Setting the Stage for ISE Deployment Success:

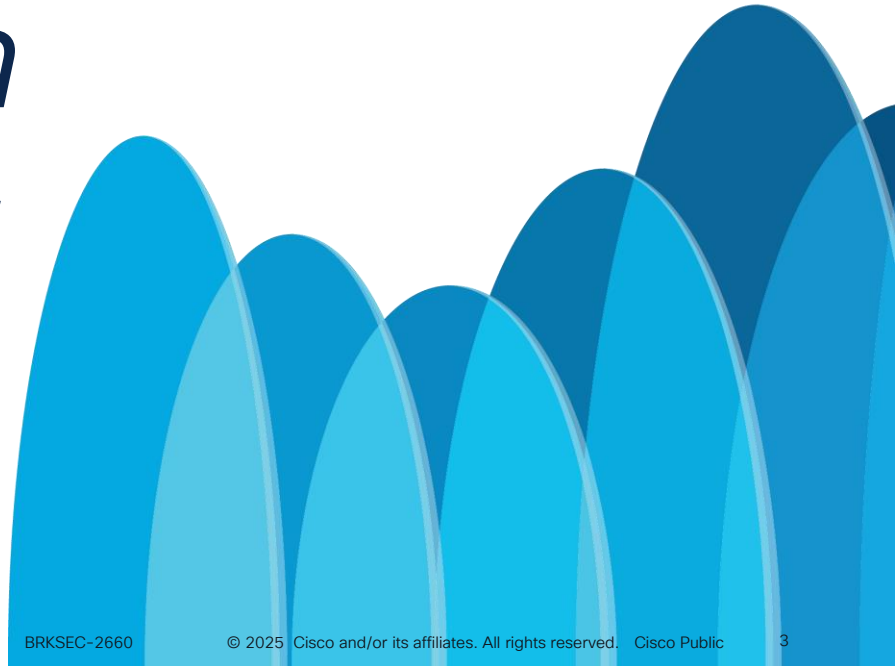
A Guide to Effective Planning

Francesca Martucci
Technical Solutions Architect – Cybersecurity EMEA

BRKSEC-2660

“A goal without a plan is just a wish”

Antoine de Saint-Exupéry



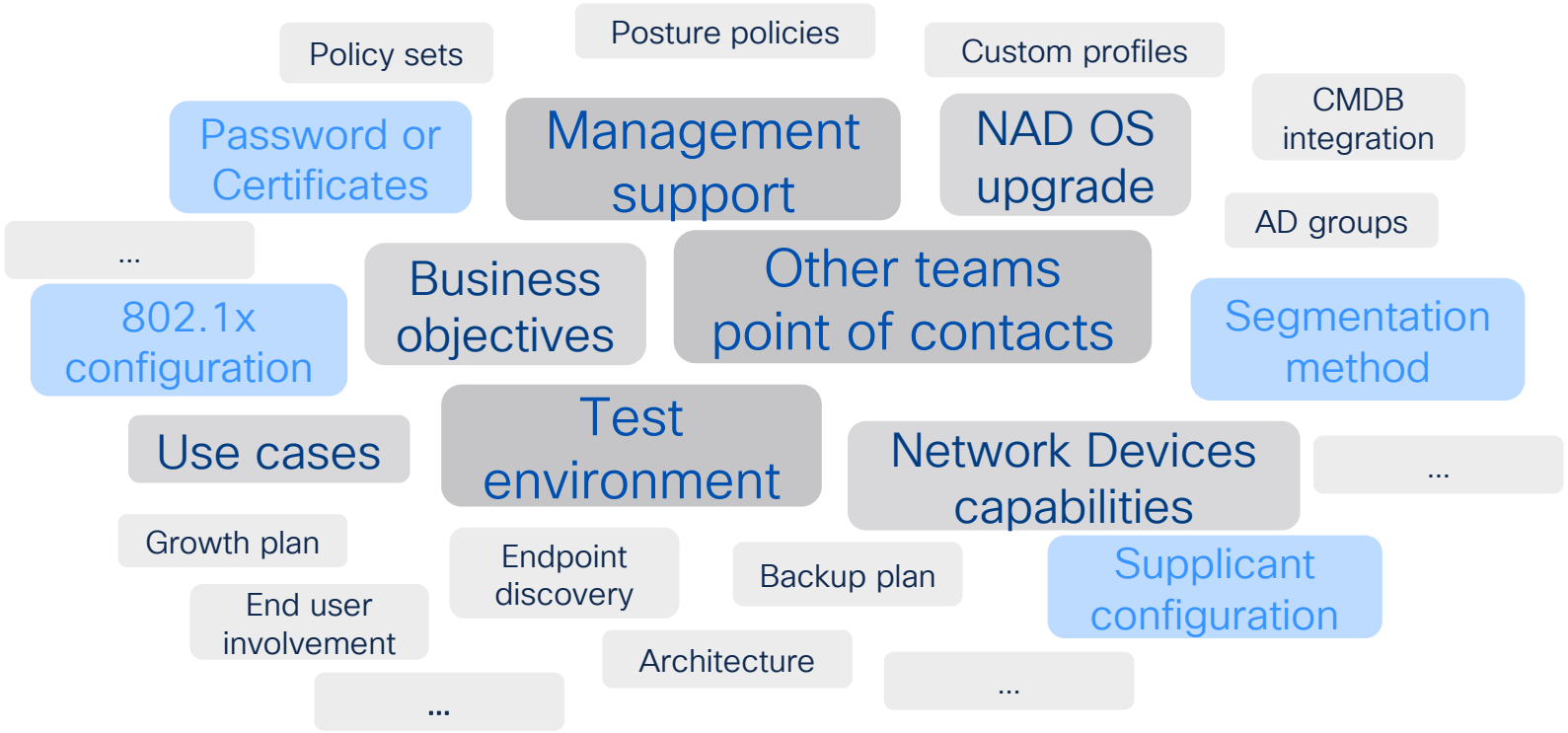
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deploying any network access control solution is crucial

but it isn't easy....

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What needs to be included in my planning?



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to a successful deployment.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

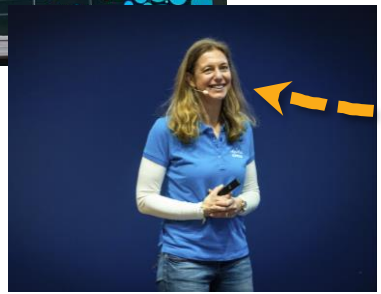
Who am I?

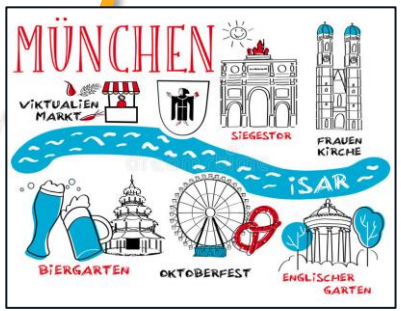
- Technical Solutions Architect
  Cyber Security EMEA
- In Cisco since 25 years...

  ... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security





© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco ISE High Level Design

- Business Objectives
- Environment
  (Network Device vendor, supplicants, PKI)
- Scenarios & Use Cases
  (Posture, BYOD, Device Administration)
- Policy Details
  (External Identity Sources, what type of posture what type of BYOD
- Operations & Management
- Scale & High Availability

ISE High Level Design (HLD)

AAA · AnyConnect · Identity Services Engine (... · Policy and Access · TrustSec · VPN

48001 VIEWS · 77 HELPFUL · 0 COMMENTS

thomas

05-07-2018 09:40 AM
Edited On: 02-04-2021 01:42 PM

Introduction

An ISE High Level Design (HLD) is recommended to assist you with the design and planning of your ISE deployment. Having a clearly written security policy – whether aspirational or active – is the first step in assessing, planning and deploying network access security. Without this, it is hard to break down the deployment into phases by location or capabilities. When seeking outside help, the HLD provides a huge time savings for education other teams, partners, Cisco Sales representative, Technical Assistance Center (TAC) representative or even the ISE product and engineering teams. Clearly state the desired solution capabilities, hardware and software environment and integrations can quickly allow people to understand what you want and how to configure it or troubleshoot it.

Business Objectives

Identify the Customer Business Objectives that ISE must solve. Typically this involves regulations and compliance or identified security threats and risks to smooth operation of the business or brand. But it also involves mitigating risks with controlled network access for everyday IT processes. This is how you begin to craft your network access control policy. The more specific you can be, the better.

Consider the following example business objectives that must translate into access control policy :

- We want to provide sponsored guest access to our visitors
- All network device administration commands must be authorized and logged for potential audit
- We want to identify all endpoints on our network so we can begin to apply access control policies
- We do not want our employees personal devices on our corporate network
- We want our employees to any device they want but we want to manage it to ensure it and any information on it is properly secured
- Printers should only talk to print servers
- We need to be able to re-image our workstations over the network via PXE
- We must comply with [PCI, HIPAA, etc.] regulation
- All Windows devices must be patched within the last 30 days to minimize known vulnerabilities
- We want to automatically quarantine endpoints when [Stealthwatch, AMP, etc.] detects malicious behavior

Business Objectives

Agenda

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What not to expect:

- Specific ISE use cases and their implementation
- Detailed configuration guidelines
- Troubleshooting information
- Licensing

This presentation has many links to resources helping with most of them

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Webex App

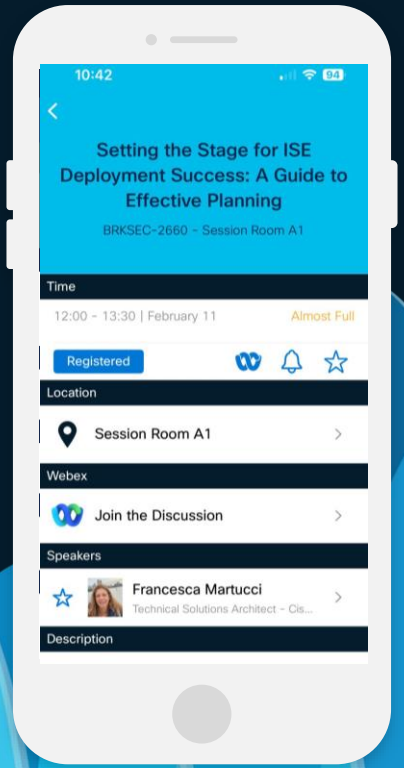
Questions?

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

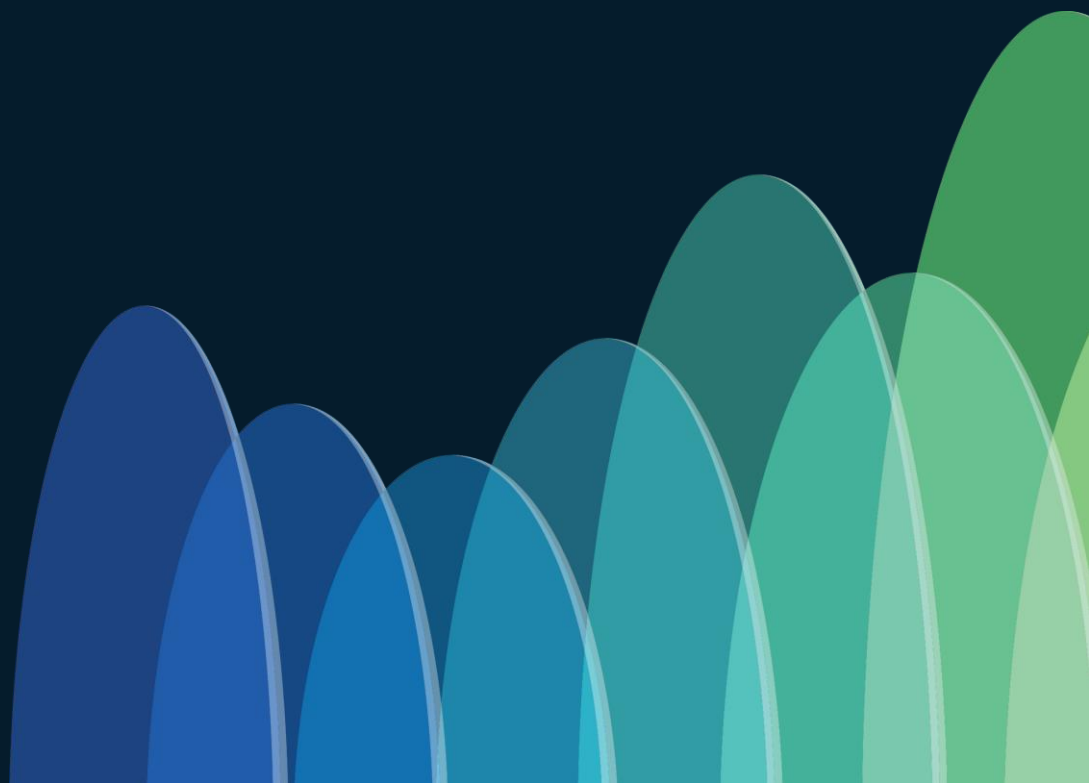
Webex spaces will be moderated by the speaker until February 28, 2025.



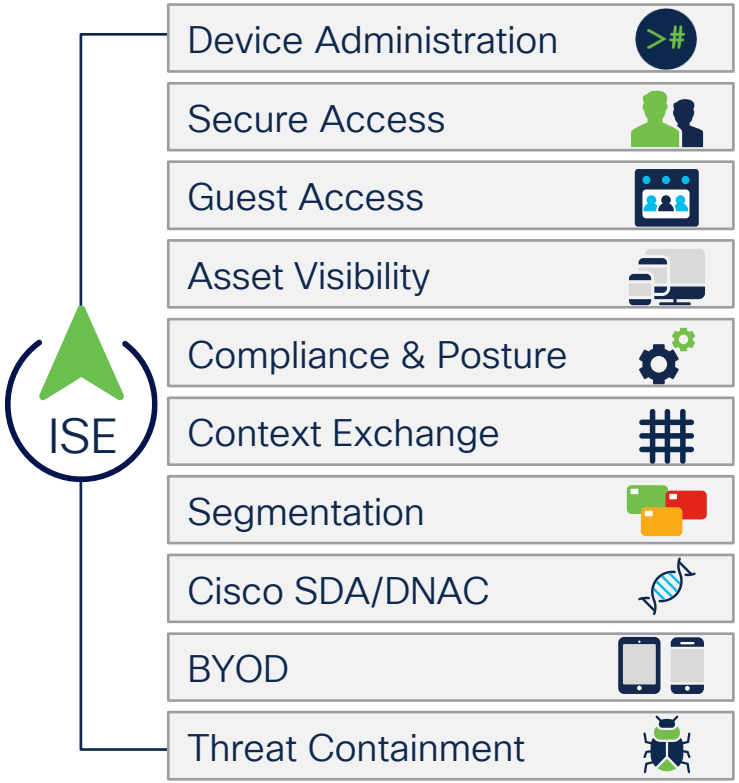
cisco Live!

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where To Start: planning
  - ISE Deployment Options
  - Certificates
  - Network Devices
  - Supplicants
  - Profiling
  - Policies optimization
  - Create your own lab
  - 802.1x Deployment Modes



What are your business priorities?



What is the business trying to accomplish with ISE?

Profiling is critical with today IoT proliferation

Do you need a BYOD policy?

From where do you want to start?

Which use cases could be considered for the future?

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Defining your Security Policy

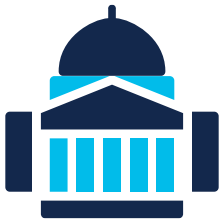
What is an IT security policy?

"It identifies the rules and procedures for all the individuals accessing and using an organization's IT assets and resources."

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Everyone Has Different Needs

Government



Financials

Healthcare

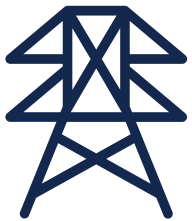
Retail

Education

Transportation

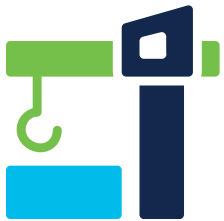
Services

Utilities



Technology

Manufacturing



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Understand Your Needs and Use cases

Objectives / Risk / Priorities

- Brand Trust
- Customer/Patient Data
- Hospitality: Fast & Easy
- IT/OT Segmentation
- Protect Intellectual Property

Environment

- Wired / Wireless / VPN
- Multi-Vendor
- Hardware & Software
- Network Device Capabilities

Scaling

- Concurrent Active Endpoints
- Scale Horizontally
- Scale Vertically
- Geography

Management & Operations

- Top Down / Bottom Up?
- Org(s) / Regions / Departments
- Collaboration or Siloes
- Scheduling Config Changes
- Tooling & Automation

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Example of your ISE policy planning

Endpoint Type	Authentication	Identity Store	Network Access	Enforcement	Staging / Provisioning
Corp PC	802.1X – Cert	ISE Cert Store	Full Access	VLAN CORP	Physical Staging Port
Guests	WebAuth	ISE Guest DB	Internet-Only	VLAN Guest	Manual Connect Sponsored account
Access Point	802.1X – User/Pass	ISE User DB	Trunk	Trunk	AP Provisioning
AP Provisioning	MAB	ISE MAC Whitelist	WLC-Only	VLAN AP	ISE Profiling
Printers	MAB	ISE MAC Whitelist	Print Servers-Only	VLAN Printers	ISE Profiling

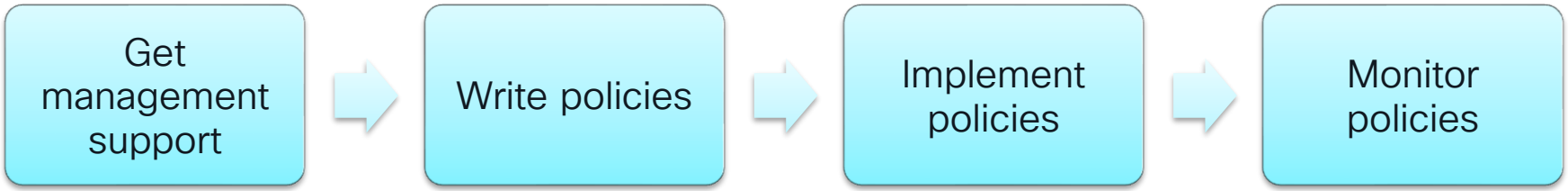
Endpoint Team Network Team Security Team

Remember: do not think only at positive outcome.
What if a corporate PC certificate is expired?

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

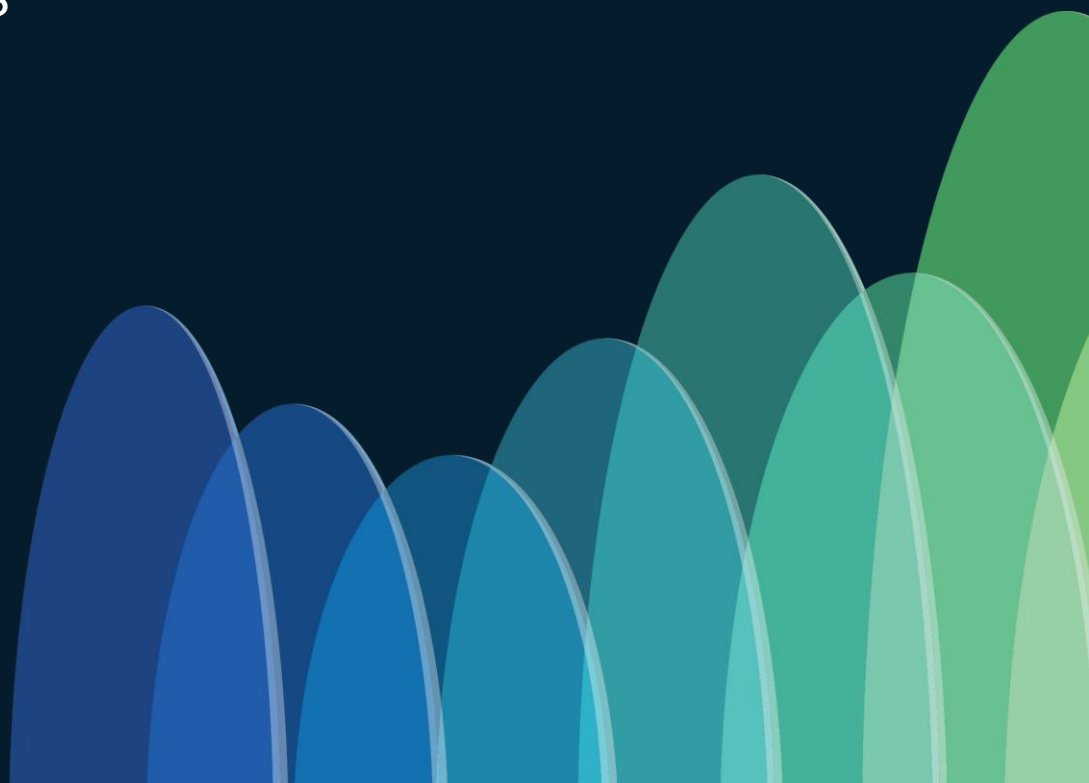
Interoperation with other teams

- Management buy in is critical to have support of your decisions
- Get the right contacts in the other teams ahead of time
- Monitor and update polices with your IT Security Policy



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- **ISE Deployment Options**
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



ISE Personas

Policy Administration Node (PAN)

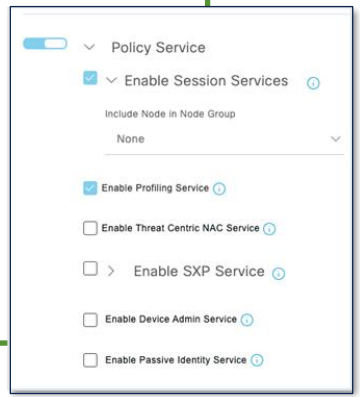
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

Monitoring & Troubleshooting Node (MNT)

- Receives logs from all nodes
- Handles remote logging targets
- Generates summary Dashboard Views
- Performs scheduled reports
- Handles reporting and API queries

Policy Service Node (PSN)

- TACACS requests
- RADIUS requests
- Endpoint profiling probes
- Identity store queries
- Hosts Guest/BYOD portals
- MDM/Posture queries
- TC-NAC & SXP services

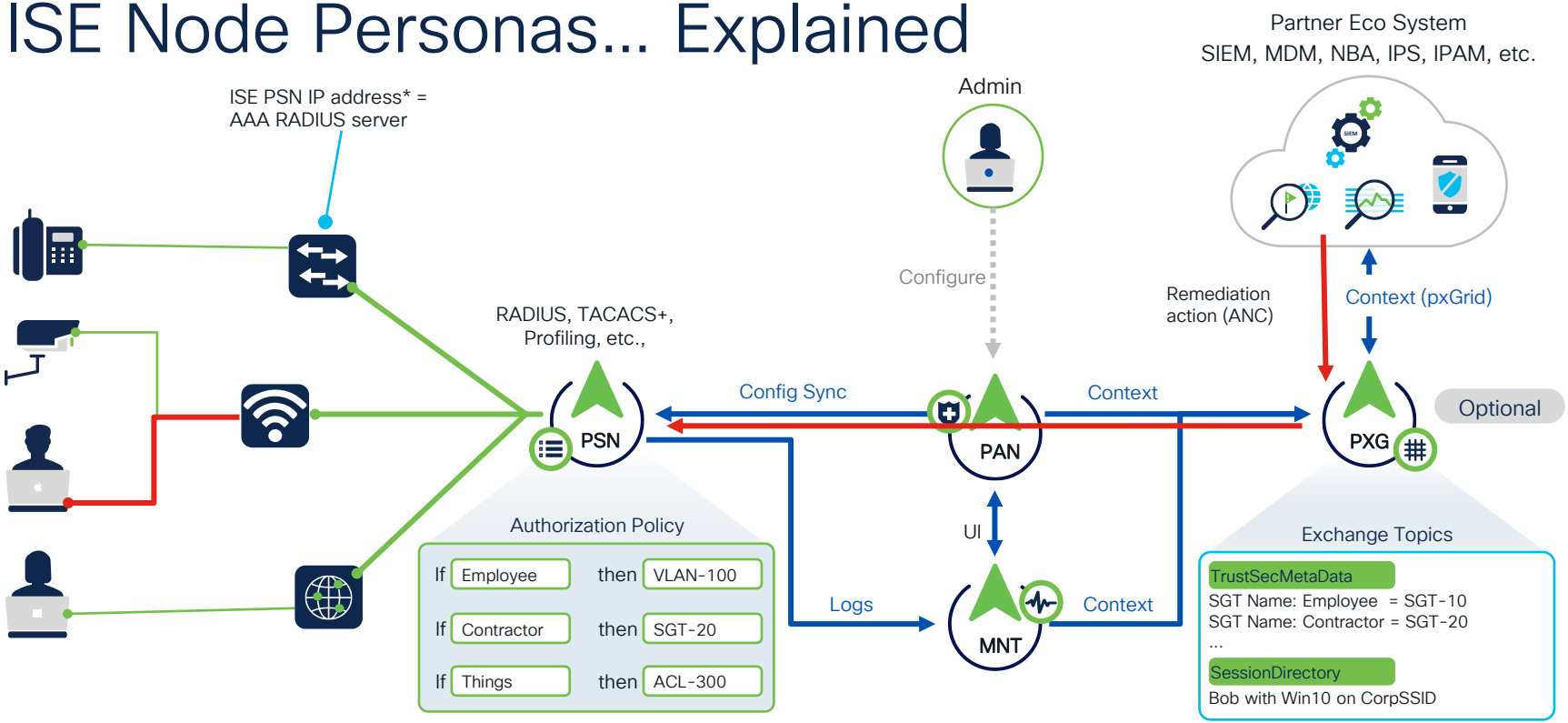


Platform Exchange Grid Node (PXG)

- Runs pxGrid controller
- Authorizes pxGrid Pubs/Subs
- Publishes pxGrid topics to subscribers
- Handles ANC/EPS requests
- REST APIs

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Node Personas... Explained



*PSNs can optionally be behind a load-balancer and can be accessed via Load Balancer Virtual IP address (VIPs)

ANC = Adaptive Network Control

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Architecture

Standalone ISE

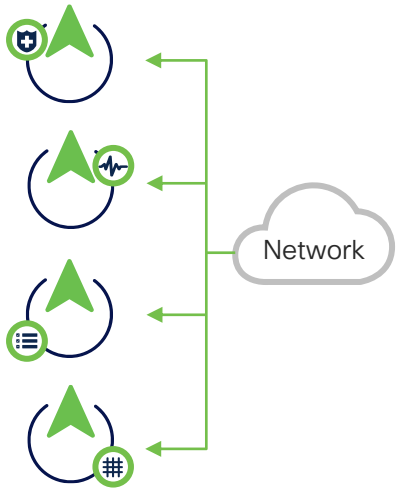
Policy Administration Node (PAN)
- Max 2 in a deployment

Monitoring & Troubleshooting Node (MnT)
- Max 2 in a deployment

Policy Services Node (PSN)
- Max 50 in a deployment

pxGrid Controller
- Max 4 in deployment

Distributed ISE



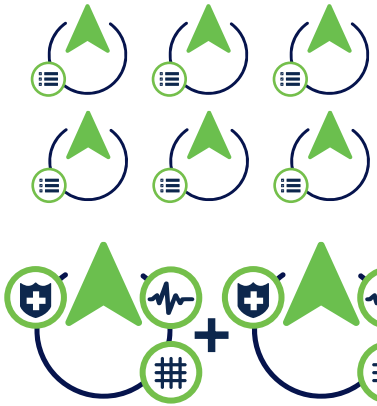
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Scaling

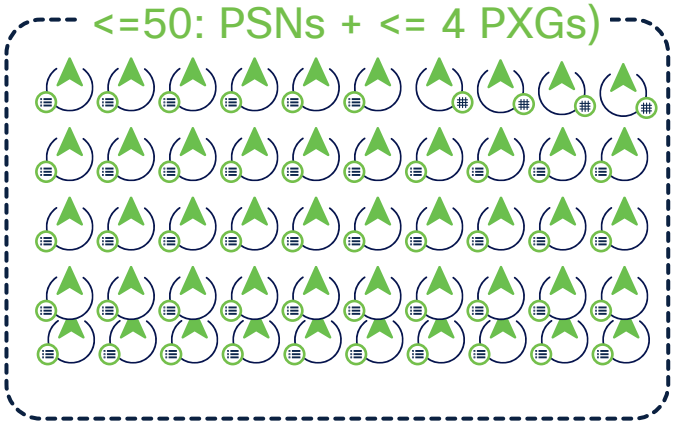
Lab and Evaluation

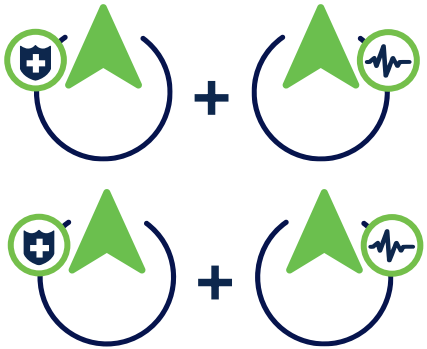
Only for Lab use (no HA)
Max 100 endpoint

Small HA Deployment
2 x (PAN+MNT+PSN)+ Extra PSN



Medium Multi-node Deployment
2 x (PAN+MNT+PXG), <= 6 PSN





Large Deployment
2 PAN, 2 MNT, <=50: PSNs +
<= 4 PXGs

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Total Maximum Concurrent Active Sessions

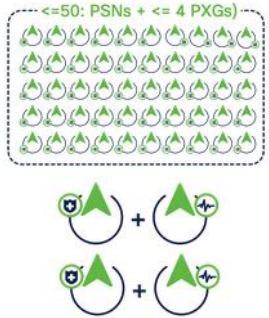
Cisco ISE

Deployment Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Large deployment	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium deployment	10,000	75,000	20,000	25,000	150,000	50,000	150,000
Small deployment	10,000	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

Medium Deployment

Large Deployment



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

PSN Maximum Concurrent Active Sessions

cs.co/ise-scale

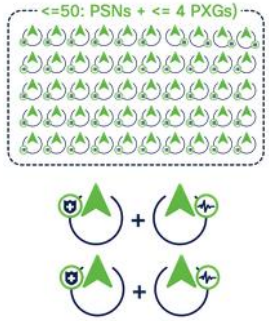
Cisco ISE

PSN Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Concurrent active endpoints supported by a dedicated PSN (ISE node has only PSN persona)	25,000	50,000	40,000	50,000	100,000	100,000	100,000
Concurrent active endpoints supported by a shared PSN (ISE node has multiple personas)	12,500	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

Medium Deployment

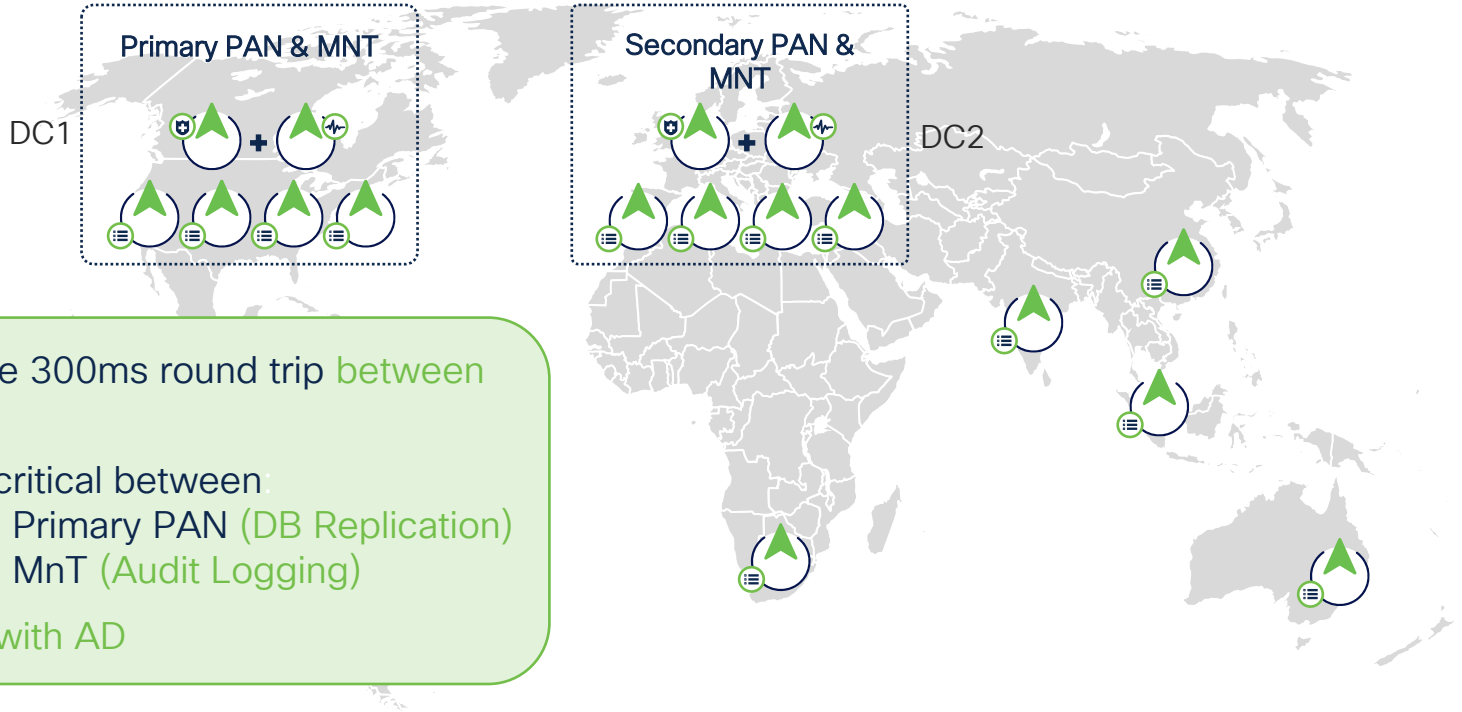
Large Deployment



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Fully Distributed Architecture

Centralize in DCs…or Distribute PSNs across Geographies



- Latency should be 300ms round trip between PAN and PSN
- Bandwidth most critical between:
  - PSNs and Primary PAN (DB Replication)
  - PSNs and MnT (Audit Logging)
- Co-locate PSNs with AD

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Nodes – Mix and Match

Physical Appliances	Virtual Machines	Cloud Instances

SNS-3715
SNS-3755
SNS-3795

SNS-3615
SNS-3655
SNS-3695

KVM

Microsoft

NUTANIX

vmware

aws

Azure

OCI

Cisco Live 2025
FOR REFERENCE
BRKSEC-2660

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reminders
ISE platforms

SNS 3615
SNS 3655
SNS 3695

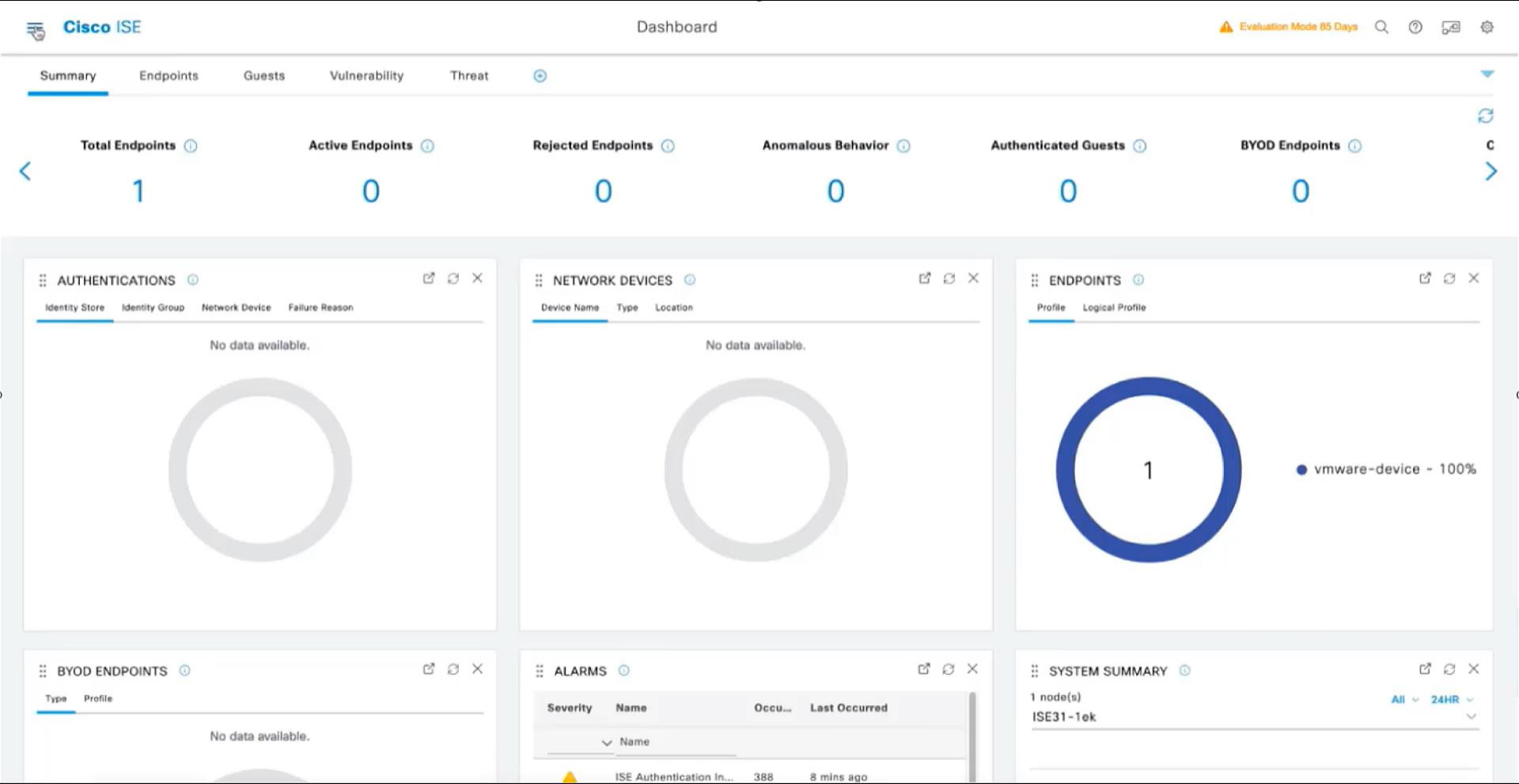
EOL

SNS 3715
SNS 3755
SNS 3795

Traditional VM
AWS
Azure & OCI

Cisco Live 2025
FOR REFERENCE
BRKSEC-2660

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

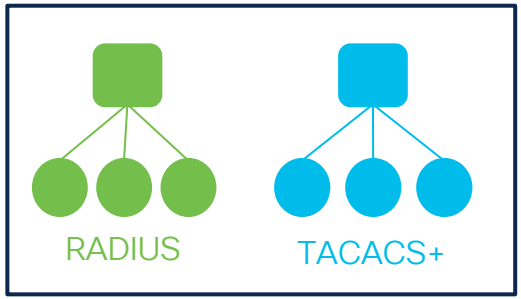


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

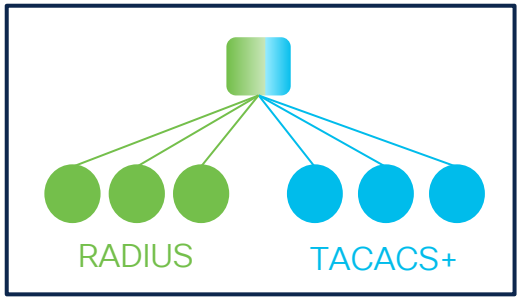
TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

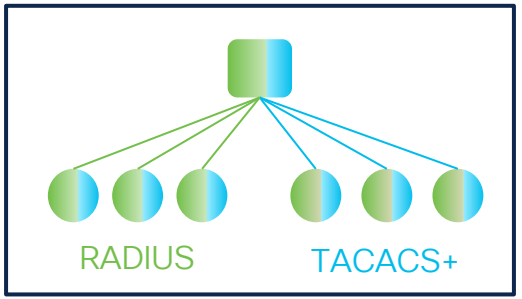
There are three different options:



Separate ISE cubes



Mixed ISE cube with separate PSNs

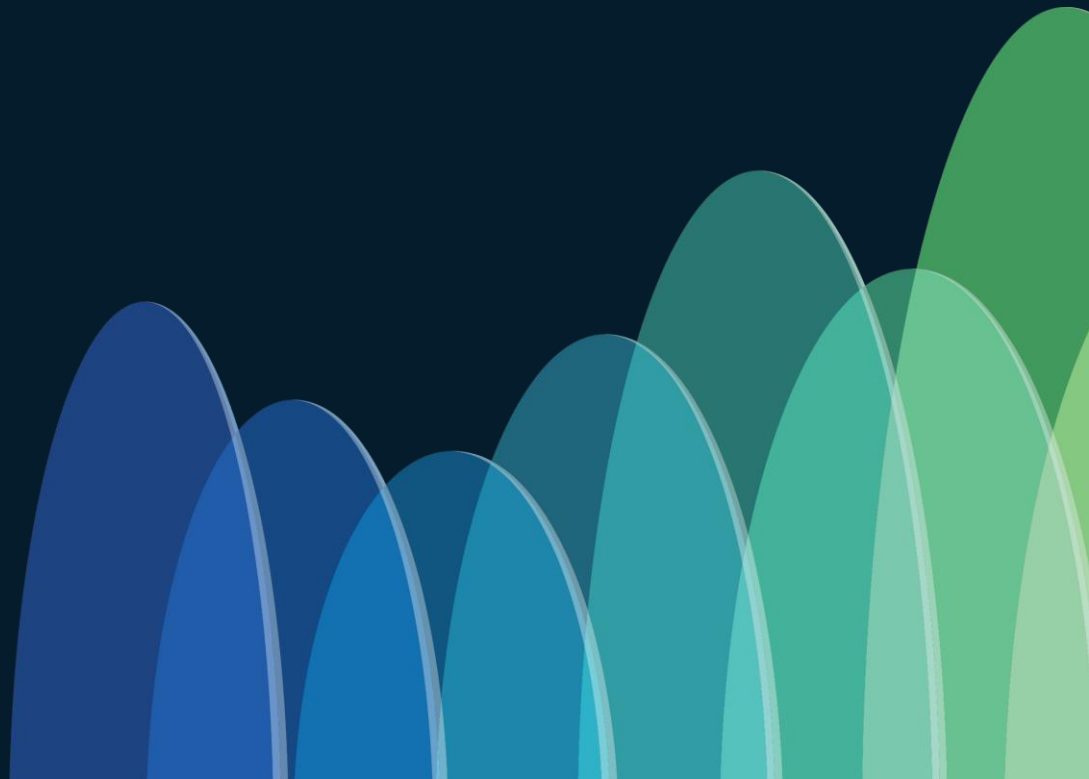


Mixed ISE cube with shared PSNs

- Scalability is transactions per second (TPS)
- Authentication or also Commands Authorization?
- Do you use scripts?
- How much Log Retention do you need?

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- ISE Deployment Options
- **Certificates**
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



ISE Certificates

System Certificates

- Identifies a cisco ISE node & services
- Specific to the node and service.
- Can manage all node's system certs from PPAN

Trusted Certificates

List of CAs

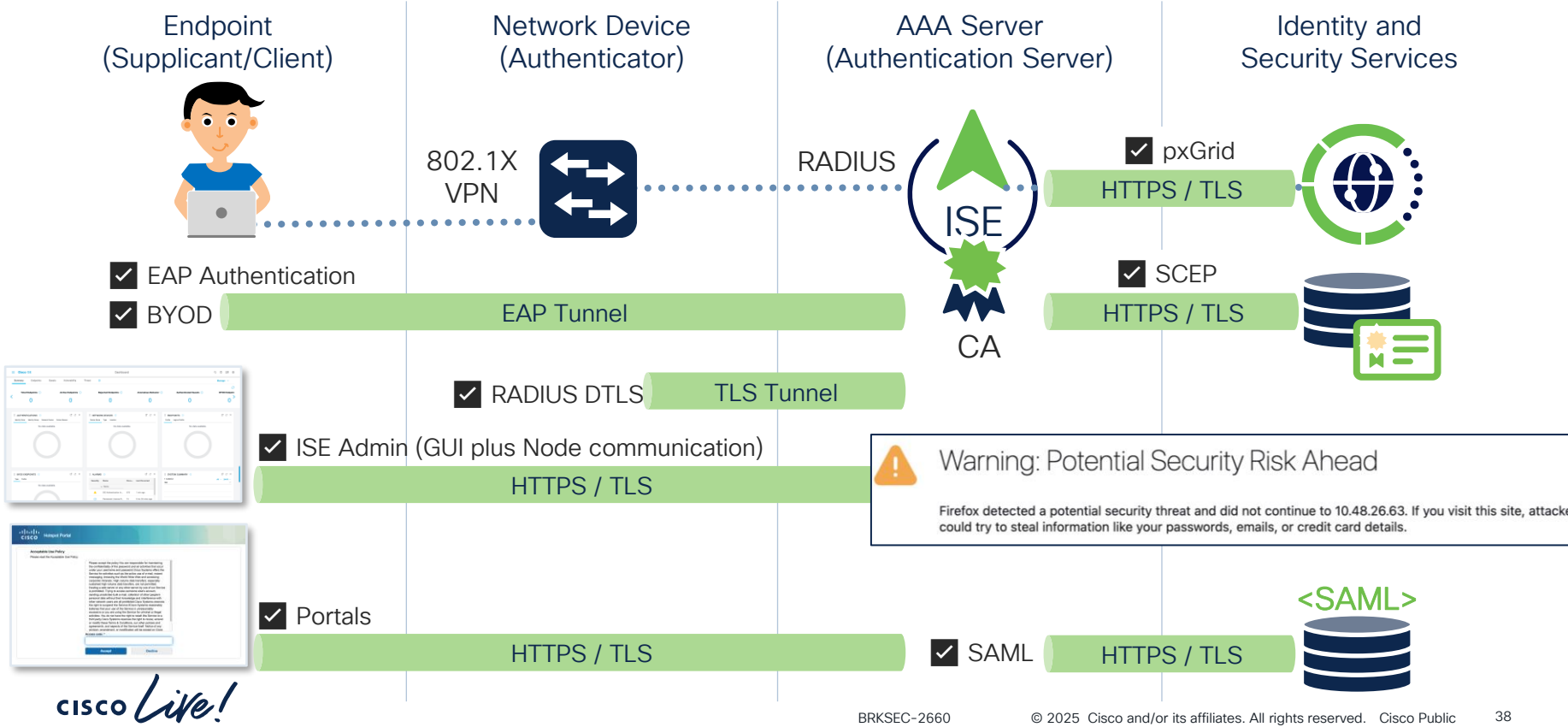
- Trusts for the identities of entities interacting with ISE
- Replicated to all the nodes in deployment

ISE Issued Certificates

- Internal CA service
- Issues and manages certificates for endpoints, pxGrid and ISE messaging

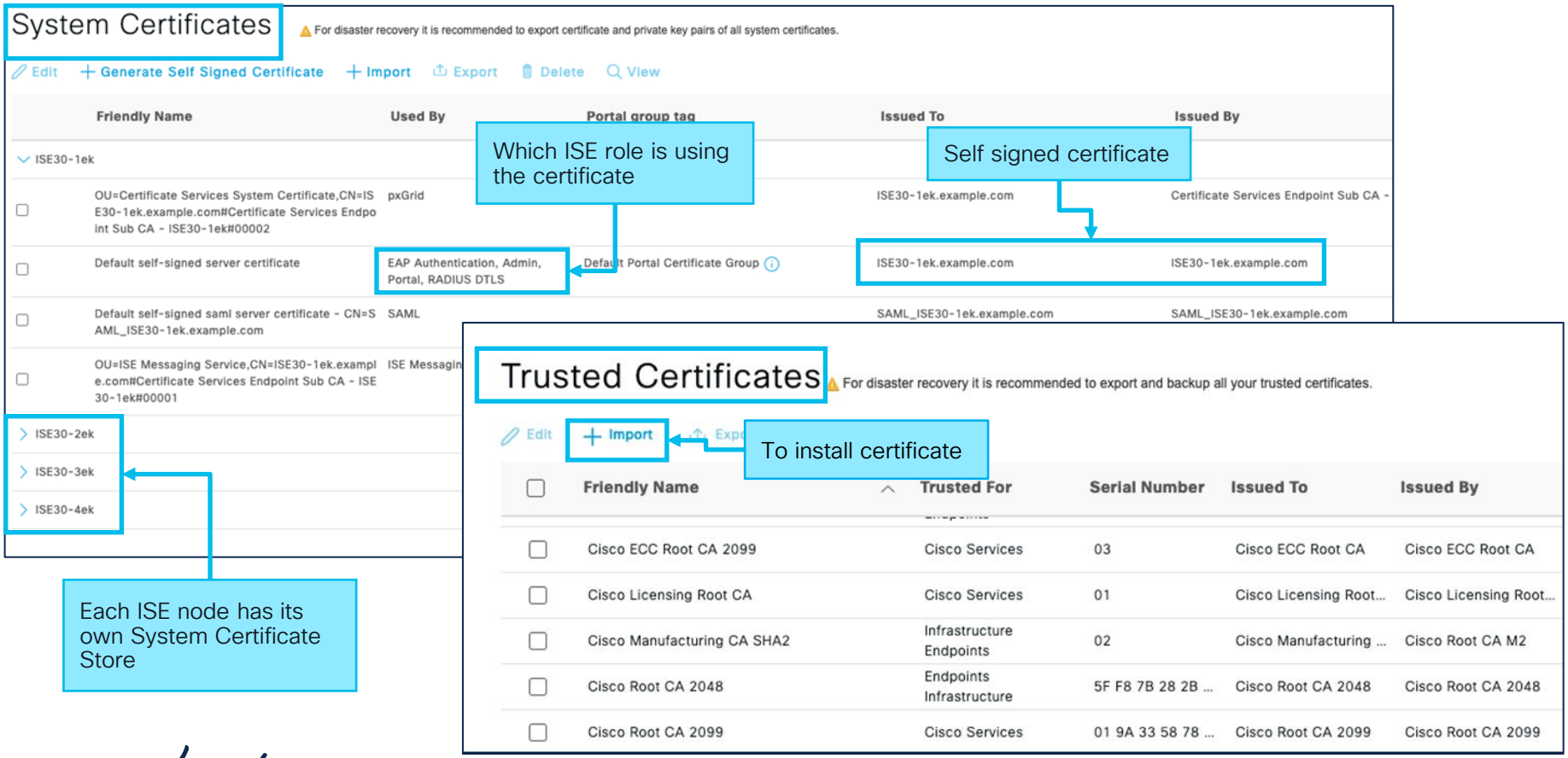
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Different ISE System certificates

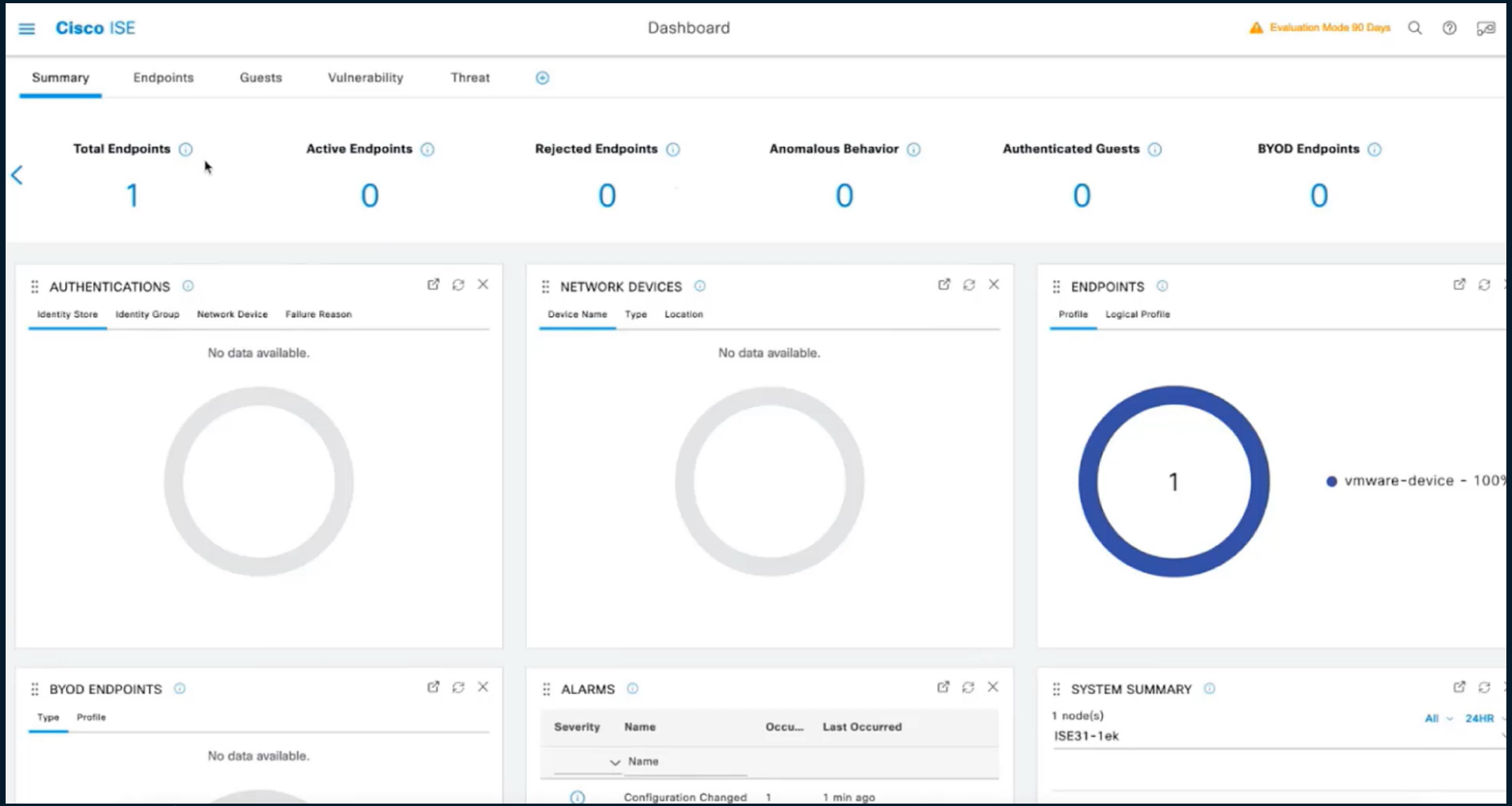


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Systems and Trusted Certificates



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public



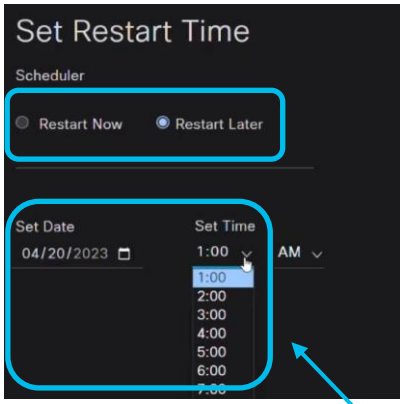
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

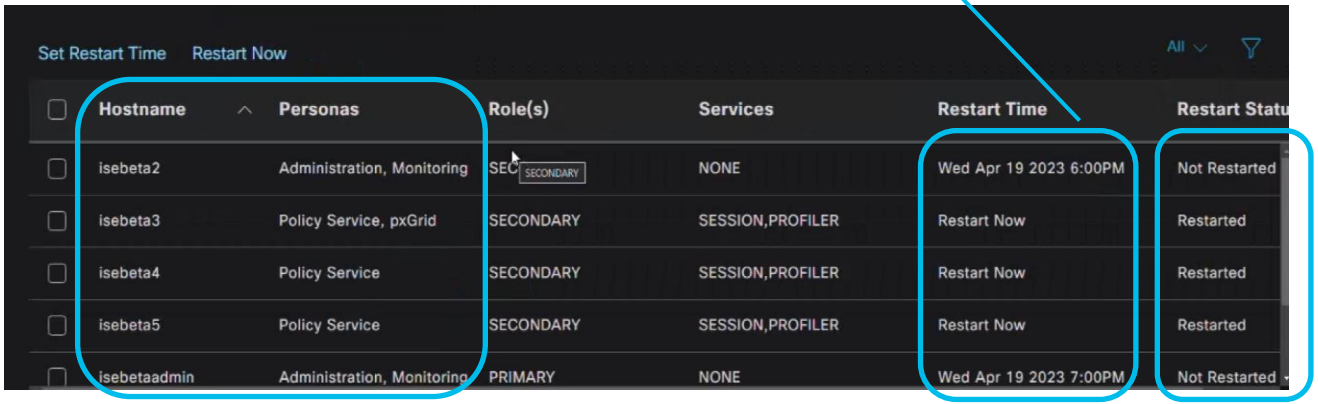
Controlled Application Restart

Up to ISE 3.2 a new ISE admin certificate requires reboot of all the nodes without any control.

From ISE 3.3, the reboot can be scheduled for each node.

Reboot must take place within 15 days





© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Improved Restart Time

~20 min in ISE 3.2

~16 min in ISE 3.3

~5.5 min in ISE 3.4

Using the commands

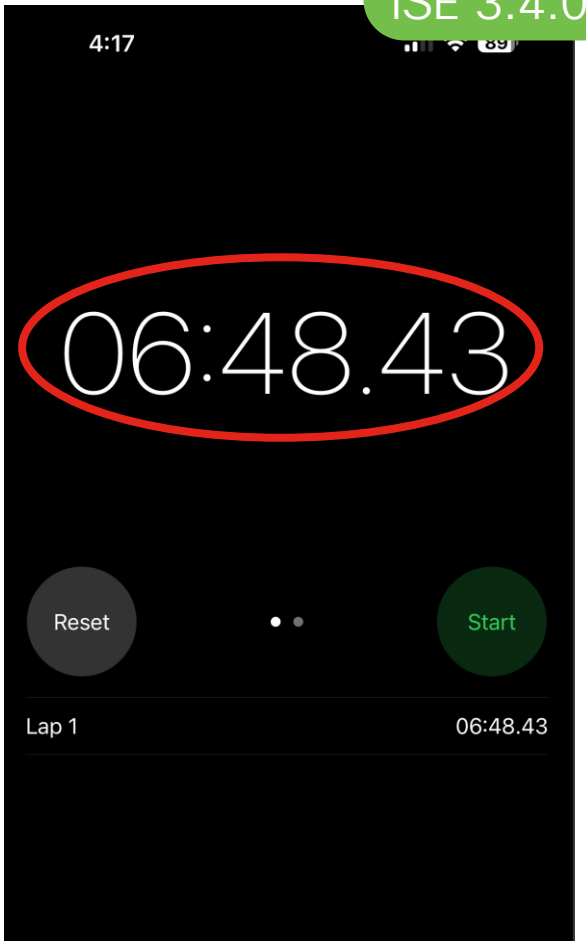
application stop ise
reload

~6.5 min in ISE 3.4

Using the commands

reload

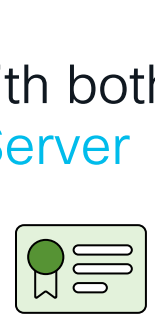
ISE 3.4.0



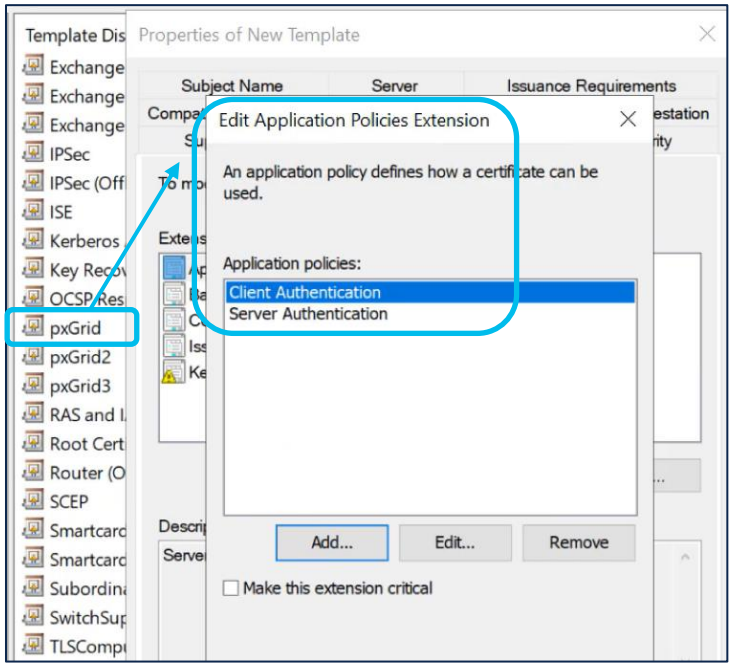
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

PxGrid Certificate

PxGrid certificate is built with both Client Authentication and Server Authentication extension

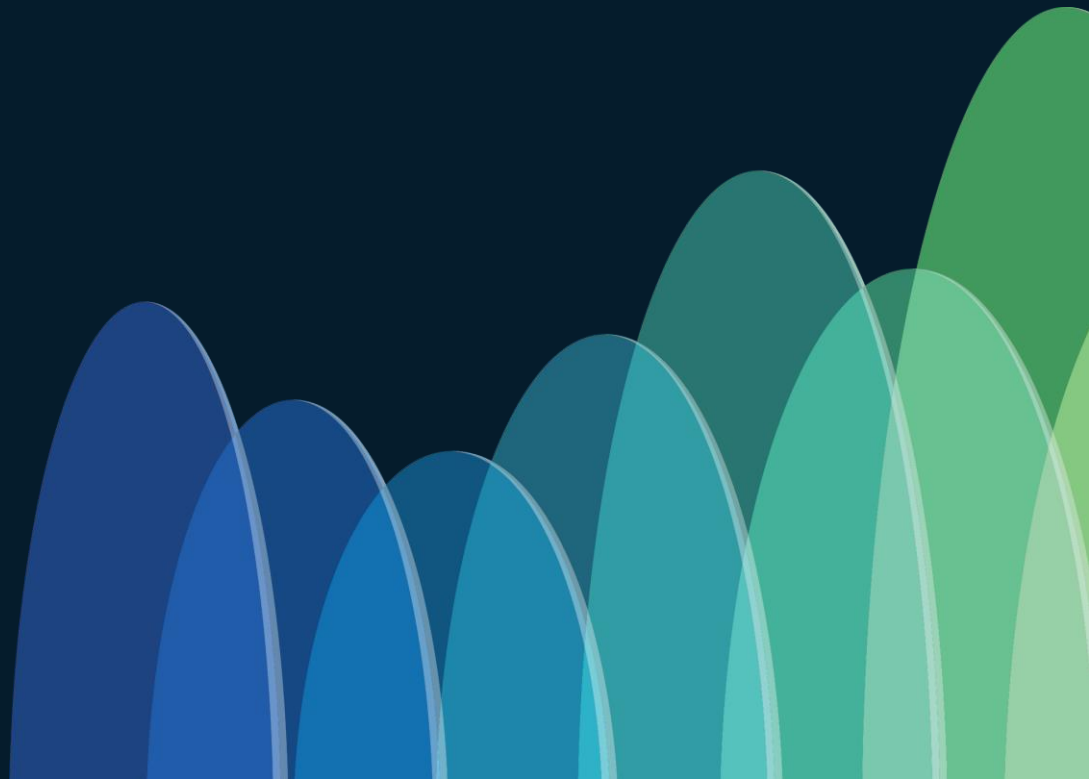


Need to create your template and use it for the Signing Request



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- ISE Deployment Options
- Certificates
- **Network Devices**
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



Network Device discovery/capabilities

- Hardware model
- IOS version
- Count
- OS Version and capabilities
- Hardware limitations

✓ : Fully supported
X : Not supported
! : Limited support, some functionalities are not supported

cs.co/nad-capabilities

[2] Refer to Cisco Compatibility Matrix

Table 1. Features and Functionalities

Feature	Functionality
AAA	802.1X, MAB, VLAN Assignment, dACL
Profiling	RADIUS CoA and Profiling Probes
BYOD	RADIUS CoA, URL Redirection and SessionID
Guest	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Guest Originating URL	RADIUS CoA, Local Web Auth, URL Redirection and SessionID
Posture	RADIUS CoA, URL Redirection and SessionID
MDM	RADIUS CoA, URL Redirection and SessionID
TrustSec	SGT Classification

Validated Cisco Access Switches

Table 2. Validated Cisco Access Switches

Device	Validated OS [1] / Minimum OS [3]	AAA	Profiling	BYOD	Guest	Guest Originating URL	Posture	MDM	TrustSec [2]
IE2000 IE3000	IOS 15.2(2)E4 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0(2)EB	√	√	√	√	X	√	√	√
IE4000 IE5000	IOS 15.2(2)E5 IOS 15.2(4)E2 IOS 15.2(4)EA6	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
IE4010	IOS 15.2(2)E5 IOS 15.2(4)E2	√	√	√	√	√	√	√	√
	IOS 15.0.2A-EX5	√	√	√	√	√	√	√	√
SMB SG500	Sx500 1.4.8.06	[4] !	!	X	X	X	X	X	X
	Sx500 1.2.0.97	!	!	X	X	X	X	X	X

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Does ISE Support my third-party Network device? Does my third-party Network Device Supports ISE?

Overview

Cisco ISE supports protocol standards like RADIUS, its associated RFC Standards, and TACACS+. For more information, see the ISE Community Resources.

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NAD) that implements common RADIUS behavior for standards-based authentication.

Cisco ISE interoperates fully with third-party TACACS+ client devices that adhere to the governing protocols. Support for TACACS+ functions depends on the device-specific implementation.

Check for Advanced capabilities support:

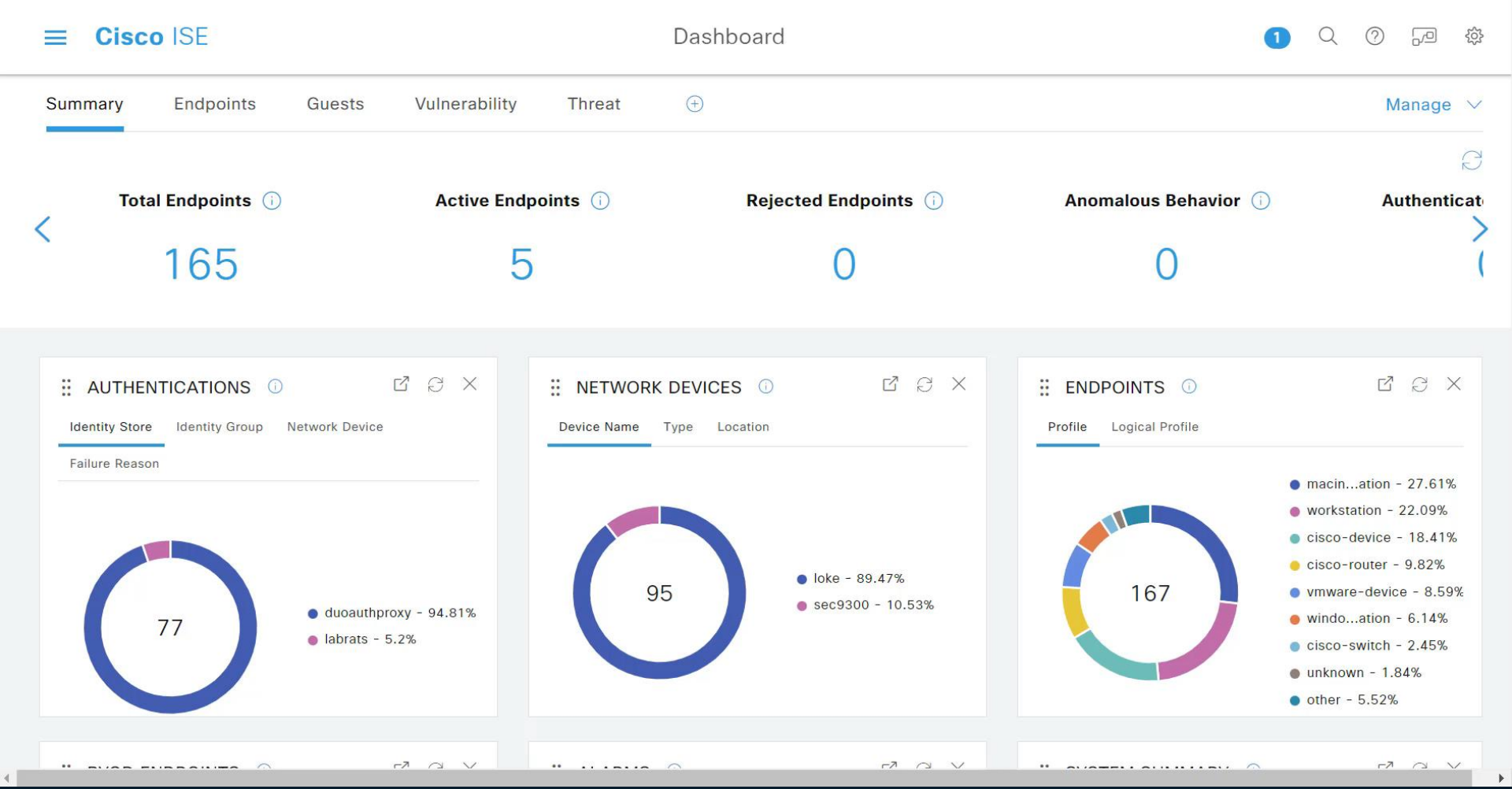
- CoA (RADIUS or SNMP)
- URL Redirection

Might need to:

- Import a Vendor Specific Dictionary
- Create Network Device Profile

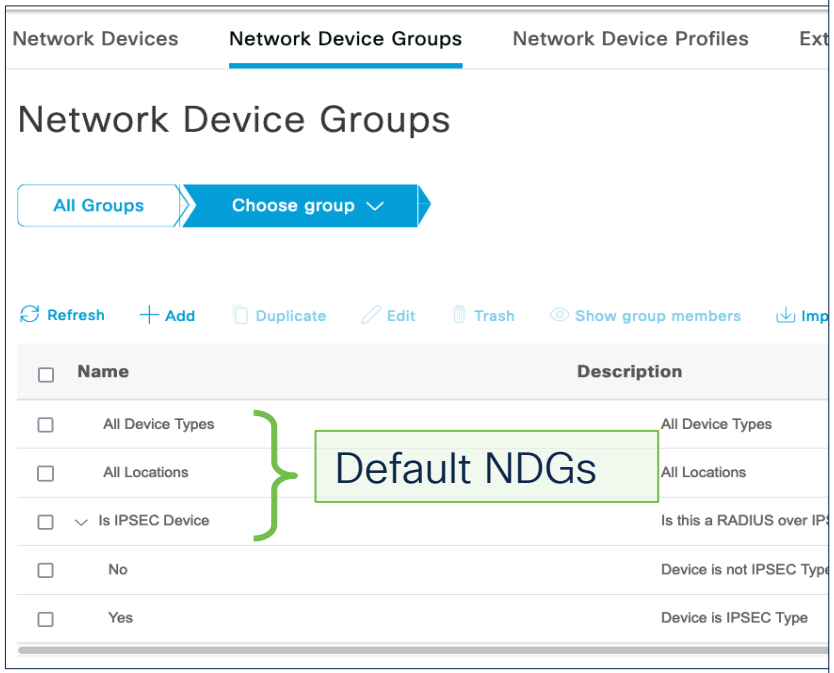
From the Network Component Compatibility, Release 3.3
https://www.cisco.com/c/en/us/td/docs/security/ise/3-3/compatibility_doc/b_ise_sdt_33.html

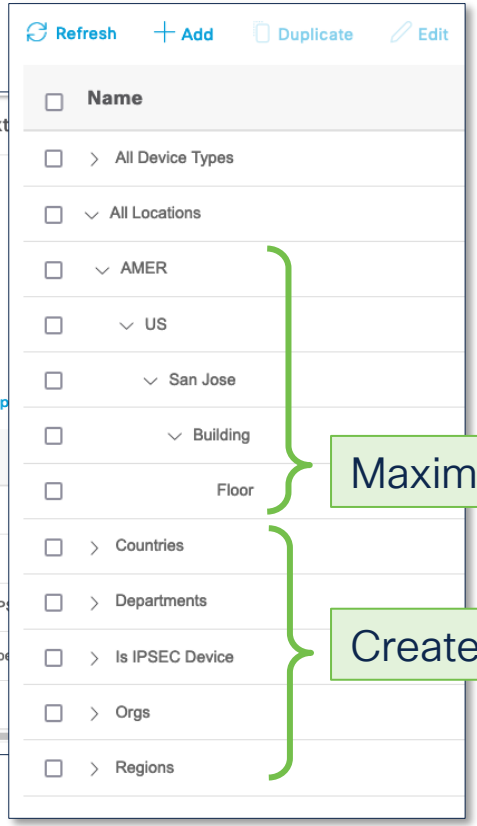
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

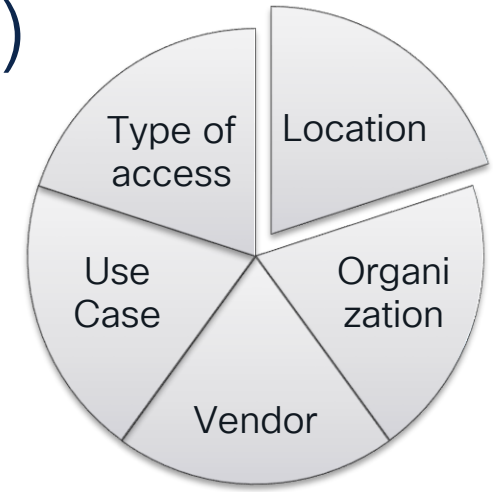


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Default Network Device Groups (NDGs)







© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional Tips

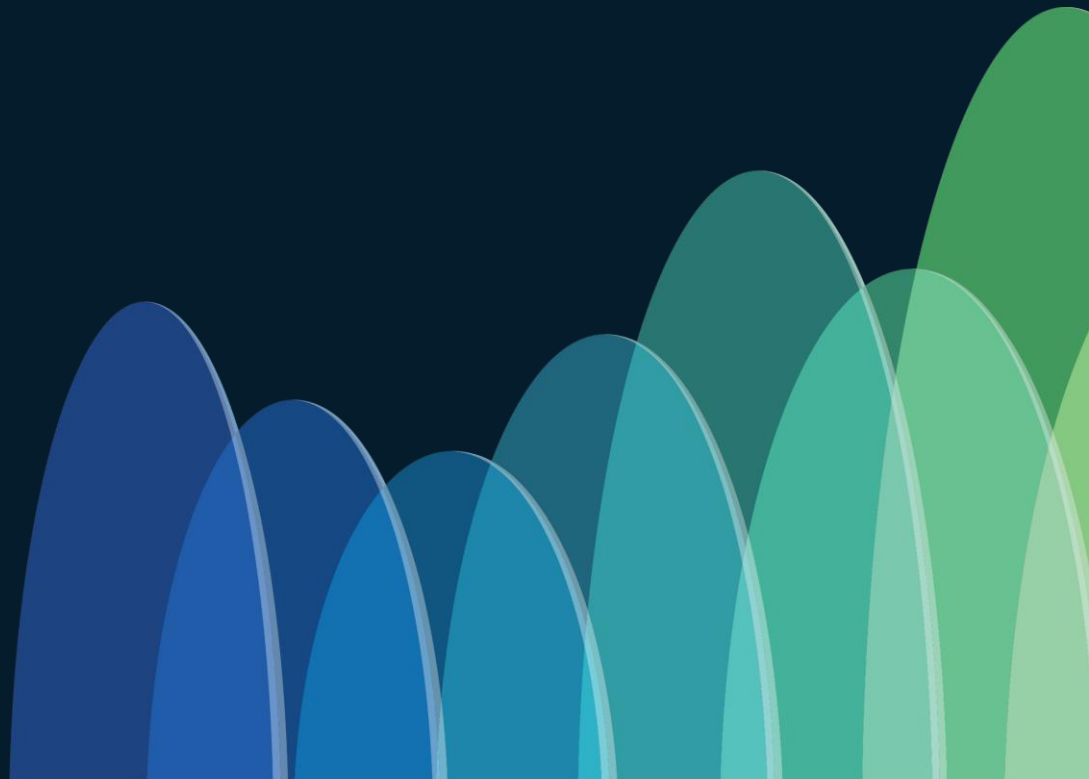
- Always Test before implementing!

- Standardize! Standardize! Standardize!
  - IOS versions
  - AAA configuration
  - Wireless configuration
  - Profiling configuration

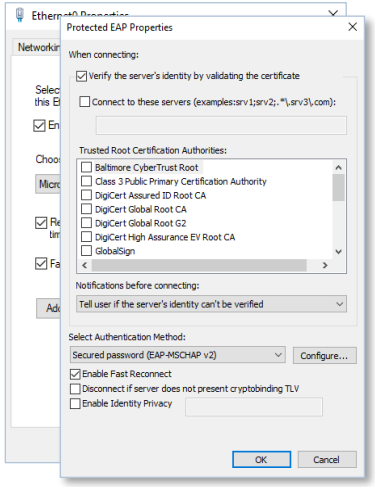
- Document everything!

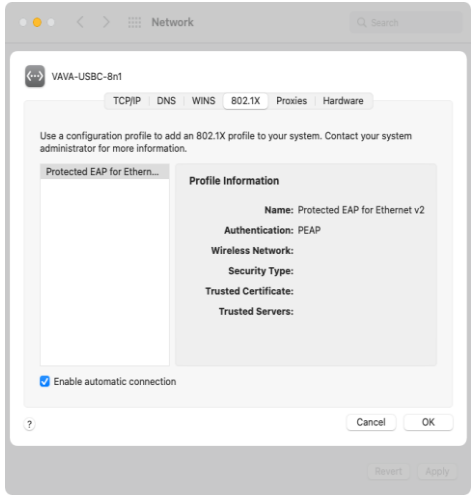
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

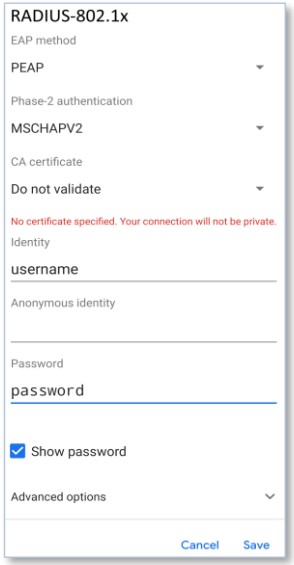
- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- **Supplicants**
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



Endpoints: Native 802.1X Supplicants







```
wpa_supplicant

NAME
wpa_supplicant - Wi-Fi Protected Access client and IEEE
802.1X supplicant

SYNOPSIS
wpa_supplicant [ -BddfhKLqqsTtuvW ]  [ -iifname ]  [ -cconfig
file ]  [ -Ddriver ]  [ -PPID_file ]  [ -foutput file ]

OVERVIEW
Wireless networks do not require physical access to the
network equipment in the same way as  wired  networks.
This makes it easier for unauthorized users to passively
monitor a network and capture all transmitted frames.
In addition, unauthorized use of the network is much
```

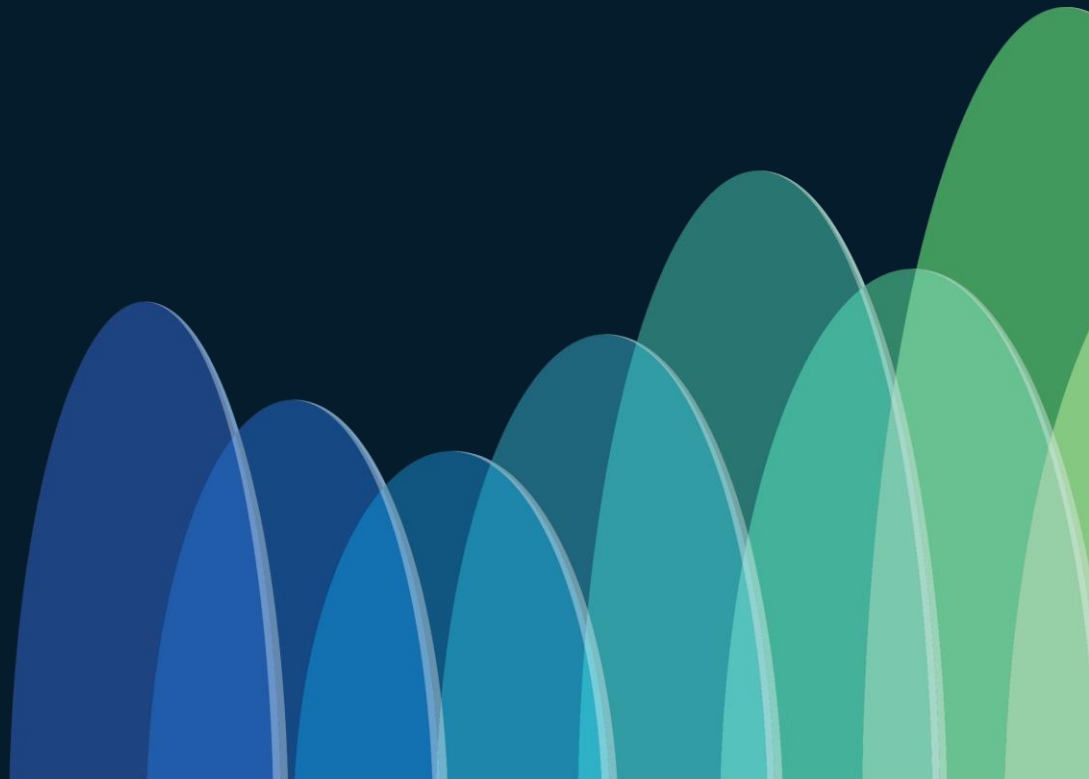
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Windows 7, 8/8.1, and 10 – Native Supplicant

- Now you can do TEAP directly in Windows for Chaining (Windows 10 build 2004 and ISE 2.7 Patch 2)
- Involve the Active Directory Team
- Group Policy for:
  - Supplicant configuration
  - Pushing certificates
  - Pre-configure SSIDs – better user experience

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- **Profiling**
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



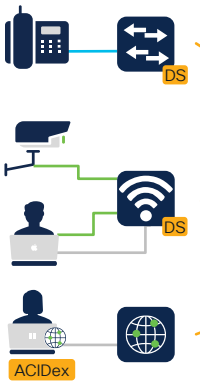
Endpoints: Everything Else

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Endpoint Profiling

The profiling service dynamically classifies devices connected to your network

Endpoints send interesting data, that reveal their device type



ISE Data Collection Methods for Device Profiling

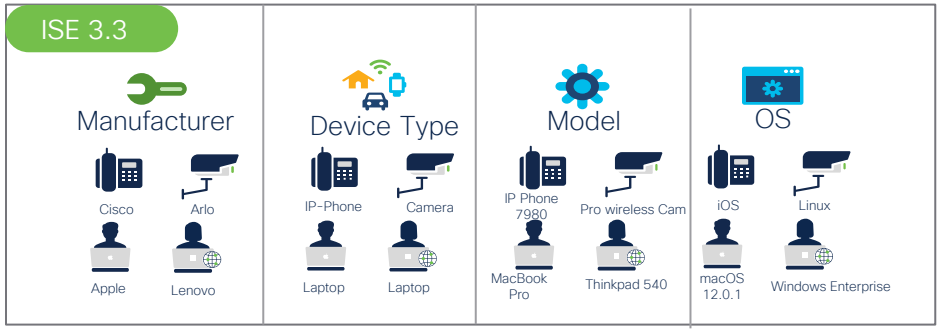
Active Probes: DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDex

pxGrid context-in: (DNAC Endpoint Analytics, CyberVision for industrial)

WIFI Edge Analytics: Firmware_version, HW_Model, Manufacturer, Model, OS_Version, Vendor (Samsung, Apple and Intel devices)



MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of RADIUS Probe

 vendor	OUI = Vendor ID, IP = xx.xx.xx.xx
 Cisco Device	OUI = Cisco, IP = xx.xx.xx.xx
 HP Device	OUI = HP, IP = xx.xx.xx.xx
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of SNMP Probe

 Unknown	OUI = Random, IP = xx.xx.xx.xx
 Cisco Device	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971
 HP Device	OUI = HP, IP = xx.xx.xx.xx
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of DHCP Probe

 Microsoft Workstation	OUI = Random, IP = xx.xx.xx.xx, **dhcp-class-identifier CONTAINS MSFT**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, **DHCP:dhcp-class-identifier CONTAINS CP-9971**
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, **DHCP:dhcp-class-identifier CONTAINS LaserJet**
 Apple Device	OUI = Apple, IP = xx.xx.xx.xx, **DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252**

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of HTTP Probe

 Microsoft Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971
 HP Printer	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet
 Apple iPad	OUI = Apple, IP = xx.xx.xx.xx, DHCP:dhcp-DHCP:dhcp-parameter-request-list EQUALS 1, 3, 6, 15, 119, 252 IP:User-Agent contains iPad

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of NMAP Probe

 Windows10-Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0, FQDN=test-laptop1.zero0k.org, **NMAP:SMB.operating-system CONTAINS Windows 10**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971, FQDN=test-phone1.zero0k.org
 HP LaserJet P4015	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, **NMAP:hrDeviceDescr CONTAINS HP LaserJet P4015**
 Apple IPad	OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-i-pad1.zero0k.org

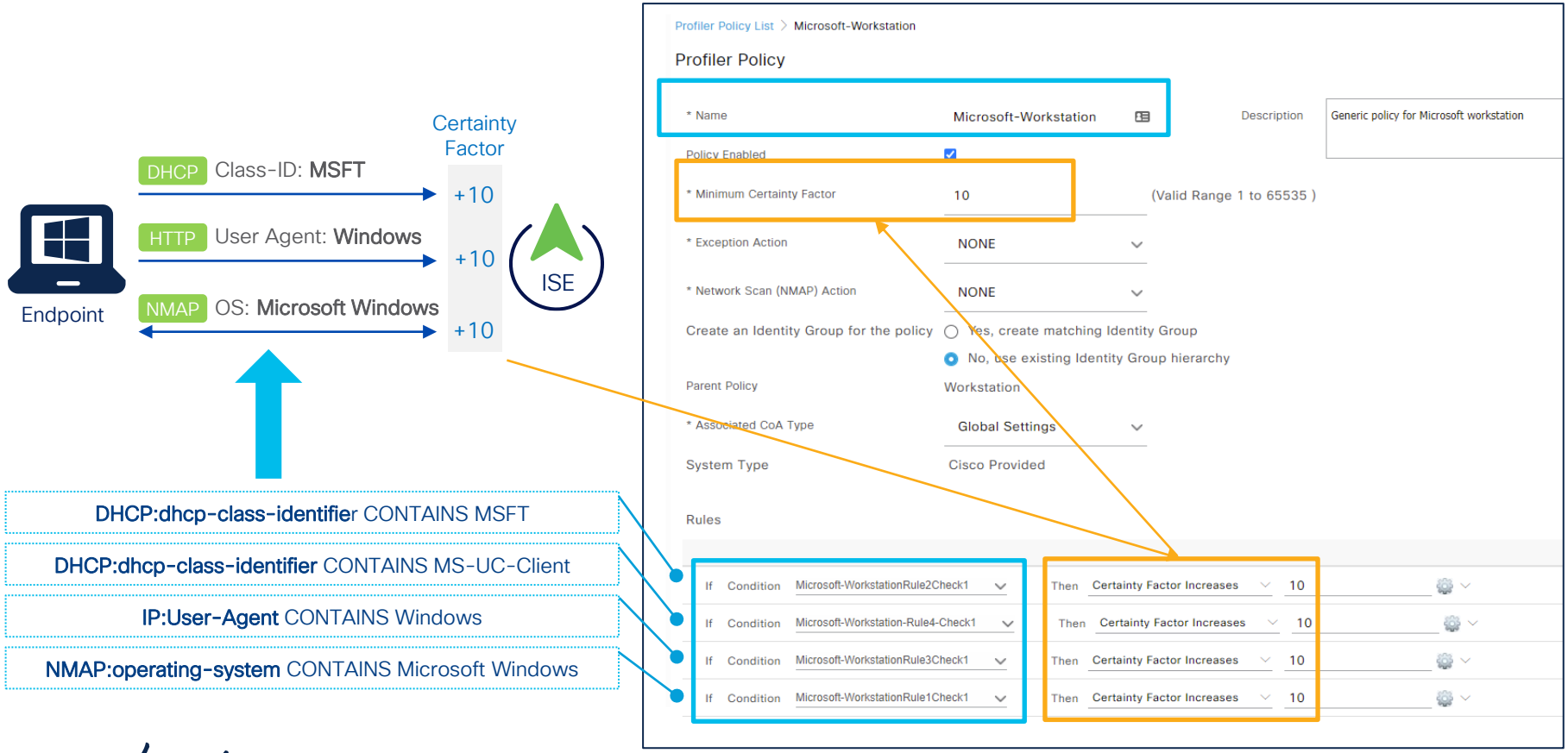
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Effect of AD Probe

 Windows10-Workstation	OUI = Random, IP = xx.xx.xx.xx, dhcp-class-identifier CONTAINS MSFT, IP:User-Agent CONTAINS Windows NT 10.0, FQDN=test-laptop1.zero0k.org, NMAP:SMB.operating-system CONTAINS Windows 10, **AD-OS = Windows 10**
 Cisco IP Phone 9971	OUI = Cisco, IP = xx.xx.xx.xx, CDP:cdpCachePlatform = Cisco IP Phone 9971, DHCP:dhcp-class-identifier CONTAINS CP-9971, FQDN=test-phone1.zero0k.org
 HP LaserJet P4015	OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015
 Apple IPad	OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-i-pad1.zero0k.org

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

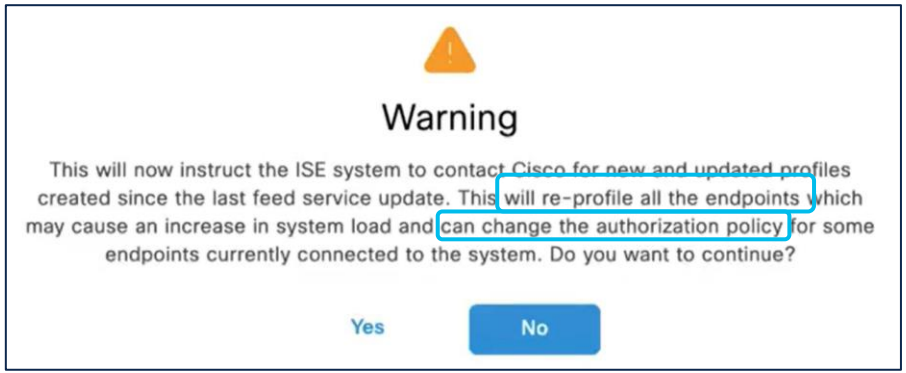
ISE profiles definition



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Feed service Updates

- Feed service updates MAC OUIs
- Feed service provides new and updated profiles
- Be careful when applying profile updates, check they do not interfere with the profiles you have been using and your policies
- Test and create correct Policies before implementing



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

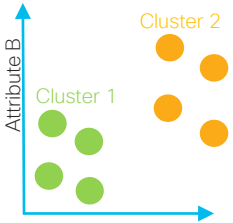
Cisco AI Machine Learning Profiling

ISE 3.3

Unknown endpoints

Clustering

ML groups different endpoints into clusters based on attribute data

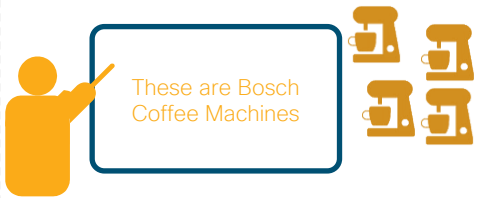


Rule Creation

Creates a rule that uniquely groups together endpoint clusters

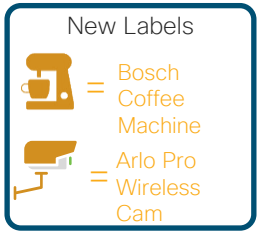
Endpoint Labeling

System recommends labels or customer can teach ML what to label the endpoints in a cluster



Active Learning

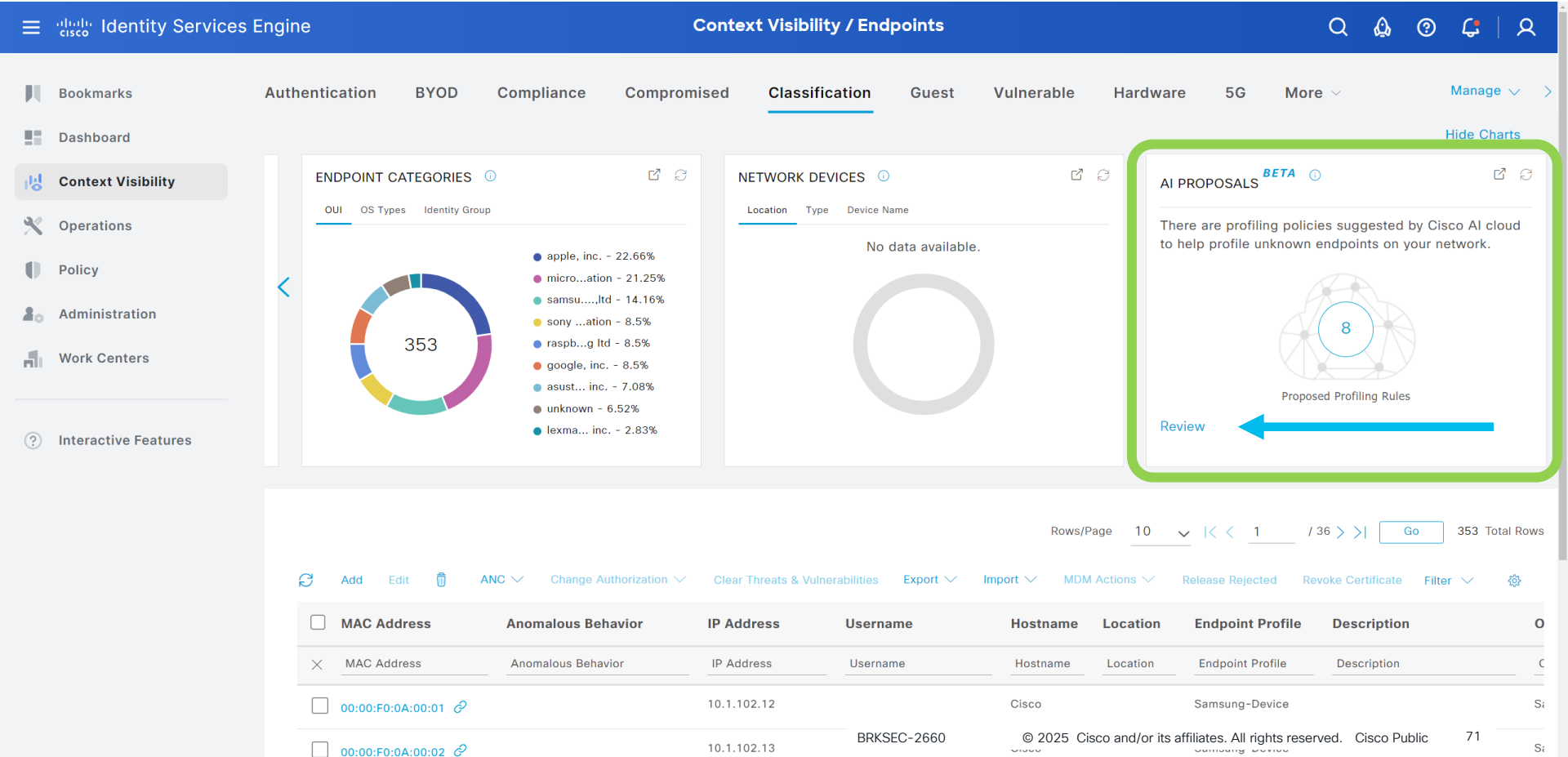
ML learns new labels and validates existing labels



= Step done in the ML Cloud

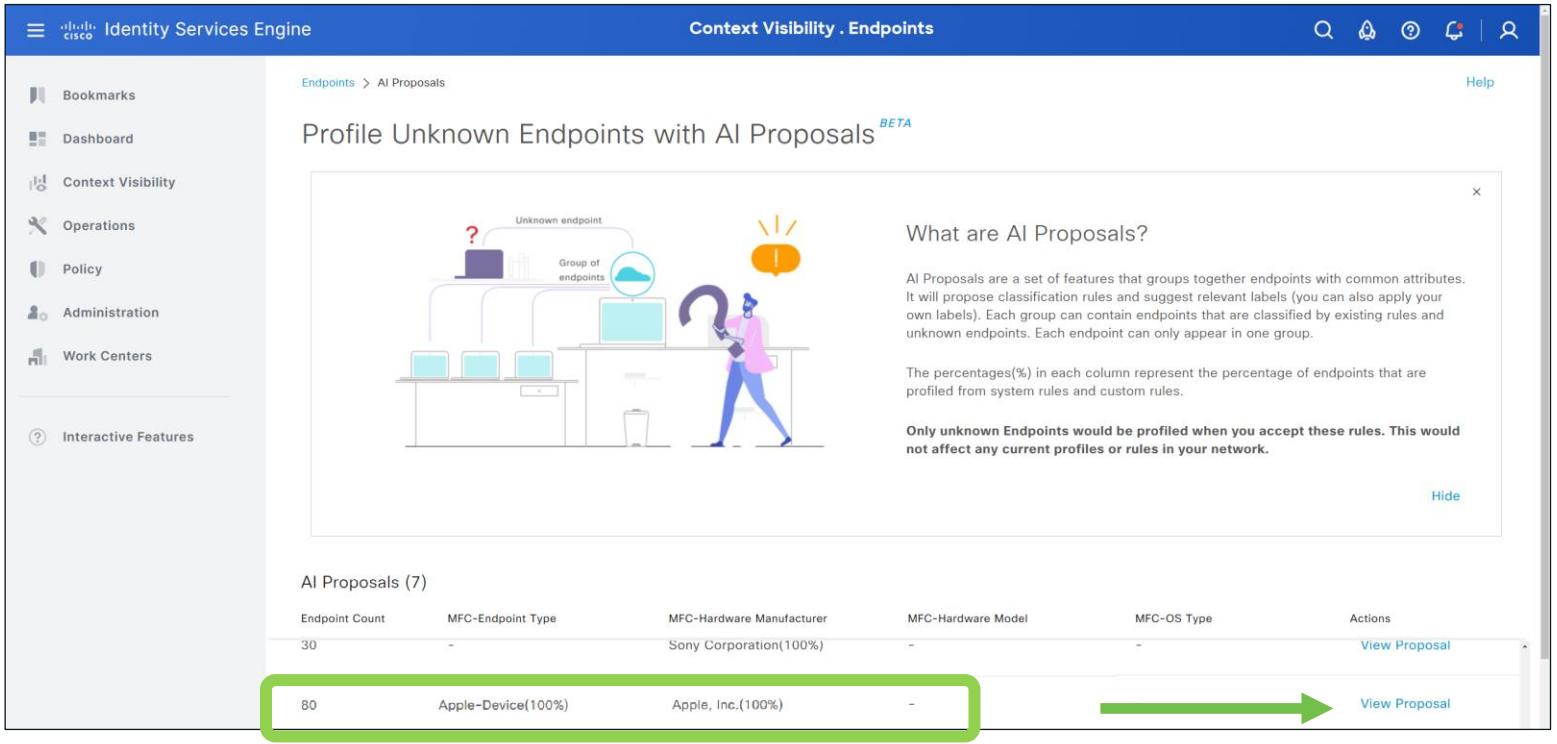
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Review the AI Proposals



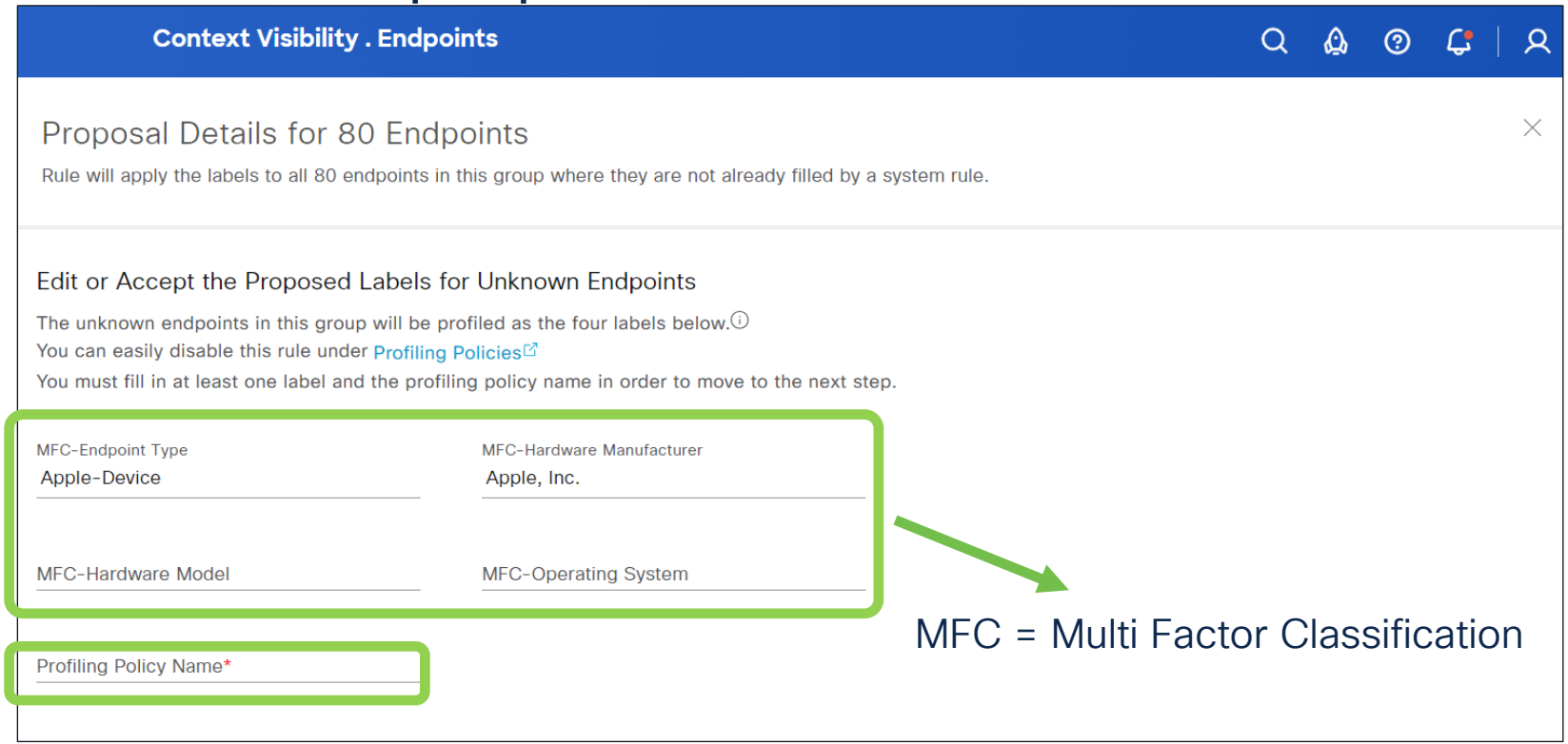
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Choose the Proposal to View

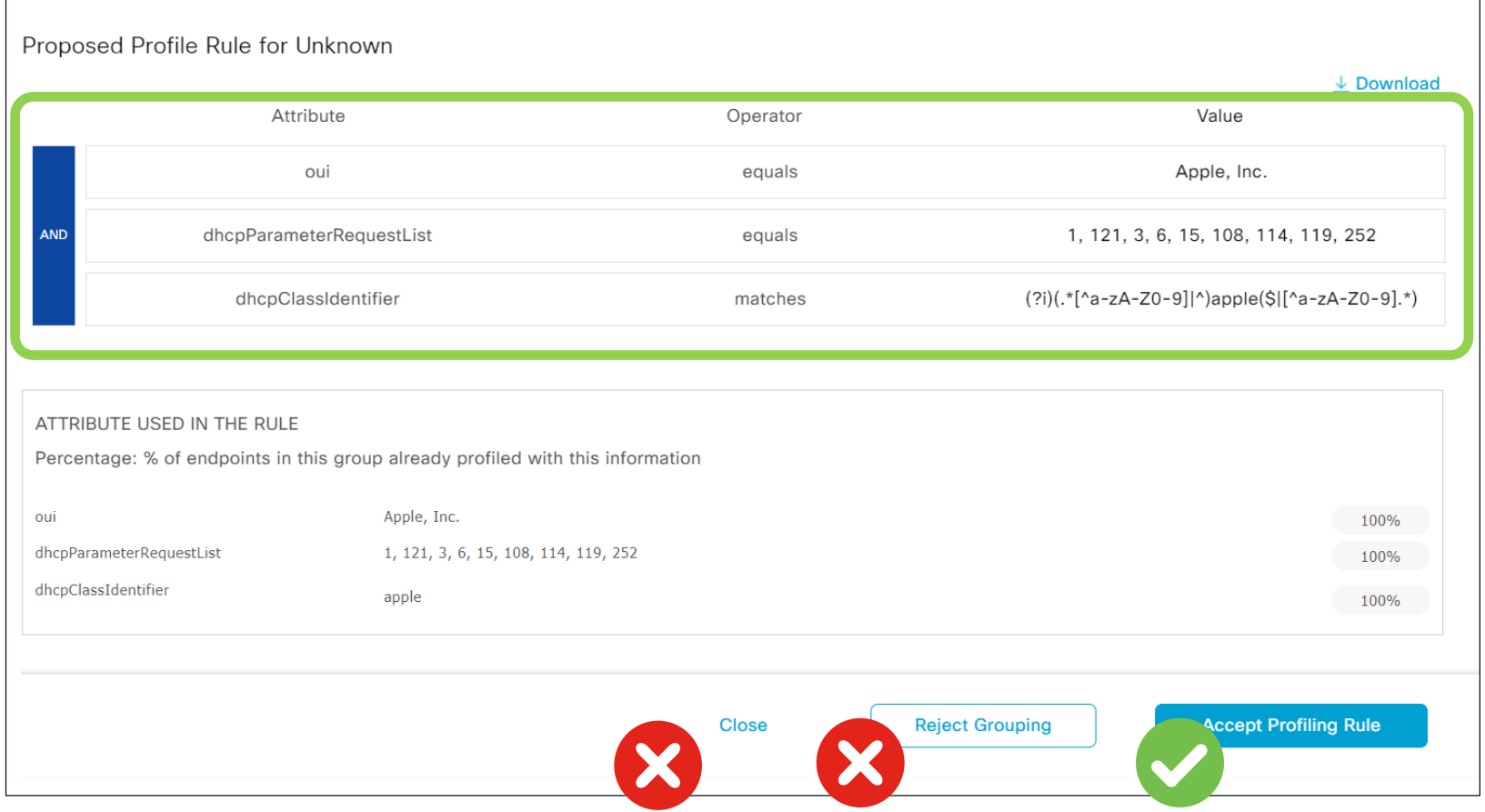


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Review the proposed labels



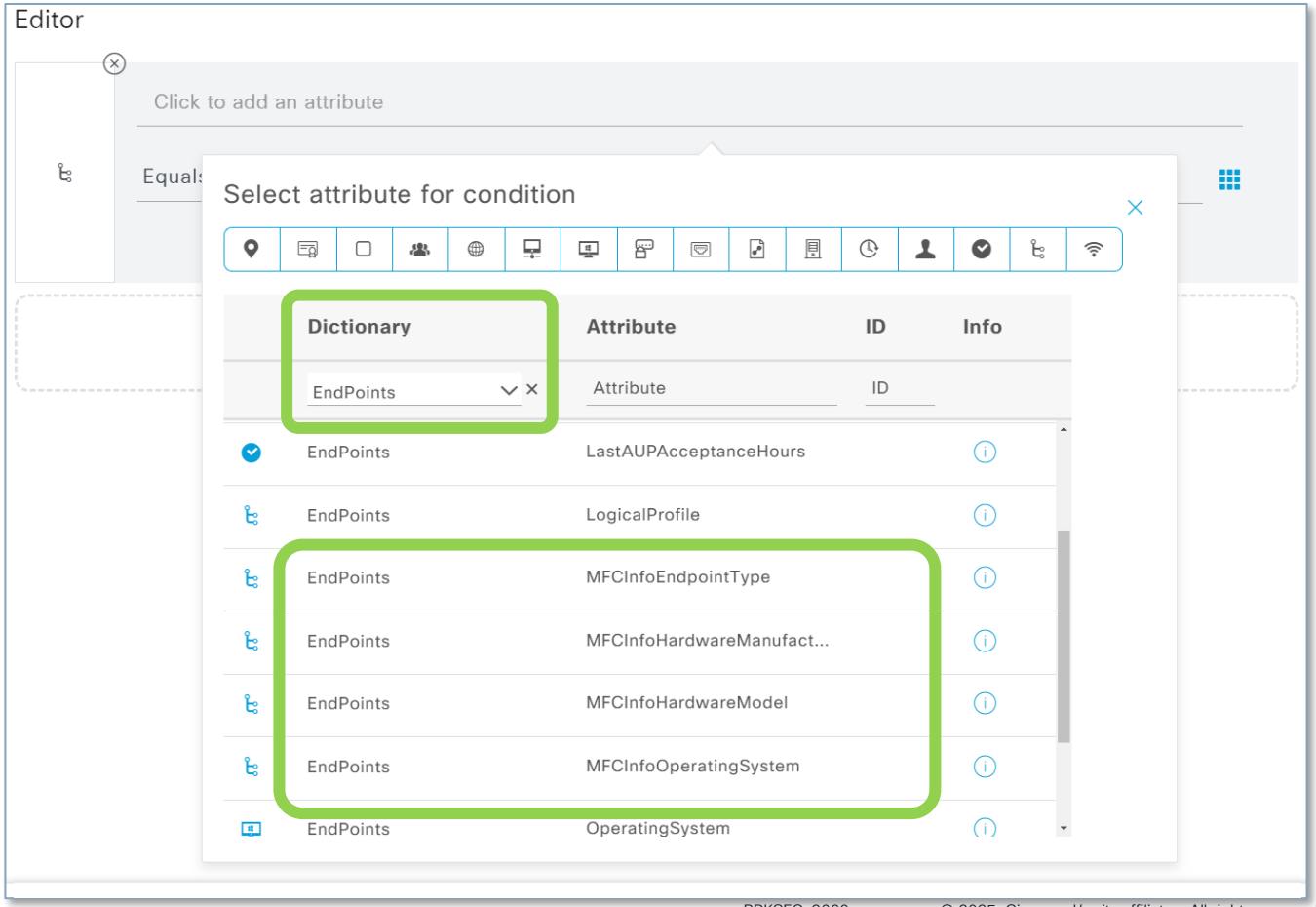
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public



Close = cancel
no changes

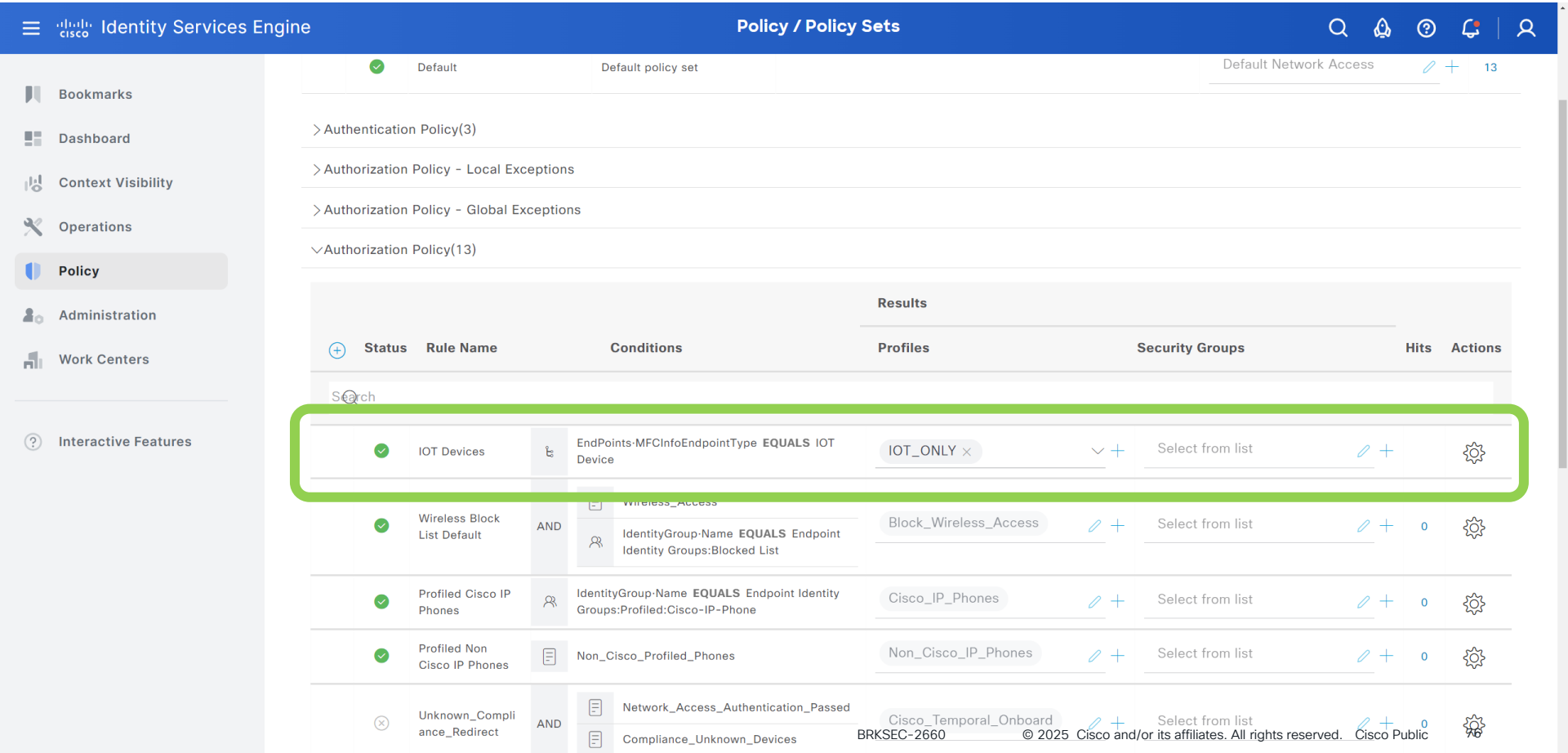
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

All the MFC Attributes Can Be Used



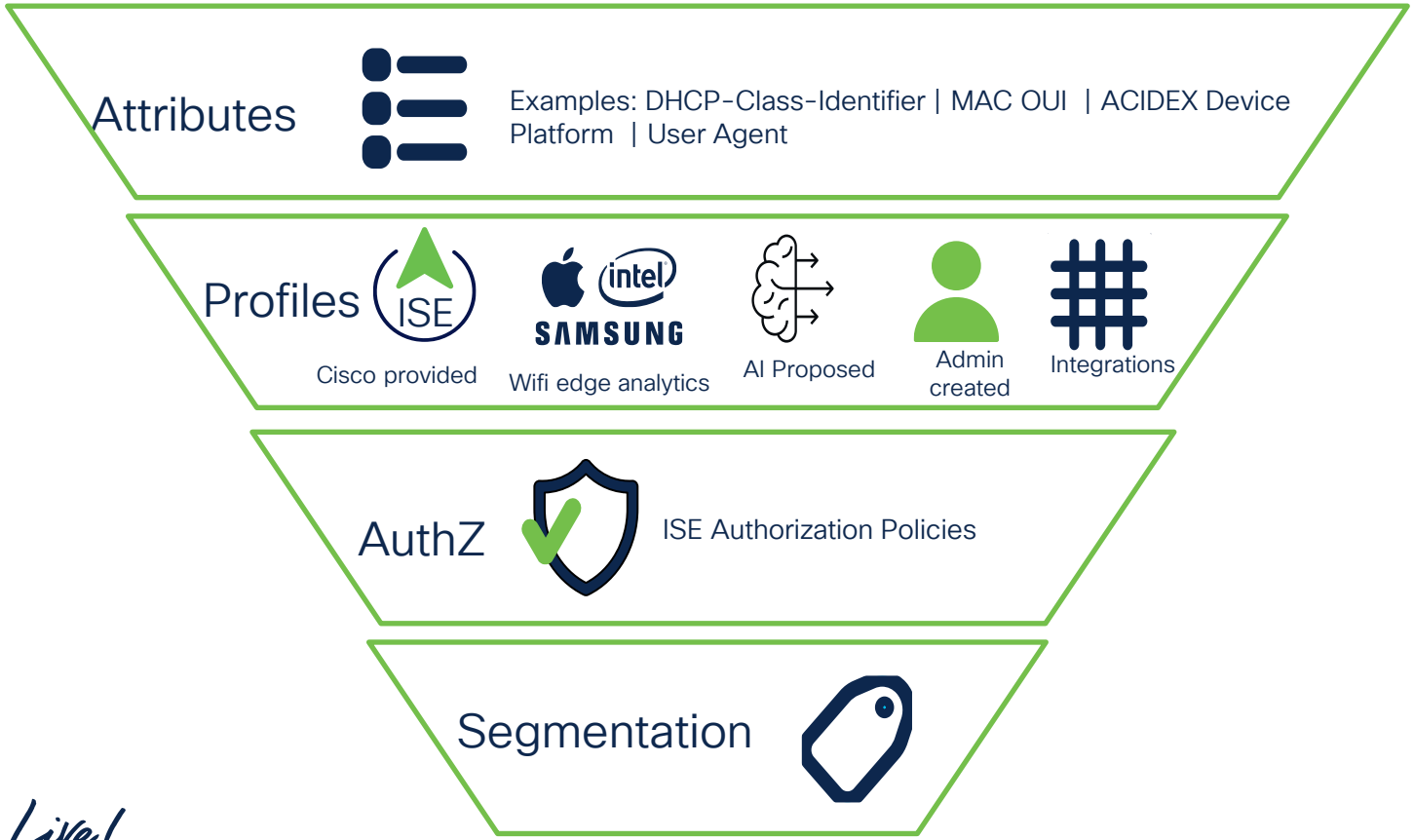
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ready to Profile!



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Turning Probes Into Profiles, Profiles Into Protection



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Behavioral vs Organizational Endpoint Information

Behavioral

- Probes and profiling
- Device Sensor
- pxGrid Context-In
- AI Analytics

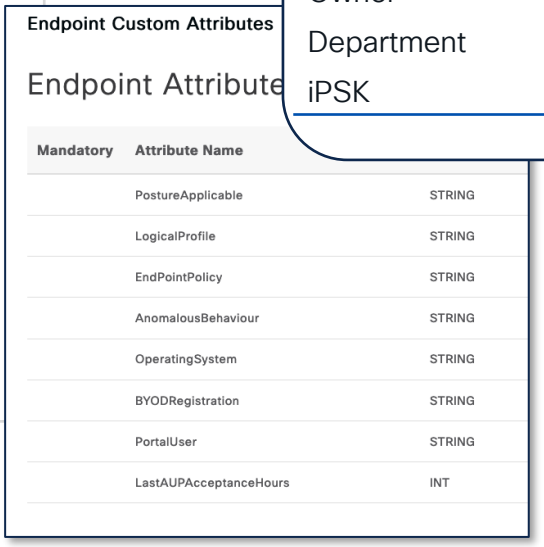
Organizational

- Endpoint Custom Attributes
- Context Visibility Input (GUI/CSV)
- Custom Attributes and endpoint REST API (JSON)

- External Databases (CMDBs)
- Active Directory / LDAP
- pxGrid Direct (ServiceNow, etc.)

Common Uses

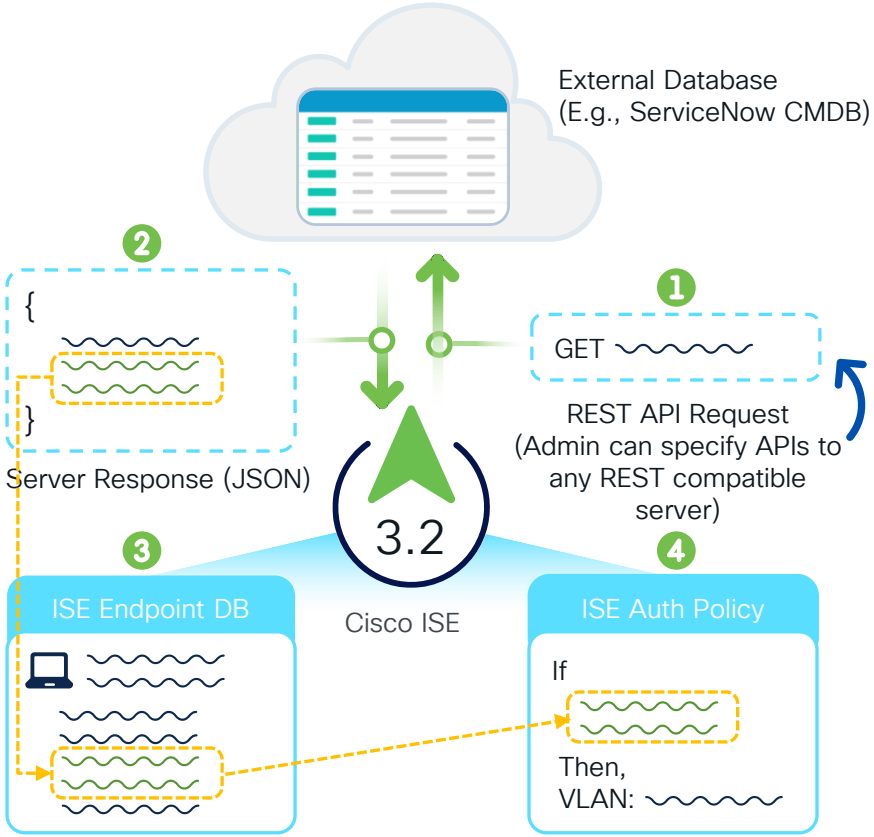
Attribute Name	Type
Created	Date
Expires	Date
Owner	String
Department	String
iPSK	String



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco ISE pxGrid Direct for CMDBs

ISE 3.2

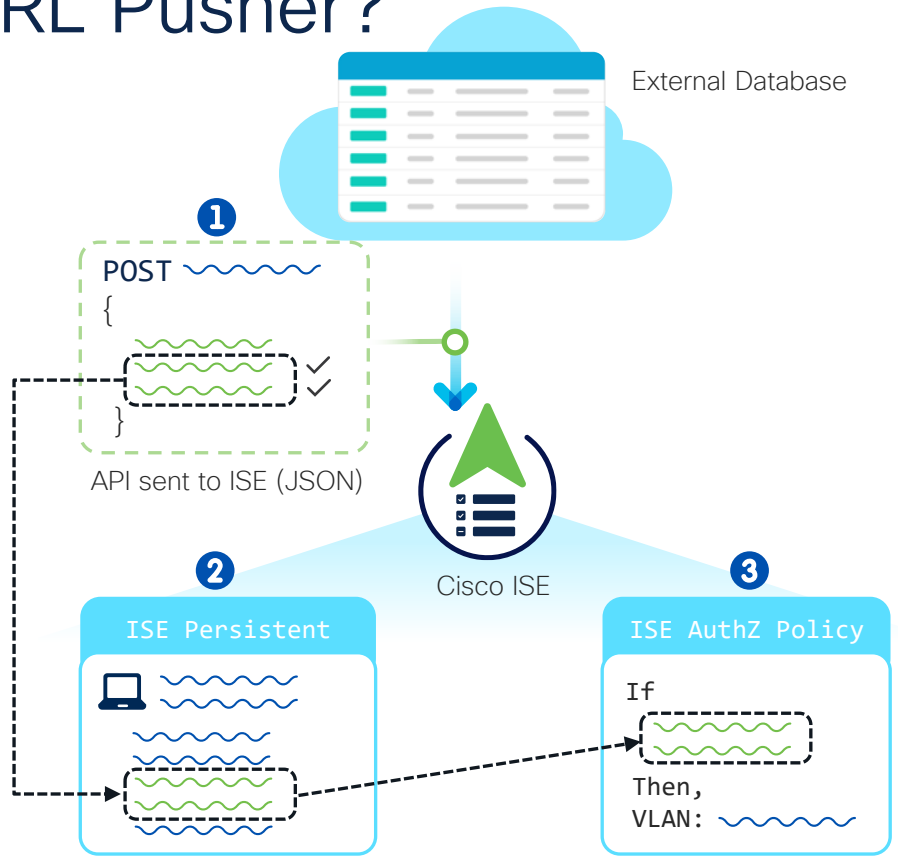



```
{
  "result": [
    {
      "sys_import_state_comment": "",
      "template_import_log": "",
      "sys_updated_on": "2022-05-17 10:53:53",
      "sys_class_name": "EDDA_Demo",
      "sys_target_sys_id": "",
      "sys_id": "00021059db6b01101f0f174b13961900",
      "sys_updated_by": "aacook",
      "sys_created_on": "2022-05-17 10:53:53",
      "sys_import_set": "ISET0011307",
      "sys_transform_map": "",
      "sys_created_by": "aacook",
      "sys_import_row": "34,285",
      "u_account_name": "Holly.Allen@example.org",
      "u_macaddress": "05:0e:33:f3:2b:03",
      "sys_row_error": "",
      "group_tag": "cts:security-group-tag=2774-000",
      "sys_target_table": "",
      "sys_mod_count": "0",
      "u_hostname": "black.williams.com",
      "import_set_run": "",
      "sys_tags": "",
      "u_community_group": "Administration",
      "sys_import_state": "Pending",
      "u_config_item": "SNtoDataMartHolly.Allen",
      "u_sync": "",
      "u_ci_status": "Operational",
      "u_host_name": "black.williams.com"
    },{ … }
  ]
}
```

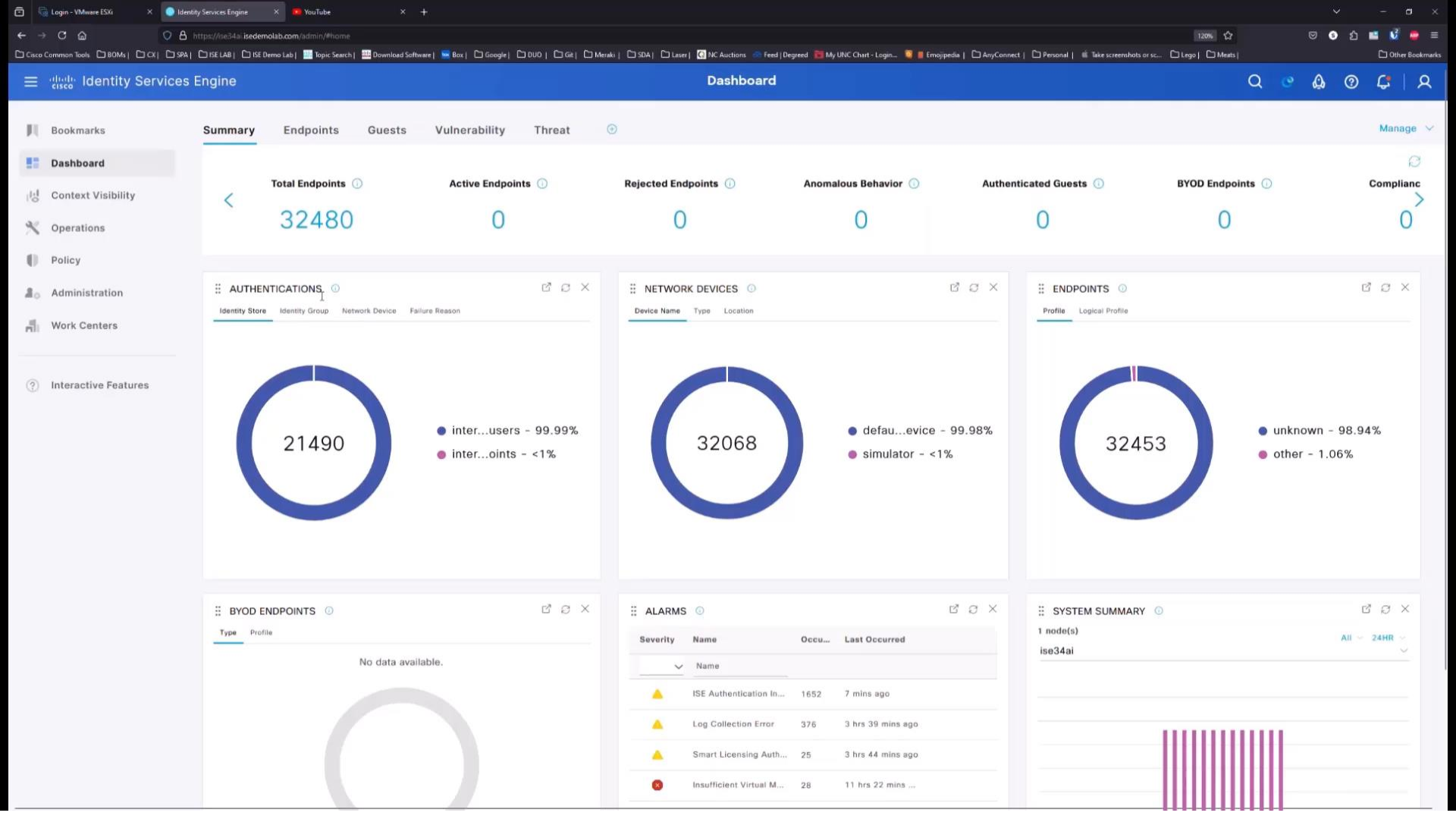

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

What is pxGrid Direct URL Pusher?

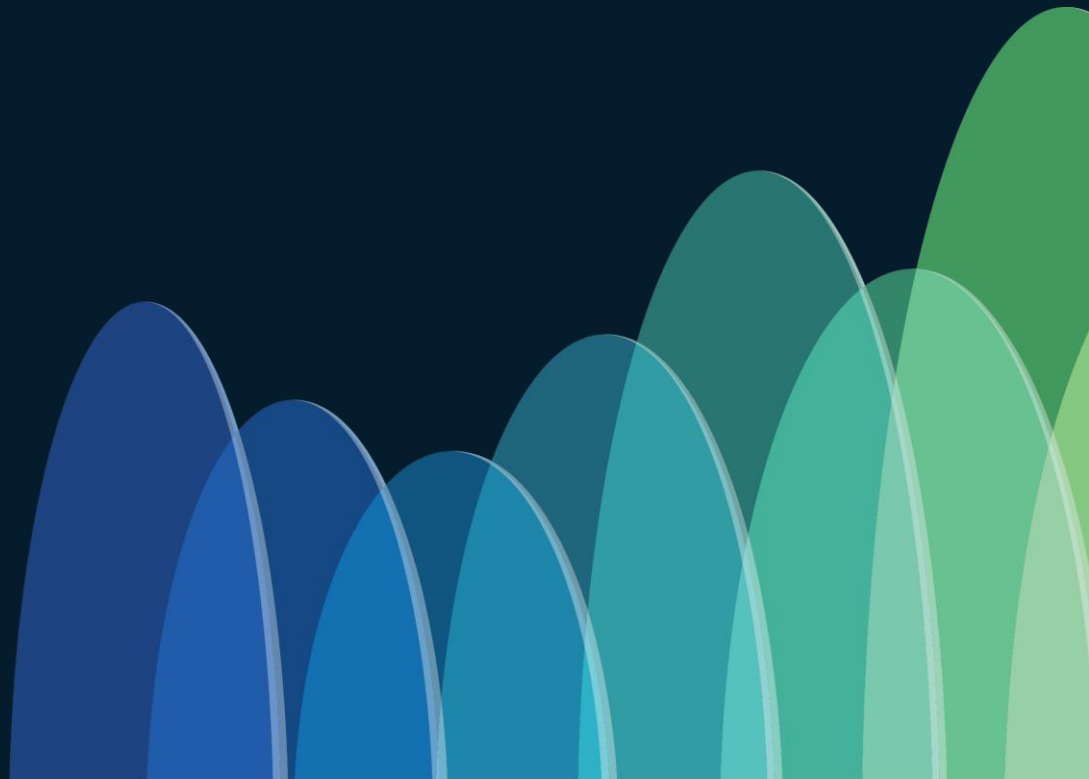
- The external server sends the API request to ISE in JSON format
- The attributes are stored in the persistent database, not the endpoint database (which is purged)



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public


Login - VMware ESXi
Identity Services Engine
YouTube
https://ise34ai.isedemolab.com/admin/#home
Identity Services Engine
Dashboard
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Features
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
32480
Active Endpoints
0
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
BYOD Endpoints
0
Complianc
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
21490
inter...users - 99.99%
inter...oints - <1%
NETWORK DEVICES
Device Name
Type
Location
32068
defau...evice - 99.98%
simulator - <1%
ENDPOINTS
Profile
Logical Profile
32453
unknown - 98.94%
other - 1.06%
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Occu...
Last Occurred
ISE Authentication In...
1652
7 mins ago
Log Collection Error
376
3 hrs 39 mins ago
Smart Licensing Auth...
25
3 hrs 44 mins ago
Insufficient Virtual M...
28
11 hrs 22 mins ...
SYSTEM SUMMARY
1 node(s)
All
24HR
ise34ai

- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- **Policies optimization**
- Create your own lab
- 802.1x Deployment Modes



Make use of Policy Sets

- Easier to read policies
- Better rule processing
- Group similar rules (MAB vs. dot1x, SSID, location)
- Conditions based on attributes from initial RADIUS packet:

Organizations

Type

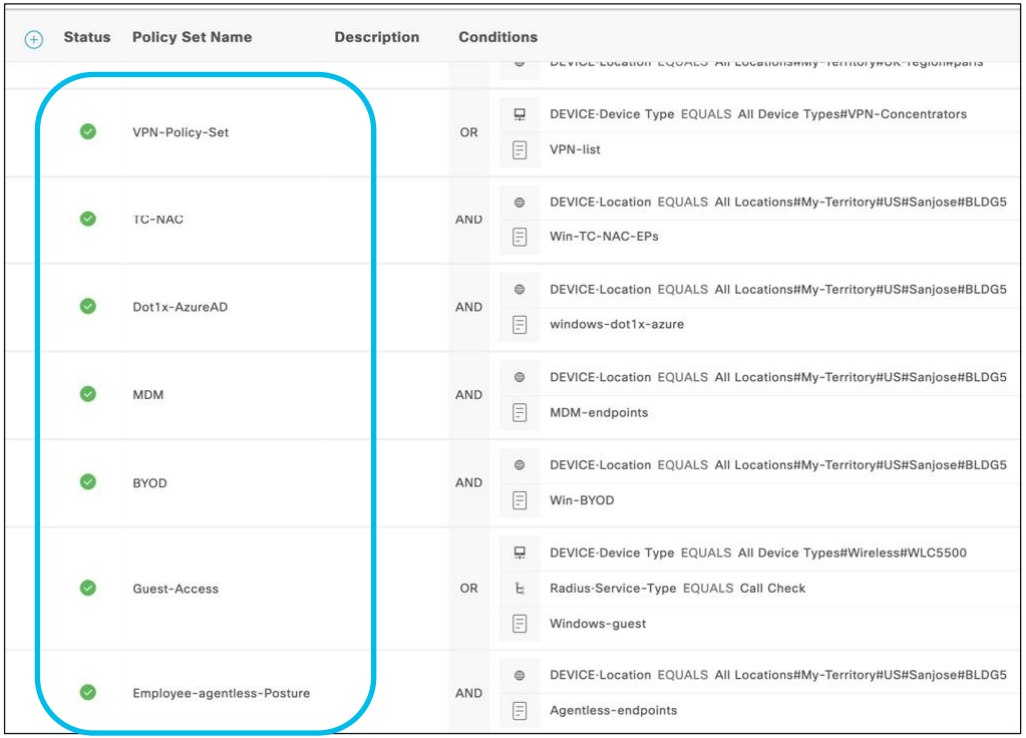
Location

Vendor/Model

Medium

RADIUS

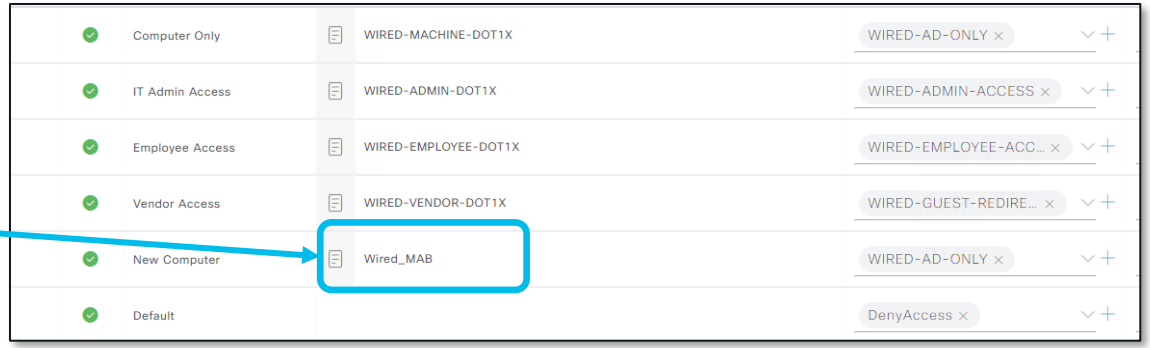
Wireless



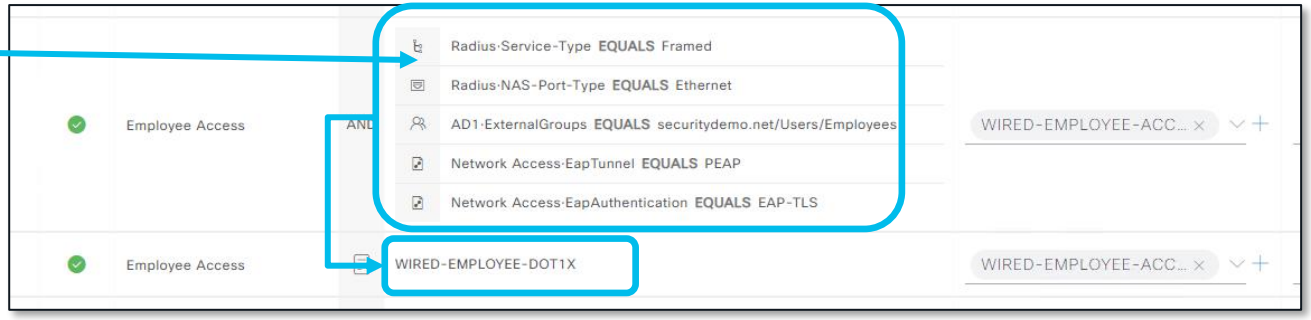
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Conditions simplification

Pre-sets Dictionary Condition are easy to read and intuitive



Custom created Conditions often are not as intuitive

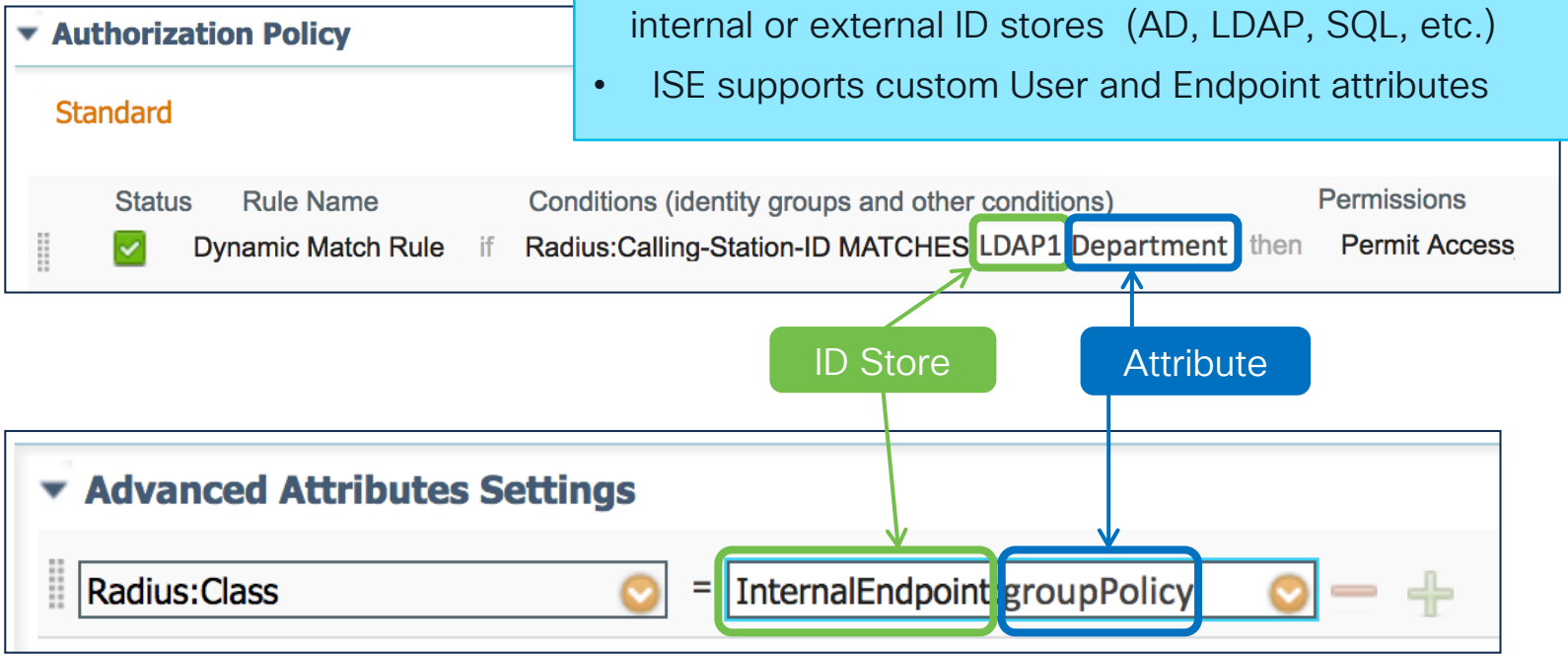


Use Compound Conditions and for custom ones

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Dynamic Variable Substitution

- Match conditions to unique values stored per- User/Endpoint in internal or external ID stores (AD, LDAP, SQL, etc.)
- ISE supports custom User and Endpoint attributes



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization

Policy Logic:
- First Match
- Top Down
- Skip Rule on first negative condition match

Employee

AND

AND

AD1·ExternalGroups **EQUALS** cts.local/Users/employees

OR

AD1·ExternalGroups **EQUALS** cts.local/Users/employees-contractors

1. AD Groups

AD1·msNPAllowDialin **EQUALS** true

2. AD Attributes

AND

MDM·DeviceRegisterStatus **EQUALS** Registered

3. MDM

CERTIFICATE·Subject - Organization Unit **CONTAINS** MyOrganization

4. Certificate

OR

IdentityGroup·Name **EQUALS** Endpoint Identity Groups:RegisteredDevices

5. ID Group

MyCorpSQL·Asset Type **EQUALS** Corporate

6. SQL Attributes

Network Access·EapAuthentication **EQUALS** EAP-TLS

7. Auth Method

AND

EndPoints·EndPointPolicy **STARTS_WITH** Windows7

OR

EndPoints·EndPointPolicy **STARTS_WITH** Windows10

8. Endpoint Profile

DEVICE·Location **EQUALS** All Locations#US#SanJose

9. Location

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Speed Test

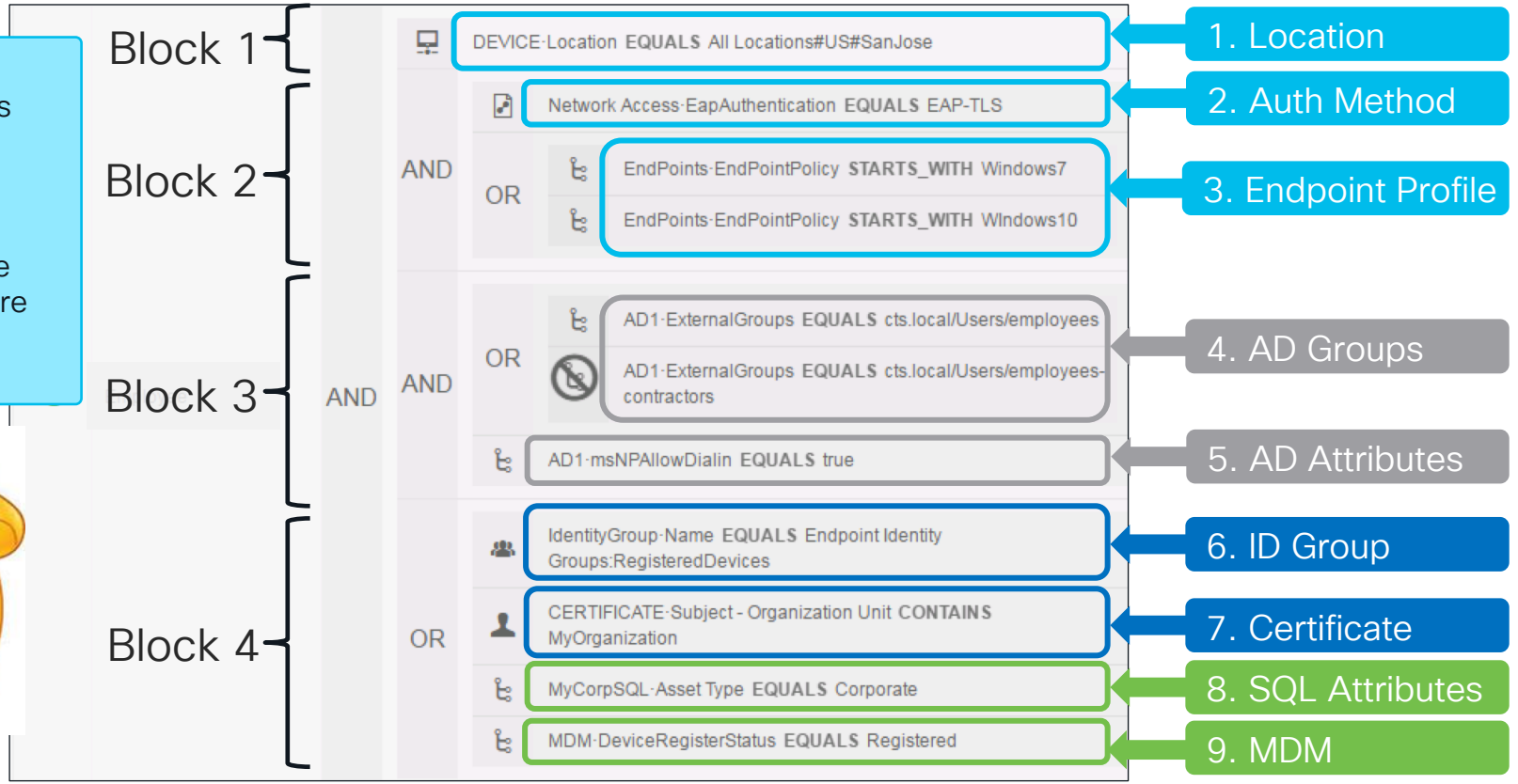
Is the image matching the condition set?

- Total stars = 10
- Total Green stars = 4
- Total red stars = 2
- Outer shape = Red triangle

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auth Policy Optimization

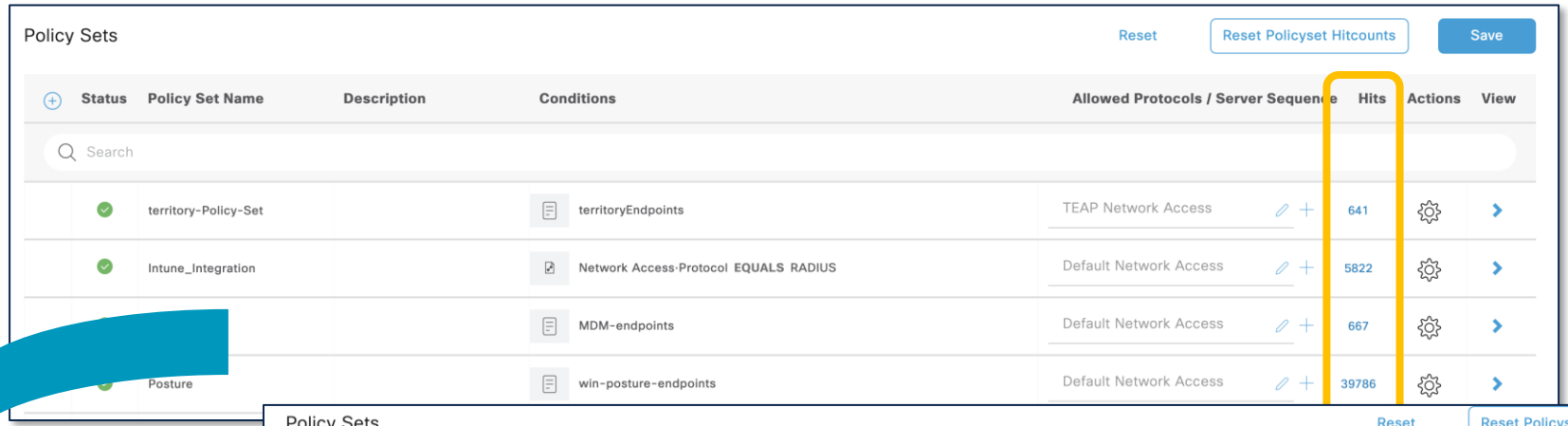
- Local conditions should be put before external
- External lookup should go at the end as take more time



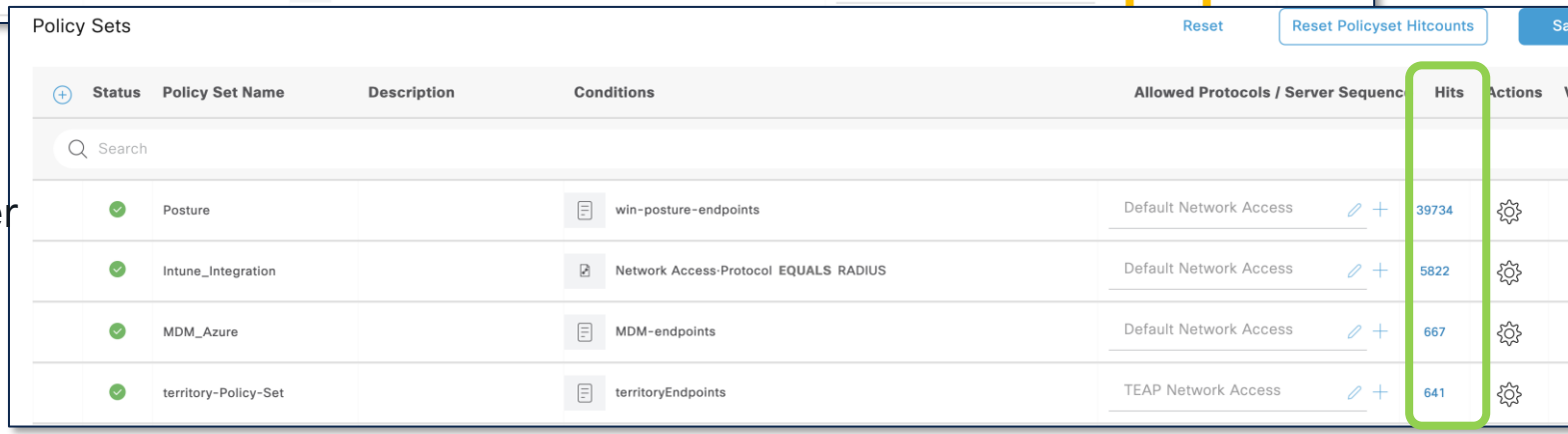
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Can you reorder some of the policy sets?

Review and Reorder

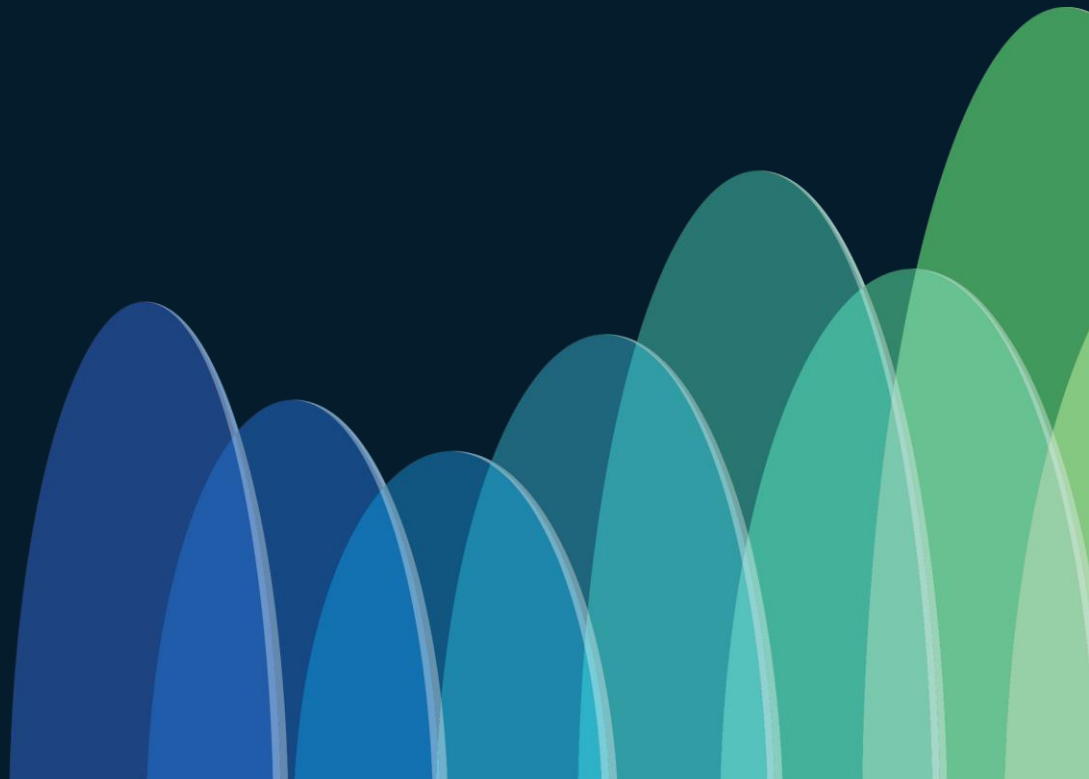


Review & Reorder



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- **Create your own lab**
- 802.1x Deployment Modes



Who Needs an ISE Lab? You do!

With ever Standalone installation :

- 90-day Evaluation license
- For 100 endpoints
- All Cisco ISE features
- 1 TACACS+ license

You can set up a limited deployment and test all the required features in your environment

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Lifecycle Orchestration & Policy Management

Zero Touch Deployment

Patch Installation

License Management

Certificate Management

Configuration Management

Policy Management

Operations Automation

ISE 3.1
Patch 1 or later

Python

Ansible

VSCode

github.com/CiscoISE

#YAML

```
network_device:
- name: lab-mr46-1
  description: ''
  profileName: Cisco
  authenticationSettings:
    dtlsRequired: false
    enableKeyWrap: false
    enableMultiSecret: 'false'
    keyEncryptionKey: ''
    keyInputFormat: ASCII
```


© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Deployment and Operational Lifecycle

Provision

VPC(s)
Networks
VPNs
ISE Nodes
Patch + Hotpatches
Load Balancers
…

Deploy

Enable APIs
Repositories
Roles
Services
Certificates
Licensing
…

Configure

Identity Stores
Network Devices
Policy Sets
Endpoints
Portals
…

Operate

Manage Endpoints
Reporting
Performance
pxGrid / Events
Backup/Restore
Patch
…

Extend

Terminate
…

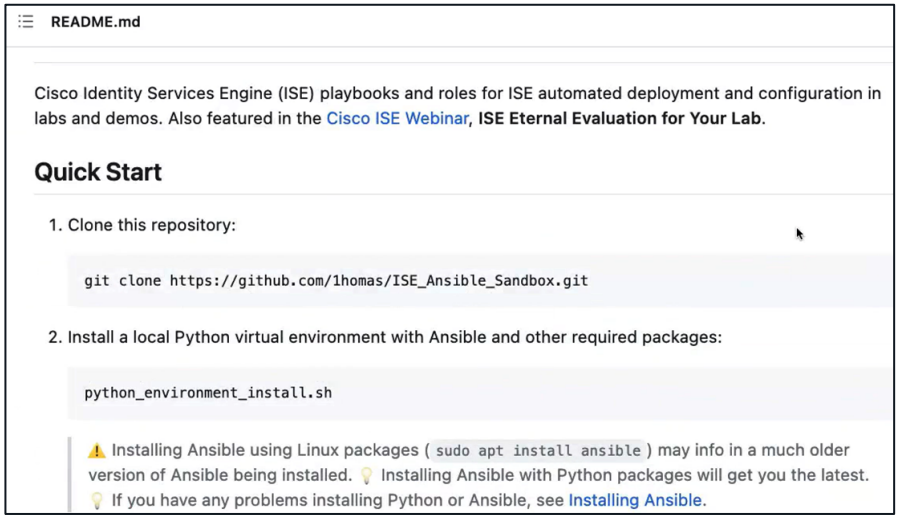
cisco Live!

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISE Eternal Evaluation

https://github.com/1homas/ISE_Ansible_Sandbox

Cisco ISE playbooks and roles for ISE automated deployment and configuration in labs and demos, beginning with the ISE Eternal Evaluation (ISEEE)


README.md

Cisco Identity Services Engine (ISE) playbooks and roles for ISE automated deployment and configuration in labs and demos. Also featured in the Cisco ISE Webinar, **ISE Eternal Evaluation for Your Lab**.

Quick Start

1. Clone this repository:

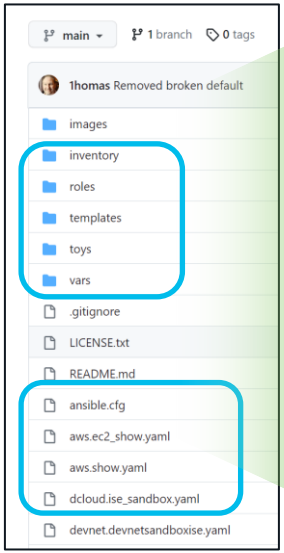
```
git clone https://github.com/1homas/ISE_Ansible_Sandbox.git
```

2. Install a local Python virtual environment with Ansible and other required packages:

```
python_environment_install.sh
```

> ⚠️ Installing Ansible using Linux packages (`sudo apt install ansible`) may info in a much older version of Ansible being installed. 💡 Installing Ansible with Python packages will get you the latest. 💡 If you have any problems installing Python or Ansible, see Installing Ansible.

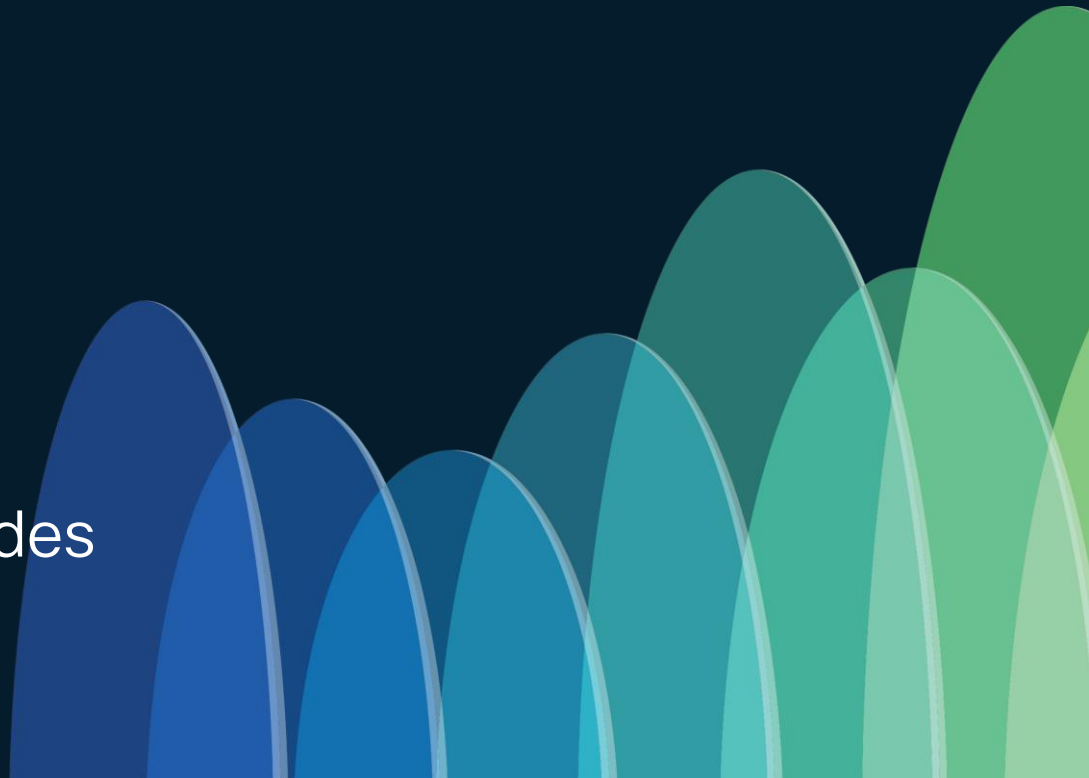
iseee.yaml



- iseee.**ssh**.yaml
- iseee.**provision**.yaml
- iseee.**facts**.yaml
- iseee.**patch**.yaml
- iseee.**deploy**.yaml
- iseee.**certificates**.yaml
- iseee.**licensing**.yaml
- iseee.**configure**.yaml
- iseee.**backup**.yaml
- iseee.**restore**.yaml
- iseee.**extend**.yaml
- iseee.**password_reset**.yaml
- iseee.**destroy**.yaml

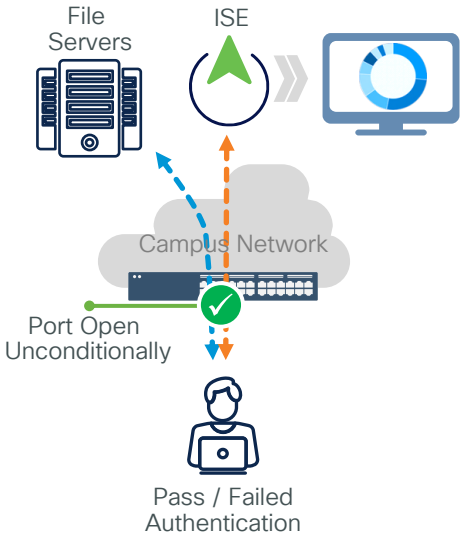
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

- Where to start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- Create your own lab
- 802.1x Deployment Modes



Deployment Modes

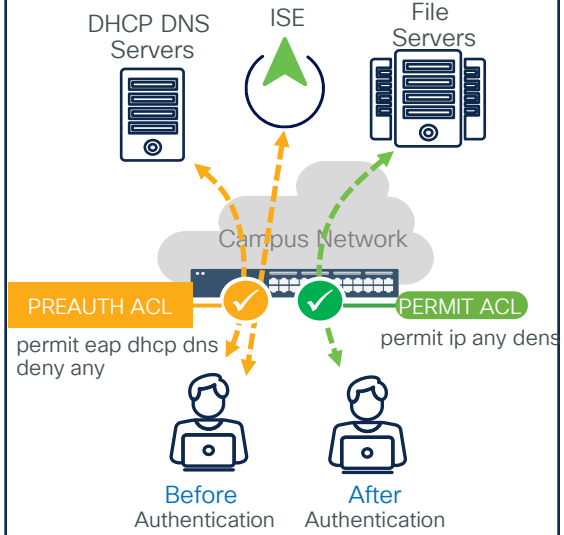
Monitor Mode (Visibility)




```
authentication open
```

No impact to existing network

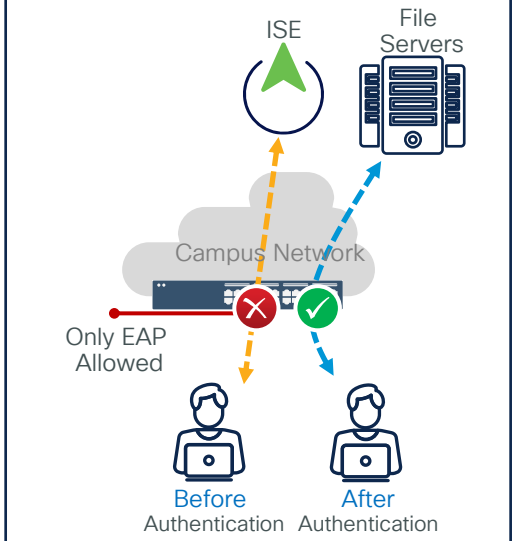
Low-Impact Mode (Visibility and Control)




```
ip access-group PRE-AUTH in
authentication open
```

Begin to control and differentiate access

Closed Mode (Visibility and Control)

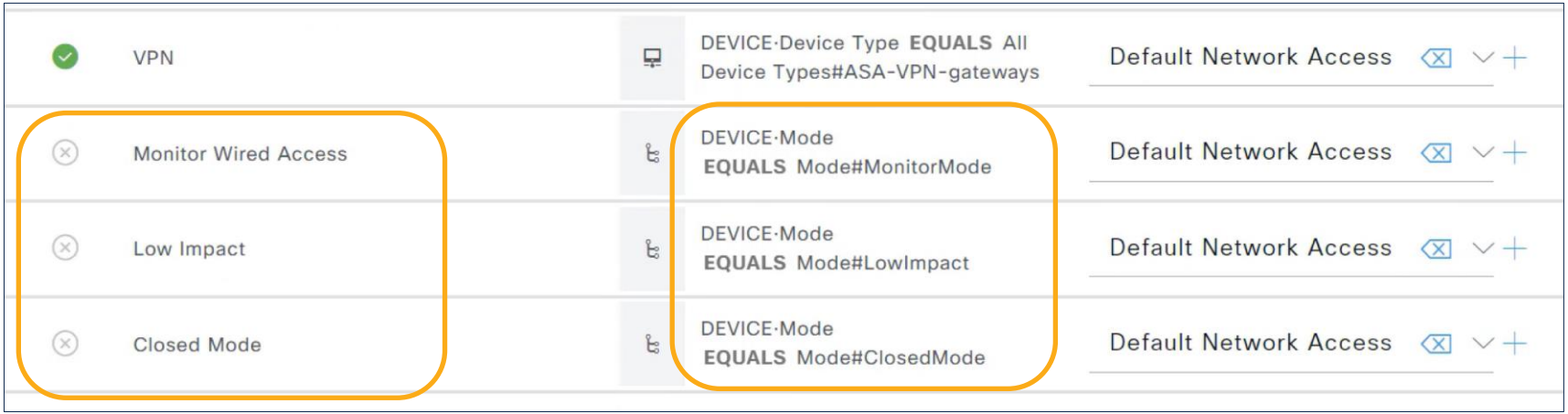


- Not everyone needs Closed Mode
- No access at all before authentication

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

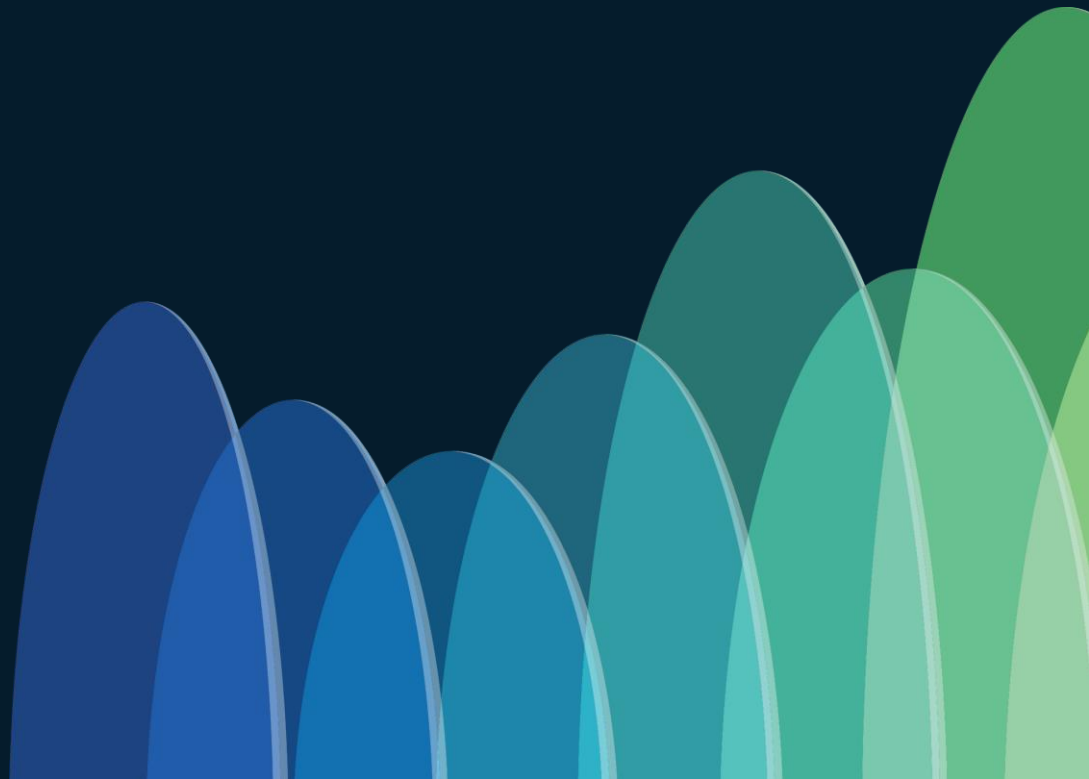
Utilizing Policy Sets with Modes

- When deploying leverage Network Device Groups
- Move devices in and out while the deployment progresses



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Day 2 Operations



User involvement

User Communication before and after ISE rollout

cisco Wired Authentication Support Page

Your workstation is Authenticated

What are we doing ?
IT Network Services are implementing 802.1x Authentication on the Wired Network in Cisco offices to bring it in line with the Wireless and CVO networks and adhere to Cisco's Network Access Policy. So that individuals with physical access to Cisco network ports cannot access Cisco data and potentially compromise Cisco's network from inside the network perimeter.

What is 802.1x ?
IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

What do I need to do ?
Cisco IT Managed devices should have 802.1x enabled on them already. If not – please see support instructions below...

Cisco Managed Windows Laptops	Mac Laptops	Remote Desktops **Windows Only**	Linux / Unix workstations	Voice/Video Endpoints	Non IT Managed Printers
Personal devices (Apple TVs, PlayStation etc.)	Routers, Switches, ESXi, and APs	Onsite (In-Office) – Patching	Demo/Training devices	Password Management	Generic Users
802.1x exception requests					

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Supporting ISE After Deployment

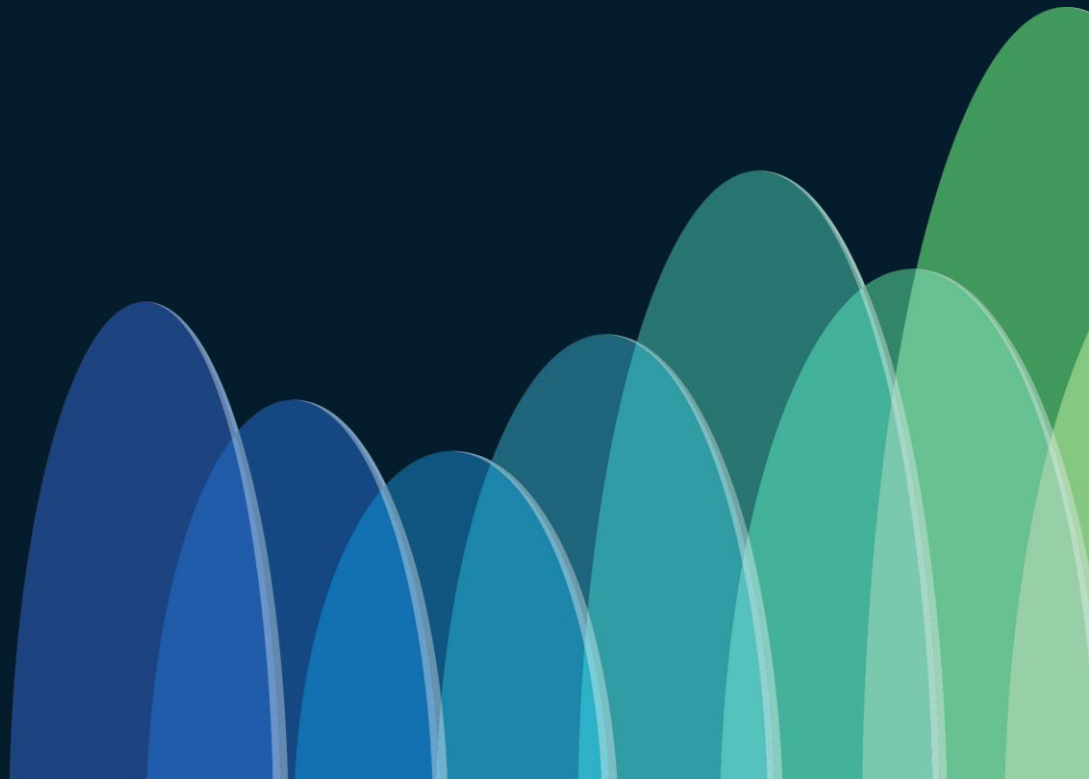
- Train Your Support with A Playbook for common issues

- Document as much as possible!
  - ✓ Policy Configuration
  - ✓ Supplicant Configuration
  - ✓ Network Access Devices

- Many document templates available on ISE Communities

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wrap up



Deploying any network access control solution is crucial

but it isn't easy....

Proper planning is essential to any successful development.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Technical Session Surveys

- Compliments ☺
- What you liked
- Suggestions?

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security

ISE

Learn how Cisco ISE will help you implement Network access Control in your campus. Sessions will cover how to plan and deploy, how to leverage the new cloud capabilities, best practices and other topics.

START

Monday, February 10 | 4:00 p.m.
BRKSEC-2100
ISE Your Meraki Network with Group Based Adaptive Policy

Tuesday, February 11 | 8:00 a.m.
BRKENS-1852
TrustSec Refresh Reinforced with Common Policy Innovations

Tuesday, February 11 | 12:00 p.m.
BRKSEC-2660
Setting the Stage for ISE Deployment Success: A Guide to Effective Planning

Tuesday, February 11 | 4:30 p.m.
BRKSEC-2416
Cisco ISE Meets Azure Cloud. Deploy, Automate, Integrate with Entra ID and Intune

Wednesday, February 12 | 8:00 a.m.
BRKSEC-2889
Mastering ISE Upgrades: Best Practices, Tips, and Tricks

Wednesday, February 12 | 1:00 p.m.
BRKSEC-2053
Zero Trust: Securing the Evolving Workplace

Thursday, February 13 | 10:45 a.m.
BRKSEC-3707
Advanced SGT - Multi Domain Context

Thursday, February 13 | 3:15 p.m.
BRKSEC-3234
Cisco ISE Performance, Scalability and Best Practices

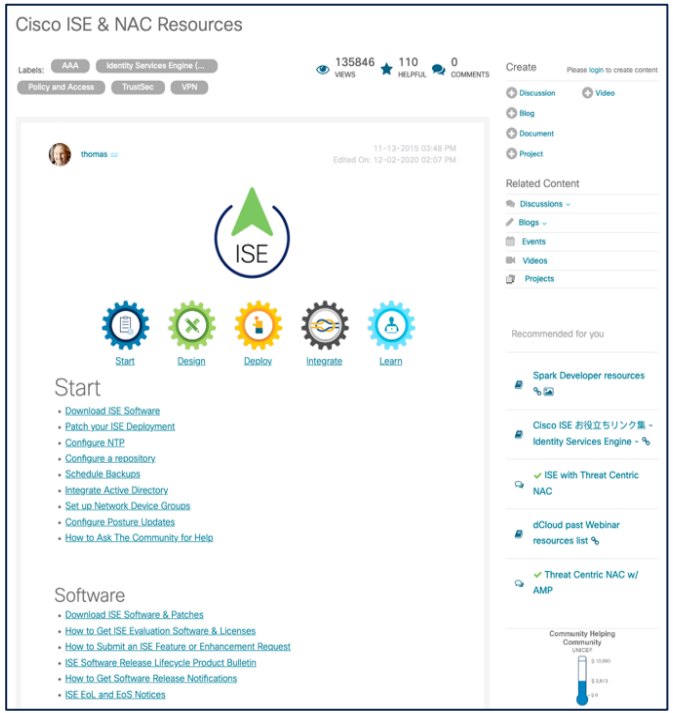
FINISH

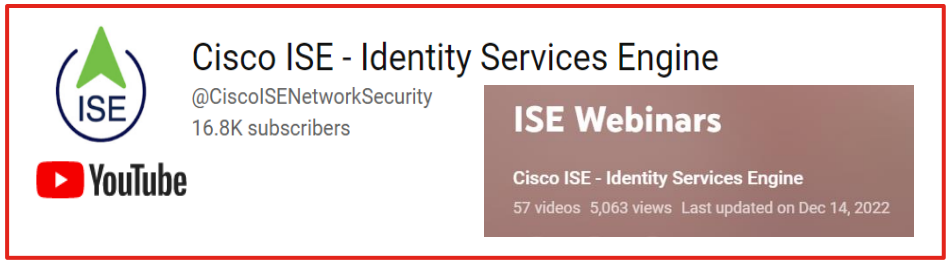
Friday, February 14 | 9:00 a.m.
BRKSEC-3077
A Song of ISE and Posture: Advanced Deployment and Troubleshooting

cisco Live!

Cisco ISE Resources

- Consolidated list of resources
  cs.co/ise-resources
- Community Q&A
  cs.co/ise-community
- Recorded webinars and other videos
  cs.co/ise-videos
- Integration Guides
  cs.co/ise-guides
- Licensing Guide
  cs.co/ise-licensing





Cisco Live 2025 FOR REFERENCE BRKSEC-2660

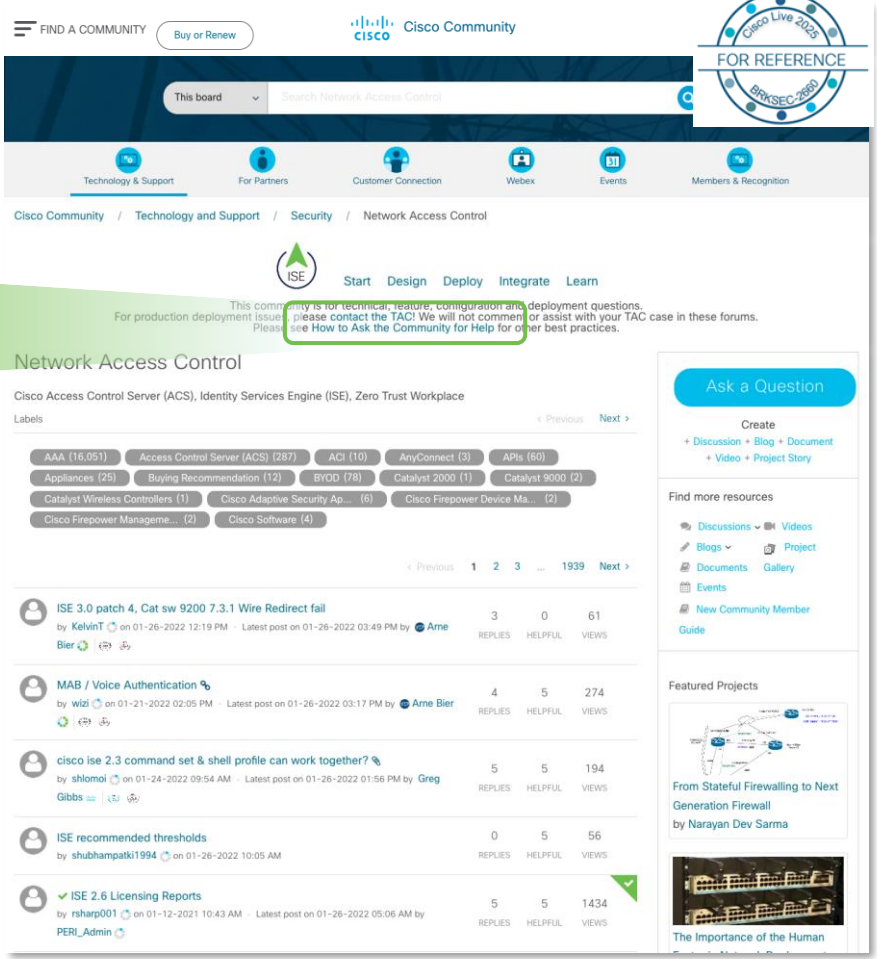
© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

Ask The Community

cs.co/ise-community

How to Ask the Community for Help

- The Community is Not TAC
- No Comment on Roadmaps or Fixes
- New Features and Feedback
- Provide Details
  - Goal/Scenario?
  - NAD Hardware & Software?
  - Endpoint OS(es)?
  - Browser(s)?
- Reproducibility (expected vs actual)
- Pictures and Video!



© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public

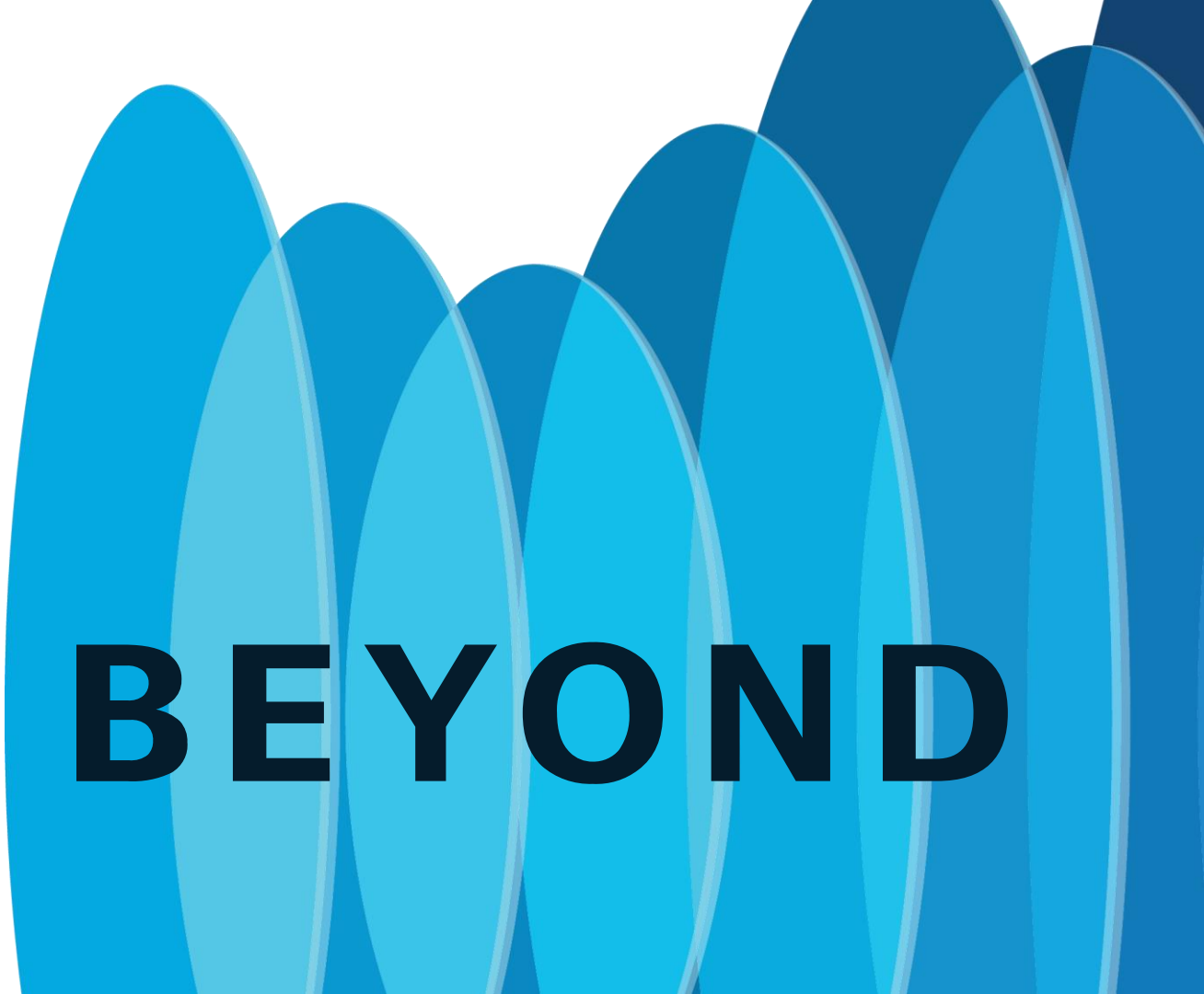
Continue your education

- 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.

© 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND