Secure the Wired Network

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

Matt Graham
Solutions Architect

BRKOPS-2584

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 :

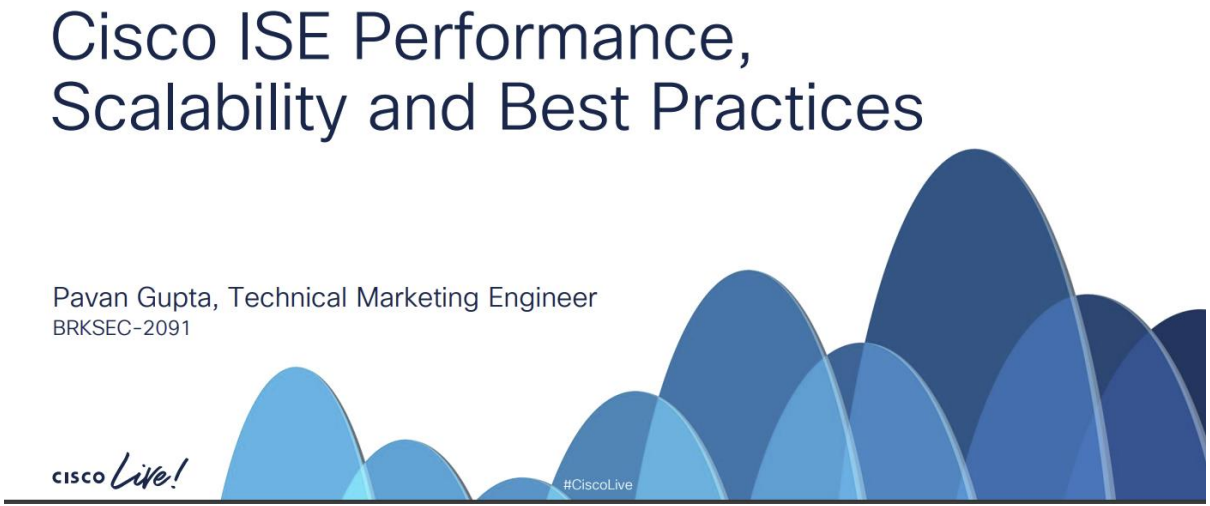
- Deep dive on how to setup ISE!
- Explore every option for IBNS
- Deep dive on ISE Policies – but enough will be provided!
- Explore all available options for Posture – there are simply too many!

Zero Trust

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

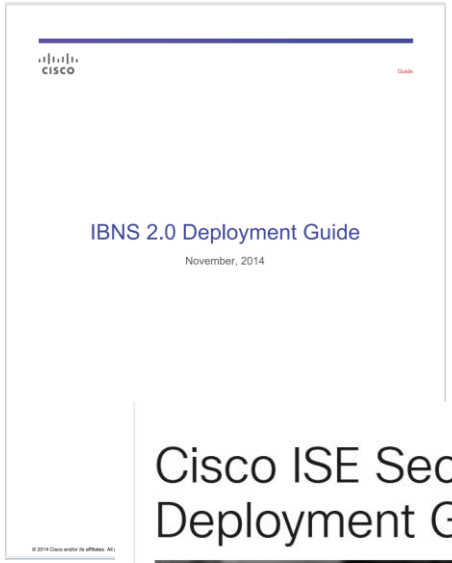
ISE – Deep Dive – BRKSEC-2091

This is a really good deep dive!



Challenges

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



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

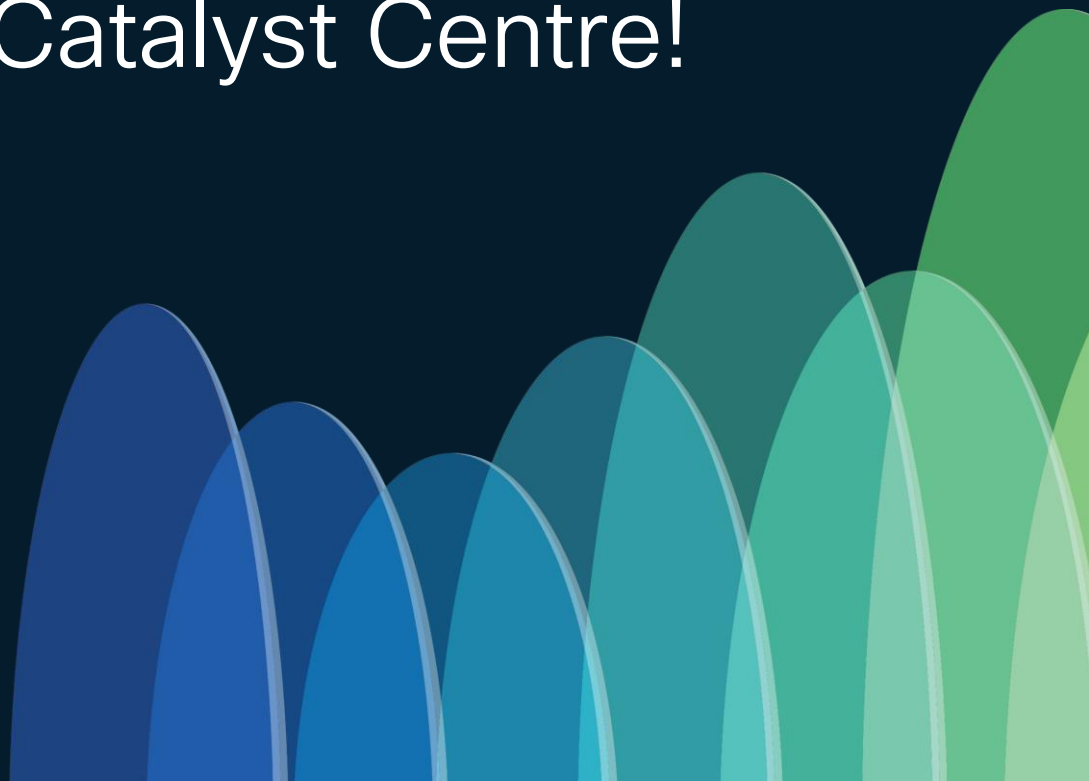
There's a lot of config...

```
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 bpdufilter enabl
 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
```

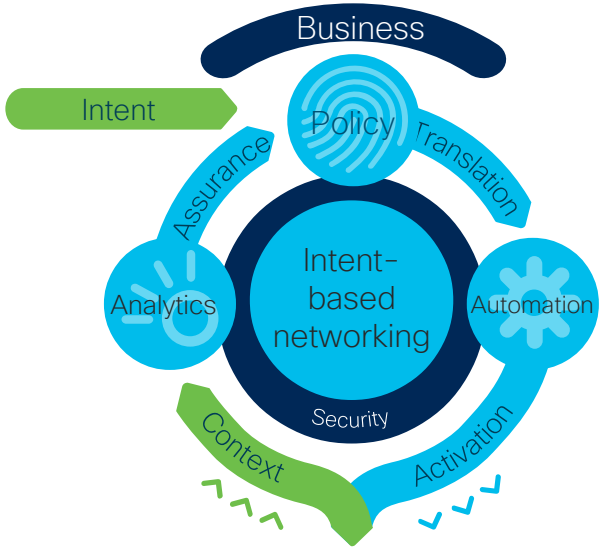
Go Beyond with Catalyst Centre!



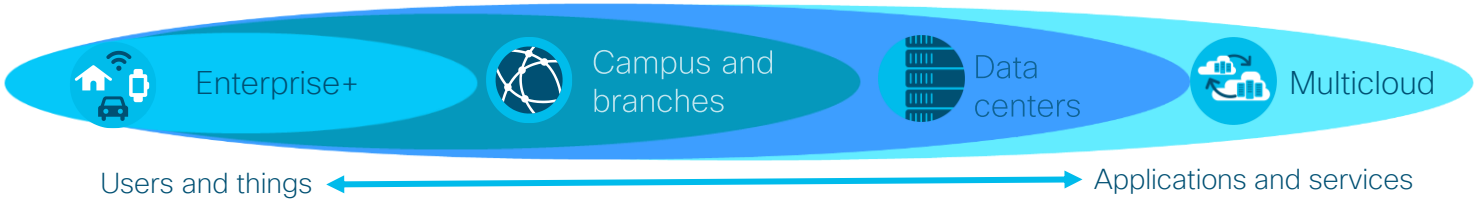
cisco Live!

Intent-based networking

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

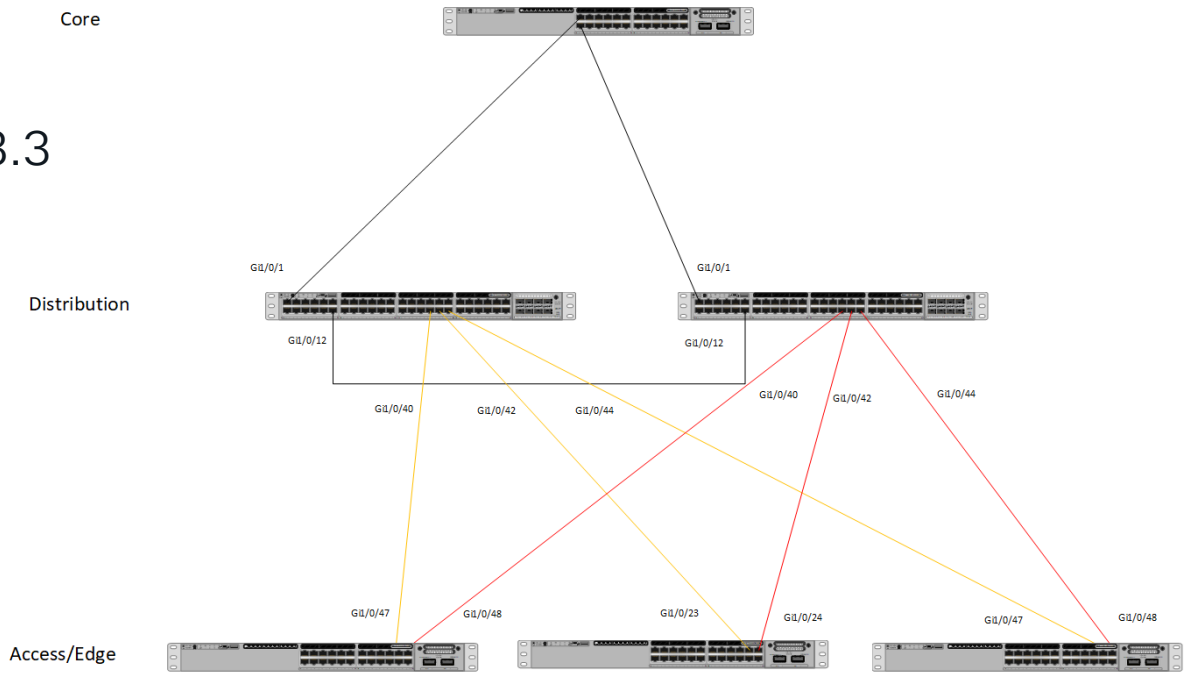


- Comprehensive automation
- Analytics and assurance
- Consistent security

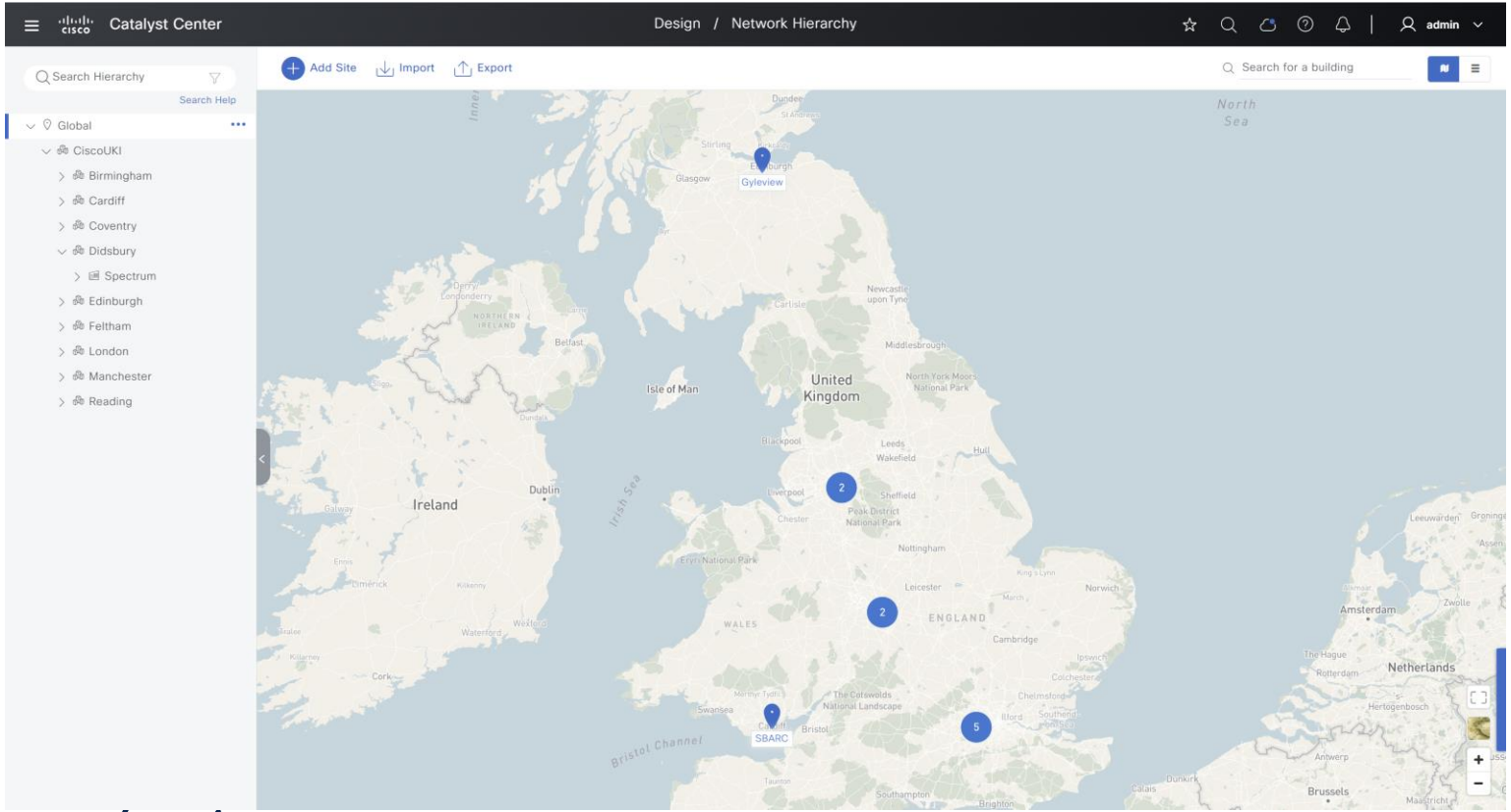


The network we are using

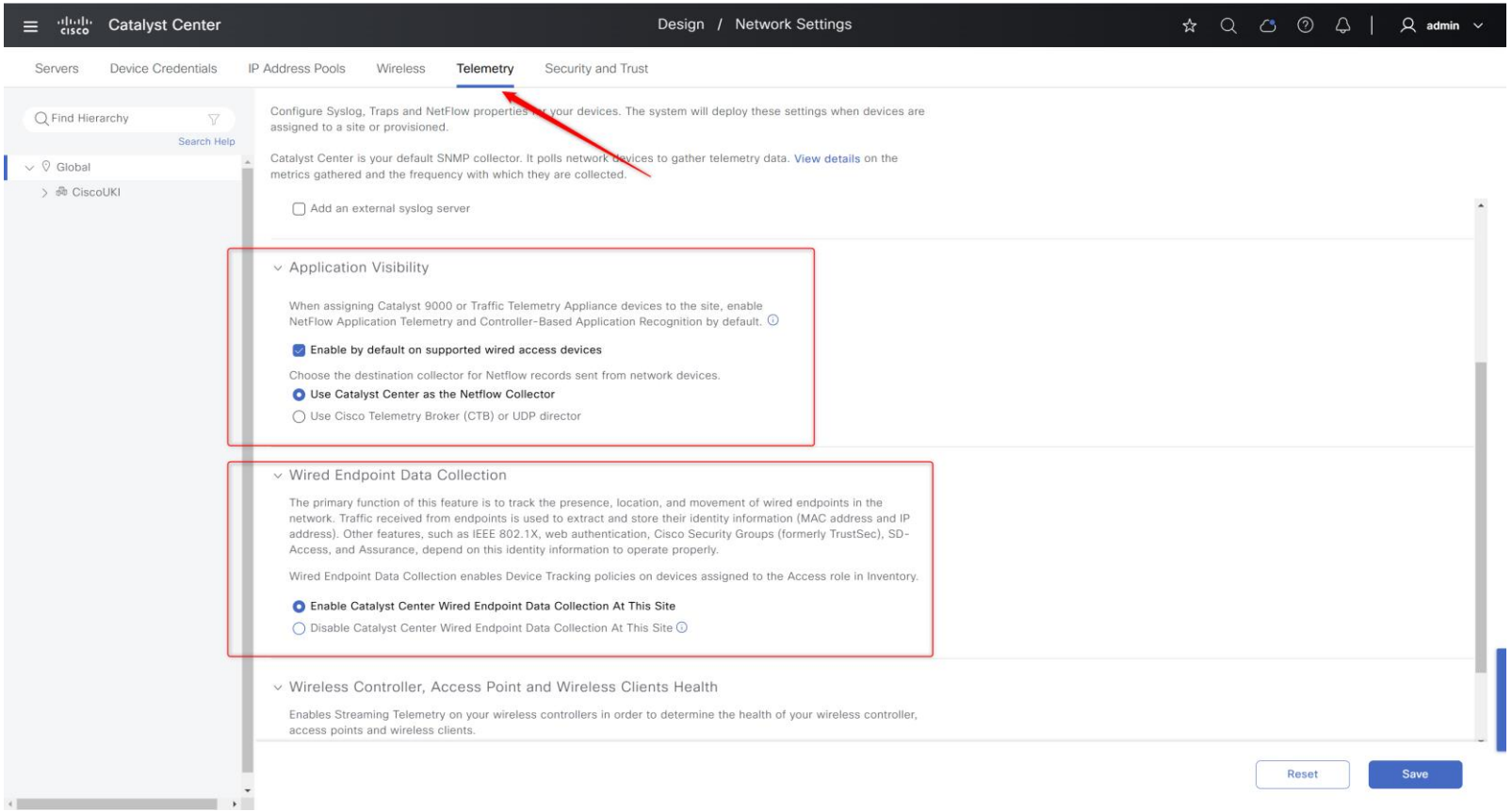
All Catalyst 9Ks
Identity Services Engine 3.3
Catalyst Centre 2.3.7.7



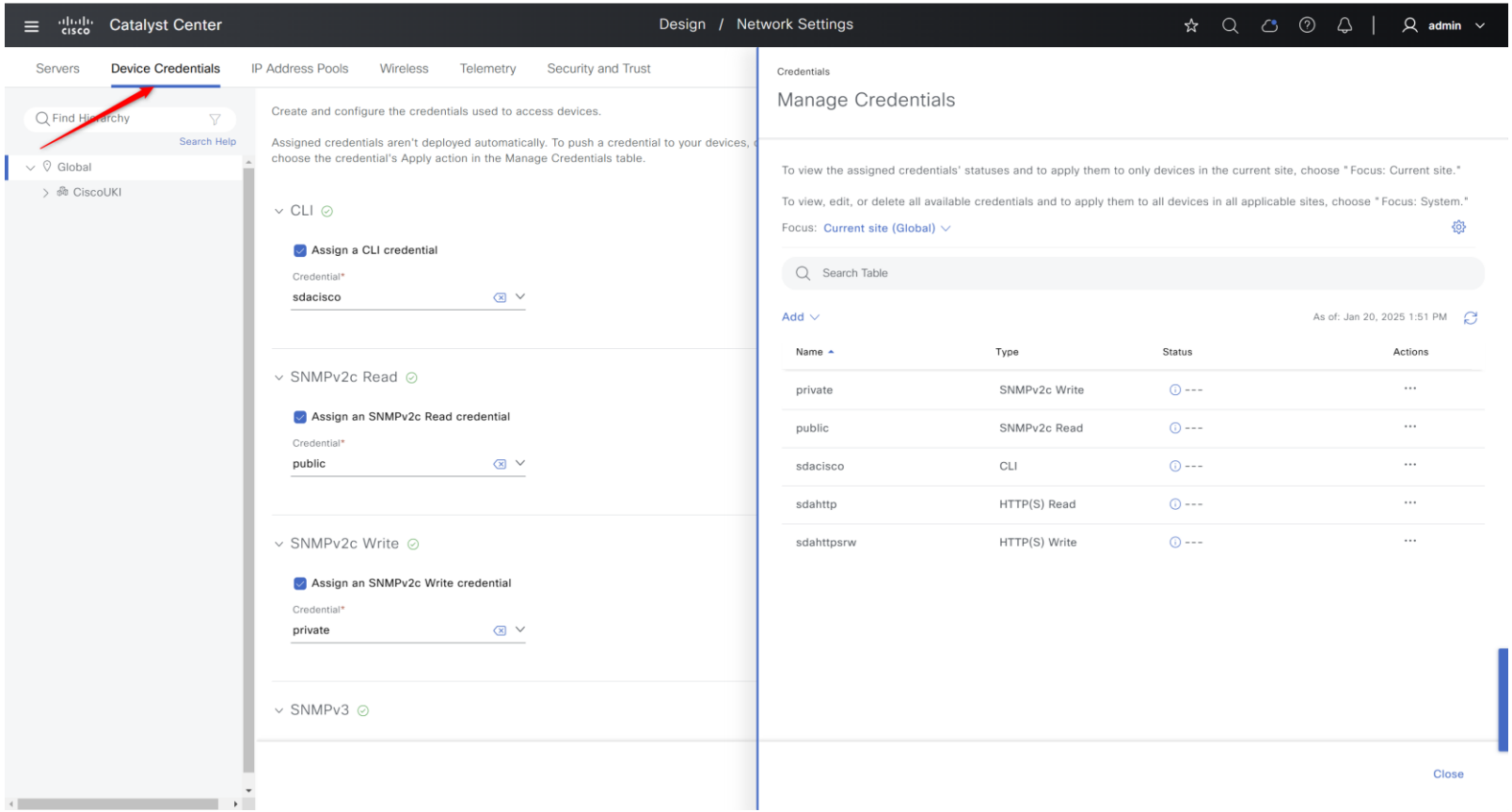
Start with Catalyst Centre



Check Telemetry and Wired Data Collection



Check Device Credentials



Typical Port Configurations

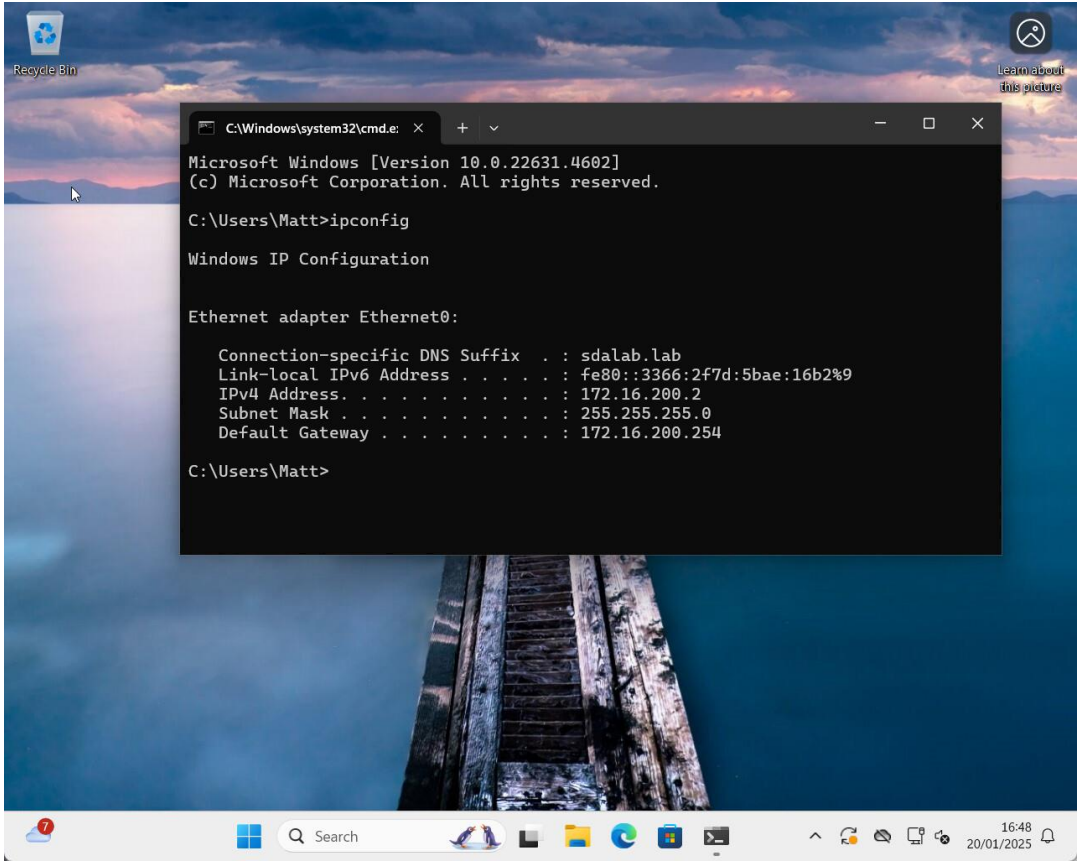
```
edge1#showint
interface GigabitEthernet1/0/1
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/2
 switchport access vlan 208
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/0/3
 switchport access vlan 208
 switchport 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
!
```

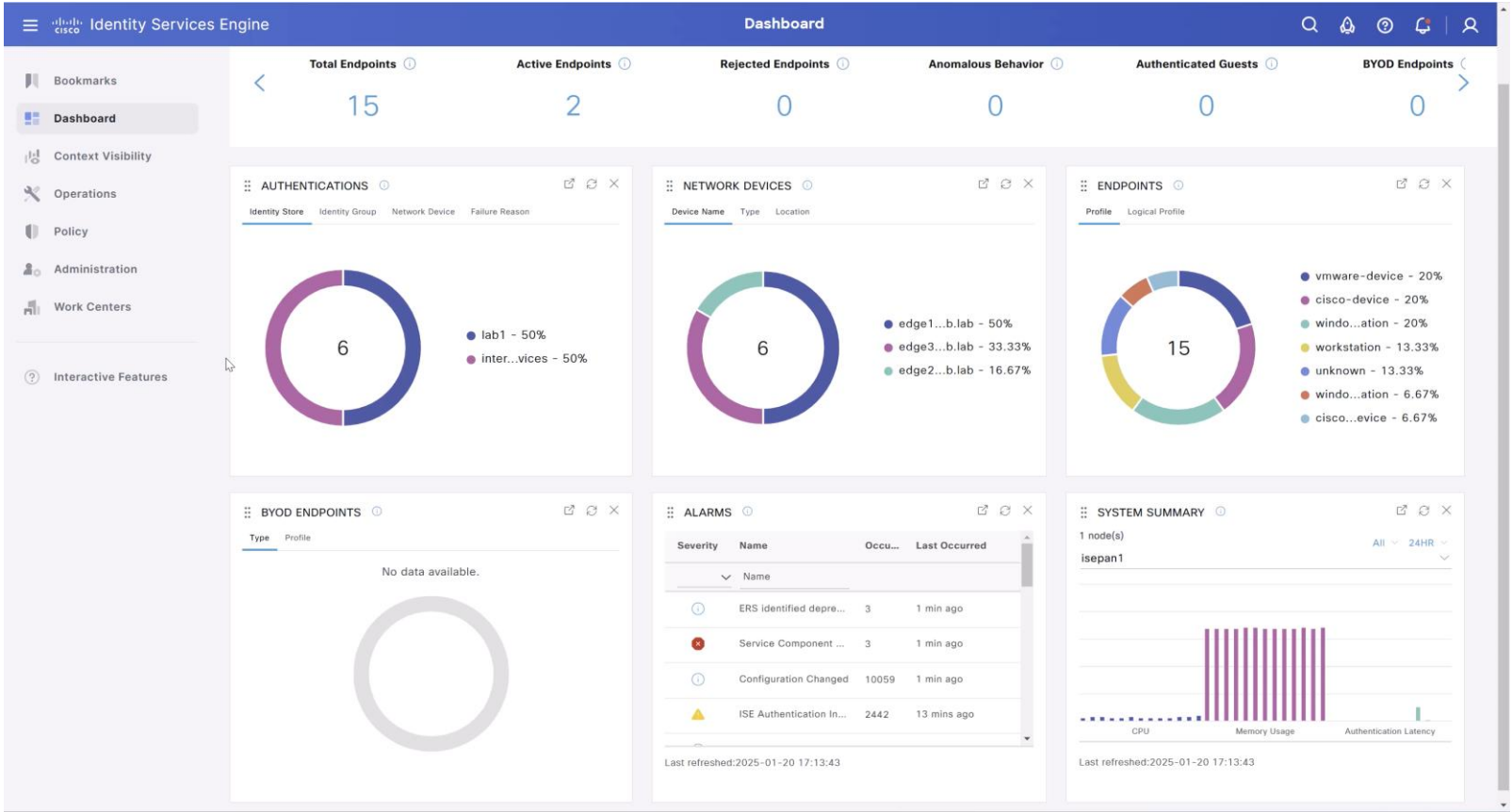
Static vlan assignment

Endpoints Connected

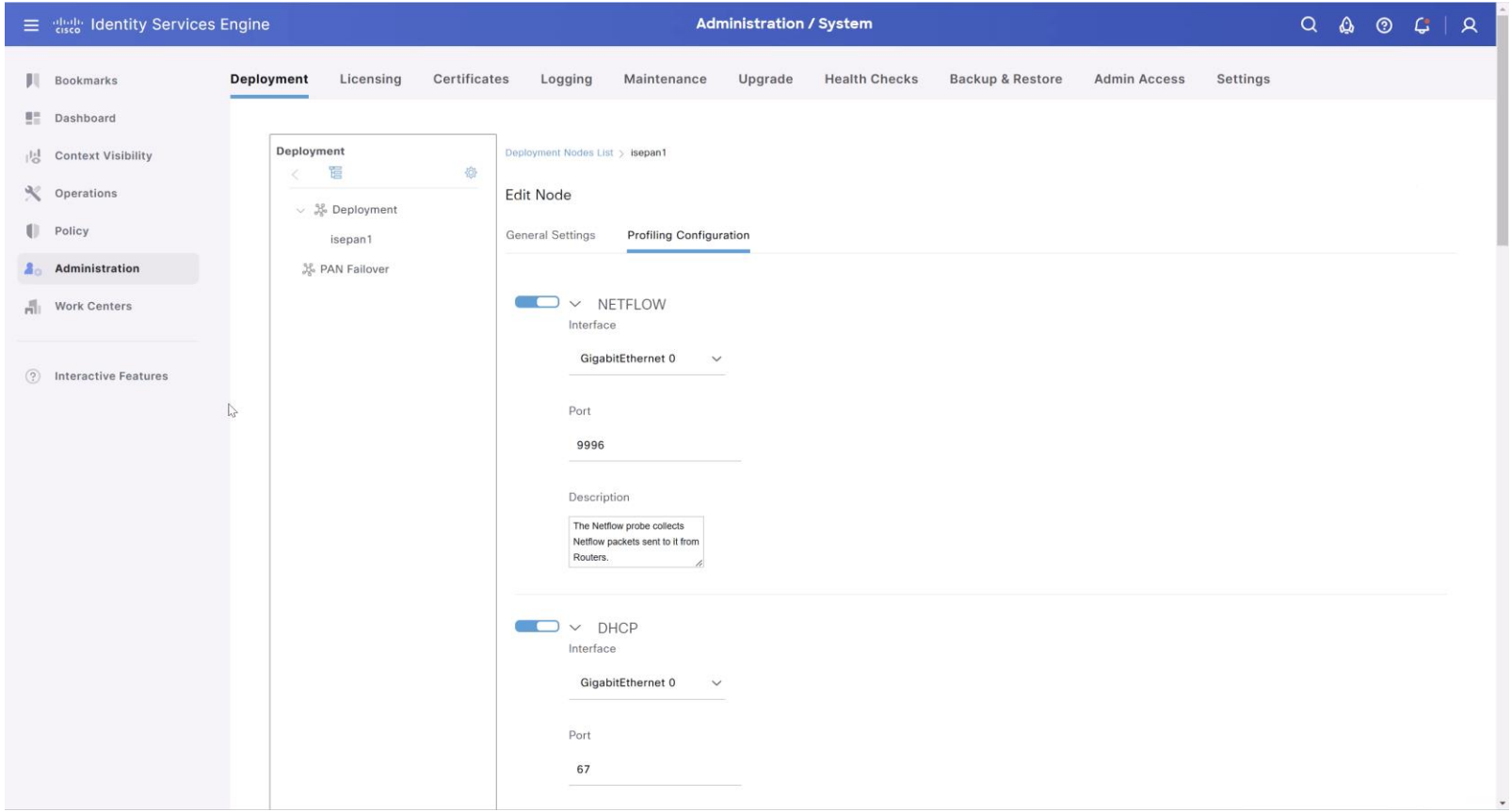
DHCP Assigned IP
No Port Security!



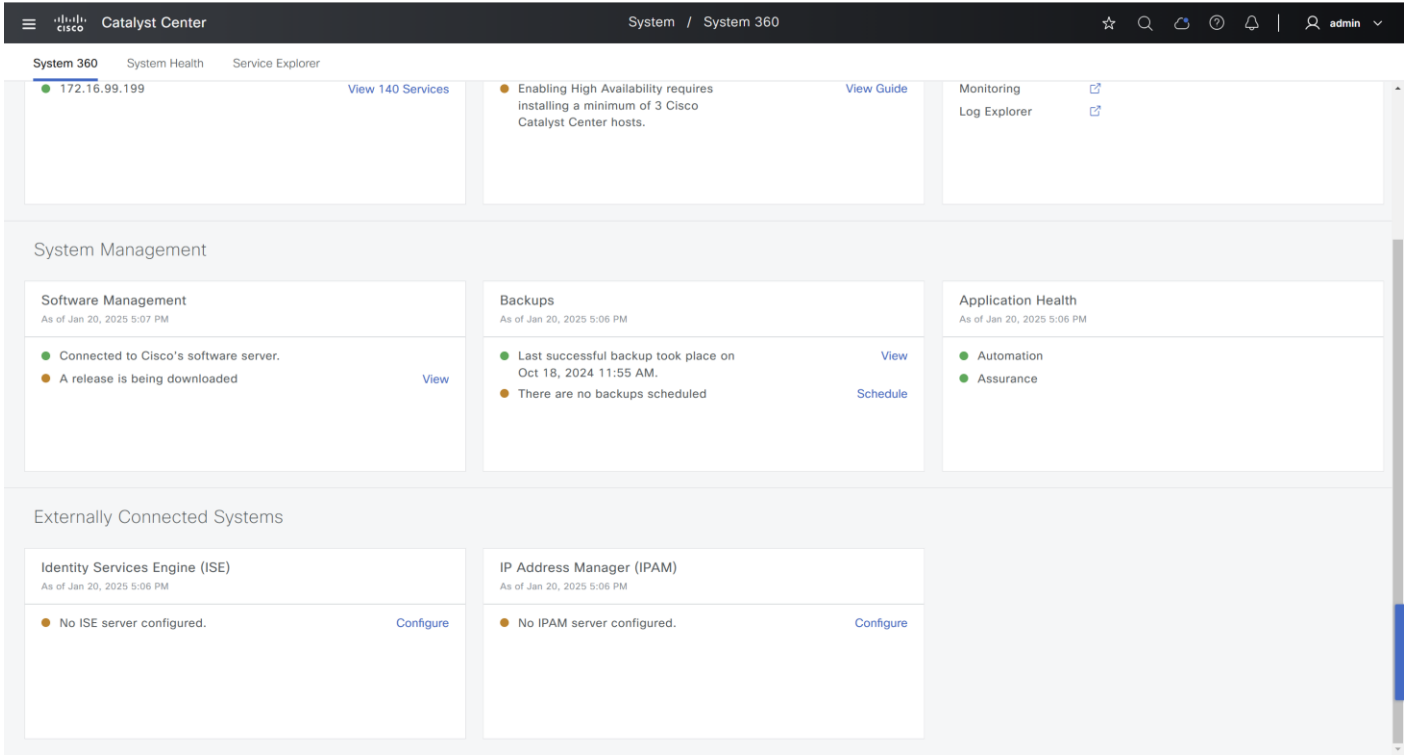
Get ISE Ready – Deployment demo



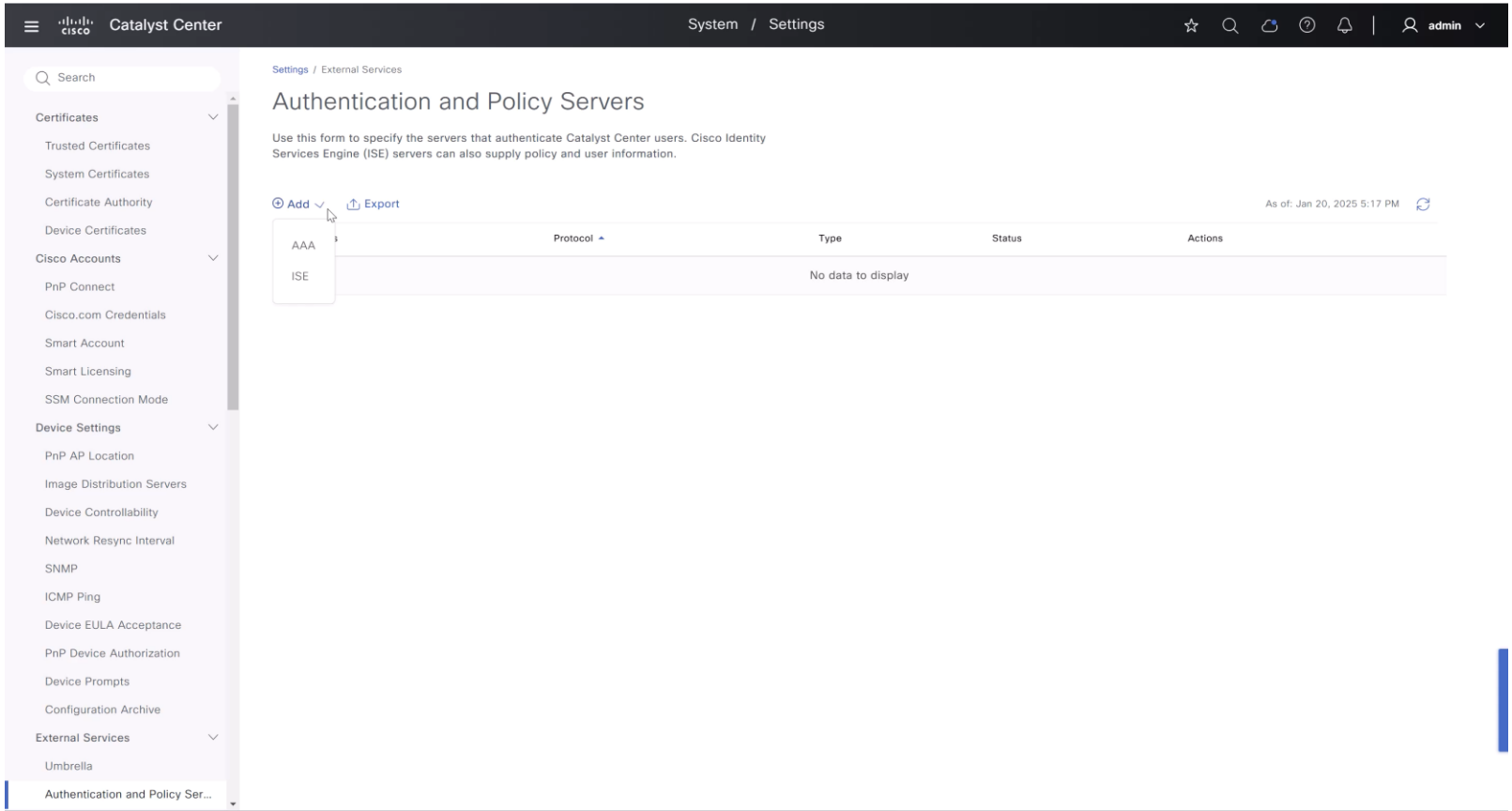
Get ISE Ready – Identity Stores demo



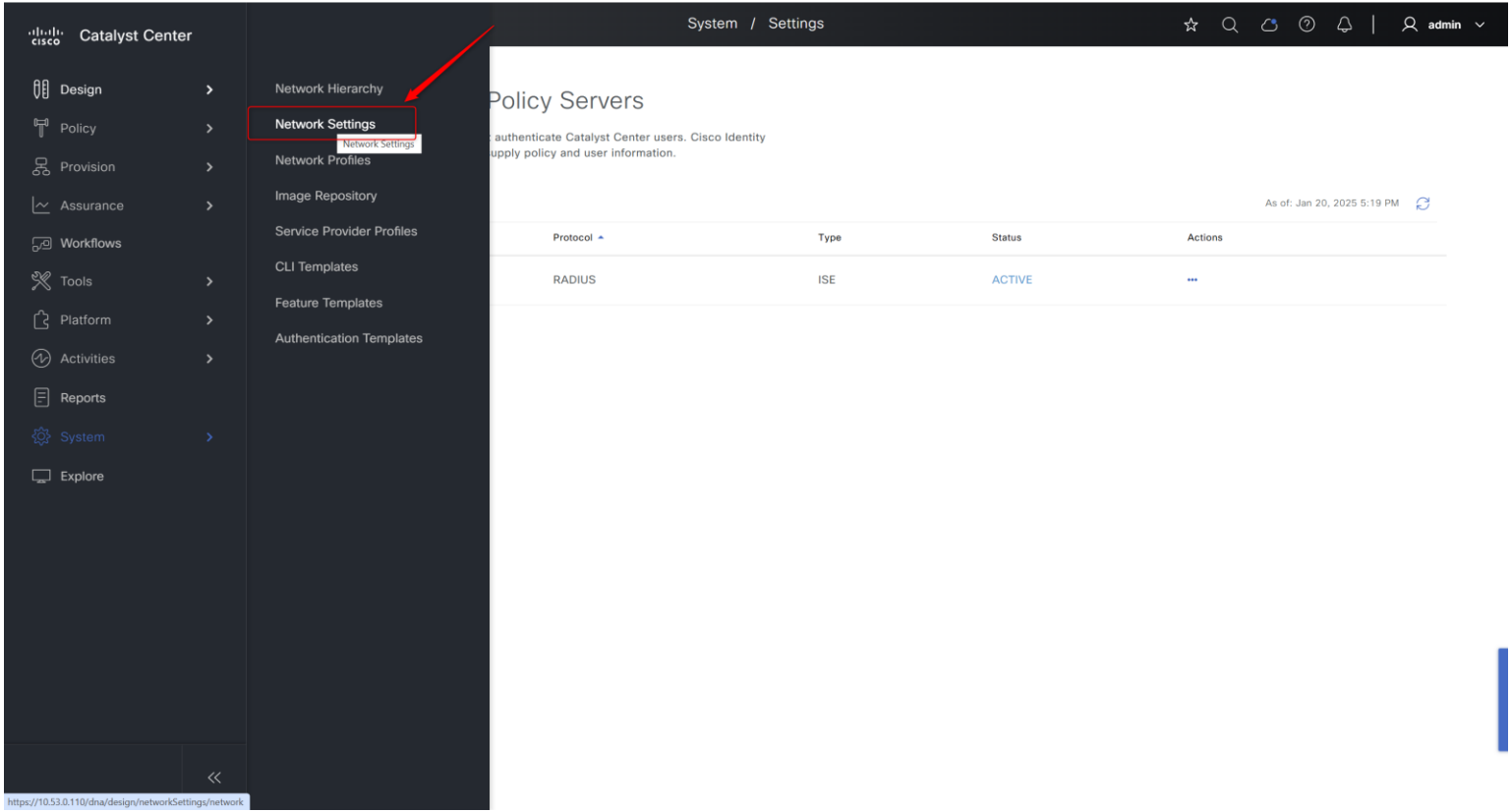
ISE and Catalyst Centre



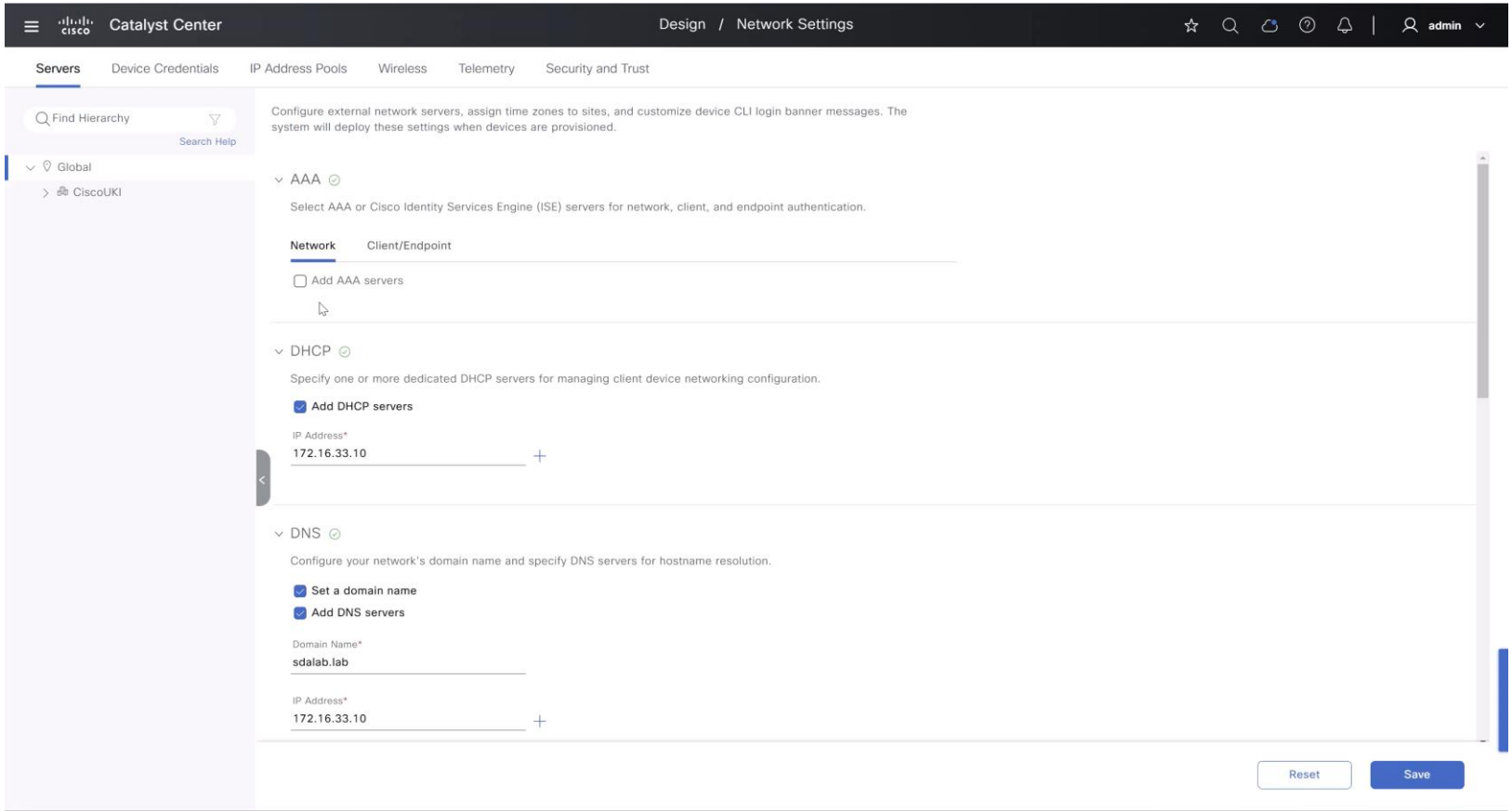
ISE and Catalyst Centre



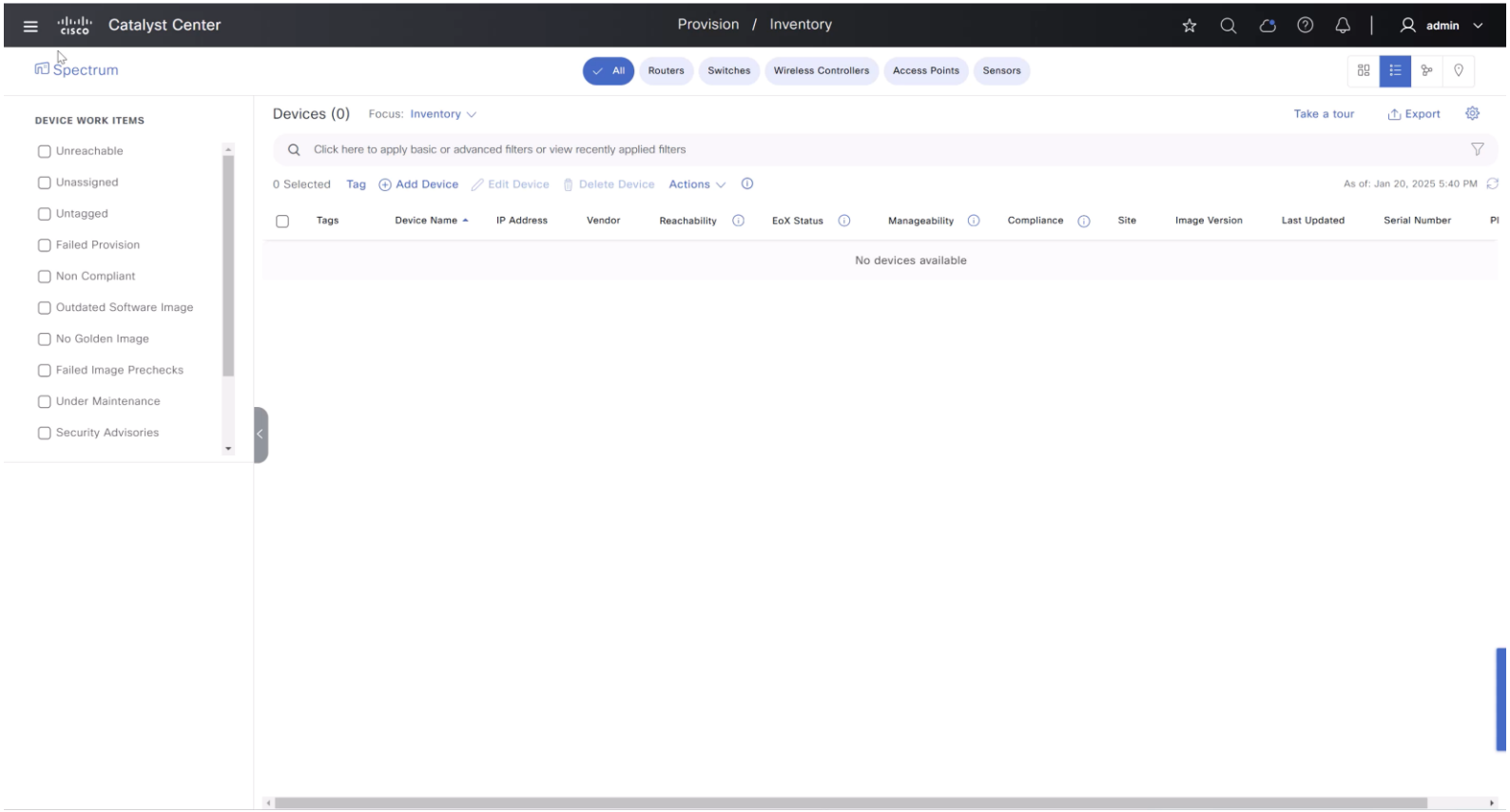
ISE and Catalyst Centre



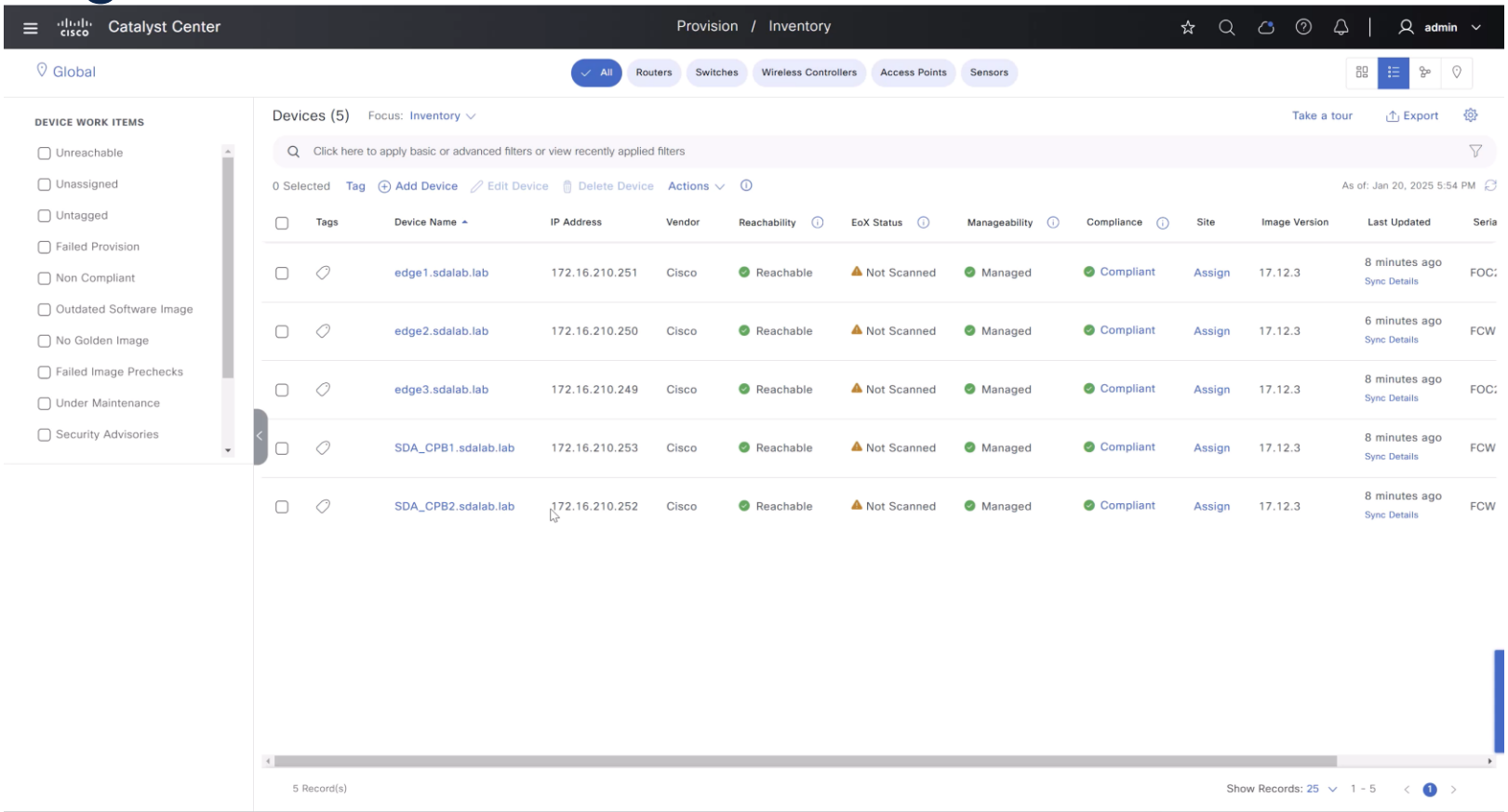
ISE and Catalyst Centre – demo



Discover the network! - demo



Assign to Site - demo



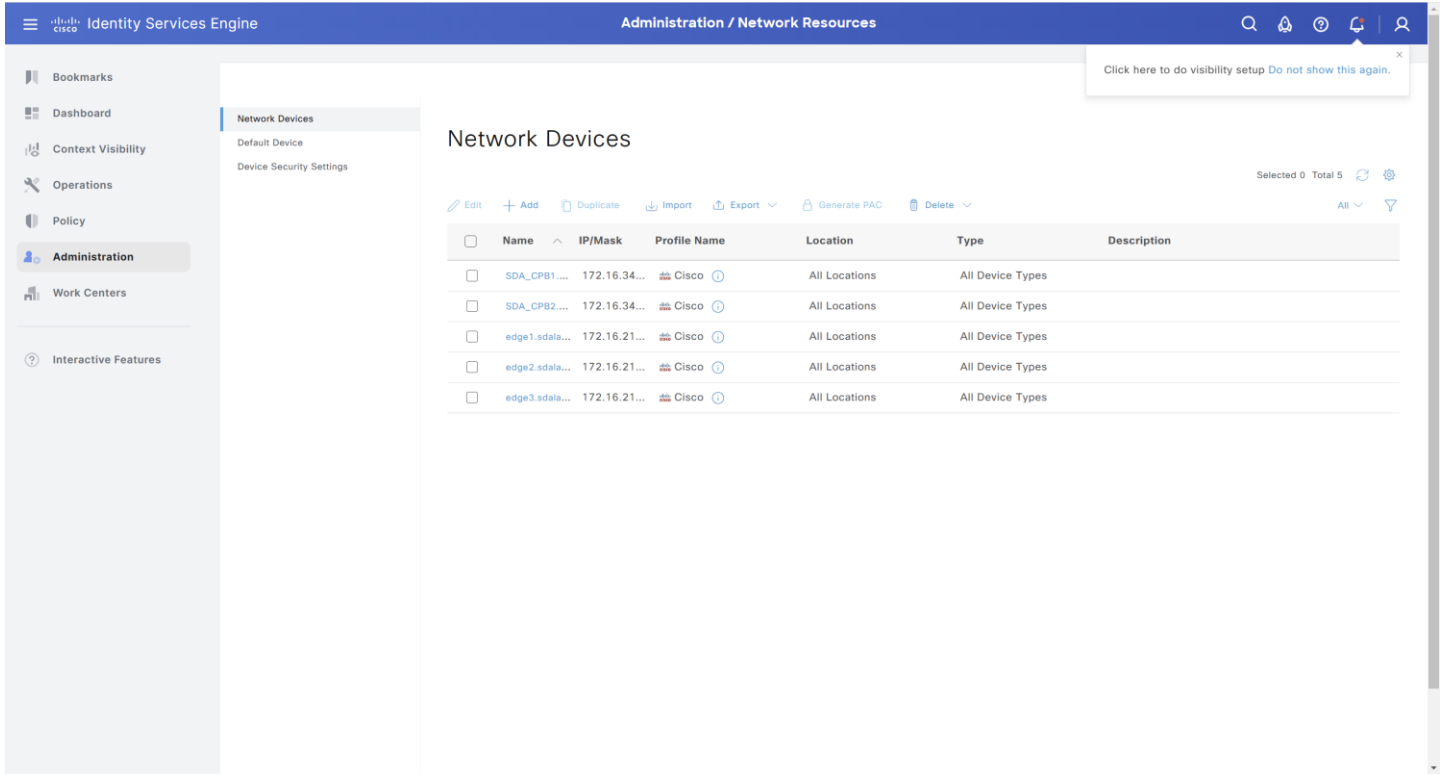
What's just happened? – config applied by Catalyst Centre – there's a lot more!


```
!
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
!
```

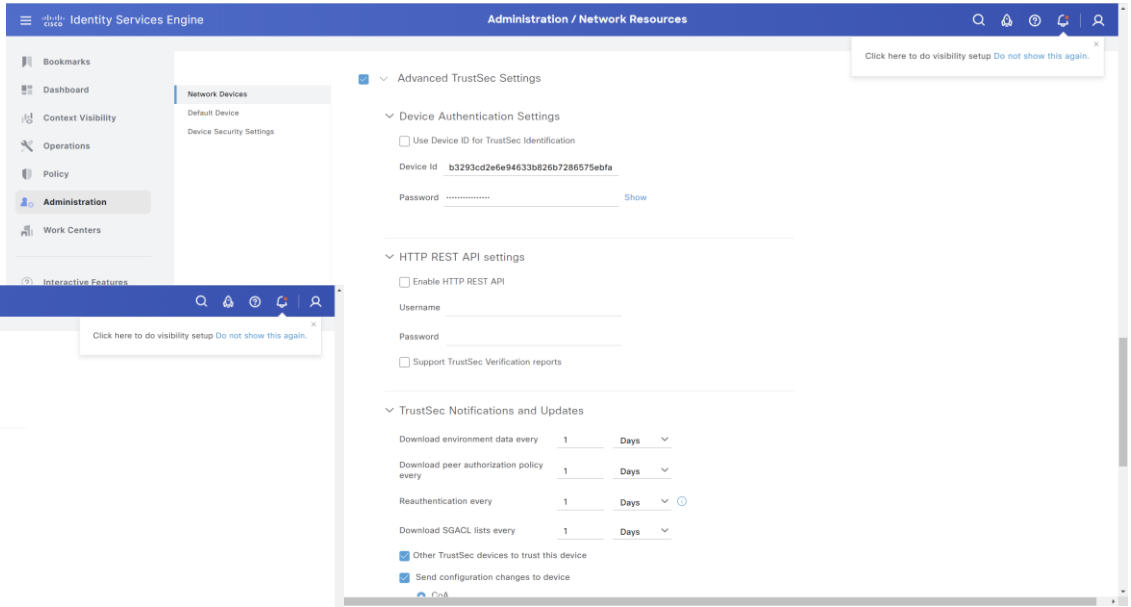
```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
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
!
!
!
```

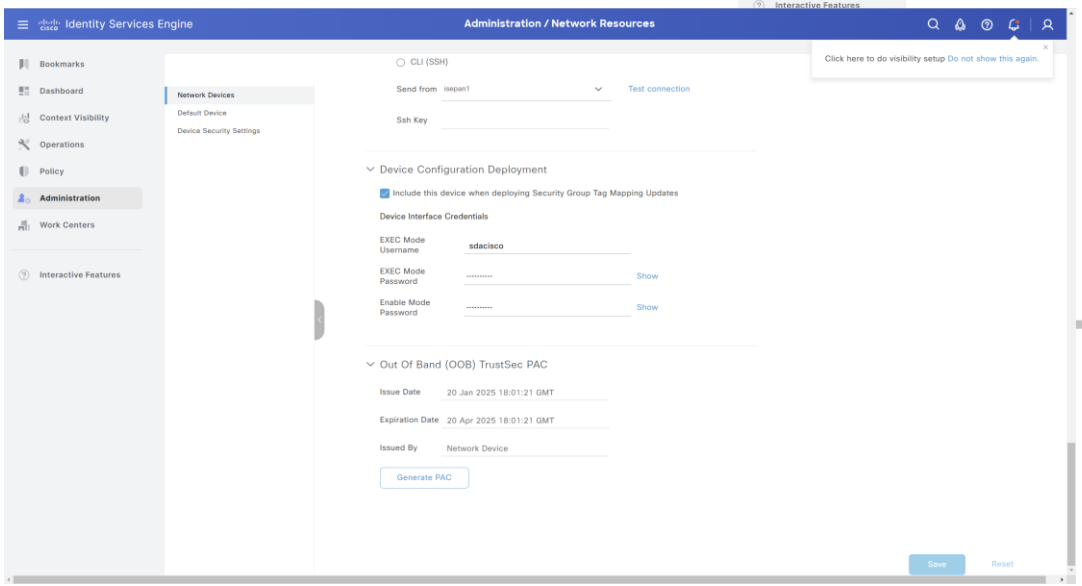
```
!
crypto pki certificate chain DNAC-CA
 certificate ca 409D8A8FF087ACB831BEC9C9B5747A83BB9E23AB nvram:CiscoDNACent#23ABCA.cer
crypto pki certificate chain sdn-network-infra-iwan
 certificate 6B0F468D14A62B8CB0E836C0DA095D1E27110AB0 nvram:sdn-network-#AB0.cer
 certificate ca 190CF73F12CEDE03028E0765E0C1BB0618B5DB2B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

It all gets added to ISE

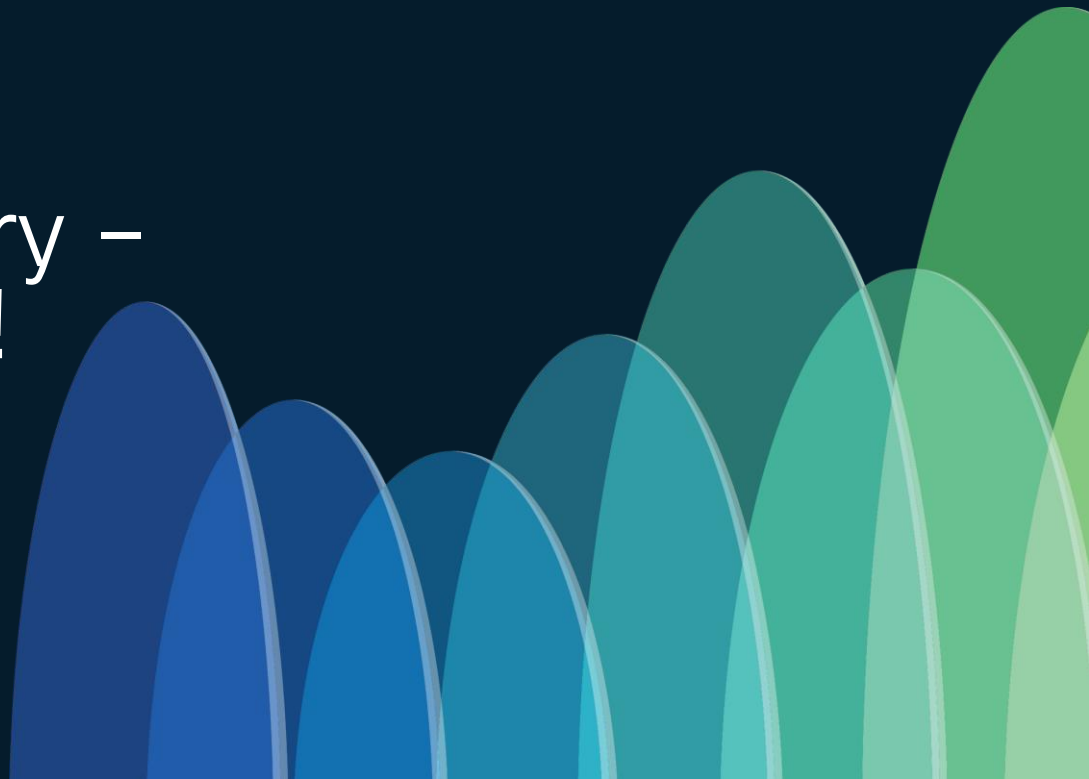


With Trustsec – Security Group





Catalyst Centre Template Delivery – making it simple!

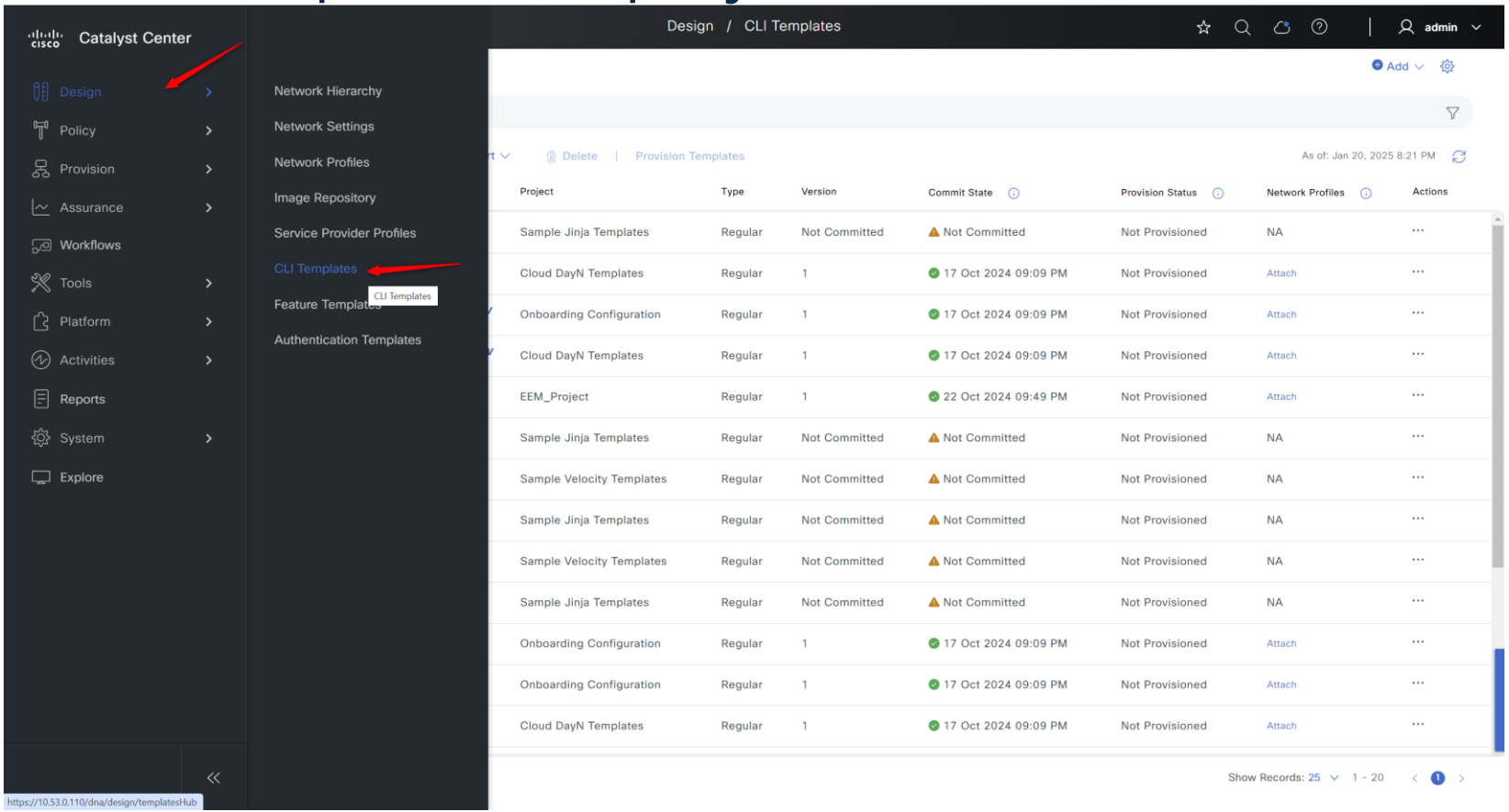


cisco Live!

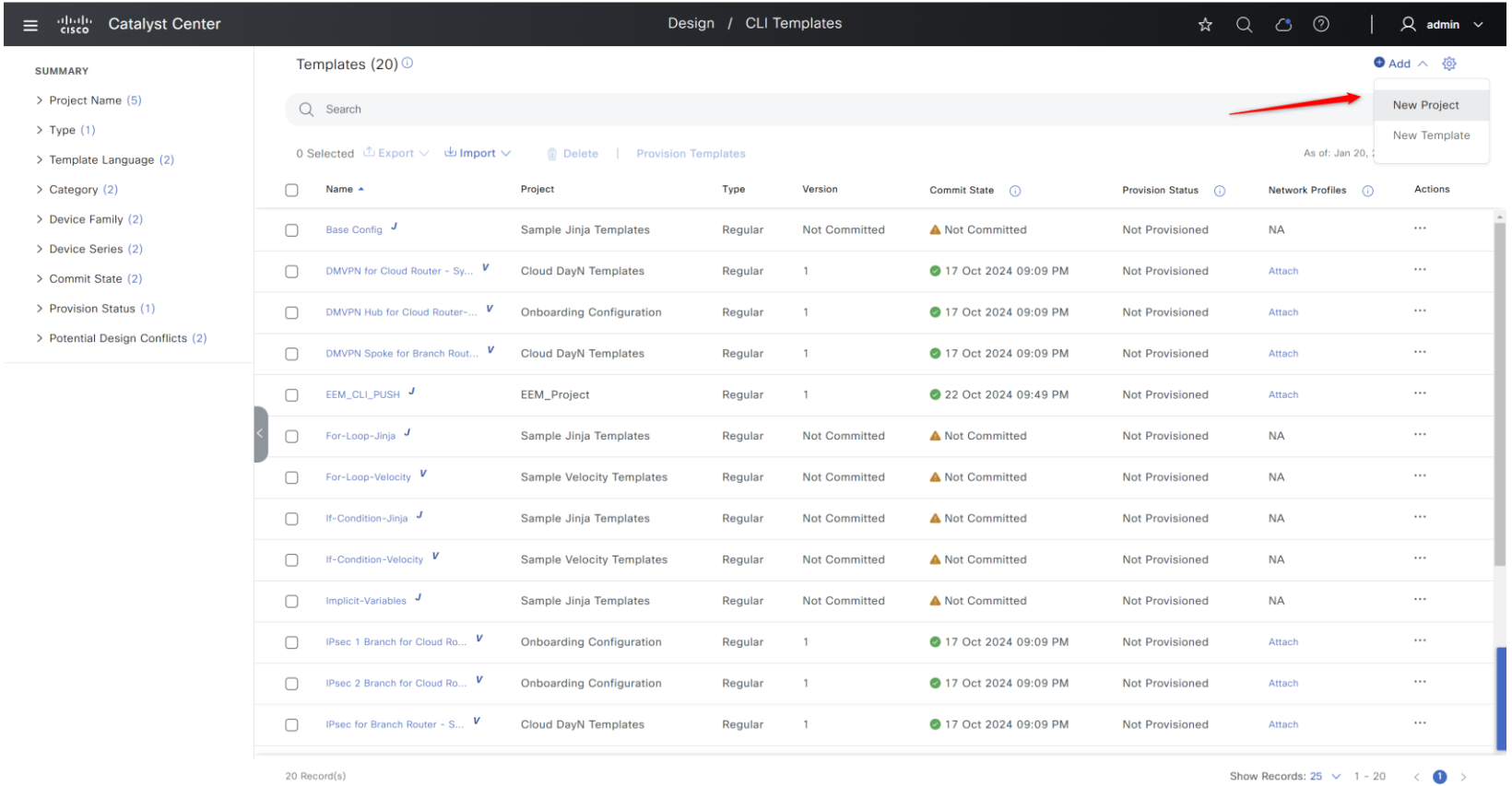
How to deliver config – reliably!

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

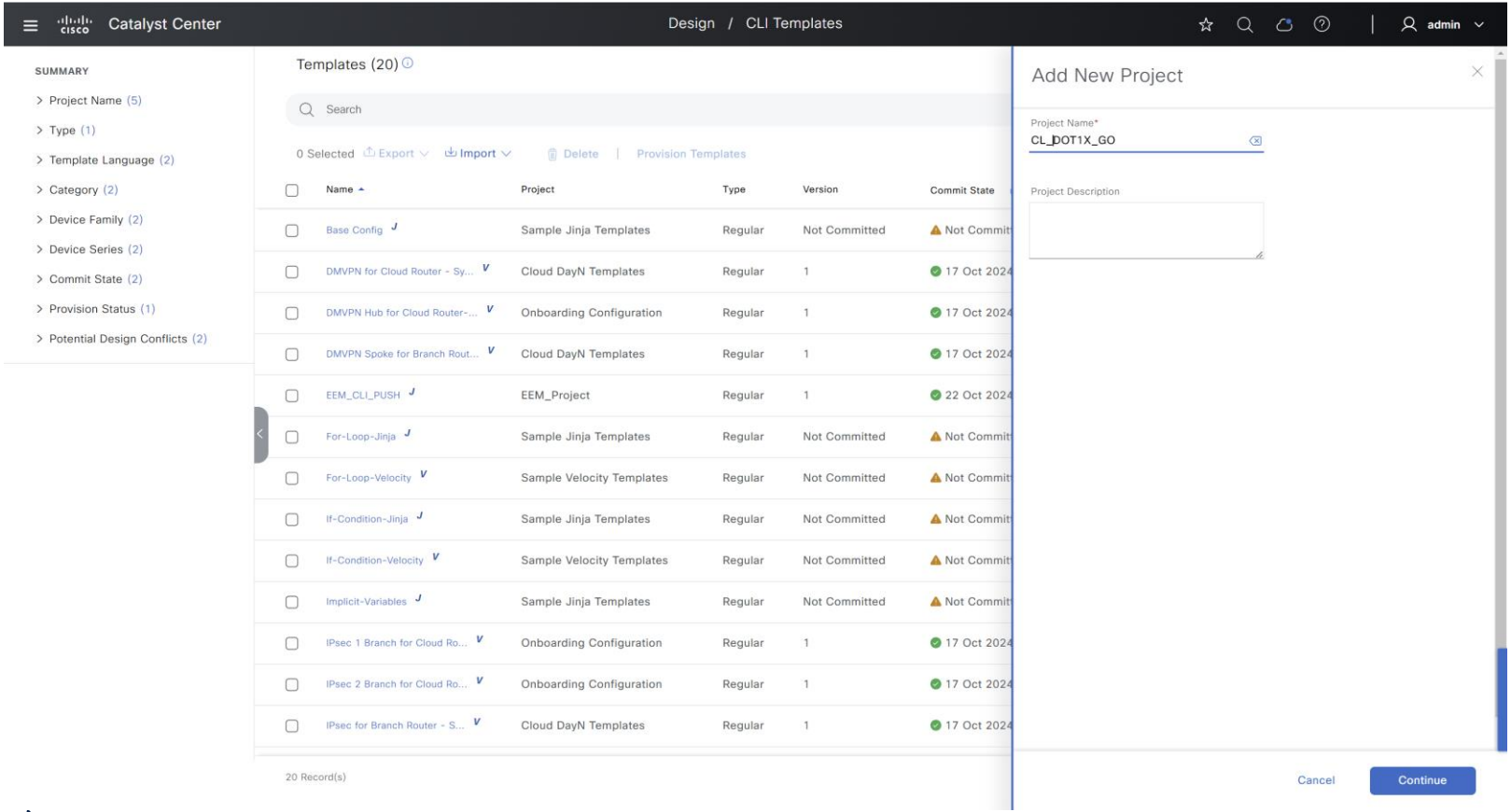
Create a template and project



Create a template and project



Create a template and project



The really useful bit! – all the template.


```
! 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 bpdufilter 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 nonegotiate
     switchport voice vlan 202
     spanning-tree portfast
     spanning-tree bpdufilter 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 ?

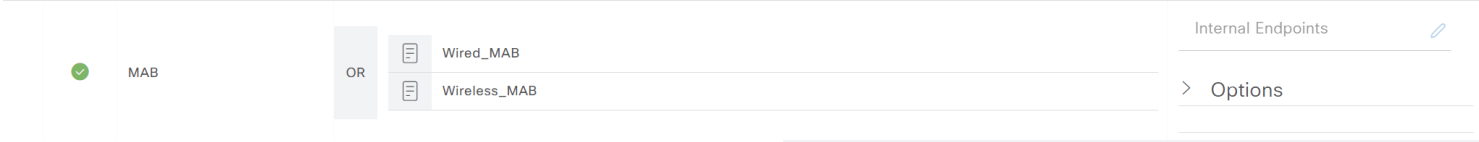
In Monitor or Low Impact mode –

ISE will discover and profile your endpoints!!

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

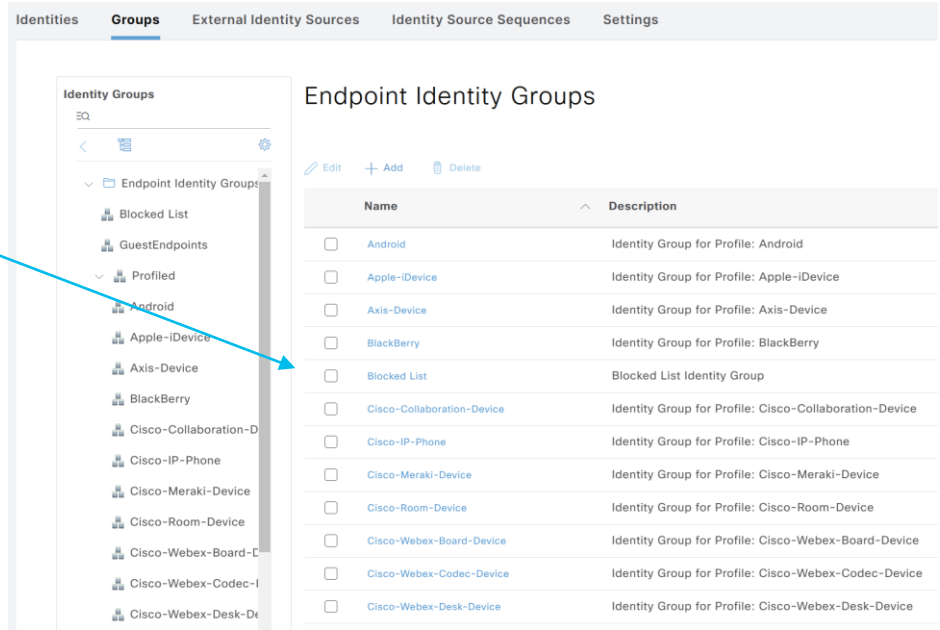
But what if an endpoint cannot logon?!

MAB – MAC Authentication Bypass

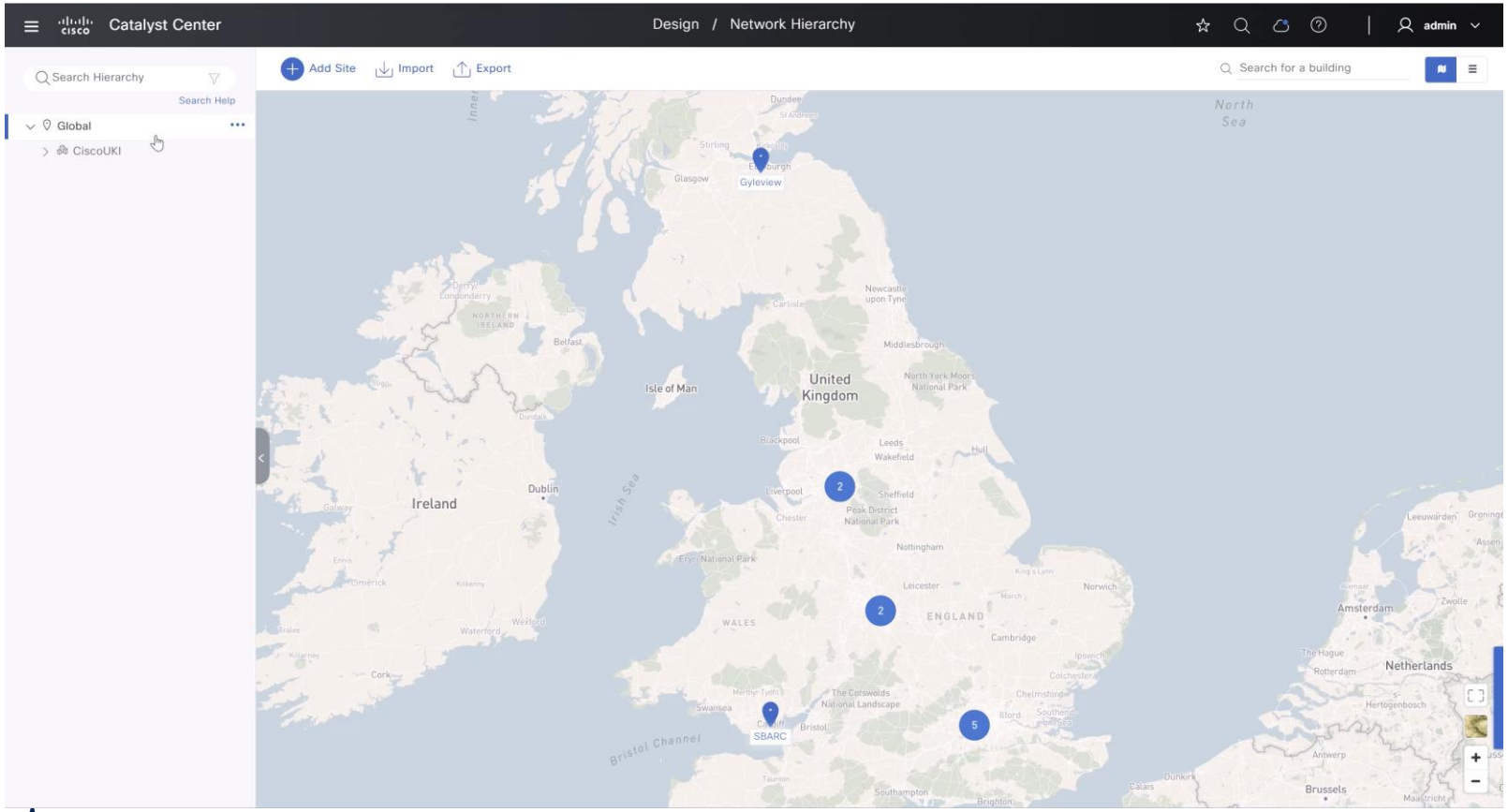


Endpoints that used MAB stored in internal ISE DB – discovered by ISE during Low impact/Monitor

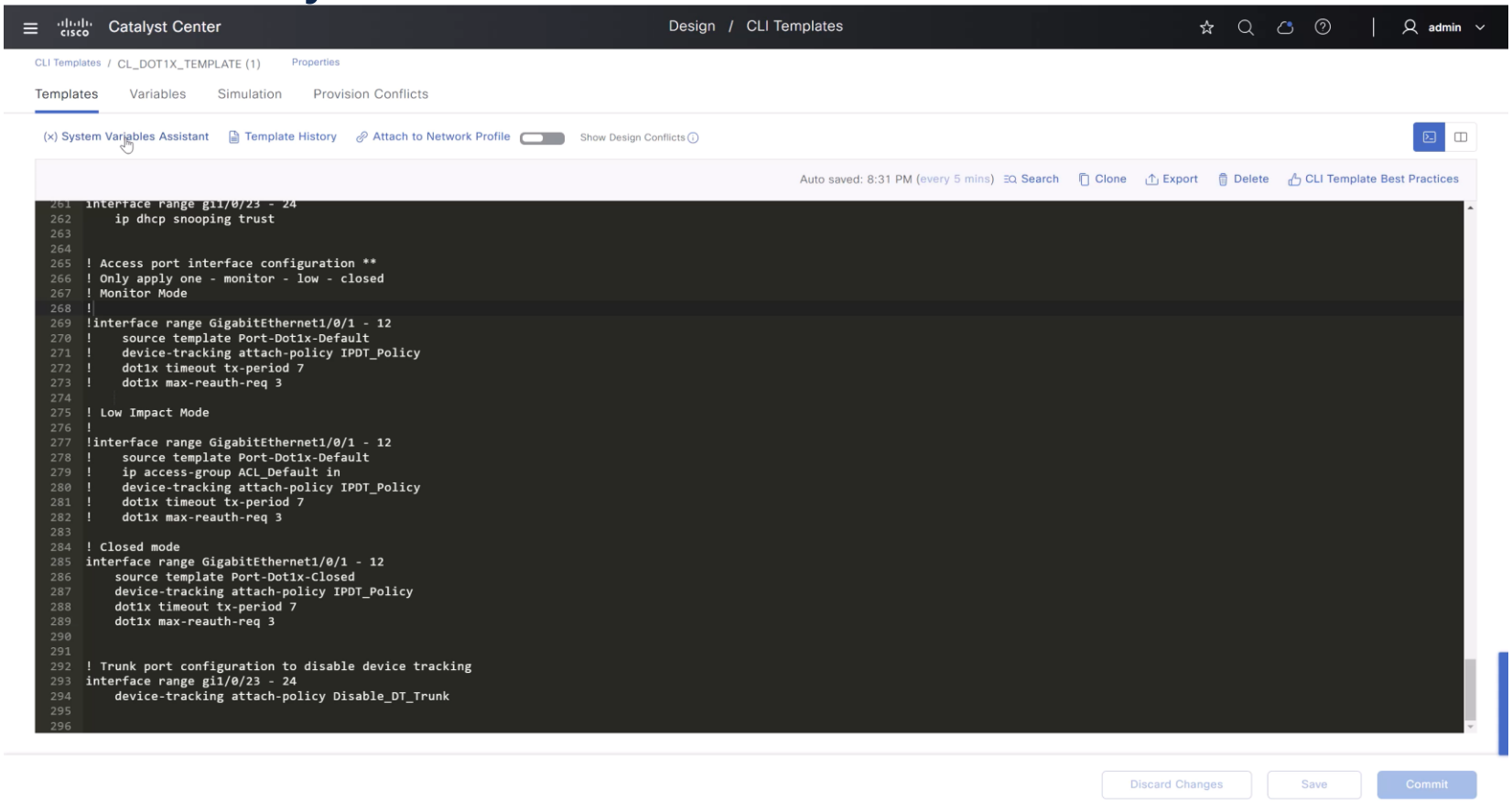
AuthZ rules created for non-auth endpoints!



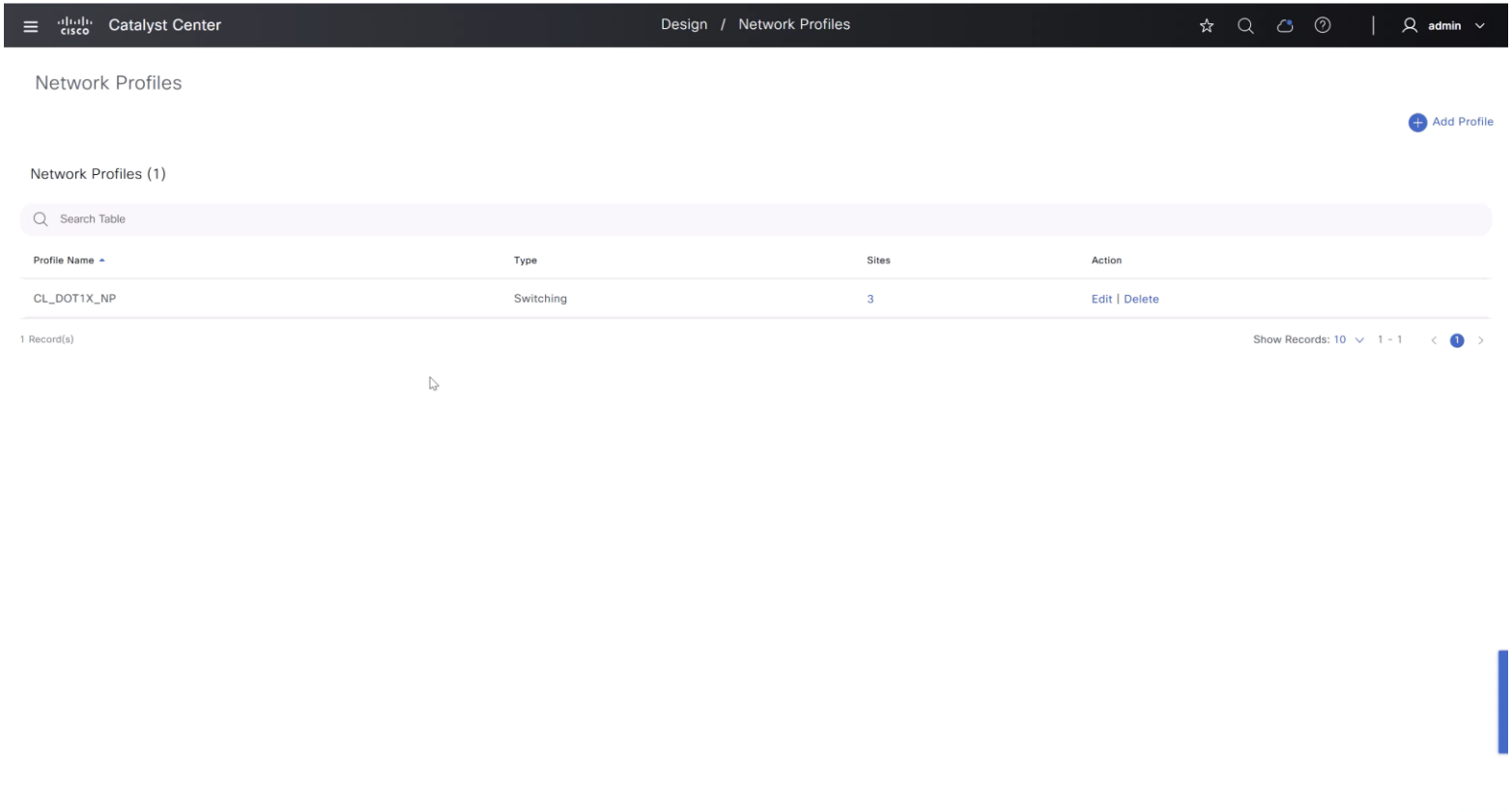
CLI via Catalyst Centre – in action demo



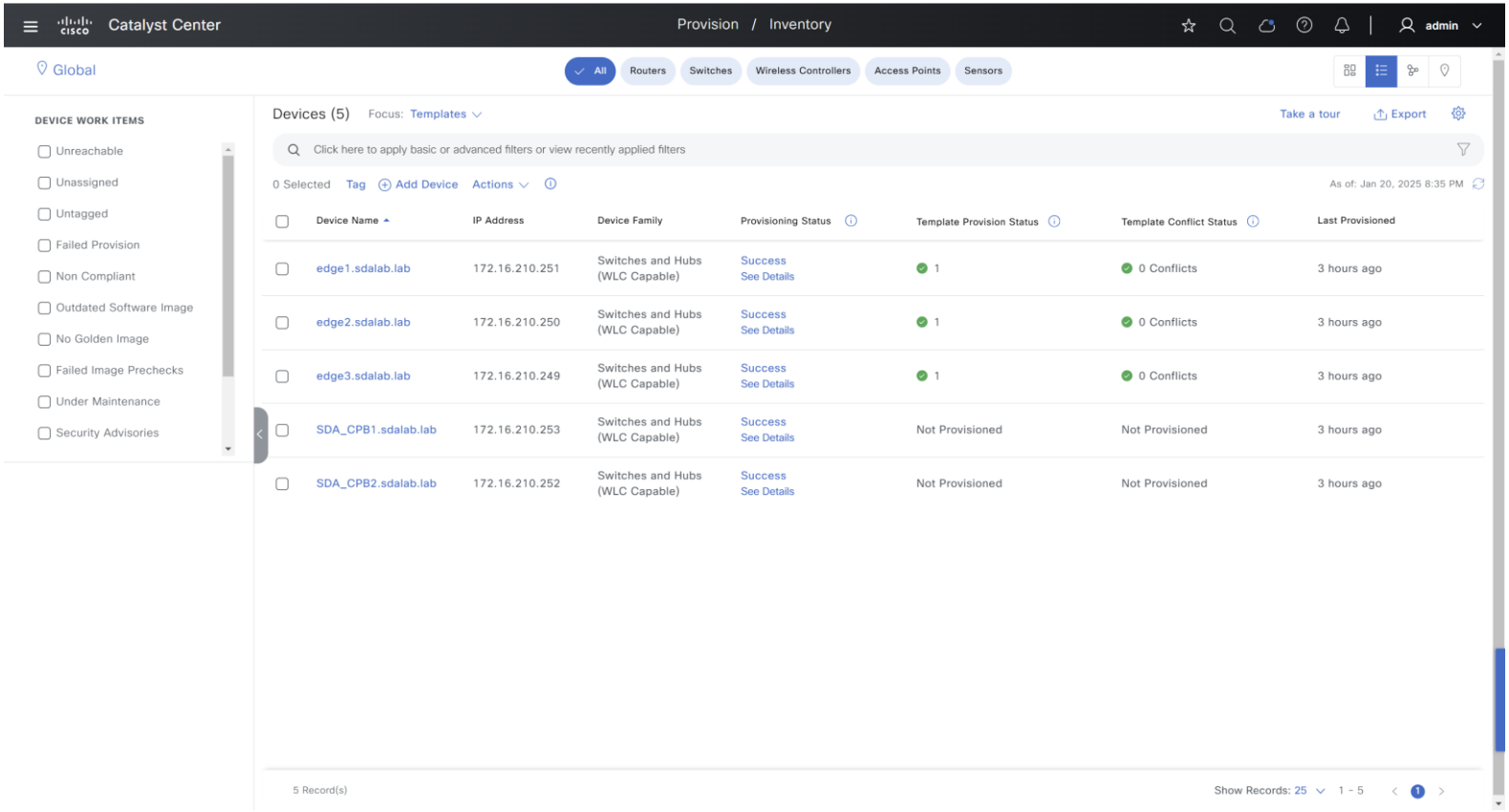
CLI via Catalyst Centre – in action demo



CLI via Catalyst Centre – in action demo



CLI via Catalyst Centre – Inventory



Port after template

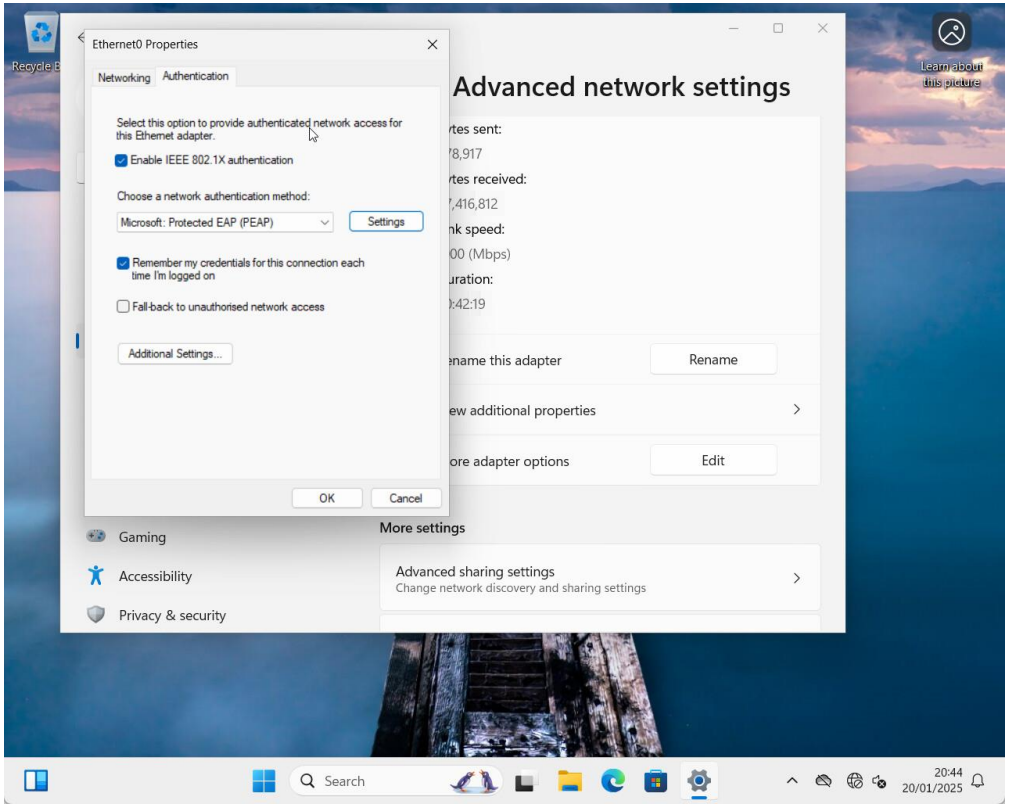

```
interface GigabitEthernet1/0/1
 switchport access vlan 208
 switchport mode access
 device-tracking attach-policy IPDT_Policy
 ip flow monitor dnacmonitor input
 ip flow monitor dnacmonitor_dns input
 ip flow monitor dnacmonitor output
 ip flow monitor dnacmonitor_dns output
 ipv6 flow monitor dnacmonitor_v6 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

```
edge1#sho derived-config interface gi1/0/1
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
```

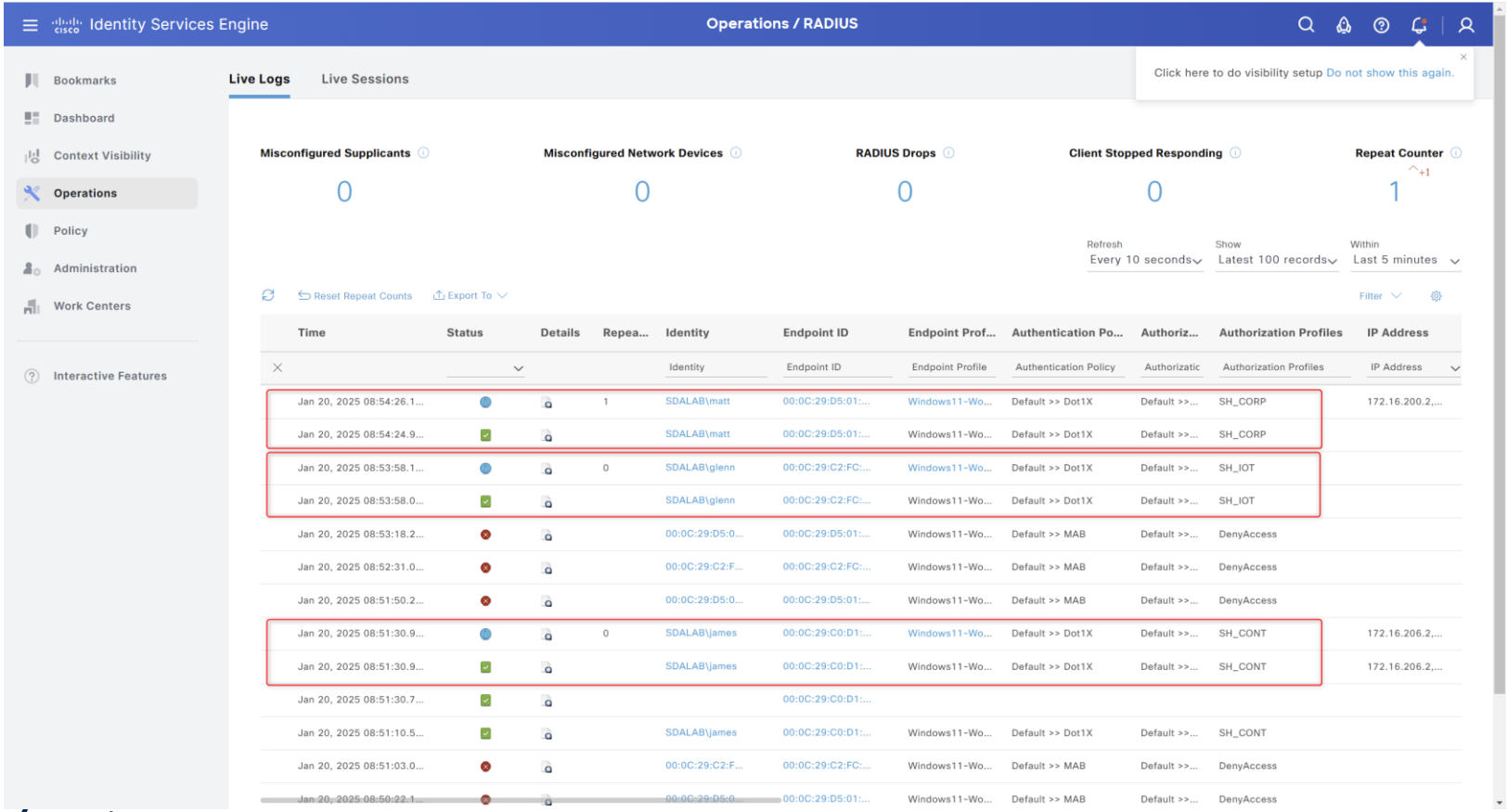
That’s useful!

Enable wired auto on endpoints – windows example

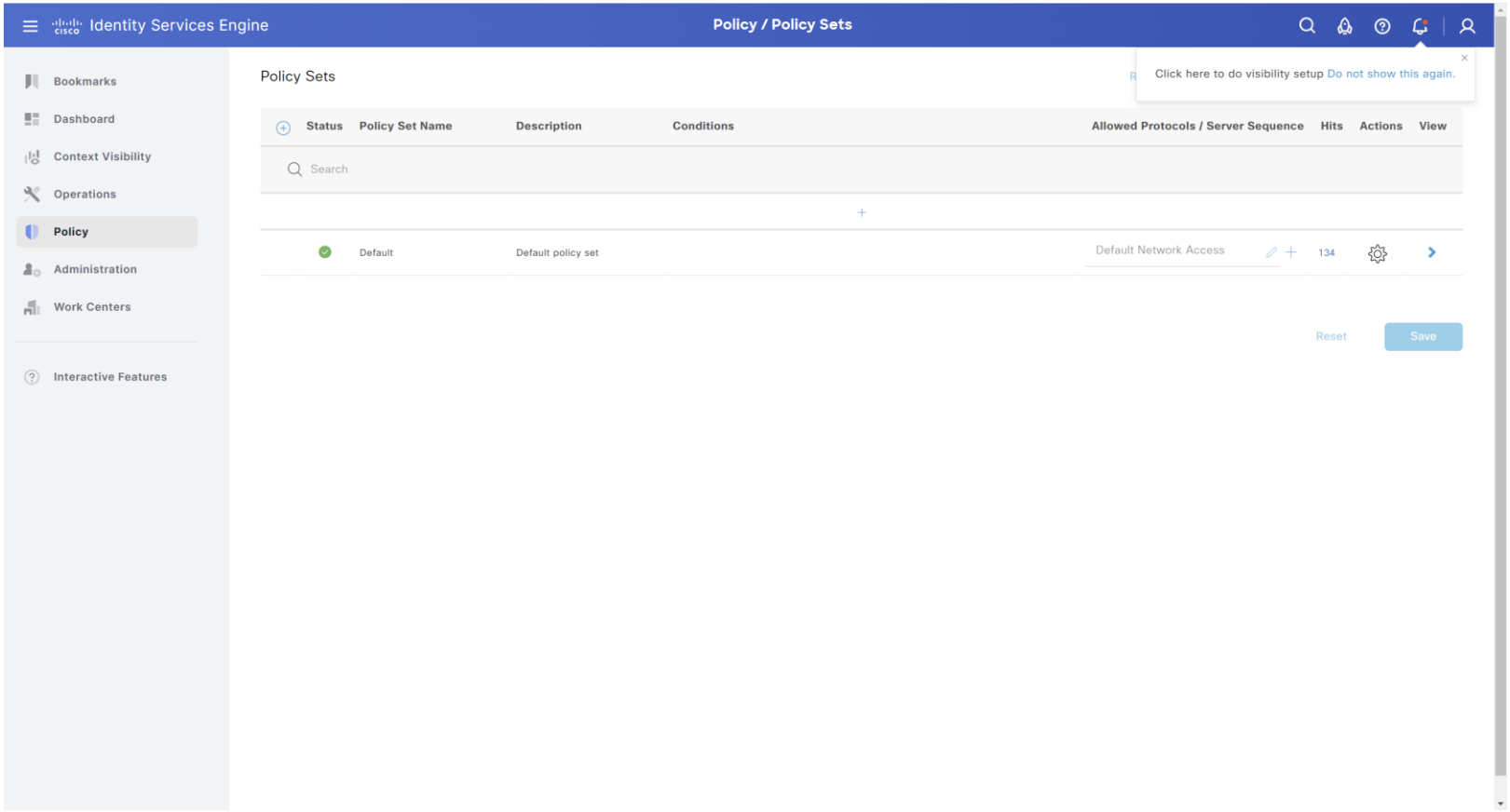


Use Group Policy, MDM, Intune

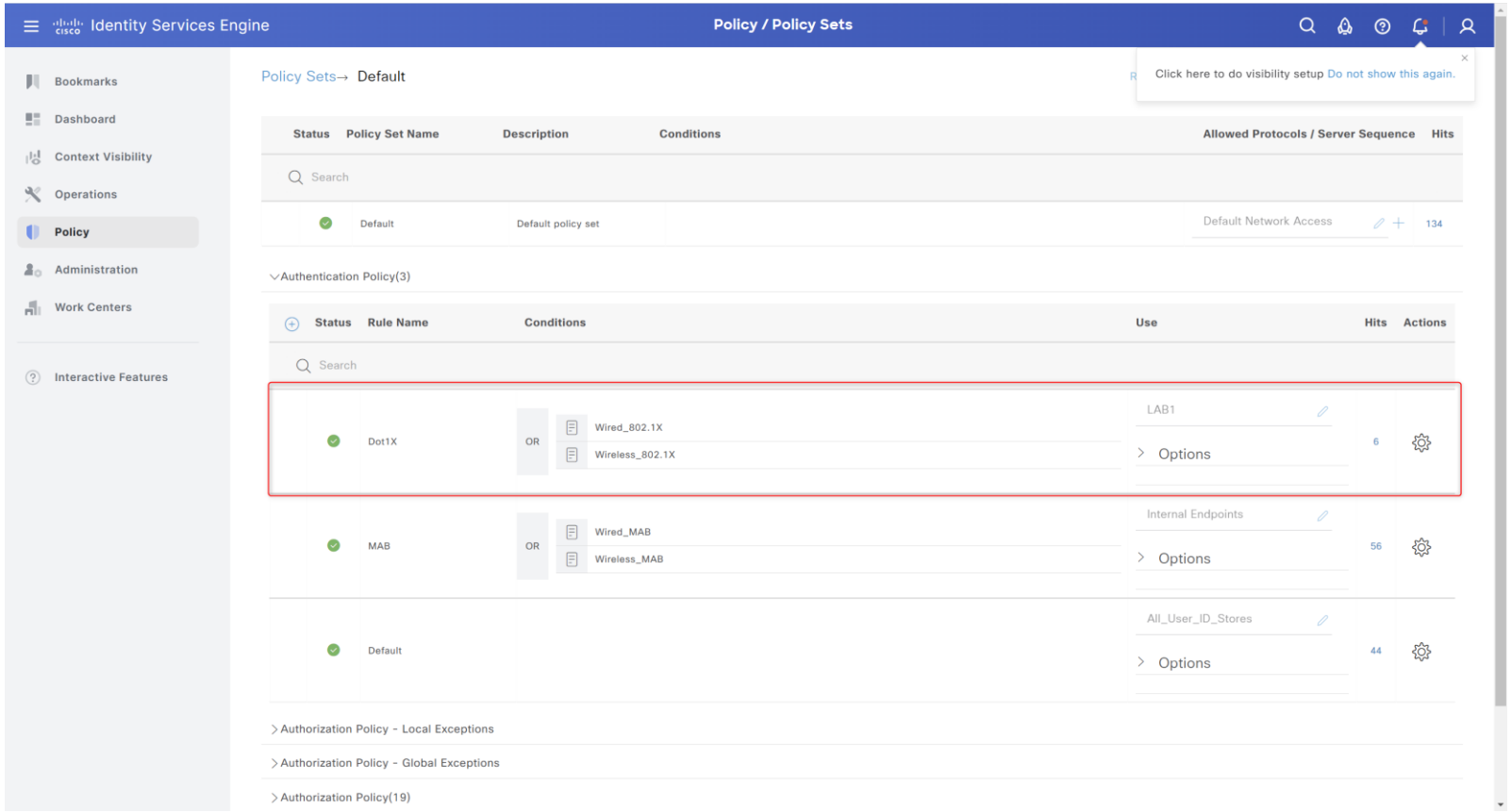
Check devices on ISE



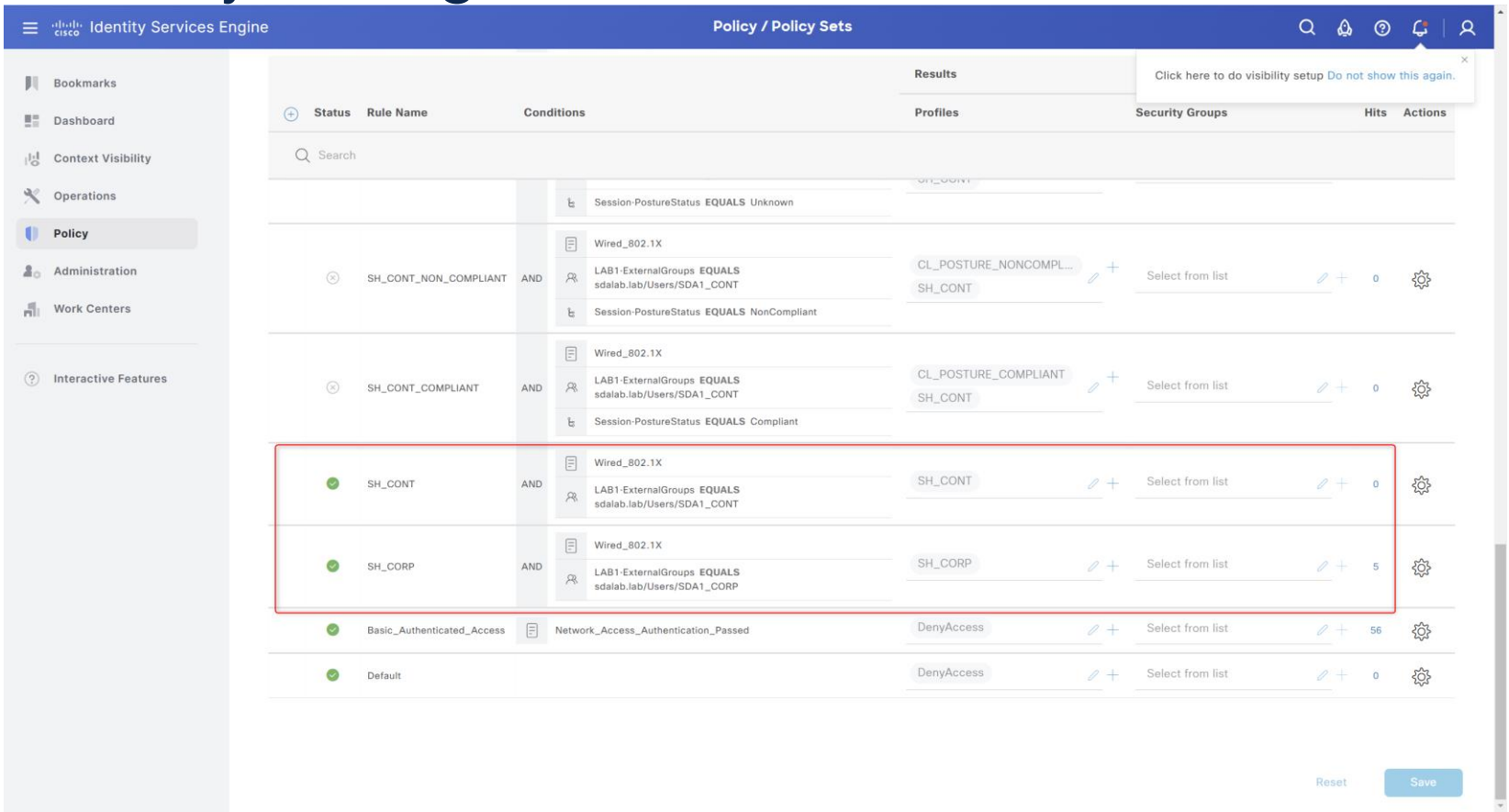
ISE Policy Configuration – Policy Sets



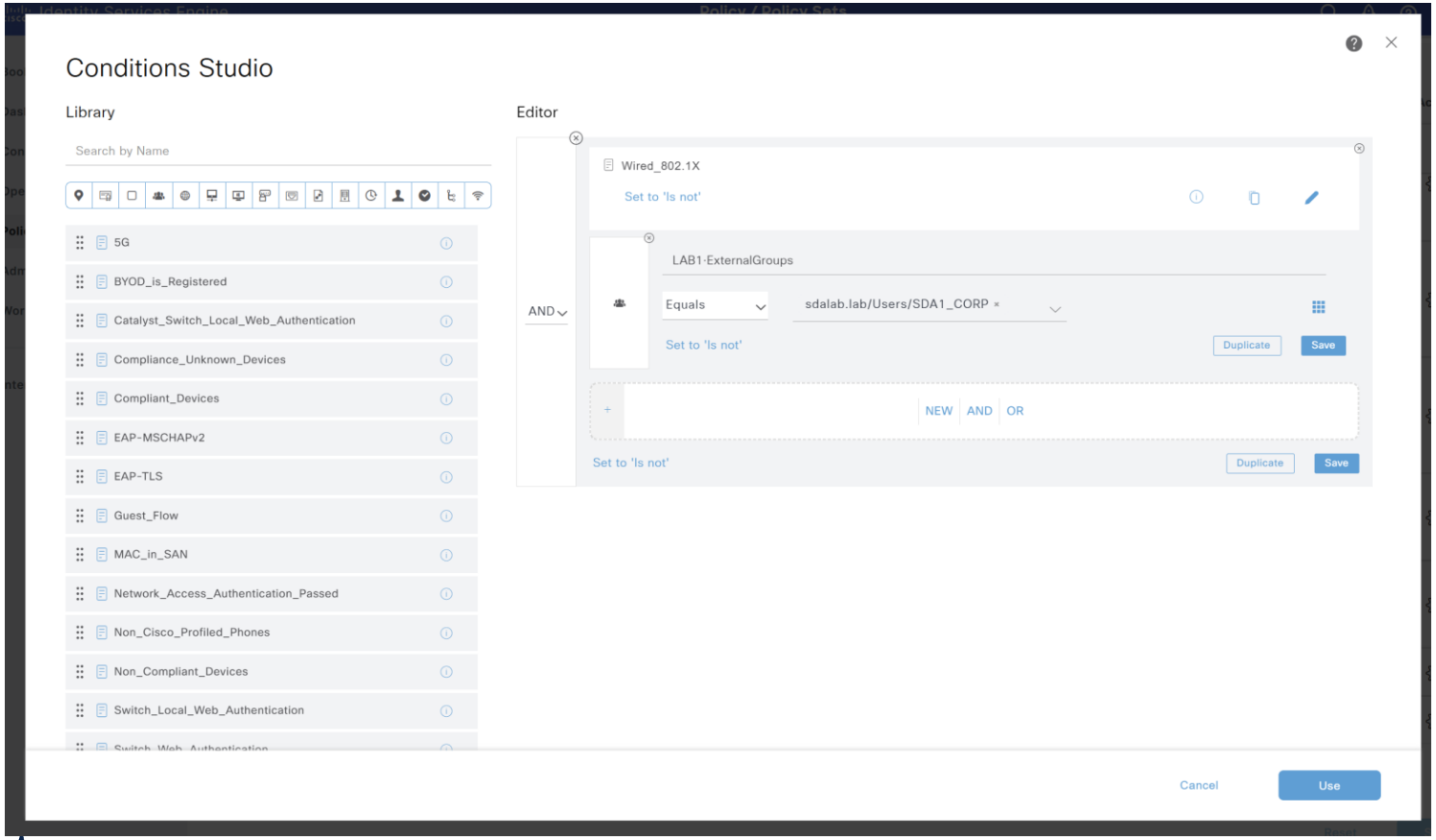
ISE Policy Configuration – Authentication



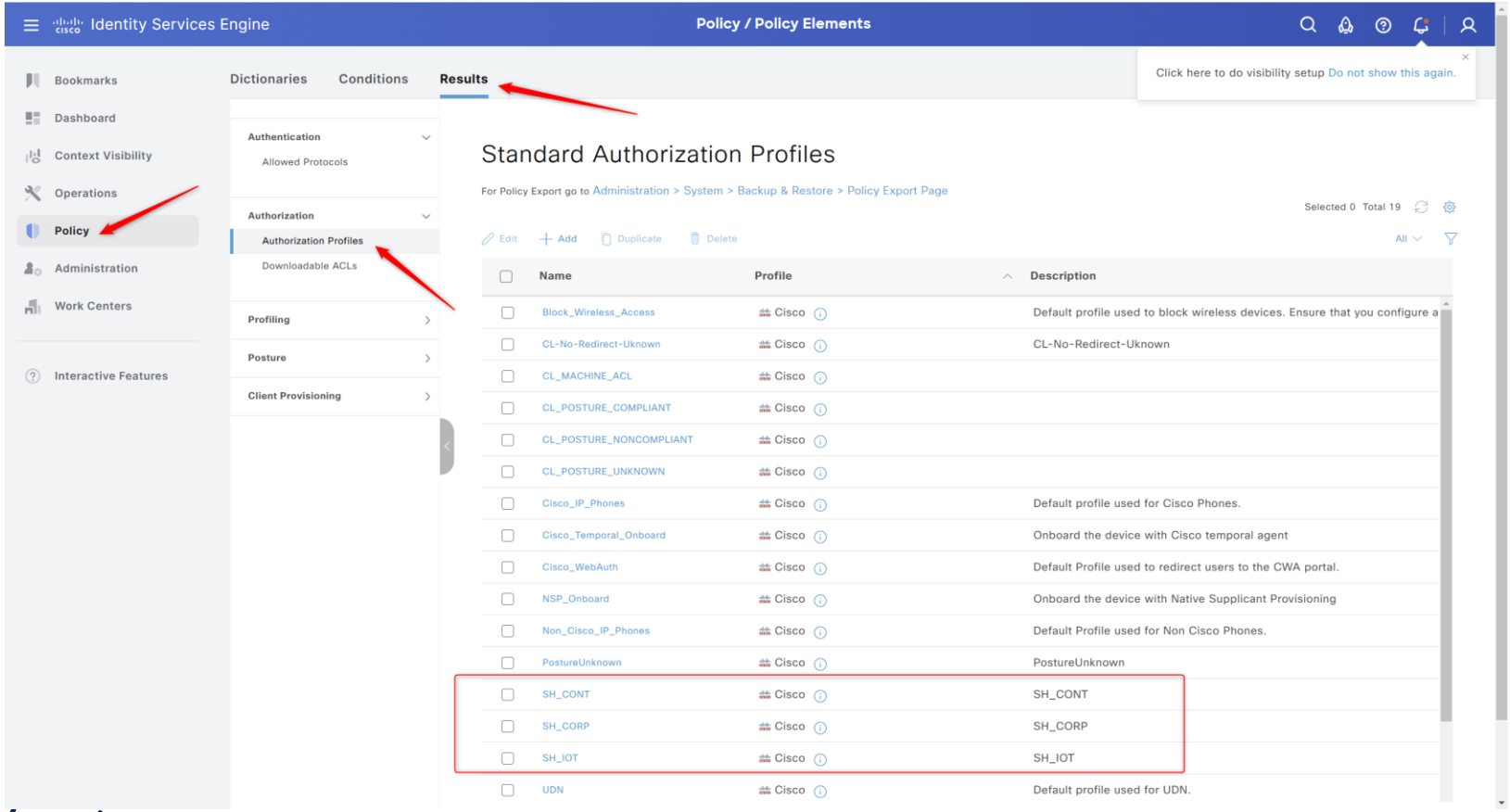
ISE Policy Configuration – Authorization



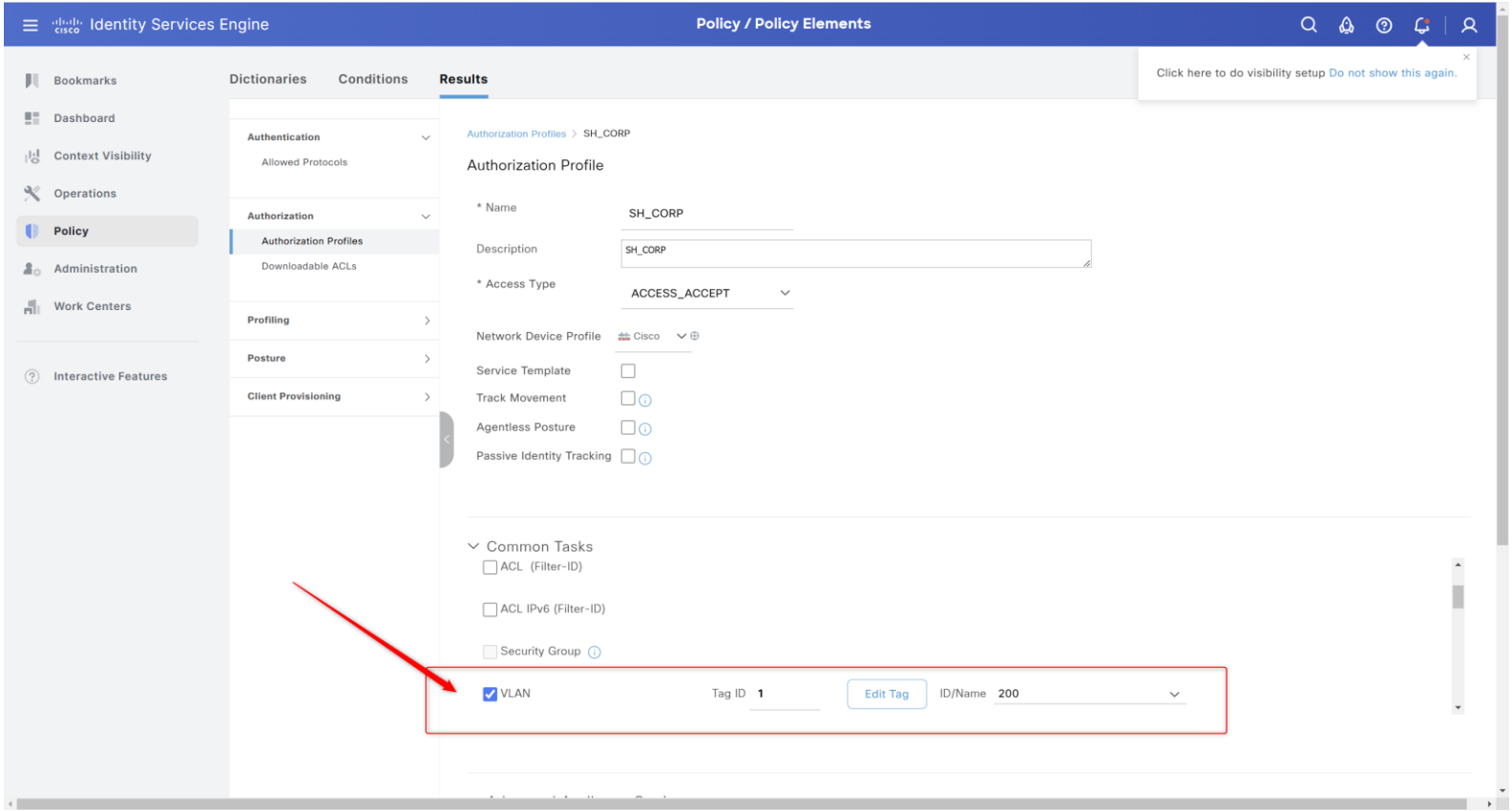
ISE Policy Configuration – Conditions Studio



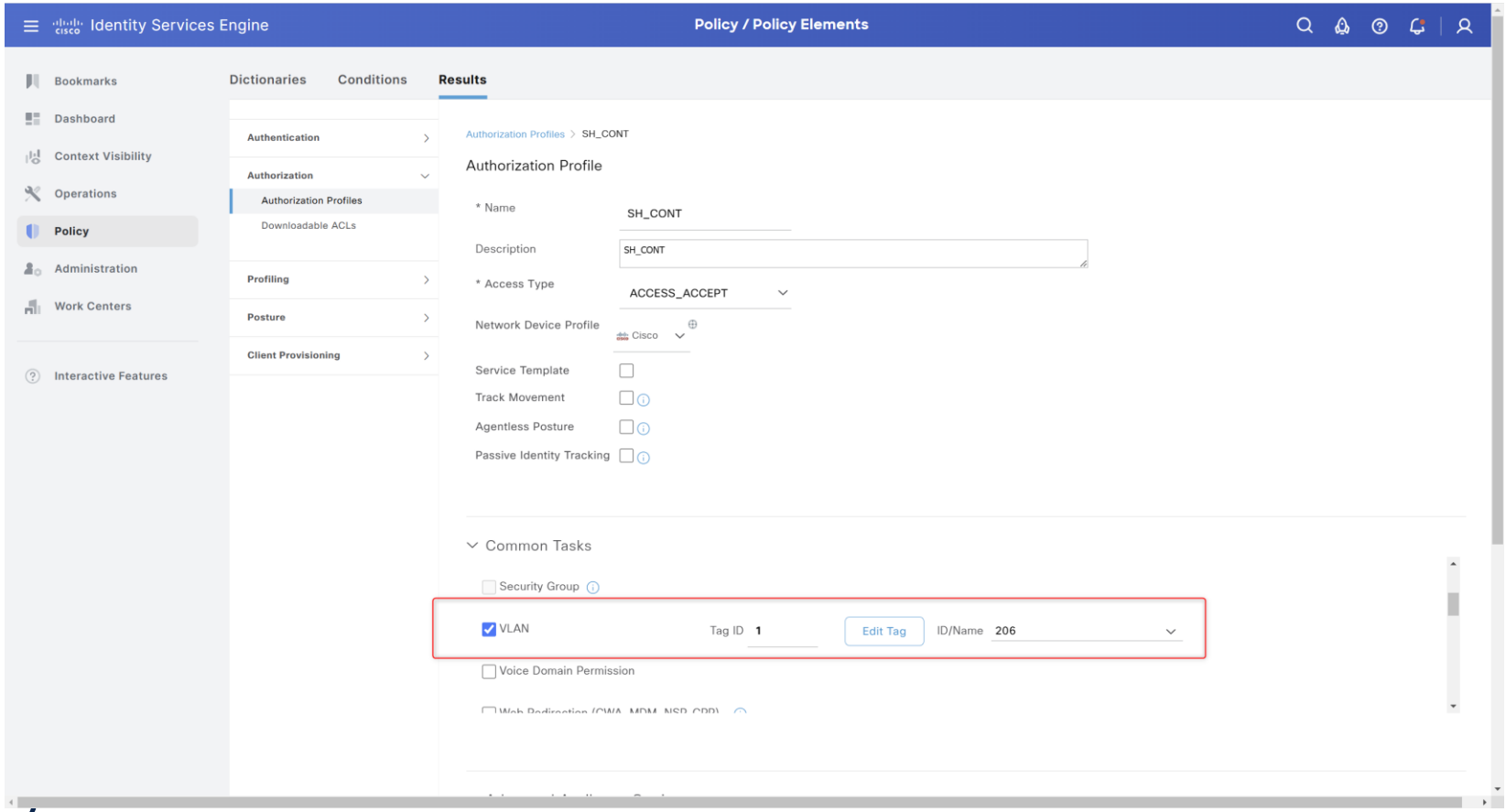
ISE Policy Configuration – Policy Results



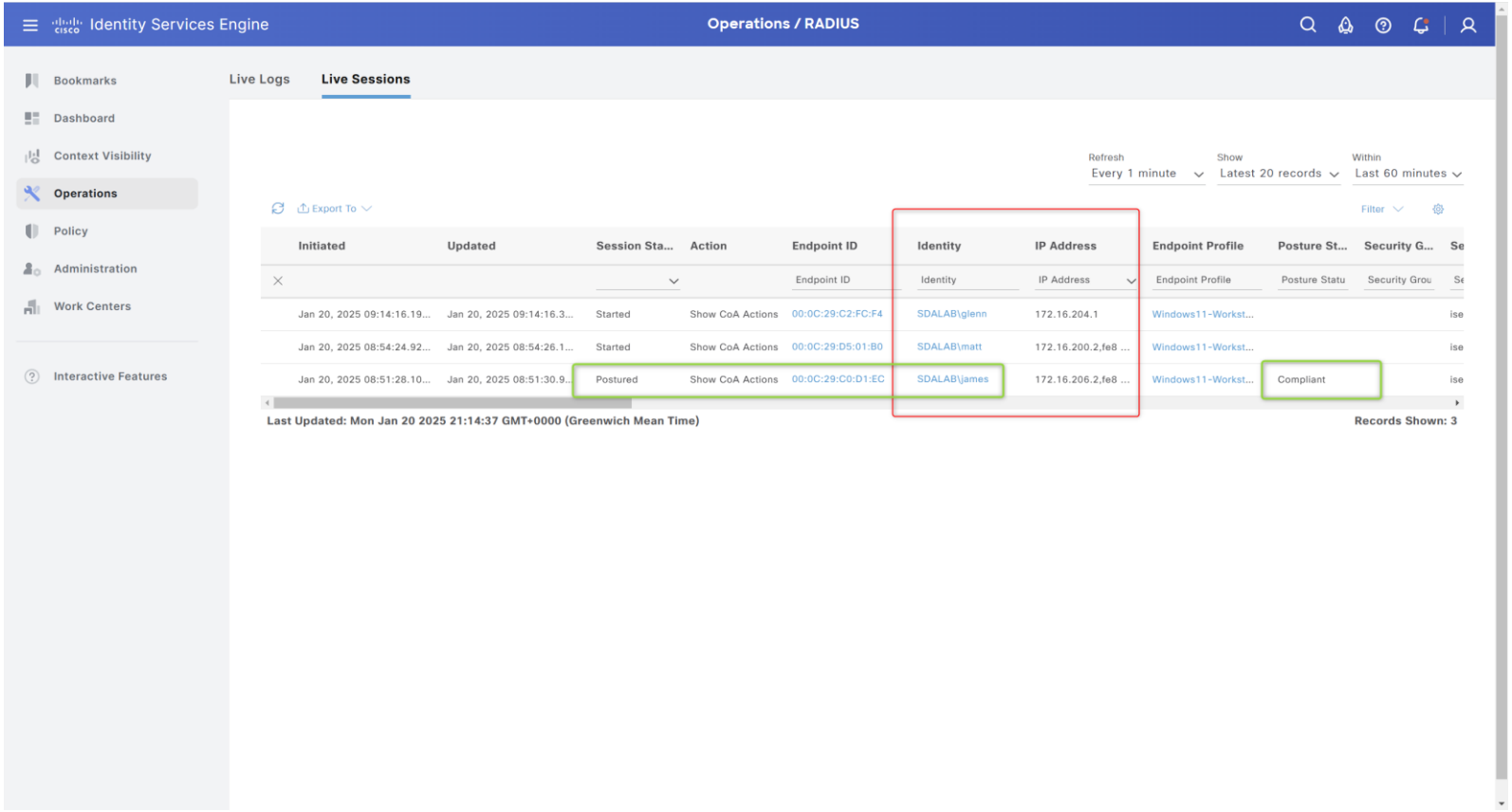
ISE Policy Configuration – Policy Results



ISE Policy Configuration – Policy Results



ISE Policy Configuration – Endpoints Authenticated



Cisco TrustSec

cisco Live!

Absolutely look at this!

Identifying Users for Group-Based Policies

Simple ways to add access control & protect new things

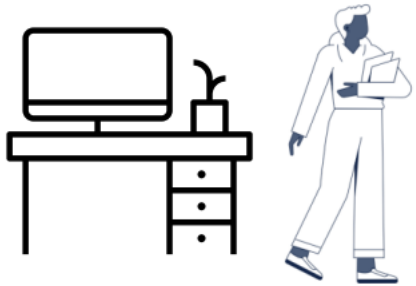
Reduce IP ACL complexity.
Reduce and simplify FW rules.
Meet compliance goals easier.
Simple segregation protection.

Reduce Risk & Represent threat state or vulnerable devices

- Use groups to protect device types that you cannot patch
- Restrict lateral movement
- Protect vulnerable systems
- Use Groups to represent suspicious devices & handle appropriately

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 ....

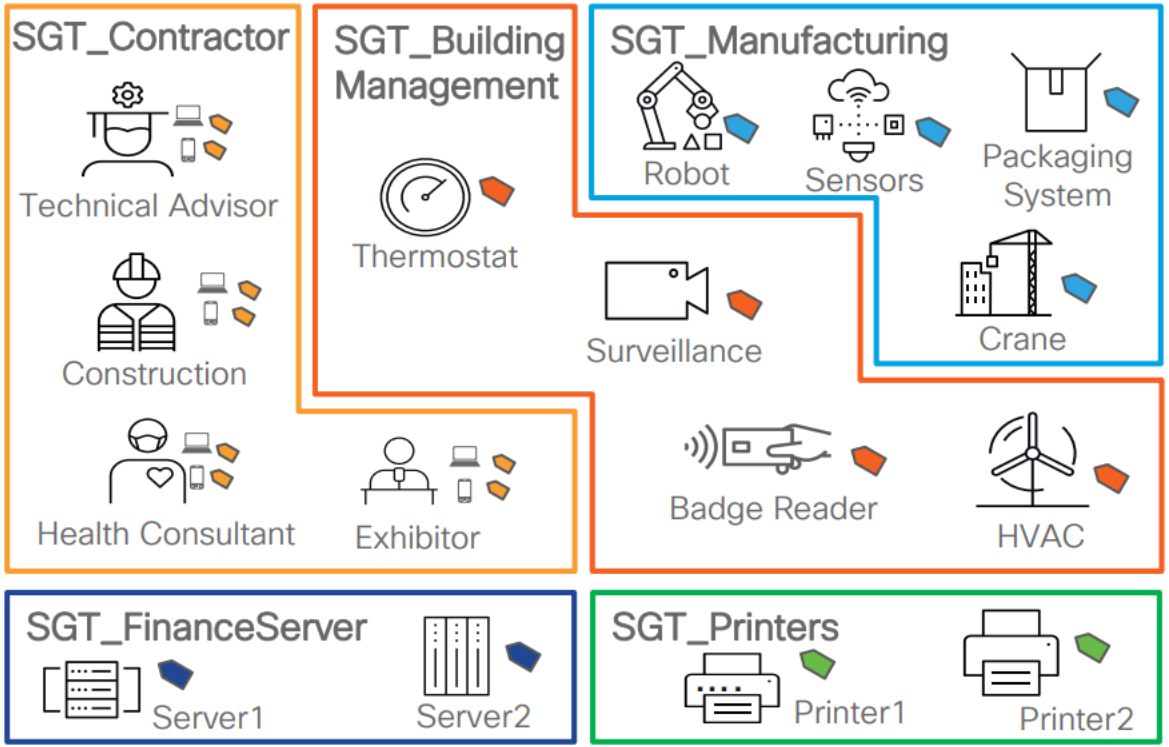
Security Policy Tied to Infra

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

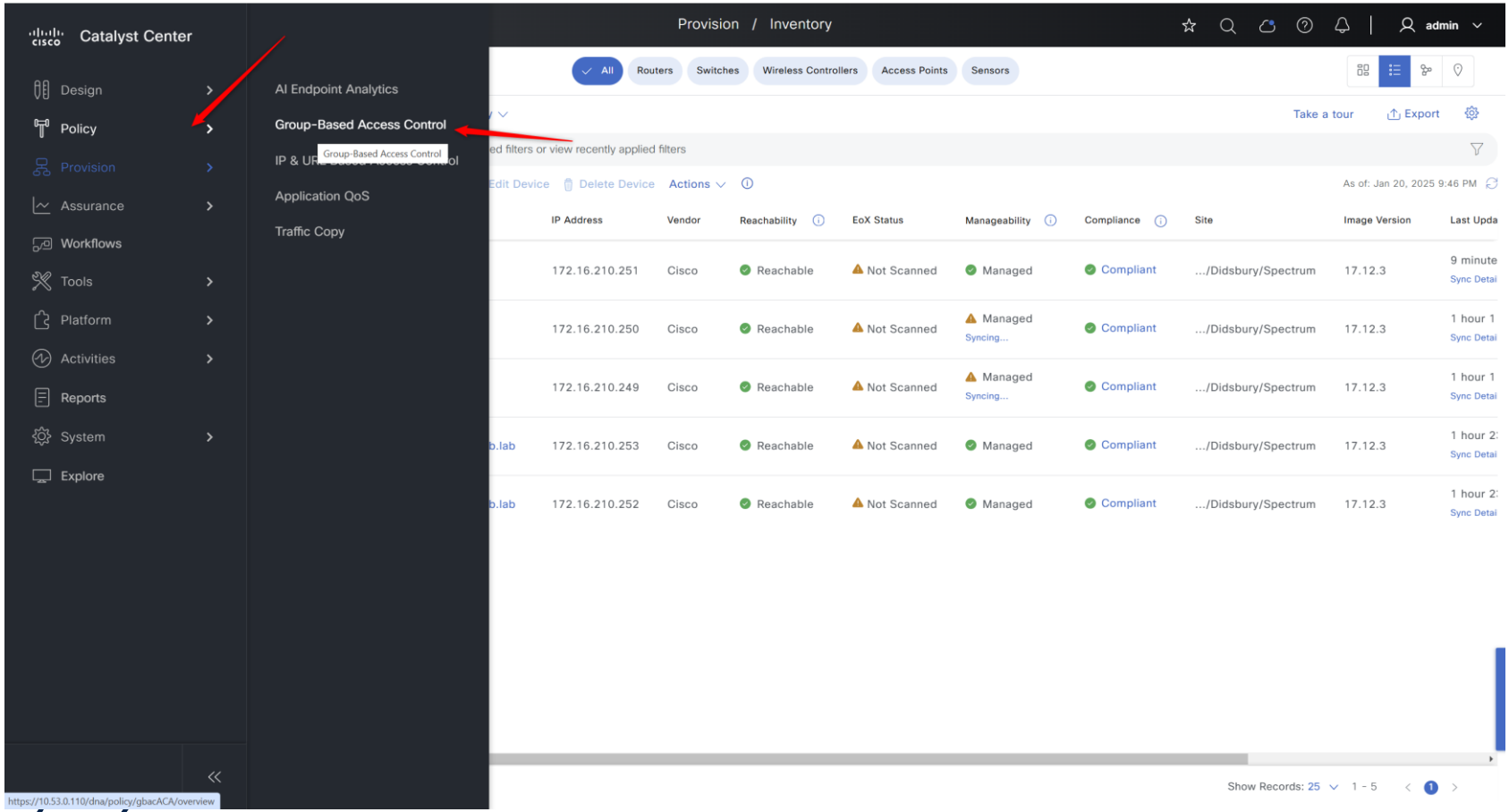
VLAN 102
Subnet I.J.K.L
↓
IPACL 21
IPACL 22 ....

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!

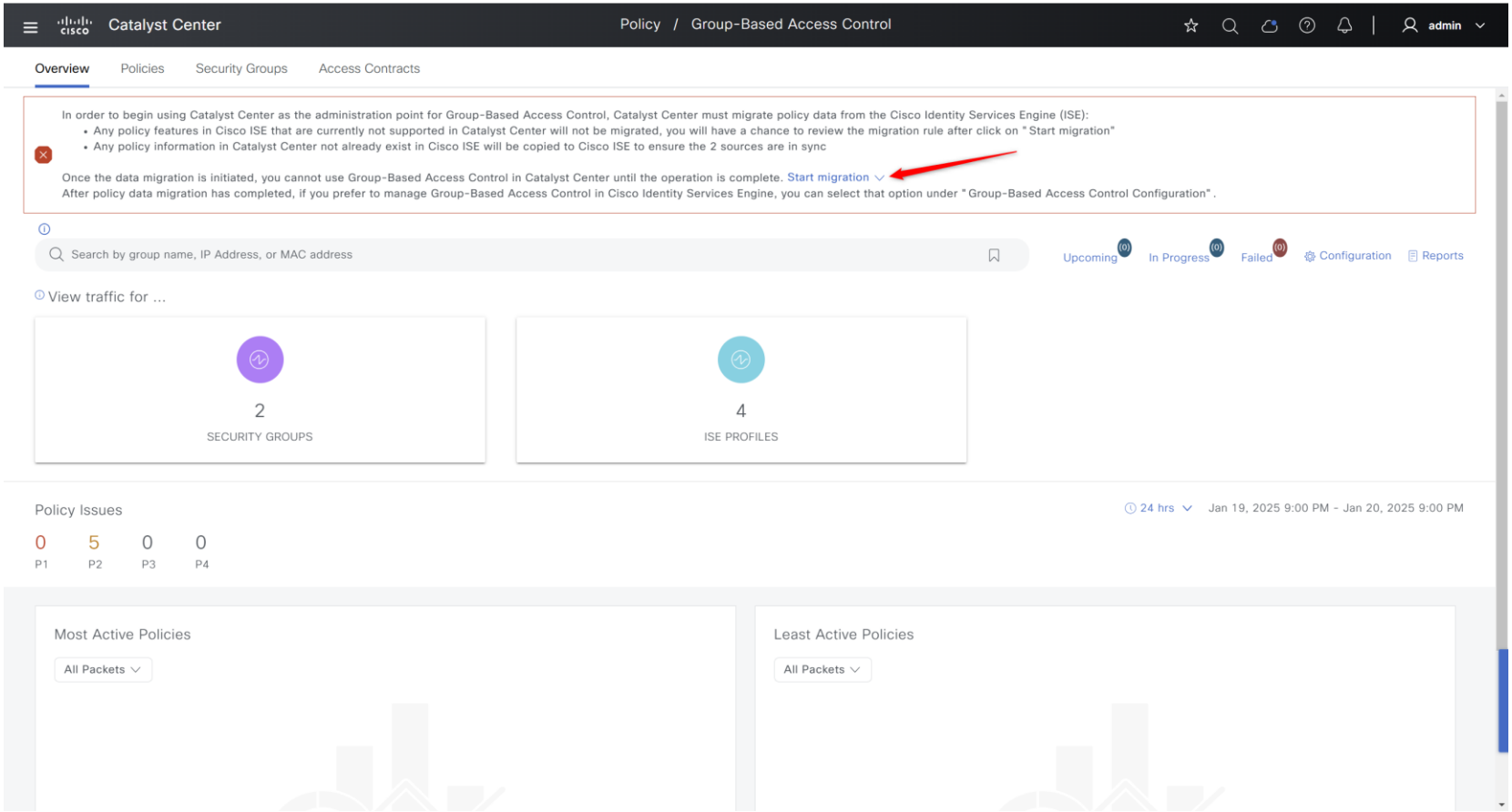


Let’s add TrustSec to the solution!

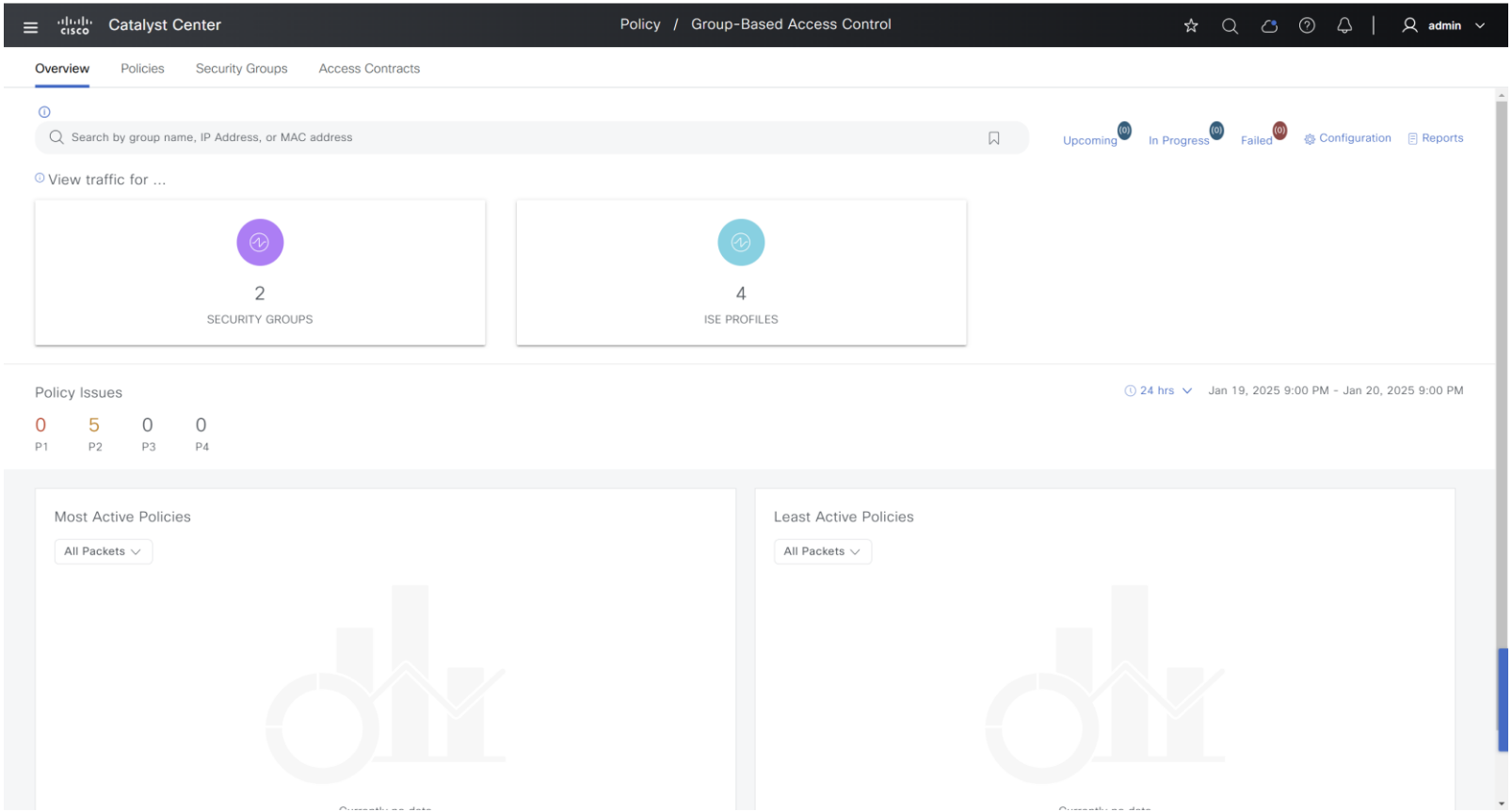

```
edge1#sho cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)

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!

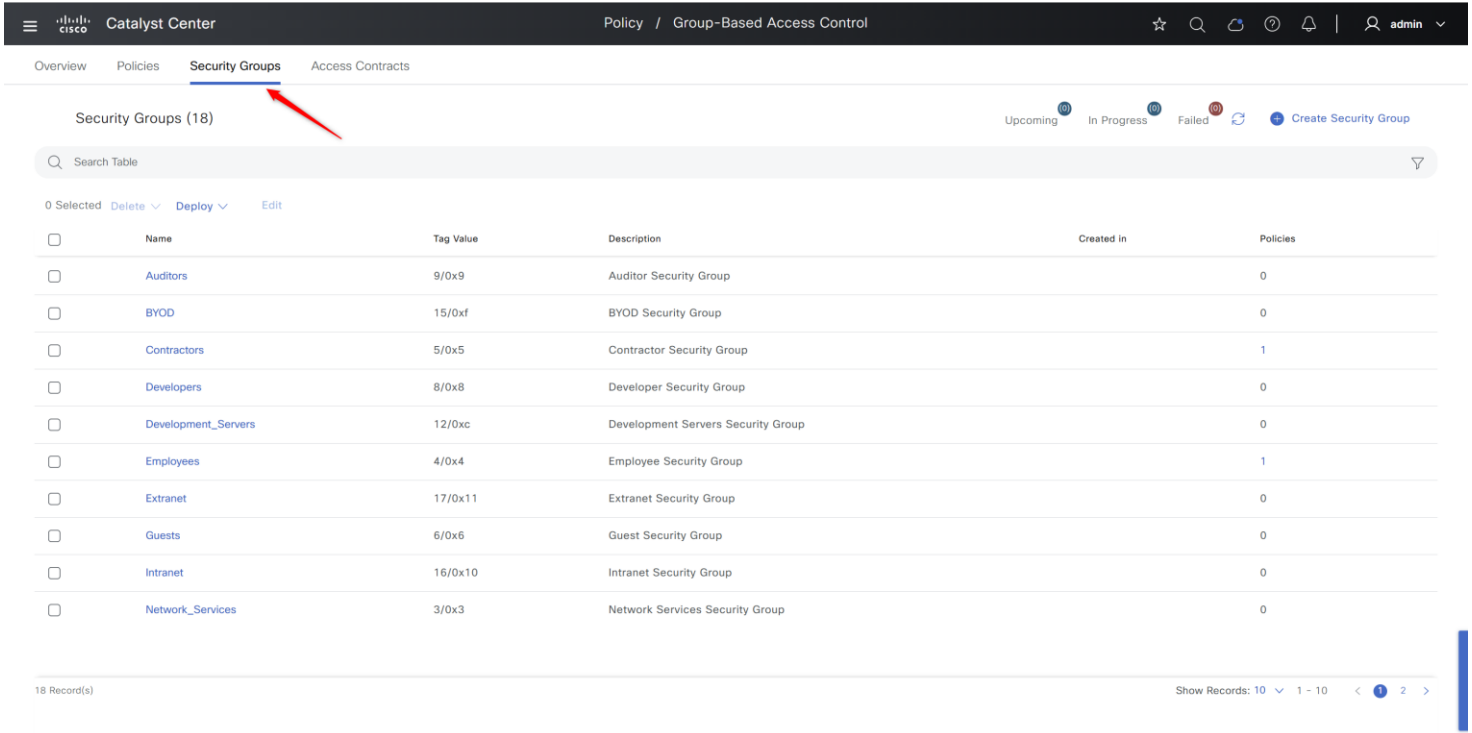
Let’s add TrustSec to the solution!



Let’s add TrustSec to the solution!

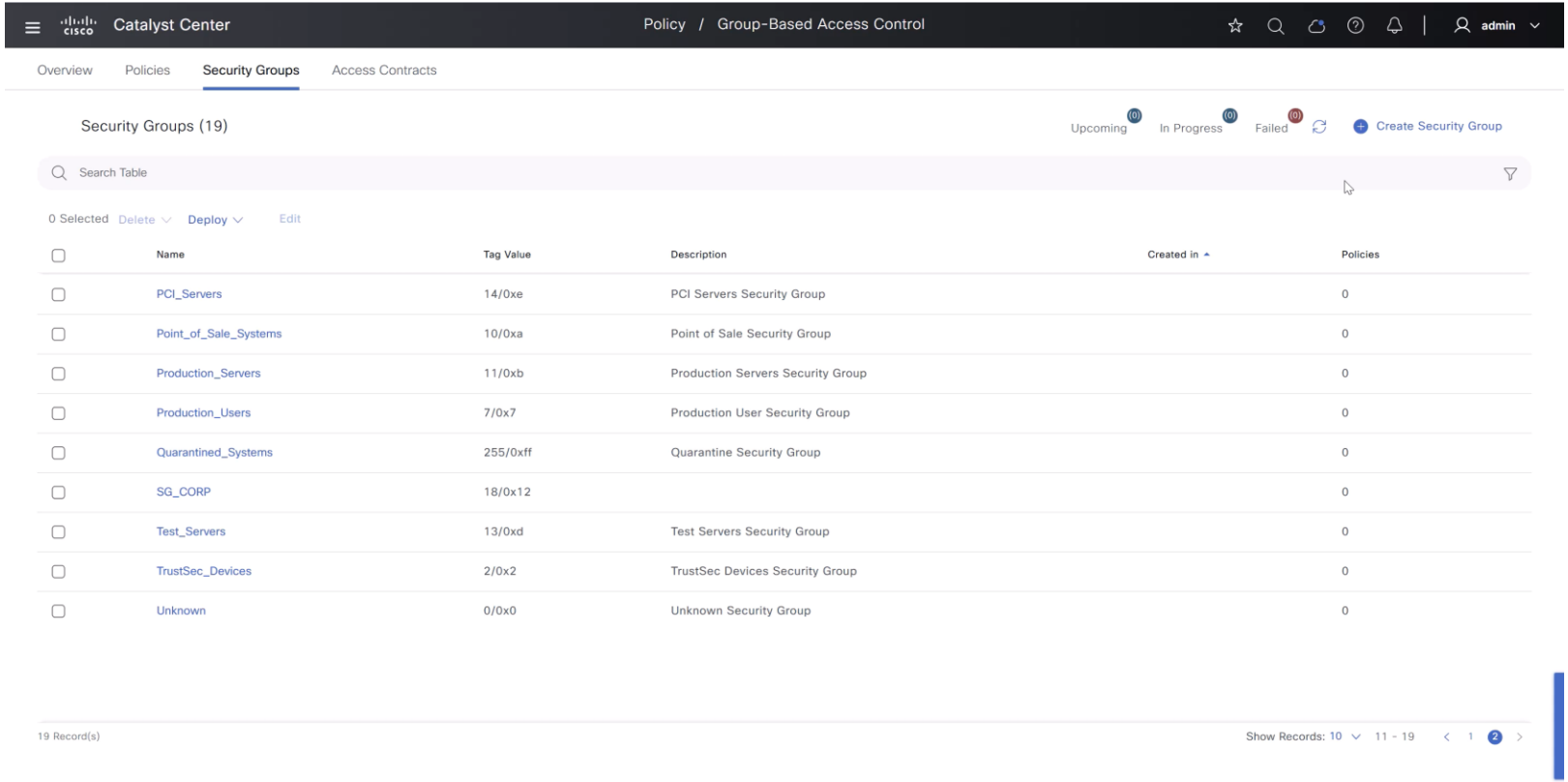


Let’s add TrustSec to the solution!

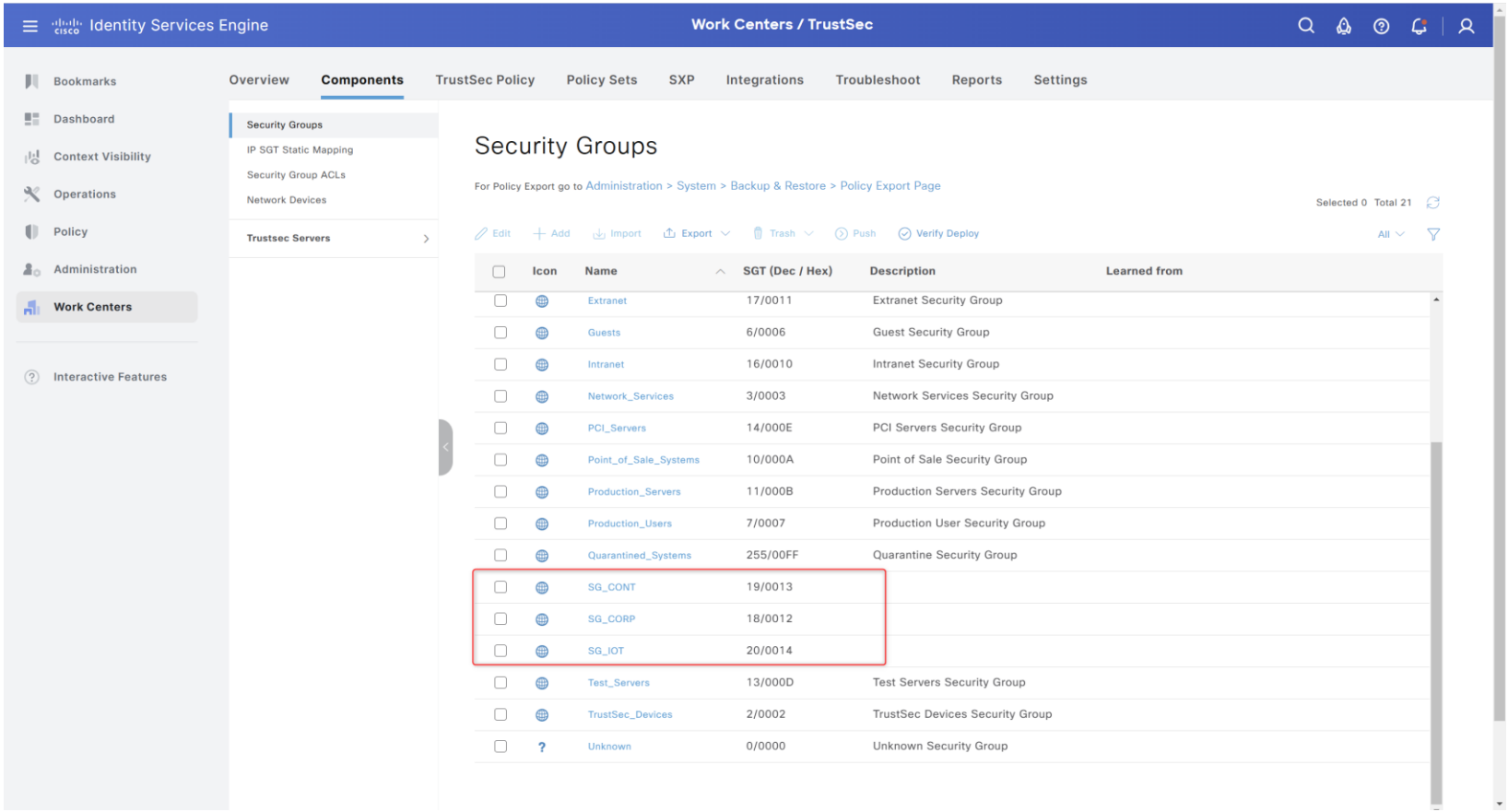


Add Security Groups from CC – not from ISE!!

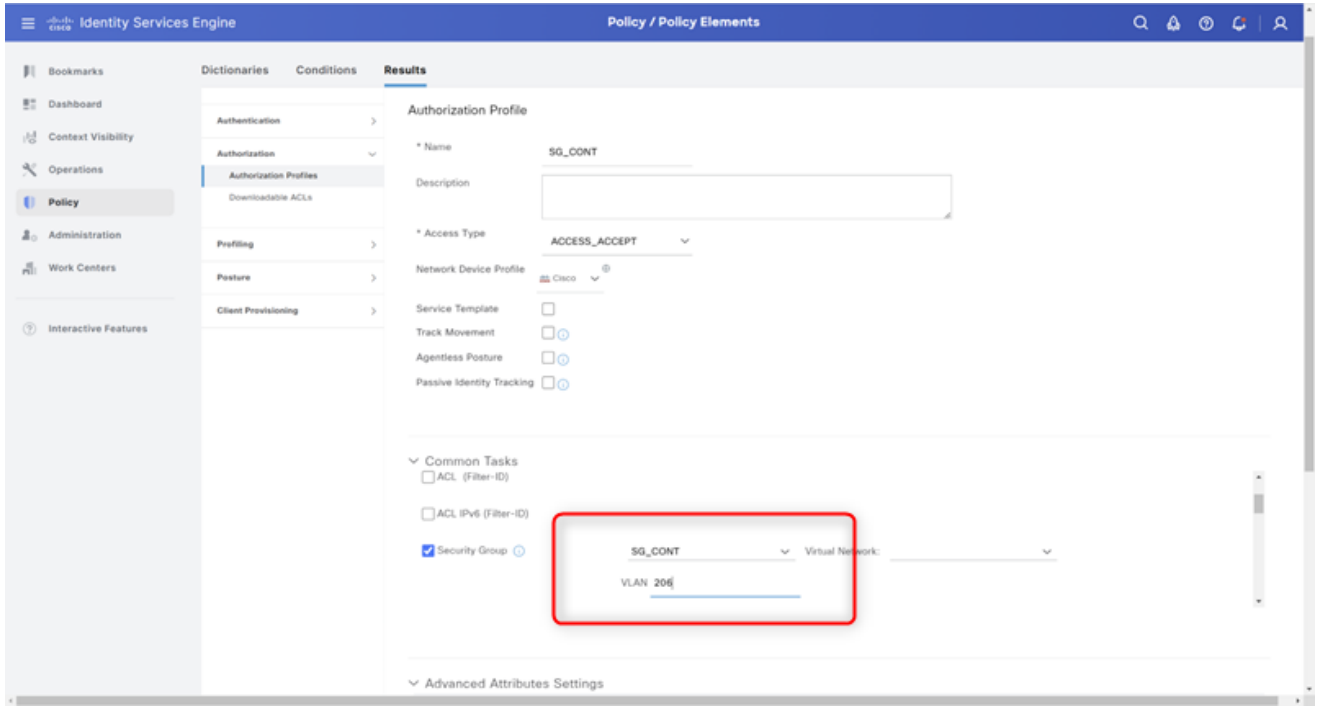
Add some Security Groups - demo



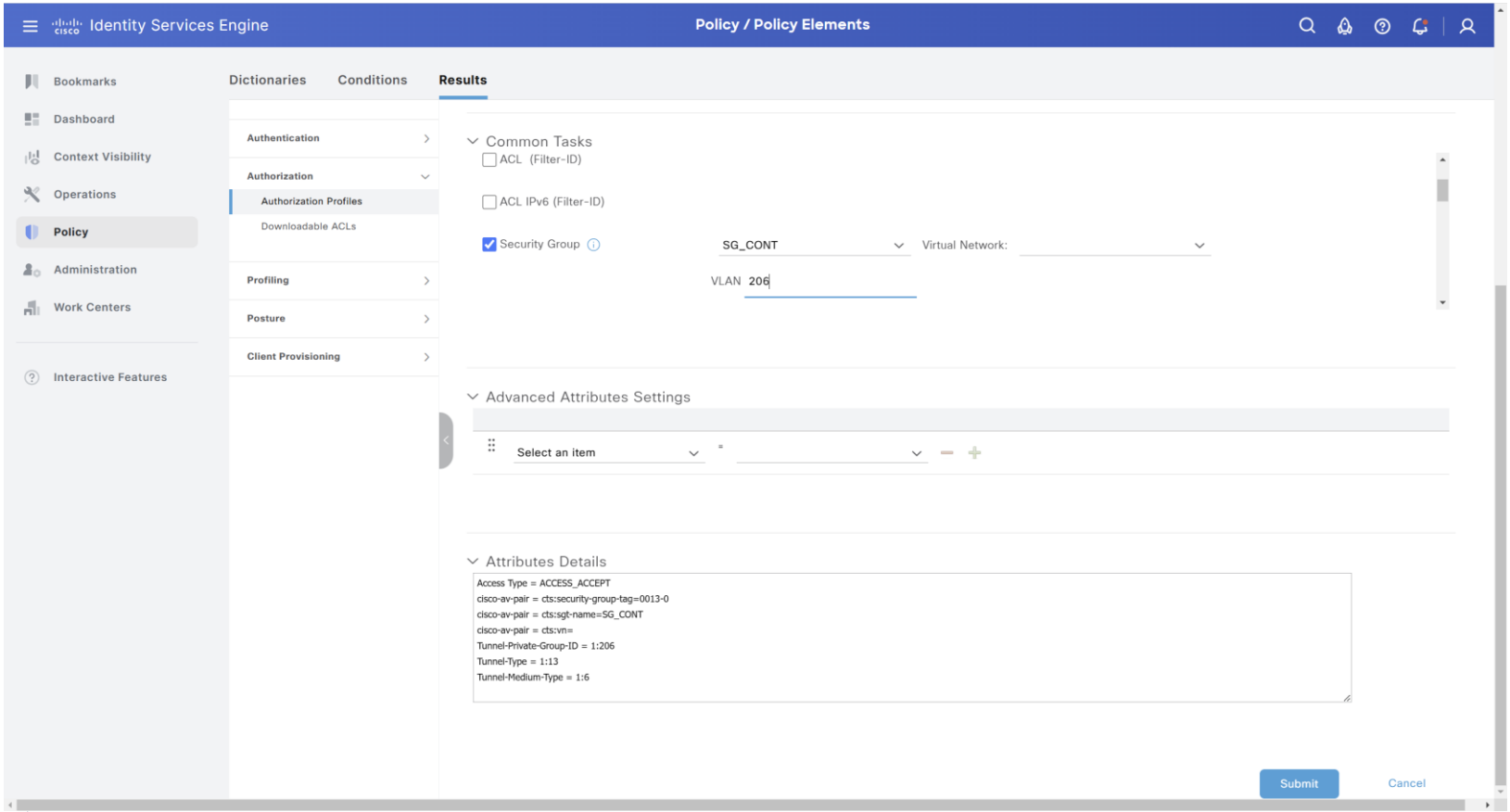
ISE Gets the SGs



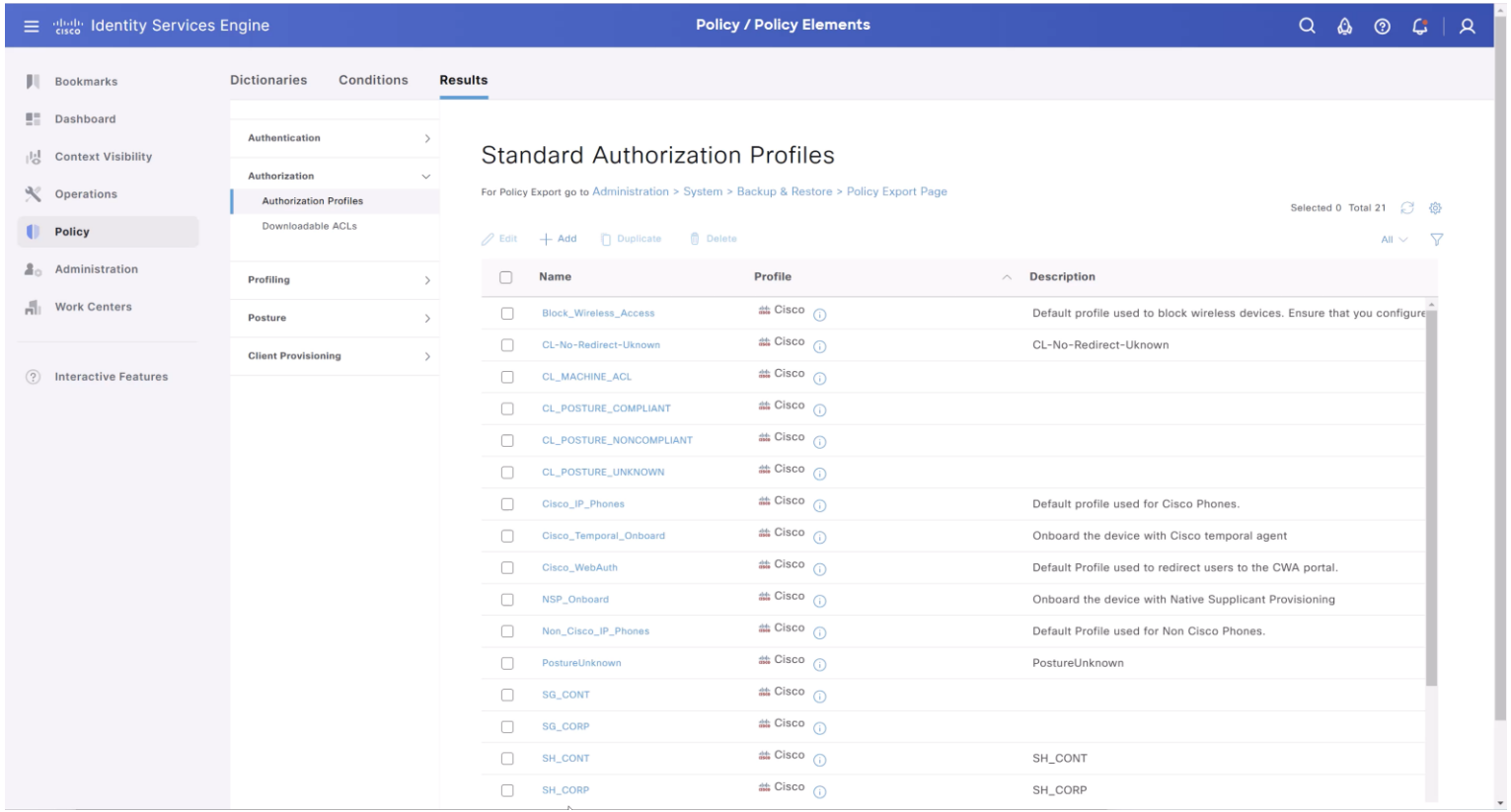
Add slightly different AuthZ Policy Results



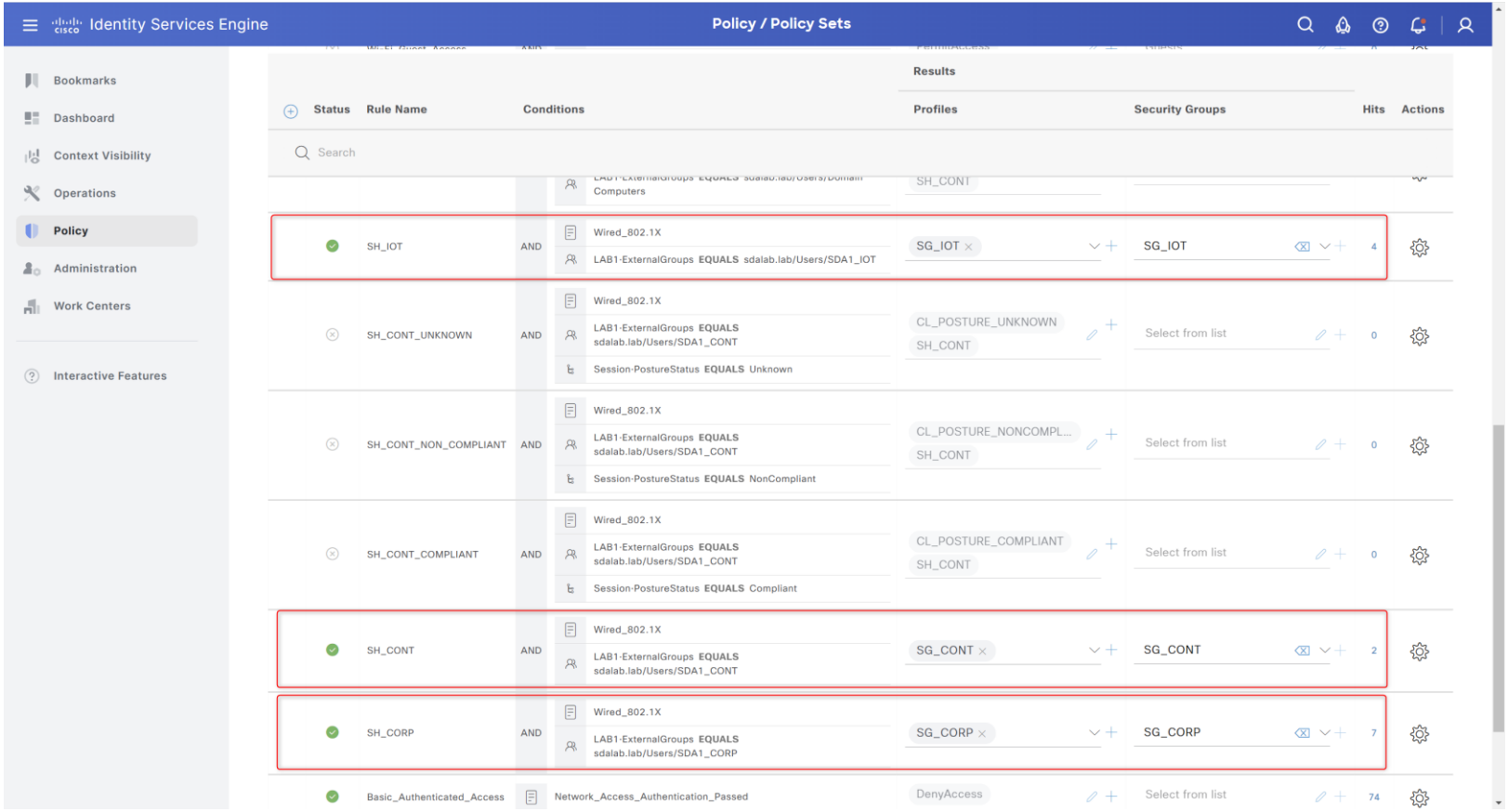
Add slightly different AuthZ Policy Results



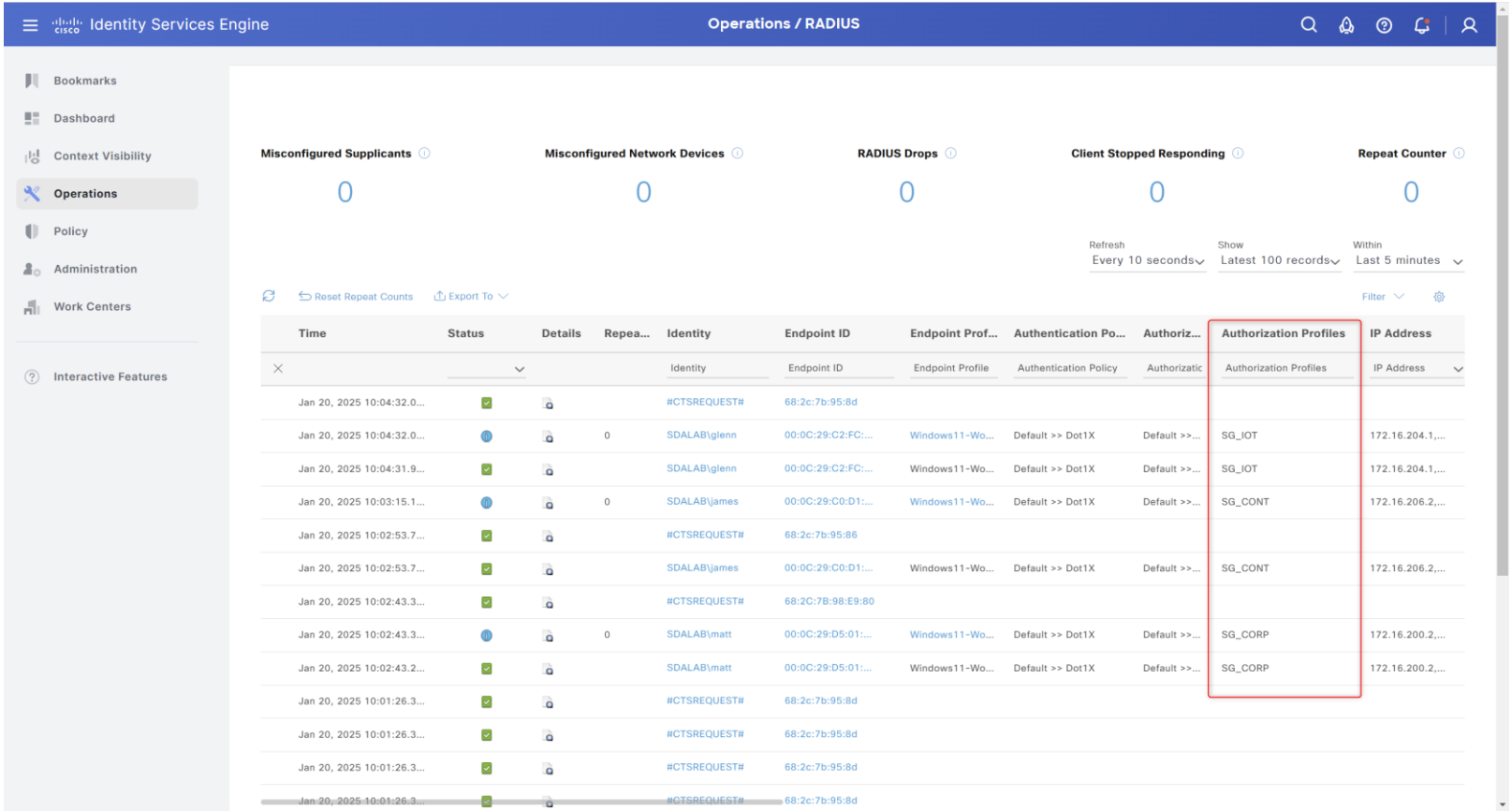
Add slightly different AuthZ Policy Results



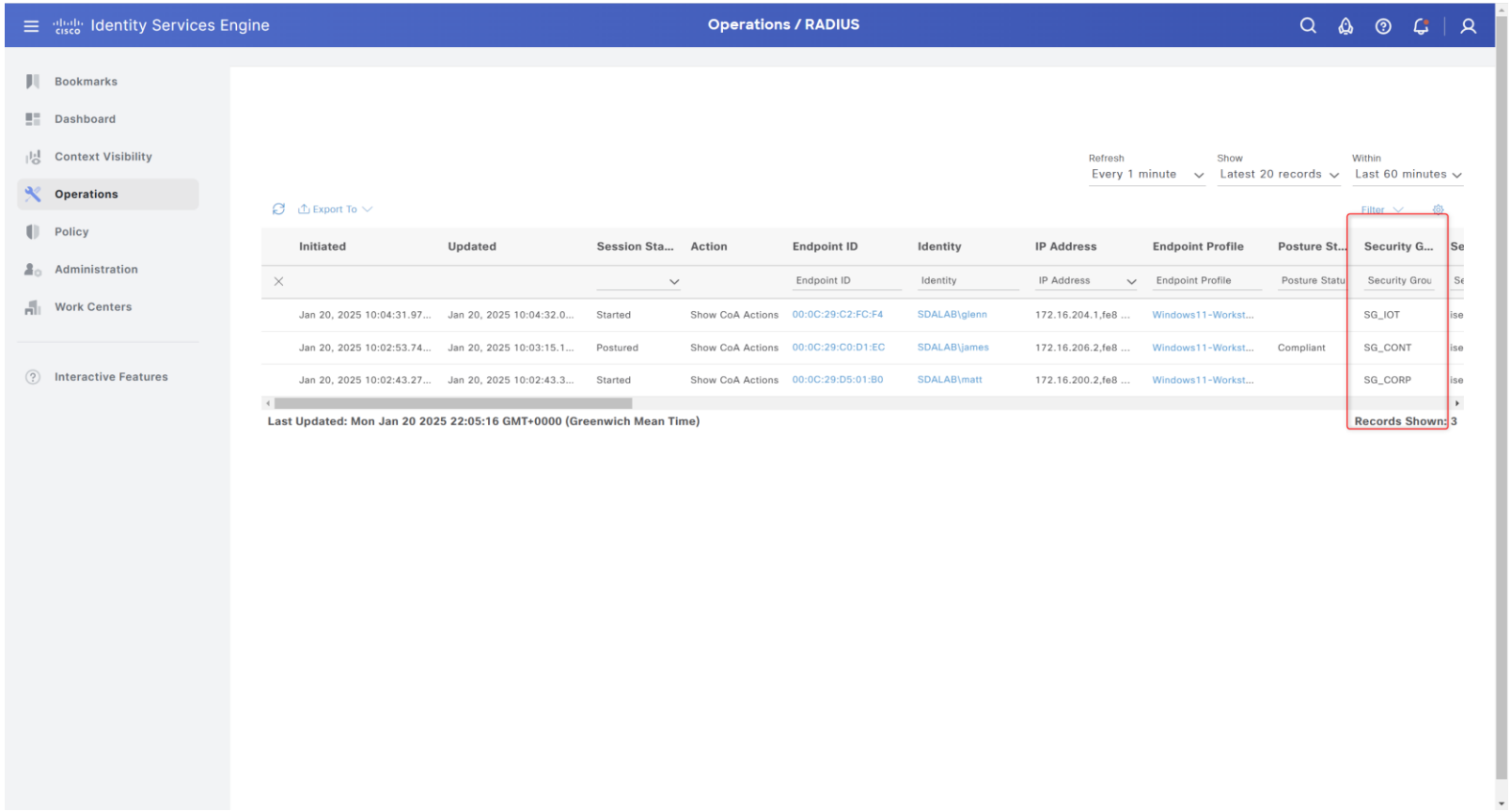
Change our AuthZ Policies to match



Endpoints using TrustSec!



Endpoints using TrustSec!



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!

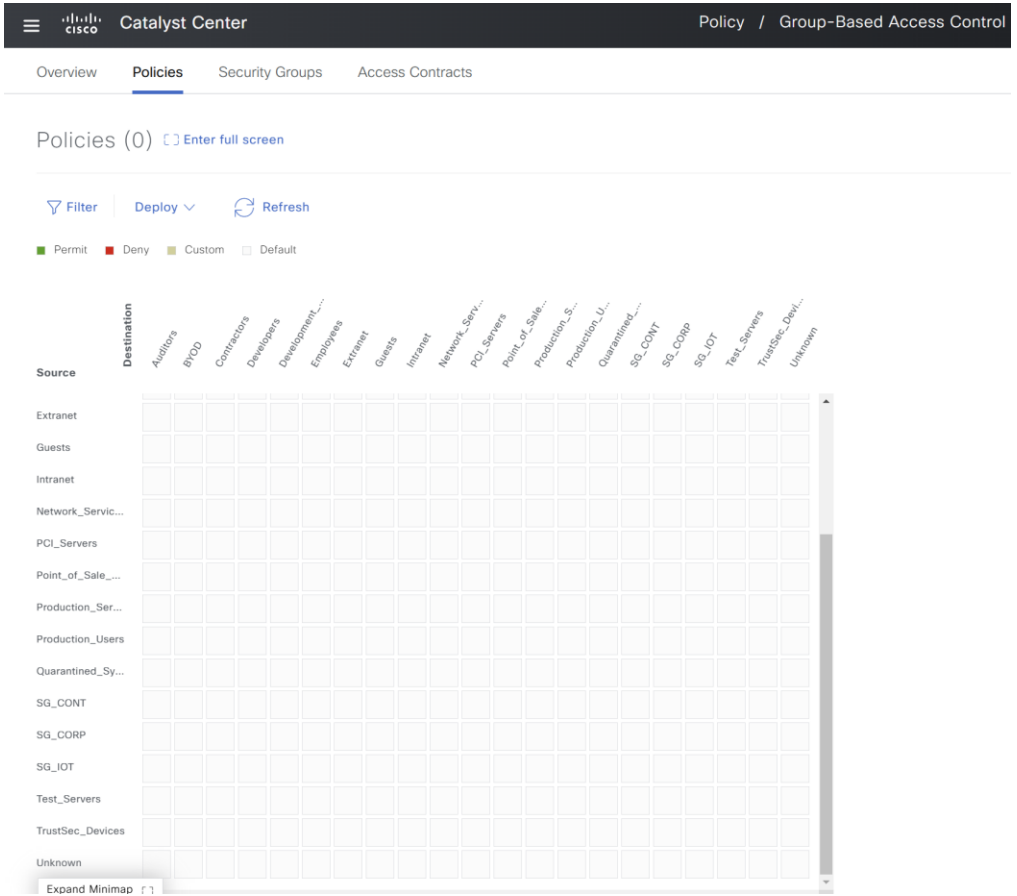
```
! Trunk configuration
int range gi1/0/23 - 24
 ip dhcp snooping trust
 cts manual
  policy static sgt 2 trusted
```

And you already know how – CLI Templates!

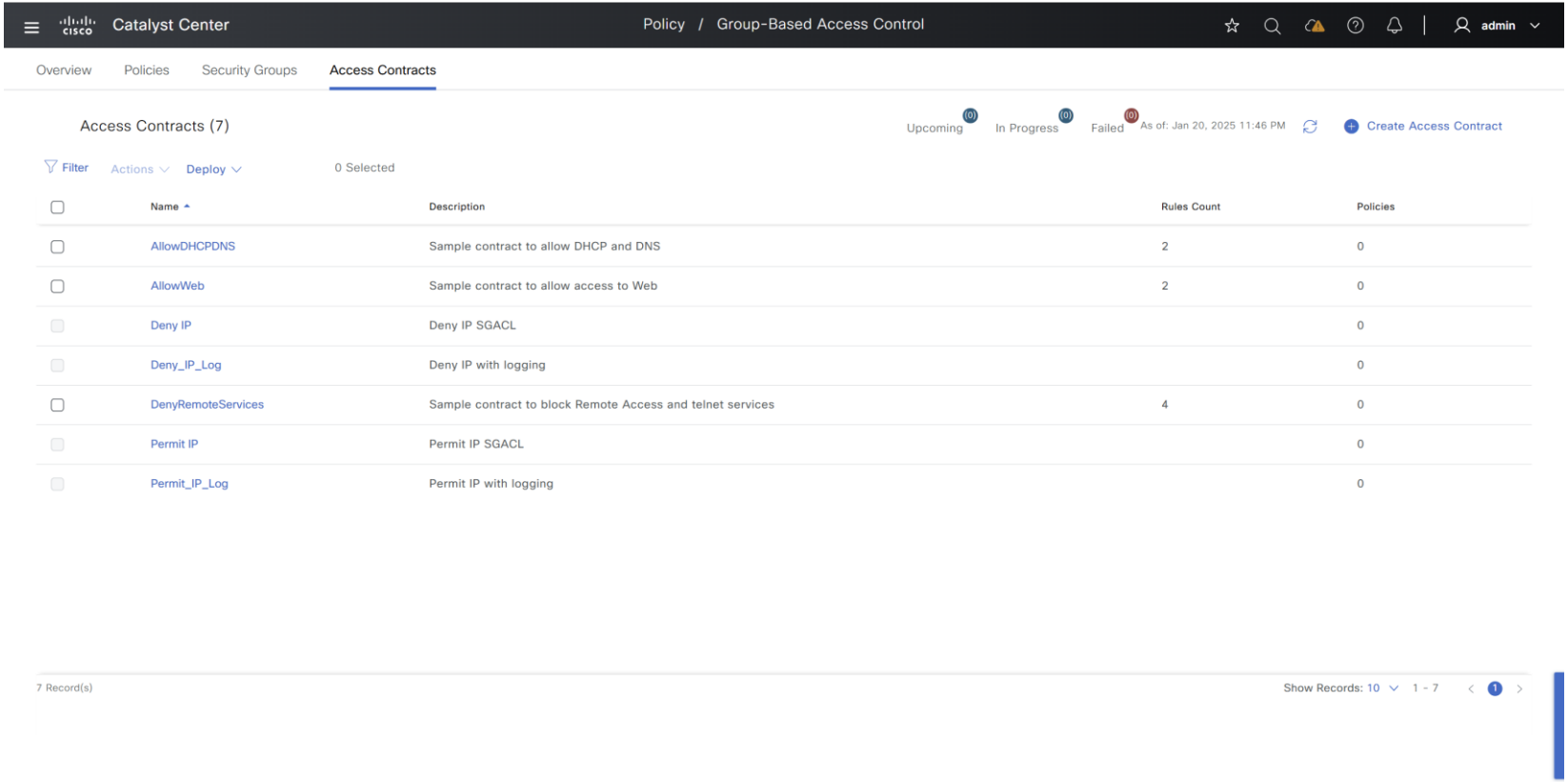
So what can we do with this?

- No Firewall Hairpinning!
- No ACLs/ACEs!
- Enforce East-West

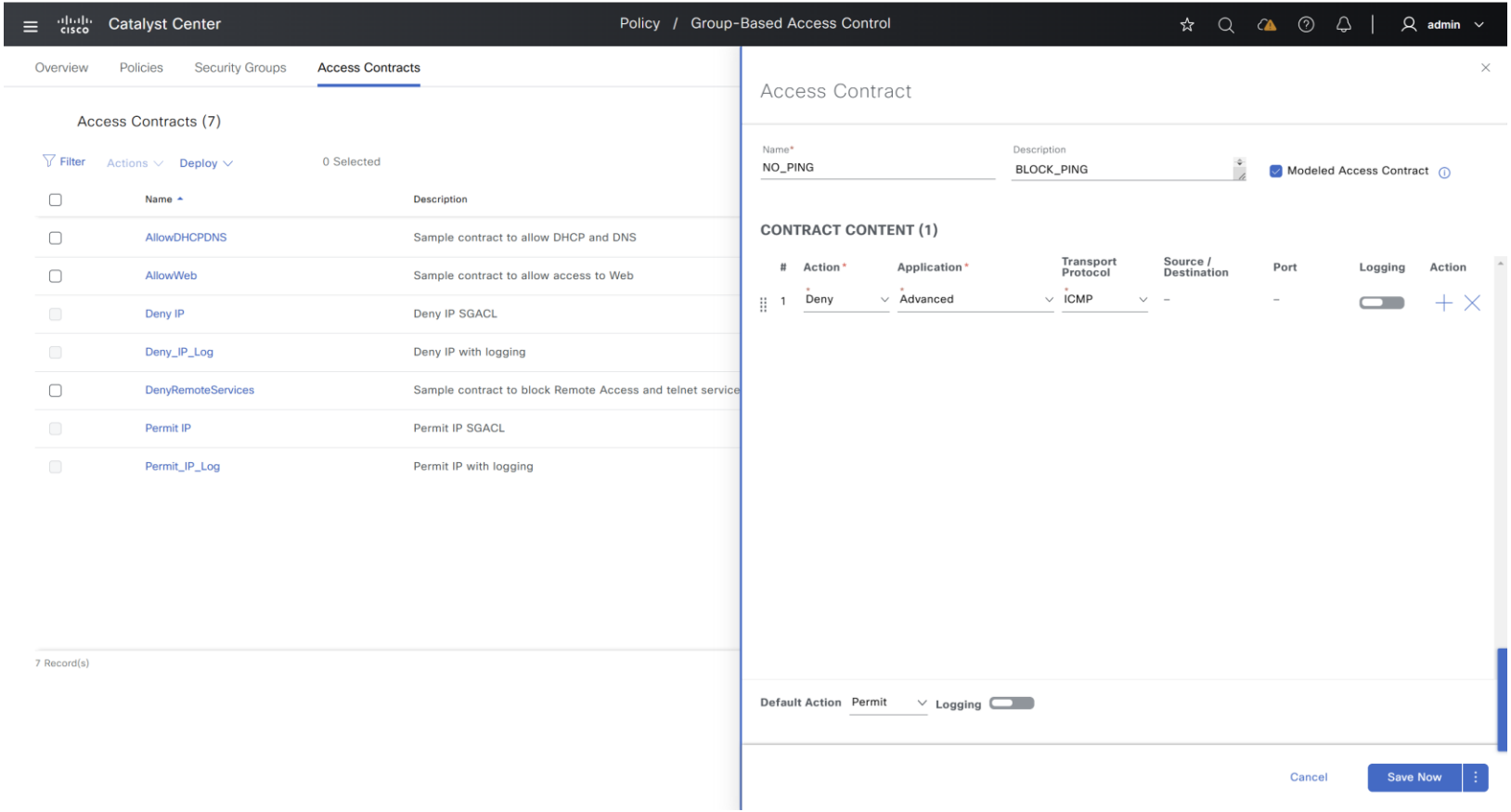
- Welcome to the Matrix!
  (not that one!)



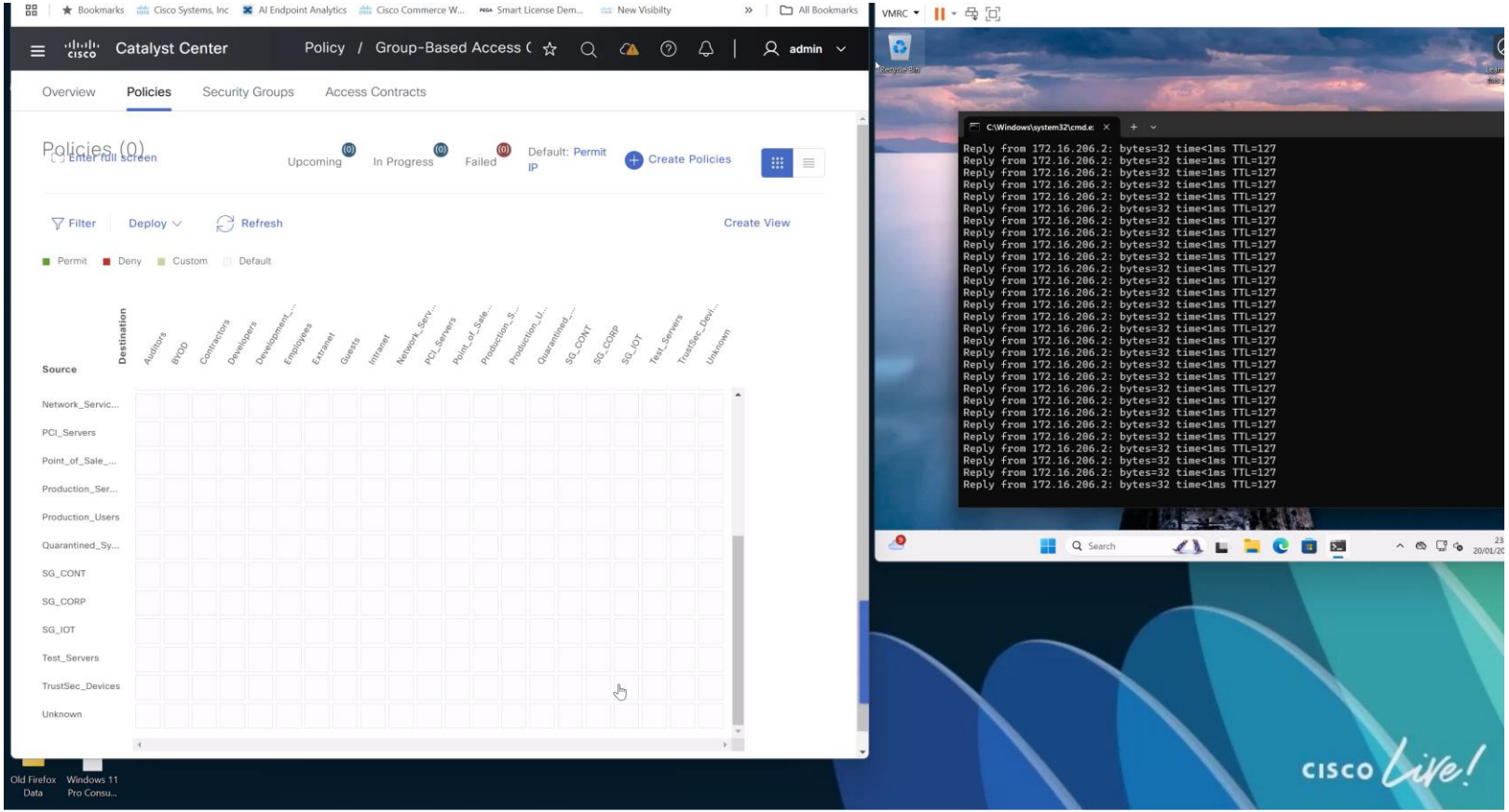
Create an Access Contract



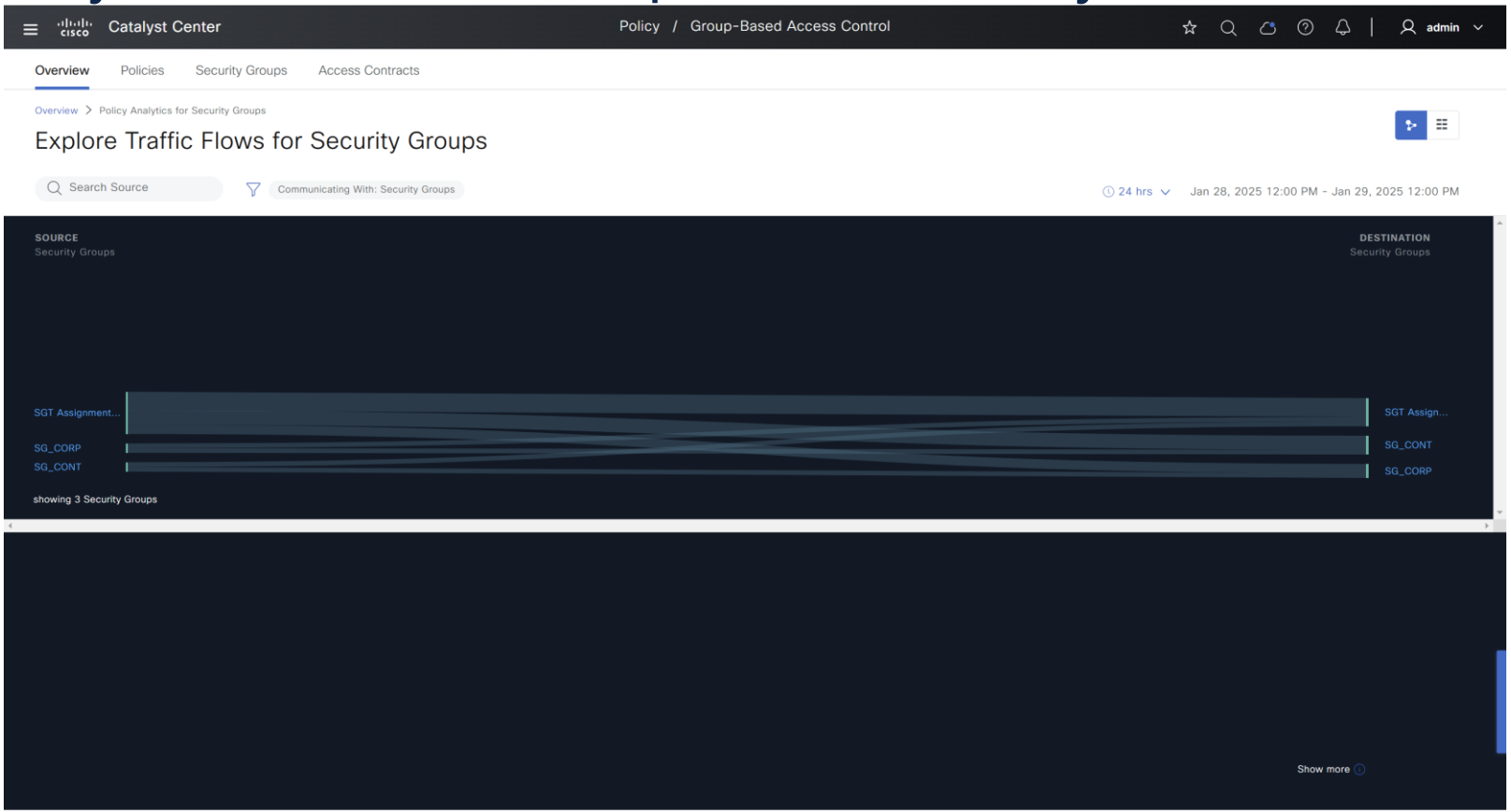
Create an Access Contract – Lets block ping!



TrustSec in Action – Demo



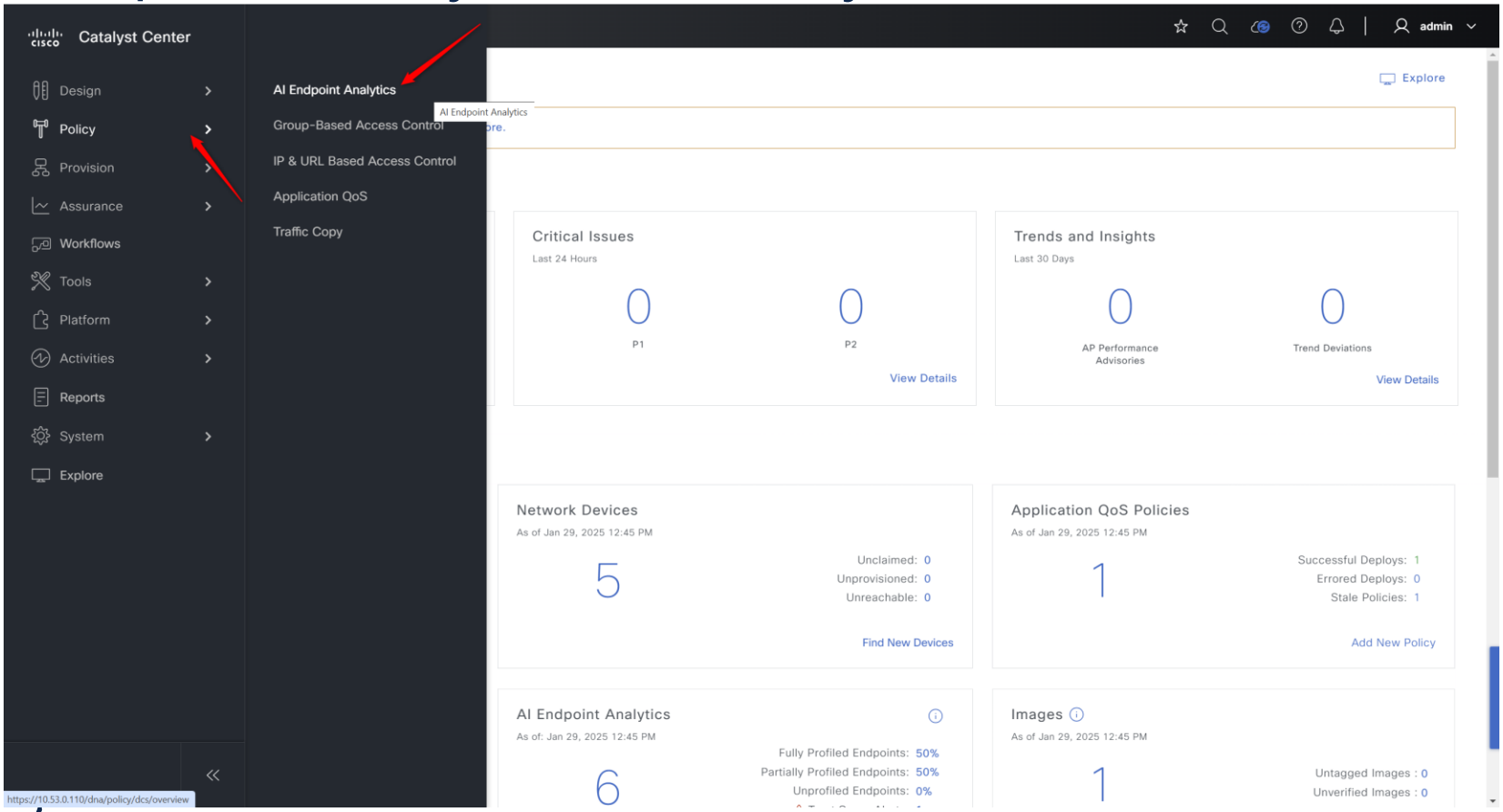
Visibility of Flows – Group Based Analytics



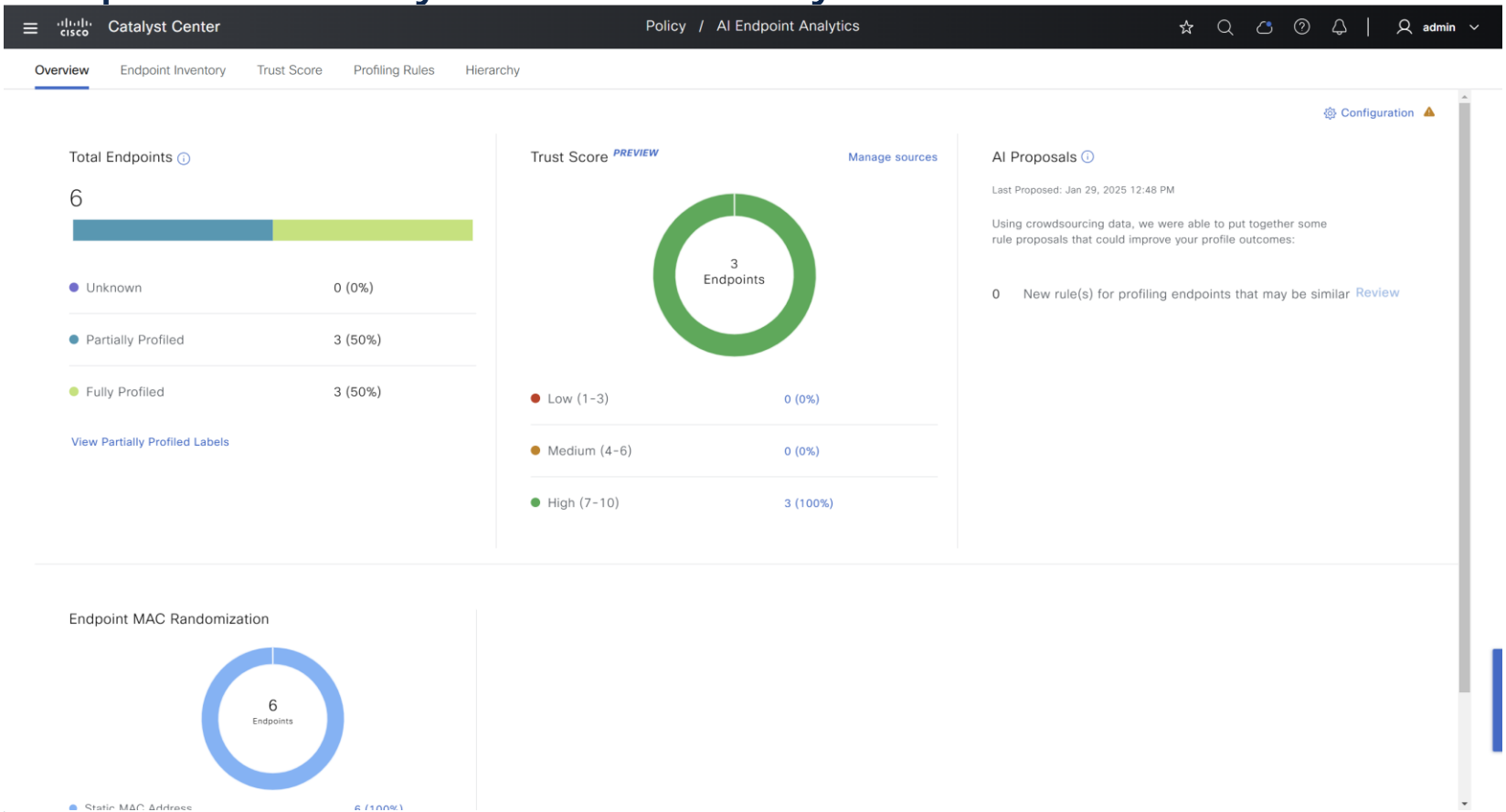
What about the AI ?

- AI Endpoint Analytics!

AI Endpoint Analytics in Catalyst Centre

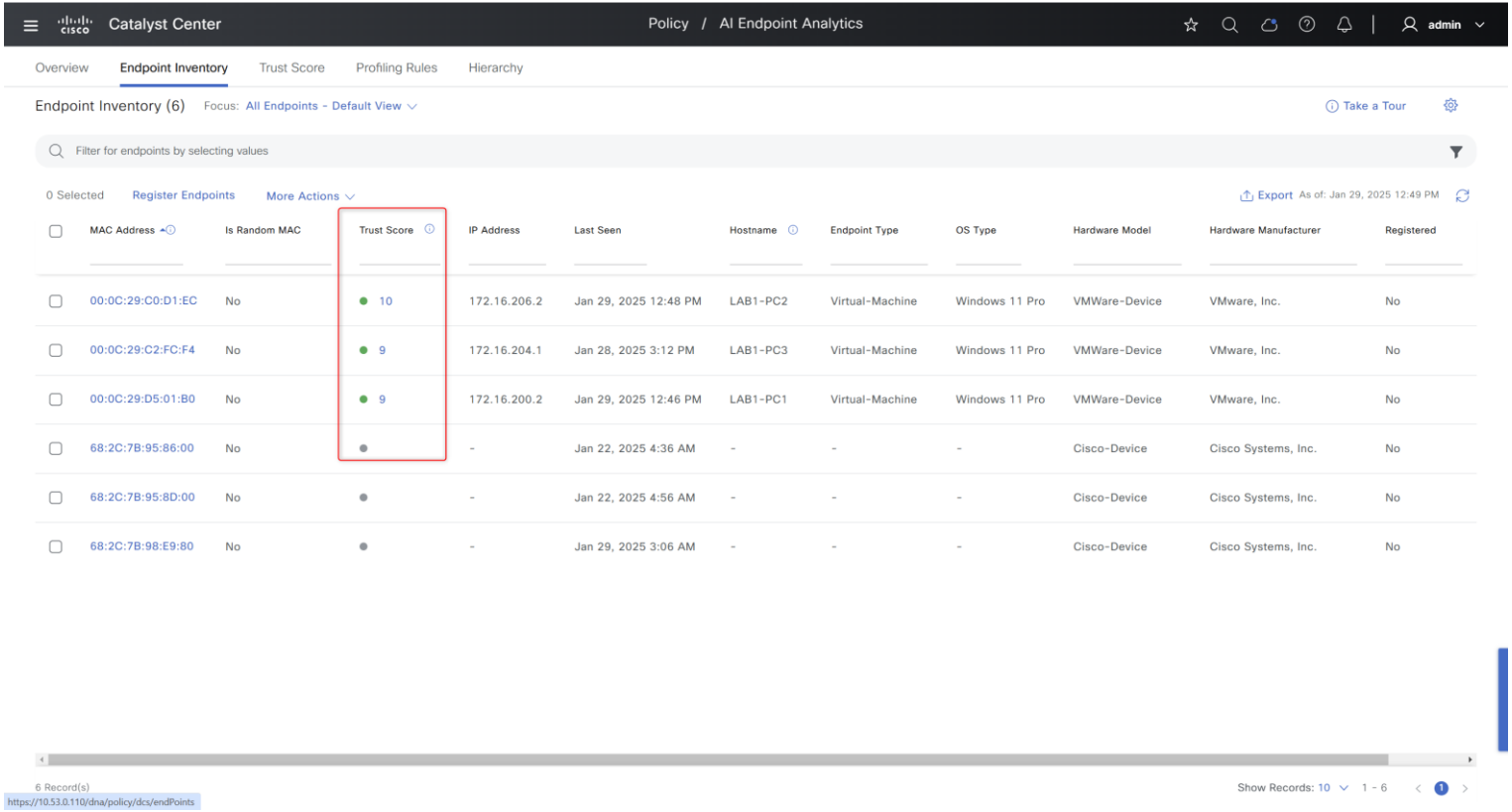


AI Endpoint Analytics in Catalyst Centre

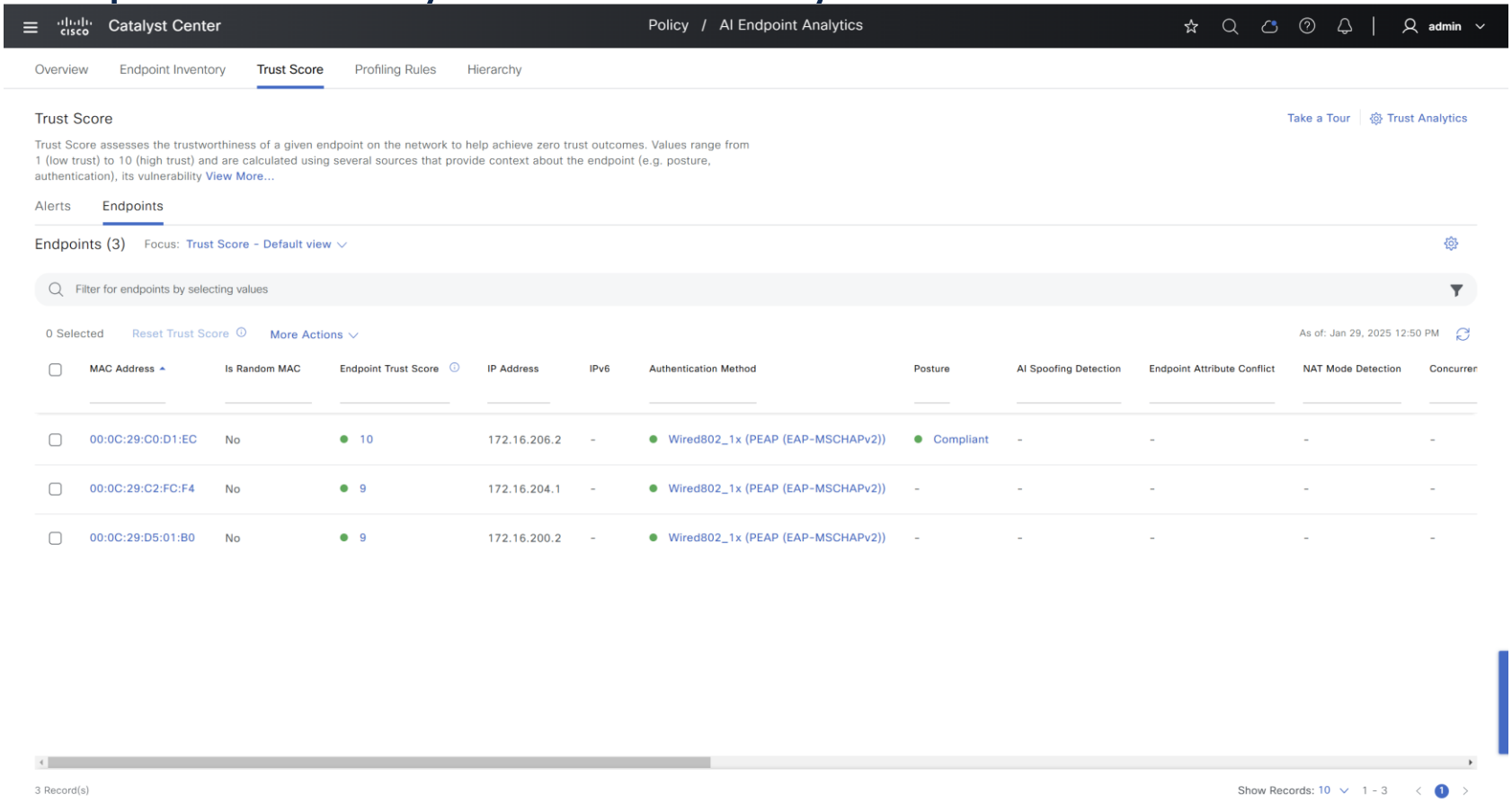


AI Endpoint Analytics in Catalyst Centre

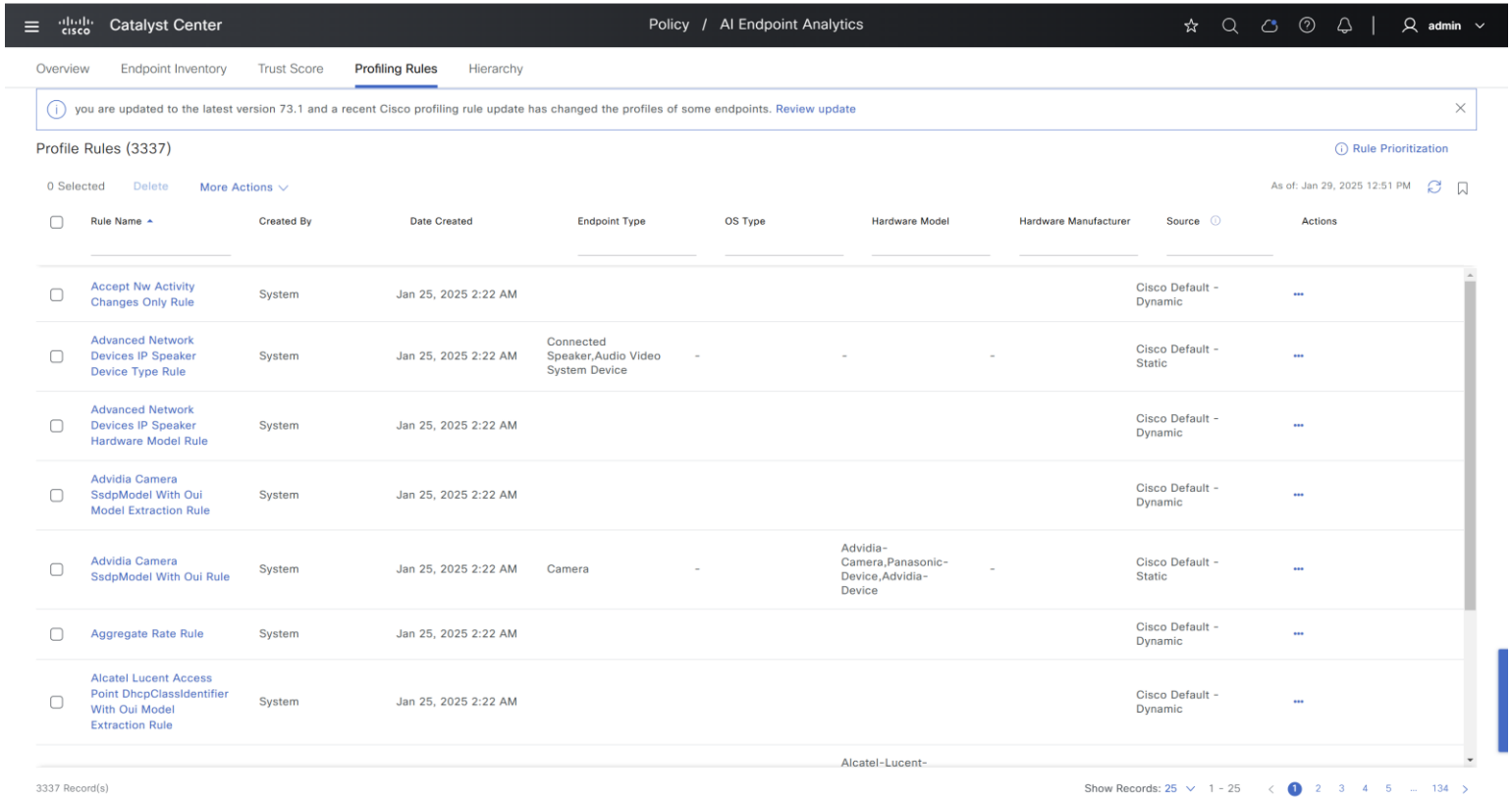
Includes a trust score



AI Endpoint Analytics in Catalyst Centre

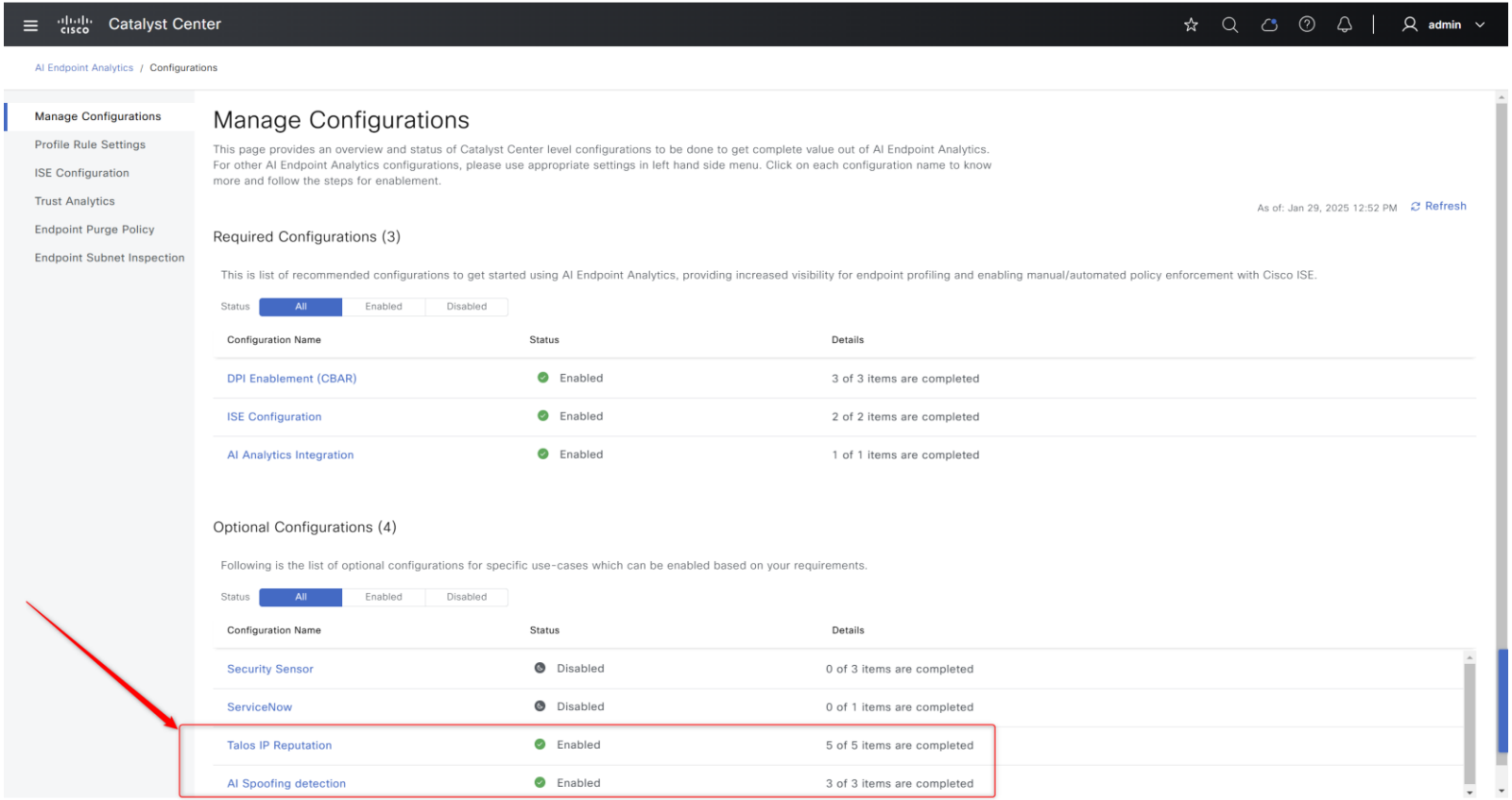


AI Endpoint Analytics in Catalyst Centre



AI Endpoint Analytics in Catalyst Centre

Talos integration



We Did It!!

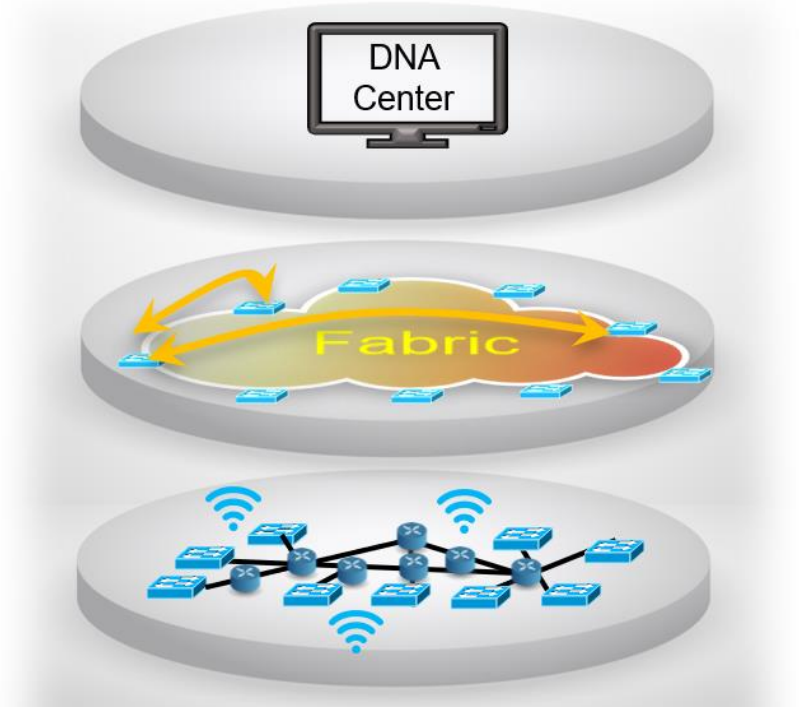
cisco Live!

But is there a better way?

Software Defined Access

cisco Live!

Cisco SD-Access – Bringing Everything Together



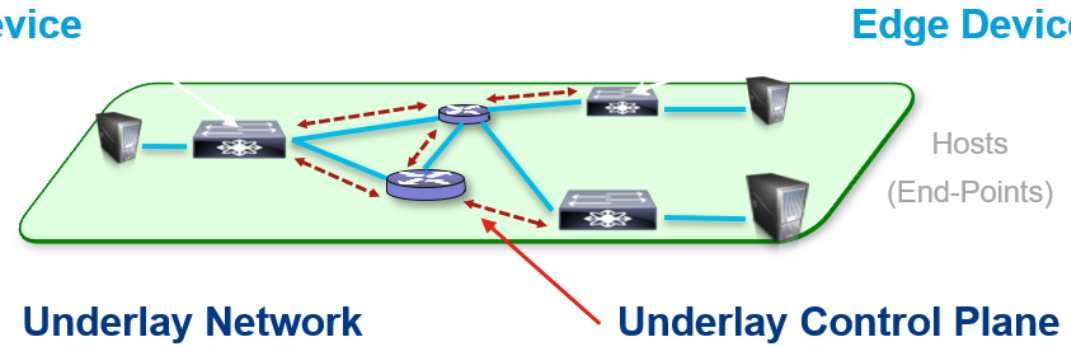
Automation and Assurance

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!



LAN Automation !!

What exactly is a Fabric?

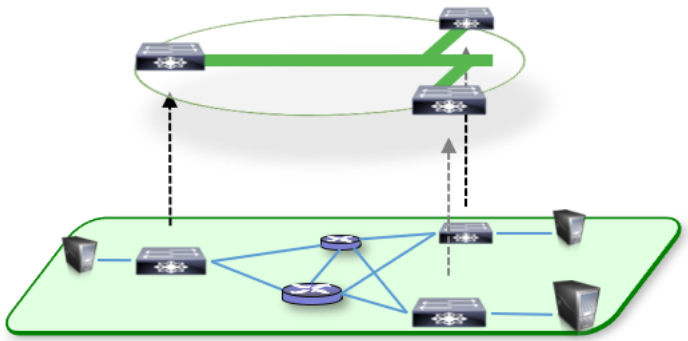
A “Fabric” is an “Overlay”

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!

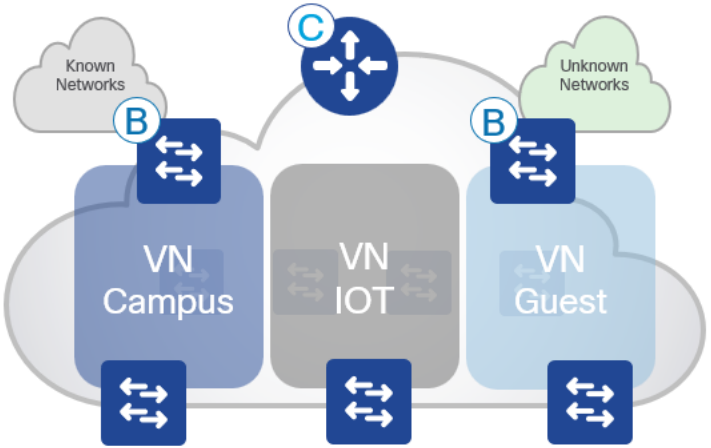
Virtual Network – A Closer Look

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…

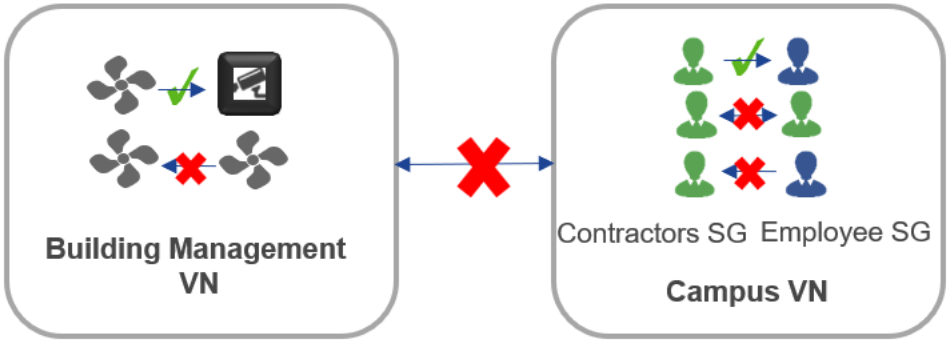
Well that's clear then…

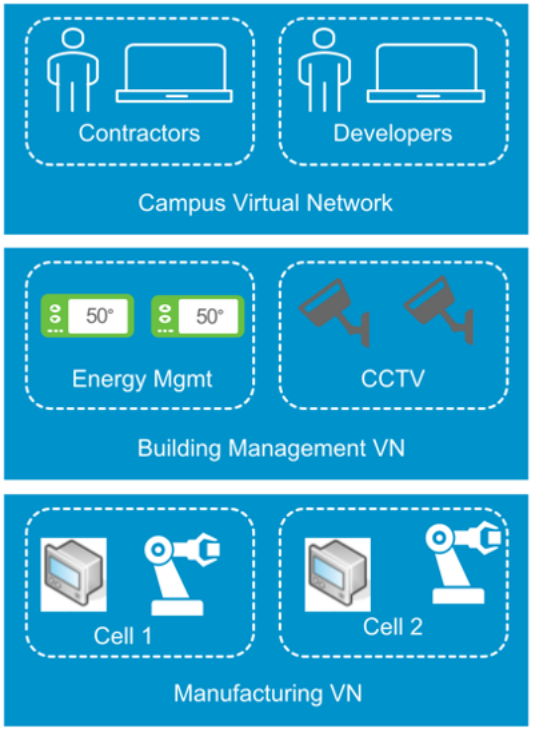


Segmentation Policies – Macro & Micro

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).

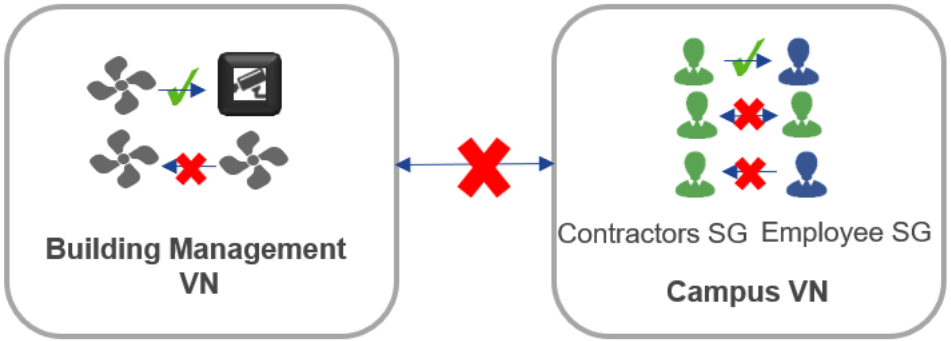


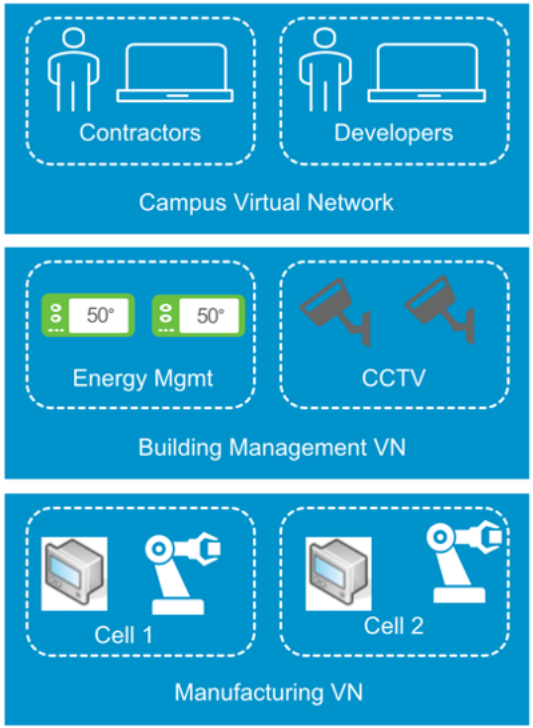


Segmentation Policies – Macro & Micro

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).

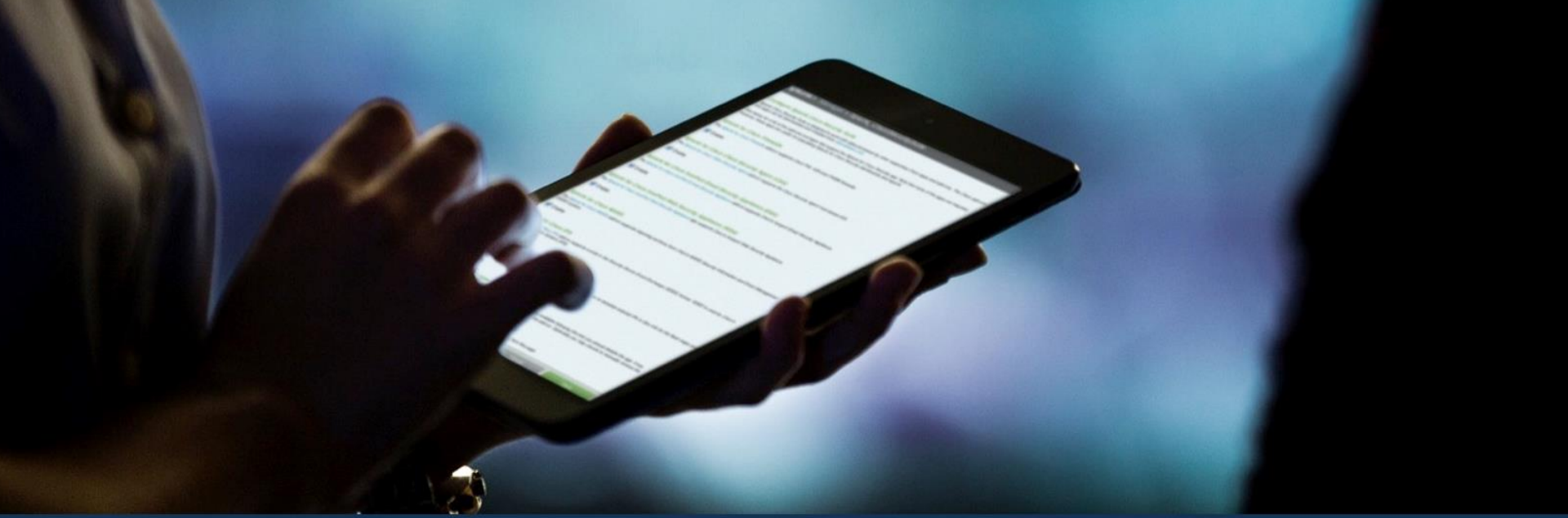




Provision

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.

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. Sessions from this event will be available from March 3.

Contact me at: magraha2@cisco.com

Thank you

cisco Live!

Bonus Content!: Posture Compliance – AKA NAC

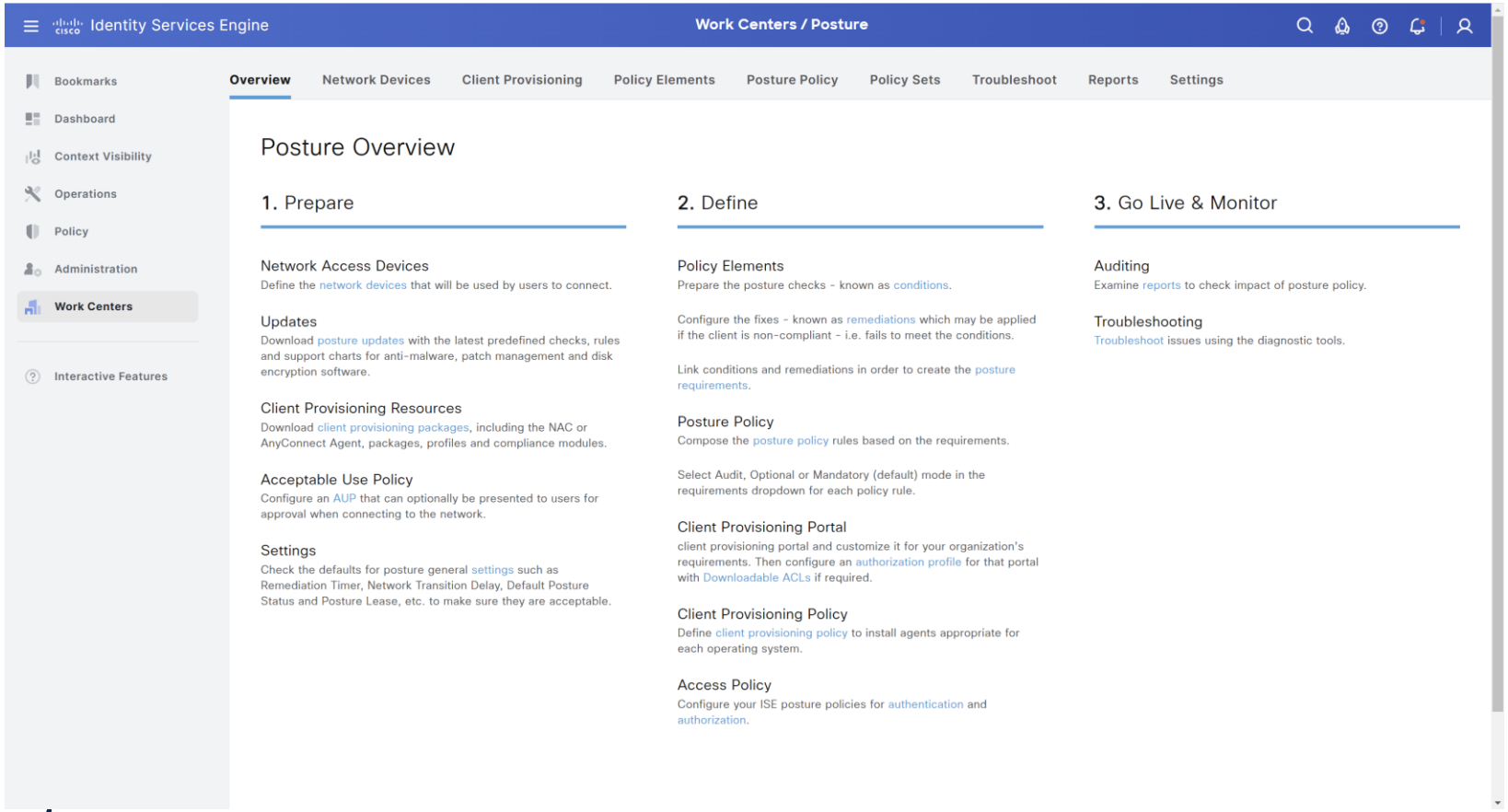
cisco Live!

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

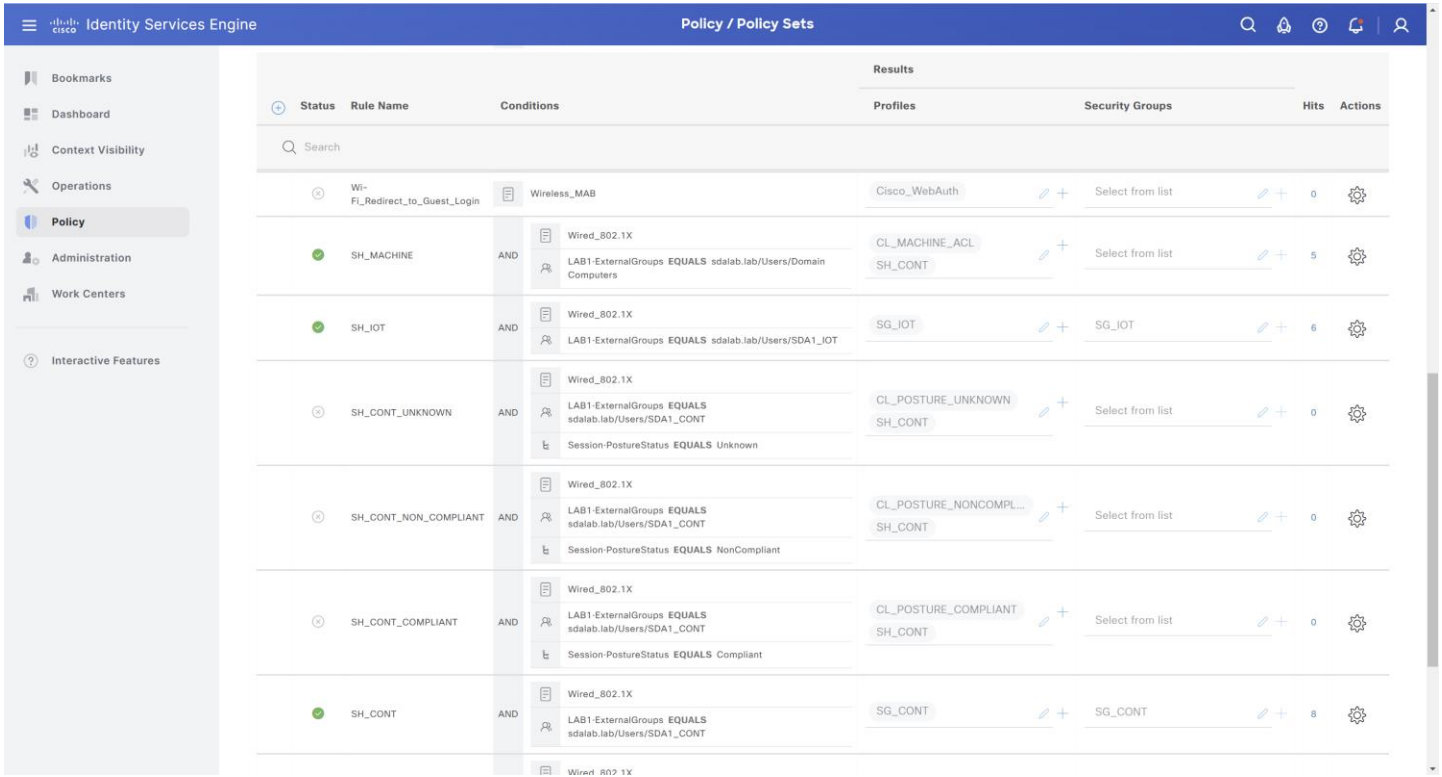
Why Posture Checking and Compliance?

Posture Checking - Workflow

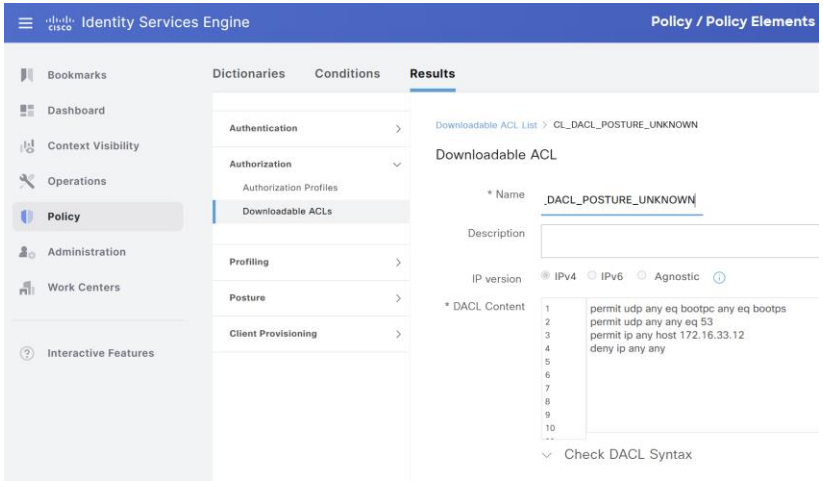


Posture Deployment

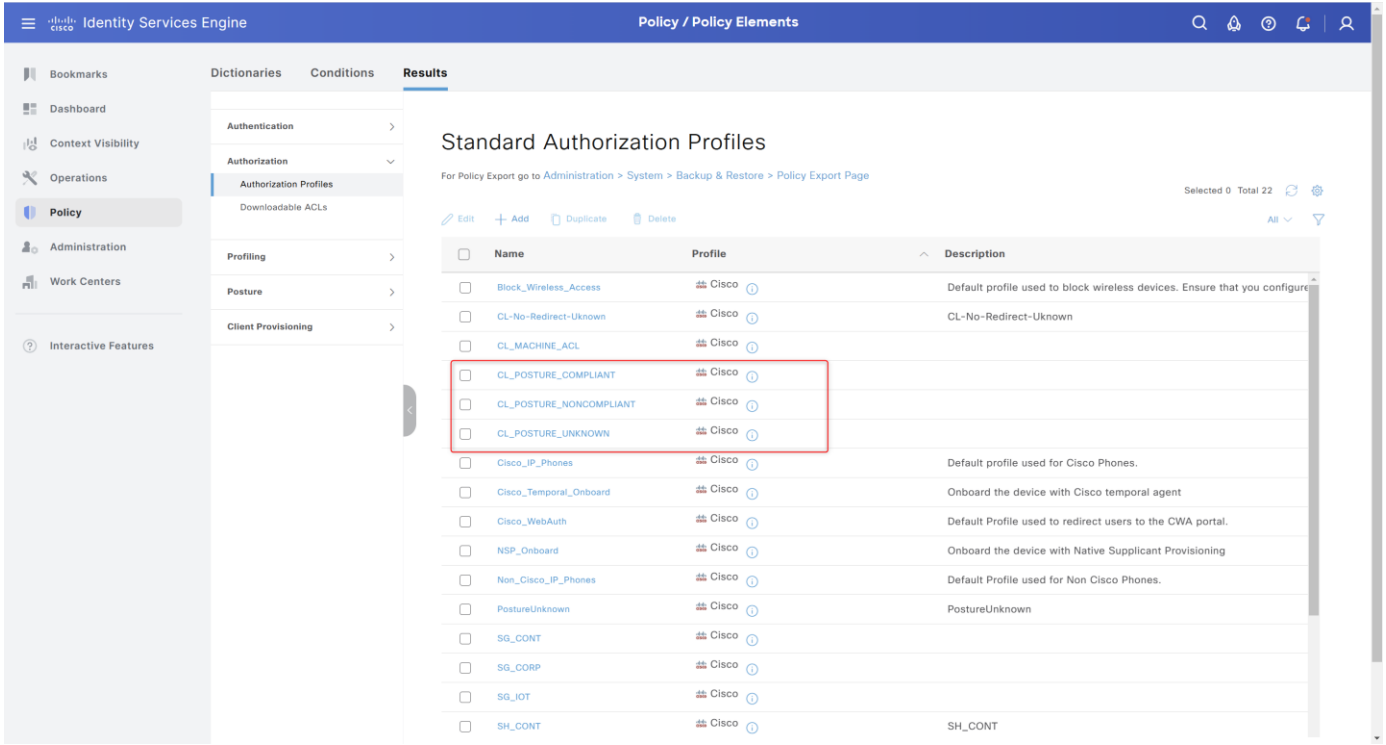
Add some new Rules`



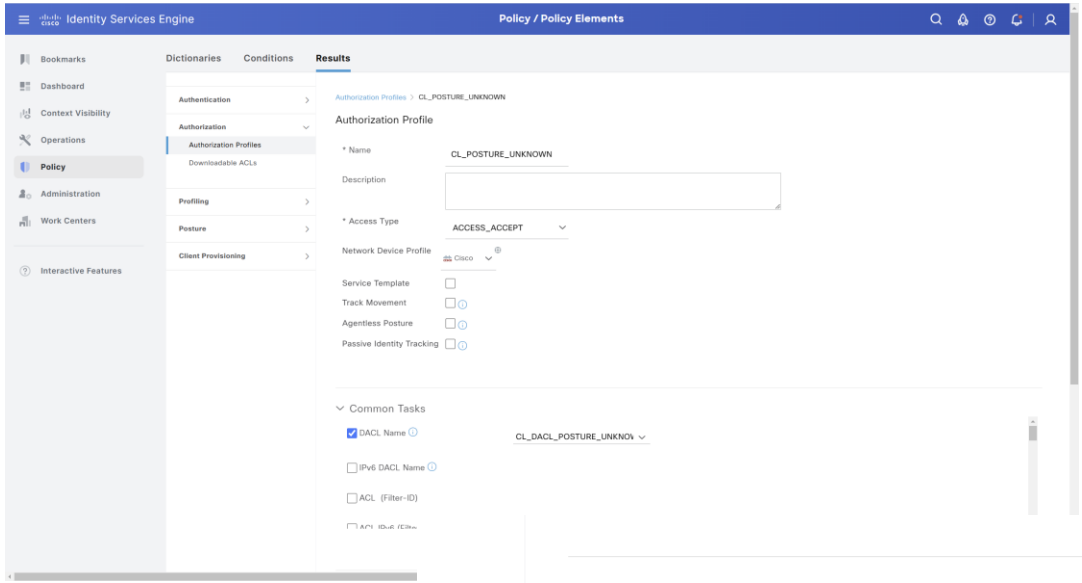
Posture Deployment – create some dACLs



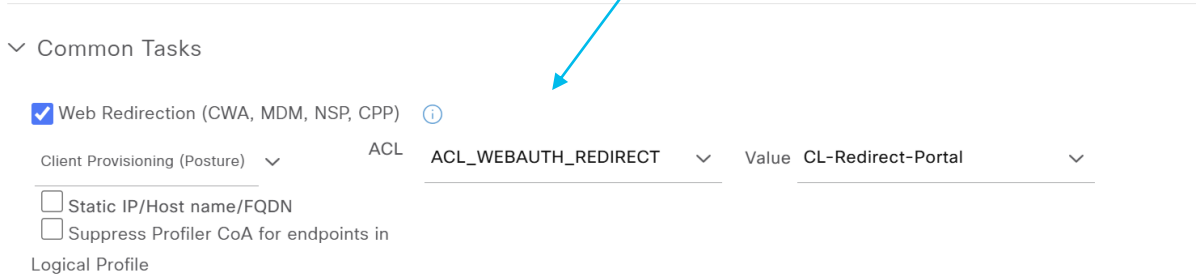
Posture Deployment – create AuthZ Profiles



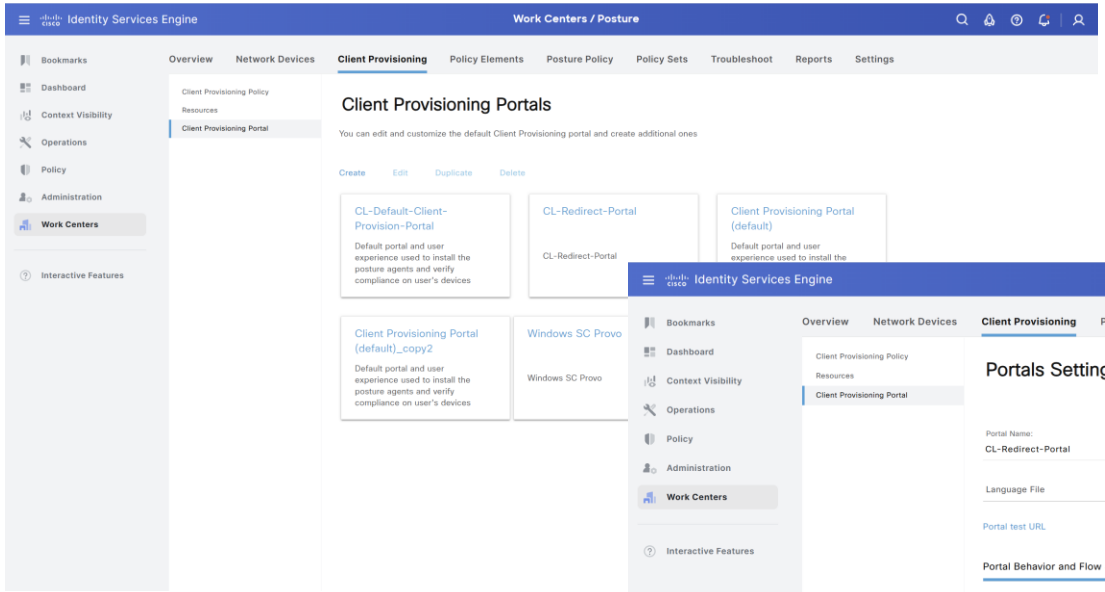
Posture Deployment – Add Policy Elements

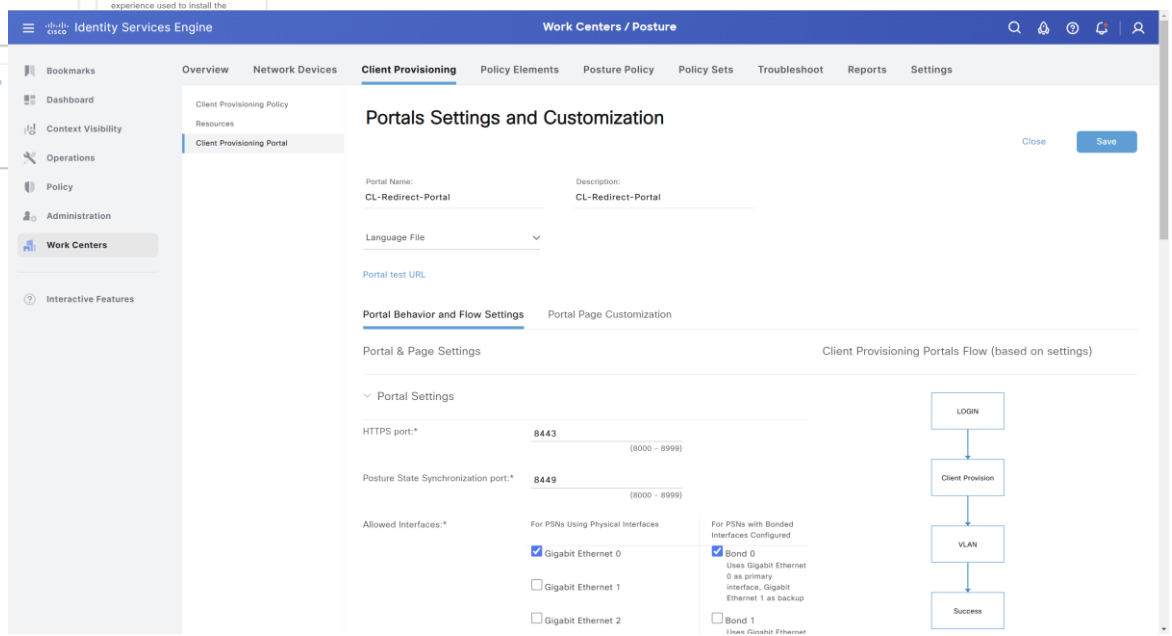


Catalyst Centre added the ACL to the Switch!



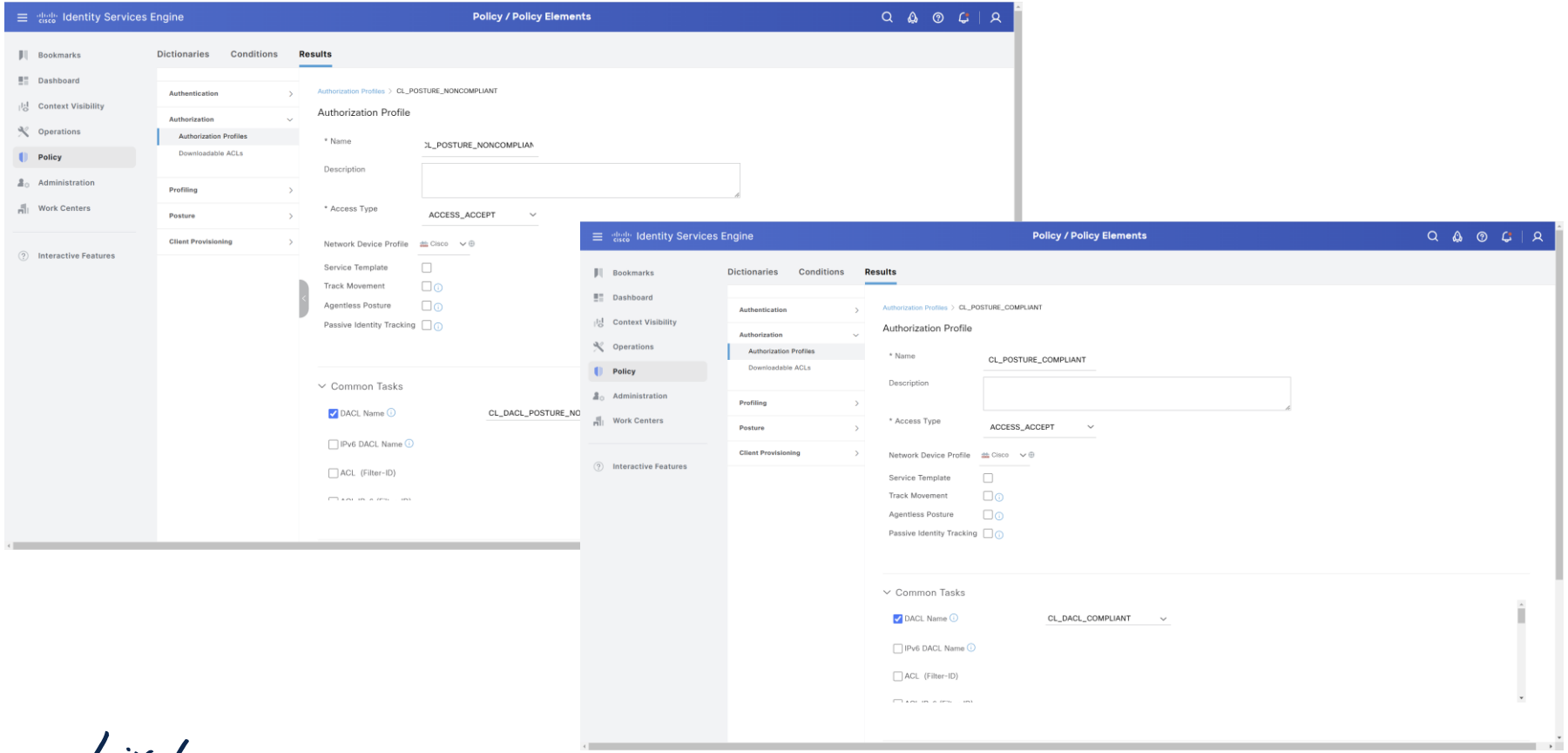
Posture Deployment – Create Client provision portal



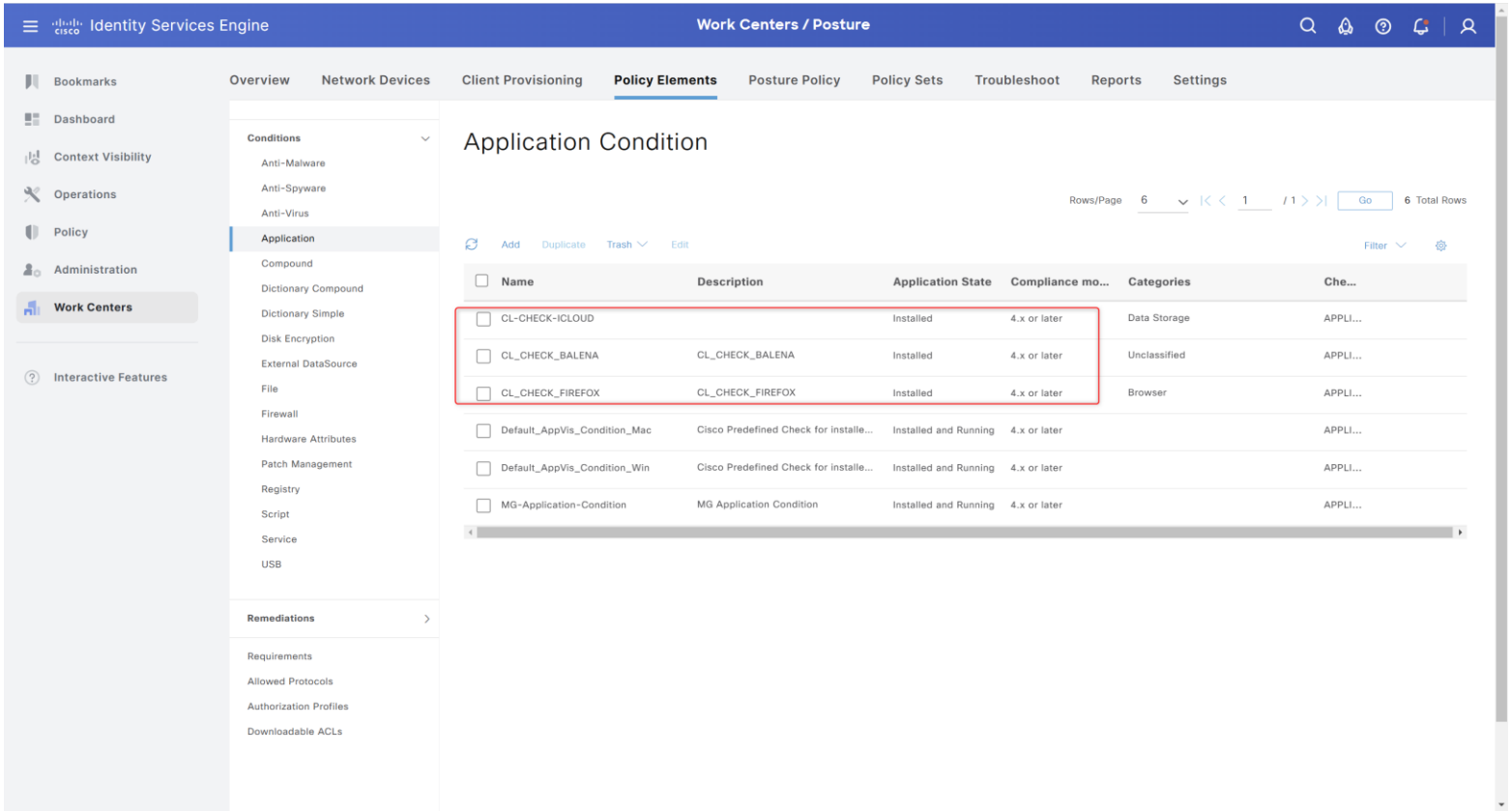


Use the one already in ISE!

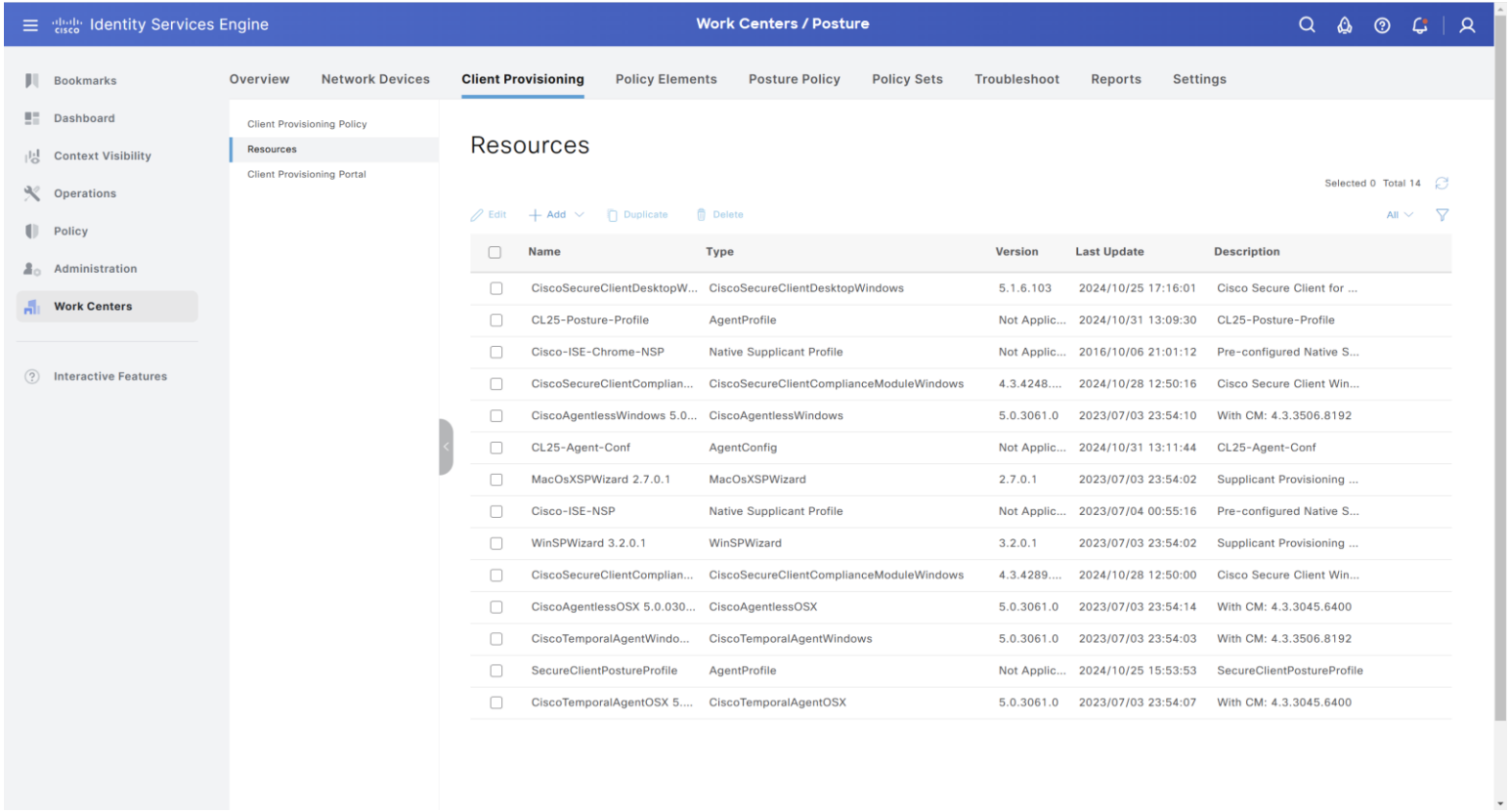
Posture Deployment – Create rules for Compliant and Non Compliant



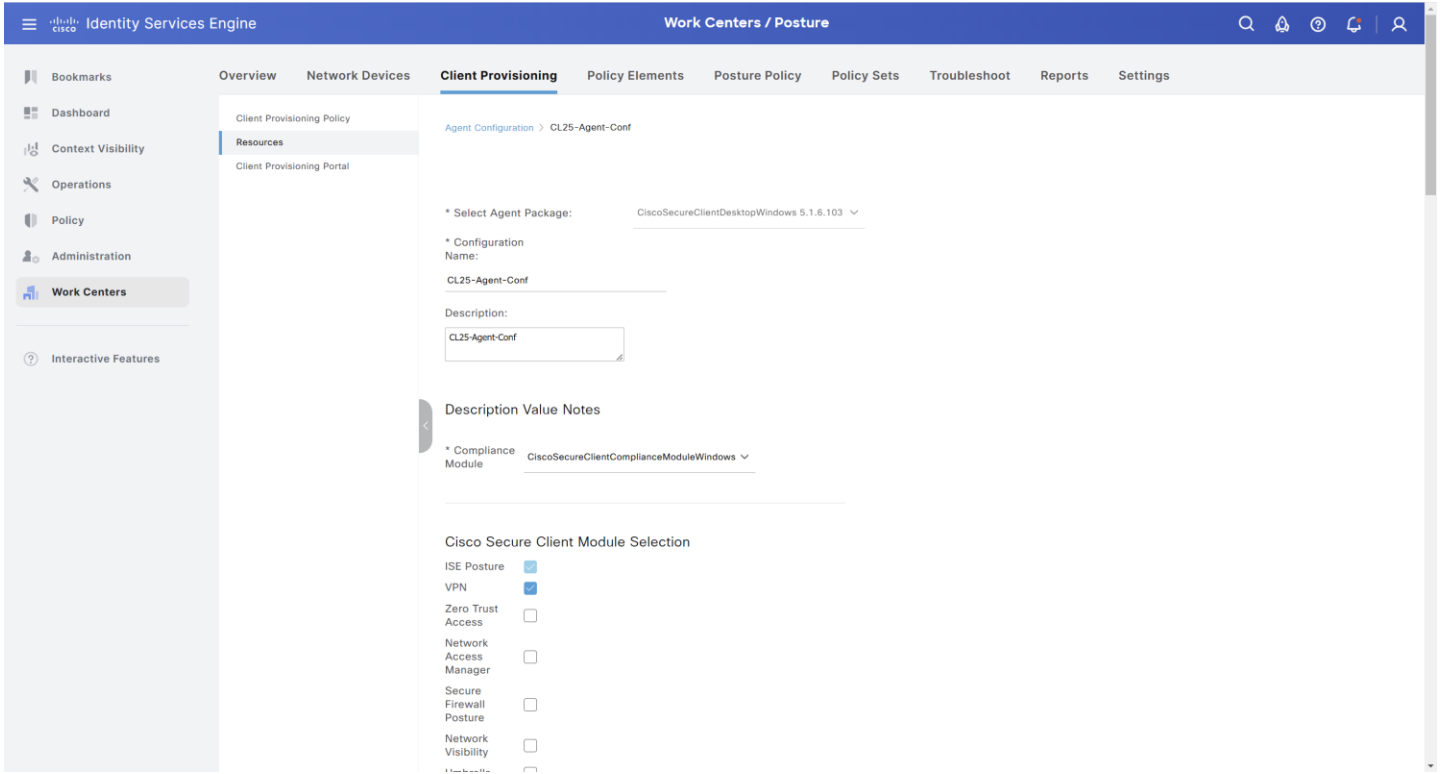
Posture Deployment – Create Some Conditions!



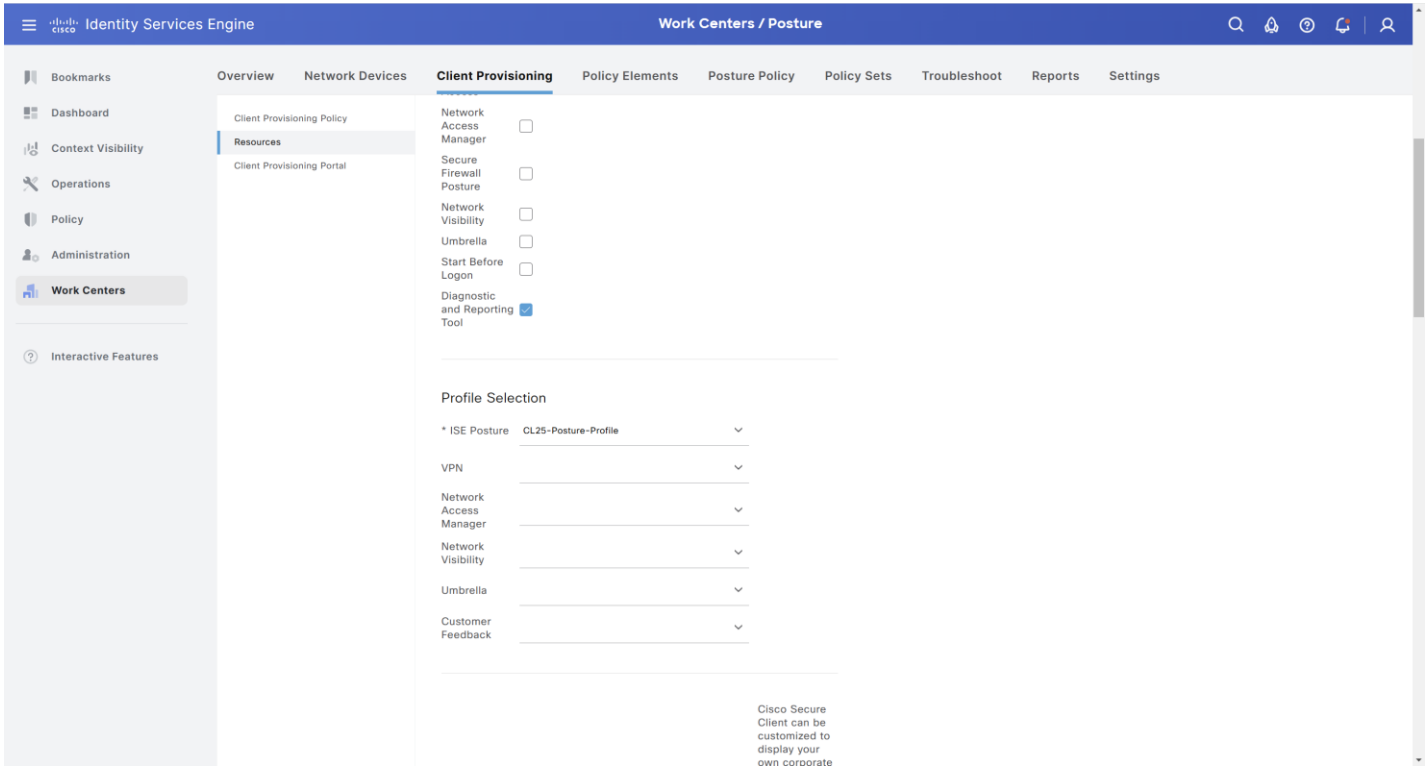
Posture Deployment – Check Resources



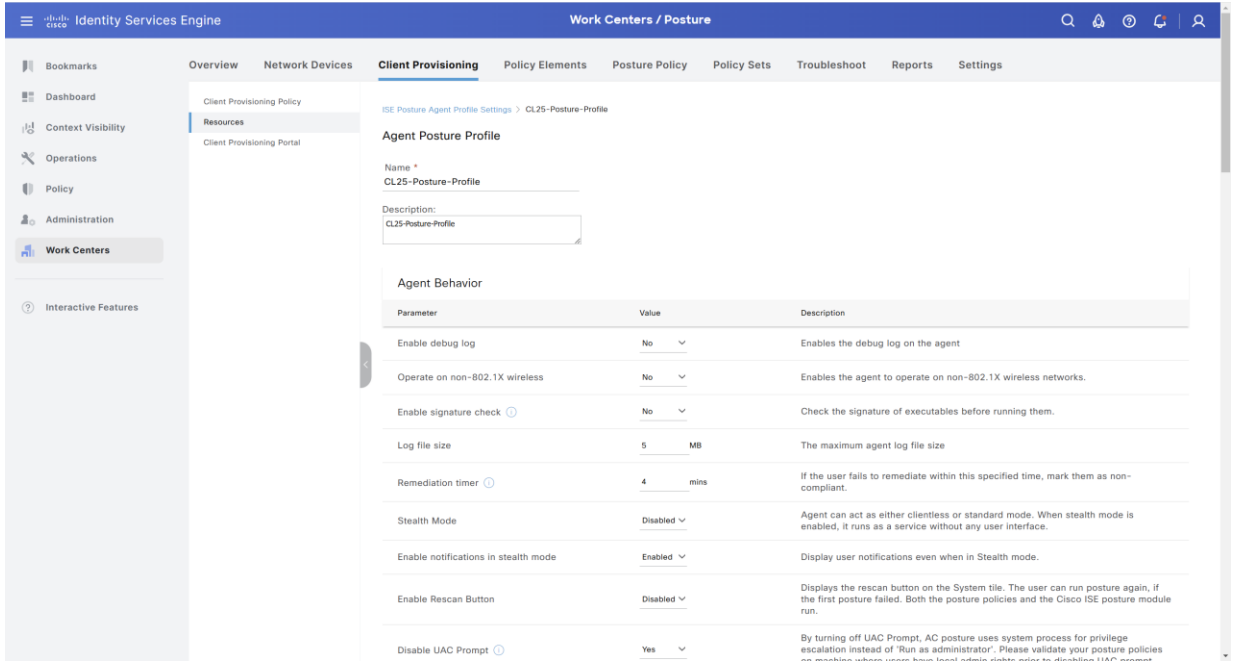
Posture Deployment – Add Agent Configuration



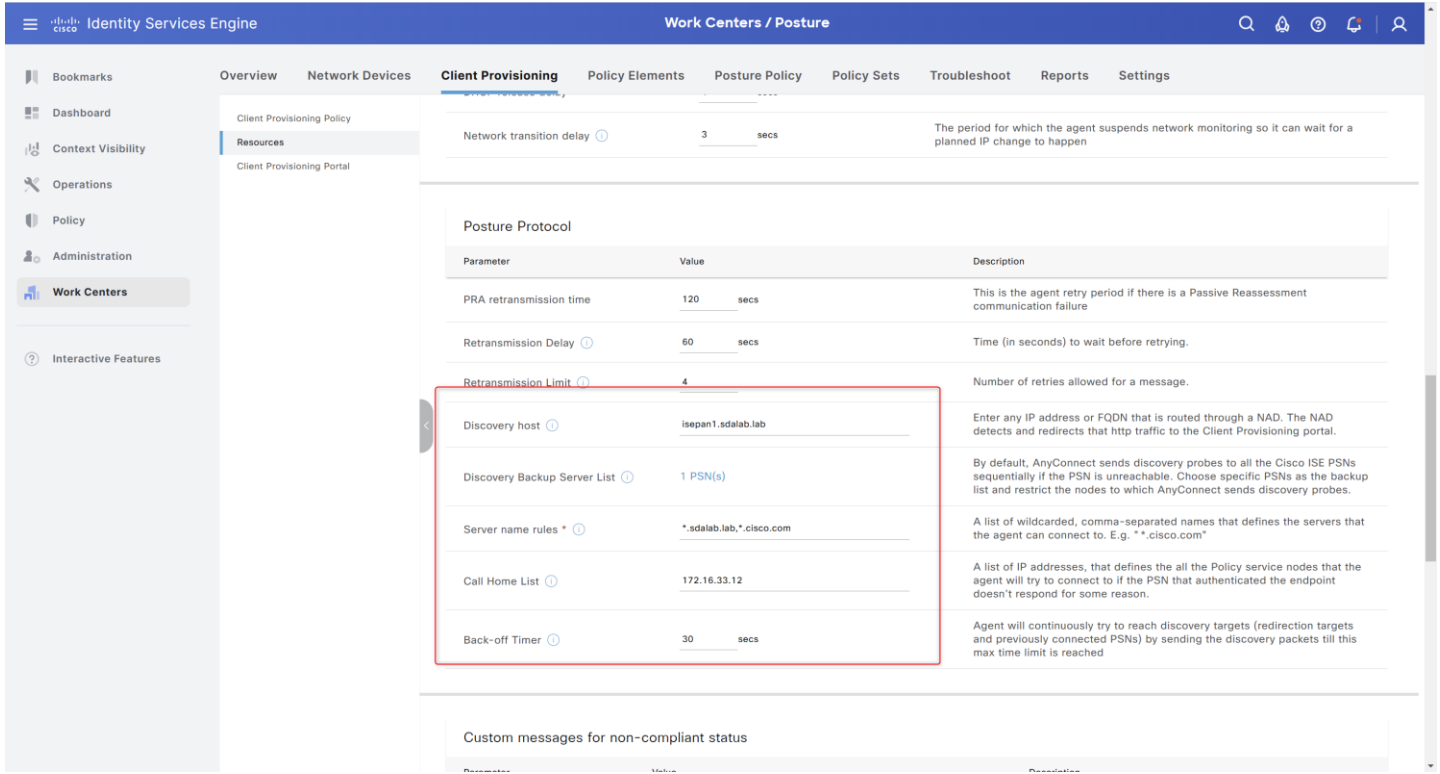
Posture Deployment – Add Agent Configuration



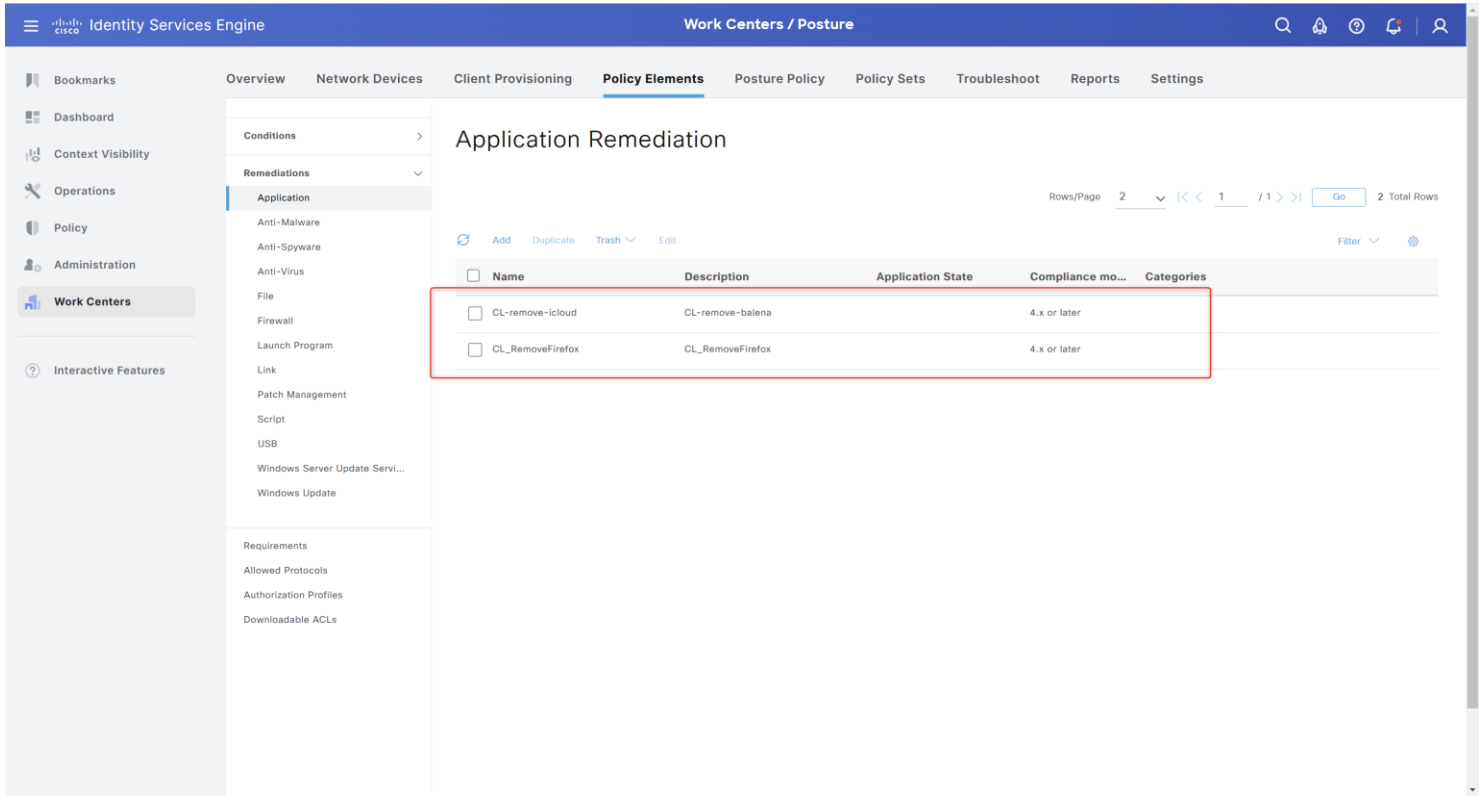
Posture Deployment – Add Agent Posture profile



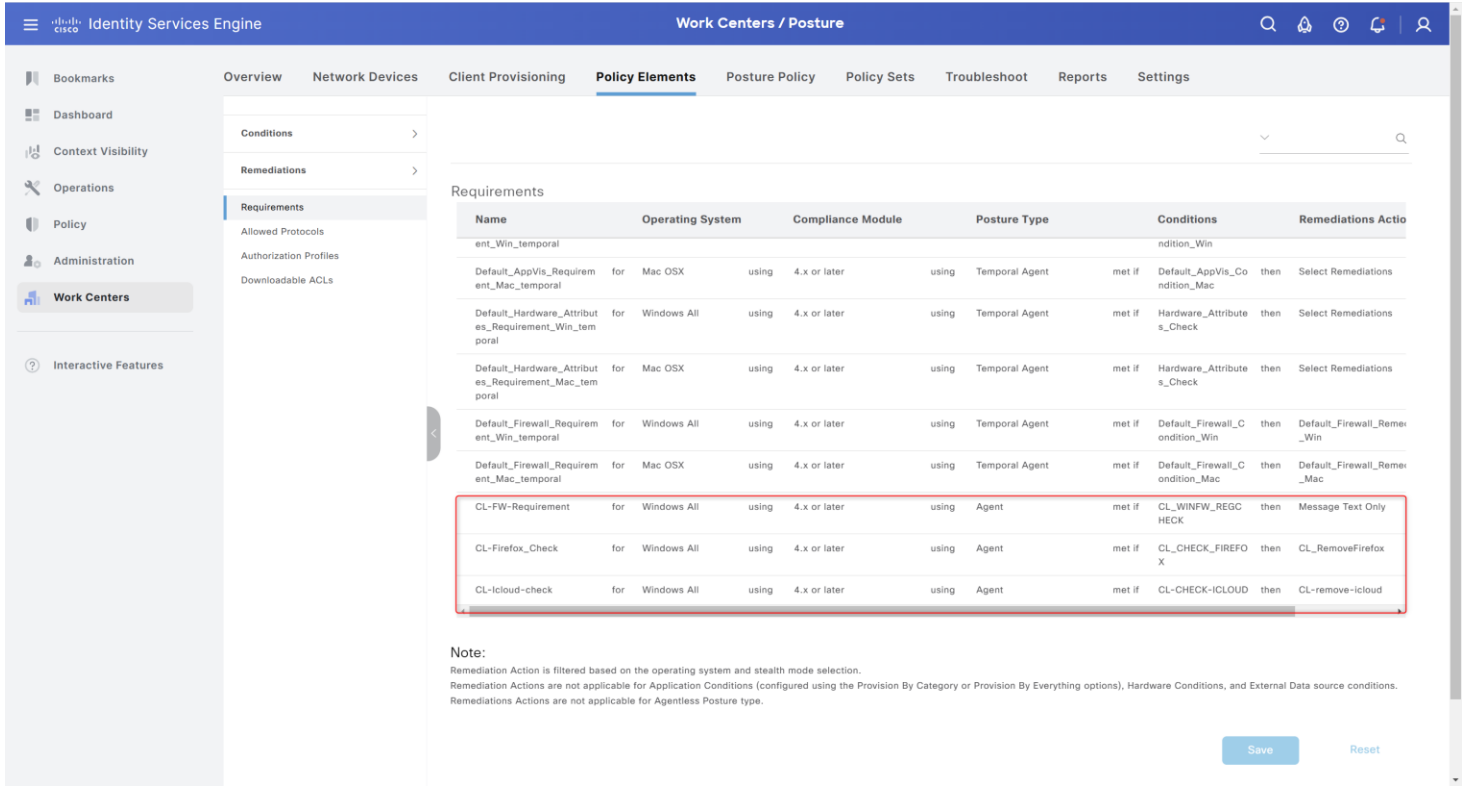
Posture Deployment – Add Agent Posture profile



Posture Deployment – Add Remediations

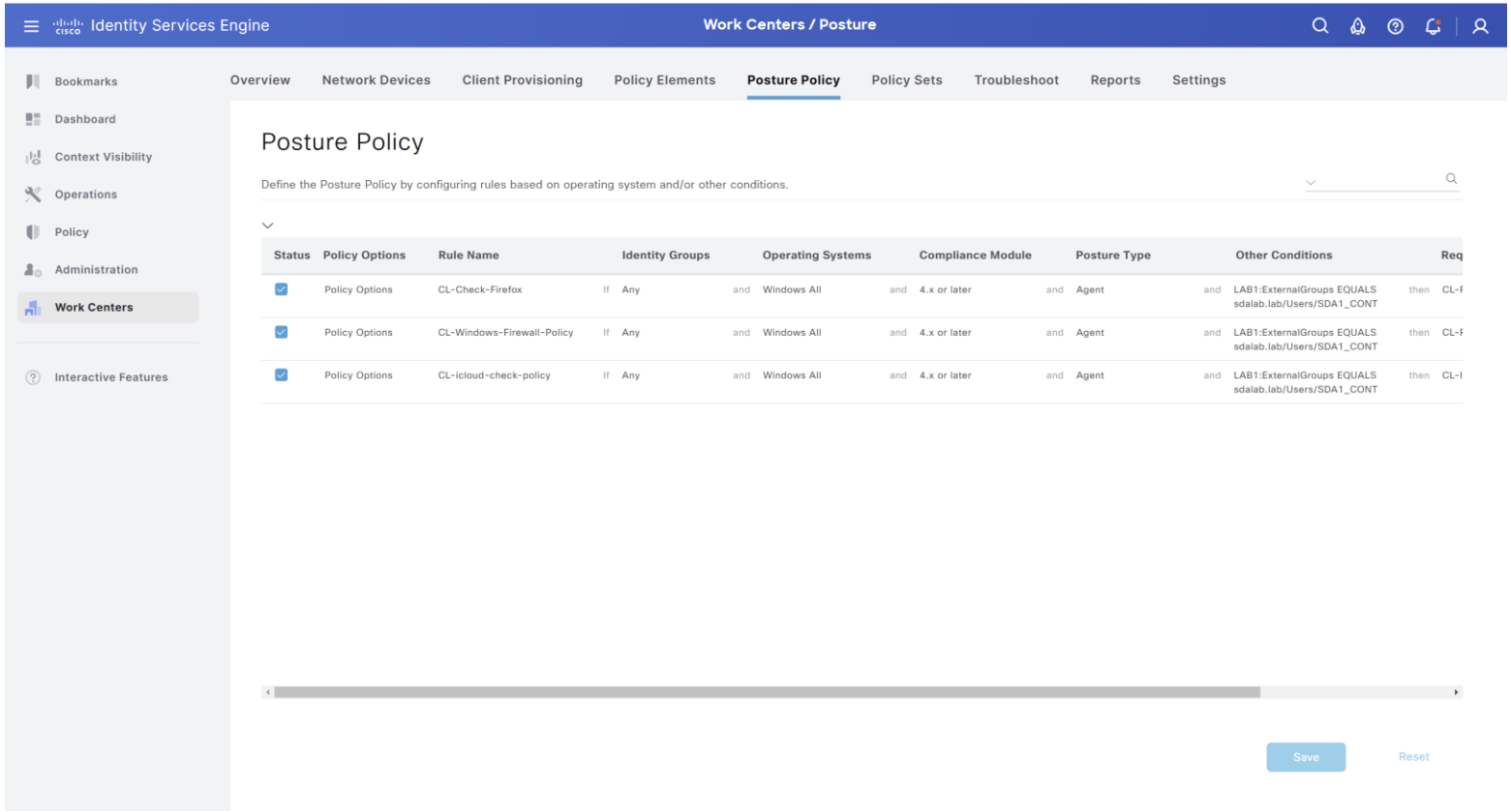


Posture Deployment – Add Requirements

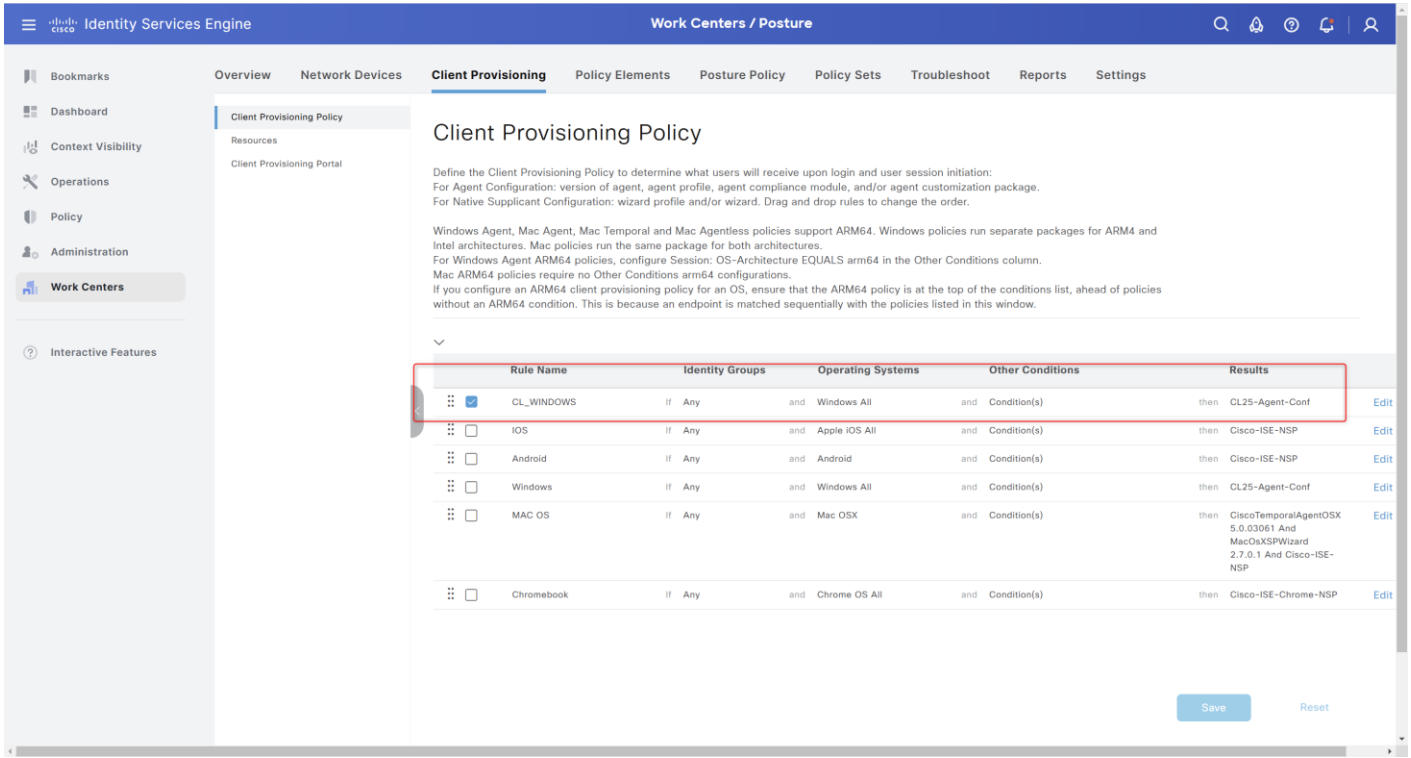


This ties it together

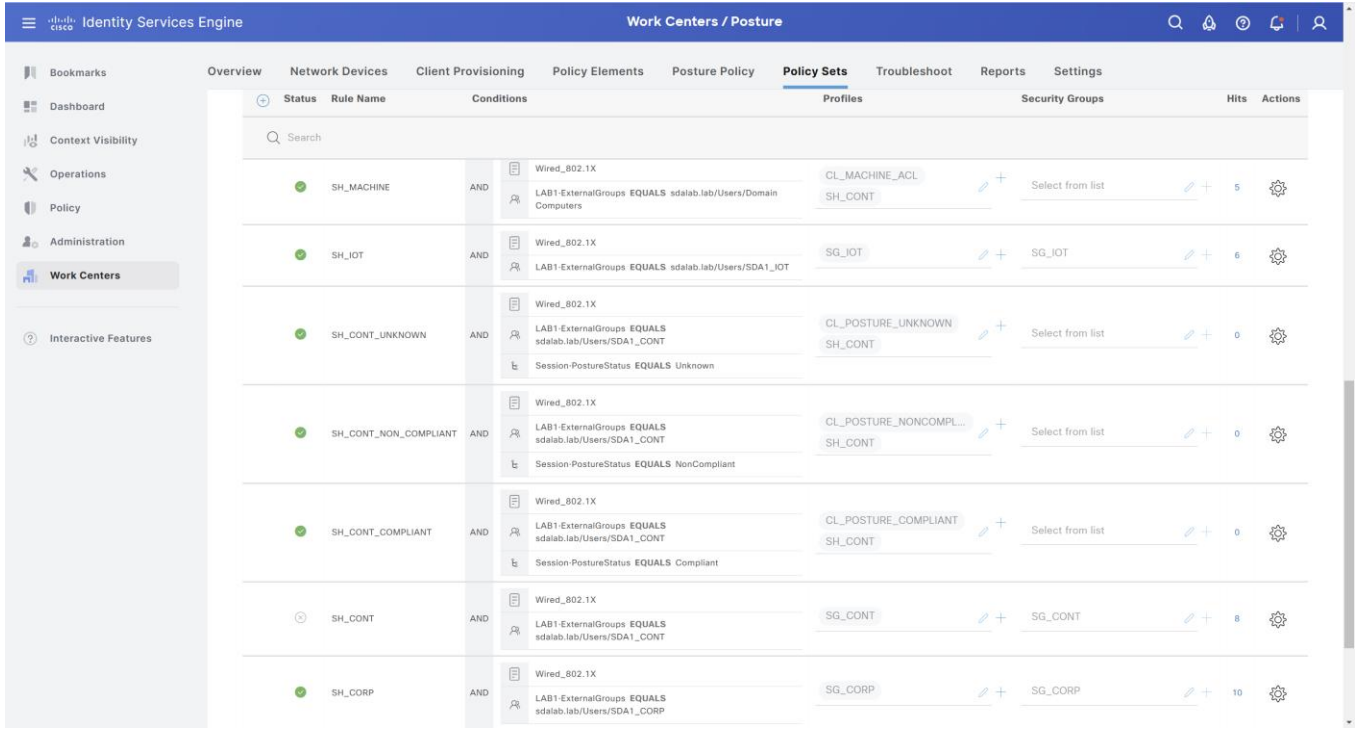
Posture Deployment – Add Posture Policy



Posture Deployment – Client provisioning

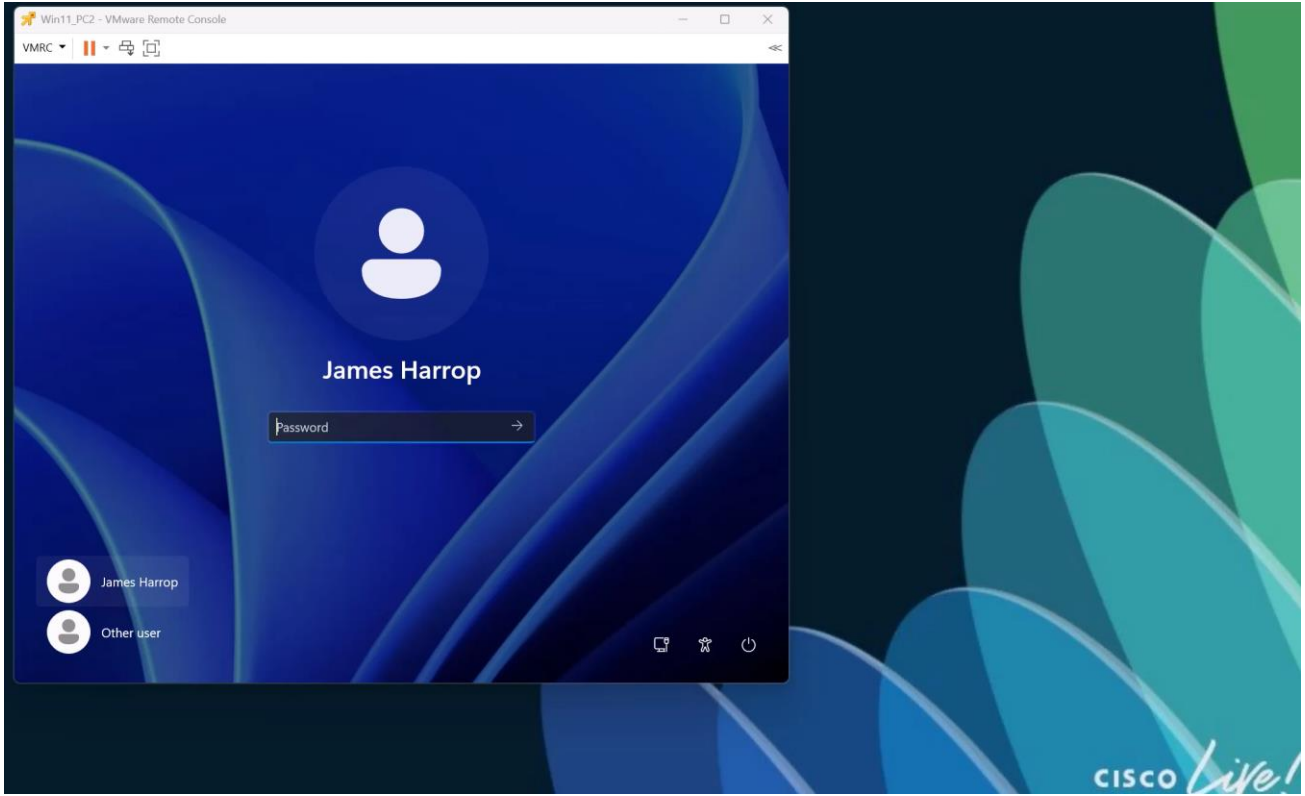


Posture Deployment – Client provisioning

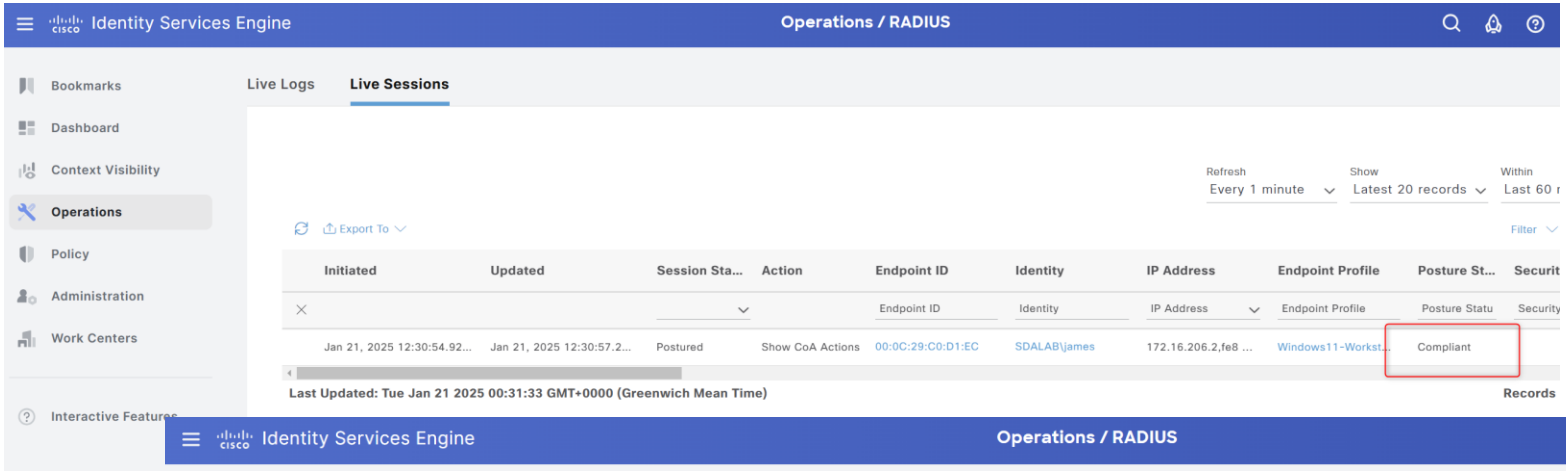


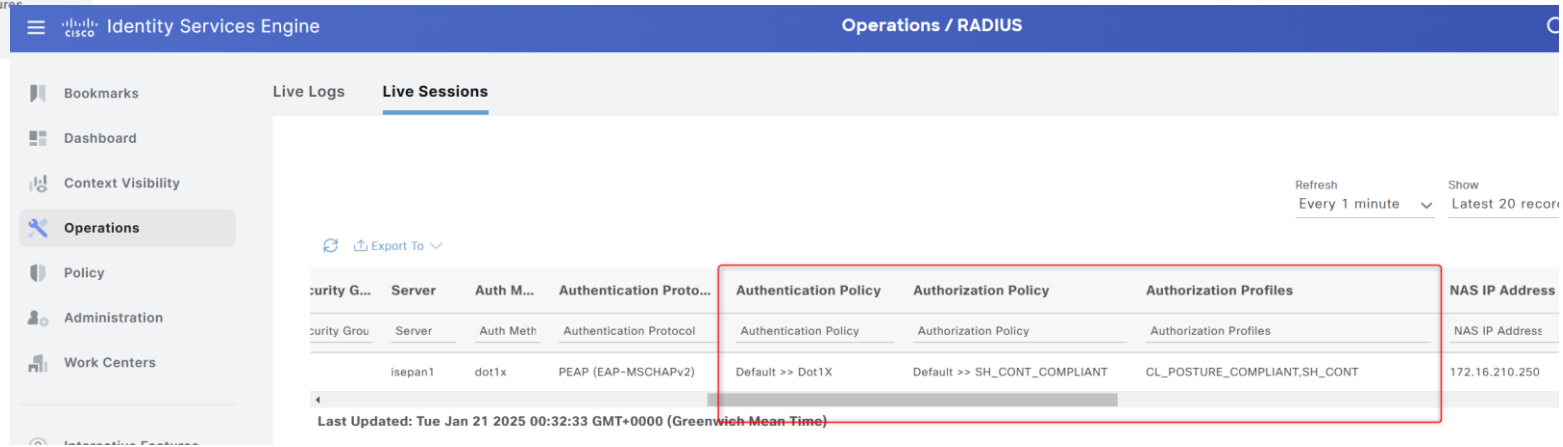
Enable Posture AuthZ rules

Posture Deployment – Posture in Action – Demo



Posture Deployment – see the result!





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 bpdufilter 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
!
```

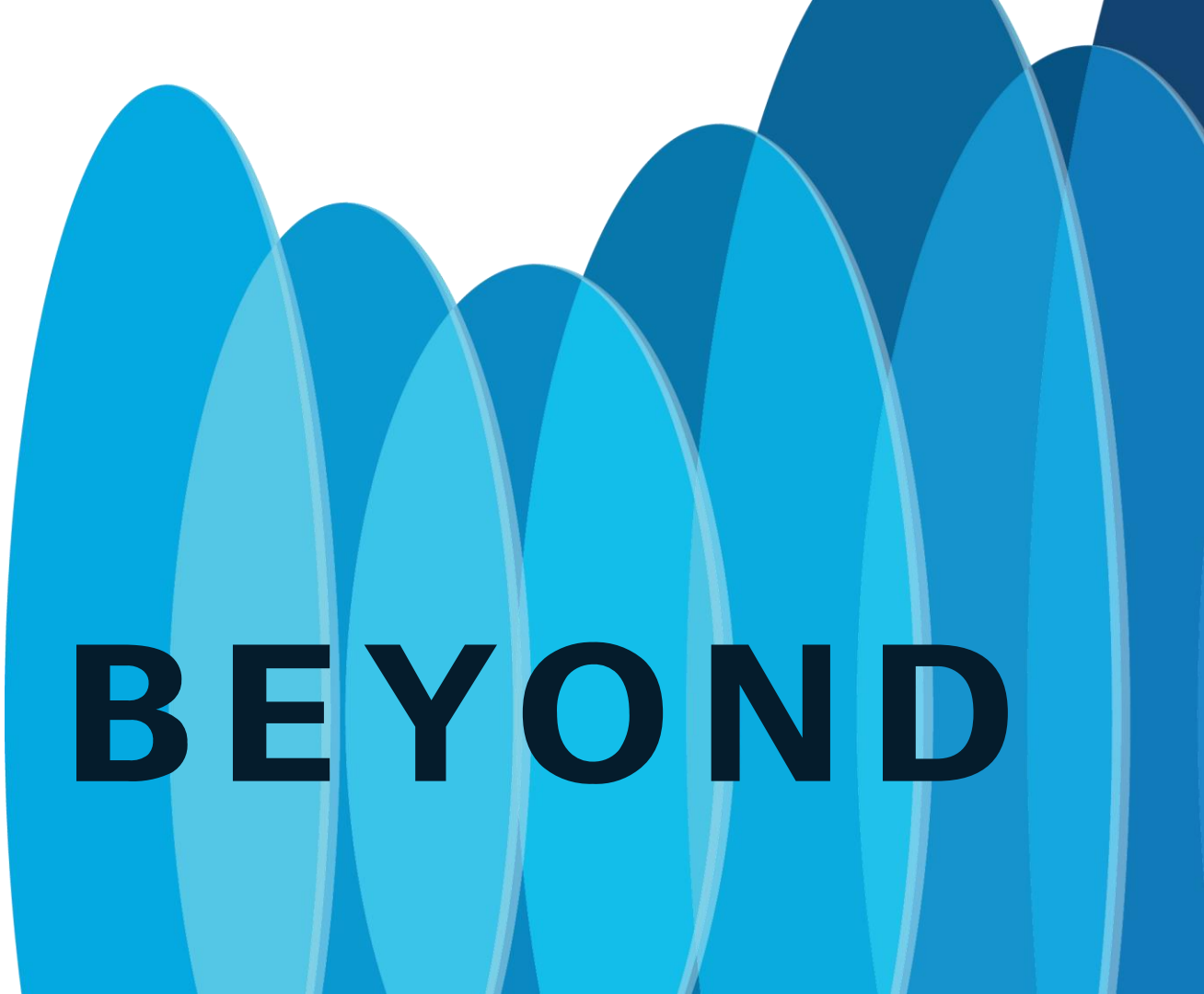
```
! Configure policy maps
! Policy map applied to all Dot1xMAB interfaces
policy-map type control subscriber Dot1x-Default
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x priority 10
 event authentication-failure match-first
  5 class Dot1x_Failed 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 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


! 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 bpdufilter 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