

ISE Deployment, Staging and Planning

Francesca Martucci, Technical Solutions Architect – Cybersecurity EMEA

ISE Planning, Deployment and Staging

Do I really need to plan?

Need to work with other teams in the organization:

- Virtualized environment
- Active Directory
- PKI
- Endpoint team
- Desktop support
- And possibly other teams



Deploying any network access
control solution is **crucial**
but it **isn't easy....**



Planning is **essential** to any
successful development.

Who am I?

- Technical Solutions Architect
Cyber Security EMEA
- In Cisco since 23 years...
... And 3 countries

Main interest on

- Policy and Access
- Segmentation
- Industrial Security





Agenda

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

What we are not covering



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



This presentation has many links at the end, to resources helping with all of them

Cisco Webex App

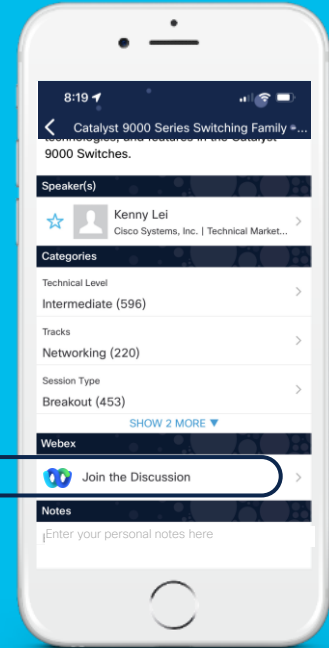
Questions?

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

How

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

Webex spaces will be moderated until February 24, 2023.



- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



Cisco ISE High Level Design (HLD)



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.

Enterprise

Security



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

Use cases

What is the business trying to accomplish with ISE?
Which ones could be considered for the future?



 Asset Visibility	Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources.
 Access Control	Consistent access control across wired, wireless and VPN Networks. 802.1X, MAC, Web Authentication and Easy connect for admission control.
 Guest Access	Fully customizable branded mobile and desktop guest portals, with dynamic visual workflows to easily manage guest user experience.
 BYOD Access	Simplified BYOD management with built-in CA and 3rd party MDM integration for on boarding and self-service of personal mobile devices
 Segmentation	Topology independent Software-defined segmentation policy to contain network threats.
 Context Exchange	Context sharing with partner eco-system to improve their overall efficacy and accelerate time to containment of network threats.
 Threat Control	Protection against threats across the attack continuum, before, during and after an attack. Reduce time-to-detection from days to hours.
 Device Admin	Cisco ISE supports device administration using the TACACS+ security protocol to control and audit the configuration of network devices

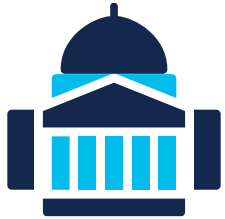
Defining your Security Policy

What is an IT security policy?

*“Identifies **rules and procedures** for all individuals **accessing and using** an organization’s **IT assets and resources.**”*

Everyone Has Different Needs

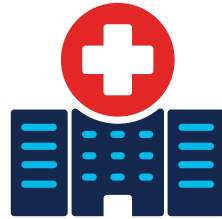
Government



Financials



Healthcare



Retail



Education



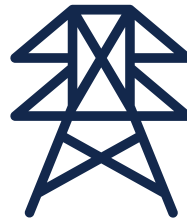
Transportation



Services



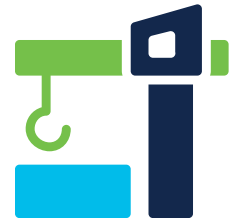
Utilities



Technology



Manufacturing



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

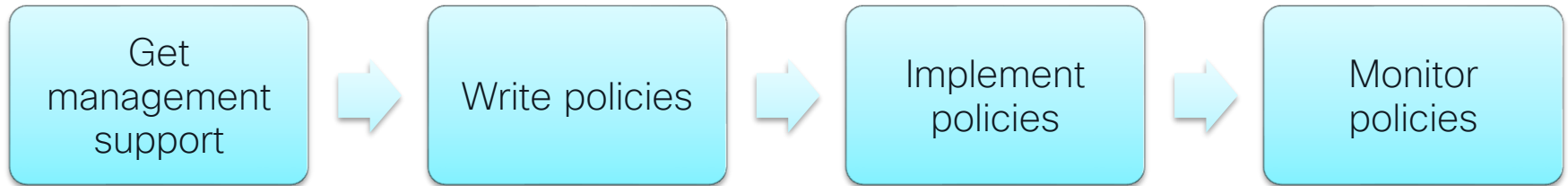
Network Team

Security Team

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

IT Security Policy important considerations

- Security Policy should not be written by “feature”
- Need to know your Security Policy prior to deploy
- Get management buy-in
- Monitor and update polices with your IT Security Policy



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

ISE Deployment Planning



cs.co/ise-hld



cs.co/ise-resources#Planning



ISE High Level Design (HLD)

- Business Objectives
- Environment
 - Physical Network Topology
 - Identity Sources
 - User Groups
 - Network Devices
 - Endpoints
 - ISE Cube
- Device Administration (TACACS+)
- Visibility
- Secure Access : Wireless / Wired / VPN
- Guest : HotSpot / Registered / Sponsored / API
- BYOD
- Integration : Context Sharing / Threat Mitigation / APIs
- Compliance
- Segmentation
- Containment
- Operations & Management
- Scale & High Availability
- Policy Details
- Resources



ISE Planning & Pre-Deployment Checklists

- Planning Checklists
 - Business Objectives
 - Organizational
 - Security Policy Creation and Maintenance
 - Scale
 - Public Key Infrastructure (PKI)
 - Directory Services
 - Network Access Devices (NADs)
 - Managed Endpoints
 - Assets
 - Cisco Identity Services Engine (ISE)
 - Guest Services
 - Monitoring, Reporting, and Troubleshooting
 - Communications
 - Support Desk
- Deployment Checklists
 - Network Services
 - Digital Certificates
 - Network Devices
 - Security Policy
 - Enforcement States
 - Endpoints
 - Test Scenarios

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



ISE Personas

Policy Administration Node (PAN)

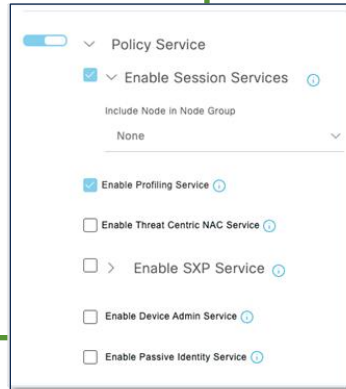
- Administrative GUI
- Policy configuration
- Policy replication
- Centralized Guest database
- Centralized BYOD database
- Configuration REST APIs

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

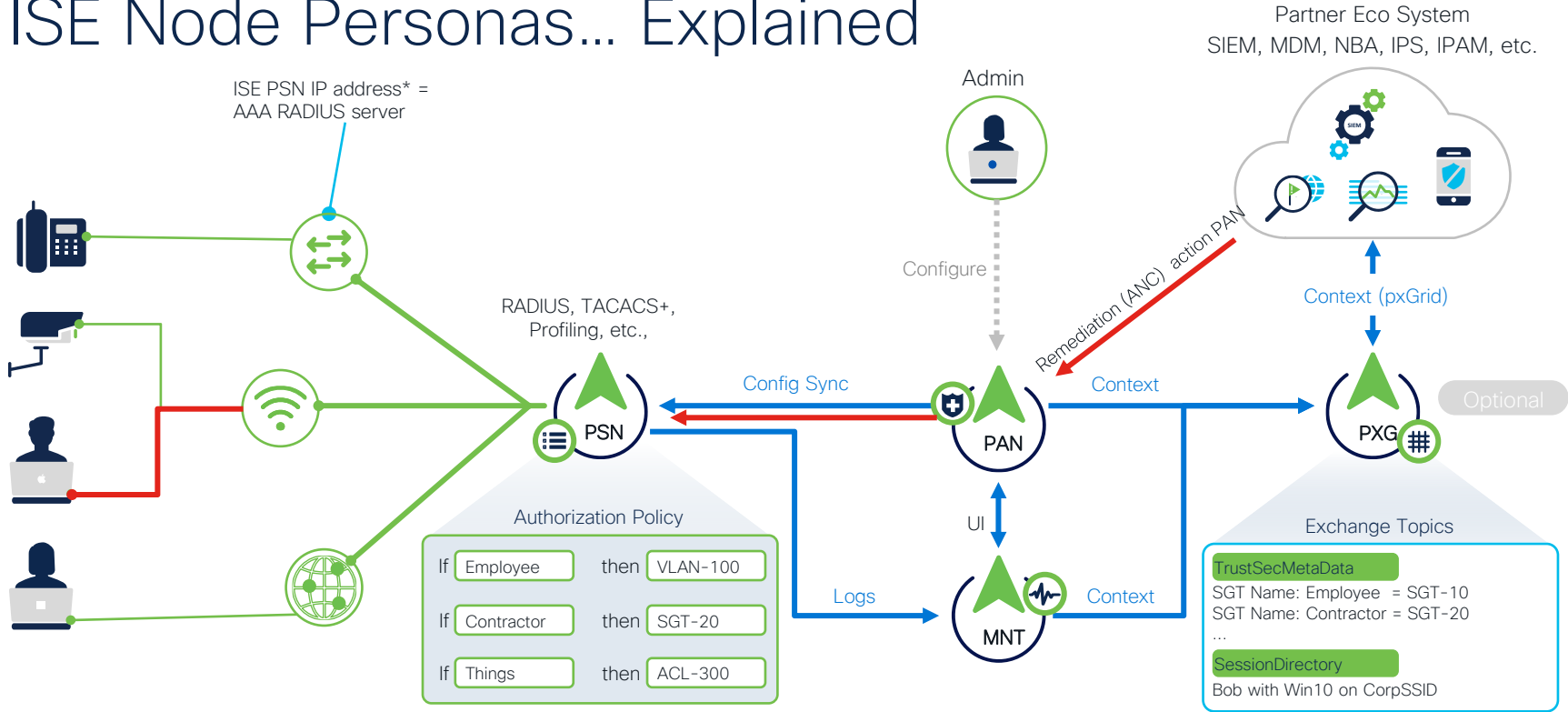


Platform Exchange Grid Node (PXG)

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



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

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)

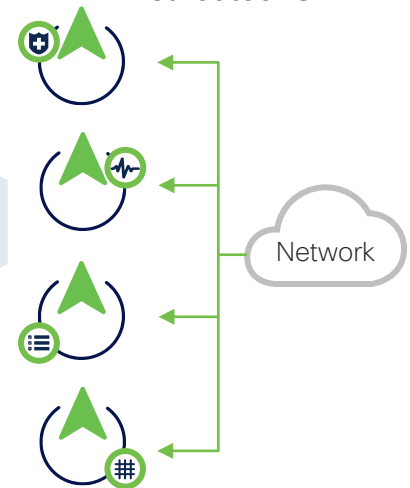
- Max 50 in a deployment



pxGrid Controller

- Max 4 in deployment

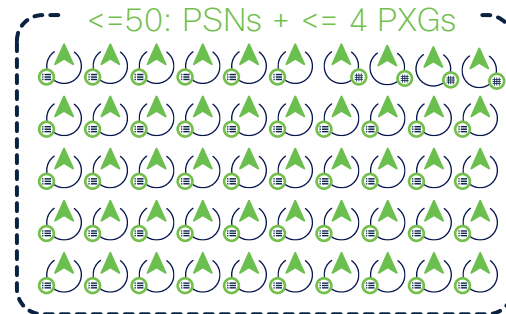
Distributed ISE



ISE Distributed Deployment Scale

Same for physical and virtual deployments

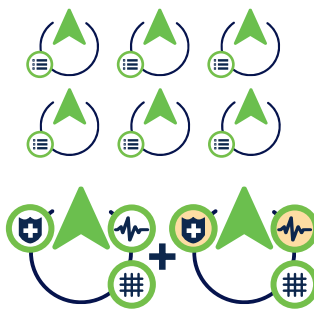
Compatible with load balancers



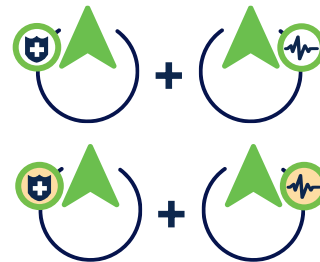
Standalone
(for Lab and
Evaluation)



Small HA
Deployment
 $2 \times (\text{PAN} + \text{MNT} + \text{PSN})$



Medium Multi-node
Deployment
 $2 \times (\text{PAN} + \text{MNT} + \text{PXG}), \leq 6 \text{ PSN}$



Large Deployment
 $2 \text{ PAN}, 2 \text{ MNT}, \leq 50: \text{PSNs}$
 $+ \leq 4 \text{ PXGs}$

100 Endpoints

Up to 20,000 Endpoints

Up to 500,000 Endpoints

3500

100 Endpoints

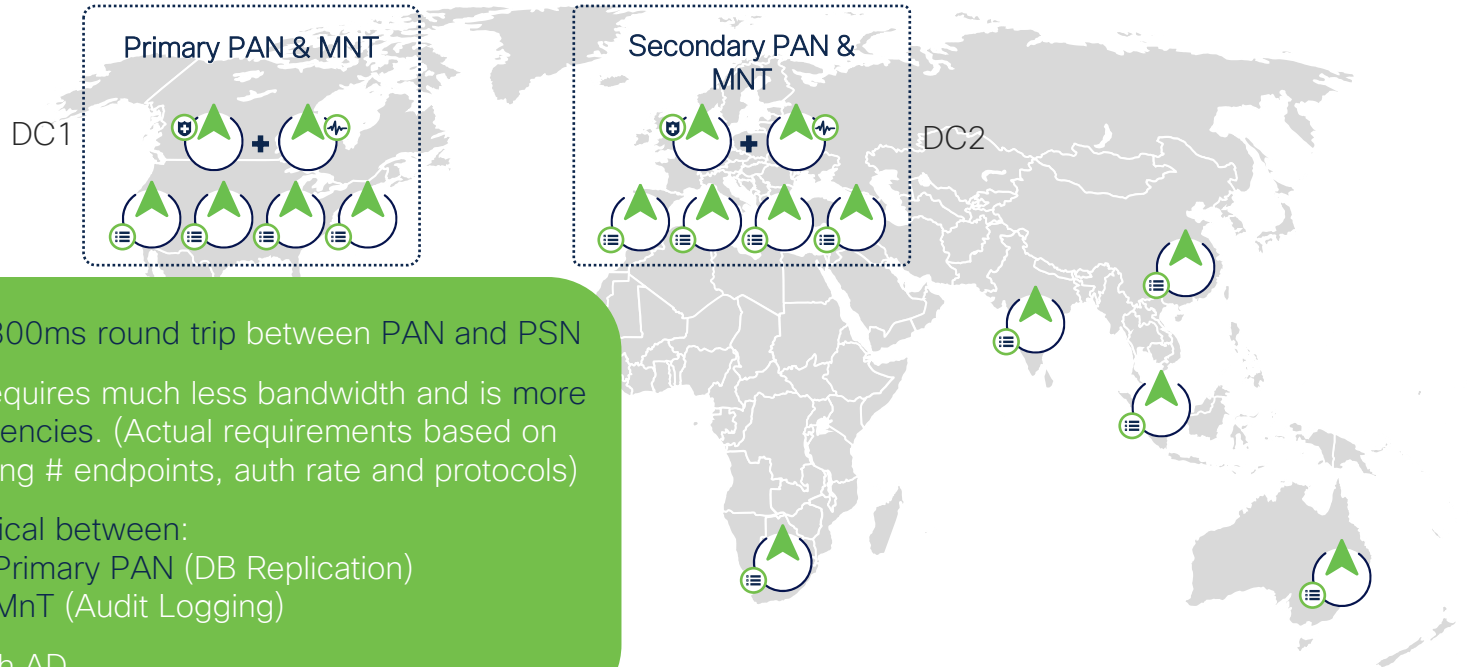
Up to 50,000 Endpoints

Up to 2,000,000 Endpoints

3600

ISE Fully Distributed Architecture

Centralize in DCs...or Distribute PSNs across Geographies



- Latency should be 300ms round trip between PAN and PSN
- RADIUS generally requires much less bandwidth and is more tolerant of higher latencies. (Actual requirements based on many factors including # endpoints, auth rate and protocols)
- Bandwidth most critical between:
 - PSNs and Primary PAN (DB Replication)
 - PSNs and MnT (Audit Logging)
- Co-locate PSNs with AD

Maximum Concurrent Active Endpoints



- ISE Licensing is counted by *active endpoint sessions*
- RADIUS Accounting defines session **Start & Stop** events
- Sessions **Start** upon RADIUS Authorization
- Sessions **Stop** upon :
 - Disconnect
 - Session Expiration
 - Idle Timeout

ISE Nodes – Mix and Match

Physical Appliances



SNS-3715

SNS-3755

SNS-3795

SNS-3615

SNS-3655

SNS-3695

SNS-3595

Virtual Machines



Cloud Instances



- Use resource reservations (built into OVAs)
- Do NOT oversubscribe!

SNS-37xx appliances

SNS-3715

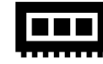
3715
Cisco Identity Services Engine



Intel 4310
2.1GHz
12 Cores



600GB HDD
800GB SSD¹
960GB SED¹



32GB



2 X 1GbE
4 X 10Gb SFP



RAID0



TPM¹

SNS-3755

3755
Cisco Identity Services Engine



Intel 4316
2.3GHz
20 Cores



4X600GB HDD
4X800GB SSD¹
4X960GB SED¹



96GB



2 X 1GbE
4 X 10Gb SFP



RAID10



TPM¹

SNS-3795

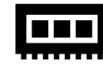
3795
Cisco Identity Services Engine



Intel 4316
2.3GHz
20 Cores



8X600GB HDD
8X800GB SSD¹
8X960GB SED¹



256GB



2 X 1GbE
4 X 10Gb SFP



RAID10



TPM¹

Distributed Scalability Numbers



 cs.co/ise-scale

Platform	Concurrent active endpoints supported by a dedicated PSN (<u>Cisco ISE node only has PSN persona</u>)	Concurrent active endpoints supported by a shared PSN (<u>Cisco ISE node has multiple personas</u>)
Extra Small (VM only)	12,000	unsupported
SNS 3615	25,000	12,500
SNS 3595	40,000	20,000
SNS 3695	50,000	25,000

Deployment Type	Platform	Max Concurrently Connected Endpoints in ISE Deployment
Standalone (All personas on a single node)	3615	10,000
	3595	20,000
	3655	25,000
	3695	50,000
Small deployment (Basic 2-node)	3615	10,000
	3595	20,000
	3655	25,000
	3695	50,000
Medium deployment (Admin + MnT; PSN dedicated)	3615	10,000
	3595	20,000
	3655	25,000
	3695	50,000
Large deployment (PAN, MnT, PXG, and PSN Nodes)	3595	500,000
	3655	500,000
	3695	2,000,000

Summary Endpoints Guests Vulnerability Threat

Total Endpoints

1

Active Endpoints

0

Rejected Endpoints

0

Anomalous Behavior

0

Authenticated Guests

0

BYOD Endpoints

0

AUTHENTICATIONS

Identity Store Identity Group Network Device Failure Reason

No data available.



NETWORK DEVICES

Device Name Type Location

No data available.

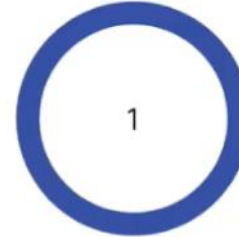


ENDPOINTS

Profile Logical Profile

1

vmware-device - 100%



BYOD ENDPOINTS

Type Profile

No data available.

ALARMS

Severity Name Occu... Last Occurred

Severity	Name	Occu...	Last Occurred
▲	ISE Authentication In...	388	8 mins ago

SYSTEM SUMMARY

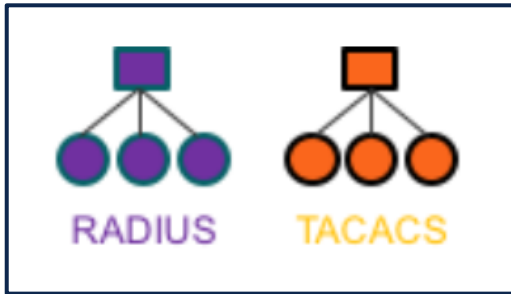
1 node(s)
ISE31-1ok

All 24HR

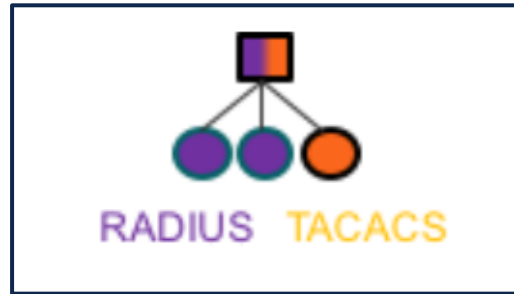
ISE RADIUS vs TACACS+ Deployment Models

Separating RADIUS & TACACS+ ISE Cubes?

There are three different options:



Separate ISE cubes for
RADIUS & TACACS+



Mixed ISE cube with
separate PSNs for
RADIUS and TACACS+



Mixed ISE cube where
PSNs are not
dedicated to either

When do we separate TACACS+ and RADIUS?

Things to consider

- Device Admin service enabled per PSN
- Sizing is NOT per device count
- Scalability is transactions per second (TPS)

- Authentication? Command authorization?
- Scripts? Network management tools?

- Number of TACACS+ & RADIUS sessions if PSN is shared
- Per-PSN utilization and load

- Where To Start: planning
- ISE Deployment Options
- **Certificates**
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



ISE Certificates



✓ System Certificates

- Identifies a [cisco ISE node & services](#)
- [Specific to the node](#)
- Can [manage](#) all node's system certs [from PPAN](#)

✓ Trusted Certificates

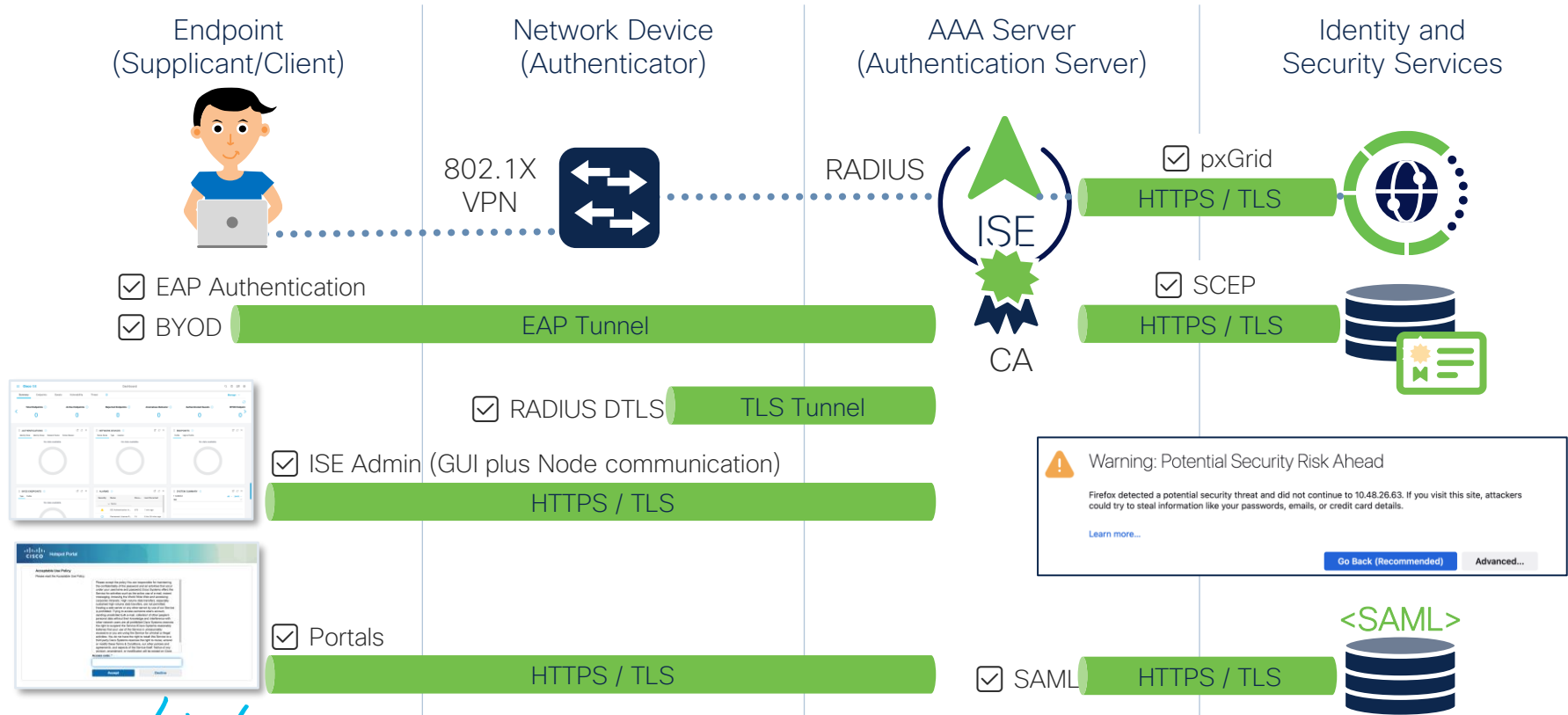
List of CAs

- from which [endpoint certs](#) are [issued](#) for [cert-based authentication](#)
- from which [users' certs](#) are issued for [admin UI access](#)
- for [secure communication](#) with [external entities](#)
- for ISE [Internal services](#)
- [Replicated](#) to [all the nodes](#) in deployment

✓ ISE Issued Certificates

- [Internal CA](#) service, [issues and manages](#) certificates for [endpoints, pxGrid and ISE messaging](#)

Different ISE System certificates



Systems and Trusted Certificates

System Certificates

⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

[Edit](#)
[+ Generate Self Signed Certificate](#)
[+ Import](#)
[Export](#)
[Delete](#)
[View](#)

Friendly Name	Used By	Portal group tag	Issued To	Issued By
<input type="checkbox"/> ISE30-1ek OU=Certificate Services System Certificate,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00002	pxGrid		ISE30-1ek.example.com	Certificate Services Endpoint Sub CA -
<input type="checkbox"/> Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ISE30-1ek.example.com	ISE30-1ek.example.com
<input type="checkbox"/> Default self-signed saml server certificate - CN=SAML_ISE30-1ek.example.com	SAML		SAML_ISE30-1ek.example.com	SAML_ISE30-1ek.example.com
<input type="checkbox"/> OU=ISE Messaging Service,CN=ISE30-1ek.example.com#Certificate Services Endpoint Sub CA - ISE30-1ek#00001	ISE Messaging			

ISE30-2ek
 ISE30-3ek
 ISE30-4ek

Which ISE role is using the certificate

Self signed certificate

EAP Authentication, Admin, Portal, RADIUS DTLS

ISE30-1ek.example.com

Trusted Certificates

⚠ For disaster recovery it is recommended to export and backup all your trusted certificates.

[Edit](#)
[+ Import](#)
[Export](#)

Friendly Name	Trusted For	Serial Number	Issued To	Issued By
<input type="checkbox"/> Cisco ECC Root CA 2099	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA
<input type="checkbox"/> Cisco Licensing Root CA	Cisco Services	01	Cisco Licensing Root...	Cisco Licensing Root...
<input type="checkbox"/> Cisco Manufacturing CA SHA2	Infrastructure Endpoints	02	Cisco Manufacturing ...	Cisco Root CA M2
<input type="checkbox"/> Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2B ...	Cisco Root CA 2048	Cisco Root CA 2048
<input type="checkbox"/> Cisco Root CA 2099	Cisco Services	01 9A 33 58 78 ...	Cisco Root CA 2099	Cisco Root CA 2099

To install certificate

Each ISE node has its own System Certificate Store

Summary Endpoints Guests Vulnerability Threat

Total Endpoints

1

Active Endpoints

0

Rejected Endpoints

0

Anomalous Behavior

0

Authenticated Guests

0

BYOD Endpoints

0

AUTHENTICATIONS

Identity Store Identity Group Network Device Failure Reason

No data available.



NETWORK DEVICES

Device Name Type Location

No data available.

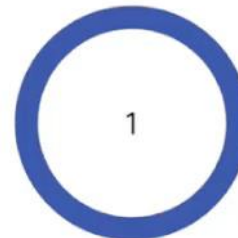


ENDPOINTS

Profile Logical Profile

1

vmware-device - 100%



BYOD ENDPOINTS

Type Profile

No data available.

ALARMS

Severity Name Occu... Last Occurred

Name

Configuration Changed 1 1 min ago

SYSTEM SUMMARY

1 node(s)
ISE31-1ek

All 24HR

Sample pxGrid Certificate Template

The screenshot displays the Server Manager interface. On the left is a navigation pane with 'Dashboard' selected. The main area is titled 'WELCOME TO SERVER MANAGER' and contains a 'QUICK START' section with a numbered list of five steps: 1. Configure this local server, 2. Add roles and features, 3. Add other servers to manage, 4. Create a server group, and 5. Connect this server to cloud services. Below this is the 'ROLES AND SERVER GROUPS' section, which shows a summary of roles (5) and server groups (1) for the local server. Three role cards are displayed: AD CS, AD DS, and DNS, each with a progress bar and a list of associated features like Manageability, Events, Services, Performance, and BPA results.

Dashboard

- Local Server
- All Servers
- AD CS
- AD DS
- DNS
- File and Storage Services ▾
- IIS

WELCOME TO SERVER MANAGER

QUICK START

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

WHAT'S NEW

LEARN MORE

Hide

ROLES AND SERVER GROUPS

Roles: 5 | Server groups: 1 | Servers total: 1

Role	Count
AD CS	1
AD DS	1
DNS	1

Role	Count
AD CS	1
AD DS	1
DNS	1

Role	Count
AD CS	1
AD DS	1
DNS	1

Role	Count
AD CS	1
AD DS	1
DNS	1

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



Network Device discovery

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

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

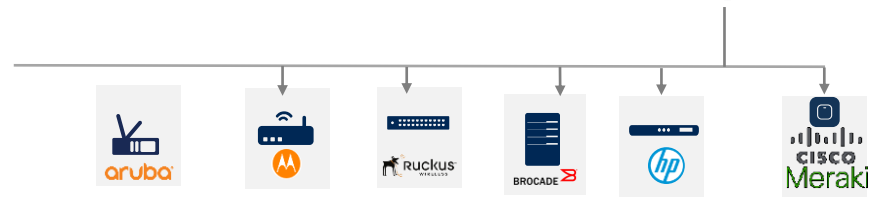
Validated Cisco Access Switches

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 Sx500 1.2.0.97	4	!	X	X	X	X	X	X
		!	!	X	X	X	X	X	X

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

Third-Party Network Device Compatibility



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.

	Aruba	Generic Wireless Router	Ruckus	Brocade	HP	Cisco Meraki
802.1X	✓	✓	✓	✓	✓	✓
Profiling	✓	✓	✓	✓	✓	✓
Posture	✓	✓		✓	✓	✓
Guest	✓	✓		✓	✓	✓
BYOD	✓	✓		✓	✓	✓

Capabilities

- Templated MAB configuration for select non-Cisco vendor devices
- CoA and URL re-direction
- Non-Cisco NADs enabled to drive regular 802.1X operations



*Refer to [Cisco Compatibility Matrix](#)
<http://cs.co/ise-compatibility>

Additional Tips

- Standardize! **Standardize!** Standardize!
 - IOS versions
 - AAA configuration
 - Wireless configuration
 - Profiling configuration
- Always **Test before implementing!**
- 3rd party device documentation
 - **Vendor Specific RAIDUS dictionary** needed?
 - **Network Device Profile creation** needed?

Total Endpoints ⓘ

165

Active Endpoints ⓘ

5

Rejected Endpoints ⓘ

0

Anomalous Behavior ⓘ

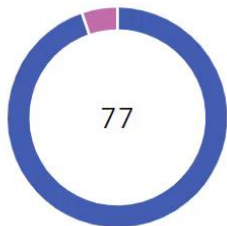
0

Authenticated

AUTHENTICATIONS ⓘ

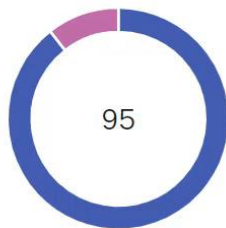
Identity Store Identity Group Network Device

Failure Reason



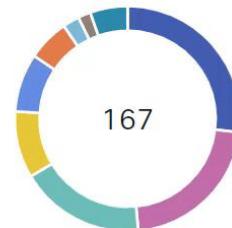
NETWORK DEVICES ⓘ

Device Name Type Location

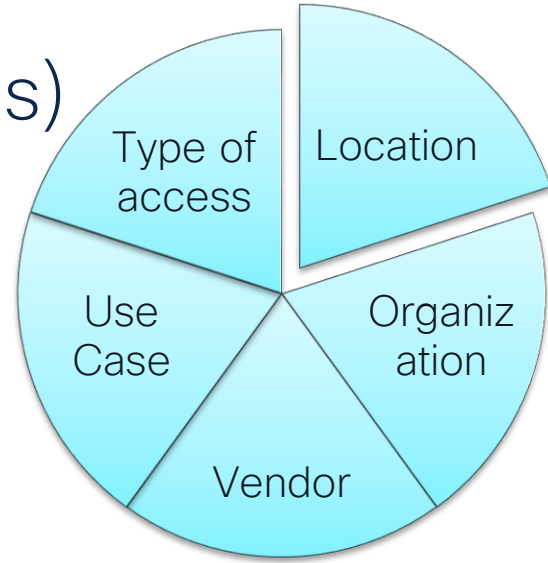


ENDPOINTS ⓘ

Profile Logical Profile



Default Network Device Groups (NDGs)



Network Devices **Network Device Groups** Network Device Profiles Ext...

Network Device Groups

All Groups Choose group ▾

Refresh Add Duplicate Edit Trash Show group members Imp...

<input type="checkbox"/> Name	Description
<input type="checkbox"/> All Device Types	All Device Types
<input type="checkbox"/> All Locations	All Locations
<input type="checkbox"/> ▾ Is IPSEC Device	Is this a RADIUS over IP...
<input type="checkbox"/> No	Device is not IPSEC Type
<input type="checkbox"/> Yes	Device is IPSEC Type

Refresh Add Duplicate Edit

- Name
- > All Device Types
- ▾ All Locations
- ▾ AMER
- ▾ US
- ▾ San Jose
- ▾ Building
- Floor
- > Countries
- > Departments
- > Is IPSEC Device
- > Orgs
- > Regions

Default NDGs

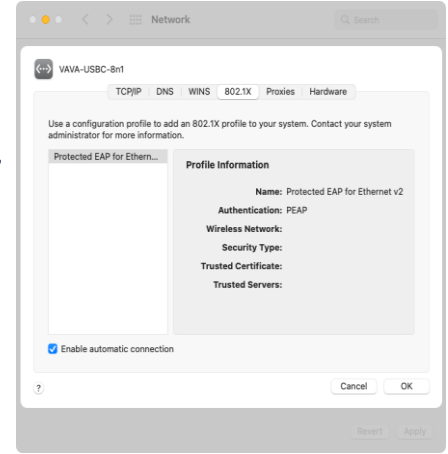
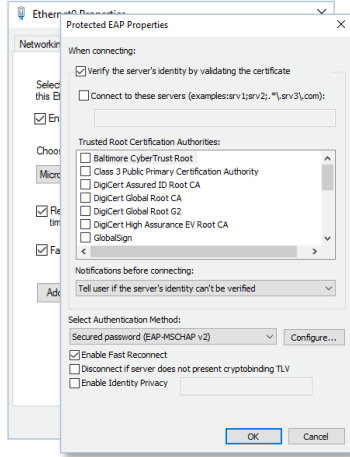
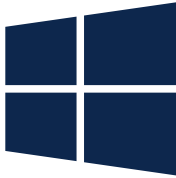
Maximum 6 Levels

Create Your Own Root NDGs

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- **Supplicants**
- Profiling
- Policies optimization
- 802.1x Deployment Phases



Endpoints: Native 802.1X Supplicants



RADIUS-802.1x

EAP method

PEAP

Phase-2 authentication

MSCHAPV2

CA certificate

Do not validate

No certificate specified. Your connection will not be private.

Identity

username

Anonymous identity

Password

password

Show password

Advanced options

Cancel Save

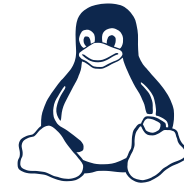


```
wpa_supplicant

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

SYNOPSIS
wpa_supplicant [ -BddfhKLqgsTtuvW ] [ -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
```



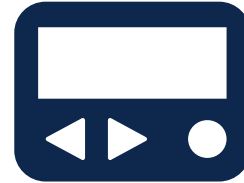
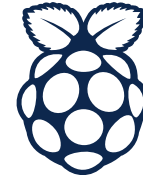
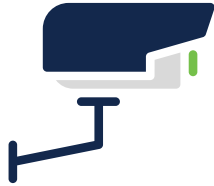
Windows 7, 8/8.1, and 10 – Native Supplicant

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

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



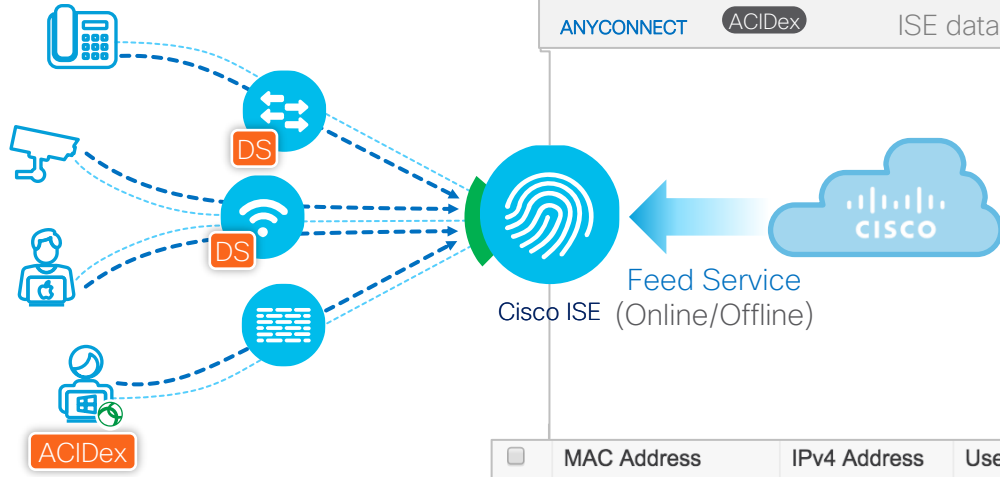
Endpoints: Everything Else



Profiling and probes

ISE data collection methods for Device profiling

ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP	AD
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS	
ANYCONNECT	ACIDex							



Configuration interface for the Feed Service:

- Enable Online Subscription Update
- Automatically check for updates every day at: 01 hh 10 mm UTC *(i)*
-
- Test result:
- Notify administrator when download occurs
- Administrator email address:

Endpoints send interesting data, that reveal their device identity

Profiling helps with differentiated access also for authenticated devices

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

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

Effect of SNMP Probe



Unknown

OUI = Random, IP = xx.xx.xx.xx



Cisco IP Phone 9971

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

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

Effect of HTTP Probe



Windows 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

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-ipad1.zero0k.org

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

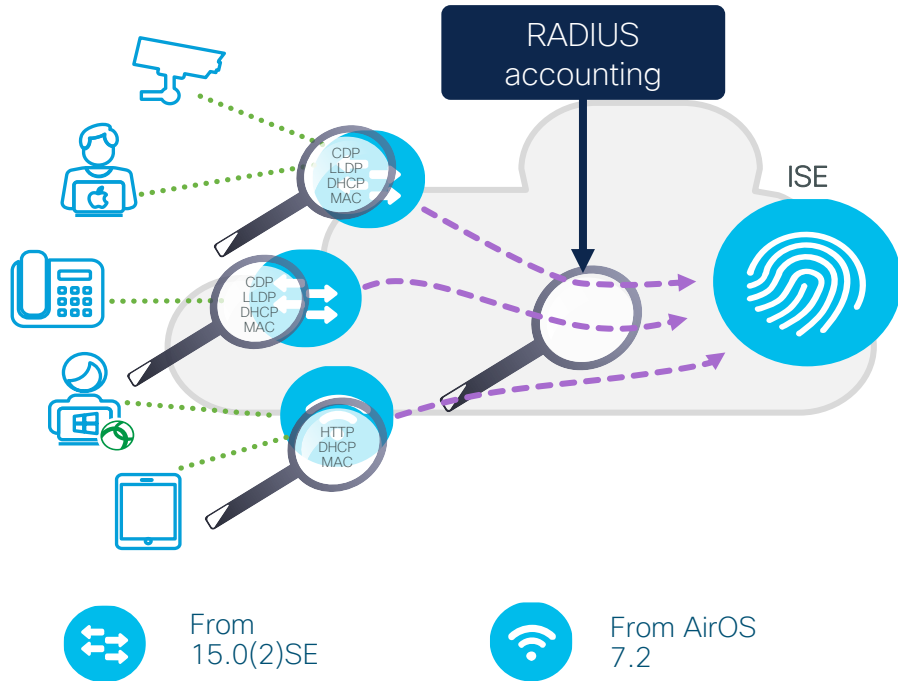
OUI = HP, IP = xx.xx.xx.xx, DHCP:dhcp-class-identifier CONTAINS LaserJet, FQDN=test-printer1.zero0k.org, SNMP:hrDeviceDescr CONTAINS HP LaserJet P4015



Apple iPad

OUI = Apple, IP = xx.xx.xx.xx, IP:User-Agent contains iPad, FQDN=test-ipad1.zero0k.org

Device Sensor

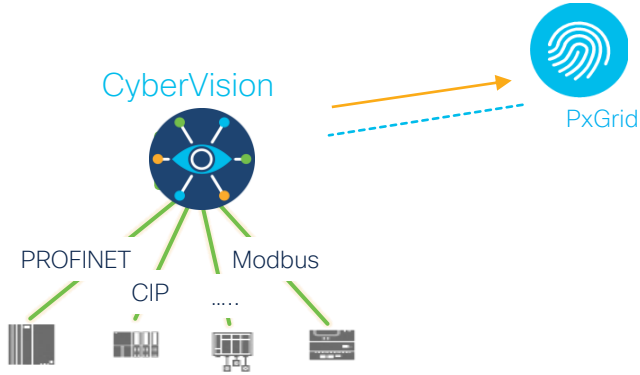


Network devices send **attributes** via **RADIUS** to ISE to optimize collection:

Attributes used:

- MAC OUI
- CDP/LLDP
- DHCP
- HTTP (WLC only)
- mDNS,
- H323,
- MSI-Proxy (4k only)

PxGrid Probe



- CyberVision classifies the OT devices.
- The attributes are then sent to ISE via pxGrid
- ISE populates the custom attributes with the ones received via profiling pxGrid probe

Profiling

Profiler Settings

CoA Type* Reauth

Current custom SNMP community strings ***** Show

Change custom SNMP community strings ? !

Confirm changed custom SNMP community strings: ? !

EndPoint Attribute Filter ?

Anomalous Behaviour Detection ?

Anomalous Behaviour Enforcement

Custom Attribute for Profiling Enforcement

Profiling for MUD

Profiler Forwarder Persistence Queue

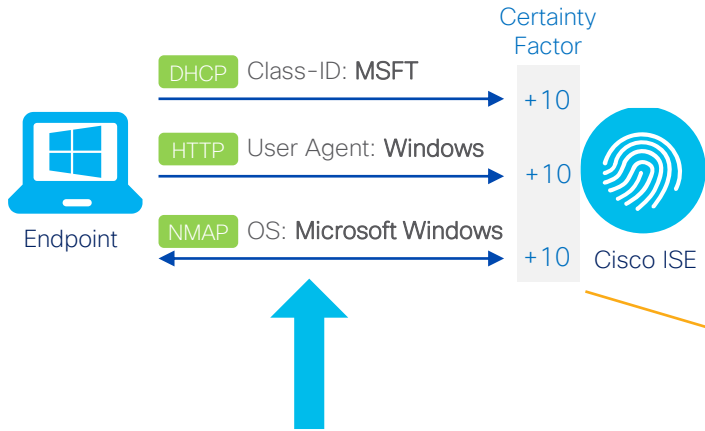
XSS Security Scan Enforcement for EndPoint Probe Data ?

Endpoint Custom Attributes

Attribute Name	Type
assetGroup	String
assetTag	String
assetVendor	String
assetDeviceType	String
assetID	String
assetName	String
assetSerialNumber	String
assetProtocol	String

MACAddress	00:1D:9C:CA:85:8B
MatchedPolicy	Rockwell-Automation-Device
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	5
assetConnectedLinks.assetDeviceType	Switch
assetConnectedLinks.assetId	40109
assetConnectedLinks.assetIpAddress	10.195.119.22
assetConnectedLinks.assetName	IE4000-119-22
assetConnectedLinks.assetPortName	GigabitEthernet1/2
assetDeviceType	Controller
assetId	60100
assetIpAddress	10.195.119.38
assetMacAddress	00:1d:9c:ca:85:8b
assetName	10.195.119.38
assetProductId	1756-EN2TR/C 217021900
assetProtocol	CIP
assetSerialNumber	12174476
assetVendor	Rockwell Automation/Allen-Bradley

ISE profiles definition



- DHCP:dhcp-class-identifier CONTAINS MSFT
- DHCP:dhcp-class-identifier CONTAINS MS-UC-Client
- IP:User-Agent CONTAINS Windows
- NMAP:operating-system CONTAINS Microsoft Windows

Profiler Policy List > Microsoft-Workstation

Profiler Policy

* Name: Microsoft-Workstation Description: Generic policy for Microsoft workstation

Policy Enabled:

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: Yes, create matching Identity Group No, use existing Identity Group hierarchy

Parent Policy: Workstation

* Associated CoA Type: Global Settings

System Type: Cisco Provided

Rules

Condition	Action	Value
If Condition: Microsoft-WorkstationRule2Check1	Then Certainty Factor Increases	10
If Condition: Microsoft-Workstation-Rule4-Check1	Then Certainty Factor Increases	10
If Condition: Microsoft-WorkstationRule3Check1	Then Certainty Factor Increases	10
If Condition: Microsoft-WorkstationRule1Check1	Then Certainty Factor Increases	10

Profiling Packages and Integrations

Medical Devices



Hospital



250+ Medical device profiles

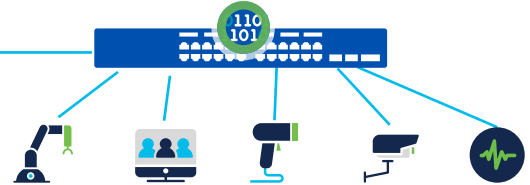
Pharma-Smart-Device
Philips-Analytical-X-Ray-Device
Philips-CareServant-Device
Philips-Healthcare-PCCI-Device
Philips-Medical-Systems-Device
Philips-Oral-Healthcare-Device
Philips-Patient-Monitoring-Device
Philips-Personal-Health-Device
Philips-Respironics-Device
Phonak-Communications-Device

IOT Building & Automation

Library



Siemens-Device
Siemens-Automation-Drives-Device
Siemens-Building-Device
Siemens-Building-Technologies-Device
Siemens-Convergence-Device
Siemens-Digital-Factory-Device
Siemens-Energy-Automation-Device
Siemens-Energy-Management-Device
Siemens-Home-Office-Device
Siemens-Industrial-Automation-Device



Cisco AI Endpoint Analytics

Profiles IOT devices and sends endpoint labels via pxGrid to ISE for authorization



Factory



Industrial Devices

pxGrid



Cisco
CyberVision

<https://community.cisco.com/t5/tag/ise-endpoint-profile/tg-p/board-id/4561-docs-security>



Using device profiles and logical profiles in ISE

The image illustrates the configuration of logical profiles in Cisco ISE. It shows three main components:

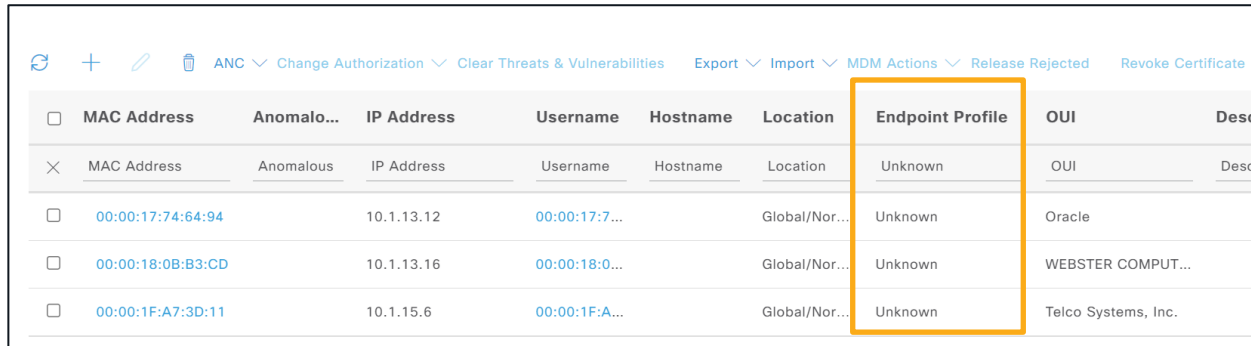
- Left Panel:** A navigation menu with categories like Profiling Policies, Logical Profiles, Cameras, Gaming Devices, Home Network Devices, IP-Phones, Infrastructure Network Devices, Medical Devices, Mobile Devices, and Printers.
- Top Middle Panel:** Configuration for the 'Printers' logical profile. It shows the name 'Printers', a description 'Default logical profile for printers.', and a list of assigned policies including Brother-HL-3040CN-series, Brother-HL-5370DW-series, Brother-MFC-8890DW, Brother-MFC-9010CN, Canon-MF4690, Canon-Printer, Epson-TM-Series-Printer, HP-Color-LaserJet-2500, and Android.
- Top Right Panel:** Configuration for the 'Cameras' logical profile. It shows the name 'Cameras', a description 'Default logical profile for cameras.', and a list of assigned policies including Axis-Network-Camera, Cisco-IP-Camera, and Trendnet-Camera.
- Bottom Panel:** A table of endpoint identity groups. The table has columns for a status icon, the group name, the identity group name, and a removal button. The groups are: 'Cisco IP Phones' (IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone), 'Printers' (EndPoints-LogicalProfile EQUALS Printers), and 'Cameras' (EndPoints-LogicalProfile EQUALS Cameras).

Arrows indicate the flow of configuration: from the 'Printers' and 'Cameras' logical profile configuration screens to the corresponding rows in the endpoint identity groups table.

Status	Group Name	Identity Group Name	Removal Button
✓	Cisco IP Phones	IdentityGroup Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone	Cisco_IP_Phones ×
✓	Printers	EndPoints-LogicalProfile EQUALS Printers	AuthZ_Printers ×
✓	Cameras	EndPoints-LogicalProfile EQUALS Cameras	AuthZ_Cameras ×

ISE Profiling 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
- You will still have unknowns For everything else: [custom profiles](#)



The screenshot shows the Cisco ISE Profiling interface. At the top, there are navigation icons and menu items: Refresh, Add, Edit, Delete, ANC, Change Authorization, Clear Threats & Vulnerabilities, Export, Import, MDM Actions, Release Rejected, and Revoke Certificate. Below this is a table with the following columns: MAC Address, Anomalous, IP Address, Username, Hostname, Location, Endpoint Profile, OUI, and Description. The 'Endpoint Profile' column is highlighted with an orange box. The table contains three rows of data, all with 'Unknown' in the 'Endpoint Profile' column.

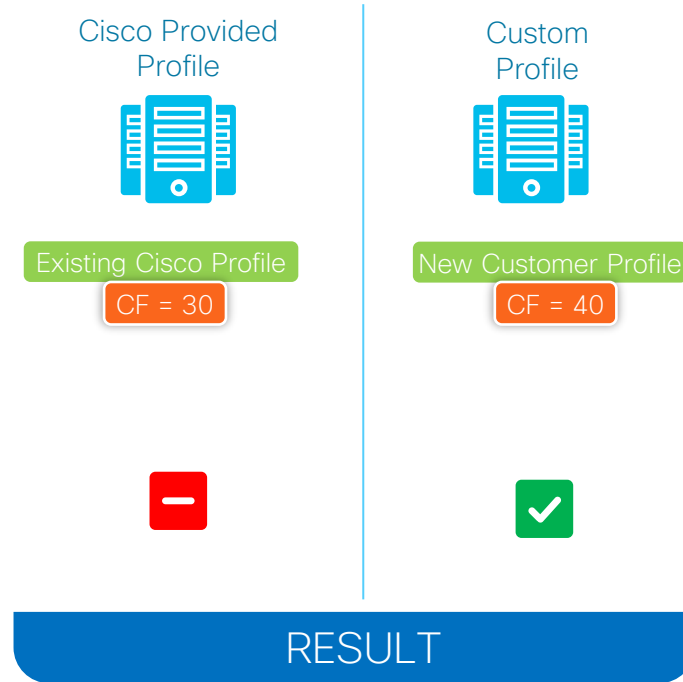
<input type="checkbox"/>	MAC Address	Anomalo...	IP Address	Username	Hostname	Location	Endpoint Profile	OUI	Descr
<input checked="" type="checkbox"/>	MAC Address	Anomalous	IP Address	Username	Hostname	Location	Unknown	OUI	Descr
<input type="checkbox"/>	00:00:17:74:64:94		10.1.13.12	00:00:17:7...		Global/Nor...	Unknown	Oracle	
<input type="checkbox"/>	00:00:18:0B:B3:CD		10.1.13.16	00:00:18:0...		Global/Nor...	Unknown	WEBSTER COMPUT...	
<input type="checkbox"/>	00:00:1F:A7:3D:11		10.1.15.6	00:00:1F:A...		Global/Nor...	Unknown	Telco Systems, Inc.	

Create custom profiles

- Gather more information
 - Create more traffic from the device
 - Run an NMAP scan
 - Enable more probes
- Find attributes or combinations of attributes unique to device type
- Focus on:
 - Attributes found every time the endpoint connects
 - Attributes found very early after the endpoint connects

dhcp-class-identifier	udhcp 0.9.7
dhcp-client-identifier	01:00:14:48:00:30:8c
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 3, 6, 12, 15, 28
dhcp-requested-address	10.1.100.103
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
Other Attributes	
5060-tcp	sip
80-tcp	http
AAA-Server	ise
hlen	6
htype	Ethernet (10Mb)
OUI	Inventec Multimedia & Telecom Corporation
OriginalUserName	00144800308c
PolicyVersion	8
PostureApplicable	Yes
op	BOOTREQUEST
operating-system	Linux 2.4.9 - 2.4.18 (likely embedded)
operating-system-result	Linux 2.4.9 - 2.4.18 (likely embedded)
yiaddr	0.0.0.0

Profiles Precedence



Endpoint Analysis Tool

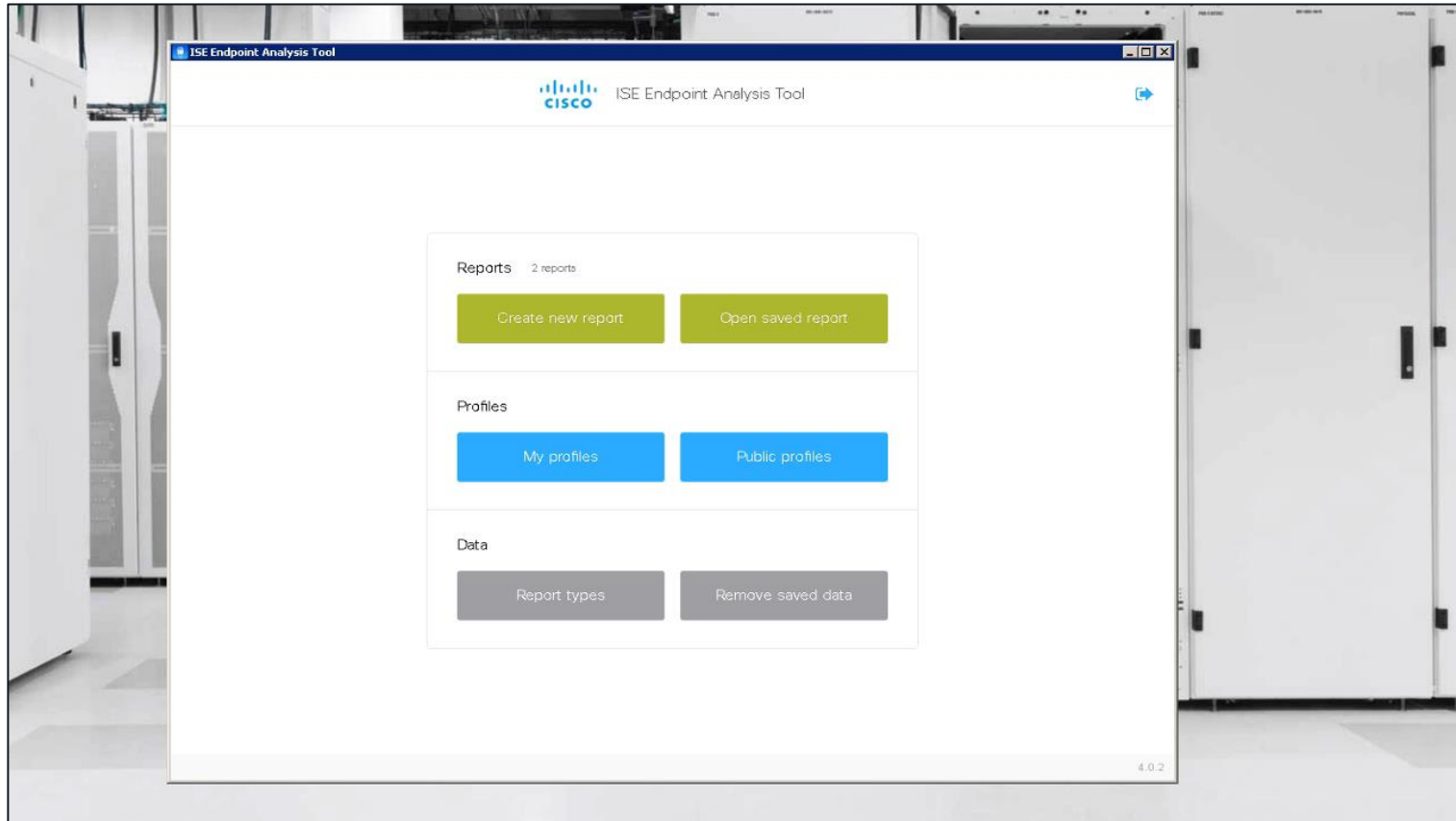
- Collects endpoint attributes from Primary PAN database
- Select attributes to be used in new profile and click “Create Profile”
- Option to edit condition criteria before complete
- Import XML into ISE
- Advanced profile tuning can be performed inside ISE

<http://iseeat.cisco.com>

The screenshot displays the ISE Endpoint Analysis Tool interface. At the top, there are buttons for 'Create new report' and 'Open saved report'. Below that, there are buttons for 'My profiles' and 'Public profiles'. The main section shows a 'Create profile' form with fields for Manufacturer (Samsung), Model (Galaxy-S8), DHCP Host Name (Galaxy-S8), DHCP Class Identifier (android-dhcp-7.0), and DHCP Parameter Request List (1, 3, 6, 15, 26, 28, 51, 58, 59, 43). A 'Create Profile' button is at the bottom right of the form. Below the form is a table with columns: OUI Name, DHCP Parameter Request List, IP Address, Endpoint Policy, DHCP Class Identifier, and DHCP Host Name. The table contains several rows of data, with the first row highlighted in blue.

OUI Name	DHCP Parameter Request List	IP Address	Endpoint Policy	DHCP Class Identifier	DHCP Host Name
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.54	Unknown	android-dhcp-7.0	Galaxy-S8
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.14	Unknown	android-dhcp-8.0.0	Hitz-S8
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.86.103.137	Unknown	android-dhcp-7.0	Galaxy-S8
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.145	Unknown	android-dhcp-8.0.0	Galaxy-S8
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.140	Unknown	android-dhcp-7.0	SAMSUNG-SM-G935A
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.26	Unknown	android-dhcp-7.0	SAMSUNG-SM-G955U
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.33	Unknown	android-dhcp-7.0	SAMSUNG-SM-G950U
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.15	Unknown	android-dhcp-8.0.0	SAMSUNG-SM-G950U
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.138	Unknown	android-dhcp-7.0	SAMSUNG-SM-G955U
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.19	Unknown	android-dhcp-7.0	Galaxy-S8
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.20	Unknown	android-dhcp-8.0.0	SD-Galaxy-S8
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.150	Unknown	android-dhcp-8.0.0	Galaxy-Note8
Murata Manufacturing ...	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.135.144	Unknown	android-dhcp-7.1.1	Galaxy-Note8
UNKNOWN	1, 3, 6, 15, 26, 28, 51, 58, 59, 43	10.40.130.10	Unknown	android-dhcp-7.0	Galaxy-S8

ISE Endpoint Analysis Tool -Endpoint Report



ISE Endpoint Analysis Tool – Custom Profile Creation

ISE Endpoint Analysis Tool

CLEUR-Report1 1/23/20, 6:13 PM / 5s Export as CSV... Create profile

Show 50 entries Showing 1 to 50 of 110 entries

MAC Address	SNMP Device Descript...	SNMP Switc...	NMAP Operating System	OUI Name	McAfee ePO 8061 T...	DHCP Parameter Request List	LLDP System Descript...
00:14:48:00:30:8C			Linux 2.4.9 - 2.4.16 (likely embedded)	Inventec Multimedia & Telecom Corporation		1, 3, 6, 12, 15, 28	
5A:69:47:43:EA:77				UNKNOWN		1, 33, 3, 6, 15, 28, 51, 58, 69	
00:0C:29:45:C7:DE				VMware, Inc.		1, 3, 12, 15, 6, 26, 33, 121, 42	
00:0C:29:7E:0C:1E				VMware, Inc.		1, 28, 2, 3, 15, 6, 12, 42	
04:62:75:97:ED:C7			Cisco Aironet 1141N (IOS 12.4) or 3602I (IOS 15...	Cisco Systems, Inc.		1, 60, 6, 13, 44, 3, 67, 12, 33, 150, 45, 120, 125	
00:0C:29:45:C7:D8				VMware, Inc.		1, 2, 3, 5, 6, 11, 12, 13, 15, 16, 17, 18, 45, 54, 60, 67, 128, 129, 130, 131...	
74:DA:38:9B:0C:49				Edimax Technology Co. Ltd.		1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 292	
A3:50:9F:9E:AC:90				Intel Corporate		1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43, 292	
00:1A:2F:69:D8:EE				Cisco Systems, Inc.		1, 60, 6, 3, 15, 150, 35	Cisco IP Phone 7961B,V...
E3:AA:77:97:77:5C				Cisco Systems, Inc.		1, 6, 13, 44, 3, 7, 33, 100, 43	
60:20:06:02:7E:86				Cisco Systems, Inc.		1, 6, 13, 44, 3, 7, 33, 100, 43	
00:0C:29:65:3F:0F				VMware, Inc.		1, 3, 6, 12, 15, 66, 67, 150	
00:0C:29:0C:6F:88				VMware, Inc.		1, 28, 2, 3, 15, 6, 12, 40, 41, 42	
00:0C:29:2E:0C:9C				VMware, Inc.			
00:0C:29:34:FF:0C				VMware, Inc.			
00:0C:29:34:FF:0A				VMware, Inc.			
00:0C:29:34:FF:14				VMware, Inc.			
00:0C:29:34:FF:1E				VMware, Inc.			
00:0C:29:36:0B:E7				VMware, Inc.			10
00:0C:29:43:2A:C6				VMware, Inc.			10
00:0C:29:45:C7:E2				VMware, Inc.			10
00:0C:29:45:C7:EC				VMware, Inc.			

Previous 1 2 3 Next

4/32

ISE Profiling Design Guide



This deployment guide is intended to provide the relevant design, configuration and operations-related guidance to deploy Cisco Identity Services Engine (ISE) Profiling.

by Craig Hyps

[ISE profiling design guide](#)

- Introduction
 - About Cisco Identity Services Engine (ISE)
 - About this guide
- Cisco ISE Profiling Services
 - Solution Overview
 - Policy Architecture and Components
 - Scenario Overview
 - Network Topology
 - Guide Components
- Profiling Service Requirements
 - Licensing
 - Appliance Requirements
 - Network Requirements
- Profiling Services Global Configuration
 - ISE Profiling Global Configuration
 - Procedure 1 Configure Global Profiling Settings from the Policy Administration Node
 - Enable ISE Profiling Services
 - Procedure 2 Enable Profiling Services on the Policy Service Node
 - Procedure 3 Access and View the Profiling Configuration Page
- Configuring Probes
 - Probe Overview
 - Probe Configuration
- Profiling Using the RADIUS Probe
 - Configuring the RADIUS Probe
 - Procedure 4 Enable the RADIUS Probe in ISE
 - Procedure 5 Verify Access Device Is Configured in ISE
 - Procedure 6 Verify That Access Devices Are Configured to Send RADIUS to ISE PSN
 - Procedure 7 Verify RADIUS Probe Data
- Profiling Using the SNMP Trap Probe
 - Configuring the SNMP Trap Probe
 - Procedure 8 Enable the SNMP Trap Probe in ISE
 - Procedure 9 Add the Network Access Device to ISE
 - Procedure 10 Configure Access Devices to Send SNMP Traps to ISE Policy Service Node
 - Procedure 11 Verify SNMP Trap Probe Data
- Profiling Using the SNMP Query Probe

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases

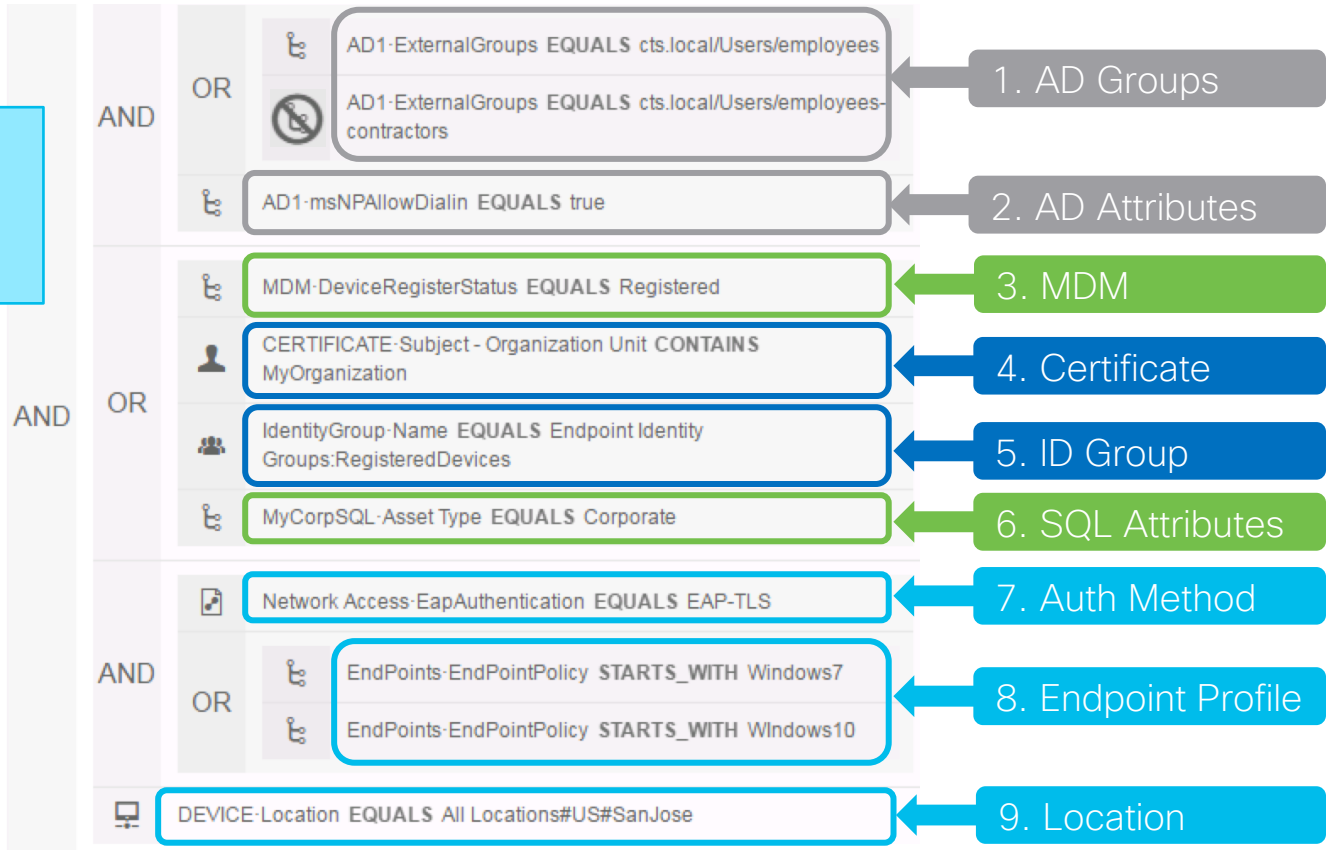


Auth Policy Optimization

Policy Logic:

- First Match, Top Down
- Skip Rule on first negative condition match

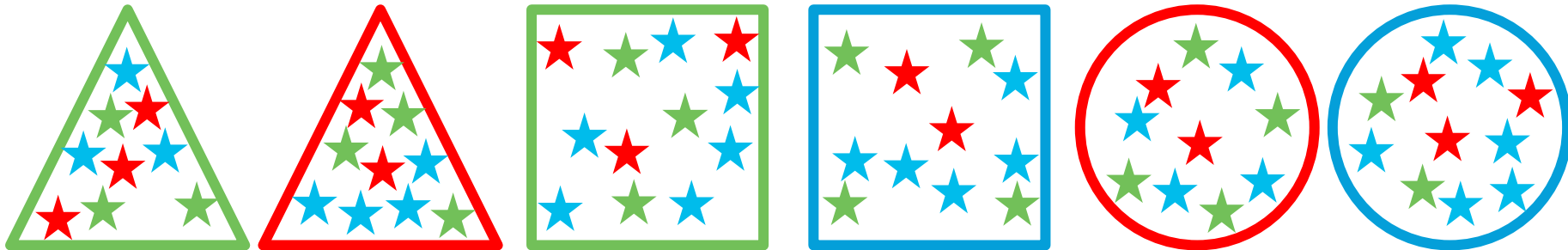
✔ Employee



Authorization Policy Optimization – Search Speed Test

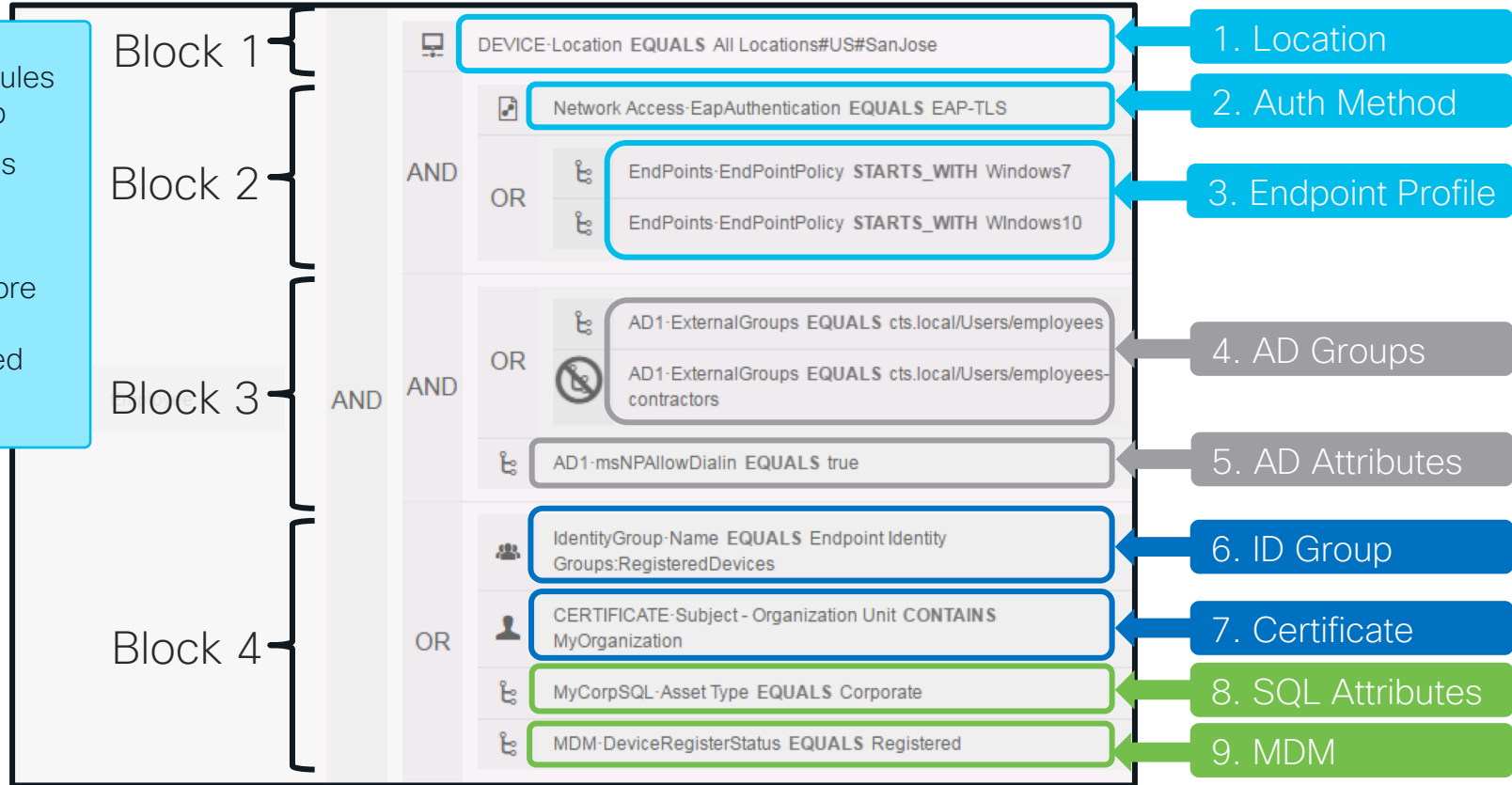
Find the object where:

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



Auth Policy Optimization

- More specific rules generally at top
- Local conditions should be put before external
- Try to place more “popular” rules before less used rules



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

▼ **Authorization Policy**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Dynamic Match Rule	if Radius:Calling-Station-ID MATCHES LDAP1 Department then	Permit Access



▼ **Advanced Attributes Settings**

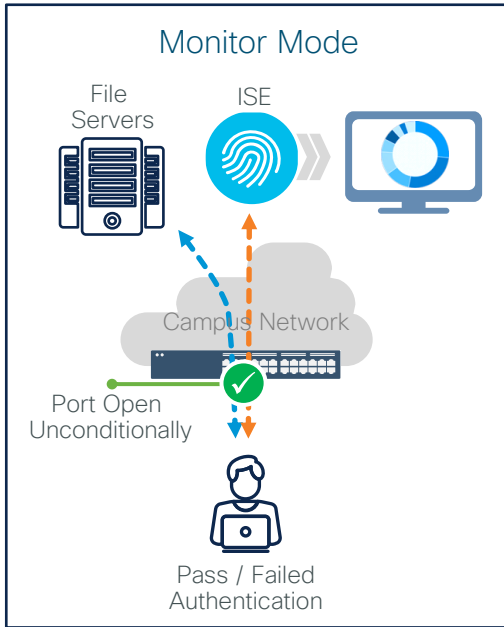
Radius:Class = InternalEndpoint groupPolicy

- Where To Start: planning
- ISE Deployment Options
- Certificates
- Network Devices
- Supplicants
- Profiling
- Policies optimization
- 802.1x Deployment Phases



Deployment Modes

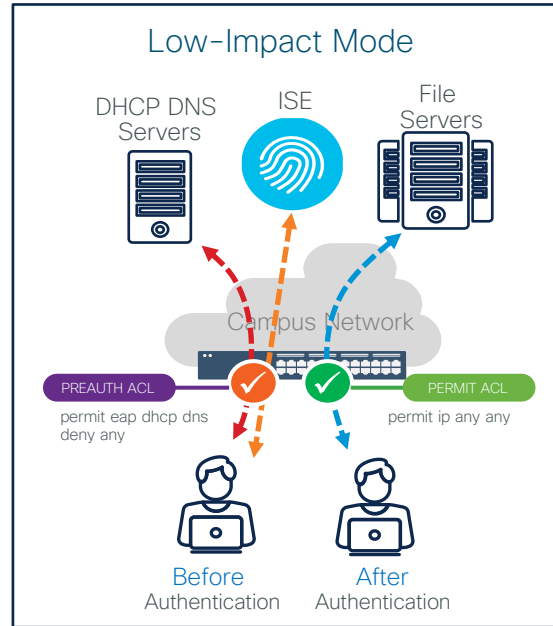
Phase I (Visibility Only)



authentication open

No impact to existing network

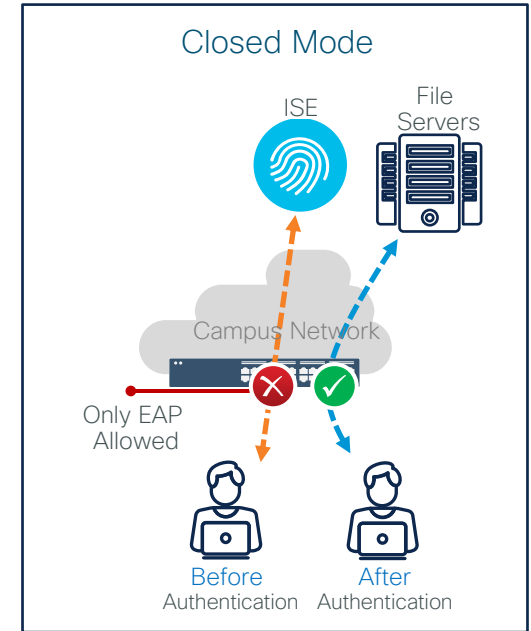
Phase II (Visibility and Control)



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

Begin to control/differentiate access





















Phase III (Visibility and Control)



- Not everyone goes into Closed Mode
- No access at all before authentication

Utilizing Policy Sets with Modes

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

	VPN		DEVICE·Device Type EQUALS All Device Types#ASA-VPN-gateways	Default Network Access   
	Monitor Wired Access		DEVICE·Mode EQUALS Mode#MonitorMode	Default Network Access   
	Low Impact		DEVICE·Mode EQUALS Mode#LowImpact	Default Network Access   
	Closed Mode		DEVICE·Mode EQUALS Mode#ClosedMode	Default Network Access   

Day 2 Operations



Supporting ISE After Deployment

- [Standardize devices configuration](#) as much as possible
- [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](#)



User involvement

User Communication before and after ISE rollout







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					

Wrap up



Deploying any network access
control solution is **crucial**
but it **isn't easy**....

Planning is **essential** to any
successful development.



Technical Session Surveys



- Compliments 😊
- What you liked
- Suggestions?



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 ISE & NAC Resources

Labels: AAA Identity Services Engine (I... Policy and Access TrustSec VPN

135846 VIEWS 110 HELPFUL 0 COMMENTS

Create: Please login to create content

Discussion Video Blog Document Project

Related Content

Discussions - Blogs - Events Videos Projects

Recommended for you

Spark Developer resources

Cisco ISE お役立ちリンク集 - Identity Services Engine -


ISE with Threat Centric NAC


Cloud past Webinar resources list

Threat Centric NAC w/ AMP

Community Helping



 Cisco ISE - Identity Services Engine
@CiscoISENetworkSecurity
16.8K subscribers

 YouTube

ISE Webinars

Cisco ISE - Identity Services Engine
57 videos 5,063 views Last updated on Dec 14, 2022

Security Technologies

Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START

Feb 5 | 16:00

LABSEC-2089

Multi-factor Authentication:
Integration of DUO with ISE for MFA

Feb 6 | 08:45

TECSEC-2007

Find Your Zen with Cisco Secure
Workload for Zero Trust Segmentation

Feb 6 | 08:45

TECSEC-2781

Zero Trust: From understanding the
risks to architecting a practical solution

Feb 6 | 15:20

PSOSEC-1210

A global view on Zero-Trust
- mapping your business resilience
requirements

Feb 7 | 08:45

BRKSEC-2445

The Art of ISE Posture, Configuration
and Troubleshooting

Feb 7 | 16:45

BRKSEC-2053

Zero Trust: Securing the
Evolving Workplace

Feb 7 | 17:00

BRKSEC-1139

Application Security
- The Final Frontier

Feb 8 | 10:45

BRKSEC-2096

Securing Industrial Networks:
Where do I start?

Feb 8 | 13:30

BRKSEC-2748

Taking Authentication to the Next Level
with Cisco Secure Access by Duo

Feb 8 | 17:00

BRKSEC-2123

Solving the Segmentation Puzzle!
Secure Workload and Secure
Firewall Integration

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

CISCO *Live!*

Feb 9 | 08:30

BRKSEC-2660

ISE Deployment Staging and Planning

Feb 9 | 13:45

BRKSEC-2834

Cisco's Unified Agent: Cisco Secure Client.
Bringing AMP, AnyConnect, Orbital &
Umbrella together

Feb 9 | 14:00

LTRSEC-2000 ISE

Deployments in the Cloud - Automate
ISE Deployments in AWS and Integrate
Them with Azure Active Directory

Feb 10 | 09:15

BRKSEC-2039

Secure Access with ISE in the Cloud

Feb 10 | 11:00

FINISH

BRKSEC-2773

How to Build a Secure Multi-Cloud
Environment with Cisco Secure Workload



If you are unable to attend a live session, you can watch it [On Demand](#) after the event

Security Technologies

Network Security

Learn about a broad range of solution and technologies which will help you better understand how to secure your network. You will find topics such as VPN, ISE, IPv6, DDoS, IoT....

START

Feb 5 | 19:00

LABSEC-2333

ISE integrations via pxGrid with FTD, WSA, StealthWatch

Feb 6 | 08:45

TECSEC-3781

Walking on solid ISE - Advanced Use Cases and Deployment Best Practices

Feb 7 | 08:45

BRKSEC-2445

The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 11:30

BRKSEC-2037

Securing Starlink Internet Services

Feb 8 | 10:45

BRKSEC-2096

Securing Industrial Networks: Where do I start?

Feb 8 | 13:30

BRKSEC-2678

DDoS Mitigation: Introducing Radware Deployment on Firepower Appliances

Feb 9 | 08:30

BRKSEC-2660

ISE Deployment Staging and Planning

Feb 9 | 10:30

BRKSEC-2101

Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Feb 9 | 15:45

BRKSEC-3058

Route based VPNs with Cisco Secure Firewall

Feb 9 | 15:45

BRKSEC-2044

Secure Operations for an IPv6 Network



Feb 10 | 09:00

BRKSEC-3019

Visibility, Detection and Response with Cisco Secure Network Analytics

If you are unable to attend a live session, you can watch it [On Demand](#) after the event

CISCO *Live!*

Feb 10 | 09:00

LTRSEC-2381

Stronger Together: Uniting IT and
OT Security with Cyber Vision

Feb 10 | 09:00

BRKIPV-3134

IPv6 Security in the Local Area
with First Hop Security

Feb 10 | 11:00

FINISH BRKSEC-2218

Cisco Secure Hybrid SWG -
Your First Step to Your SASE Journey



If you are unable to attend a live session, you can watch it [On Demand](#) after the event

CISCO *Live!*

Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.



The bridge to possible

Thank you

CISCO *Live!*

CISCO *Live!*

ALL IN