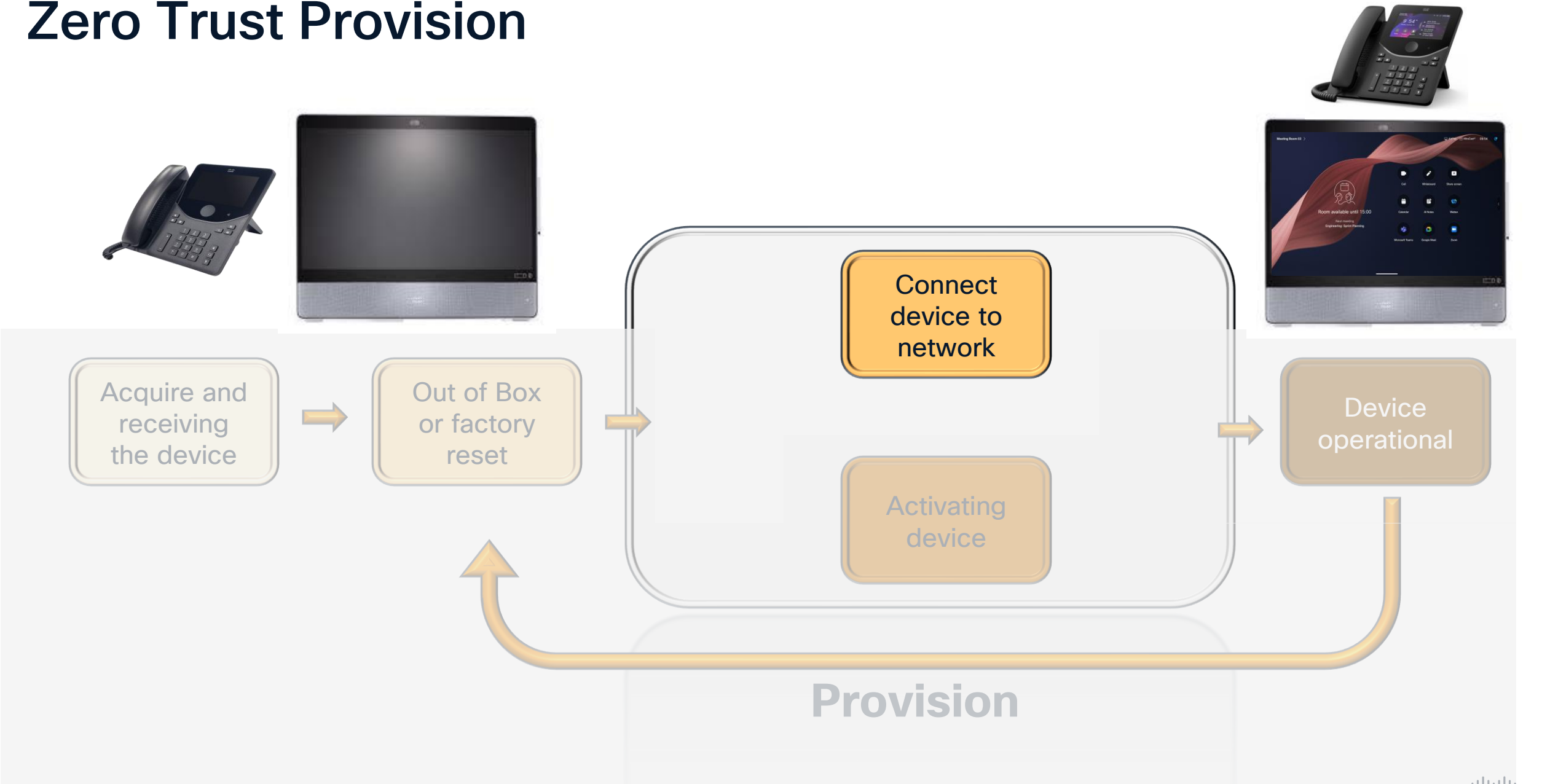
Activating  
device

## Zero Touch Provision (ZTP)

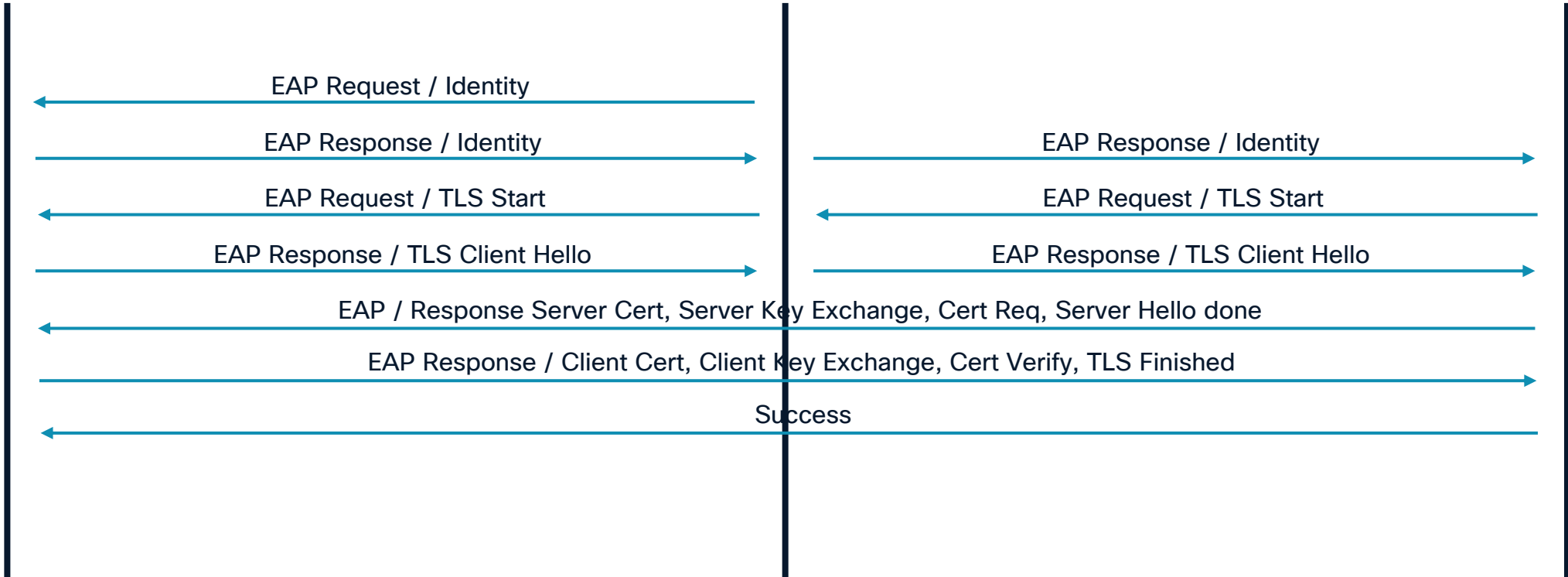
- The only touch needed is to plug in the cords and power on the device.
- No required access to SSH/TSH or device web page.
- The only configuration needed is **a list of devices (MACs/SNs) allowed on the network.**

# Zero Trust Provision

# Zero Trust Provision



# IEEE802.1X negotiation between Device and network Registrar



# What kind of Certificates are available in Cisco Collaboration devices out of the box ?

The **Secure Unique Device Identifier (SUDI)** in the device is an X.509 certificate that provides a factory-installed, unique device identity. The SUDI certificate is embedded in the device at manufacturing and serves as a trust anchor for secure device onboarding and authentication processes.

The **Manufacturing Installed Certificate (MIC)** in a video device is an X.509 digital certificate that is pre-installed by the manufacturer. The MIC works alongside the Cisco CA and Cisco Manufacturing CA certificates, which act as root certificates to validate the device identity.



**RoomOS Codecs**

**SUDI** – Secure Unique Device Identifier  
**MIC** – Manufacturing Installed Certificate



**RoomOS Navigator**

**SUDI** – Secure Unique Device Identifier



**PhoneOS**

**SUDI** – Secure Unique Device Identifier  
**MIC** – Manufacturing Installed Certificate

# Where did we start ?



**RoomOS Codecs**

Certificate would be generated off device and the admin would import the Public/Private key video device that after could be use for .1x AuthN



**PhoneOS**

The device could only do .1x with the MIC



**RoomOS Navigator**

Navigators can do .1x in remote pair in standalone modes with the same process as the Codes.

# Where are we now?



## RoomOS Codecs



## PhoneOS



## RoomOS Navigator

Certificates can be Obtained and Renew via SCEP, SCEP details can be provided manually or via DHCP

Certificates can be Obtained and Renew via SCEP, SCEP details can be provided manually or via DHCP

Certificates can be Obtained and Renew via SCEP, SCEP details can be provided manually or via DHCP, this will apply to Standalone or Remote pair

# Common mechanisms and protocols for certificate enrollment and renewal for devices

## Simple Certificate Enrollment Protocol (SCEP)

Widely used for 802.1X authentication on devices.

SCEP uses HTTP(S) for communication, supports RSA cryptography, and requires a challenge password shared between the server and device for security.

## Enrollment over Secure Transport (EST)

EST is a secure certificate enrollment protocol that operates over HTTPS, providing encrypted and authenticated certificate requests.

## Manual Enrollment

Devices can also use manual certificate installation by uploading PEM files or generating CSRs for signing outside automated protocols.



# SCEP to automate Certificate Enrollment

- SCEP is designed to **automate the process of requesting and issuing signed certificates** in a PKI system
- It is widely used for enrolling certificates on devices such as routers, switches and mobile devices
- SCEP is supported in Control Hub to enroll Cisco Collaboration devices

## How to Provide SCEP parameters to Devices



PhoneOS

- Phone Web interface
- Webex Control Hub
- XML provisioning
- DHCP option 43



RoomOS

- Video device Web interface
- Webex Control Hub
- CLI using xCommands
- DHCP option 43

# How do we build DHCP Option 43 for SCEP

Sub options (10–15) are reserved for Custom Device Certificate (CDC).

The maximum length of DHCP option 43 is 255 bytes.

The maximum length of **Server + Challenge Password** shall be less than 208 bytes

| DHCP Option 43 Parameters      |             |                |                                   |           |
|--------------------------------|-------------|----------------|-----------------------------------|-----------|
| Parameters on the Video Device | Sub-options | Type           | Length (byte)                     | Mandatory |
| FIPS Mode                      | 10          | boolean        | 1                                 | No        |
| Server                         | 11          | string         | 208 - length (challenge Password) | Yes       |
| Root CA Fingerprint            | 12          | binary         | 20 or 32                          | Yes       |
| Challenge Password             | 13          | string         | 208 - length (server)             | No        |
| Enable 802.1X Authentication   | 14          | boolean        | 1                                 | No        |
| Certificate Select             | 15          | Unsigned 8-bit | 1                                 | No        |

## Example of Values used in the Option 43

FIPS Mode = Disable

Server = http://198.18.6.12/CertSrv/mscep/mscep.dll

Root CA Fingerprint = 0944E1E4A3B2D885E9101E6941E1E37D

Challenge Password = 5D1D763F12463E5BFE5D58E501D1AFFBF48F

Enable 802.1X Authentication = Yes

Certificate Select = Custom installed

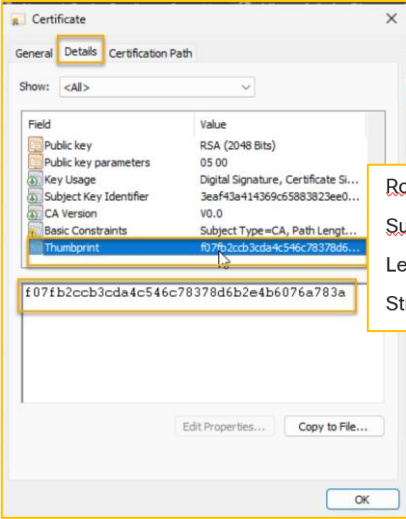
# Automatically provision SCEP from DHCP information

FIPS Mode = Disable  
Suboption: **0A**  
Length: **01**  
Value: **00**  
String: **0A0100**

Server = <http://198.18.6.12/CertSrv/mscep/mscep.dll>  
In Hex = 687474703A2F2F3139382E31382E362E31322F436572745372762F6D736365702F6D736365702E646C6C  
Suboption: **0B**  
Length: 84 characters / 2 = 42 bytes = **2A**  
String: 0B2A687474703A2F2F3139382E31382E362E31322F436572745372762F6D736365702F6D736365702E646C6C

Challenge Password = 5D1D763F12463E5BFE5D58E501D1AFFBF48F  
In Hex = 354431443736334631323436334535424645354435384535303144314146464246343846  
Suboption: **0D**  
Value: 354431443736334631323436334535424645354435384535303144314146464246343846  
Length: 72 characters / 2 = 36 bytes = **24**  
String: 0D24354431443736334631323436334535424645354435384535303144314146464246343846

Enable 802.1X Authentication = Yes  
Suboption: **0E**  
Length: **01**  
Value: **01**  
String: **0E0101**



Root CA Fingerprint = f07fb2ccb3cda4c546c78378d6b2e4b6076a783a  
Suboption: **0C**  
Length: 40 characters / 2 = 20 bytes = **14**  
String: **0C14f07fb2ccb3cda4c546c78378d6b2e4b6076a783a**

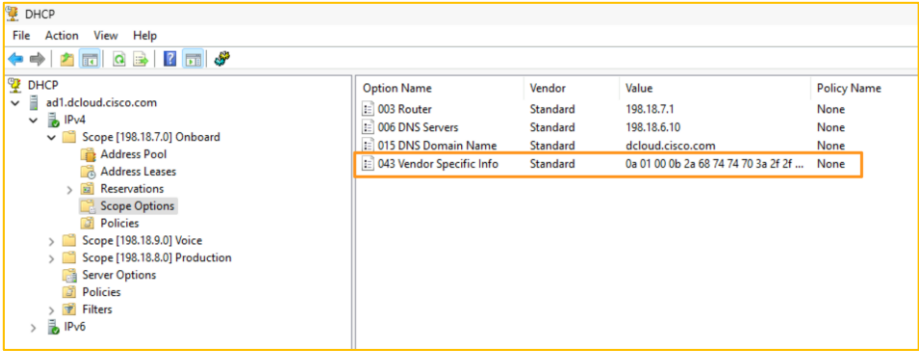
Certificate Select = Custom installed  
Suboption: **0F**  
Length: **01**  
Value: **01**  
String: **0F0101**

## Let's build it all together

“FIPS-Mode” + “SCEP-URL” + “CA-Fingerprint” + ”Challenge-Password” + “Enable 802.1x Setting” + ”Certificate Selection Setting”

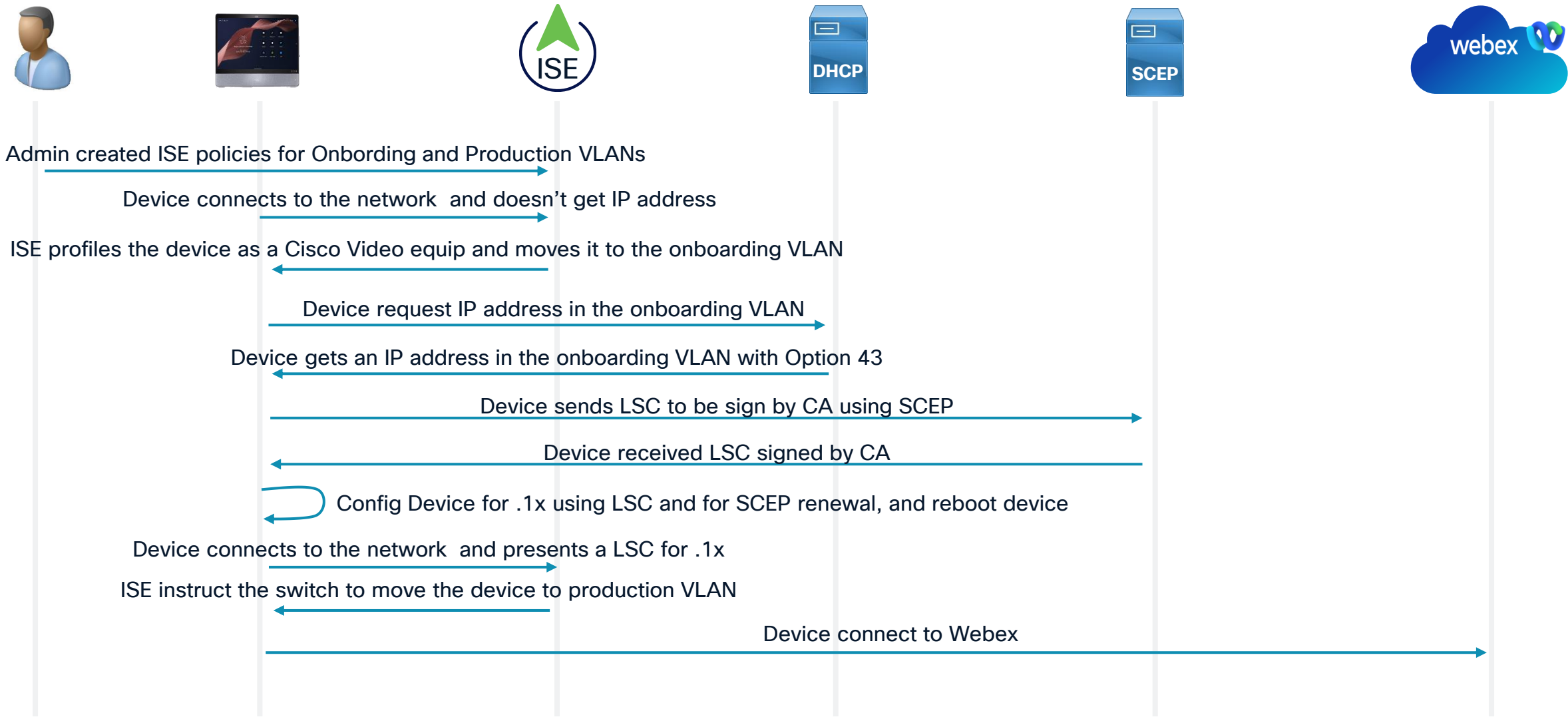
## Result

0A01000B2A687474703A2F2F3139382E31382E362E31322F436572745372762F6D736365702F6D736365702E646C6C0C14f07fb2ccb3cda4c546c78378d6b2e4b6076a783a0D243544314437363346313234363345354246453544353845353031443141464642463438460E01010F0101



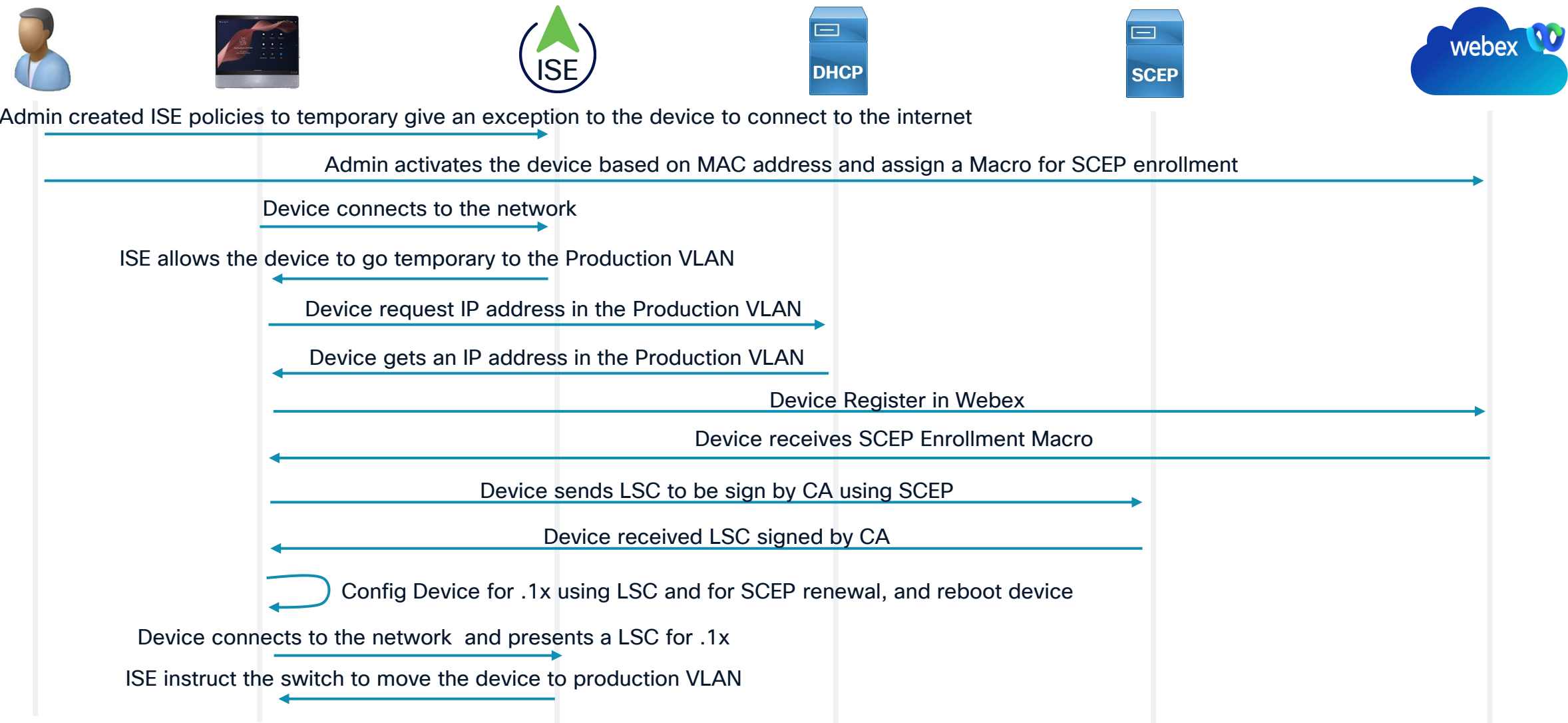
# Zero Trust Provision a Video Device

Option 1 – No connection to internet before LSC installed



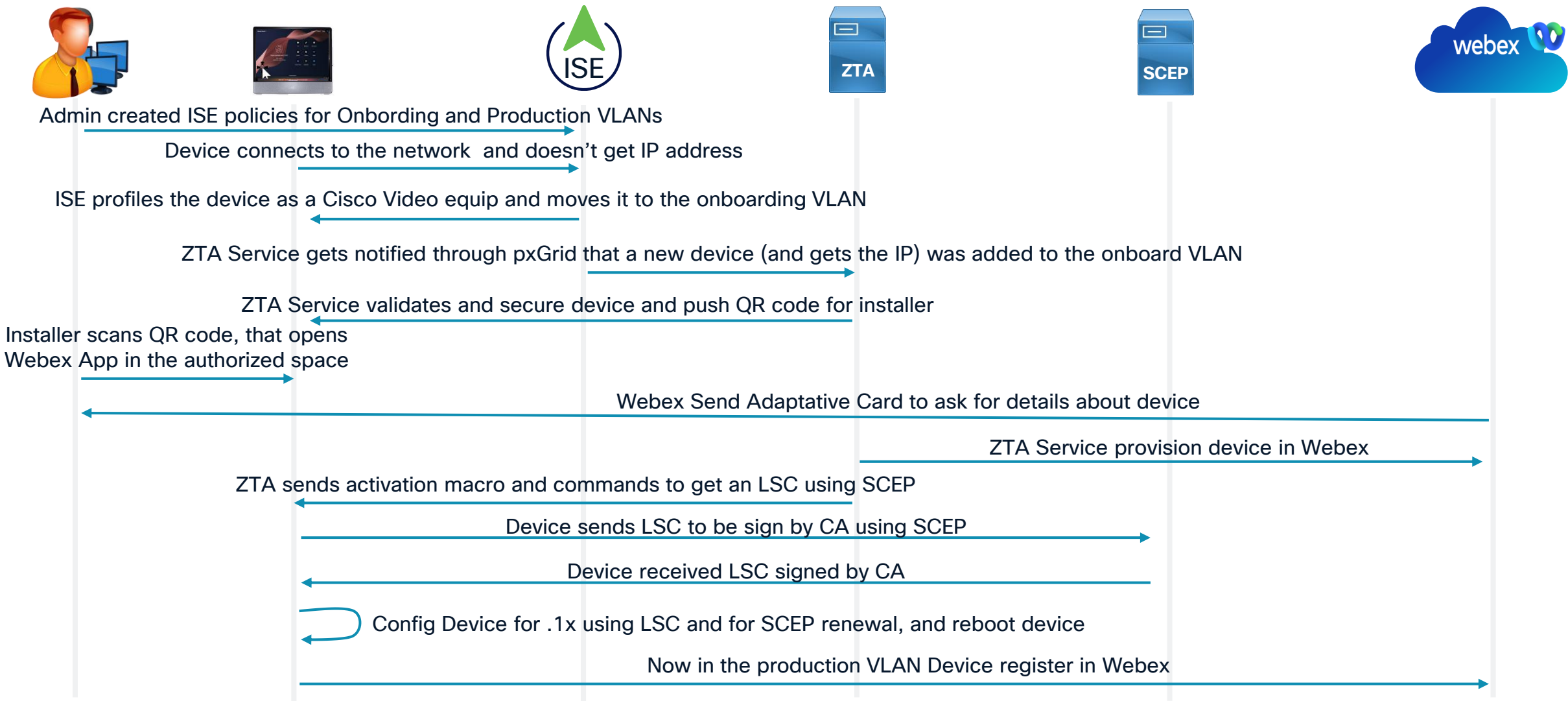
# Zero Trust Provision a Video Device

Option 2 – Time based exception in the internet connection before LSC installed



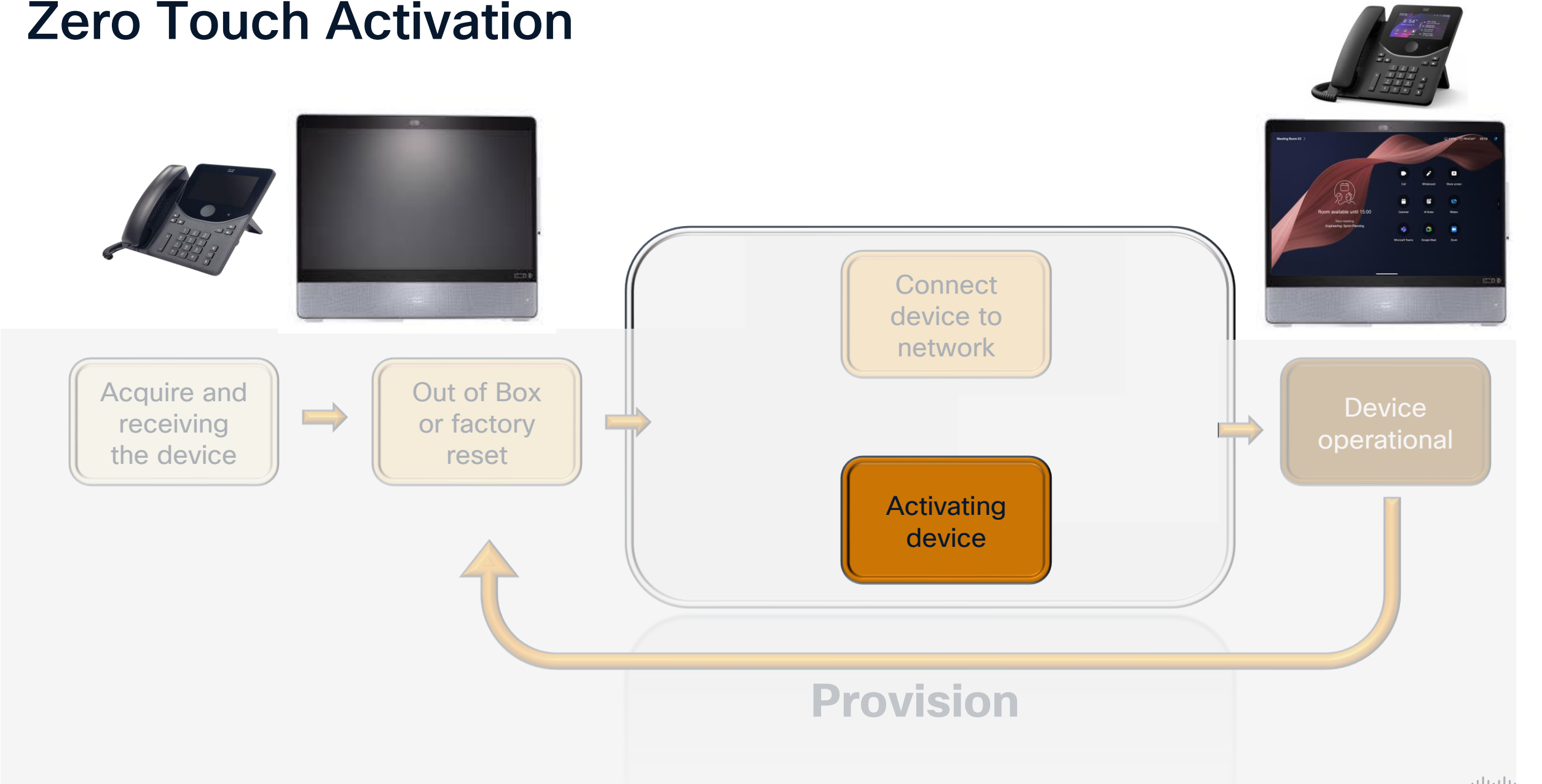
# Zero Trust Provision a Video Device

Option 3 – No connection to internet before LSC installed with **custom** ZTA method



# Zero Touch Activation

# Zero Touch Activation



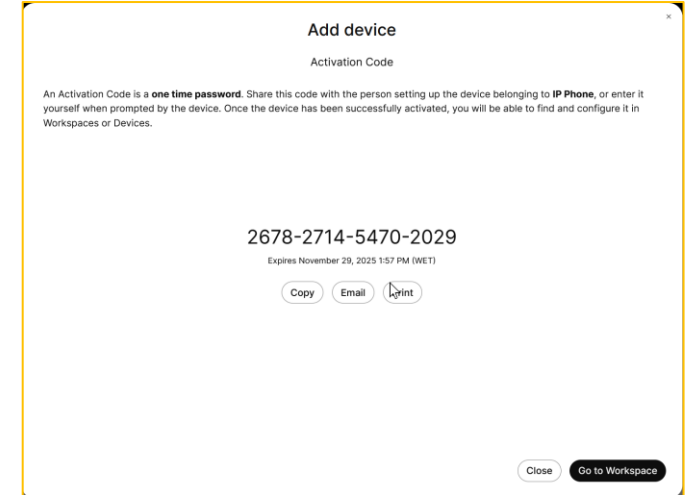
# Zero Touch Activation

Zero Touch Activation (ZTA for Cisco devices streamlines the deployment process by automating as much as possible the initial setup and configuration.

Traditionally the activation of a device is always done device by device with an activation code.

Device Activation should:

- Be possible in advance even before the device connect to the network
- It should be possible to activate multiple devices
- There shouldn't be a need to assign it to a specific workspace

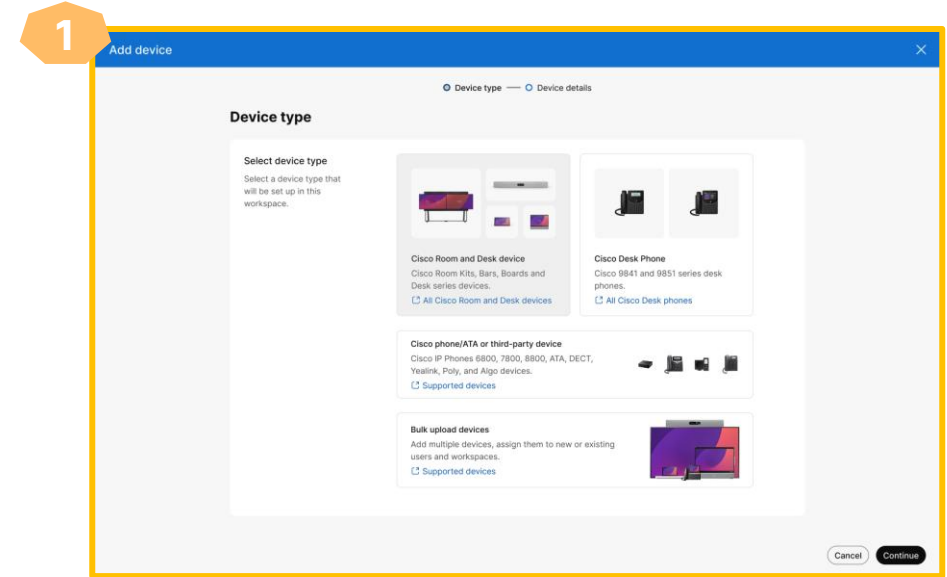
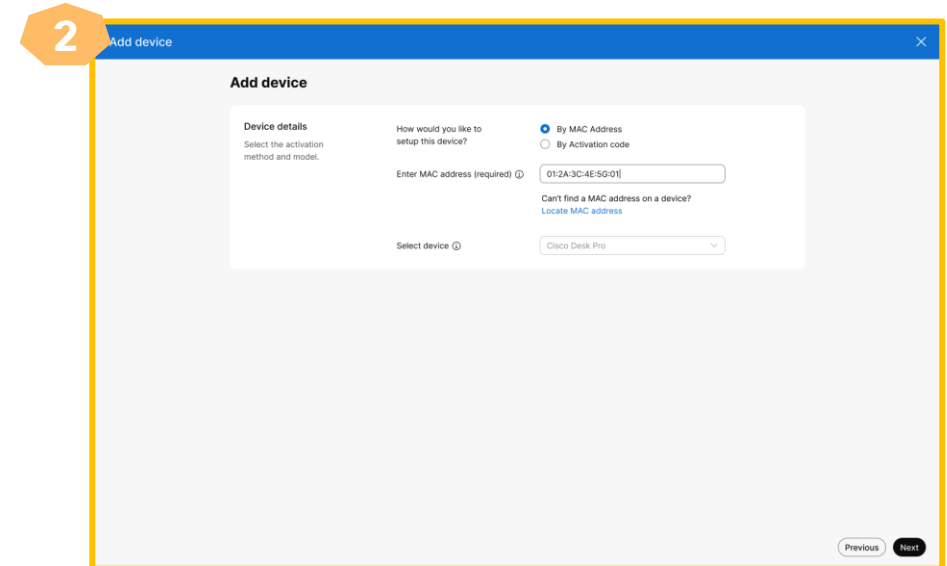


# Zero Touch Activation

## Adding One Device

Video Devices like IP Phone will have the capability of activating the device in advance by providing the MAC address.

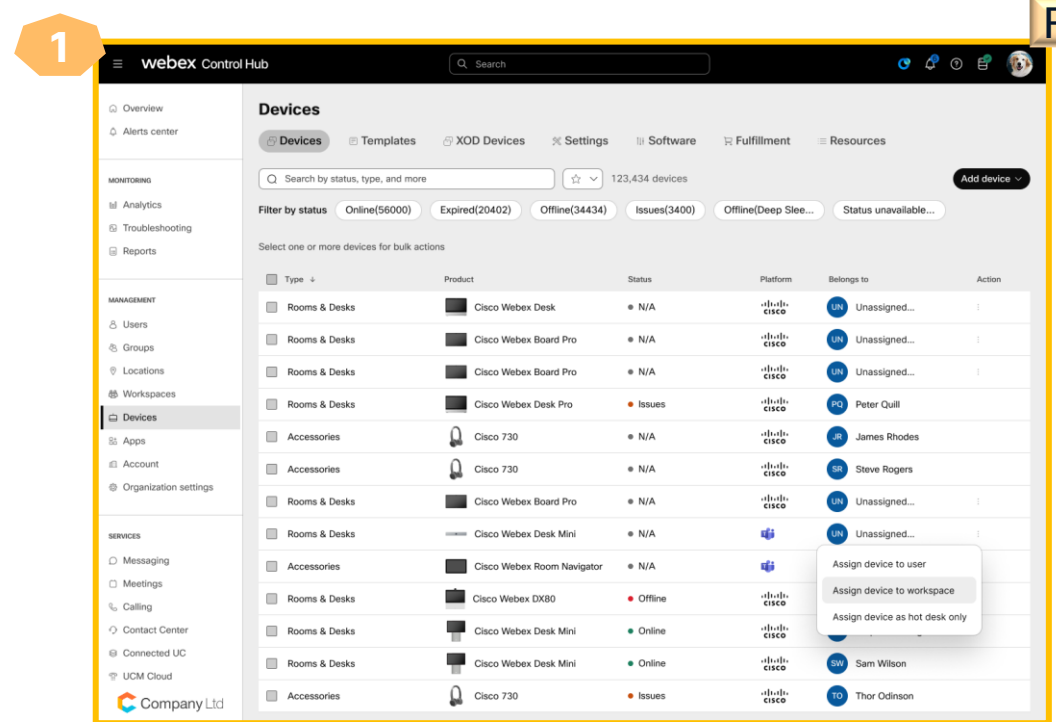
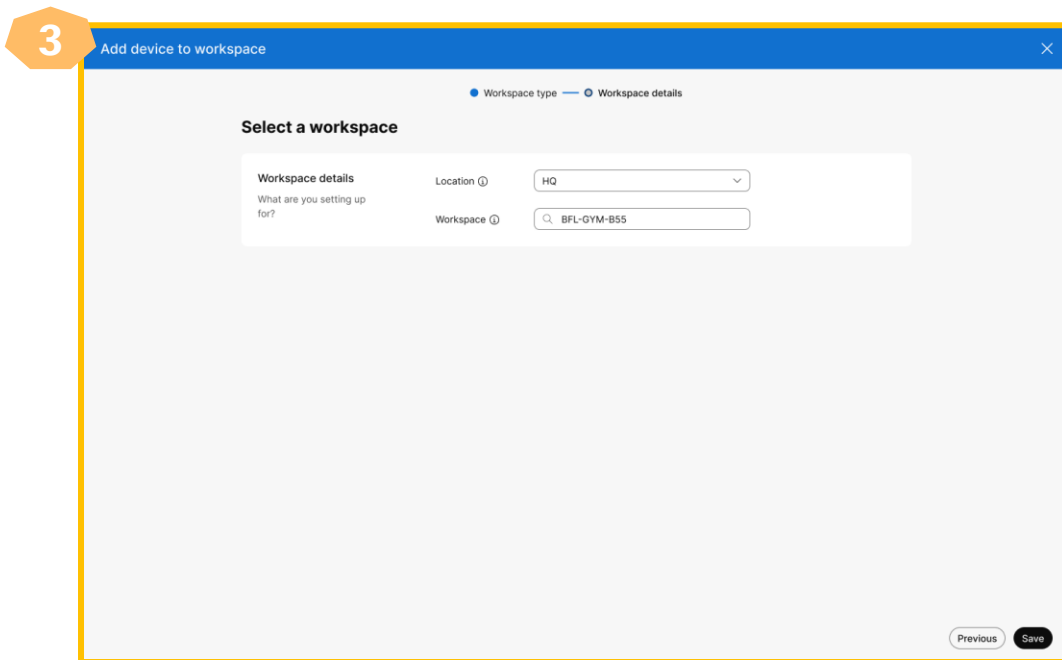
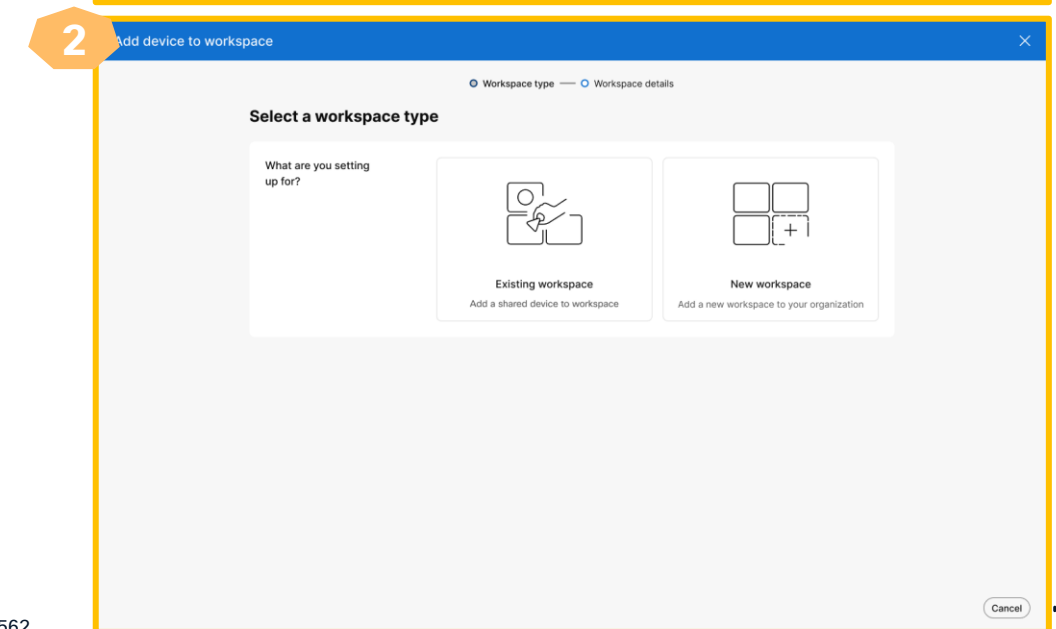
MAC address are available to the customer after been shipped from Cisco.



# Zero Touch Activation

## Assigning to Workspace

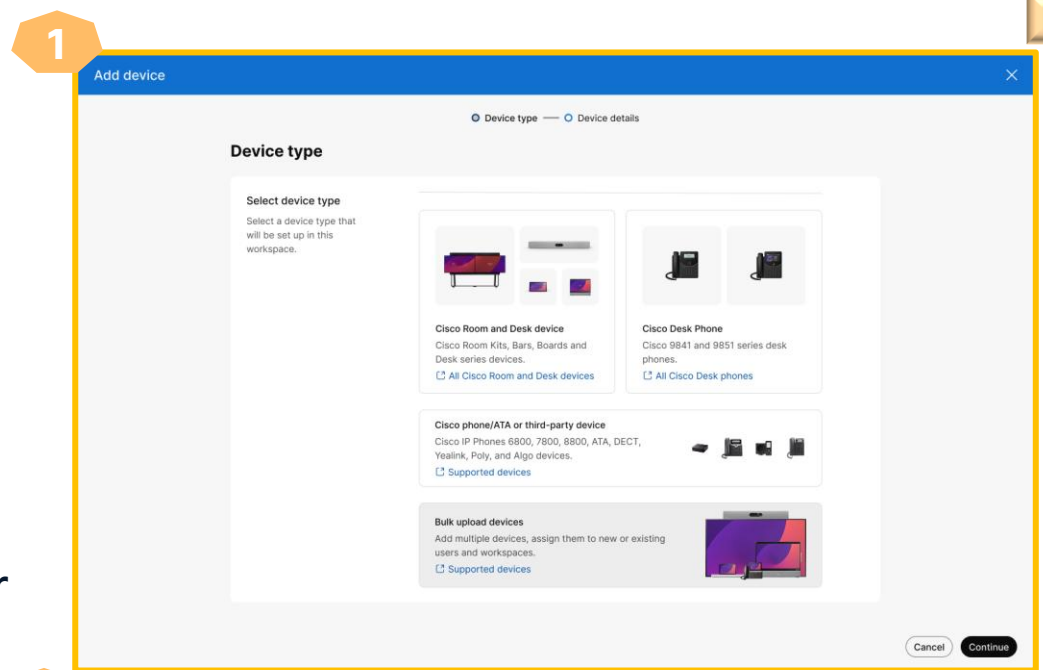
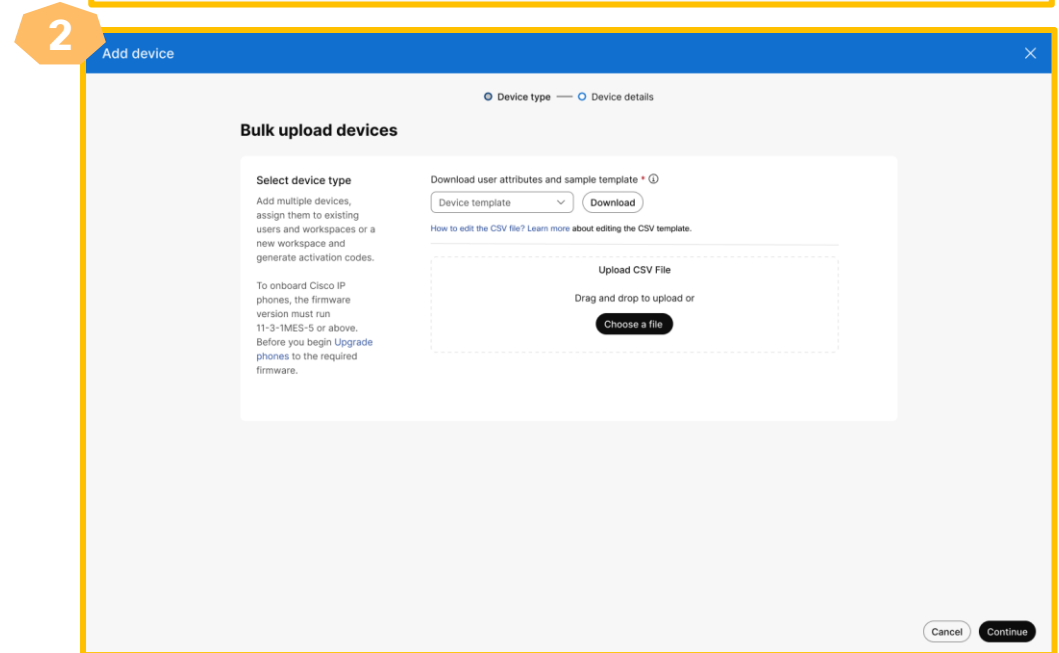
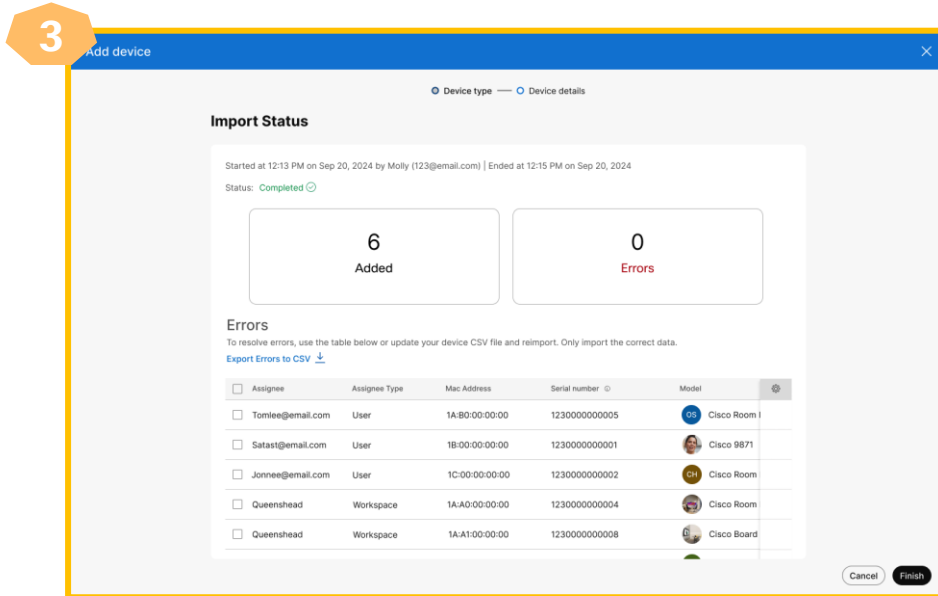
When a device is added in advance it will not be assign to any workspace that task will came later in the Activation process.



# Zero Touch Activation

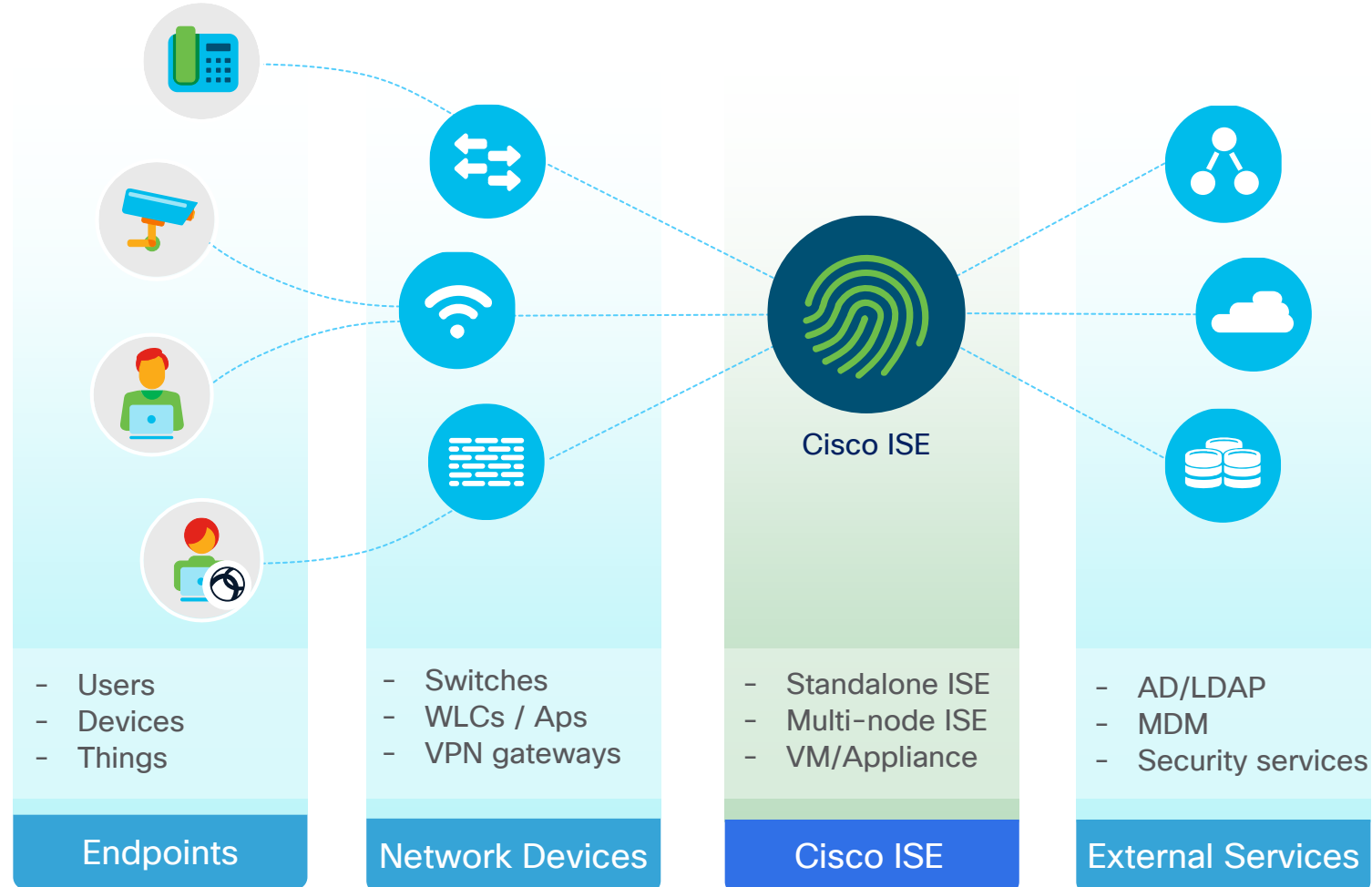
## Bulk Add Devices

By importing a CSV with the MAC address and part number of the devices we can do Bulk operations, similar to IP Phone.

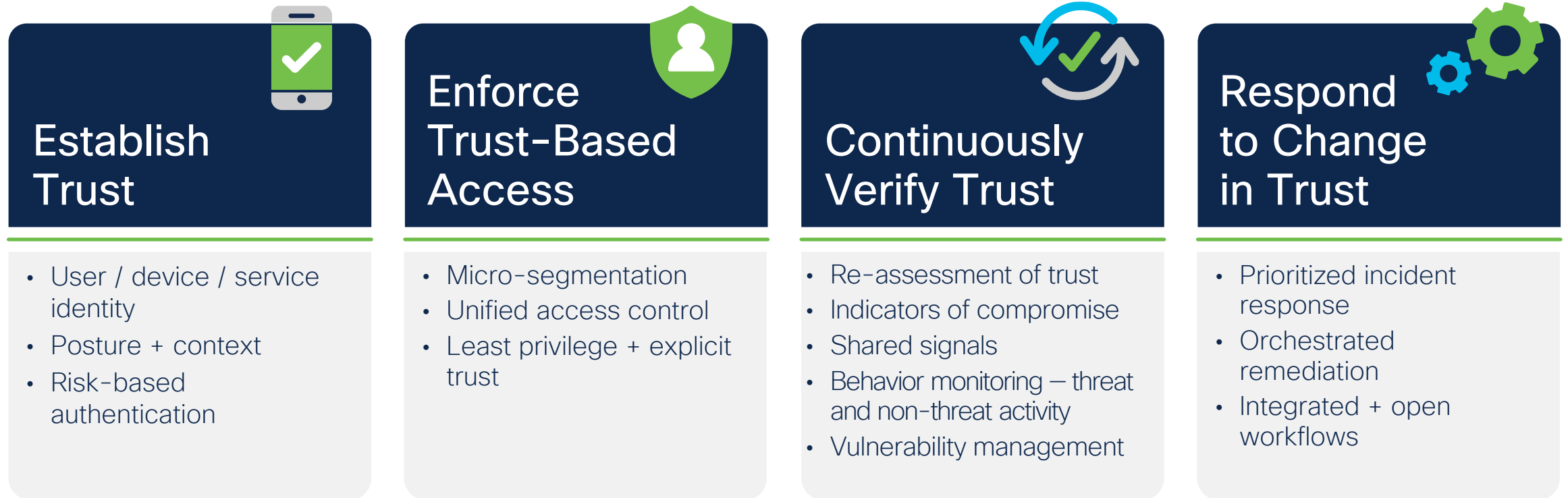


**Bringing it all up together with  
ISE and Webex CH**

# What makes a typical ISE deployment?



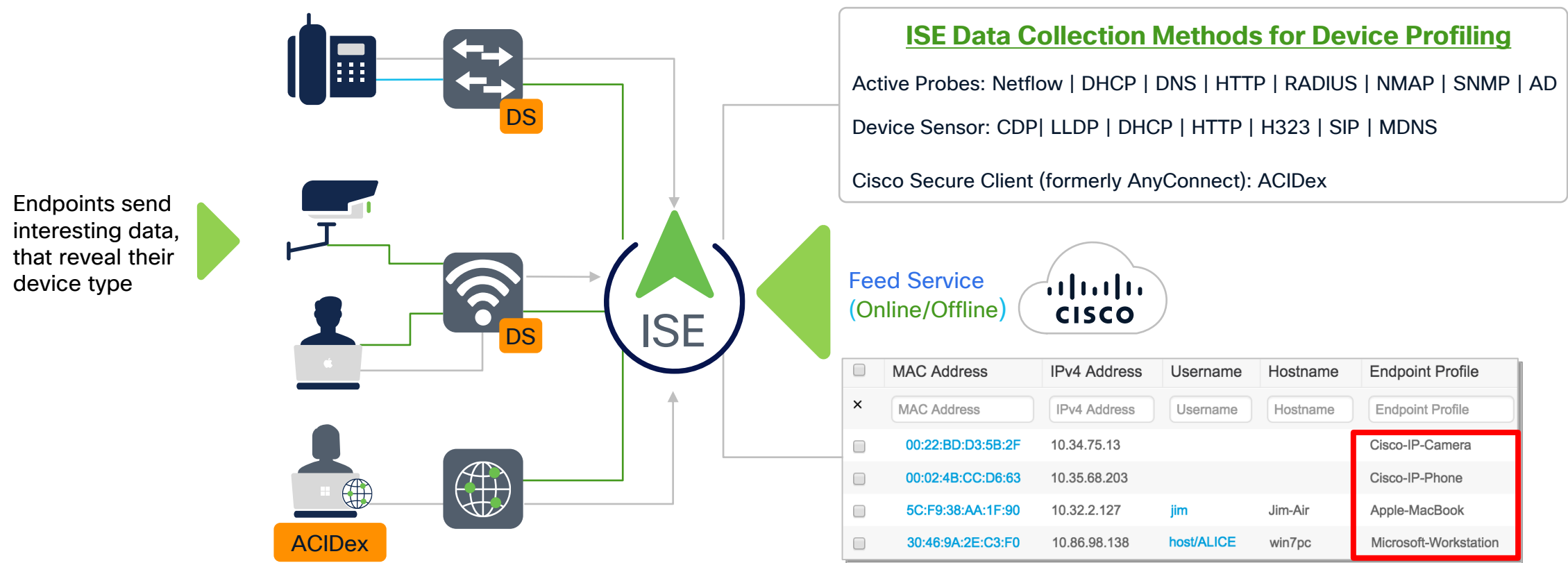
# Cisco's zero trust capabilities



**Unified Policy Lifecycle Management**  
across users, devices, apps, networks and cloud

# Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network

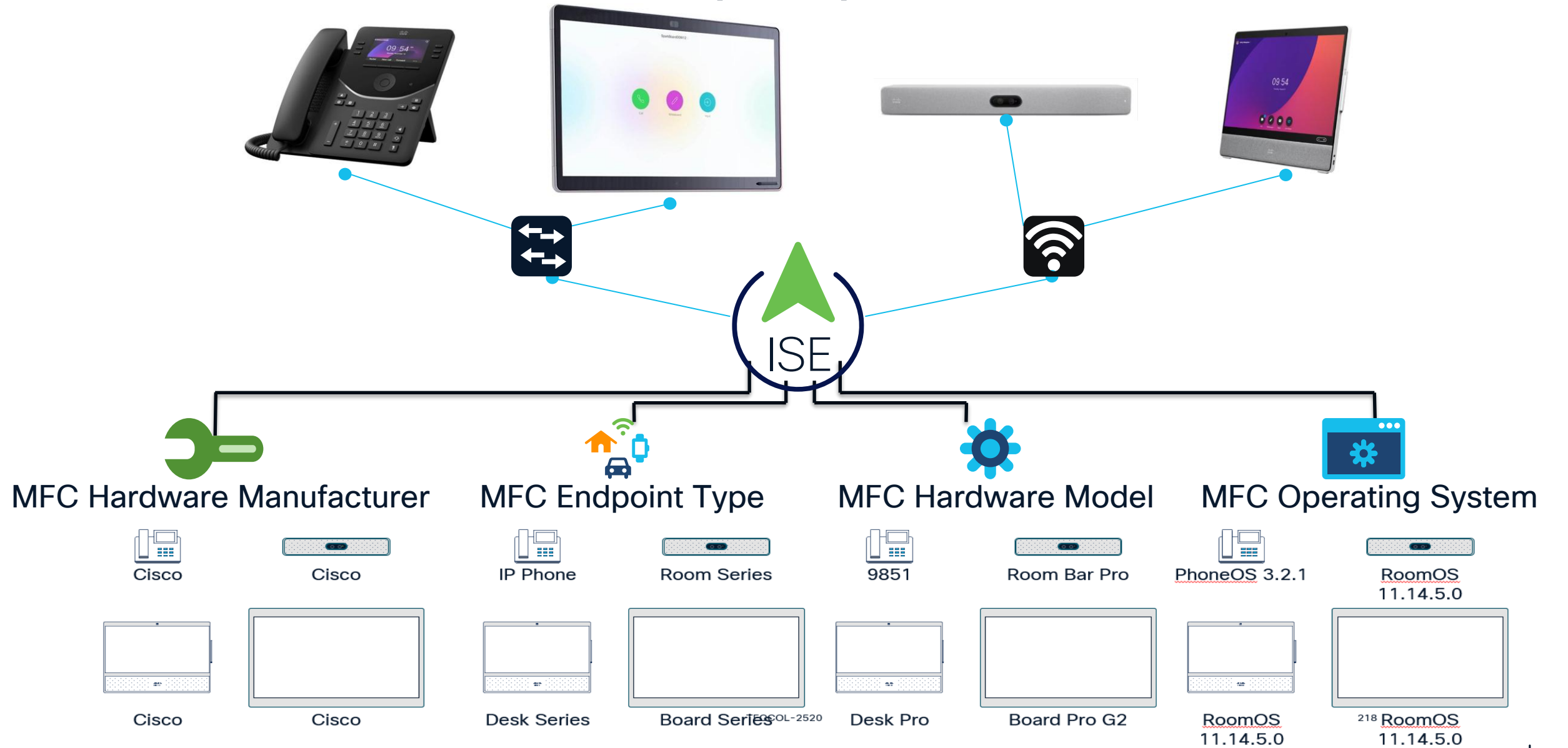


Cisco Secure Client Identity Extensions (ACIDex) | Device Sensor (DS)



|                            |               |
|----------------------------|---------------|
| MFC Endpoint Type:         | IP Phone      |
| MFC Hardware Manufacturer: | Cisco         |
| MFC Hardware Model:        | 9851          |
| MFC Operating System:      | PhoneOS 3.2.1 |

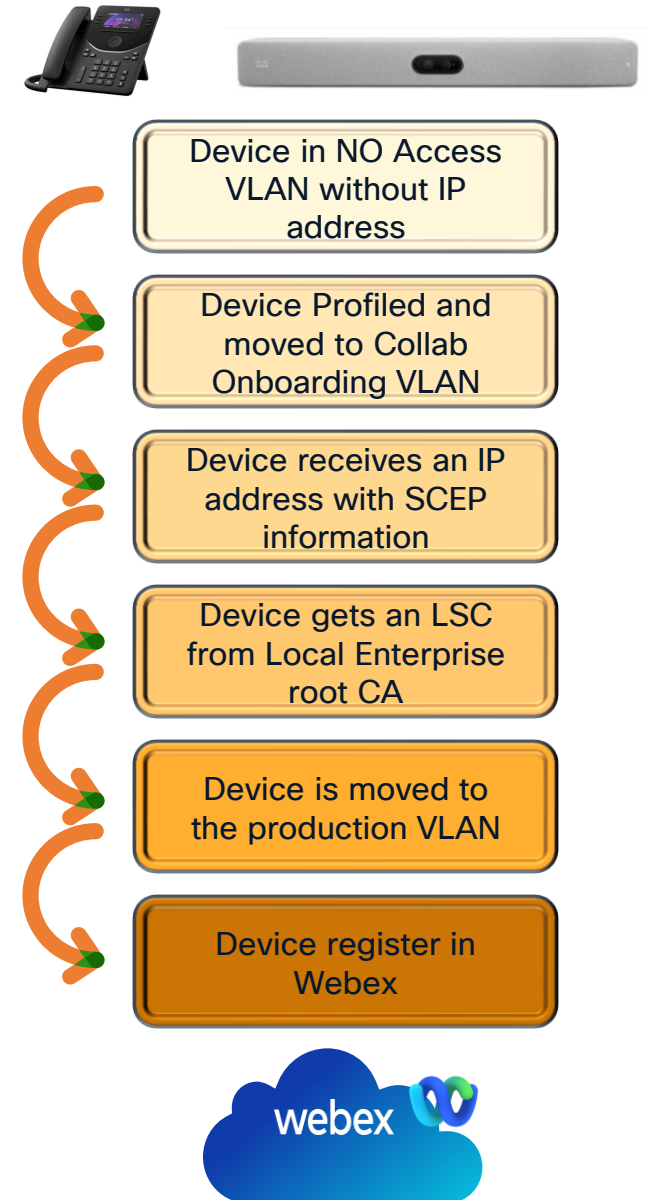
# Multi-Factor Classification (MFC) on ISE



# Using ISE to deliver a Zero Trust network Enrollment for Cisco Collaboration Devices

## Principles :

- Switch is configured so that a device doesn't get an IP address before been profiled.
- Only Cisco IP Phones or Cisco Video Devices go to the Collaboration onboarding VLAN.
- Onboarding VLAN only has access to CA and SCEP server
- Onboarding VLAN provides DHCP option 43 that allows for SCEP to be configured in the device.
- After having a LSC signed by a Enterprise root CA the Collaboration device will be moved by ISE to the production VLAN, with internet access, that will allow for the Webex registration



# Configure the switch for default behavior of no access VLAN

- Switch configured to not provided IP address if a device in not profiled by ISE
- The Switch Port will do .1x and fallback to MAB for initial onboarding

```
!
template Collab-PORT-TEMPLATE
dot1x pae authenticator
dot1x timeout quiet-period 5
dot1x timeout tx-period 5
dot1x timeout supp-timeout 5
dot1x max-req 3
dot1x max-reauth-req 3
switchport access vlan 199
switchport mode access
switchport voice vlan 198
mab
access-session host-mode multi-domain
access-session closed
access-session port-control auto
authentication periodic
authentication timer reauthenticate server
service-policy type control subscriber Collab_1X_MAB
!
```

```
!
interface GigabitEthernet1/0/1
ip flow monitor dnacmonitor input
ip flow monitor dnacmonitor output
source template Collab-PORT-TEMPLATE
spanning-tree portfast
ip nbar protocol-discovery
!
```

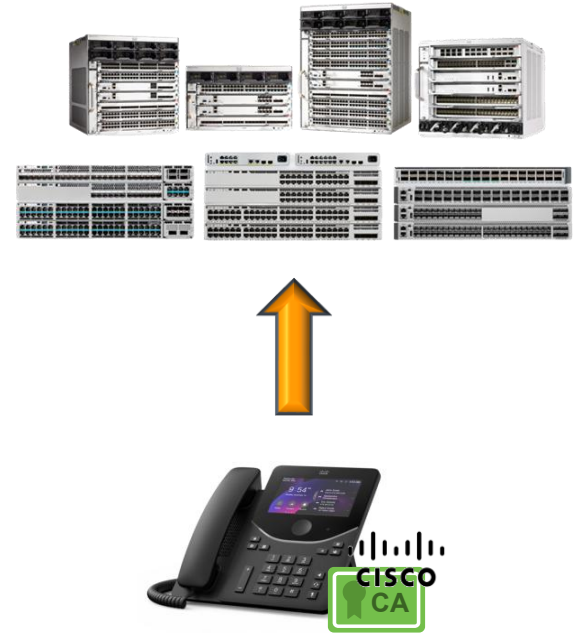
```
!
interface Vlan198
description NO IP addresses in Voice VLAN just initial starting
no ip address
!
interface Vlan199
description NO IP addresses just initial starting point
no ip address
!
```

```
C9200-Home#sh vlan
```

| VLAN | Name              | Status | Ports                      |
|------|-------------------|--------|----------------------------|
| 1    | default           | active | Gi1/1/2, Te1/1/3, Te1/1/4  |
| 100  | AVoIP_Accessories | active | Gi1/0/5, Gi1/0/6, Gi1/0/7, |
| 198  | NOACCESS2         | active | Gi1/0/1, Gi1/0/3, Gi1/0/4  |
| 199  | NOACCESS          | active | Gi1/0/1, Gi1/0/3, Gi1/0/4  |
| 300  | ONBOARD-VLAN-NEW  | active |                            |
| 310  | PRODUCTION-VLAN   | active | Gi1/0/2, Gi1/0/12          |
| 320  | VOICE-VLAN        | active | Gi1/0/2, Gi1/0/12          |

# How to onboard an IP Phone ?

- IP Phones can present a **MIC/SUDI** when they establish the initial trust for **Authentication** in ISE
- To be able to be admitted to the onboarding VLAN the IP Phone needs to have a valid certificate sign by one of the Cisco Cas but also **needs to be profiled as an IP Phone**



# How to onboard a Video Device?

- Video devices can't **authenticate** by present MIC/SUDI in .1x so the only way to establish the initial trust is by using **MAC Address Bypass (MAB)**
- We need to provide the MAC address of the device or all MAC addresses used by Cisco to bring the device to **the Authorization process and be profiled**



# What to configure in ISE to secure onboard Cisco Collaboration Devices

Certificates to add

Add Customer Enterprise Root CA to ISE Certificate store

Download cbarc2099, cmca3 and HA SUDI

Cisco Certificate authorities Root and Subordinated Cas download page  
<https://www.cisco.com/security/pki/>

## Customer Enterprise Root CA

Deployment Licensing **Certificates** Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings

Certificate Management  
System Certificates  
Admin Certificate Node  
Restart  
**Trusted Certificates**  
OCSP Client Profile  
Certificate Signing  
Requests  
Certificate Periodic Check  
Settings  
Certificate Authority

Import a new Certificate into the Certificate Store

\* Certificate File

Friendly Name

Trusted For:

☒ Trust for authentication within ISE  
☒ Trust for client authentication and Synting  
☒ Trust for certificate based admin authentication  
☒ Trust for authentication of Cisco Services  
☒ Trust for Native IPsec certificate based authentication  
☐ Validate Certificate Extensions

Description

Subordinated CAs

|                                                                                       |
|---------------------------------------------------------------------------------------|
| ACT2 ECC SUDI CA - CER / PEM                                                          |
| ACT2 SUDI CA - CER / PEM                                                              |
| Airespace - CER / PEM                                                                 |
| Attestation CA - CER / PEM                                                            |
| Cisco Client CA 001 (aca) - CER / PEM                                                 |
| Cisco Employee CA (ceca) - CER / PEM                                                  |
| Cisco Generic Software Identity Sub CA EC P384 SHA384 2099 (cgsiscap384) - CER / PEM  |
| Cisco Generic Software Identity Sub CA RSA 4096 SHA512 2099 (cgsisca4096) - CER / PEM |
| Cisco IOSXE Software Identity Sub CA EC P384 SHA384 2099 (cisiscap384) - CER / PEM    |
| Cisco Manufacturing CA (cmca) - CER / PEM                                             |
| Cisco Manufacturing CA (cmca2) - CER / PEM                                            |
| Cisco Manufacturing CA III (cmca3) - CER / PEM                                        |
| Cisco Manufacturing CA IV (cmca4) - CER / PEM                                         |
| Cisco Software Transparency SubCA (cswtscsca) - CER / PEM                             |
| Cisco Virtual UEFI SubCA (vuefiscsca) - CER / PEM                                     |
| Cisco Virtual UEFI SubCA V2 (vuefiscav2) - CER / PEM                                  |
| Cisco Virtual UEFI SubCA V3 (vuefiscav3) - CER / PEM                                  |
| Cisco XSSL-R2 (xssl-r2) - CER / PEM                                                   |
| Device Identity Basic Assurance Sub CA 2099 (dibasca2099) - CER / PEM                 |
| EC P384 Attestation CA (p384aca) - CER / PEM                                          |
| HA SUDI CA - CER / PEM                                                                |
| IRRA CA (irrac) - CER / PEM                                                           |
| Innerspace CA SHA-256 - CER                                                           |
| Innerspace CA SHA-512 - CER                                                           |
| IRRA CA (irrac) - CER / PEM                                                           |

Subordinated CAs

|                                |
|--------------------------------|
| ACT2 ECC SUDI CA               |
| ACT2 SUDI CA                   |
| Airespace                      |
| Cisco Client CA 001 (aca)      |
| Cisco Manufacturing CA (cmca)  |
| Cisco Manufacturing CA (cmca2) |
| Cisco XSSL-R2 (xssl-r2)        |

Cisco PKI: Policies, Certificates, and Documents

Certificate Policies and Certification Practice Statements  
CP and CPS documents are available on a separate page.

Certificates

|                                                                               |
|-------------------------------------------------------------------------------|
| Root CAs                                                                      |
| Cisco Basic Assurance Root CA 2099 (cbarc2099) - CER / PEM                    |
| Cisco Basic Assurance SUDI Root CA RSA 4096 2099 (cbsarsca4k2099) - CER / PEM |
| Cisco ECC Root CA (rx-e2) - CER / PEM                                         |
| Cisco Root CA 2048 (cra2048) - CER / PEM                                      |
| Cisco Root CA 2099 (cra2099) - CER / PEM                                      |
| Cisco Root CA M1 (cram1) - CER / PEM                                          |
| Cisco Root CA M2 (cram2) - CER / PEM                                          |
| Cisco Root CA RSA4K 2099 (cra2099/4k) - CER / PEM                             |
| Cisco RXC-R2 (rx-r2) - CER / PEM                                              |
| Cisco Secure Access China Custom Root CA (csaccrca) - CER / PEM               |
| Cisco Secure Access China Custom Production Root CA (csaccprca) - CER / PEM   |
| Cisco Secure Access China Production Root CA (csacprca) - CER / PEM           |
| Cisco Secure Access China Root CA (csacra) - CER / PEM                        |
| Cisco Software Identity Root CA EC P384 SHA384 2099 (cisrca384) - CER / PEM   |

Certificate Revocation Lists (CRLs)

|                                                                   |
|-------------------------------------------------------------------|
| Root CAs                                                          |
| Cisco Basic Assurance Root CA 2099 (cbarc2099)                    |
| Cisco Basic Assurance SUDI Root CA RSA 4096 2099 (cbsarsca4k2099) |
| Cisco ECC Root CA (rx-e2)                                         |
| Cisco Root CA 2048 (cra2048)                                      |
| Cisco Root CA 2099 (cra2099)                                      |
| Cisco Root CA M1 (cram1)                                          |
| Cisco Root CA M2 (cram2)                                          |
| Cisco Root CA RSA4K 2099 (cra2099/4k)                             |
| Cisco RXC-R2 (rx-r2)                                              |
| Cisco Secure Access China Custom Root CA (csaccrca)               |
| Cisco Secure Access China Custom Production Root CA (csaccprca)   |
| Cisco Secure Access China Production Root CA (csacprca)           |
| Cisco Secure Access China Root CA (csacra)                        |
| Cisco Software Identity Root CA EC P384 SHA384 2099 (cisrca384)   |

# What to configure in ISE to secure onboard Cisco Collaboration Devices

ISE Change of Authorization (RFC 5176)

Live Logs

Live Sessions

| Time                       | Status | Details | Repea... | Identity             | Endpoint ID       | Endpoint Profile    | Authentication Policy         | Authorization Policy          | Authorization Profiles  | IP Address | Network Device | Device Port          | Identity Group |
|----------------------------|--------|---------|----------|----------------------|-------------------|---------------------|-------------------------------|-------------------------------|-------------------------|------------|----------------|----------------------|----------------|
| Nov 03, 2025 11:24:14.1... |        |         | 0        | CP-9871-SEP845A3E... | 84:5A:3E:C2:5C:A4 | Cisco-IP-Phone-9871 | Collaboration Device with ... | Collaboration Device with ... | Cisco_Device_Production |            |                | GigabitEthernet1/0/2 |                |
| Nov 03, 2025 11:23:00.4... |        |         |          | #ACSACL#-IP-PERMI... |                   |                     |                               |                               |                         |            | C9200-Home     |                      |                |
| Nov 03, 2025 11:23:00.3... |        |         |          | CP-9871-SEP845A3E... | 84:5A:3E:C2:5C:A4 | Cisco-IP-Phone-9871 | Collaboration Device with ... | Collaboration Device with ... | Cisco_Device_Production |            | C9200-Home     | GigabitEthernet1/0/2 | Cisco-IP-Phone |
| Nov 03, 2025 11:18:18.1... |        |         |          | #ACSACL#-IP-PERMI... |                   |                     |                               |                               |                         |            | C9200-Home     |                      |                |
| Nov 03, 2025 11:18:18.0... |        |         |          | CP-9871-SEP845A3E... | 84:5A:3E:C2:5C:A4 | Cisco-IP-Phone-9871 | Collaboration Device with ... | Collaboration Device with ... | Cisco_Device_Onboarding |            | C9200-Home     | GigabitEthernet1/0/2 | Cisco-IP-Phone |
| Nov 03, 2025 11:17:16.4... |        |         |          | #ACSACL#-IP-PERMI... |                   |                     |                               |                               |                         |            | C9200-Home     |                      |                |
| Nov 03, 2025 11:17:16.3... |        |         |          | CP-9871-SEP845A3E... | 84:5A:3E:C2:5C:A4 | Cisco-IP-Phone-9871 | Collaboration Device with ... | Collaboration Device with ... | Cisco_Device_Onboarding |            | C9200-Home     | GigabitEthernet1/0/2 | Cisco-IP-Phone |
| Nov 03, 2025 11:16:47.2... |        |         |          | 84:5A:3E:C2:5C:A4    | 84:5A:3E:C2:5C:A4 | Cisco-IP-Phone-9871 | Collaboration Device with ... | Collaboration Device with ... | Cisco_WebAuth           |            | C9200-Home     | GigabitEthernet1/0/2 | Cisco-IP-Phone |

We want that the collaboration devices start in a no access VLAN and after change to the onboarding VLAN and finally stop in the production VLAN

RADIUS CoA (Change of Authorization) is a feature that allows ISE to adjust an active client session.

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Deployment

Licensing

Certificates

Logging

Maintenance

Upgrade

Health Checks

Backup & Restore

Admin Access

Settings

General Settings

Reassessments

Updates

Acceptable Use Policy

Profiling

Protocols

Endpoint Scripts

Proxy

SMTP Server

SMS Gateway

Profiling

▼ Profiler Settings

CoA Type\* Reauth

Current custom SNMP community strings \*\*\*\*\* Show

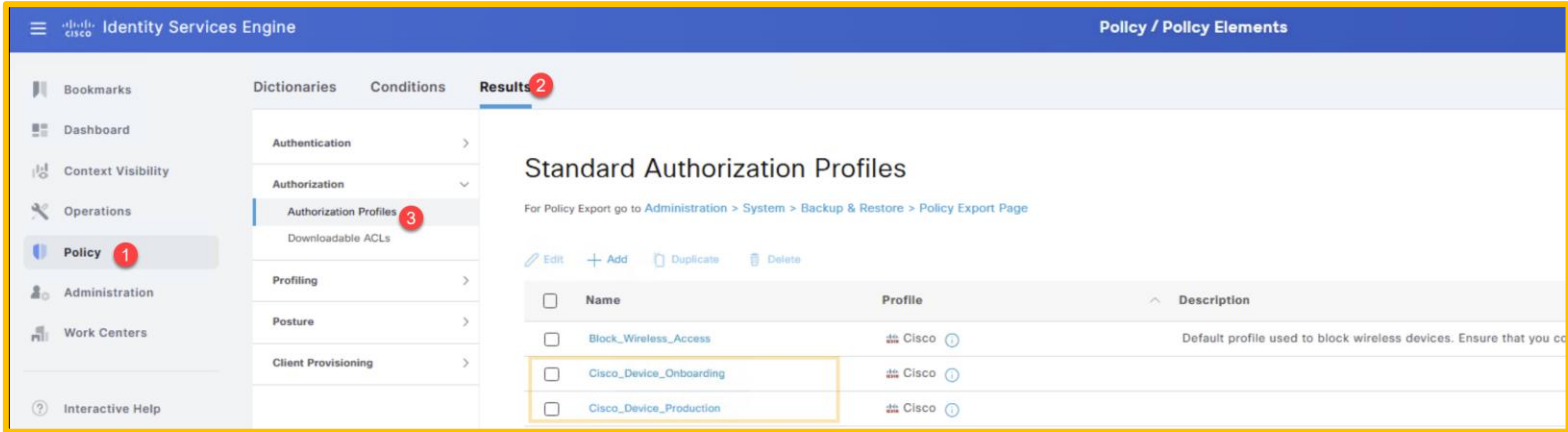
Change custom SNMP community strings

Confirm changed custom SNMP community strings:

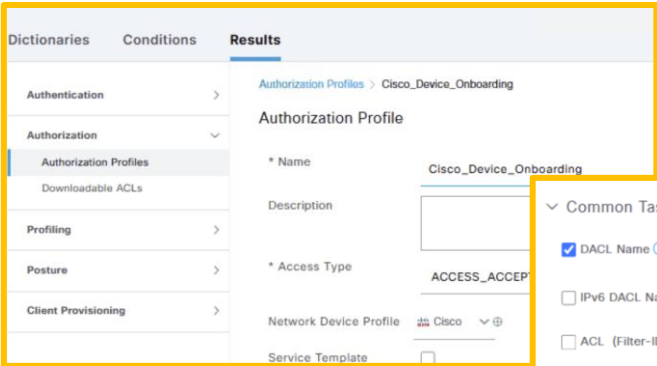
☐ EndPoint Attribute Filter

# What to configure in ISE to secure onboard Cisco Collaboration Devices

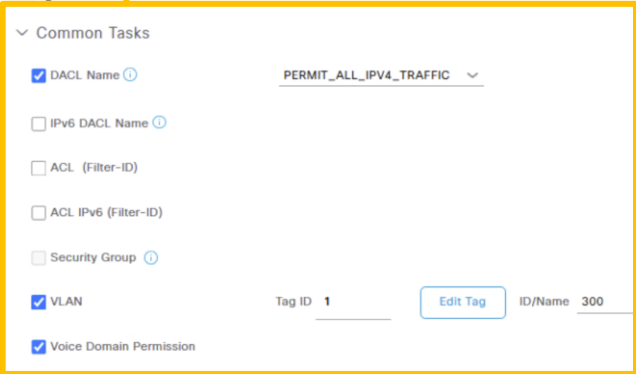
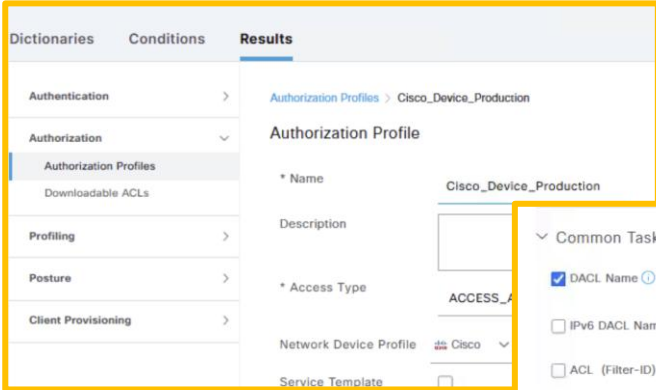
## Authorization Profiles



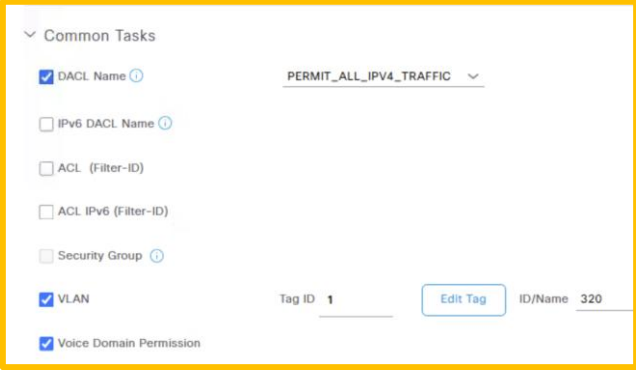
We need to create two different Authorization Profiles



Authorization Profile with onboarding VLAN



Authorization Profile with Production VLAN



# What to configure in ISE to secure onboard Cisco Collaboration Devices

## Policy Sets

Since we are going to use MAB for video devices and .1x manufactory certs for the onboarding VLAN we need to create two policy sets for each situation.

Identity Services Engine

Policy / Policy Sets

Search

Reset

Reset Policy Set Hit Counts

Save

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Policy Sets

| Status | Policy Set Name                 | Description        | Conditions                                            | Allowed Protocols / Server Sequence | Hits | Actions | View |
|--------|---------------------------------|--------------------|-------------------------------------------------------|-------------------------------------|------|---------|------|
| ✓      | Collaboration Device with Certs |                    | OR <div>Wireless_802.1X</div> <div>Wired_802.1X</div> | Default Network Access              | 8894 |         |      |
| ✓      | Collaboration Device with MAB   |                    | OR <div>Wired_MAB</div> <div>Wireless_MAB</div>       | Default Network Access              | 6314 |         |      |
| ✓      | Default                         | Default policy set |                                                       | Default Network Access              | 542  |         |      |

Reset

Save

# What to configure in ISE to secure onboard Cisco Collaboration Devices

Policy Set – Collaboration Device with MAB  
**onboarding** Video Device

- The **Authentication** will use **MAB**
- The Authorization will **profile the device using (CDP, LLDP, SNMP, DHCP)** and will detect it as a **Video device**, and only with that condition will move it to the Onboarding VLAN

Policy Sets→ Collaboration Device with MAB

Reset

Reset Policy Set Hit Counts

Save

| Status | Policy Set Name               | Description | Conditions                                      | Allowed Protocols / Server Sequence | Hits |
|--------|-------------------------------|-------------|-------------------------------------------------|-------------------------------------|------|
| ✓      | Collaboration Device with MAB |             | OR <div>Wired_MAB</div> <div>Wireless_MAB</div> | Default Network Access              | 6314 |

Authentication Policy(2)

| Status | Rule Name                   | Conditions                                      | Use                | Hits | Actions |
|--------|-----------------------------|-------------------------------------------------|--------------------|------|---------|
| ✓      | Authentication Video Device | OR <div>Wired_MAB</div> <div>Wireless_MAB</div> | Internal Endpoints | 6864 |         |
| ✓      | Default                     |                                                 | All_User_ID_Stores | 0    |         |

Authorization Policy(2)

| Status | Rule Name                  | Conditions                                                                | Profiles                | Security Groups  | Hits | Actions |
|--------|----------------------------|---------------------------------------------------------------------------|-------------------------|------------------|------|---------|
| ✓      | Authorization Video Device | EndPoints:EndPointPolicy CONTAINS Cisco-Device:Cisco-Collaboration-Device | Cisco_Device_Onboarding | Select from list | 23   |         |
| ✓      | Default                    |                                                                           | Cisco_WebAuth           | Select from list | 2832 |         |

# What to configure in ISE to secure onboard Cisco Collaboration Devices

Policy Set – Collaboration Device with .1x  
**onboarding** IP Phones

- The **Authentication** will use the **a .1x certificate**
- The Authorization will **profile the device using (CDP, LLDP, SNMP, DHCP)** and will detect it as an **IP Phone**, but also inspects the Certificate and look for **SEP in the Cert Subject** and either that the **issuer is the MIC Root CA or the SUDI Root CA** and only with those conditions will move it to the Onboarding VLAN

This screenshot shows the 'Policy Sets - Collaboration Device with Certs' configuration page in Cisco ISE. The top section displays a table with columns for Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, the 'Authentication Policy(2)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. The 'Dot1x' rule is highlighted, showing conditions for 'Wireless\_802.1X' and 'Wired\_802.1X'. The 'Certificate\_Request\_Sequence' condition is highlighted with a yellow box. The 'Default' rule is also visible at the bottom.

This screenshot shows the 'Authorization Policy - Global Exceptions' configuration page in Cisco ISE. The top section displays a table with columns for Status, Rule Name, Conditions, Results, Profiles, and Security. Below this, the 'Authorization Policy(3)' section is expanded, showing a table with columns for Status, Rule Name, Conditions, Results, Profiles, and Security. The 'IP Phone Onboarding' rule is highlighted, showing conditions for 'CERTIFICATE-Subject CONTAINS SEP', 'CERTIFICATE-Issuer - Common Name EQUALS dcloud-AD1-CA', 'EndPoints-EndPointPolicy EQUALS Cisco-Device:Cisco-Collaboration-Device', and 'EndPoints-EndPointPolicy EQUALS Cisco-Device:Cisco-IP-Phone'. The 'Cisco\_Device\_Onboarding' profile is highlighted with a yellow box. The 'Default' rule is also visible at the bottom.

# What to configure in ISE to secure onboard Cisco Collaboration Devices

Policy Set – Collaboration Device with .1x

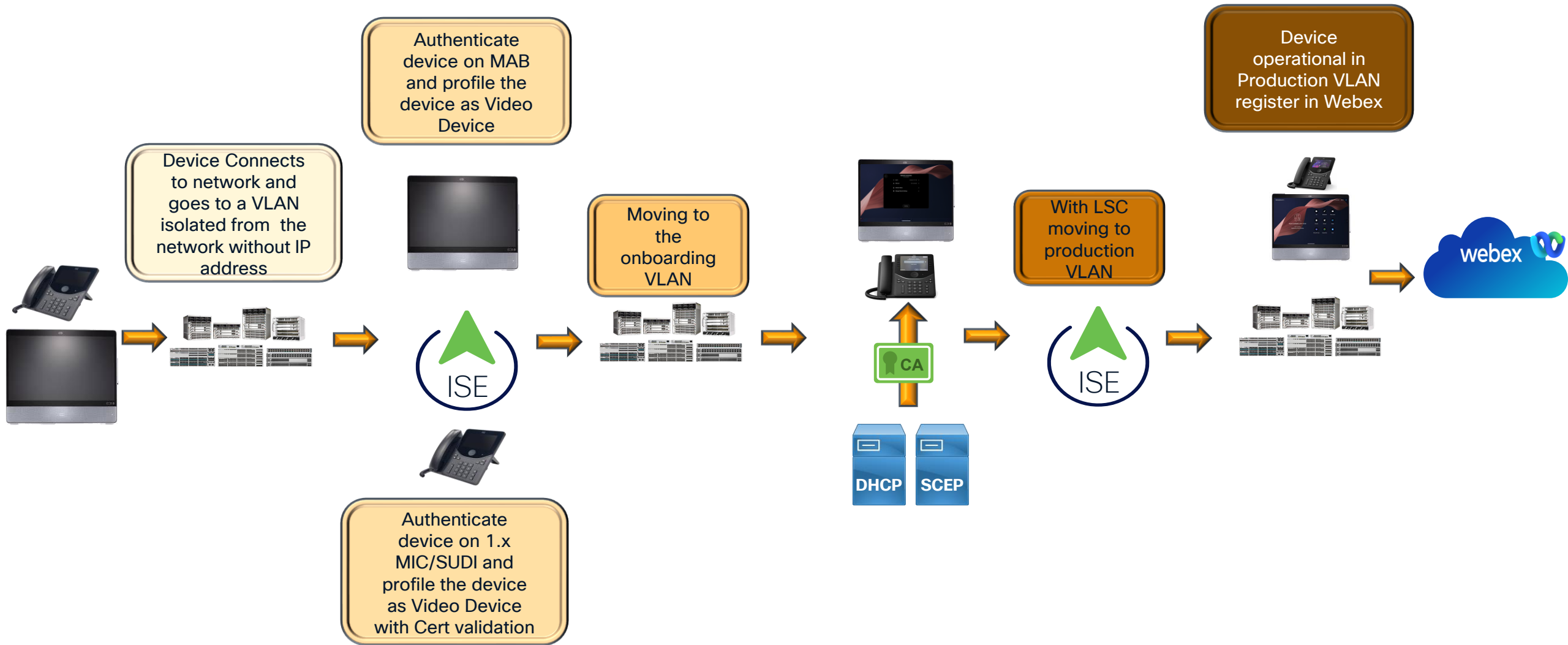
**Production** for IP Phones and Video devices

- The **Authentication** will use the **a .1x certificate**
- The Authorization will **profile the device using (CDP, LLDP, SNMP, DHCP)** and will detect it as an **IP Phone or Video Device**, and also inspects the Certificate and look for **SEP in the Cert Subject** and that the **issuer is the Customer Enterprise Root CA** only with those conditions will move it to the Production VLAN

This screenshot shows the 'Policy Sets - Collaboration Device with Certs' configuration page in Cisco ISE. The top section shows the policy set status and a table with columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, and Hits. Below this, the 'Authentication Policy(2)' is expanded, showing a table with columns: Status, Rule Name, Conditions, Use, Hits, and Actions. The 'Dot1x' rule is highlighted, showing conditions for 'Wireless\_802.1X' and 'Wired\_802.1X', and a 'Certificate\_Request\_Sequence' condition. The 'Default' rule is also visible.

This screenshot shows the 'Authorization Policy - Global Exceptions' configuration page in Cisco ISE. The top section shows the policy set status and a table with columns: Status, Rule Name, Conditions, Results, Profiles, and Security. Below this, the 'Authorization Policy(3)' is expanded, showing a table with columns: Status, Rule Name, Conditions, Results, Profiles, and Security. The 'Collaboration Device Production' rule is highlighted, showing conditions for 'CERTIFICATE-Subject CONTAINS SEP', 'CERTIFICATE-Issuer - Common Name EQUALS dcloud-AD1-CA', 'EndPoints-EndPointPolicy EQUALS Cisco-Device:Cisco-Collaboration-Device', and 'EndPoints-EndPointPolicy EQUALS Cisco-Device:Cisco-IP-Phone'. The 'Cisco\_Device\_Production' profile is assigned to this rule. The 'IP Phone Onboarding' rule is also visible, showing conditions for 'CERTIFICATE-Subject CONTAINS SEP', 'CERTIFICATE-Issuer - Common Name CONTAINS SUDI', and 'CERTIFICATE-Issuer - Common Name CONTAINS Cisco Manufacturing'. The 'Default' rule is also visible.

# Full journey with ISE with Zero Trust Provision



# Key takeaways

# Key Takeaways



## Rapid, Secure Device Provisioning

Zero Touch Provisioning enable organizations to **quickly and securely deploy collaboration devices—including IP phones, video endpoints**, and AVoIP accessories—across enterprise networks, minimizing manual configuration and reducing deployment time.

## Zero Trust Security Principles

Applying Zero Trust principles to device provisioning, **ensuring that only authorized devices and users can access network resources** and protecting against unauthorized access and data breaches.

## Integration with Network Access Control Solutions

Cisco ISE is a very powerful product to **enforce security policies, enhance visibility, and automate compliance** for collaboration endpoints.

# Complete your session evaluations



**Complete** a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.



**Earn** up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



**Level up** and earn exclusive prizes!



**Complete your surveys** in the Cisco Live Events app.

# Continue your education



**Visit** the Cisco Stand for related demos



**Book** your one-on-one Meet the Expert meeting



**Attend** the interactive education with 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)

**Contact me at:** [paucorre@cisco.com](mailto:paucorre@cisco.com)

**Thank you**

**CISCO** Live !