



# Secure the Wired Network

Secure the Wired Network using Identity - in Less than 60 Minutes!

Matt Graham  
Solutions Architect  
BRKOPS-2584

CISCO *Live!*



# Agenda

- Introduction
- Why?
- Using Catalyst Centre
- Dot1x & Profiling
- Trustsec
- SDA as an option
- Conclusion
- Bonus Content : Posture

# Who's Matt Graham ....?

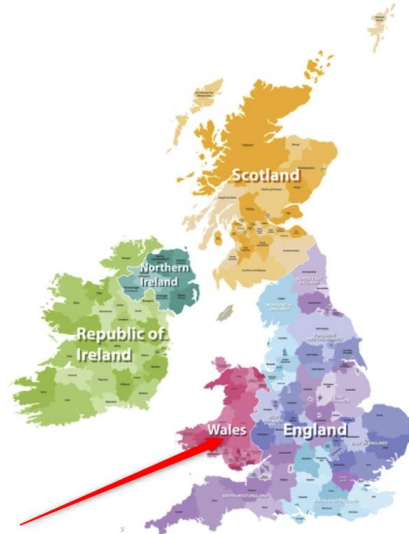
Solutions Engineer in the UK

A Long time in UK National Health Service!

8 years as a Partner

10 Years at Cisco!

- Pilot!
- Biker
- Ex-drummer
  
- I'm Welsh!



# Why Secure the Wired Network?

- Standard Practice on Wireless – so why not Wired?
- Prevent Shadow-IT!
- ACME – adds, changes, moves, errors!
- Malicious attacks
- Rapid deployment
- Agile IT and Users!
- Security, segmentation, consistency.
- Only authorized endpoints!
- Use Identity



# Session Objectives

## We Will be :

- Demonstrate how Catalyst Centre greatly simplifies deployment
- Provide a working example of how to deploy 801.x
- Demonstrate how TrustSec enhances access control
- Show how to get visibility into endpoints
- Explore SDA as an option
- Bonus of Posture Checking! (time permitting!)

## We Wont be :

- Deep dive on how to setup ISE!
- Explore every option for IBNS
- Deep dive on ISE Policies – but enough will be provided!
- Explore all available options for Posture – there are simply too many!

# Zero Trust

- Never assume trust
- Always verify
- Enforce least privilege
- Reaffirm when trust changes

# ISE – Deep Dive – BRKSEC-2091

This is a really  
good deep dive!

## Cisco ISE Performance, Scalability and Best Practices

Pavan Gupta, Technical Marketing Engineer  
BRKSEC-2091

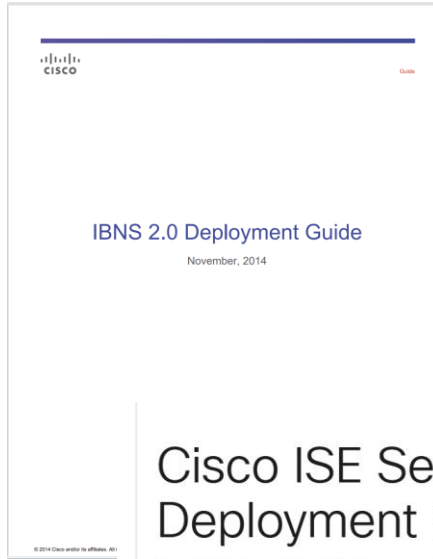
*CISCO Live!*

#CiscoLive

*CISCO Live!*

# Challenges

- Time to deploy
- Perception
- Risk?
- It's complicated!!
- What's out there?



## Cisco ISE Secure Wired Access Prescriptive Deployment Guide



# Cisco ISE Secure Wired Access Prescriptive Deployment Guide



<https://community.cisco.com/t5/security-knowledge-base/ise-secure-wired-access-prescriptive-deployment-guide/ta-p/3641515#toc-hId--1823767250>

# There's a lot of config...

```
aaa new-model
!
!
aaa group server radius dnac-client-radius-group
 server name dnac-radius_172.16.33.12
 ip radius source-interface Vlan210
!
aaa authentication login default local
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec default local
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group dnac-client-radius-group
!
!
aaa server radius dynamic-author
 client 172.16.33.12 server-key 7 xxxxxxxx
!
aaa session-id common
switch 1 provision c9300-24u
!
```

```
template Port-Dot1x-Default
dot1x pae authenticator
dot1x timeout tx-period 7
dot1x max-reauth-req 3
spanning-tree portfast
spanning-tree bpdupfilter enable
switchport access vlan 208
switchport mode access
switchport nonegotiate
switchport voice vlan 202
subscriber aging probe
mab
access-session control-direction in
access-session port-control auto
authentication periodic
authentication timer reauthenticate server
service-policy type control subscriber Dot1x-Default
description ** Port for Endpoints **
ip dhcp snooping limit rate 10
!
!
```

```
policy-map type control subscriber Dot1x-Default
event session-started match-all
10 class always do-until-failure
10 authenticate using dot1x priority 10
event authentication-failure match-first
5 class Dot1x_Failed do-until-failure
10 terminate dot1x
20 authenticate using mab priority 20
10 class AAA-Down_UnAuth_Host do-until-failure
10 clear-authenticated-data-hosts-on-port
20 activate service-template Critical_Access
30 activate service-template Critical_Voice
40 authorize
50 pause reauthentication
20 class AAA-Down_Auth_Host do-until-failure
10 pause reauthentication
20 authorize
30 class Dot1x_No-Resp do-until-failure
10 terminate dot1x
20 authenticate using mab priority 20
40 class MAB_Failed do-until-failure
10 terminate mab
20 authentication-restart 60
60 class always do-until-failure
10 terminate dot1x
20 terminate mab
30 authentication-restart 60
event agent-found match-all
10 class always do-until-failure
10 terminate mab
20 authenticate using dot1x priority 10
event aaa-available match-all
10 class Critical_Auth do-until-failure
10 clear-session
20 class NOT_Critical_Auth do-until-failure
10 resume reauthentication
event inactivity-timeout match-all
10 class always do-until-failure
10 clear-session
event authentication-success match-all
10 class always do-until-failure
10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
event violation match-all
10 class always do-until-failure
10 restrict
```



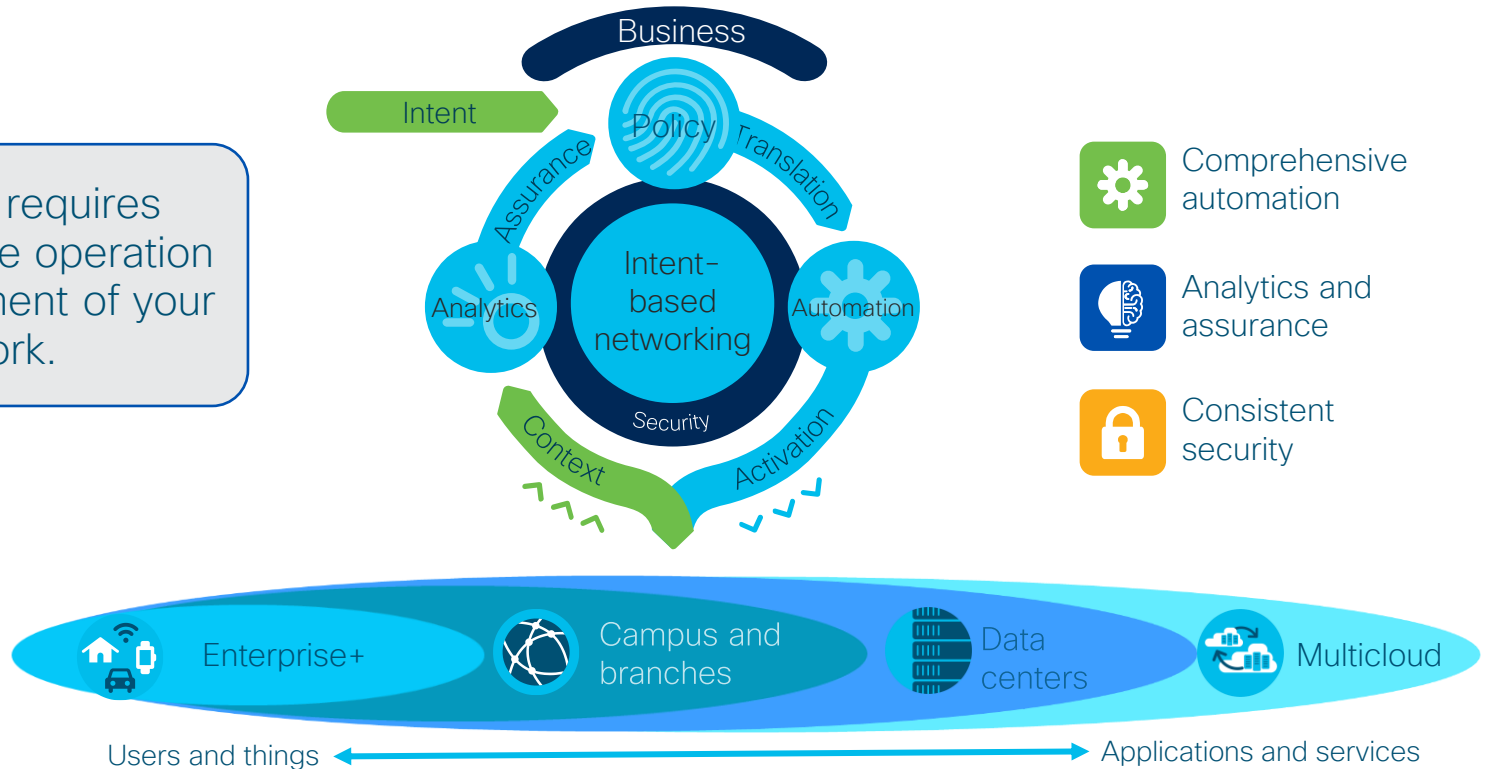
# Go Beyond with Catalyst Centre!

CISCO *Live!*



# Intent-based networking

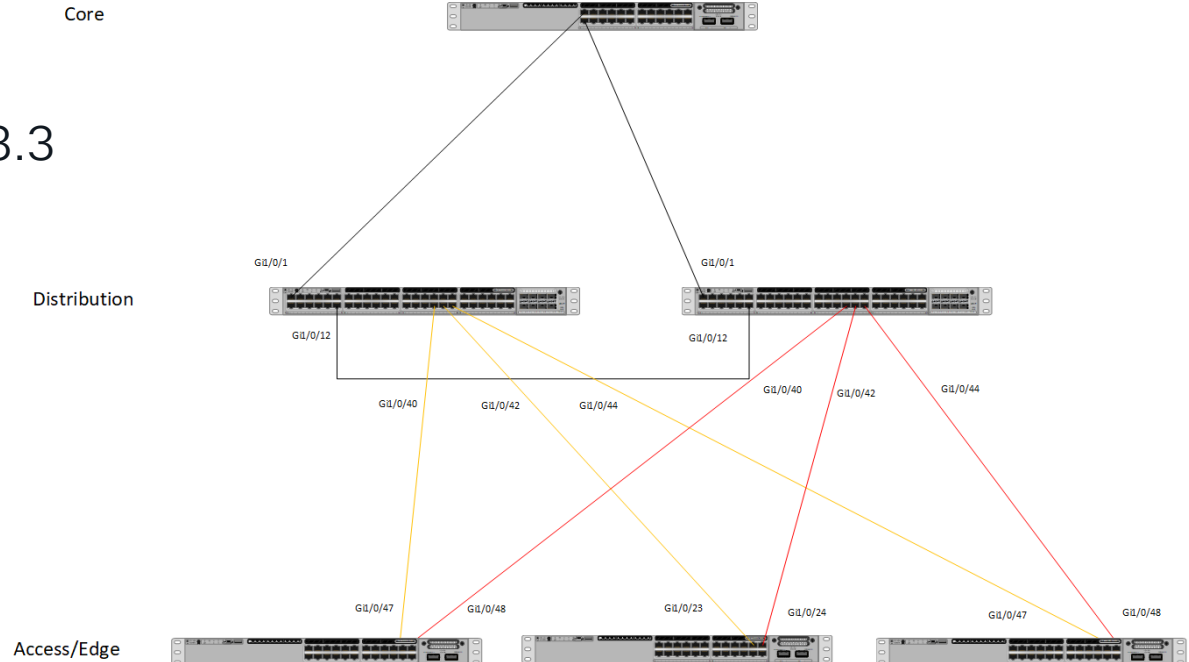
IT success requires automating the operation and management of your network.





# The network we are using

All Catalyst 9Ks  
Identity Services Engine 3.3  
Catalyst Centre 2.3.7.7



# Start with Catalyst Centre

The screenshot displays the Cisco Catalyst Center interface for Network Hierarchy. The top navigation bar includes the Cisco logo, the title 'Catalyst Center', and the current view 'Design / Network Hierarchy'. On the right side of the top bar, there are icons for favorites, search, refresh, help, and notifications, along with a user profile for 'admin'.

The main interface is divided into three sections:

- Left Panel:** A search bar for 'Search Hierarchy' and a search help icon. Below it is a tree view showing the hierarchy: 'Global' (expanded) > 'CiscoUKI' (expanded) > 'Birmingham', 'Cardiff', 'Coventry', 'Didsbury', 'Spectrum', 'Edinburgh', 'Feltham', 'London', 'Manchester', and 'Reading'.
- Top Center:** Action buttons for '+ Add Site', 'Import', and 'Export'.
- Right Panel:** A search bar for 'Search for a building' and a menu icon.

The central area is a map of the United Kingdom and Ireland. Several locations are marked with blue circular icons containing numbers:

- A blue pin icon labeled 'Gyleview' is located near Glasgow.
- A blue circle with the number '2' is located near Liverpool.
- Another blue circle with the number '2' is located near Nottingham.
- A blue circle with the number '5' is located near Bristol.
- A blue pin icon labeled 'Catalyst SBARC' is located near Bristol.

The map also shows various geographical features and cities across the UK and Ireland, including London, Manchester, Edinburgh, and Dublin.

# Check Telemetry and Wired Data Collection

**Cisco Catalyst Center** Design / Network Settings

Servers Device Credentials IP Address Pools Wireless **Telemetry** Security and Trust

Configure Syslog, Traps and NetFlow properties for your devices. The system will deploy these settings when devices are assigned to a site or provisioned.

Catalyst Center is your default SNMP collector. It polls network devices to gather telemetry data. [View details](#) on the metrics gathered and the frequency with which they are collected.

Add an external syslog server

▼ Application Visibility

When assigning Catalyst 9000 or Traffic Telemetry Appliance devices to the site, enable NetFlow Application Telemetry and Controller-Based Application Recognition by default. ⓘ

**Enable by default on supported wired access devices**

Choose the destination collector for Netflow records sent from network devices.

**Use Catalyst Center as the Netflow Collector**

Use Cisco Telemetry Broker (CTB) or UDP director

▼ Wired Endpoint Data Collection

The primary function of this feature is to track the presence, location, and movement of wired endpoints in the network. Traffic received from endpoints is used to extract and store their identity information (MAC address and IP address). Other features, such as IEEE 802.1X, web authentication, Cisco Security Groups (formerly TrustSec), SD-Access, and Assurance, depend on this identity information to operate properly.

Wired Endpoint Data Collection enables Device Tracking policies on devices assigned to the Access role in Inventory.

**Enable Catalyst Center Wired Endpoint Data Collection At This Site**

Disable Catalyst Center Wired Endpoint Data Collection At This Site ⓘ

▼ Wireless Controller, Access Point and Wireless Clients Health

Enables Streaming Telemetry on your wireless controllers in order to determine the health of your wireless controller, access points and wireless clients.

# Check Device Credentials

The screenshot displays the Cisco Catalyst Center interface. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the path 'Design / Network Settings'. The user is logged in as 'admin'. The main content area is divided into two panes. The left pane, titled 'Device Credentials', shows configuration options for CLI, SNMPv2c Read, and SNMPv2c Write. The right pane, titled 'Manage Credentials', shows a table of configured credentials.

**Device Credentials Configuration:**

- CLI:** Assign a CLI credential. Credential: `sdacisco`.
- SNMPv2c Read:** Assign an SNMPv2c Read credential. Credential: `public`.
- SNMPv2c Write:** Assign an SNMPv2c Write credential. Credential: `private`.

**Manage Credentials Table:**

Name	Type	Status	Actions
private	SNMPv2c Write	○ ---	...
public	SNMPv2c Read	○ ---	...
sdacisco	CLI	○ ---	...
sdahttp	HTTP(S) Read	○ ---	...
sdahttpsrw	HTTP(S) Write	○ ---	...

# Typical Port Configurations

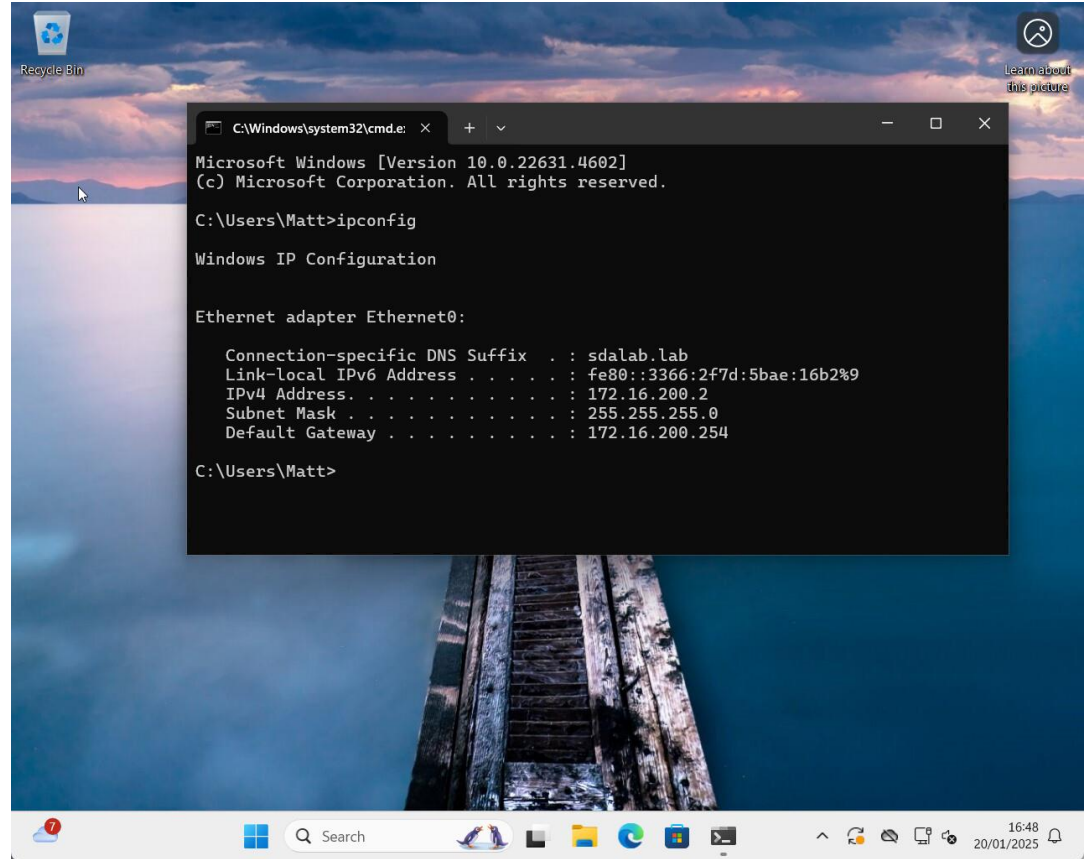
```
edgel#showint
interface GigabitEthernet1/0/1
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/5
 switchport access vlan 208
 switchport mode access
```

```
edge2#showint
interface GigabitEthernet1/0/1
 switchport access vlan 206
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/4
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
```

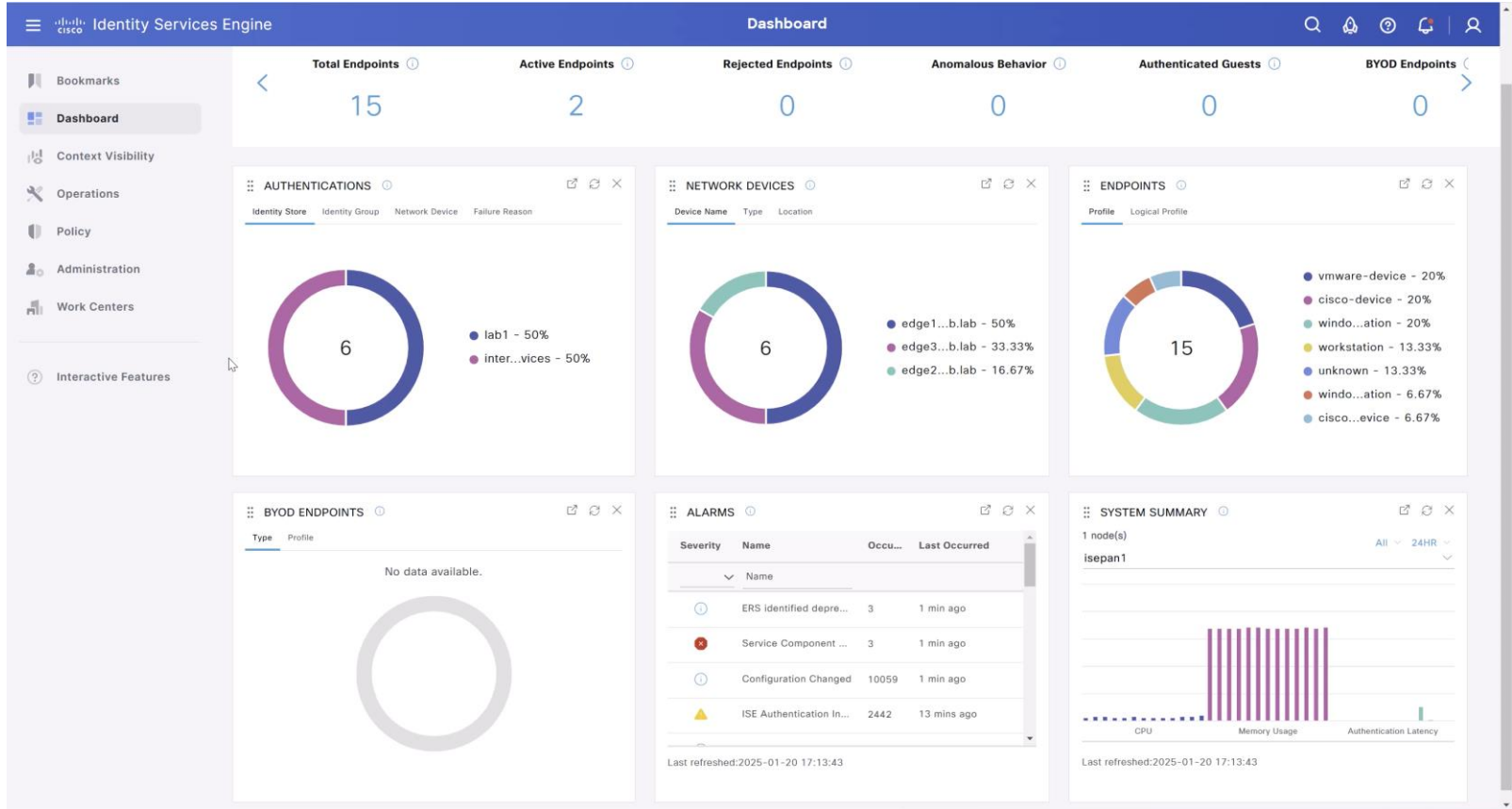
Static vlan  
assignment

# Endpoints Connected

DHCP Assigned IP  
No Port Security!



# Get ISE Ready – Deployment demo



# Get ISE Ready – Identity Stores demo

The screenshot displays the Cisco Identity Services Engine (ISE) Administration / System interface. The top navigation bar includes the Cisco logo, the text "Identity Services Engine", and the current page title "Administration / System". The main navigation menu on the left lists various sections: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (highlighted), Work Centers, and Interactive Features. The main content area is divided into several tabs: Deployment (selected), Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, and Settings. The "Deployment" tab is active, showing a tree view of the deployment structure with "isepan1" selected. The "Edit Node" page for "isepan1" is displayed, with the "Profiling Configuration" sub-tab selected. This sub-tab contains two sections: "NETFLOW" and "DHCP". The "NETFLOW" section is enabled (toggle is on) and shows the following configuration: Interface: GigabitEthernet 0, Port: 9996, and Description: "The Netflow probe collects Netflow packets sent to it from Routers." The "DHCP" section is also enabled (toggle is on) and shows the following configuration: Interface: GigabitEthernet 0, Port: 67.



# ISE and Catalyst Centre

The screenshot displays the Cisco Catalyst Center interface for System 360. The top navigation bar includes the Cisco logo, the text 'Catalyst Center', and the system path 'System / System 360'. On the right side of the navigation bar, there are icons for favorites, search, refresh, help, and notifications, along with a user profile for 'admin'.

The main content area is divided into several sections:

- System 360**: Includes 'System Health' and 'Service Explorer'. A card shows the IP address '172.16.99.199' with a 'View 140 Services' link. Another card indicates that 'Enabling High Availability requires installing a minimum of 3 Cisco Catalyst Center hosts.' with a 'View Guide' link. A 'Monitoring Log Explorer' card is also present.
- System Management**: Contains three sub-cards:
  - Software Management** (As of Jan 20, 2025 5:07 PM): Shows 'Connected to Cisco's software server.' and 'A release is being downloaded' with a 'View' link.
  - Backups** (As of Jan 20, 2025 5:06 PM): Shows 'Last successful backup took place on Oct 18, 2024 11:55 AM.' and 'There are no backups scheduled' with 'View' and 'Schedule' links.
  - Application Health** (As of Jan 20, 2025 5:06 PM): Shows 'Automation' and 'Assurance' status.
- Externally Connected Systems**: Contains two sub-cards:
  - Identity Services Engine (ISE)** (As of Jan 20, 2025 5:06 PM): Shows 'No ISE server configured.' with a 'Configure' link.
  - IP Address Manager (IPAM)** (As of Jan 20, 2025 5:06 PM): Shows 'No IPAM server configured.' with a 'Configure' link.

# ISE and Catalyst Centre

The screenshot shows the Cisco Catalyst Center interface. At the top, the breadcrumb is 'System / Settings'. The page title is 'Authentication and Policy Servers'. Below the title, there is a descriptive text: 'Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.' There are 'Add' and 'Export' buttons. A table with the following structure is present:

Protocol	Type	Status	Actions
No data to display			

The left navigation menu includes: Certificates, Trusted Certificates, System Certificates, Certificate Authority, Device Certificates, Cisco Accounts, PnP Connect, Cisco.com Credentials, Smart Account, Smart Licensing, SSM Connection Mode, Device Settings, PnP AP Location, Image Distribution Servers, Device Controllability, Network Resync Interval, SNMP, ICMP Ping, Device EULA Acceptance, PnP Device Authorization, Device Prompts, Configuration Archive, External Services, and Umbrella.

# ISE and Catalyst Centre

The screenshot displays the Cisco Catalyst Center web interface. On the left, a dark sidebar contains a navigation menu with categories like Design, Policy, Provision, Assurance, Workflows, Tools, Platform, Activities, Reports, System, and Explore. The 'System' category is expanded, and 'Network Settings' is highlighted with a red box and a red arrow. The main content area shows the 'Policy Servers' configuration page. At the top, it says 'System / Settings' and 'admin'. Below the title, there is a table with columns for Protocol, Type, Status, and Actions. One entry is visible: RADIUS, ISE, ACTIVE.

Protocol	Type	Status	Actions
RADIUS	ISE	ACTIVE	...

# ISE and Catalyst Centre - demo

The screenshot shows the Cisco Catalyst Center interface. At the top, the navigation bar includes the Cisco logo, 'Catalyst Center', and the path 'Design / Network Settings'. On the right side of the navigation bar are icons for star, search, refresh, help, and notifications, along with a user profile 'admin'. Below the navigation bar, there are tabs for 'Servers', 'Device Credentials', 'IP Address Pools', 'Wireless', 'Telemetry', and 'Security and Trust'. The 'Servers' tab is active.

On the left side, there is a 'Find Hierarchy' search bar and a tree view showing 'Global' and 'CiscoUKI'. The main content area is titled 'Configure external network servers, assign time zones to sites, and customize device CLI login banner messages. The system will deploy these settings when devices are provisioned.'

The configuration is organized into sections:

- AAA**: Select AAA or Cisco Identity Services Engine (ISE) servers for network, client, and endpoint authentication. It has sub-tabs for 'Network' and 'Client/Endpoint'. There is an unchecked checkbox for 'Add AAA servers'.
- DHCP**: Specify one or more dedicated DHCP servers for managing client device networking configuration. It has a checked checkbox for 'Add DHCP servers' and an input field for 'IP Address\*' containing '172.16.33.10' with a plus sign to add more.
- DNS**: Configure your network's domain name and specify DNS servers for hostname resolution. It has checked checkboxes for 'Set a domain name' and 'Add DNS servers'. The 'Domain Name\*' is 'sdalab.lab' and the 'IP Address\*' is '172.16.33.10' with a plus sign to add more.

At the bottom right, there are 'Reset' and 'Save' buttons.

# Discover the network! - demo

Cisco Catalyst Center Provision / Inventory

Spectrum

All Routers Switches Wireless Controllers Access Points Sensors

Devices (0) Focus: Inventory

Take a tour Export

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Tag Add Device Edit Device Delete Device Actions

As of: Jan 20, 2025 5:40 PM

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Updated	Serial Number	PI
No devices available												

DEVICE WORK ITEMS

- Unreachable
- Unassigned
- Untagged
- Failed Provision
- Non Compliant
- Outdated Software Image
- No Golden Image
- Failed Image Prechecks
- Under Maintenance
- Security Advisories

# Assign to Site - demo

Provision / Inventory

Global

Device Work Items:

- Unreachable
- Unassigned
- Untagged
- Failed Provision
- Non Compliant
- Outdated Software Image
- No Golden Image
- Failed Image Prechecks
- Under Maintenance
- Security Advisories

Devices (5) Focus: Inventory

0 Selected Tag Add Device Edit Device Delete Device Actions

As of: Jan 20, 2025 5:54 PM

Tags	Device Name	IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Updated	Serial
	<a href="#">edge1.sdalab.lab</a>	172.16.210.251	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.12.3	8 minutes ago <a href="#">Sync Details</a>	FOC:
	<a href="#">edge2.sdalab.lab</a>	172.16.210.250	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.12.3	6 minutes ago <a href="#">Sync Details</a>	FCW
	<a href="#">edge3.sdalab.lab</a>	172.16.210.249	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.12.3	8 minutes ago <a href="#">Sync Details</a>	FOC:
	<a href="#">SDA_CPB1.sdalab.lab</a>	172.16.210.253	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.12.3	8 minutes ago <a href="#">Sync Details</a>	FCW
	<a href="#">SDA_CPB2.sdalab.lab</a>	172.16.210.252	Cisco	Reachable	Not Scanned	Managed	Compliant	Assign	17.12.3	8 minutes ago <a href="#">Sync Details</a>	FCW

5 Record(s) Show Records: 25 1 - 5

# What's just happened? – config applied by Catalyst Centre – there's a lot more!



```
!
aaa new-model
!
aaa group server radius dnac-client-radius-group
  server name dnac-radius_172.16.33.12
  ip radius source-interface Vlan210
!
aaa authentication login default local
aaa authentication login dnac-cts-list group dnac-client-radius-group local
aaa authentication dot1x default group dnac-client-radius-group
aaa authorization exec default local
aaa authorization network default group dnac-client-radius-group
aaa authorization network dnac-cts-list group dnac-client-radius-group
aaa accounting update newinfo periodic 2880
aaa accounting identity default start-stop group dnac-client-radius-group
!
!
aaa server radius dynamic-author
  client 172.16.33.12 server-key 7 123A540411045D56797F71
!
aaa session-id common
!
ip name-server 172.16.33.10
ip domain lookup source-interface Vlan210
!
```

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
radius server dnac-radius_172.16.33.12
  address ipv4 172.16.33.12 auth-port 1812 acct-port 1813
  timeout 4
  retransmit 3
  automate-tester username dummy ignore-acct-port probe-on
  pac key 7 06255E324F41584B564347
!
!
```

```
!
crypto pki certificate chain DNAC-CA
  certificate ca 409D8A8FF087ACB831BEC9C9B5747A83BB9E23AB nvram:CiscoDNACent#23ABCA.cer
crypto pki certificate chain sdn-network-infra-iwan
  certificate 6B0F468D14A62B8CB0E836C0DA095D1E27110AB0 nvram:sdn-network-#AB0.cer
  certificate ca 190CF73F12CEDE03028E0765E0C1BB0618B5DB2B nvram:sdn-network-#DB2BCA.cer
!
cts authorization list dnac-cts-list
!
```

# It all gets added to ISE

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar shows "Administration / Network Resources". The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration (selected), Work Centers, and Interactive Features. The main content area is titled "Network Devices" and shows a table of devices. A notification bubble in the top right corner says "Click here to do visibility setup Do not show this again." Below the table, there are action buttons: Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete. The table has columns for Name, IP/Mask, Profile Name, Location, Type, and Description. Five devices are listed, all with "All Locations" and "All Device Types".

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	SDA_CP1...	172.16.34...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	SDA_CP2...	172.16.34...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	edge1.sdala...	172.16.21...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	edge2.sdala...	172.16.21...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	edge3.sdala...	172.16.21...	Cisco	All Locations	All Device Types	



# With Trustsec – Security Group

The image displays two screenshots of the Cisco Identity Services Engine (ISE) Administration console, specifically the 'Administration / Network Resources' section.

**Top Screenshot: Advanced TrustSec Settings**

- Navigation:** Bookmarks, Dashboard, Context Visibility, Operations, Policy, **Administration**, Work Centers, Interactive Features.
- Network Devices:** Default Device, Device Security Settings.
- Advanced TrustSec Settings:**
  - Device Authentication Settings:**
    - Use Device ID for TrustSec Identification
    - Device Id: `b3293cd2e6e94633b826b7286575ebfa`
    - Password: [Redacted] [Show](#)
  - HTTP REST API settings:**
    - Enable HTTP REST API
    - Username: [Redacted]
    - Password: [Redacted]
    - Support TrustSec Verification reports
  - TrustSec Notifications and Updates:**
    - Download environment data every: 1 Days
    - Download peer authorization policy every: 1 Days
    - Reauthentication every: 1 Days
    - Download SGACL lists every: 1 Days
    - Other TrustSec devices to trust this device
    - Send configuration changes to device

**Bottom Screenshot: Device Configuration Deployment**

- CLI (SSH):** Send from: `lwp@1` [Test connection](#), Ssh Key: [Redacted]
- Device Configuration Deployment:**
  - Include this device when deploying Security Group Tag Mapping Updates
  - Device Interface Credentials:**
    - EXEC Mode Username: `sdacisco`
    - EXEC Mode Password: [Redacted] [Show](#)
    - Enable Mode Password: [Redacted] [Show](#)
  - Out Of Band (OOB) TrustSec PAC:**
    - Issue Date: 20 Jan 2025 18:01:21 GMT
    - Expiration Date: 20 Apr 2025 18:01:21 GMT
    - Issued By: Network Device
    - [Generate PAC](#)
- Buttons:** [Save](#), [Reset](#)

# Catalyst Centre Template Delivery – making it simple!

# How to deliver config – reliably!

- Use a Jinja/Velocity template – it's CLI
- Deploy to multiple devices – concurrently
- No errors!

# Create a template and project

Design / CLI Templates

Design | Policy | Provision | Assurance | Workflows | Tools | Platform | Activities | Reports | System | Explore

Network Hierarchy | Network Settings | Network Profiles | Image Repository | Service Provider Profiles | **CLI Templates** | Feature Templates | Authentication Templates

Delete | Provision Templates

As of: Jan 20, 2025 8:21 PM

Project	Type	Version	Commit State	Provision Status	Network Profiles	Actions
Sample Jinja Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Cloud DayN Templates	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
Onboarding Configuration	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
Cloud DayN Templates	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
EEM_Project	Regular	1	● 22 Oct 2024 09:49 PM	Not Provisioned	Attach	...
Sample Jinja Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Sample Velocity Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Sample Jinja Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Sample Velocity Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Sample Jinja Templates	Regular	Not Committed	▲ Not Committed	Not Provisioned	NA	...
Onboarding Configuration	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
Onboarding Configuration	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
Cloud DayN Templates	Regular	1	● 17 Oct 2024 09:09 PM	Not Provisioned	Attach	...

Show Records: 25 | 1 - 20 | 1

https://10.53.0.110/dna/design/templatesHub

# Create a template and project

Catalyst Center Design / CLI Templates

admin

SUMMARY

- > Project Name (5)
- > Type (1)
- > Template Language (2)
- > Category (2)
- > Device Family (2)
- > Device Series (2)
- > Commit State (2)
- > Provision Status (1)
- > Potential Design Conflicts (2)

Templates (20)

Search

0 Selected Export Import Delete Provision Templates

As of: Jan 20, 2025

Add New Project New Template

<input type="checkbox"/>	Name	Project	Type	Version	Commit State	Provision Status	Network Profiles	Actions
<input type="checkbox"/>	Base Config	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	DMVPN for Cloud Router - Sy...	Cloud DayN Templates	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	DMVPN Hub for Cloud Router...	Onboarding Configuration	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	DMVPN Spoke for Branch Rout...	Cloud DayN Templates	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	EEM_CLI_PUSH	EEM_Project	Regular	1	22 Oct 2024 09:49 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	For-Loop-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	For-Loop-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	If-Condition-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	If-Condition-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	Implicit-Variables	Sample Jinja Templates	Regular	Not Committed	Not Committed	Not Provisioned	NA	...
<input type="checkbox"/>	IPsec 1 Branch for Cloud Ro...	Onboarding Configuration	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	IPsec 2 Branch for Cloud Ro...	Onboarding Configuration	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...
<input type="checkbox"/>	IPsec for Branch Router - S...	Cloud DayN Templates	Regular	1	17 Oct 2024 09:09 PM	Not Provisioned	Attach	...

20 Record(s) Show Records: 25 1 - 20

# Create a template and project

The screenshot shows the Cisco Catalyst Center interface for managing CLI Templates. The main view displays a table of 20 templates. An 'Add New Project' dialog is open on the right, showing the 'Project Name\*' field with the value 'CL\_DOT1X\_GO' and an empty 'Project Description' field. The dialog has 'Cancel' and 'Continue' buttons at the bottom.

**Templates (20)**

<input type="checkbox"/>	Name	Project	Type	Version	Commit State
<input type="checkbox"/>	Base Config	Sample Jinja Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	DMVPN for Cloud Router - Sy...	Cloud DayN Templates	Regular	1	17 Oct 2024
<input type="checkbox"/>	DMVPN Hub for Cloud Router...	Onboarding Configuration	Regular	1	17 Oct 2024
<input type="checkbox"/>	DMVPN Spoke for Branch Rout...	Cloud DayN Templates	Regular	1	17 Oct 2024
<input type="checkbox"/>	EEM_CLI_PUSH	EEM_Project	Regular	1	22 Oct 2024
<input type="checkbox"/>	For-Loop-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	For-Loop-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	If-Condition-Jinja	Sample Jinja Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	If-Condition-Velocity	Sample Velocity Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	Implicit-Variables	Sample Jinja Templates	Regular	Not Committed	Not Committed
<input type="checkbox"/>	IPsec 1 Branch for Cloud Ro...	Onboarding Configuration	Regular	1	17 Oct 2024
<input type="checkbox"/>	IPsec 2 Branch for Cloud Ro...	Onboarding Configuration	Regular	1	17 Oct 2024
<input type="checkbox"/>	IPsec for Branch Router - S...	Cloud DayN Templates	Regular	1	17 Oct 2024

20 Record(s)

**Add New Project**

Project Name\*  
CL\_DOT1X\_GO

Project Description

Cancel Continue

# The really useful bit! – all the template.



```
! create test user on ISE internal DB as well
username isetest secret 0 C1sco12345

!
radius-server ysa send authentication
radius-server ysa send accounting

! Local ACLs
!
ip access-list extended ACL_Default
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 permit tcp any host 172.16.33.10 eq 8443
 deny ip any any
!
! Create ACL used when AAA is down to fail open (Internet only)
ip access-list extended AAA-Down
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny ip any 10.0.0.0 0.255.255.255
 deny ip any 192.168.0.0 0.0.255.255
 permit ip any any
! Create Blackhole ACL
ip access-list extended ACL_Blackhole
 permit tcp any any eq www
 deny ip any any

! Prevent consumption of BPDUs for all portfast edge ports globally
spanning-tree portfast bpdupfilter default

! Global 802.1x commands
! Enable 802.1x globally
dot1x system-auth-control
dot1x critical eapol

! Allow session tear down when MAC address detected elsewhere
no access-session mac-move deny
access-session acl default passthrough
```

```
! This is for device profiling ***
! Enable device sensors
! DHCP snooping is required for device sensor data to work properly
ip dhcp snooping
no ip dhcp snooping information option
! VLAN list is comma separated
ip dhcp snooping vlan 200,202,204,206,208

! Enable specific device sensors for profiling
device-sensor filter-list dhcp list dhcp_list
option name host-name
option name requested-address
option name parameter-request-list
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list dhcp_list
! Enable CDP globally
cdp run
device-sensor filter-list cdp list cdp_list
tlv name device-name
tlv name address-type
tlv name capabilities-type
tlv name platform-type
device-sensor filter-spec cdp include list cdp_list
! Enable LLDP globally
lldp run
device-sensor filter-list lldp list lldp_list
tlv name system-name
tlv name system-description
tlv name system-capabilities
device-sensor filter-spec lldp include list lldp_list
! Send sensor data to ISE and disable local analyzer
device-sensor notify all-changes
```

# The really useful bit! – all the template.



```
! Include CDP, LLDP, and DHCP information for the access session
access-session attributes filter-list list sensor_list
cdp
lldp
dhcp
access-session accounting attributes filter-spec include list sensor_list
access-session authentication attributes filter-spec include list sensor_list
```

```
! This are the dot1x bits ****
! Create critical endpoint vlan access
service-template Critical_Access
  vlan 208
  access-group AAA-Down
```

```
! Create critical phone vlan access
service-template Critical_Voice
  voice vlan
```

```
! Configure control classes
class-map type control subscriber match-all AAA-Down_Auth_Host
  match result-type aaa-timeout
  match authorization-status authorized
!
class-map type control subscriber match-all AAA-Down_UnAuth_Host
  match result-type aaa-timeout
  match authorization-status unauthorized
!
class-map type control subscriber match-all Dot1x
  match method dot1x
!
class-map type control subscriber match-all Dot1x_Failed
  match method dot1x
  match result-type method dot1x authoritative
!
class-map type control subscriber match-all Dot1x_No-Resp
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all Dot1x_Timeout
  match method dot1x
  match result-type method dot1x method-timeout
!
class-map type control subscriber match-any Critical_Auth
  match activated-service-template Critical_Access
  match activated-service-template Critical_Voice
```

```
class-map type control subscriber match-all MAB
  match method mab
!
class-map type control subscriber match-all MAB_Failed
  match method mab
  match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_Critical_Auth
  match activated-service-template Critical_Access
  match activated-service-template Critical_Voice
!
```



# The really useful bit! – all the template.



```
! Configure policy maps
! Policy map applied to all Dot1xMAB interfaces
policy-map type control subscriber Dot1x-Default
event session-started match-all
  10 class always do-until-failure
  10 authenticate using dot1x priority 10
event authentication-failure match-first
  5 class Dot1x_Failed do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  10 class AAA-Down_UnAuth_Host do-until-failure
  10 clear-authenticated-data-hosts-on-port
  20 activate service-template Critical_Access
  30 activate service-template Critical_Voice
  40 authorize
  50 pause reauthentication
  20 class AAA-Down_Auth_Host do-until-failure
  10 pause reauthentication
  20 authorize
  30 class Dot1x_No-Resp do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
  40 class MAB_Failed do-until-failure
  10 terminate mab
  20 authentication-restart 60
  60 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event agent-found match-all
  10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x priority 10
event aaa-available match-all
  10 class Critical_Auth do-until-failure
  10 clear-session
  20 class NOT_Critical_Auth do-until-failure
  10 resume reauthentication
event inactivity-timeout match-all
  10 class always do-until-failure
  10 clear-session
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
event violation match-all
  10 class always do-until-failure
  10 restrict
```

```
! create port-templates ****
! Monitor mode or Low Impact port template
template Port-Dot1x-Default
  description ** Port for Endpoints **
  switchport mode access
  switchport access vlan 208
  switchport nonegotiate
  switchport voice vlan 202
  spanning-tree portfast
  spanning-tree bpdufilter enable
  authentication periodic
  authentication timer reauthenticate server
  mab
  access-session host-mode multi-auth
  access-session control-direction in
  no access-session closed
  dot1x pae authenticator
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
  access-session port-control auto
  spanning-tree portfast
  ip dhcp snooping limit rate 10
  subscriber aging inactivity-timer 8400 probe
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default
```

# The really useful bit! – all the template.



```
! Closed mode port template
template Port-Dot1x-Closed
  description ** Port for Endpoints **
  switchport mode access
  switchport access vlan 208
  switchport negotiate
  switchport voice vlan 202
  spanning-tree portfast
  spanning-tree bpduguard enable
  authentication periodic
  authentication timer reauthenticate server
  mab
  access-session host-mode multi-domain
  access-session control-direction in
  access-session closed
  dot1x pae authenticator
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
  access-session port-control auto
  spanning-tree portfast
  ip dhcp snooping limit rate 10
  subscriber aging inactivity-timer 8400 probe
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default

device-tracking tracking auto-source

! Standard IPDT policy - modify DNAC deployed one.
device-tracking policy IPDT_Policy
  security-level glean
  limit address-count 10
  tracking enable

! Only apply to a trunk port
device-tracking policy Disable_DT_Trunk
  trusted-port
  device-role switch

! Uplink interface must be trusted for DHCP traffic
! If there is a port channel configured for the uplink ports, add to the
! port channel interface configuration instead of the port interface.
interface range gi1/0/23 - 24
  ip dhcp snooping trust
```

```
! Closed mode
interface range GigabitEthernet1/0/1 - 12
  source template Port-Dot1x-Closed
  device-tracking attach-policy IPDT_Policy
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
```

```
! Trunk port configuration to disable device tracking
interface range gi1/0/23 - 24
  device-tracking attach-policy Disable_DT_Trunk
```

# The really useful bit! – or Monitor or Low Impact



```
! Access port interface configuration **
! Only apply one - monitor - low - closed
! Monitor Mode
!
!interface range GigabitEthernet1/0/1 - 12
!   source template Port-Dot1x-Default
!   device-tracking attach-policy IPDT_Policy
!   dot1x timeout tx-period 7
!   dot1x max-reauth-req 3

! Low Impact Mode
!|
!interface range GigabitEthernet1/0/1 - 12
!   source template Port-Dot1x-Default
!   ip access-group ACL_Default in
!   device-tracking attach-policy IPDT_Policy
!   dot1x timeout tx-period 7
!   dot1x max-reauth-req 3
```

Chose either Monitor, Low Impact or Closed Mode

# Demo – deploying 802.1x

CISCO *Live!*



# Did you know ?

In Monitor or Low Impact mode –

ISE will discover and profile your endpoints!!

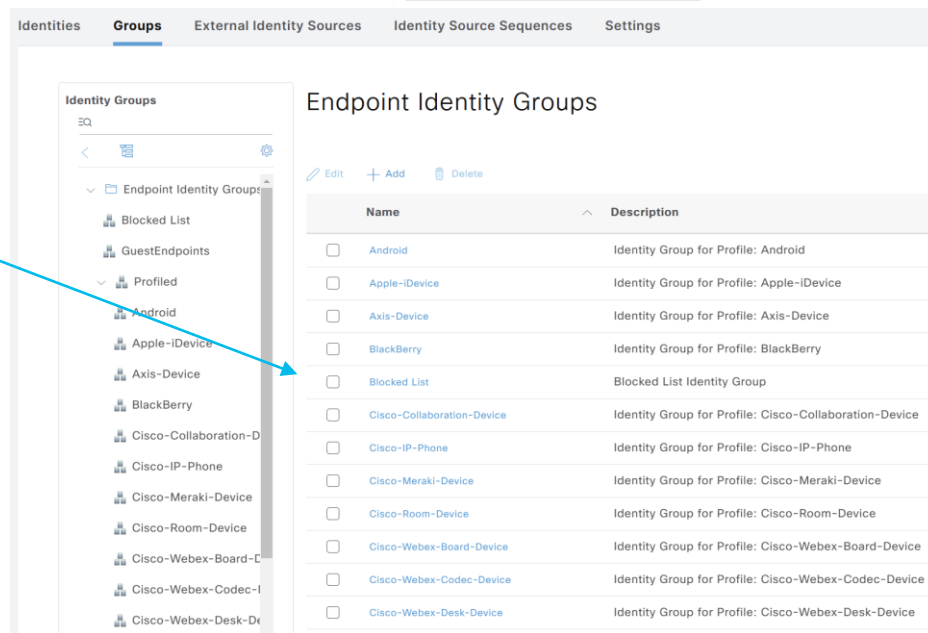
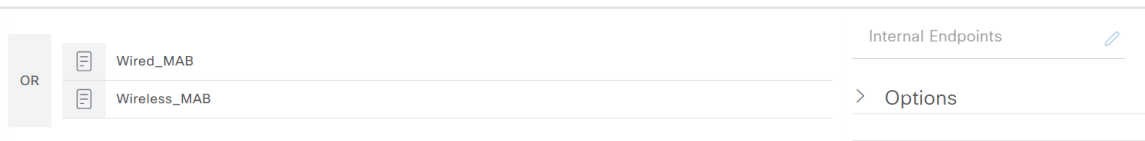
Discover what's on your network, and where it is!!

# But what if an endpoint cannot logon?!

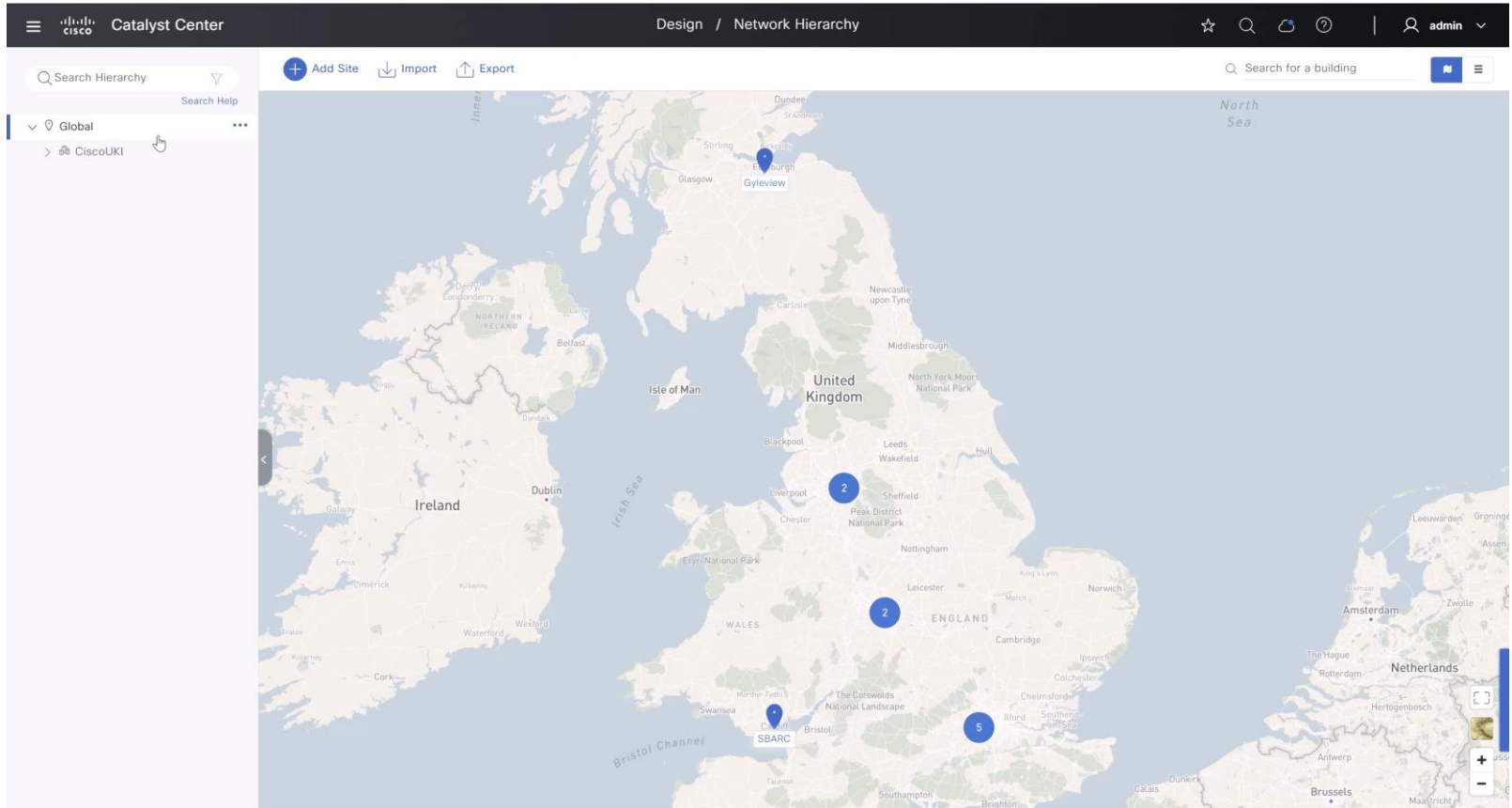
## MAB – MAC Authentication Bypass

Endpoints that used MAB  
stored in internal ISE DB –  
discovered by ISE during  
Low impact/Monitor

AuthZ rules created for  
non-auth endpoints!



# CLI via Catalyst Centre – in action demo



# CLI via Catalyst Centre – in action demo

The screenshot displays the Cisco Catalyst Centre web interface for editing a CLI template. The breadcrumb path is "CLI Templates / CL\_DOT1X\_TEMPLATE (1) / Properties". The "Templates" tab is selected. The interface includes a toolbar with options like "System Variables Assistant", "Template History", and "Attach to Network Profile". A status bar at the top right indicates "Auto saved: 8:31 PM (every 5 mins)".

```
261 interface range g11/0/23 - 24
262     ip dhcp snooping trust
263
264
265 ! Access port interface configuration **
266 ! Only apply one - monitor - low - closed
267 ! Monitor Mode
268 !
269 !interface range GigabitEthernet1/0/1 - 12
270 !     source template Port-Dot1x-Default
271 !     device-tracking attach-policy IPDT_Policy
272 !     dot1x timeout tx-period 7
273 !     dot1x max-reauth-req 3
274
275 ! Low Impact Mode
276 !
277 !interface range GigabitEthernet1/0/1 - 12
278 !     source template Port-Dot1x-Default
279 !     ip access-group ACL_Default in
280 !     device-tracking attach-policy IPDT_Policy
281 !     dot1x timeout tx-period 7
282 !     dot1x max-reauth-req 3
283
284 ! Closed mode
285 interface range GigabitEthernet1/0/1 - 12
286     source template Port-Dot1x-Closed
287     device-tracking attach-policy IPDT_Policy
288     dot1x timeout tx-period 7
289     dot1x max-reauth-req 3
290
291
292 ! Trunk port configuration to disable device tracking
293 interface range g11/0/23 - 24
294     device-tracking attach-policy Disable_DT_Trunk
295
296
```

At the bottom of the interface, there are three buttons: "Discard Changes", "Save", and "Commit".



# CLI via Catalyst Centre – in action demo

Network Profiles

[+ Add Profile](#)

Network Profiles (1)

Search Table

Profile Name ▾	Type	Sites	Action
CL_DOT1X_NP	Switching	3	<a href="#">Edit</a>   <a href="#">Delete</a>

1 Record(s) Show Records: 10 ▾ 1 - 1 < 1 >

# CLI via Catalyst Centre – Inventory

The screenshot shows the Cisco Catalyst Centre interface for the Inventory section. The top navigation bar includes the Cisco logo, 'Catalyst Center', and 'Provision / Inventory'. The user is logged in as 'admin'. The main content area is titled 'Devices (5)' and shows a list of devices with columns for Device Name, IP Address, Device Family, Provisioning Status, Template Provision Status, Template Conflict Status, and Last Provisioned. The devices listed are edge1.sdalab.lab, edge2.sdalab.lab, edge3.sdalab.lab, SDA\_CPB1.sdalab.lab, and SDA\_CPB2.sdalab.lab. The first three devices are provisioned successfully, while the last two are not provisioned. A left sidebar contains 'DEVICE WORK ITEMS' with various filters like 'Unreachable', 'Unassigned', etc. The bottom of the page shows '5 Record(s)' and pagination controls.

Global

Provision / Inventory

admin

Global

All Routers Switches Wireless Controllers Access Points Sensors

Devices (5) Focus: Templates

Take a tour Export

Click here to apply basic or advanced filters or view recently applied filters

0 Selected Tag Add Device Actions

As of: Jan 20, 2025 8:35 PM

Device Name	IP Address	Device Family	Provisioning Status	Template Provision Status	Template Conflict Status	Last Provisioned
edge1.sdalab.lab	172.16.210.251	Switches and Hubs (WLC Capable)	Success <a href="#">See Details</a>	1	0 Conflicts	3 hours ago
edge2.sdalab.lab	172.16.210.250	Switches and Hubs (WLC Capable)	Success <a href="#">See Details</a>	1	0 Conflicts	3 hours ago
edge3.sdalab.lab	172.16.210.249	Switches and Hubs (WLC Capable)	Success <a href="#">See Details</a>	1	0 Conflicts	3 hours ago
SDA_CPB1.sdalab.lab	172.16.210.253	Switches and Hubs (WLC Capable)	Success <a href="#">See Details</a>	Not Provisioned	Not Provisioned	3 hours ago
SDA_CPB2.sdalab.lab	172.16.210.252	Switches and Hubs (WLC Capable)	Success <a href="#">See Details</a>	Not Provisioned	Not Provisioned	3 hours ago

5 Record(s)

Show Records: 25 1 - 5

# Port after template



```
interface GigabitEthernet1/0/1
  switchport access vlan 208
  switchport mode access
  device-tracking attach-policy IPDT_Policy
  ip flow monitor dnacmonitor input
  ip flow monitor dnacmonitor_dns input
  ip flow monitor dnacmonitor_output
  ip flow monitor dnacmonitor_dns_output
  ipv6 flow monitor dnacmonitor_v6 input
  ipv6 flow monitor dnacmonitor_dns_v6 input
  ipv6 flow monitor dnacmonitor_v6_output
  ipv6 flow monitor dnacmonitor_dns_v6_output
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
  source template Port-Dot1x-Closed
  spanning-tree portfast
  ip nbar protocol-discovery
end
```

# Derived Config

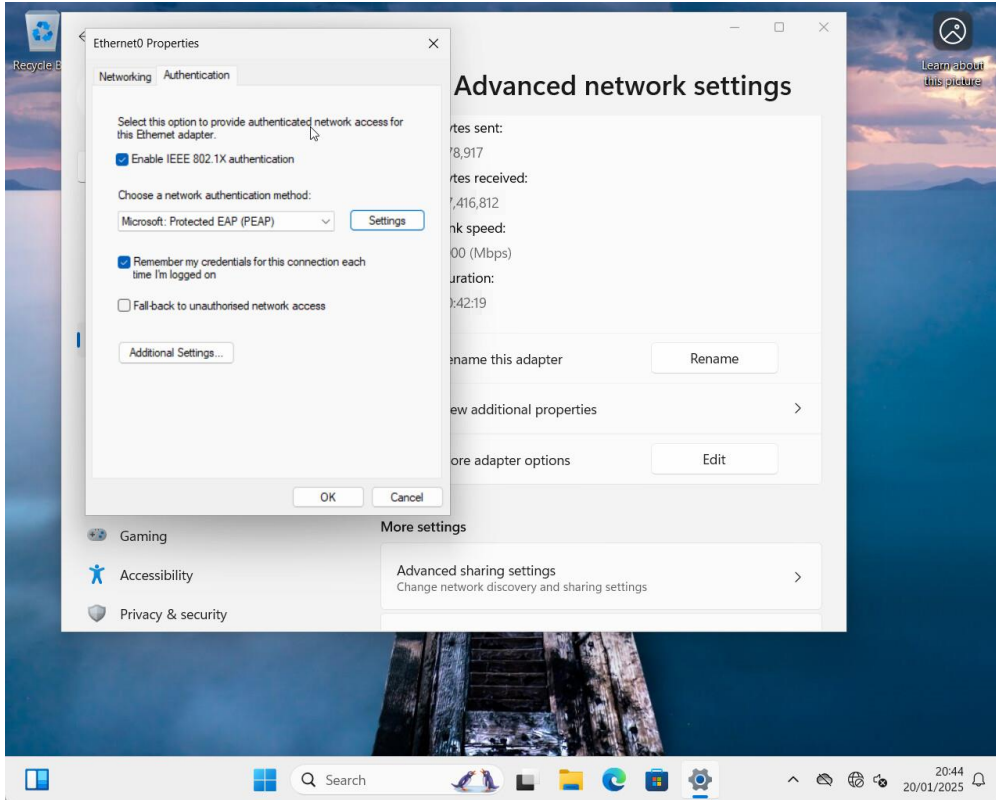
That's useful!

```
edge1#sho derived-config interface gil/0/1
Building configuration...

Derived configuration : 1020 bytes
!
interface GigabitEthernet1/0/1
 description ** Port for Endpoints **
 subscriber aging probe
 switchport access vlan 208
 switchport mode access
 switchport nonegotiate
 switchport voice vlan 202
 device-tracking attach-policy IPDT_Policy
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor_dns input
 ip flow monitor dnacmonitor_output
 ip flow monitor dnacmonitor_dns_output
 ipv6 flow monitor dnacmonitor_v6 input
 ipv6 flow monitor dnacmonitor_dns_v6 input
 ipv6 flow monitor dnacmonitor_v6_output
 ipv6 flow monitor dnacmonitor_dns_v6_output
 authentication periodic
 authentication timer reauthenticate server
 access-session host-mode multi-domain
 access-session control-direction in
 access-session closed
 access-session port-control auto
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 spanning-tree portfast
 spanning-tree bpdufilter enable
 service-policy type control subscriber Dot1x-Default
 ip nbar protocol-discovery
 ip dhcp snooping limit rate 10
end
```



# Enable wired auto on endpoints – windows example



Use Group Policy, MDM, Intune

# Check devices on ISE

**Operations / RADIUS**

**Live Logs** | Live Sessions

Click here to do visibility setup [Do not show this again.](#)

**Misconfigured Supplicants** 0 | **Misconfigured Network Devices** 0 | **RADIUS Drops** 0 | **Client Stopped Responding** 0 | **Repeat Counter** 1

Refresh: Every 10 seconds | Show: Latest 100 records | Within: Last 5 minutes

[Reset Repeat Counts](#) | [Export To](#) | Filter

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Prof...	Authentication Po...	Authoriz...	Authorization Profiles	IP Address
Jan 20, 2025 08:54:26.1...	●	🔒	1	SDALAB\matt	00:0C:29:D5:01...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_CORP	172.16.200.2...
Jan 20, 2025 08:54:24.9...	■	🔒		SDALAB\matt	00:0C:29:D5:01...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_CORP	
Jan 20, 2025 08:53:58.1...	●	🔒	0	SDALAB\glenn	00:0C:29:C2:FC...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_IOT	
Jan 20, 2025 08:53:58.0...	■	🔒		SDALAB\glenn	00:0C:29:C2:FC...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_IOT	
Jan 20, 2025 08:53:18.2...	●	🔒		00:0C:29:D5:0...	00:0C:29:D5:01...	Windows11-Wo...	Default >> MAB	Default >>...	DenyAccess	
Jan 20, 2025 08:52:31.0...	●	🔒		00:0C:29:C2:F...	00:0C:29:C2:FC...	Windows11-Wo...	Default >> MAB	Default >>...	DenyAccess	
Jan 20, 2025 08:51:50.2...	●	🔒		00:0C:29:D5:0...	00:0C:29:D5:01...	Windows11-Wo...	Default >> MAB	Default >>...	DenyAccess	
Jan 20, 2025 08:51:30.9...	●	🔒	0	SDALAB\james	00:0C:29:C0:D1...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_CONT	172.16.206.2...
Jan 20, 2025 08:51:30.9...	■	🔒		SDALAB\james	00:0C:29:C0:D1...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_CONT	172.16.206.2...
Jan 20, 2025 08:51:30.7...	■	🔒			00:0C:29:C0:D1...					
Jan 20, 2025 08:51:10.5...	■	🔒		SDALAB\james	00:0C:29:C0:D1...	Windows11-Wo...	Default >> Dot1X	Default >>...	SH_CONT	
Jan 20, 2025 08:51:03.0...	●	🔒		00:0C:29:C2:F...	00:0C:29:C2:FC...	Windows11-Wo...	Default >> MAB	Default >>...	DenyAccess	
Jan 20, 2025 08:50:22.1...	●	🔒		00:0C:29:D5:0...	00:0C:29:D5:01...	Windows11-Wo...	Default >> MAB	Default >>...	DenyAccess	

# ISE Policy Configuration – Policy Sets

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Policy Sets. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and the current page title 'Policy / Policy Sets'. A search bar and several utility icons are visible in the top right corner.

The main content area is titled 'Policy Sets' and features a table with the following columns: Status, Policy Set Name, Description, Conditions, Allowed Protocols / Server Sequence, Hits, Actions, and View. A search bar is located above the table. A single policy set is listed:

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	Default	Default policy set		Default Network Access	134		

At the bottom right of the table area, there are 'Reset' and 'Save' buttons.

# ISE Policy Configuration - Authentication

Identity Services Engine Policy / Policy Sets

Policy Sets → Default

Click here to do visibility setup [Do not show this again.](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	134

Authentication Policy(3)

Status	Rule Name	Conditions	Use	Hits	Actions
✓	Dot1X	OR Wired_802.1X Wireless_802.1X	LAB1 > Options	6	⚙️
✓	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	56	⚙️
✓	Default		All_User_ID_Stores > Options	44	⚙️

> Authorization Policy - Local Exceptions

> Authorization Policy - Global Exceptions

> Authorization Policy(19)



# ISE Policy Configuration - Authorization

Identity Services Engine Policy / Policy Sets

Click here to do visibility setup Do not show this again.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
		<ul style="list-style-type: none"> <li>Session-PostureStatus EQUALS Unknown</li> </ul>				
⊖	SH_CONT_NON_COMPLIANT	<ul style="list-style-type: none"> <li>Wired_802.1X</li> <li>LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT</li> <li>Session-PostureStatus EQUALS NonCompliant</li> </ul>	<ul style="list-style-type: none"> <li>CL_POSTURE_NONCOMPL...</li> <li>SH_CONT</li> </ul>	Select from list	0	⚙️
⊖	SH_CONT_COMPLIANT	<ul style="list-style-type: none"> <li>Wired_802.1X</li> <li>LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT</li> <li>Session-PostureStatus EQUALS Compliant</li> </ul>	<ul style="list-style-type: none"> <li>CL_POSTURE_COMPLIANT</li> <li>SH_CONT</li> </ul>	Select from list	0	⚙️
✔️	SH_CONT	<ul style="list-style-type: none"> <li>Wired_802.1X</li> <li>LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT</li> </ul>	<ul style="list-style-type: none"> <li>SH_CONT</li> </ul>	Select from list	0	⚙️
✔️	SH_CORP	<ul style="list-style-type: none"> <li>Wired_802.1X</li> <li>LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CORP</li> </ul>	<ul style="list-style-type: none"> <li>SH_CORP</li> </ul>	Select from list	5	⚙️
✔️	Basic_Authenticated_Access	<ul style="list-style-type: none"> <li>Network_Access_Authentication_Passed</li> </ul>	<ul style="list-style-type: none"> <li>DenyAccess</li> </ul>	Select from list	56	⚙️
✔️	Default		<ul style="list-style-type: none"> <li>DenyAccess</li> </ul>	Select from list	0	⚙️

Reset Save

# ISE Policy Configuration – Conditions Studio

The screenshot displays the Cisco ISE Conditions Studio interface. On the left is the 'Library' section with a search bar and a list of conditions. On the right is the 'Editor' section for a selected condition.

**Library**

Search by Name

Icons: Location, Copy, Paste, Print, Refresh, Undo, Redo, Home, Search, Help, Logout, Settings, Network, Wi-Fi

- 5G
- BYOD\_is\_Registered
- Catalyst\_Switch\_Local\_Web\_Authentication
- Compliance\_Unknown\_Devices
- Compliant\_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest\_Flow
- MAC\_in\_SAN
- Network\_Access\_Authentication\_Passed
- Non\_Cisco\_Profiled\_Phones
- Non\_Compliant\_Devices
- Switch\_Local\_Web\_Authentication
- Switch\_Web\_Authentication

**Editor**

Wired\_802.1X

Set to 'Is not'

LAB1-ExternalGroups

Equals sdalab.lab/Users/SDA1\_CORP \*

Set to 'Is not'

Buttons: Duplicate, Save

AND

Buttons: NEW, AND, OR

Set to 'Is not'

Buttons: Duplicate, Save

Buttons: Cancel, Use

# ISE Policy Configuration – Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Policy / Policy Elements'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (highlighted with a red arrow), Administration, and Work Centers. The main content area is titled 'Standard Authorization Profiles' and is divided into three tabs: Dictionaries, Conditions, and Results (highlighted with a red arrow). Under the Results tab, a sub-menu on the left shows 'Authentication', 'Authorization' (selected), and 'Client Provisioning'. Under 'Authorization', 'Authorization Profiles' is selected (highlighted with a red arrow). The main area displays a table of profiles with columns for Name, Profile, and Description. A red box highlights the last three rows of the table: SH\_CONT, SH\_CORP, and SH\_IOT. A notification banner at the top right reads 'Click here to do visibility setup Do not show this again.'

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure a
<input type="checkbox"/>	CL-No-Redirect-Unknown	Cisco	CL-No-Redirect-Unknown
<input type="checkbox"/>	CL_MACHINE_ACL	Cisco	
<input type="checkbox"/>	CL_POSTURE_COMPLIANT	Cisco	
<input type="checkbox"/>	CL_POSTURE_NONCOMPLIANT	Cisco	
<input type="checkbox"/>	CL_POSTURE_UNKNOWN	Cisco	
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	PostureUnknown	Cisco	PostureUnknown
<input type="checkbox"/>	SH_CONT	Cisco	SH_CONT
<input type="checkbox"/>	SH_CORP	Cisco	SH_CORP
<input type="checkbox"/>	SH_IOT	Cisco	SH_IOT
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.

# ISE Policy Configuration – Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The breadcrumb navigation shows 'Authorization Profiles > SH\_CORP'. The main configuration area is titled 'Authorization Profile' and includes the following fields:

- \* Name: SH\_CORP
- Description: SH\_CORP
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Agentless Posture:
- Passive Identity Tracking:

Under the 'Common Tasks' section, the following options are listed:

- ACL (Filter-ID)
- ACL IPv6 (Filter-ID)
- Security Group
- VLAN

The 'VLAN' option is selected, and its configuration is shown as follows:

Tag ID	1	Edit Tag	ID/Name	200
--------	---	----------	---------	-----

A red arrow points to the 'VLAN' checkbox, and a red box highlights the entire configuration row for the selected VLAN.

# ISE Policy Configuration – Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar shows 'Identity Services Engine' and 'Policy / Policy Elements'. The left sidebar contains navigation options like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Features'. The main content area is divided into 'Dictionaries', 'Conditions', and 'Results' tabs. Under 'Results', the 'Authorization Profiles' section is selected, showing a list of profiles including 'SH\_CONT'. The configuration details for 'SH\_CONT' are displayed, including fields for Name, Description, Access Type, Network Device Profile, Service Template, Track Movement, Agentless Posture, and Passive Identity Tracking. The 'Common Tasks' section is expanded, showing a list of tasks. A red box highlights the 'VLAN' task, which is checked and has a 'Tag ID' of 1 and an 'ID/Name' of 206. An 'Edit Tag' button is visible next to the tag ID.

# ISE Policy Configuration – Endpoints Authenticated

Identity Services Engine Operations / RADIUS

Live Logs **Live Sessions**

Refresh Every 1 minute Show Latest 20 records Within Last 60 minutes

Export To Filter

Initiated	Updated	Session Sta...	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Se
Jan 20, 2025 09:14:16.19...	Jan 20, 2025 09:14:16.3...	Started	Show CoA Actions	00:0C:29:C2:FC:F4	SDALAB\glenn	172.16.204.1	Windows11-Workst...			ise
Jan 20, 2025 08:54:24.92...	Jan 20, 2025 08:54:26.1...	Started	Show CoA Actions	00:0C:29:D5:01:B0	SDALAB\matt	172.16.200.2,fe8 ...	Windows11-Workst...			ise
Jan 20, 2025 08:51:28.10...	Jan 20, 2025 08:51:30.9...	Postured	Show CoA Actions	00:0C:29:C0:D1:EC	SDALAB\james	172.16.206.2,fe8 ...	Windows11-Workst...	Compliant		ise

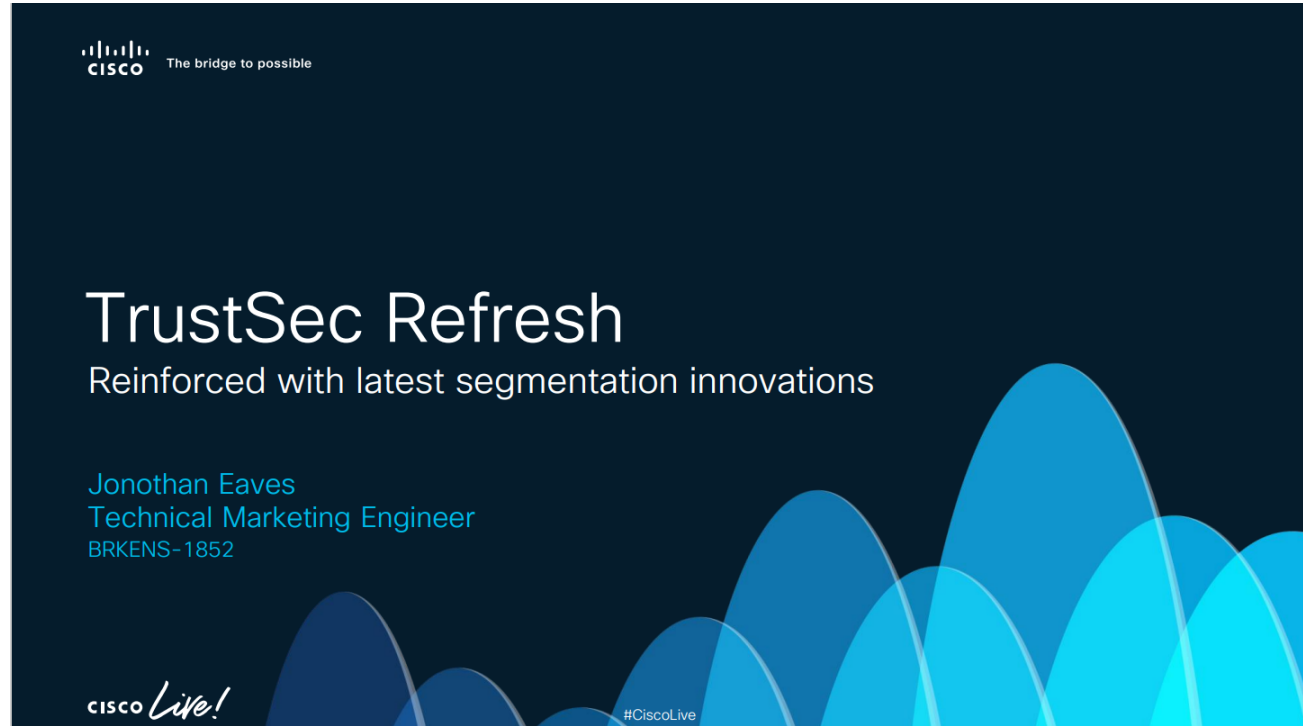
Last Updated: Mon Jan 20 2025 21:14:37 GMT+0000 (Greenwich Mean Time) Records Shown: 3


# Cisco TrustSec

CISCO *Live!*



# Absolutely look at this!


A presentation slide for Cisco TrustSec Refresh. The slide has a dark blue background with a light blue abstract graphic of overlapping shapes at the bottom right. The Cisco logo and tagline 'The bridge to possible' are in the top left. The main title 'TrustSec Refresh' is in large white font, with the subtitle 'Reinforced with latest segmentation innovations' below it. The speaker's name 'Jonothan Eaves' and title 'Technical Marketing Engineer' are in light blue, with the session ID 'BRKENS-1852' below. The 'cisco Live!' logo is in the bottom left, and the hashtag '#CiscoLive' is in the bottom right.

 The bridge to possible

# TrustSec Refresh

Reinforced with latest segmentation innovations

Jonothan Eaves  
Technical Marketing Engineer  
BRKENS-1852

 #CiscoLive



# Identifying Users for Group-Based Policies

Simple ways to add access control & protect new things



Reduce IP ACL complexity.  
Reduce and simplify FW rules.  
Meet compliance goals easier.  
Simple segregation protection.

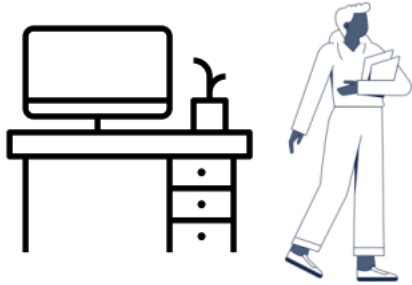
Reduce Risk & Represent threat state or vulnerable devices



Reduce SecOps effort in adds, moves & changes



# Policy Challenge



VLAN 100  
Subnet A.B.C.D  
↓  
IPACL 1  
IPACL 2 ....



VLAN 103  
Subnet M.N.O.P  
↓  
IPACL 31  
IPACL 32 ....

Security  
Policy  
Tied to  
Infra



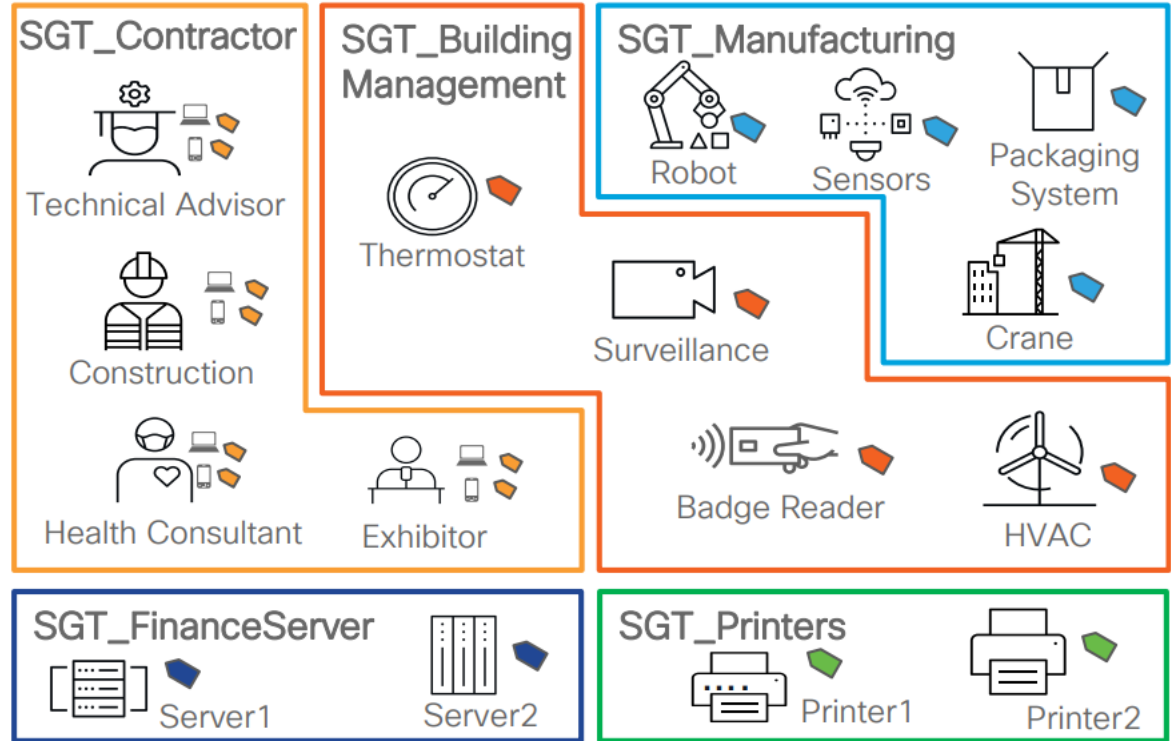
VLAN 101  
Subnet E.F.G.H  
↓  
IPACL 11  
IPACL 12 ....



VLAN 102  
Subnet I.J.K.L  
↓  
IPACL 21  
IPACL 22 ....

# Classification into Intent-Based Groups

- Business-based groupings to provide consistent policy and access independent of network topology
- Leverage items such as location, device type, RADIUS attributes, AD membership etc. to allocate group assignments



# Let's add TrustSec to the solution!

The screenshot displays the Cisco Catalyst Center interface. The left sidebar shows the navigation menu with 'Policy' selected. A red arrow points to 'Group-Based Access Control' in the sub-menu. The main content area shows the 'Provision / Inventory' page for 'Access Points'. A table lists several devices with their IP addresses, vendors, and various status indicators. A red arrow points to the 'Group-Based Access Control' link in the table header.

IP Address	Vendor	Reachability	EoX Status	Manageability	Compliance	Site	Image Version	Last Update
172.16.210.251	Cisco	Reachable	Not Scanned	Managed	Compliant	.../Didsbury/Spectrum	17.12.3	9 minute Sync Detail
172.16.210.250	Cisco	Reachable	Not Scanned	Managed Syncing...	Compliant	.../Didsbury/Spectrum	17.12.3	1 hour 1 Sync Detail
172.16.210.249	Cisco	Reachable	Not Scanned	Managed Syncing...	Compliant	.../Didsbury/Spectrum	17.12.3	1 hour 1 Sync Detail
172.16.210.253	Cisco	Reachable	Not Scanned	Managed	Compliant	.../Didsbury/Spectrum	17.12.3	1 hour 2: Sync Detail
172.16.210.252	Cisco	Reachable	Not Scanned	Managed	Compliant	.../Didsbury/Spectrum	17.12.3	1 hour 2: Sync Detail

<https://10.53.0.110/dna/policy/gbacACA/overview>

# Let's add TrustSec to the solution!



```
edge1#sho cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 172.16.33.12, port 1812, A-ID 945907B3C05837D889807E1F72BFA3AC
       Status = ALIVE
       auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime =
20 secs
edge1#
```

Catalyst Centre already added the CTS server!

# Let's add TrustSec to the solution!


The screenshot displays the Cisco Catalyst Center interface for Group-Based Access Control. At the top, the navigation bar includes the Cisco logo, the text 'Catalyst Center', and the breadcrumb 'Policy / Group-Based Access Control'. On the right side of the navigation bar, there are icons for star, search, refresh, help, and notifications, along with a user profile icon labeled 'admin'.

Below the navigation bar, there are tabs for 'Overview', 'Policies', 'Security Groups', and 'Access Contracts'. The 'Overview' tab is selected.

A prominent notification box with a red border and a red 'x' icon contains the following text:

In order to begin using Catalyst Center as the administration point for Group-Based Access Control, Catalyst Center must migrate policy data from the Cisco Identity Services Engine (ISE):

- Any policy features in Cisco ISE that are currently not supported in Catalyst Center will not be migrated, you will have a chance to review the migration rule after click on "Start migration"
- Any policy information in Catalyst Center not already exist in Cisco ISE will be copied to Cisco ISE to ensure the 2 sources are in sync

Once the data migration is initiated, you cannot use Group-Based Access Control in Catalyst Center until the operation is complete. [Start migration](#)  After policy data migration has completed, if you prefer to manage Group-Based Access Control in Cisco Identity Services Engine, you can select that option under "Group-Based Access Control Configuration".

Below the notification, there is a search bar with the placeholder text 'Search by group name, IP Address, or MAC address'. To the right of the search bar are several status indicators: 'Upcoming' (0), 'In Progress' (0), 'Failed' (0), 'Configuration', and 'Reports'.

Under the search bar, there is a section titled 'View traffic for ...' with two cards:

- A card for 'SECURITY GROUPS' with a purple circular icon and the number '2'.
- A card for 'ISE PROFILES' with a teal circular icon and the number '4'.

Below these cards is a 'Policy Issues' section. It shows a summary of issues by priority: P1 (0), P2 (5), P3 (0), and P4 (0). The time range is set to '24 hrs' and 'Jan 19, 2025 9:00 PM - Jan 20, 2025 9:00 PM'.

At the bottom, there are two panels for 'Most Active Policies' and 'Least Active Policies', each with a dropdown menu set to 'All Packets' and a bar chart visualization.

# Let's add TrustSec to the solution!

The screenshot shows the Cisco Catalyst Center interface for configuring Group-Based Access Control. The top navigation bar includes the Cisco logo, 'Catalyst Center', and the current page path 'Policy / Group-Based Access Control'. A user profile 'admin' is visible in the top right. Below the navigation, there are tabs for 'Overview', 'Policies', 'Security Groups', and 'Access Contracts'. A search bar is present with the placeholder text 'Search by group name, IP Address, or MAC address'. To the right of the search bar are status indicators for 'Upcoming' (0), 'In Progress' (0), and 'Failed' (0), along with links for 'Configuration' and 'Reports'. A section titled 'View traffic for ...' contains two cards: 'SECURITY GROUPS' with a count of 2 and 'ISE PROFILES' with a count of 4. Below this is a 'Policy Issues' section with a time range of '24 hrs' and a date range of 'Jan 19, 2025 9:00 PM - Jan 20, 2025 9:00 PM'. It displays four issue counts: P1 (0), P2 (5), P3 (0), and P4 (0). The bottom half of the page is divided into two panels: 'Most Active Policies' and 'Least Active Policies'. Each panel has a 'All Packets' dropdown menu and a placeholder for a chart with the text 'Something data'.

# Let's add TrustSec to the solution!

Security Groups (18)

Upcoming In Progress Failed Create Security Group

Search Table

0 Selected Delete Deploy Edit

<input type="checkbox"/>	Name	Tag Value	Description	Created in	Policies
<input type="checkbox"/>	Auditors	9/0x9	Auditor Security Group		0
<input type="checkbox"/>	BYOD	15/0xf	BYOD Security Group		0
<input type="checkbox"/>	Contractors	5/0x5	Contractor Security Group		1
<input type="checkbox"/>	Developers	8/0x8	Developer Security Group		0
<input type="checkbox"/>	Development_Servers	12/0xc	Development Servers Security Group		0
<input type="checkbox"/>	Employees	4/0x4	Employee Security Group		1
<input type="checkbox"/>	Extranet	17/0x11	Extranet Security Group		0
<input type="checkbox"/>	Guests	6/0x6	Guest Security Group		0
<input type="checkbox"/>	Intranet	16/0x10	Intranet Security Group		0
<input type="checkbox"/>	Network_Services	3/0x3	Network Services Security Group		0

18 Record(s) Show Records: 10 1 - 10 < 1 2 >

Add Security Groups from CC – not from ISE!!



# Add some Security Groups - demo

Navigation: Overview Policies **Security Groups** Access Contracts

Policy / Group-Based Access Control

admin

Security Groups (19)

Upcoming In Progress Failed Create Security Group

Search Table

0 Selected Delete Deploy Edit

<input type="checkbox"/>	Name	Tag Value	Description	Created in	Policies
<input type="checkbox"/>	PCI_Servers	14/0xe	PCI Servers Security Group		0
<input type="checkbox"/>	Point_of_Sale_Systems	10/0xa	Point of Sale Security Group		0
<input type="checkbox"/>	Production_Servers	11/0xb	Production Servers Security Group		0
<input type="checkbox"/>	Production_Users	7/0x7	Production User Security Group		0
<input type="checkbox"/>	Quarantined_Systems	255/0xff	Quarantine Security Group		0
<input type="checkbox"/>	SG_CORP	18/0x12			0
<input type="checkbox"/>	Test_Servers	13/0xd	Test Servers Security Group		0
<input type="checkbox"/>	TrustSec_Devices	2/0x2	TrustSec Devices Security Group		0
<input type="checkbox"/>	Unknown	0/0x0	Unknown Security Group		0

19 Record(s) Show Records: 10 11 - 19 < 1 2 >

# ISE Gets the SGs

The screenshot displays the Cisco Identity Services Engine (ISE) Work Centers / TrustSec interface. The main content area is titled "Security Groups" and shows a list of security groups. The interface includes a navigation menu on the left, a top navigation bar, and a main content area with a table of security groups. The table has columns for "Icon", "Name", "SGT (Dec / Hex)", "Description", and "Learned from". The rows list various security groups, with the last three rows (SG\_CONT, SG\_CORP, SG\_IOT) highlighted by a red box.

Work Centers / TrustSec

Overview **Components** TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Security Groups

IP SGT Static Mapping  
Security Group ACLs  
Network Devices

Trustsec Servers >

For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Selected 0 Total 21

Edit + Add Import Export Trash Push Verify Deploy All

<input type="checkbox"/>	Icon	Name	SGT (Dec / Hex)	Description	Learned from
<input type="checkbox"/>		Extranet	17/0011	Extranet Security Group	
<input type="checkbox"/>		Guests	6/0006	Guest Security Group	
<input type="checkbox"/>		Intranet	16/0010	Intranet Security Group	
<input type="checkbox"/>		Network_Services	3/0003	Network Services Security Group	
<input type="checkbox"/>		PCI_Servers	14/000E	PCI Servers Security Group	
<input type="checkbox"/>		Point_of_Sale_Systems	10/000A	Point of Sale Security Group	
<input type="checkbox"/>		Production_Servers	11/000B	Production Servers Security Group	
<input type="checkbox"/>		Production_Users	7/0007	Production User Security Group	
<input type="checkbox"/>		Quarantined_Systems	255/00FF	Quarantine Security Group	
<input type="checkbox"/>		SG_CONT	19/0013		
<input type="checkbox"/>		SG_CORP	18/0012		
<input type="checkbox"/>		SG_IOT	20/0014		
<input type="checkbox"/>		Test_Servers	13/000D	Test Servers Security Group	
<input type="checkbox"/>		TrustSec_Devices	2/0002	TrustSec Devices Security Group	
<input type="checkbox"/>		Unknown	0/0000	Unknown Security Group	

# Add slightly different AuthZ Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for an Authorization Profile. The page title is "Policy / Policy Elements". The left sidebar shows navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Features. The main content area is divided into "Dictionaries", "Conditions", and "Results" tabs, with "Results" being the active tab. Under "Results", there are sub-sections for "Authentication", "Authorization Profiles" (selected), "Downloadable ACLs", "Profiling", "Posture", and "Client Provisioning". The "Authorization Profile" configuration shows: Name: SG\_CONT, Description: (empty text area), Access Type: ACCESS\_ACCEPT, Network Device Profile: Cisco, Service Template: (unchecked), Track Movement: (unchecked), Agentless Posture: (unchecked), and Passive Identity Tracking: (unchecked). Under "Common Tasks", "ACL (Filter-ID)", "ACL IPv6 (Filter-ID)", and "Security Group" (checked) are listed. The "Security Group" dropdown menu is highlighted with a red box, showing "SG\_CONT" and "VLAN 206". Below it, "Virtual Network:" and "VLAN:" fields are visible but empty.

# Add slightly different AuthZ Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Policy Element. The top navigation bar shows "Identity Services Engine" and "Policy / Policy Elements". The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Features. The main content area is divided into three tabs: Dictionaries, Conditions, and Results (selected). Under the Results tab, there are sections for "Common Tasks", "Advanced Attributes Settings", and "Attributes Details".

**Common Tasks:**

- ACL (Filter-ID)
- ACL IPv6 (Filter-ID)
- Security Group ⓘ

**Configuration:**

- SG: SG\_CONT
- Virtual Network: \_\_\_\_\_
- VLAN: 206

**Advanced Attributes Settings:**

Select an item

**Attributes Details:**

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = cts:security-group-tag=0013-0
cisco-av-pair = cts:sg-name=SG_CONT
cisco-av-pair = cts:vm=
Tunnel-Private-Group-ID = 1:206
Tunnel-Type = 1:13
Tunnel-Medium-Type = 1:6
```

Buttons: Submit, Cancel

# Add slightly different AuthZ Policy Results

The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the 'Policy / Policy Elements' section. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Features. The main content area is titled 'Standard Authorization Profiles' and shows a list of profiles. The 'Results' tab is active, and the 'Authorization Profiles' sub-tab is selected. The table lists various profiles with their names, profiles (all Cisco), and descriptions.

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure
<input type="checkbox"/>	CL-No-Redirect-Uknown	Cisco	CL-No-Redirect-Uknown
<input type="checkbox"/>	CL_MACHINE_ACL	Cisco	
<input type="checkbox"/>	CL_POSTURE_COMPLIANT	Cisco	
<input type="checkbox"/>	CL_POSTURE_NONCOMPLIANT	Cisco	
<input type="checkbox"/>	CL_POSTURE_UNKNOWN	Cisco	
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/>	PostureUnknown	Cisco	PostureUnknown
<input type="checkbox"/>	SG_CONT	Cisco	
<input type="checkbox"/>	SG_CORP	Cisco	
<input type="checkbox"/>	SH_CONT	Cisco	SH_CONT
<input type="checkbox"/>	SH_CORP	Cisco	SH_CORP

# Change our AuthZ Policies to match

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+						
+	SH_IOT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_IOT	SG_IOT	SG_IOT	4	
⊖	SH_CONT_UNKNOWN	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Unknown	CL_POSTURE_UNKNOWN SH_CONT	Select from list	0	
⊖	SH_CONT_NON_COMPLIANT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS NonCompliant	CL_POSTURE_NONCOMPL... SH_CONT	Select from list	0	
⊖	SH_CONT_COMPLIANT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Compliant	CL_POSTURE_COMPLIANT SH_CONT	Select from list	0	
+	SH_CONT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	SG_CONT	SG_CONT	2	
+	SH_CORP	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CORP	SG_CORP	SG_CORP	7	
+	Basic_Authenticated_Access	Network_Access_Authentication_Passed	DenyAccess	Select from list	74	

# Endpoints using TrustSec!

The screenshot shows the Cisco Identity Services Engine (ISE) Operations / RADIUS page. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Operations / RADIUS'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations (selected), Policy, Administration, and Work Centers. The main content area displays five summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (0), Client Stopped Responding (0), and Repeat Counter (0). Below these cards are controls for Refresh (Every 10 seconds), Show (Latest 100 records), and Within (Last 5 minutes). A table of RADIUS events is shown below, with a red box highlighting the 'Authorization Profiles' column. The table columns are: Time, Status, Details, Repea..., Identity, Endpoint ID, Endpoint Prof..., Authentication Po..., Authoriz..., Authorization Profiles, and IP Address.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint Prof...	Authentication Po...	Authoriz...	Authorization Profiles	IP Address
Jan 20, 2025 10:04:32.0...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:8d					
Jan 20, 2025 10:04:32.0...	●	🔒	0	SDALAB\glenn	00:0C:29:C2:FC:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_IOT	172.16.204.1...
Jan 20, 2025 10:04:31.9...	✓	🔒		SDALAB\glenn	00:0C:29:C2:FC:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_IOT	172.16.204.1...
Jan 20, 2025 10:03:15.1...	●	🔒	0	SDALAB\james	00:0C:29:C0:D1:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_CONT	172.16.206.2...
Jan 20, 2025 10:02:53.7...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:86					
Jan 20, 2025 10:02:53.7...	✓	🔒		SDALAB\james	00:0C:29:C0:D1:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_CONT	172.16.206.2...
Jan 20, 2025 10:02:43.3...	✓	🔒		#CTSREQUEST#	68:2C:7B:98:E9:80					
Jan 20, 2025 10:02:43.3...	●	🔒	0	SDALAB\matt	00:0C:29:D5:01:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_CORP	172.16.200.2...
Jan 20, 2025 10:02:43.2...	✓	🔒		SDALAB\matt	00:0C:29:D5:01:...	Windows11-Wo...	Default >> Dot1X	Default >>...	SG_CORP	172.16.200.2...
Jan 20, 2025 10:01:26.3...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:8d					
Jan 20, 2025 10:01:26.3...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:8d					
Jan 20, 2025 10:01:26.3...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:8d					
Jan 20, 2025 10:01:26.3...	✓	🔒		#CTSREQUEST#	68:2c:7b:95:8d					

# Endpoints using TrustSec!

Identity Services Engine Operations / RADIUS

Refresh Every 1 minute Show Latest 20 records Within Last 60 minutes

Export To

Initiated	Updated	Session Sta...	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Security G...	Se
Jan 20, 2025 10:04:31.97...	Jan 20, 2025 10:04:32.0...	Started	Show CoA Actions	00:0C:29:C2:FC:F4	SDALAB\glenn	172.16.204.1,fe8 ...	Windows11-Workst...		SG_IOT	ise
Jan 20, 2025 10:02:53.74...	Jan 20, 2025 10:03:15.1...	Postured	Show CoA Actions	00:0C:29:C0:D1:EC	SDALAB\james	172.16.206.2,fe8 ...	Windows11-Workst...	Compliant	SG_CONT	ise
Jan 20, 2025 10:02:43.27...	Jan 20, 2025 10:02:43.3...	Started	Show CoA Actions	00:0C:29:D5:01:B0	SDALAB\matt	172.16.200.2,fe8 ...	Windows11-Workst...		SG_CORP	ise

Last Updated: Mon Jan 20 2025 22:05:16 GMT+0000 (Greenwich Mean Time)

Records Shown: 3



# Switch Configuration required



```
cts role-based enforcement
cts role-based enforcement vlan-list 200,202,204,206,208,210
cts sxp enable
```

Add this to every switch!

```
! Trunk configuration
int range gi1/0/23 - 24
  ip dhcp snooping trust
  cts manual
  policy static sgt 2 trusted
```

And you already know how – CLI Templates!

# So what can we do with this?

- No Firewall Hairpinning!
- No ACLs/ACEs!
- Enforce East-West
  
- Welcome to the Matrix!  
(not that one!)

The screenshot shows the Cisco Catalyst Center interface for the 'Policies' section. The page title is 'Policies (0)' with a link to 'Enter full screen'. Below the title are controls for 'Filter', 'Deploy', and 'Refresh'. A legend indicates policy types: Permit (green), Deny (red), Custom (yellow), and Default (grey). The main area is a matrix with 'Source' on the vertical axis and 'Destination' on the horizontal axis. The 'Source' list includes: Extranet, Guests, Intranet, Network\_Servic..., PCI\_Servers, Point\_of\_Sale..., Production\_Ser..., Production\_Users, Quarantined\_Sy..., SG\_CONT, SG\_CORP, SG\_IOT, Test\_Servers, TrustSec\_Devices, and Unknown. The 'Destination' list includes: Auditors, BYOD, Contractors, Developers, Development..., Employees, Extranet, Guests, Intranet, Network\_Serv..., PCI\_Servers, Point\_of\_Sale..., Production\_S..., Production\_U..., Quarantined..., SG\_CONT, SG\_CORP, SG\_IOT, Test\_Servers, TrustSec\_Dev..., and Unknown. The matrix cells are currently empty.

# Create an Access Contract

Cisco Catalyst Center Policy / Group-Based Access Control

Overview Policies Security Groups **Access Contracts**

Access Contracts (7) Upcoming (0) In Progress (0) Failed (0) As of: Jan 20, 2025 11:46 PM [Refresh](#) [+ Create Access Contract](#)

[Filter](#) [Actions](#) [Deploy](#) 0 Selected

<input type="checkbox"/>	Name	Description	Rules Count	Policies
<input type="checkbox"/>	<a href="#">AllowDHCPDNS</a>	Sample contract to allow DHCP and DNS	2	0
<input type="checkbox"/>	<a href="#">AllowWeb</a>	Sample contract to allow access to Web	2	0
<input type="checkbox"/>	<a href="#">Deny IP</a>	Deny IP SGACL		0
<input type="checkbox"/>	<a href="#">Deny_IP_Log</a>	Deny IP with logging		0
<input type="checkbox"/>	<a href="#">DenyRemoteServices</a>	Sample contract to block Remote Access and telnet services	4	0
<input type="checkbox"/>	<a href="#">Permit IP</a>	Permit IP SGACL		0
<input type="checkbox"/>	<a href="#">Permit_IP_Log</a>	Permit IP with logging		0

7 Record(s) Show Records: 10 1 - 7

# Create an Access Contract – Lets block ping!

**Access Contracts (7)**

Name	Description
AllowDHCPDNS	Sample contract to allow DHCP and DNS
AllowWeb	Sample contract to allow access to Web
Deny IP	Deny IP SGACL
Deny_IP_Log	Deny IP with logging
DenyRemoteServices	Sample contract to block Remote Access and telnet services
Permit IP	Permit IP SGACL
Permit_IP_Log	Permit IP with logging

**Access Contract**

Name\* **NO\_PING** Description **BLOCK\_PING**  Modeled Access Contract

**CONTRACT CONTENT (1)**

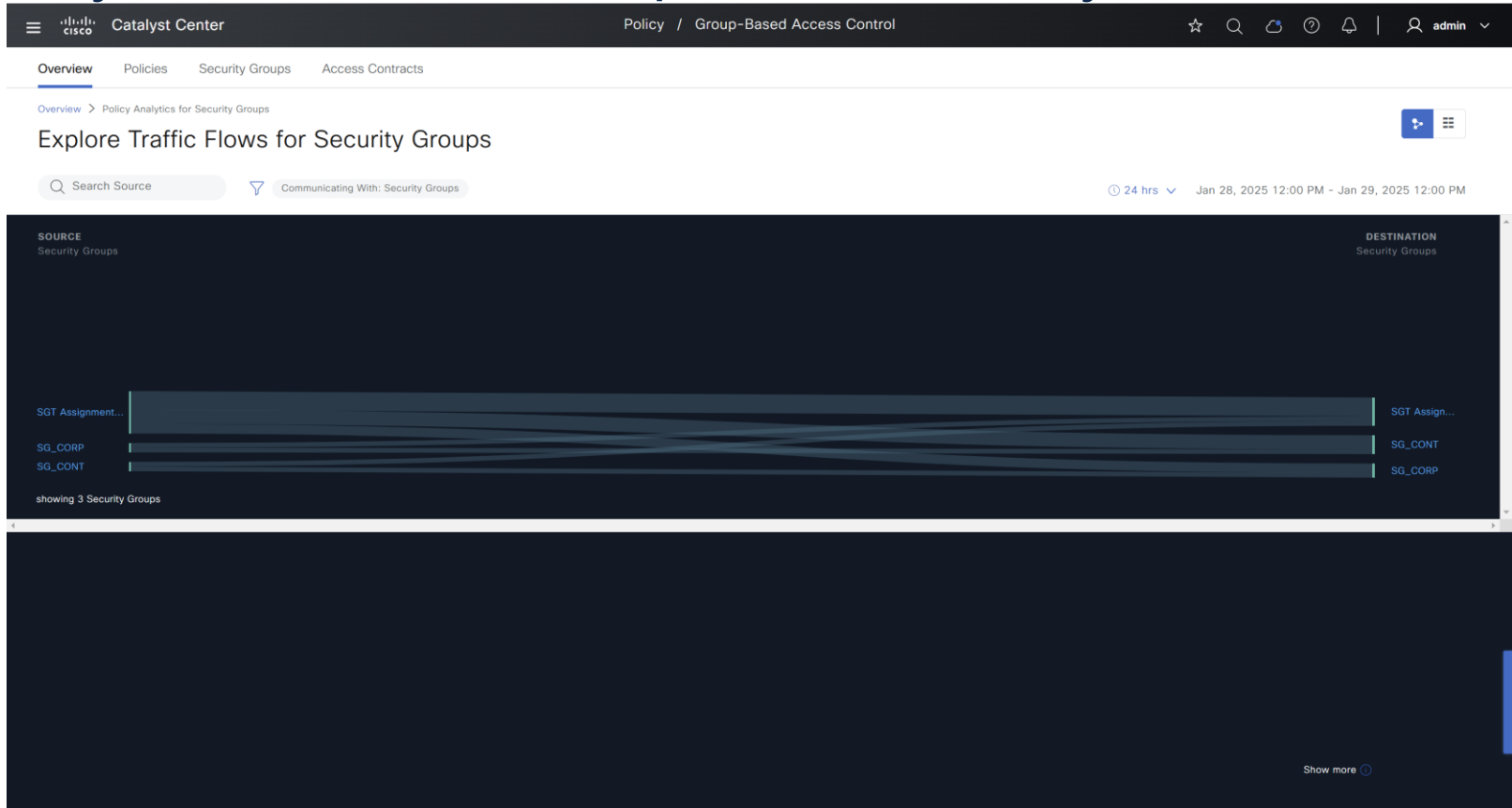
#	Action	Application	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	Advanced	ICMP	-	-	<input checked="" type="checkbox"/>	+ X

Default Action **Permit** Logging

Cancel Save Now



# Visibility of Flows – Group Based Analytics



# What about the AI ?

- AI Endpoint  
Analytics!

CISCO *Live!*



# AI Endpoint Analytics in Catalyst Centre

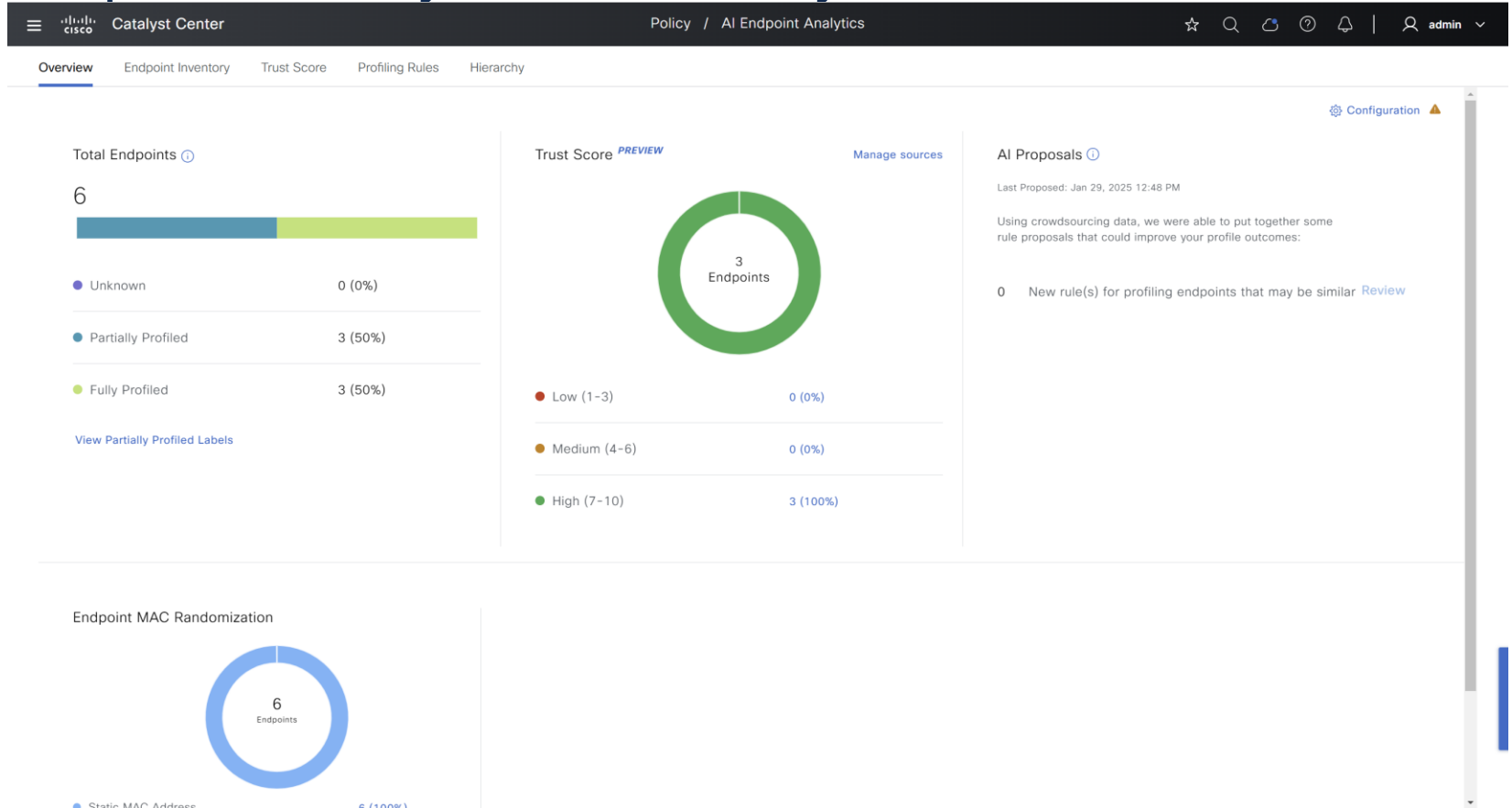
The screenshot displays the Cisco Catalyst Center interface. On the left, a dark sidebar contains a navigation menu with the following items: Design, Policy, Provision, Assurance, Workflows, Tools, Platform, Activities, Reports, System, and Explore. The 'AI Endpoint Analytics' menu item is highlighted with a red arrow. The main content area features a top navigation bar with search, help, and user profile icons. Below this, there are several dashboard cards:

- Critical Issues (Last 24 Hours):** Shows 0 P1 and 0 P2 issues. A 'View Details' link is present.
- Trends and Insights (Last 30 Days):** Shows 0 AP Performance Advisories and 0 Trend Deviations. A 'View Details' link is present.
- Network Devices (As of Jan 29, 2025 12:45 PM):** Shows 5 total devices. Breakdown: Unclaimed: 0, Unprovisioned: 0, Unreachable: 0. A 'Find New Devices' link is present.
- Application QoS Policies (As of Jan 29, 2025 12:45 PM):** Shows 1 total policy. Breakdown: Successful Deploys: 1, Errored Deploys: 0, Stale Policies: 1. An 'Add New Policy' link is present.
- AI Endpoint Analytics (As of Jan 29, 2025 12:45 PM):** Shows 6 total endpoints. Breakdown: Fully Profiled Endpoints: 50%, Partially Profiled Endpoints: 50%, Unprofiled Endpoints: 0%.
- Images (As of Jan 29, 2025 12:45 PM):** Shows 1 total image. Breakdown: Untagged Images: 0, Unverified Images: 0.

<https://10.53.0.110/dna/policy/dcs/overview>

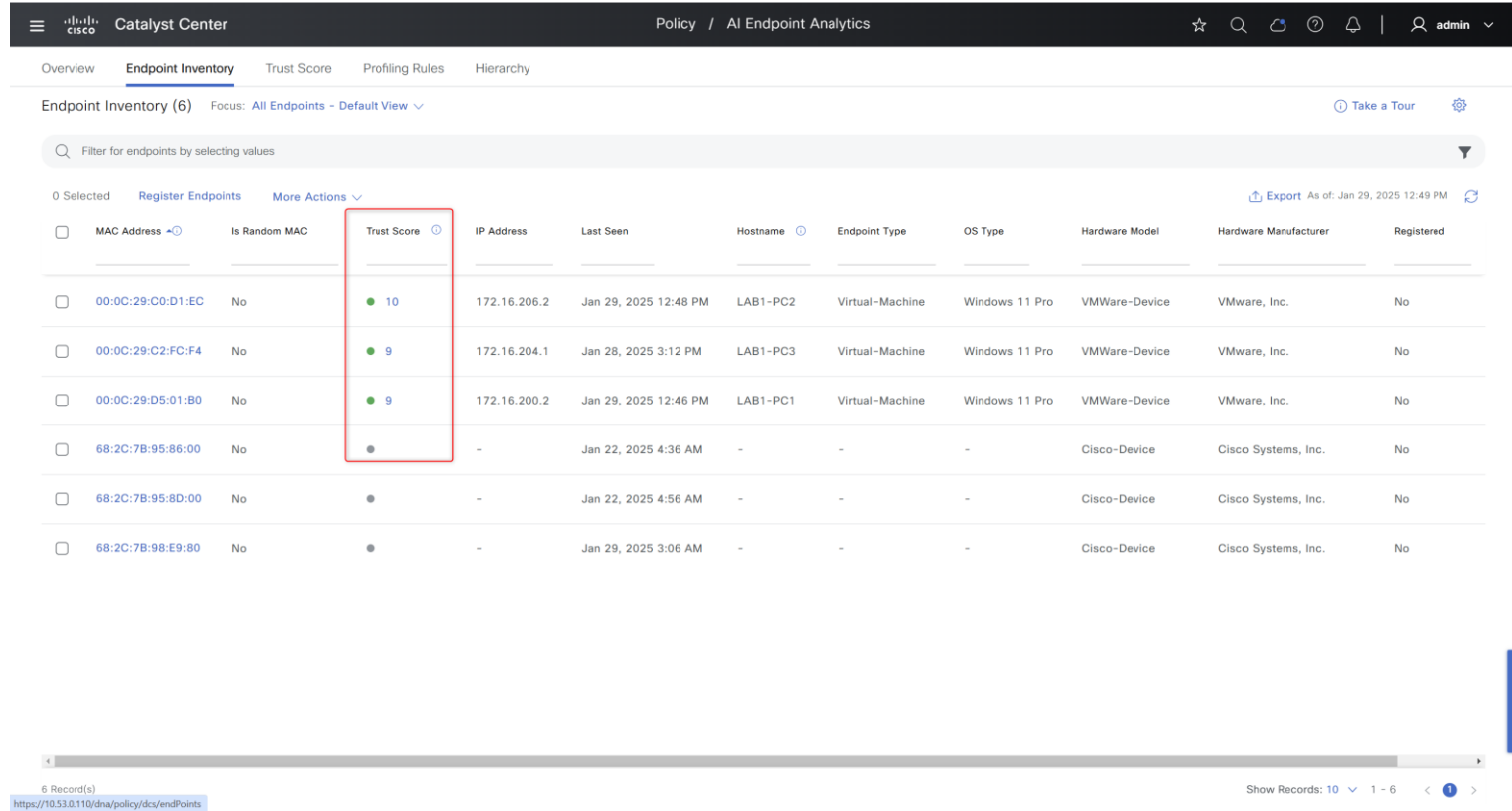


# AI Endpoint Analytics in Catalyst Centre



# AI Endpoint Analytics in Catalyst Centre


Includes a trust score



The screenshot displays the Catalyst Center interface for AI Endpoint Analytics. The main content area shows a table of endpoints with the following columns: MAC Address, Is Random MAC, Trust Score, IP Address, Last Seen, Hostname, Endpoint Type, OS Type, Hardware Model, Hardware Manufacturer, and Registered. The 'Trust Score' column is highlighted with a red box, showing values of 10, 9, 9, and three empty cells for the first four rows. The interface includes a search bar, a filter dropdown, and a table with 6 records. The URL at the bottom is https://10.53.0.110/dna/policy/dca/endPoints.

MAC Address	Is Random MAC	Trust Score	IP Address	Last Seen	Hostname	Endpoint Type	OS Type	Hardware Model	Hardware Manufacturer	Registered
00:0C:29:C0:D1:EC	No	10	172.16.206.2	Jan 29, 2025 12:48 PM	LAB1-PC2	Virtual-Machine	Windows 11 Pro	VMWare-Device	VMware, Inc.	No
00:0C:29:C2:FC:F4	No	9	172.16.204.1	Jan 28, 2025 3:12 PM	LAB1-PC3	Virtual-Machine	Windows 11 Pro	VMWare-Device	VMware, Inc.	No
00:0C:29:D5:01:B0	No	9	172.16.200.2	Jan 29, 2025 12:46 PM	LAB1-PC1	Virtual-Machine	Windows 11 Pro	VMWare-Device	VMware, Inc.	No
68:2C:7B:95:86:00	No		-	Jan 22, 2025 4:36 AM	-	-	-	Cisco-Device	Cisco Systems, Inc.	No
68:2C:7B:95:8D:00	No		-	Jan 22, 2025 4:56 AM	-	-	-	Cisco-Device	Cisco Systems, Inc.	No
68:2C:7B:98:E9:80	No		-	Jan 29, 2025 3:06 AM	-	-	-	Cisco-Device	Cisco Systems, Inc.	No

# AI Endpoint Analytics in Catalyst Centre

 Catalyst Center Policy / AI Endpoint Analytics ☆ 🔍 🔄 ? 🔔 | 👤 admin ▾

Overview [Endpoint Inventory](#) **[Trust Score](#)** [Profiling Rules](#) [Hierarchy](#)

### Trust Score [Take a Tour](#) | [Trust Analytics](#)

Trust Score assesses the trustworthiness of a given endpoint on the network to help achieve zero trust outcomes. Values range from 1 (low trust) to 10 (high trust) and are calculated using several sources that provide context about the endpoint (e.g. posture, authentication), its vulnerability [View More...](#)

Alerts **[Endpoints](#)**

**Endpoints (3)** Focus: [Trust Score - Default view](#) ⚙️

🔍 Filter for endpoints by selecting values ▾

0 Selected [Reset Trust Score](#) [More Actions](#) As of: Jan 29, 2025 12:50 PM 🔄

<input type="checkbox"/>	MAC Address ▾	Is Random MAC	Endpoint Trust Score 🕒	IP Address	IPv6	Authentication Method	Posture	AI Spoofing Detection	Endpoint Attribute Conflict	NAT Mode Detection	Concurrer
<input type="checkbox"/>	00:0C:29:C0:D1:EC	No	● 10	172.16.206.2	-	● Wired802_1x (PEAP (EAP-MSCHAPv2))	● Compliant	-	-	-	-
<input type="checkbox"/>	00:0C:29:C2:FC:F4	No	● 9	172.16.204.1	-	● Wired802_1x (PEAP (EAP-MSCHAPv2))	-	-	-	-	-
<input type="checkbox"/>	00:0C:29:D5:01:B0	No	● 9	172.16.200.2	-	● Wired802_1x (PEAP (EAP-MSCHAPv2))	-	-	-	-	-

3 Record(s) Show Records: 10 ▾ 1 - 3 < 1 >

# AI Endpoint Analytics in Catalyst Centre

Catalyst Center Policy / AI Endpoint Analytics

Overview Endpoint Inventory Trust Score **Profiling Rules** Hierarchy

*i* you are updated to the latest version 73.1 and a recent Cisco profiling rule update has changed the profiles of some endpoints. [Review update](#)

Profile Rules (3337) ⓘ Rule Prioritization

0 Selected [Delete](#) [More Actions](#) As of: Jan 29, 2025 12:51 PM

<input type="checkbox"/>	Rule Name	Created By	Date Created	Endpoint Type	OS Type	Hardware Model	Hardware Manufacturer	Source	Actions
<input type="checkbox"/>	<a href="#">Accept Nw Activity Changes Only Rule</a>	System	Jan 25, 2025 2:22 AM					Cisco Default - Dynamic	⋮
<input type="checkbox"/>	<a href="#">Advanced Network Devices IP Speaker Device Type Rule</a>	System	Jan 25, 2025 2:22 AM	Connected Speaker,Audio Video System Device	-	-	-	Cisco Default - Static	⋮
<input type="checkbox"/>	<a href="#">Advanced Network Devices IP Speaker Hardware Model Rule</a>	System	Jan 25, 2025 2:22 AM					Cisco Default - Dynamic	⋮
<input type="checkbox"/>	<a href="#">Avvidia Camera SsdpModel With Oui Model Extraction Rule</a>	System	Jan 25, 2025 2:22 AM					Cisco Default - Dynamic	⋮
<input type="checkbox"/>	<a href="#">Avvidia Camera SsdpModel With Oui Rule</a>	System	Jan 25, 2025 2:22 AM	Camera	-	Avvidia-Camera, Panasonic-Device,Avvidia-Device	-	Cisco Default - Static	⋮
<input type="checkbox"/>	<a href="#">Aggregate Rate Rule</a>	System	Jan 25, 2025 2:22 AM					Cisco Default - Dynamic	⋮
<input type="checkbox"/>	<a href="#">Alcatel Lucent Access Point DhcpClassifier With Oui Model Extraction Rule</a>	System	Jan 25, 2025 2:22 AM					Cisco Default - Dynamic	⋮

3337 Record(s) Show Records: 25 1 - 25 < 1 2 3 4 5 ... 134 >

# AI Endpoint Analytics in Catalyst Centre

AI Endpoint Analytics / Configurations

Manage Configurations

Profile Rule Settings

ISE Configuration

Trust Analytics

Endpoint Purge Policy

Endpoint Subnet Inspection

## Manage Configurations

This page provides an overview and status of Catalyst Center level configurations to be done to get complete value out of AI Endpoint Analytics. For other AI Endpoint Analytics configurations, please use appropriate settings in left hand side menu. Click on each configuration name to know more and follow the steps for enablement.

As of: Jan 29, 2025 12:52 PM [Refresh](#)

### Required Configurations (3)

This is list of recommended configurations to get started using AI Endpoint Analytics, providing increased visibility for endpoint profiling and enabling manual/automated policy enforcement with Cisco ISE.

Status:  All  Enabled  Disabled

Configuration Name	Status	Details
<a href="#">DPI Enablement (CBAR)</a>	● Enabled	3 of 3 items are completed
<a href="#">ISE Configuration</a>	● Enabled	2 of 2 items are completed
<a href="#">AI Analytics Integration</a>	● Enabled	1 of 1 items are completed

### Optional Configurations (4)

Following is the list of optional configurations for specific use-cases which can be enabled based on your requirements.

Status:  All  Enabled  Disabled

Configuration Name	Status	Details
<a href="#">Security Sensor</a>	● Disabled	0 of 3 items are completed
<a href="#">ServiceNow</a>	● Disabled	0 of 1 items are completed
<a href="#">Talos IP Reputation</a>	● Enabled	5 of 5 items are completed
<a href="#">AI Spoofing detection</a>	● Enabled	3 of 3 items are completed

Talos  
integration

We Did It!!

CISCO *Live!*



But is there a  
better way?

CISCO *Live!*



# Software Defined Access

CISCO *Live!*





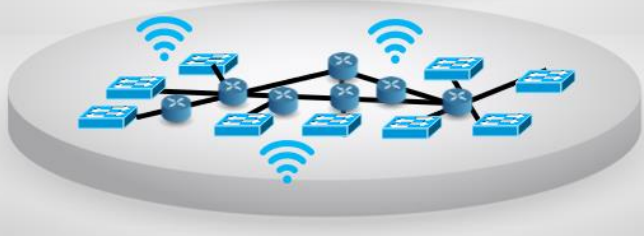
# Cisco SD-Access – Bringing Everything Together



Automation and Assurance



Programmable Overlay



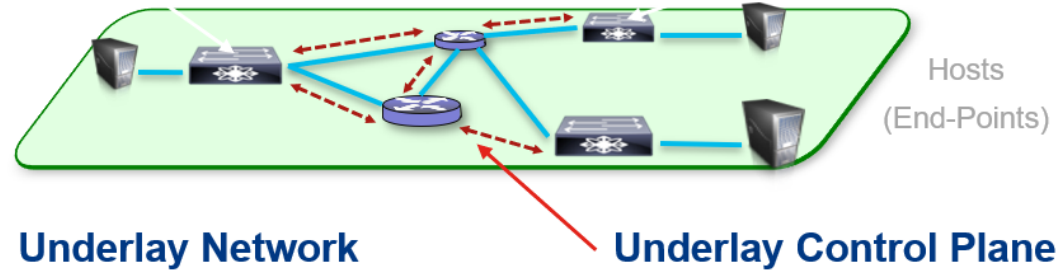
Simplified Underlay

# Requirements for the Underlay

- **Routed Network (L3 to edge)** – Intelligent Packet Handling/ECMP
- Reliability – Maximize Network Availability
- Simplicity – **No STP**, No Blocking Links, No HSRP, No VSS, no horrible L2 stuff!

Edge Device

Edge Device



**LAN Automation !!**

# What exactly is a Fabric?



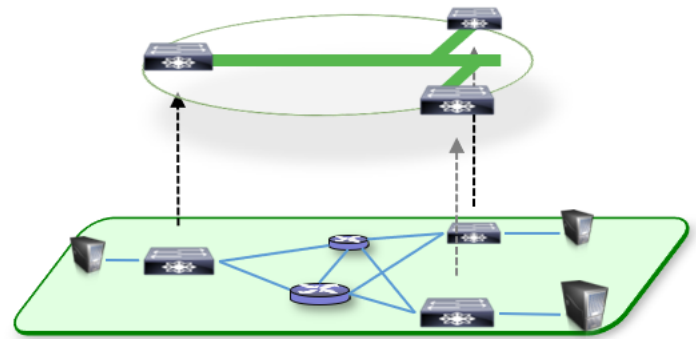
## A “Fabric” is an “Overlay”

An Overlay network is a *virtual topology* used to *logically connect* devices, built on top of an arbitrary Underlay physical topology.

An Overlay network often uses *alternate forwarding attributes* to provide *additional services* not provided by the Underlay network.

### Examples of Network Overlays

- GRE , mGRE , NVGRE
- MPLS , EoMPLS , VPLS
- GETVPN , DMVPN
- Fabric Path (FP)
- OTV
- LISP
- DFA
- ACI





# SD-Access Fabric – Segmentation without ACLs!

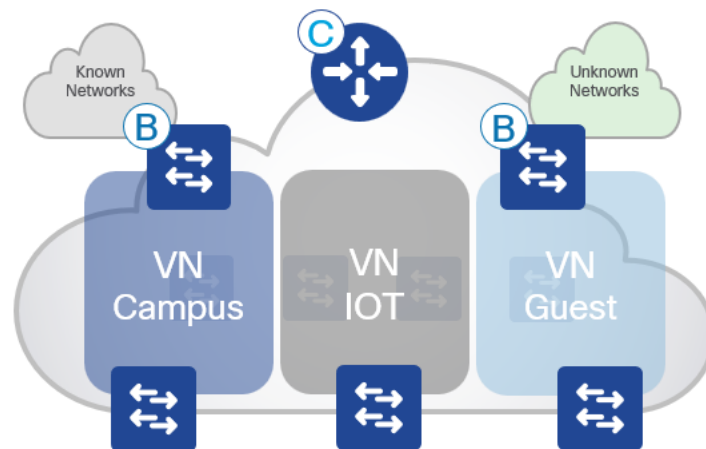
## Virtual Network – A Closer Look

**Virtual Network** maintains a separate Routing & Switching table for each instance

The what with the where now??

A virtual network is just that – it splits the common network in logically separate constructs...

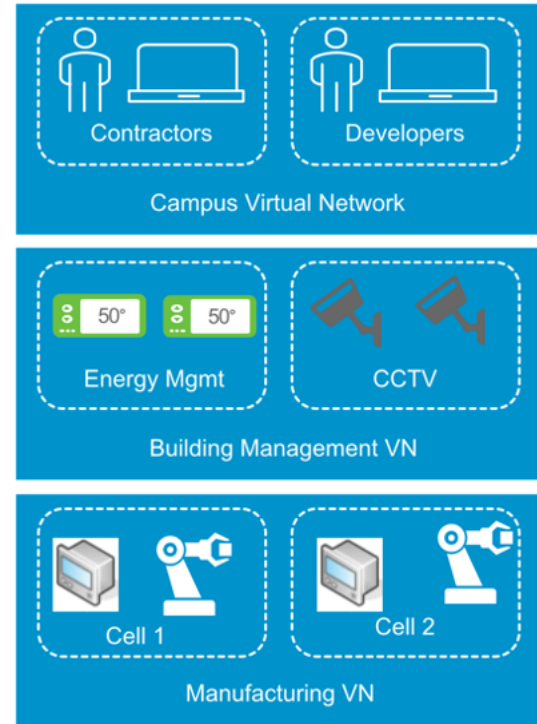
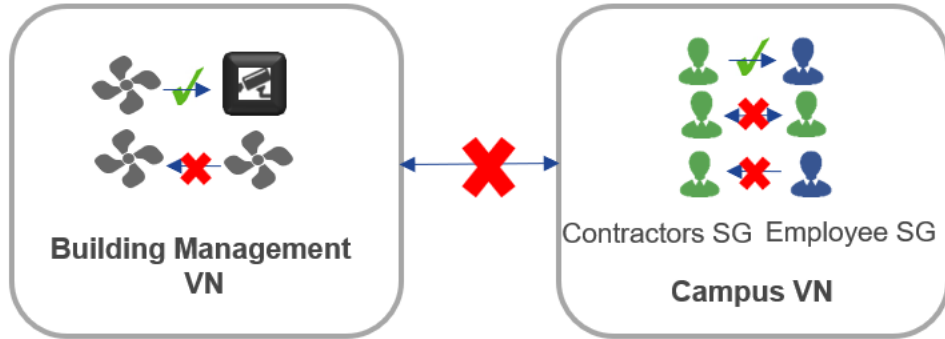
Well that's clear then...



# Segmentation Policies – Macro & Micro

Macro: VN to VN traffic is not allowed

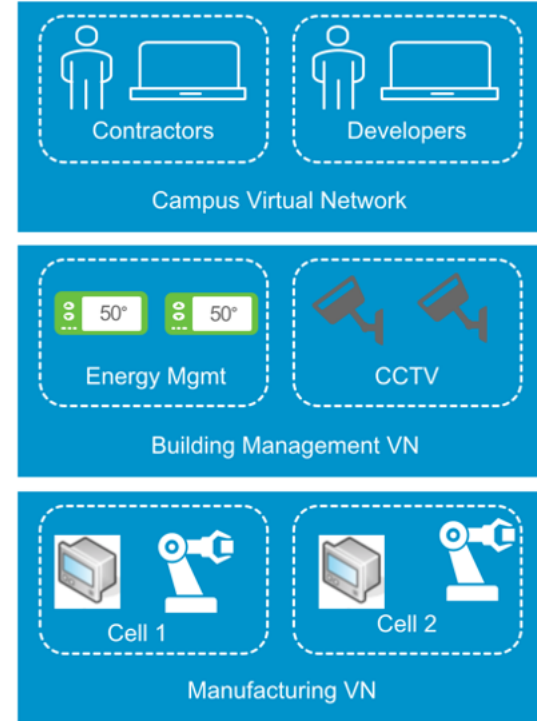
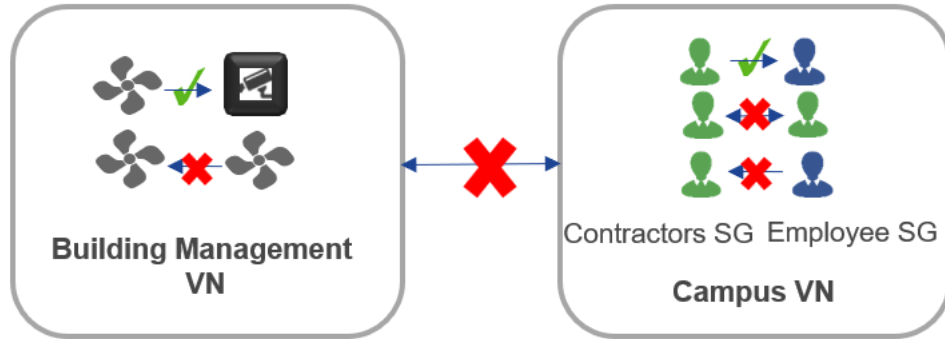
Micro: SGT to SGT policy within a VN is defined globally from DNAC (Application level policy can also be set here too).



# Segmentation Policies – Macro & Micro

Macro: VN to VN traffic is not allowed

Micro: SGT to SGT policy within a VN is defined globally from DNAC (Application level policy can also be set here too).





Provision

## Simplified Provisioning

Deploy devices using “best practice” configurations from a simple user interface





Mobility

## Wired and Wireless **Host Mobility**

because you get stretched subnets with broadcast suppression at each switch





Intelligent  
Policy

Network Wide  
**Policy Enforcement**  
based on your identity, not on your address

# In Conclusion

- Catalyst Centre – automate the steps without templates!
  - Built on best practice
  - Deploy an entire network – consistent policy
  - Identity Based Network
  - Visibility and Assurance
- 
- All via Cisco Catalyst Centre!!

# Webex App

## Questions?

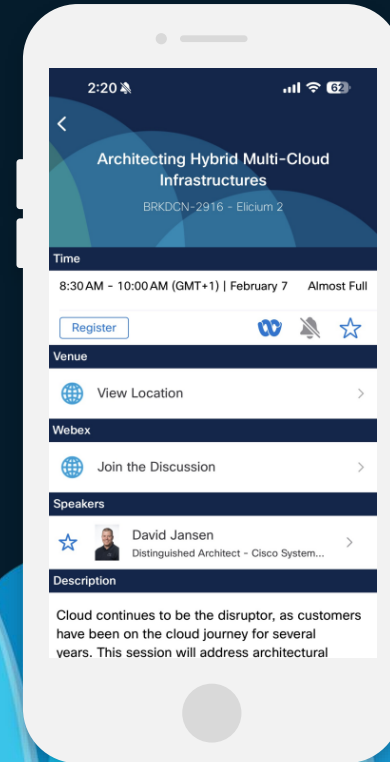
Use the Webex app to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events mobile app
- 2 Click “Join the Discussion”
- 3 Install 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 February 28, 2025.

**CISCO** *Live!*



# Next Steps!

- Read the documentation – get a thorough understanding
- Re-watch the videos and session (will be in Webex space)
- Sandbox it or lab it! – test, test, test
- Reach out to your Account Team, find a friendly SE!

# Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

# Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand). Sessions from this event will be available from March 3.

Contact me at: [magraha2@cisco.com](mailto:magraha2@cisco.com)



Thank you

CISCO *Live!*



# Bonus Content!:

## Posture Compliance – AKA NAC

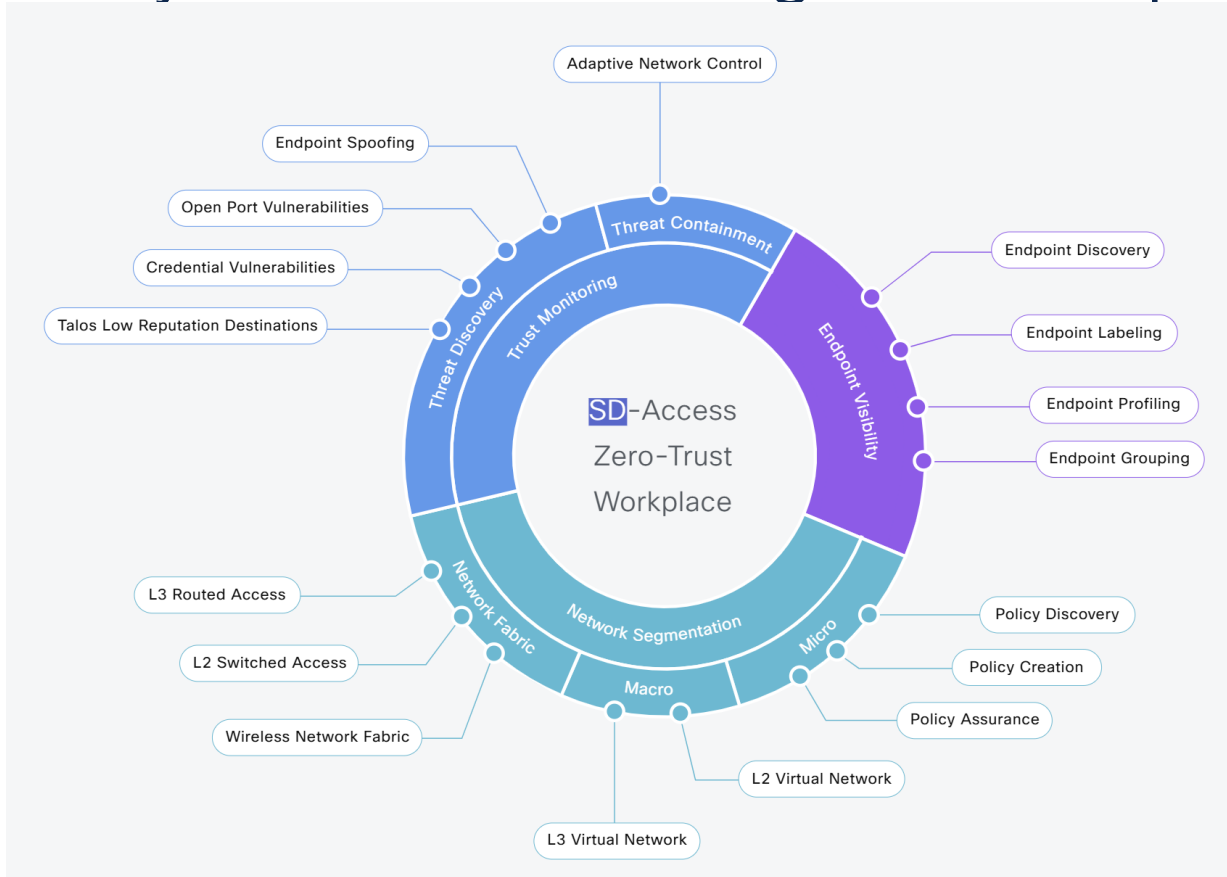




# Why Posture Checking and Compliance?

- Rules defined based on Organization requirements
- Ensures Endpoints are meeting requirements
- Automatically check for compliance – on login and periodically!
- Remediate if non Compliant – Segment, Isolate and Prevent
- So many criteria can be defined!
- Agent based or agentless (NB – remediation requires Agent!)
- No NetOps or SecOps requirement – automated.
- Forms core element of our Zero Trust Approach

# Why Posture Checking and Compliance?



# Posture Checking – Workflow

**Identity Services Engine** Work Centers / Posture

**Overview** Network Devices Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

## Posture Overview

### 1. Prepare

#### Network Access Devices

Define the [network devices](#) that will be used by users to connect.

#### Updates

Download [posture updates](#) with the latest predefined checks, rules and support charts for anti-malware, patch management and disk encryption software.

#### Client Provisioning Resources

Download [client provisioning packages](#), including the NAC or AnyConnect Agent, packages, profiles and compliance modules.

#### Acceptable Use Policy

Configure an [AUP](#) that can optionally be presented to users for approval when connecting to the network.

#### Settings

Check the defaults for posture general [settings](#) such as Remediation Timer, Network Transition Delay, Default Posture Status and Posture Lease, etc. to make sure they are acceptable.

### 2. Define

#### Policy Elements

Define the posture checks – known as [conditions](#).

Configure the fixes – known as [remediations](#) which may be applied if the client is non-compliant – i.e. fails to meet the conditions.

Link conditions and remediations in order to create the [posture requirements](#).

#### Posture Policy

Compose the [posture policy](#) rules based on the requirements.

Select Audit, Optional or Mandatory (default) mode in the requirements dropdown for each policy rule.

#### Client Provisioning Portal

Configure the [client provisioning portal](#) and customize it for your organization's requirements. Then configure an [authorization profile](#) for that portal with [Downloadable ACLs](#) if required.

#### Client Provisioning Policy

Define [client provisioning policy](#) to install agents appropriate for each operating system.

#### Access Policy

Configure your ISE posture policies for [authentication](#) and [authorization](#).

### 3. Go Live & Monitor

#### Auditing

Examine [reports](#) to check impact of posture policy.

#### Troubleshooting

[Troubleshoot](#) issues using the diagnostic tools.

# Posture Deployment

Add some new Rules`

Identity Services Engine			Policy / Policy Sets			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
⊖	Wi-Fi_Redirect_to_Guest_Login	Wireless_MAB	Cisco_WebAuth	Select from list	0	⚙️
⊕	SH_MACHINE	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/Domain Computers	CL_MACHINE_ACL SH_CONT	Select from list	5	⚙️
⊕	SH_IOT	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_IOT	SG_IOT	SG_IOT	6	⚙️
⊖	SH_CONT_UNKNOWN	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Unknown	CL_POSTURE_UNKNOWN SH_CONT	Select from list	0	⚙️
⊖	SH_CONT_NON_COMPLIANT	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS NonCompliant	CL_POSTURE_NONCOMPL... SH_CONT	Select from list	0	⚙️
⊖	SH_CONT_COMPLIANT	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Compliant	CL_POSTURE_COMPLIANT SH_CONT	Select from list	0	⚙️
⊕	SH_CONT	AND Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	SG_CONT	SG_CONT	8	⚙️

# Posture Deployment – create some dACLs

Identity Services Engine Policy / Policy Elements

Downloadable ACL List > CL\_DACL\_POSTURE\_UNKNOWN

Downloadable ACL

\* Name \_DACL\_POSTURE\_UNKNOWN

Description

IP version  IPv4  IPv6  Agnostic ⓘ

\* DACL Content

```
1 permit udp any eq bootpc any eq bootps
2 permit udp any any eq 53
3 permit ip any host 172.16.33.12
4 deny ip any any
```

✓ Check DACL Syntax

Downloadable ACL List > CL\_DACL\_POSTURE\_NONCOMPLIANT

Downloadable ACL

\* Name \_POSTURE\_NONCOMPLIANT

Description

IP version  IPv4  IPv6  Agnostic ⓘ

\* DACL Content

```
1 permit udp any eq bootpc any eq bootps
2 permit udp any any eq 53
3 deny ip any 10.0.0.0.0.255.255.255
4 deny ip any 172.16.0.0.0.15.255.255
5 deny ip any 192.168.0.0.0.0.255.255
6 permit ip any any
```

✓ Check DACL Syntax

Downloadable ACL List > CL\_DACL\_COMPLIANT

Downloadable ACL

\* Name CL\_DACL\_COMPLIANT

Description

IP version  IPv4  IPv6  Agnostic ⓘ

\* DACL Content

```
1 permit udp any eq bootpc any eq bootps
2 permit udp any any eq 53
3 permit ip any any
```

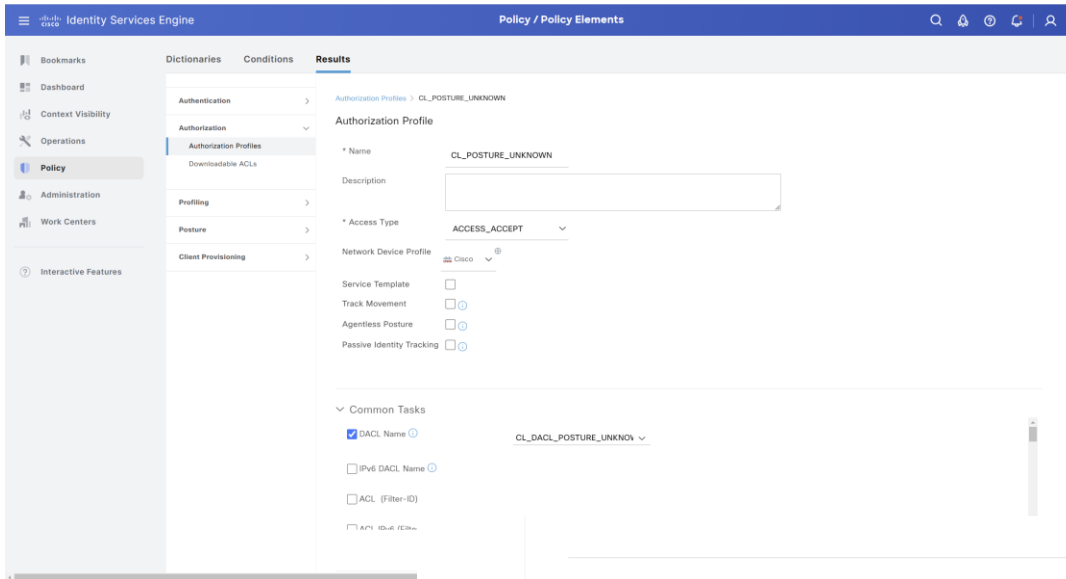
✓ Check DACL Syntax

# Posture Deployment – create AuthZ Profiles

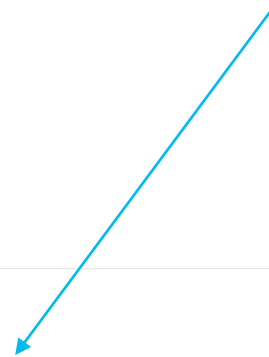
The screenshot displays the Cisco Identity Services Engine (ISE) interface. The top navigation bar shows 'Identity Services Engine' and 'Policy / Policy Elements'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy (selected), Administration, Work Centers, and Interactive Features. The main content area is titled 'Standard Authorization Profiles' and includes a sub-header 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below this, there are action buttons for Edit, Add, Duplicate, and Delete, along with a selection count 'Selected 0 Total 22'. A table lists various authorization profiles, with three posture-related profiles highlighted by a red box:

Name	Profile	Description
<input type="checkbox"/> Block_Wireless_Access	Cisco	Default profile used to block wireless devices. Ensure that you configure...
<input type="checkbox"/> CL-No-Redirect-Unknown	Cisco	CL-No-Redirect-Unknown
<input type="checkbox"/> CL_MACHINE_ACL	Cisco	
<input type="checkbox"/> CL_POSTURE_COMPLIANT	Cisco	
<input type="checkbox"/> CL_POSTURE_NONCOMPLIANT	Cisco	
<input type="checkbox"/> CL_POSTURE_UNKNOWN	Cisco	
<input type="checkbox"/> Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/> Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/> Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/> NSP_Onboard	Cisco	Onboard the device with Native Supplicant Provisioning
<input type="checkbox"/> Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input type="checkbox"/> PostureUnknown	Cisco	PostureUnknown
<input type="checkbox"/> SG_CONT	Cisco	
<input type="checkbox"/> SG_CORP	Cisco	
<input type="checkbox"/> SG_IOT	Cisco	
<input type="checkbox"/> SH_CONT	Cisco	SH_CONT

# Posture Deployment – Add Policy Elements



Catalyst Centre added the ACL to the Switch!



## Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Client Provisioning (Posture)  ACL  Value

Static IP/Host name/FQDN

Suppress Profiler CoA for endpoints in

Logical Profile

# Posture Deployment – Create Client provision portal

The image displays two screenshots from the Cisco Identity Services Engine (ISE) interface. The top screenshot shows the 'Client Provisioning Portals' page, which lists several portals: 'CL-Default-Client-Provision-Portal', 'CL-Redirect-Portal', 'Client Provisioning Portal (default)', and 'Client Provisioning Portal (default)\_copy2'. The bottom screenshot shows the 'Portals Settings and Customization' page for the 'CL-Redirect-Portal'. This page includes fields for 'Portal Name' and 'Description', a 'Language File' dropdown, and a 'Portal test URL' field. Below these are sections for 'Portal Behavior and Flow Settings' and 'Portal Page Customization'. The 'Portal & Page Settings' section includes 'Portal Settings' with fields for 'HTTPS port' (8443) and 'Posture State Synchronization port' (8449), and 'Allowed Interfaces' with checkboxes for 'Gigabit Ethernet 0', 'Gigabit Ethernet 1', and 'Gigabit Ethernet 2'. The 'Client Provisioning Portals Flow (based on settings)' section shows a flowchart: LOGIN -> Client Provision -> VLAN -> Success.

Use the one already in ISE!



# Posture Deployment – Create rules for Compliant and Non Compliant

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a non-compliant posture profile. The breadcrumb navigation is "Policy / Policy Elements > Authorization Profiles > CL\_POSTURE\_NONCOMPLIANT". The "Authorization Profile" section shows the following configuration:

- \* Name: CL\_POSTURE\_NONCOMPLIANT
- Description: (Empty text box)
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Agentless Posture:
- Passive Identity Tracking:

Under the "Common Tasks" section, the "DAACL Name" is set to CL\_DACL\_POSTURE\_NO, with a checked checkbox.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a compliant posture profile. The breadcrumb navigation is "Policy / Policy Elements > Authorization Profiles > CL\_POSTURE\_COMPLIANT". The "Authorization Profile" section shows the following configuration:

- \* Name: CL\_POSTURE\_COMPLIANT
- Description: (Empty text box)
- \* Access Type: ACCESS\_ACCEPT
- Network Device Profile: Cisco
- Service Template:
- Track Movement:
- Agentless Posture:
- Passive Identity Tracking:

Under the "Common Tasks" section, the "DAACL Name" is set to CL\_DACL\_COMPLIANT, with a checked checkbox.

# Posture Deployment – Create Some Conditions!

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application**
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Requirements
- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

## Application Condition

Rows/Page 6 << 1 / 1 >> Go 6 Total Rows

Add Duplicate Trash Edit Filter

<input type="checkbox"/>	Name	Description	Application State	Compliance mo...	Categories	Che...
<input type="checkbox"/>	CL-CHECK-ICLOUD		Installed	4.x or later	Data Storage	APPLI...
<input type="checkbox"/>	CL-CHECK_BALENA	CL-CHECK_BALENA	Installed	4.x or later	Unclassified	APPLI...
<input type="checkbox"/>	CL-CHECK_FIREFOX	CL-CHECK_FIREFOX	Installed	4.x or later	Browser	APPLI...
<input type="checkbox"/>	Default_AppVis_Condition_Mac	Cisco Predefined Check for installe...	Installed and Running	4.x or later		APPLI...
<input type="checkbox"/>	Default_AppVis_Condition_Win	Cisco Predefined Check for installe...	Installed and Running	4.x or later		APPLI...
<input type="checkbox"/>	MG-Application-Condition	MG Application Condition	Installed and Running	4.x or later		APPLI...

# Posture Deployment – Check Resources

The screenshot shows the Cisco Identity Services Engine (ISE) Work Centers / Posture interface. The main navigation bar includes 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar shows 'Work Centers' as the active section. The 'Resources' page is displayed, showing a table of posture resources.

<input type="checkbox"/>	Name	Type	Version	Last Update	Description
<input type="checkbox"/>	CiscoSecureClientDesktopW...	CiscoSecureClientDesktopWindows	5.1.6.103	2024/10/25 17:16:01	Cisco Secure Client for ...
<input type="checkbox"/>	CL25-Posture-Profile	AgentProfile	Not Applic...	2024/10/31 13:09:30	CL25-Posture-Profile
<input type="checkbox"/>	Cisco-ISE-Chrome-NSP	Native Supplicant Profile	Not Applic...	2016/10/06 21:01:12	Pre-configured Native S...
<input type="checkbox"/>	CiscoSecureClientComplian...	CiscoSecureClientComplianceModuleWindows	4.3.4248....	2024/10/28 12:50:16	Cisco Secure Client Win...
<input type="checkbox"/>	CiscoAgentlessWindows 5.0...	CiscoAgentlessWindows	5.0.3061.0	2023/07/03 23:54:10	With CM: 4.3.3506.8192
<input type="checkbox"/>	CL25-Agent-Conf	AgentConfig	Not Applic...	2024/10/31 13:11:44	CL25-Agent-Conf
<input type="checkbox"/>	MacOsXSPWizard 2.7.0.1	MacOsXSPWizard	2.7.0.1	2023/07/03 23:54:02	Supplicant Provisioning ...
<input type="checkbox"/>	Cisco-ISE-NSP	Native Supplicant Profile	Not Applic...	2023/07/04 00:55:16	Pre-configured Native S...
<input type="checkbox"/>	WinSPWizard 3.2.0.1	WinSPWizard	3.2.0.1	2023/07/03 23:54:02	Supplicant Provisioning ...
<input type="checkbox"/>	CiscoSecureClientComplian...	CiscoSecureClientComplianceModuleWindows	4.3.4289....	2024/10/28 12:50:00	Cisco Secure Client Win...
<input type="checkbox"/>	CiscoAgentlessOSX 5.0.030...	CiscoAgentlessOSX	5.0.3061.0	2023/07/03 23:54:14	With CM: 4.3.3045.6400
<input type="checkbox"/>	CiscoTemporalAgentWindo...	CiscoTemporalAgentWindows	5.0.3061.0	2023/07/03 23:54:03	With CM: 4.3.3506.8192
<input type="checkbox"/>	SecureClientPostureProfile	AgentProfile	Not Applic...	2024/10/25 15:53:53	SecureClientPostureProfile
<input type="checkbox"/>	CiscoTemporalAgentOSX 5....	CiscoTemporalAgentOSX	5.0.3061.0	2023/07/03 23:54:07	With CM: 4.3.3045.6400

# Posture Deployment – Add Agent Configuration

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring a Client Provisioning Policy. The breadcrumb trail is 'Agent Configuration > CL25-Agent-Conf'. The configuration includes:

- Select Agent Package:** CiscoSecureClientDesktopWindows 5.1.6.103
- Configuration Name:** CL25-Agent-Conf
- Description:** CL25-Agent-Conf
- Description Value Notes:** A section for additional notes.
- Compliance Module:** CiscoSecureClientComplianceModuleWindows
- Cisco Secure Client Module Selection:** A list of modules with checkboxes:
  - ISE Posture:
  - VPN:
  - Zero Trust Access:
  - Network Access Manager:
  - Secure Firewall Posture:
  - Network Visibility:
  - ...:

# Posture Deployment – Add Agent Configuration

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring Posture. The top navigation bar includes the Cisco logo, 'Identity Services Engine', and 'Work Centers / Posture'. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers, and Interactive Features. The main content area is divided into tabs: Overview, Network Devices, Client Provisioning (selected), Policy Elements, Posture Policy, Policy Sets, Troubleshoot, Reports, and Settings.

Under the 'Client Provisioning' tab, there are two sections:

- Resources:** A list of resources with checkboxes for selection:
  - Client Provisioning Policy
  - Client Provisioning Portal
  - Network Access Manager
  - Secure Firewall Posture
  - Network Visibility
  - Umbrella
  - Start Before Logon
  - Diagnostic and Reporting Tool
- Profile Selection:** A dropdown menu for selecting profiles:
  - \* ISE Posture: CL25-Posture-Profile
  - VPN
  - Network Access Manager
  - Network Visibility
  - Umbrella
  - Customer Feedback

At the bottom right, there is a note: "Cisco Secure Client can be customized to display your own corporate logo".

# Posture Deployment – Add Agent Posture profile

The screenshot displays the Cisco Identity Services Engine (ISE) interface for configuring an Agent Posture Profile. The breadcrumb path is "ISE Posture Agent Profile Settings > CL25-Posture-Profile".

**Agent Posture Profile**

Name \*  
CL25-Posture-Profile

Description:  
CL25-Posture-Profile

**Agent Behavior**

Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent
Operate on non-802.1X wireless	No	Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	Check the signature of executables before running them.
Log file size	5 MB	The maximum agent log file size
Remediation timer	4 mins	If the user fails to remediate within this specified time, mark them as non-compliant.
Stealth Mode	Disabled	Agent can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Enabled	Display user notifications even when in Stealth mode.
Enable Rescan Button	Disabled	Displays the rescan button on the System tile. The user can run posture again, if the first posture failed. Both the posture policies and the Cisco ISE posture module run.
Disable UAC Prompt	Yes	By turning off UAC Prompt, AC posture uses system process for privilege escalation instead of "Run as administrator". Please validate your posture policies as enabling this option may have local admin rights even in disabled UAC prompt.

# Posture Deployment – Add Agent Posture profile

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Posture profile. The main navigation bar includes 'Work Centers / Posture' and various utility icons. The left sidebar contains navigation options like 'Bookmarks', 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration', 'Work Centers', and 'Interactive Features'. The main content area is divided into tabs: 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The 'Client Provisioning' tab is active, showing a 'Client Provisioning Policy' configuration. A 'Resources' section is visible on the left. The 'Posture Protocol' section is highlighted with a red box and contains the following parameters:

Parameter	Value	Description
Network transition delay	3 secs	The period for which the agent suspends network monitoring so it can wait for a planned IP change to happen
Posture Protocol		
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery host	isepan1.sdalab.lab	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List	1 PSN(s)	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules *	*.sdalab.lab,*.cisco.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. *.cisco.com
Call Home List	172.16.33.12	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Below the 'Posture Protocol' section, there is a 'Custom messages for non-compliant status' section with a table structure.

# Posture Deployment – Add Remediations

The screenshot shows the Cisco Identity Services Engine (ISE) Work Centers / Posture interface. The main navigation bar includes 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar contains various navigation options, with 'Work Centers' selected. The main content area is titled 'Application Remediation' and features a table of remediations. The table has the following data:

<input type="checkbox"/>	Name	Description	Application State	Compliance mo...	Categories
<input type="checkbox"/>	CL-remove-icloud	CL-remove-balena		4.x or later	
<input type="checkbox"/>	CL_RemoveFirefox	CL_RemoveFirefox		4.x or later	



# Posture Deployment – Add Requirements

Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Action
Default_AppVis_Requirement_Win_temporal	Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Win	then Select Remediations
Default_AppVis_Requirement_Mac_temporal	Mac OSX	using 4.x or later	using Temporal Agent	met if Default_AppVis_Condition_Mac	then Select Remediations
Default_Hardware_Attributes_Requirement_Win_temporal	Windows All	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Hardware_Attributes_Requirement_Mac_temporal	Mac OSX	using 4.x or later	using Temporal Agent	met if Hardware_Attributes_Check	then Select Remediations
Default_Firewall_Requirement_Win_temporal	Windows All	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Win	then Default_Firewall_Remediation_Win
Default_Firewall_Requirement_Mac_temporal	Mac OSX	using 4.x or later	using Temporal Agent	met if Default_Firewall_Condition_Mac	then Default_Firewall_Remediation_Mac
CL-FW-Requirement	for Windows All	using 4.x or later	using Agent	met if CL_WINFW_REGCHECK	then Message Text Only
CL-Firefox_Check	for Windows All	using 4.x or later	using Agent	met if CL_CHECK_FIREFOX	then CL_RemoveFirefox
CL-Icloud-check	for Windows All	using 4.x or later	using Agent	met if CL-CHECK-ICLOUD	then CL-remove-icloud

**Note:**  
Remediation Action is filtered based on the operating system and stealth mode selection.  
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.  
Remediations Actions are not applicable for Agentless Posture type.

Save Reset

This ties it together

# Posture Deployment – Add Posture Policy

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning Policy Elements **Posture Policy** Policy Sets Troubleshoot Reports Settings

## Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Req
<input checked="" type="checkbox"/>	Policy Options	CL-Check-Firefox	If Any	and Windows All	and 4.x or later	and Agent	and LAB1:ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	then CL-f
<input checked="" type="checkbox"/>	Policy Options	CL-Windows-Firewall-Policy	If Any	and Windows All	and 4.x or later	and Agent	and LAB1:ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	then CL-f
<input checked="" type="checkbox"/>	Policy Options	CL-icloud-check-policy	If Any	and Windows All	and 4.x or later	and Agent	and LAB1:ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	then CL-l

# Posture Deployment – Client provisioning

**Client Provisioning Policy**

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation.  
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.  
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.  
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.  
Mac ARM64 policies require no Other Conditions arm64 configurations.  
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
<input checked="" type="checkbox"/> CL_WINDOWS	If Any	and Windows All	and Condition(s)	then CL25-Agent-Conf
<input type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
<input type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
<input type="checkbox"/> Windows	If Any	and Windows All	and Condition(s)	then CL25-Agent-Conf
<input type="checkbox"/> MAC OS	If Any	and Mac OSX	and Condition(s)	then CiscoTemporalAgentOSX 5.0.03061 And MacOsXSPWizard 2.7.0.1 And Cisco-ISE-NSP
<input type="checkbox"/> Chromebook	If Any	and Chrome OS All	and Condition(s)	then Cisco-ISE-Chrome-NSP

Save Reset

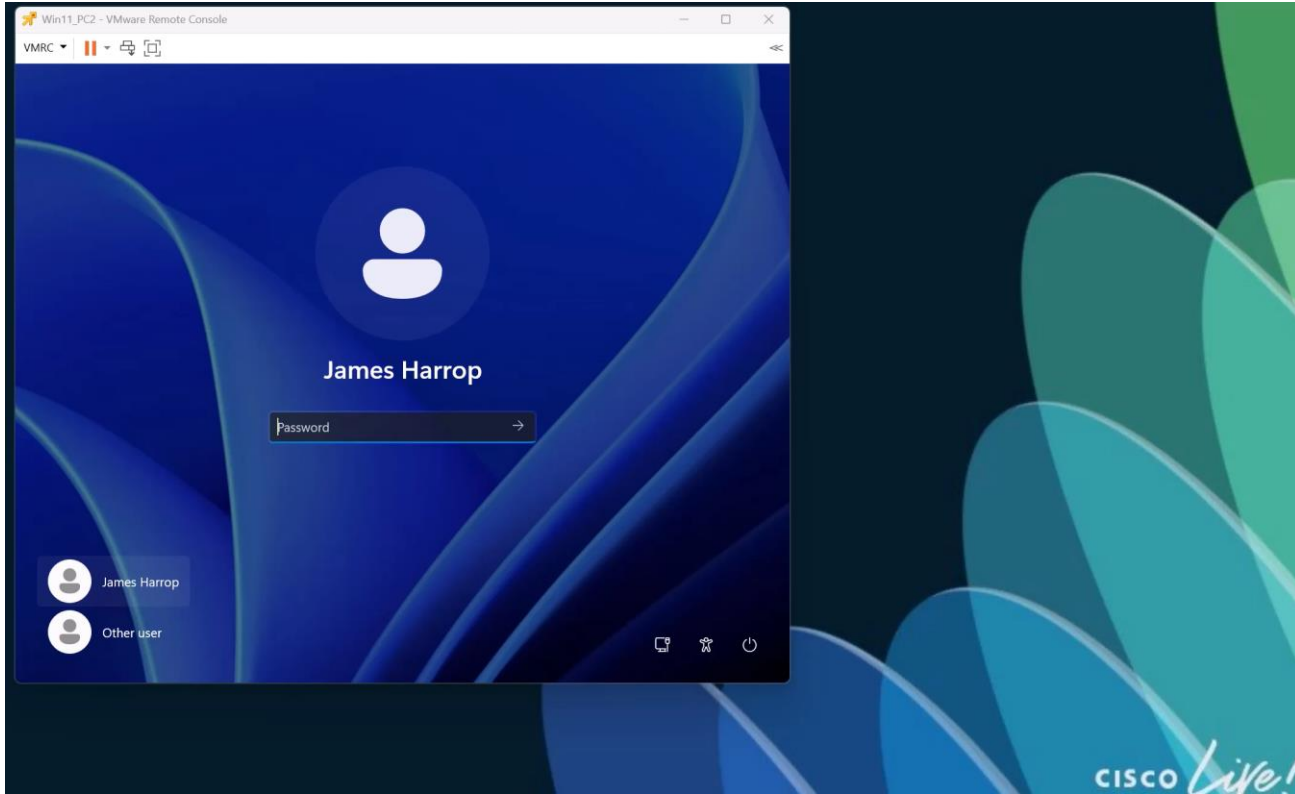
# Posture Deployment – Client provisioning

The screenshot displays the Cisco Identity Services Engine (ISE) Work Centers / Posture interface. The left sidebar contains navigation options: Bookmarks, Dashboard, Context Visibility, Operations, Policy, Administration, Work Centers (selected), and Interactive Features. The main content area shows a table of Policy Sets under the 'Policy Sets' tab. The table has columns for Status, Rule Name, Conditions, Profiles, Security Groups, Hits, and Actions. The table lists several policy sets, each with a status icon, a rule name, a list of conditions, associated profiles, security groups, and hit counts.

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
🟢	SH_MACHINE	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/Domain Computers	CL_MACHINE_ACL SH_CONT	Select from list	5	⚙️
🟢	SH_IOT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_IOT	SG_IOT	SG_IOT	6	⚙️
🟢	SH_CONT_UNKNOWN	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Unknown	CL_POSTURE_UNKNOWN SH_CONT	Select from list	0	⚙️
🟢	SH_CONT_NON_COMPLIANT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS NonCompliant	CL_POSTURE_NONCOMPL... SH_CONT	Select from list	0	⚙️
🟢	SH_CONT_COMPLIANT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT Session-PostureStatus EQUALS Compliant	CL_POSTURE_COMPLIANT SH_CONT	Select from list	0	⚙️
🟡	SH_CONT	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CONT	SG_CONT	SG_CONT	8	⚙️
🟢	SH_CORP	Wired_802.1X LAB1-ExternalGroups EQUALS sdalab.lab/Users/SDA1_CORP	SG_CORP	SG_CORP	10	⚙️

Enable Posture AuthZ rules

# Posture Deployment – Posture in Action – Demo



# Posture Deployment – see the result!

The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the Operations / RADIUS Live Sessions page. The interface includes a navigation sidebar on the left with options like Bookmarks, Dashboard, Context Visibility, Operations (selected), Policy, Administration, and Work Centers. The main content area shows a table of live sessions with columns for Initiated, Updated, Session Status, Action, Endpoint ID, Identity, IP Address, Endpoint Profile, Posture Status, and Security. A session is shown with a 'Compliant' posture status, highlighted by a red box. Below this, a detailed view of the session is shown, with columns for Security Group, Server, Auth Method, Authentication Protocol, Authentication Policy, Authorization Policy, Authorization Profiles, and NAS IP Address. The 'Authentication Policy', 'Authorization Policy', and 'Authorization Profiles' columns are highlighted by a red box.

Initiated	Updated	Session Sta...	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture St...	Securit
Jan 21, 2025 12:30:54.92...	Jan 21, 2025 12:30:57.2...	Postured	Show CoA Actions	00-0C:29-C0-D1:EC	SDALAB\james	172.16.206.2,fe8 ...	Windows11-Workst...	Compliant	Security

Security G...	Server	Auth M...	Authentication Proto...	Authentication Policy	Authorization Policy	Authorization Profiles	NAS IP Address
Security Grou	Server	Auth Meth	Authentication Protocol	Authentication Policy	Authorization Policy	Authorization Profiles	NAS IP Address
	isepan1	dot1x	PEAP (EAP-MSCHAPv2)	Default >> Dot1X	Default >> SH_CONT_COMPLIANT	CL_POSTURE_COMPLIANT,SH_CONT	172.16.210.250

# Dot1X – Full Config to add

```
! create test user on ISE internal DB as well
username isetest secret 0 C1sco12345
```

```
!
radius-server vsa send authentication
radius-server vsa send accounting
```

```
! Local ACLs
```

```
!
ip access-list extended ACL_Default
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 permit tcp any host 172.16.33.10 eq 8443
 deny ip any any
```

```
!
! Create ACL used when AAA is down to fail open (Internet only)
```

```
ip access-list extended AAA-Down
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny ip any 10.0.0.0 0.255.255.255
 deny ip any 192.168.0.0 0.0.255.255
 permit ip any any
```

```
! Create Blackhole ACL
```

```
ip access-list extended ACL_Blackhole
 permit tcp any any eq www
 deny ip any any
```

```
! Prevent consumption of BPDUs for all portfast edge ports globally
spanning-tree portfast bpdupfilter default
```

```
! Enable 802.1x globally
dot1x system-auth-control
dot1x critical eapol
```

```
! Allow session tear down when MAC address detected elsewhere
no access-session mac-move deny
access-session acl default passthrough
```

```
! This is for device profiling ***
! Enable device sensors
! DHCP snooping is required for device sensor data to work properly
ip dhcp snooping
no ip dhcp snooping information option
! VLAN list is comma separated
ip dhcp snooping vlan 200,202,204,206,208
```

```
! Enable specific device sensors for profiling
device-sensor filter-list dhcp list dhcp_list
option name host-name
option name requested-address
option name parameter-request-list
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list dhcp_list
! Enable CDP globally
cdp run
device-sensor filter-list cdp list cdp_list
tlv name device-name
tlv name address-type
tlv name capabilities-type
tlv name platform-type
device-sensor filter-spec cdp include list cdp_list
! Enable LLDP globally
lldp run
device-sensor filter-list lldp list lldp_list
tlv name system-name
tlv name system-description
tlv name system-capabilities
device-sensor filter-spec lldp include list lldp_list
! Send sensor data to ISE and disable local analyzer
device-sensor notify all-changes
```

```
! Include CDP, LLDP, and DHCP information for the access session
access-session attributes filter-list list sensor_list
cdp
lldp
dhcp
access-session accounting attributes filter-spec include list sensor_list
access-session authentication attributes filter-spec include list sensor_list
```



```
! These are the dot1x bits ****
! Create critical endpoint vlan access
service-template Critical_Access
  vlan 208
  access-group AAA-Down
```

```
! Create critical phone vlan access
service-template Critical_Voice
  voice vlan
```

```
! Configure control classes
class-map type control subscriber match-all AAA-Down_Auth_Host
  match result-type aaa-timeout
  match authorization-status authorized
!
class-map type control subscriber match-all AAA-Down_UnAuth_Host
  match result-type aaa-timeout
  match authorization-status unauthorized
!
class-map type control subscriber match-all Dot1x
  match method dot1x
!
class-map type control subscriber match-all Dot1x_Failed
  match method dot1x
  match result-type method dot1x authoritative
!
class-map type control subscriber match-all Dot1x_No-Resp
  match method dot1x
  match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all Dot1x_Timeout
  match method dot1x
  match result-type method dot1x method-timeout
!
class-map type control subscriber match-any Critical_Auth
  match activated-service-template Critical_Access
  match activated-service-template Critical_Voice
!
class-map type control subscriber match-all MAB
  match method mab
!
class-map type control subscriber match-all MAB_Failed
  match method mab
  match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_Critical_Auth
  match activated-service-template Critical_Access
  match activated-service-template Critical_Voice
!
```

```
! Configure policy maps
! Policy map applied to all Dot1xMAB interfaces
policy-map type control subscriber Dot1x-Default
event session-started match-all
  10 class always do-until-failure
  10 authenticate using dot1x priority 10
event authentication-failure match-first
5 class Dot1x_Failed do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
10 class AAA-Down_UnAuth_Host do-until-failure
  10 clear-authenticated-data-hosts-on-port
  20 activate service-template Critical_Access
  30 activate service-template Critical_Voice
  40 authorize
  50 pause reauthentication
20 class AAA-Down_Auth_Host do-until-failure
  10 pause reauthentication
  20 authorize
30 class Dot1x_No-Resp do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
40 class MAB_Failed do-until-failure
  10 terminate mab
  20 authentication-restart 60
60 class always do-until-failure
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
event agent-found match-all
10 class always do-until-failure
  10 terminate mab
  20 authenticate using dot1x priority 10
event aaa-available match-all
10 class Critical_Auth do-until-failure
  10 clear-session
20 class NOT_Critical_Auth do-until-failure
  10 resume reauthentication
event inactivity-timeout match-all
10 class always do-until-failure
  10 clear-session
event authentication-success match-all
  10 class always do-until-failure
  10 activate service-template DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
event violation match-all
10 class always do-until-failure
  10 restrict
!
```

```
! create port-templates ****
! Monitor mode or Low Impact port template
template Port-Dot1x-Default
  switchport mode access
  switchport access vlan 208
  switchport nonegotiate
  switchport voice vlan 202
  spanning-tree portfast
  spanning-tree bpduguard enable
  authentication periodic
  authentication timer reauthenticate server
  mab
  access-session host-mode multi-auth
  access-session control-direction in
  no access-session closed
  dot1x pae authenticator
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
  access-session port-control auto
  spanning-tree portfast
  ip dhcp snooping limit rate 10
  subscriber aging inactivity-timer 8400 probe
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default
```

```
! Closed mode port template
template Port-Dot1x-Closed
  switchport mode access
  switchport access vlan 208
  switchport nonegotiate
  switchport voice vlan 202
  spanning-tree portfast
  spanning-tree bpduguard enable
  authentication periodic
  authentication timer reauthenticate server
  mab
  access-session host-mode multi-domain
  access-session control-direction in
  access-session closed
  dot1x pae authenticator
  dot1x timeout tx-period 7
  dot1x max-reauth-req 3
  access-session port-control auto
  spanning-tree portfast
  ip dhcp snooping limit rate 10
  subscriber aging inactivity-timer 8400 probe
  subscriber aging probe
  service-policy type control subscriber Dot1x-Default
```

```
device-tracking tracking auto-source
```

```
! Standard IPDT policy - modify DNAC deployed one.
device-tracking policy IPDT_Policy
  security-level glean
  limit address-count 10
  tracking enable
```

```
! Only apply to a trunk port
device-tracking policy Disable_DT_Trunk
  trusted-port
  device-role switch
```

```
! Uplink interface must be trusted for DHCP traffic
! If there is a port channel configured for the uplink ports, add to the
! port channel interface configuration instead of the port interface.
interface range gi1/0/23 - 24
  ip dhcp snooping trust
```

```
! Access port interface configuration **
! Only apply one - monitor - low - closed
! Monitor Mode
!
!interface range GigabitEthernet1/0/1 - 12
! source template Port-Dot1x-Default
! device-tracking attach-policy IPDT_Policy
! dot1x timeout tx-period 7
! dot1x max-reauth-req 3

! Low Impact Mode
!
!interface range GigabitEthernet1/0/1 - 12
! source template Port-Dot1x-Default
! ip access-group ACL_Default in
! device-tracking attach-policy IPDT_Policy
! dot1x timeout tx-period 7
! dot1x max-reauth-req 3

! Closed mode
interface range GigabitEthernet1/0/1 - 12
 source template Port-Dot1x-Closed
 device-tracking attach-policy IPDT_Policy
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3

! Trunk port configuration to disable device tracking
interface range gi1/0/23 - 24
 device-tracking attach-policy Disable_DT_Trunk
```

CISCO *Live!*

GO BEYOND

A series of overlapping, rounded, teardrop-shaped abstract forms in various shades of blue, ranging from light to dark, positioned on the right side of the image.