

Cisco ISE Meets Azure Cloud

cisco Live !

Deploy, Automate, Integrate with Entra ID and Intune

Eugene Korneychuk
Security Technical Leader

About Eugene Korneychuk

- Security TAC Technical Leadership Team
- 15+ years of security and networking experience
- 20+ published documents
- On personal note:
 - Family time
 - Travel
 - Football
- Lives in Cary, North Carolina, US



Session Objective



The Goal of this session is to:

- Make you familiar with ISE Cloud deployments and designs in Azure
- Cover ISE automation techniques
- Explain the SAML Authentication functionality and its implementation on ISE
- Walk you through REST ID Store authentication with ISE and Entra ID
- Demonstrate how Intune integrates with ISE and you can benefit from Compliance Status

Cisco Webex App

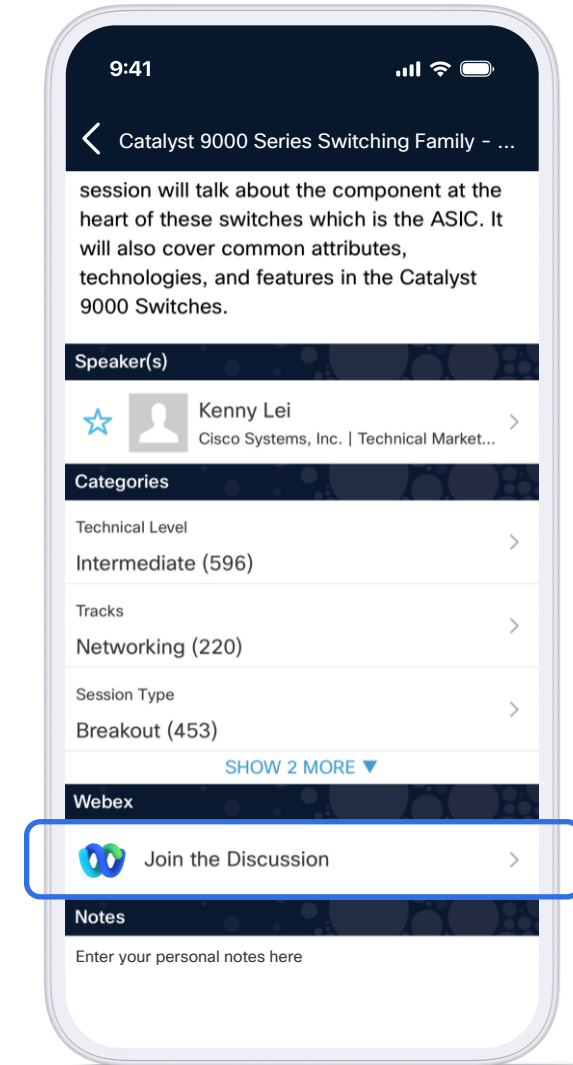
Questions?

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

How

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

Webex spaces will be moderated by the speaker until 14 November 2025.



<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2416>

Agenda

- 01 ISE Architecture Concepts**
- 02 ISE in Azure Cloud**
- 03 ISE SAML SSO**
- 04 Entra ID Authentications**
- 05 Intune Integration**
- 06 Conclusion**

ISE Architecture Concepts

ISE Design Concepts



Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Owns ISE database and replicates it to other nodes



Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Collects health and log information from other nodes



Policy Services Node (PSN)

- Makes policy decisions
- RADIUS / TACACS+ Servers



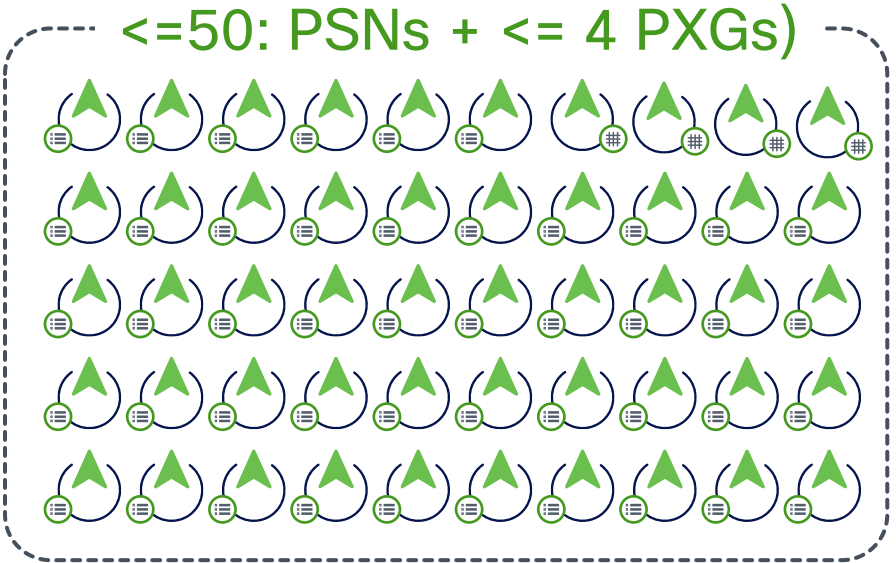
pxGrid Controller

- Facilitates sharing of context

ISE Scaling



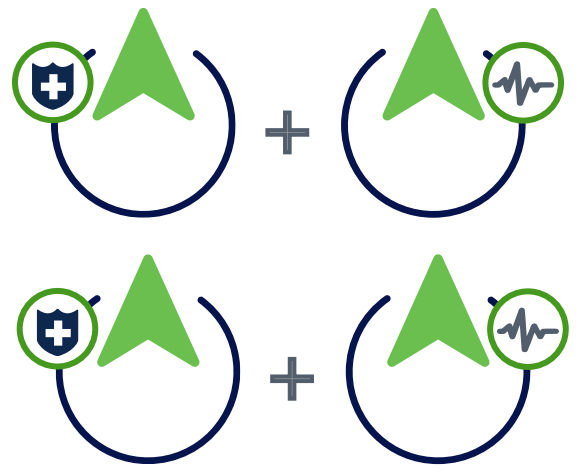
Lab and Evaluation



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



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



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

Total Maximum Concurrent Active Sessions

Cisco ISE



Deployment Type	SNS 3615	SNS 3715, SNS 3815	SNS 3595	SNS 3655	SNS 3755, SNS 3855	SNS 3695	SNS 3795, SNS 3895
Large deployment	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium deployment	12,500	75,000	20,000	25,000	150,000	50,000	150,000
Small deployment	12,500	25,000	20,000	25,000	50,000	50,000	50,000

Small Deployment

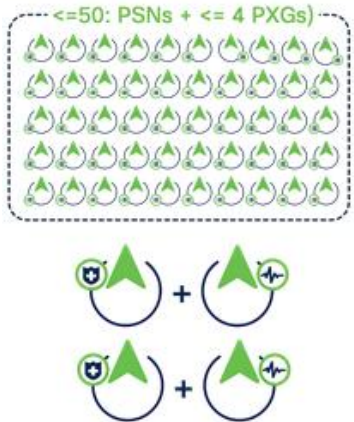


Medium Deployment



BRKSEC-2416

Large Deployment



PSN Maximum Concurrent Active Sessions

Cisco ISE



PSN Type

Concurrent active endpoints supported by a dedicated PSN (ISE node has only PSN persona)

Concurrent active endpoints supported by a shared PSN (ISE node has multiple personas)

	SNS 3615	SNS 3715, SNS 3815	SNS 3595	SNS 3655	SNS 3755, SNS 3855	SNS 3695	SNS 3795, SNS 3895
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

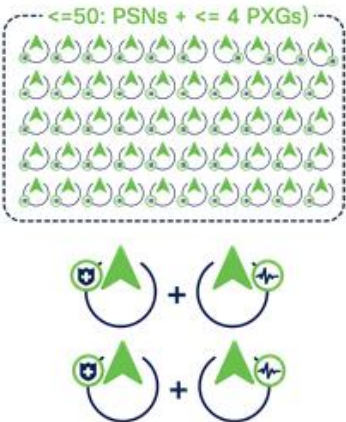
Small Deployment



Medium Deployment



Large Deployment



Cisco Cloud Platforms Sizing

Cisco ISE



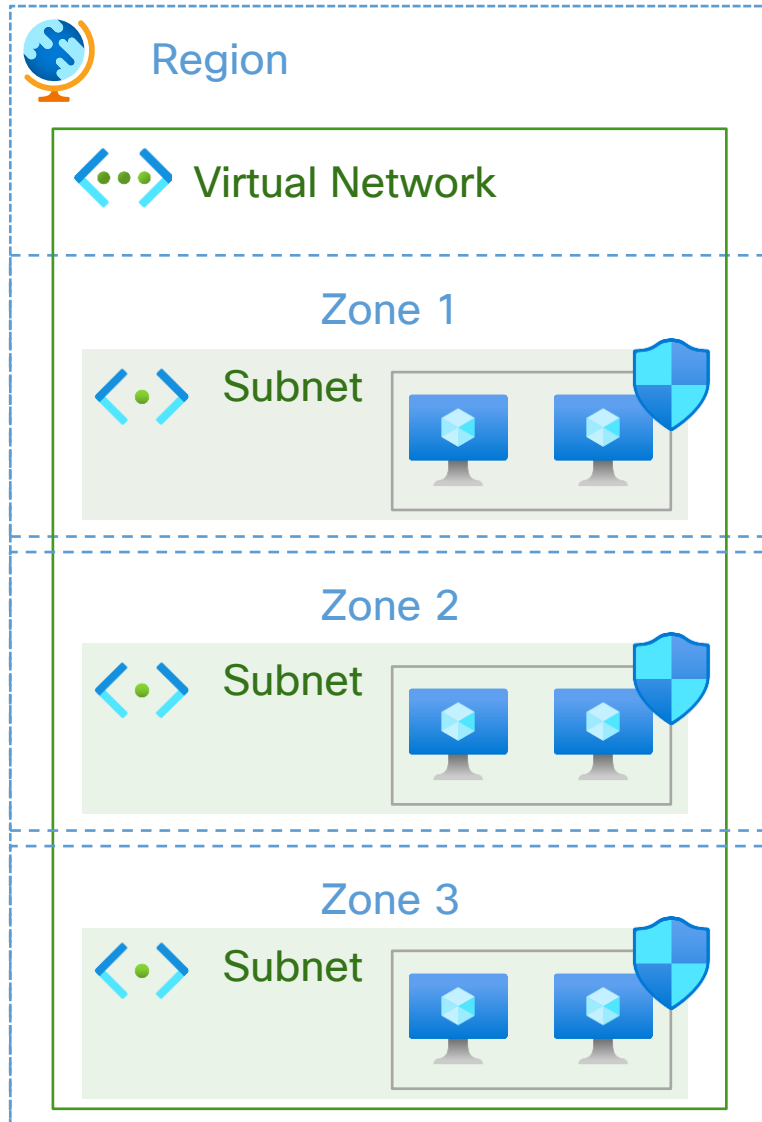
Models	SNS 3615	SNS 3595	SNS 3655	SNS 3695	SNS 3715	SNS 3795
VM Appliance	16 vCPU 32 GB	16 vCPU 64 GB	24 vCPU 96 GB	24 vCPU 256 GB	24 vCPU 32 GB	40 vCPU 256 GB
AWS	c5.4xlarge*	m5.4xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge	c5.9xlarge* m5.8xlarge	m5.16xlarge
	c7i.4xlarge**	-	m7i.8xlarge**	m7i.16xlarge**	m7i.4xlarge**	m7i.16xlarge**
Azure	Standard_F16s_v2*	Standard_D16s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4	Standard_F32s_v2* Standard_D32s_v4	Standard_D64s_v4
OCI	Optimized3.Flex* (8 OCPU and 32 GB)	Standard3.Flex (8 OCPU and 64 GB)	Optimized3.Flex* (16 OCPU and 64 GB) Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (16 OCPU and 256 GB)	Optimized3.Flex* (16 OCPU and 64 GB) Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (32 OCPU and 256 GB)

* This instance is compute-optimized and provides better performance compared to the general purpose instances.

** Cisco ISE release 3.5 and later supports M7i and C7i instance types on AWS

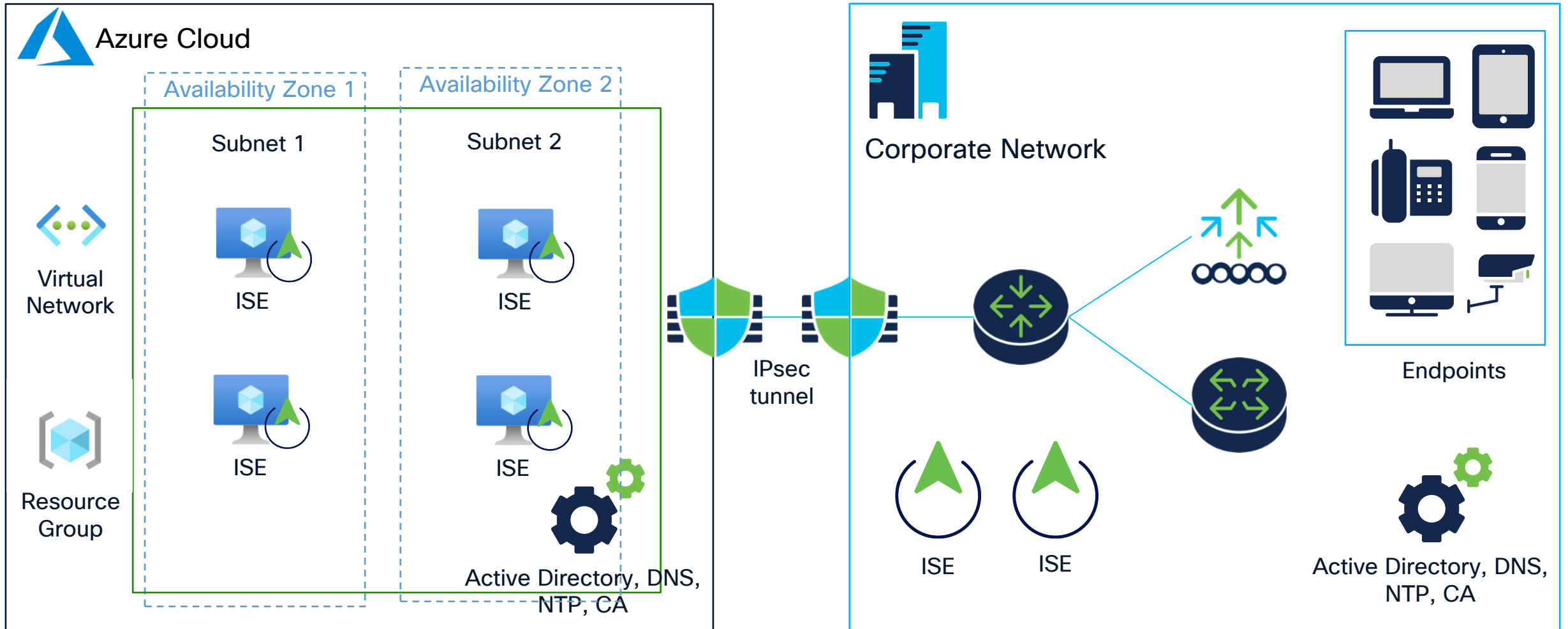
ISE in Azure Cloud

Azure basics



- Each **Region** is fully isolated from another region to achieve fault tolerance.
 - (US) East US
 - (Europe) West Europe
 - (Asia Pacific) Central India
- Each **Zone** has independent power, cooling, and networking, making it highly resilient.
 - Zone 1
 - Zone 2
- **Virtual Network** spans all the Availability Zones in the Region.
- **Subnets** are subsets of Virtual Network to isolate Virtual Machines
- **Network Security Group** is used to filter inbound and outbound traffic from the Virtual Machine
- **Virtual Machine** hosted in Azure Cloud

Design Scenarios - Azure



Know Before You Go



Problem: EAP-TLS Authentications might fail due to the fragmentation issue.

Failure Reason: 5440 Endpoint abandoned EAP Session and started new

Failure Reason: 5411 Supplicant stopped responding to ISE



Technical Background:

1. Certain Generation of Azure hardware drops out of order packets
2. In Azure, the networking virtual network stack, by default, drops out-of-order fragments without forwarding them to the end virtual machine host.

Microsoft cannot enable the option that prevents the dropping of out-of-order fragments on Azure VPN Gateway, Azure ExpressRoute (with FastPath disabled), and Azure vWAN. As a result, out-of-order fragments may not be received and processed properly.

Know Before You Go



Solution:

Cisco has validated third-party VPN gateways like Cisco Catalyst 8000V as Azure virtual machine to terminate VPN tunnel from on-premises deployment. To ensure proper handling of out-of-order UDP packets:

- Select regions where Microsoft Azure Cloud has already implemented the fixes: Central Canada (CanadaCentral), Central France (FranceCentral), Central India (CentralIndia), Central Poland (PolandCentral), Central Sweden (SwedenCentral), Central UAE (UAECentral), Central US (uscentral), East Asia (eastasia), East Australia (australiaeast), East Canada (CanadaEast), East Japan (japaneast), East Norway (NorwayEast), East US (eastus), North Central US (northcentralus), North Germany (GermanyNorth), North EU (EUNorth), North Switzerland (SwitzerlandNorth), North UAE (UAENorth), South Africa North (SouthAfricaNorth), South Brazil (brazilsouth), South US (ussouth), South Central US (southcentralus), South East Asia (southeastasia), South East Australia (australiasoutheast), South India (SouthIndia), South UK (uksouth), West Central US (westcentralus), West Central Germany (GermanyWestCentral), West Europe (westeurope), West UK (ukwest), and West US (westus).
- Cisco ISE customers should raise an Microsoft Azure support ticket to enable the option to allow out-of-order fragments to reach the destination instead of being dropped.
- For other regions, Cisco ISE customers should raise an Microsoft Azure support ticket to update these configurations:
 - Pin the subscription to ensure all instances within that subscription are deployed on hardware generation 7.
 - Enable the option to allow out-of-order fragments.

Demo. ISE Azure Application Deployment

Azure services

+

Create a resource



Network security groups



Virtual machines



Marketplace



Public IP addresses



Private DNS zones



DNS zones



Network security grou...



Microsoft Entra ID

➔

More services

Resources

Recent Favorite

Name	Type	Last Viewed
 ISE1-Azure	Virtual machine	11 minutes ago
 ASAv-ekorneyc	Virtual machine	40 minutes ago
 ekorneyc-RG	Resource group	41 minutes ago
 ASAv-Outside-NSG	Network security group	2 days ago
 ASAv-ekorneyc-SecurityGroup	Network security group	2 days ago

Azure VM vs Azure Application

Home > Marketplace > Cisco Identity Services Engine (ISE) >

Create a virtual machine ...

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right

User data

Pass a script, configuration file, or other data that will be accessible to your applications throughout the lifetime of the virtual machine. Don't use user data for storing your secrets or passwords. [Learn more about user data for VMs](#)

Enable user data ☒

User data *

Performance (NVMe)

Enable capabilities to enhance the performance of your resources.

Higher remote disk storage performance with NVMe ☐

i The selected image and size are not supported for NVMe. [See supported VM images and sizes](#)

ISE as Azure Virtual Machine

- Use User data to bootstrap ISE
- Offers choice for Availability Zones

Create ISE Instance using Azure Virtual Machine / Application



Home > Marketplace > Cisco Identity Services Engine (ISE) >

Create Cisco Identity Services Engine (ISE) BYOL 3.4 ...

1 Basics 2 Network Settings 3 Services 4 User Details 5 Review + submit

ISE ARM Template Deployment

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

cx-tac-rtp-aaa-azure (cxsecurity)

Resource group * ⓘ

[Create new](#)

Instance details

Region * ⓘ

East US

Host Name * ⓘ

Time Zone * ⓘ

Etc/UTC

VM Size * ⓘ

Standard_F16s_v2

Disk Storage Type * ⓘ

Premium SSD

Disk Encryption Key ⓘ

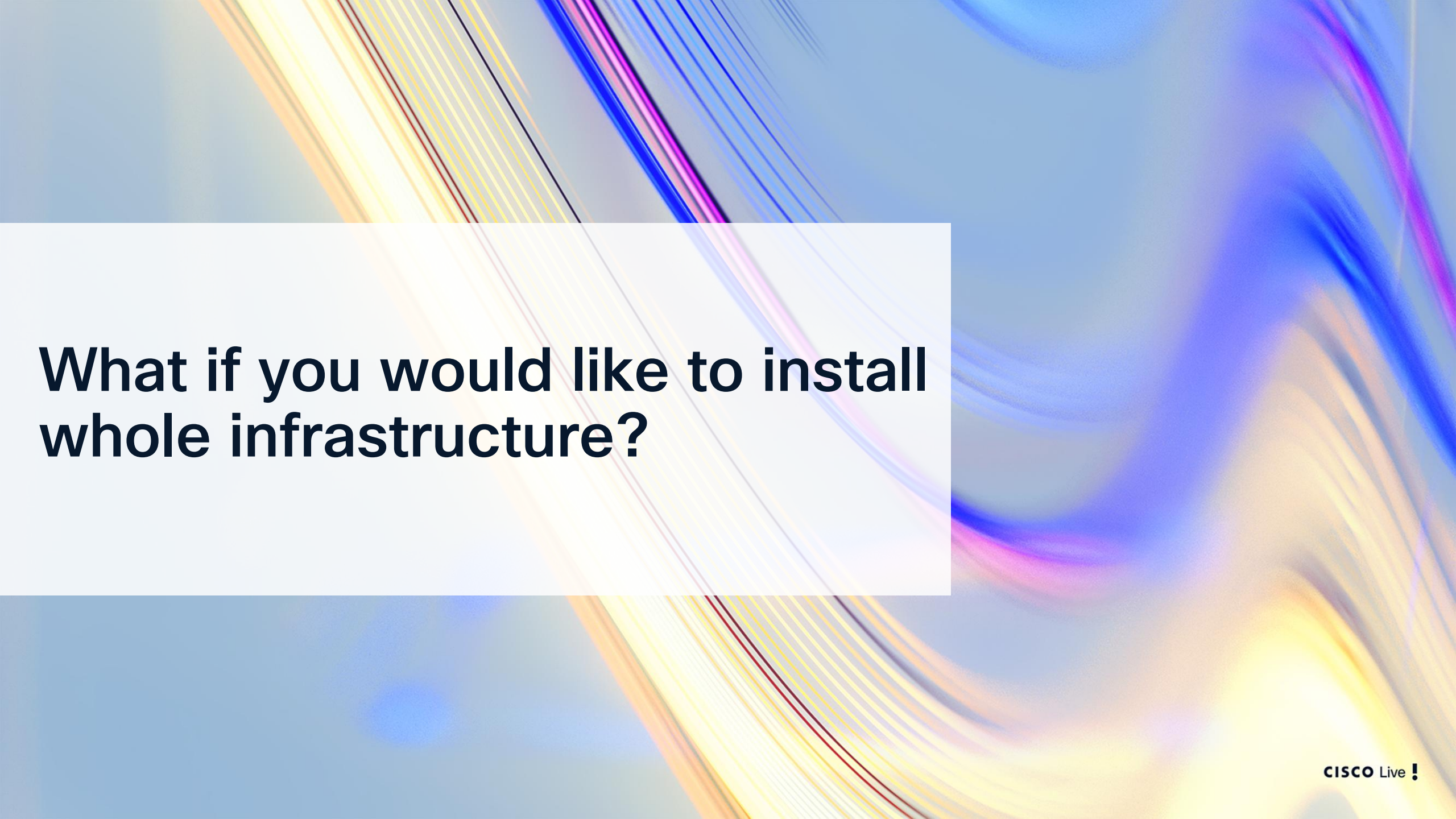
Volume Size * ⓘ

600

ISE as Azure Application

- ARM Template helps to setup ISE with menu prompts

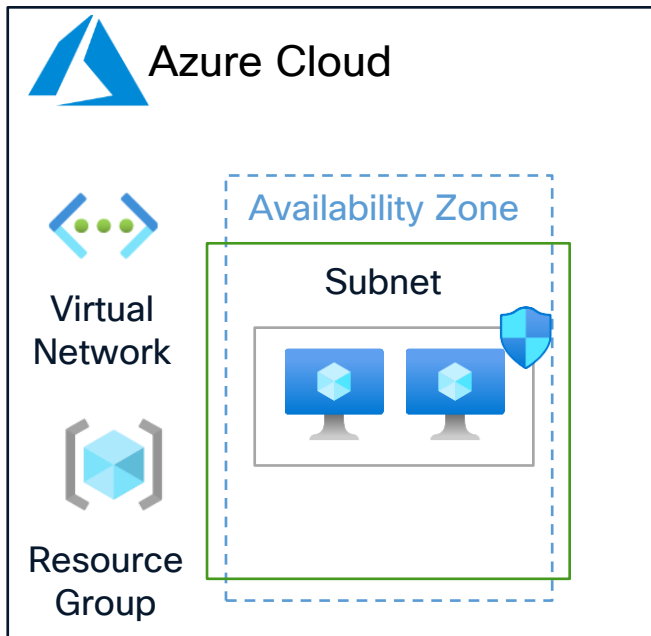




**What if you would like to install
whole infrastructure?**

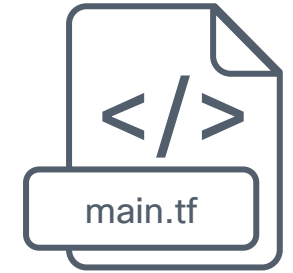
Terraform

- Infrastructure as a Code to automate the provisioning of your infrastructure resources



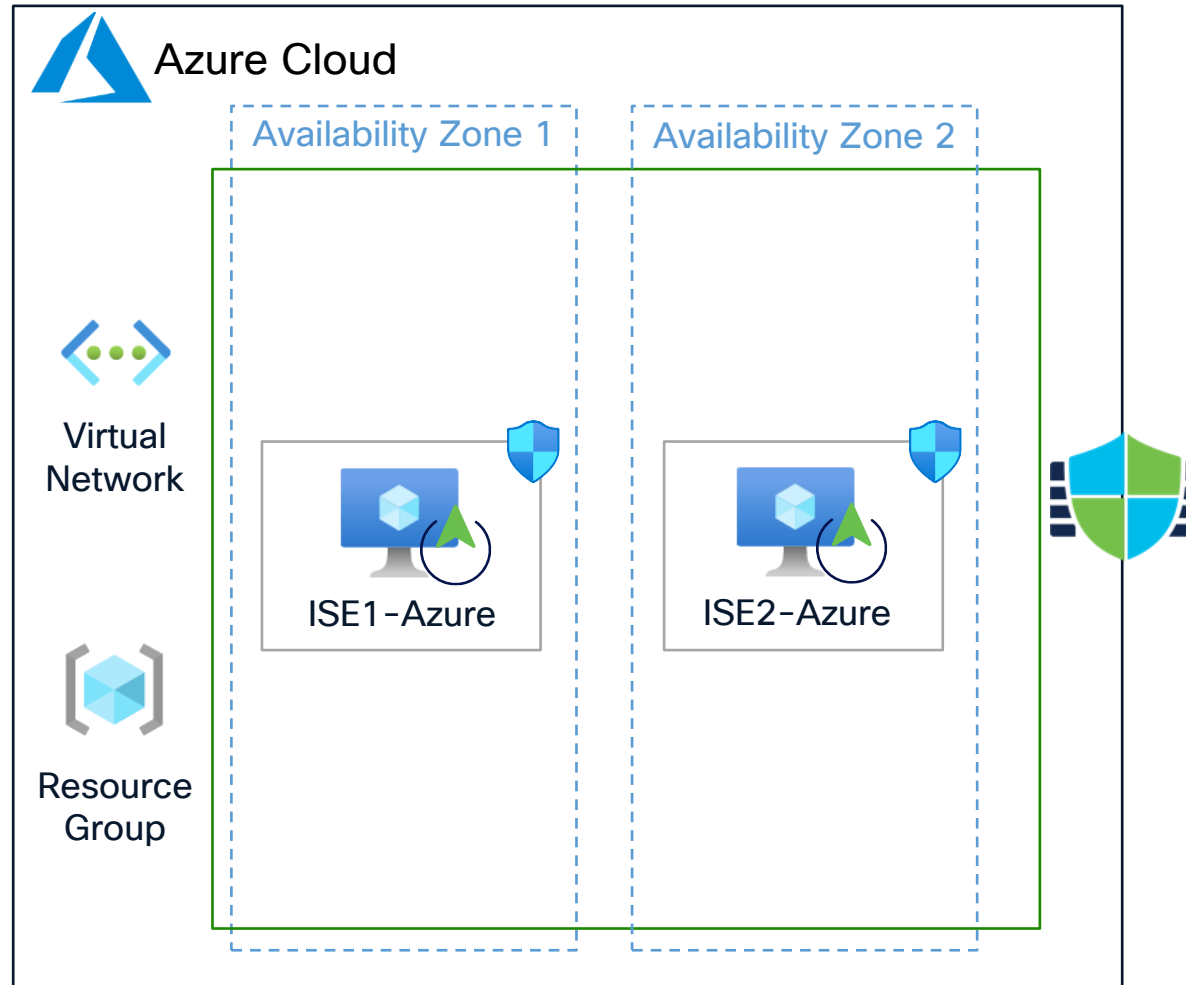
- Create Network Interface
- Create Network Security Group
- Create Virtual Machine
- Create Resource Group

- Relies on the main.tf (terraform config) file to provision resources
- Terraform keeps the state of the infrastructure, compare the end result to what the current state is and provisions resources accordingly



Demo. ISE installation on Azure using Terraform

Demo Topology



```
ekorneyc@EKORNEYC-M-CW9R Terraform % terraform apply
```

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the following symbols:

+ create

Terraform will perform the following actions:

azurerm_linux_virtual_machine.ise-azure-1 will be created

```
+ resource "azurerm_linux_virtual_machine" "ise-azure-1" {
  + admin_username           = "iseadmin"
  + allow_extension_operations = true
  + computer_name            = (known after apply)
  + disable_password_authentication = true
  + extensions_time_budget   = "PT1H30M"
  + id                       = (known after apply)
  + location                 = "eastus"
  + max_bid_price            = -1
  + name                     = "ISE1-Azure"
  + network_interface_ids    = (known after apply)
  + patch_mode               = "ImageDefault"
  + platform_fault_domain    = -1
  + priority                 = "Regular"
  + private_ip_address       = (known after apply)
  + private_ip_addresses     = (known after apply)
  + provision_vm_agent       = true
  + public_ip_address        = (known after apply)
  + public_ip_addresses     = (known after apply)
  + resource_group_name      = "ekorneyc-RG"
```

Common Installation Problems with Terraform



ISE Virtual Machine created, but you:

Can't login to it via Serial Console (wrong credentials)

Services are not coming up

Terraform Takes longer time to setup Virtual Machines

Hostname is different from the one configured

```
ISE2-Azure login: iseadmin
Password:
Login incorrect
```

User
data

```
azurerm_linux_virtual_machine.ise-azure-2: Still creating... [20m20s elapsed]
azurerm_linux_virtual_machine.ise-azure-1: Still creating... [20m20s elapsed]

Error: waiting for creation of Linux Virtual Machine: (Name "ISE1-Azure" / Resource Group "ekorneyc-RG"): Code="OSProvisioningTimeout" Message="OS Provisioning for VM 'ISE1-Azure' did not finish in the allotted time. The VM may still finish provisioning successfully. Please check provisioning state later. For details on how to check current provisioning state of Windows VMs, refer to https://aka.ms/WindowsVMLifecycle and Linux VMs, refer to https://aka.ms/LinuxVMLifecycle."

with azurerm_linux_virtual_machine.ise-azure-1,
on main.tf line 85, in resource "azurerm_linux_virtual_machine" "ise-azure-1":
85: resource "azurerm_linux_virtual_machine" "ise-azure-1" {}

Error: waiting for creation of Linux Virtual Machine: (Name "ISE2-Azure" / Resource Group "ekorneyc-RG"): Code="OSProvisioningTimeout" Message="OS Provisioning for VM 'ISE2-Azure' did not finish in the allotted time. The VM may still finish provisioning successfully. Please check provisioning state later. For details on how to check current provisioning state of Windows VMs, refer to https://aka.ms/WindowsVMLifecycle and Linux VMs, refer to https://aka.ms/LinuxVMLifecycle."

with azurerm_linux_virtual_machine.ise-azure-2,
on main.tf line 121, in resource "azurerm_linux_virtual_machine" "ise-azure-2":
121: resource "azurerm_linux_virtual_machine" "ise-azure-2" {}

(CCL) ekorneyc@EKORNEYC-M-CW9R Terraform %
```

ISE1-Azure | Serial console ...

Virtual machine

» ? Feedback [?] [?] [?] [?]

```
2025-01-21T20:34:11.162826Z INFO Daemon Daemon Certificate with thumbprint

Failed to log in 1 time(s)
Last failed login on Wed Jan 22 02:31:53 2025 from ttyS0
Failed to connect to server
Exit

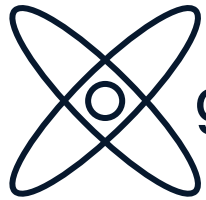
ISE1-Azure login: [?]
```



**That's not it, you need to
configure things...**

Ansible

- Ansible playbooks are written in YAML
- Ansible playbooks consist of plays, which are sets of Tasks



galaxy.ansible.com

Namespaces > cisco > ise

 cisco.ise

Version 2.9.6 updated 2 months ago (lat... Last updated 2 months ago

Install Documentation Contents Import log Dependencies

Install

Ansible Modules for Cisco ISE

collection sdn ise cisco cloud networking

Installation `ansible-galaxy collection install cisco.ise`

Note: Installing collections with ansible-galaxy is only supported in ansible-core >= 2.13.9

Download [Download tarball](#)

Requires Ansible >= 2.15.0

Ansible Collection - cisco.ise

Play (set of tasks)

Task

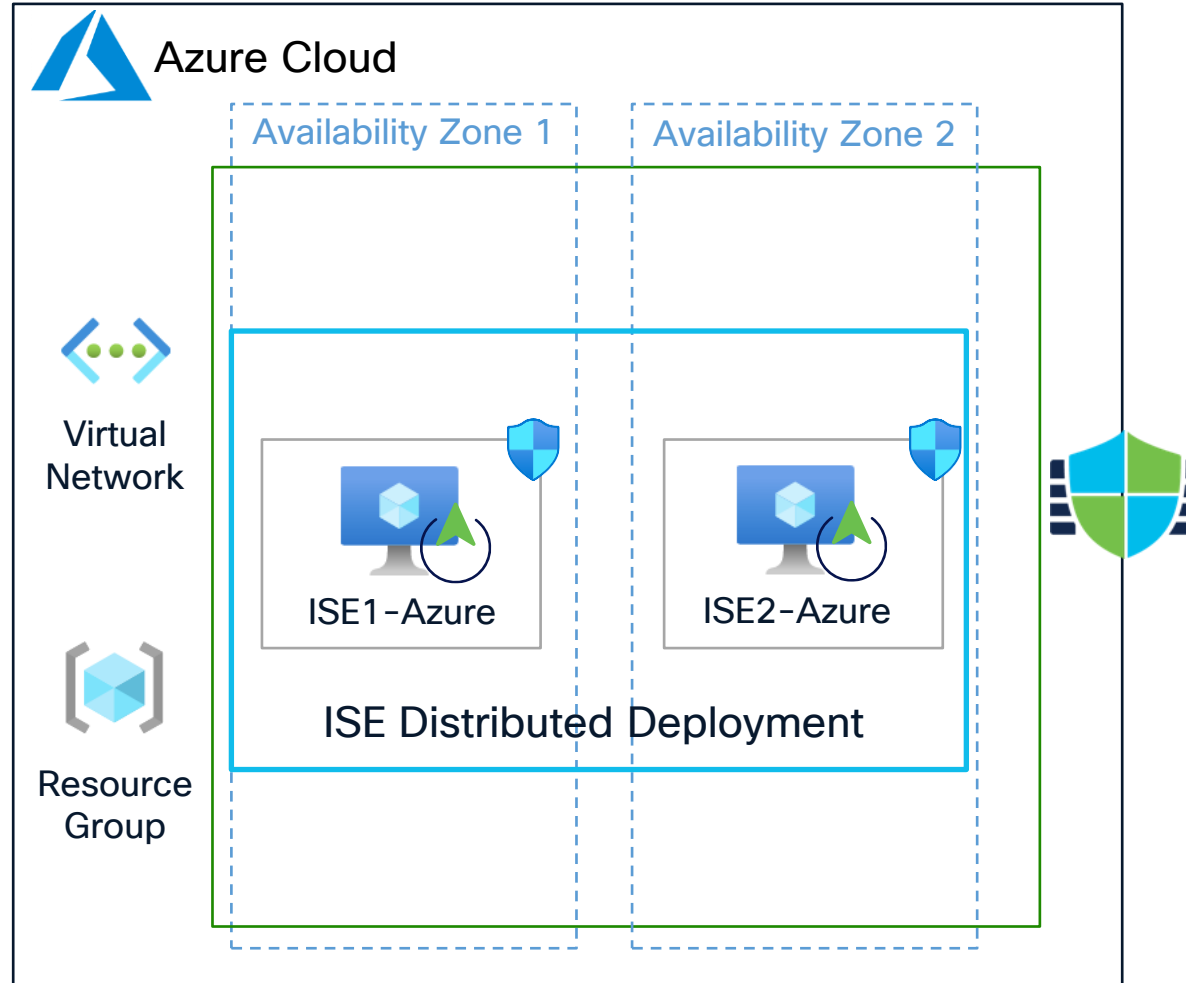
```
- hosts: ise_servers
vars_files:
  - credentials_emea.yml
gather_facts: no
tasks:

- name: Create or update ASAv
  cisco.ise.network_device:
    ise_hostname: "{{ise_hostname}}"
    ise_username: "{{ise_username}}"
    ise_password: "{{ise_password}}"
    ise_verify: "{{ise_verify}}"
    state: present
    name: ASAv2
  NetworkDeviceIPList:
    - ipaddress: 172.31.108.43
      mask: 32
  authenticationSettings:
    radiusSharedSecret: 'cisco'
    networkProtocol: 'RADIUS'
    description: 'ASAv in AWS'
  register: result
```

Playbook (set of plays)

Demo. ISE configuration using Ansible

Demo Topology



ISE Configuration

```
(CL) ekorneyc@EKORNEYC-M-CW9R Ansible % ansible-playbook -i hosts cl-ise-playbook.yaml
```



ISE in the Cloud. Licensing

Cisco ISE leverages the Bring Your Own License (BYOL)

- ISE Comes with 90-days Evaluation License
- Use the Common VM License to enable Cisco ISE on cloud platforms, in addition to the other Cisco ISE licenses that you need for the Cisco ISE features you want to use.

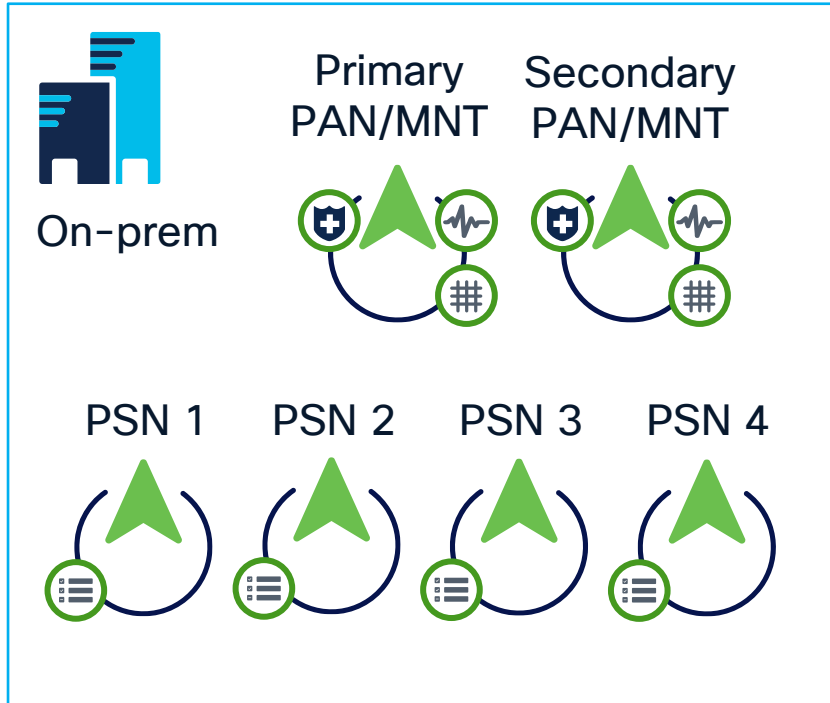


Migration and Upgrades

Migration



Azure Cloud

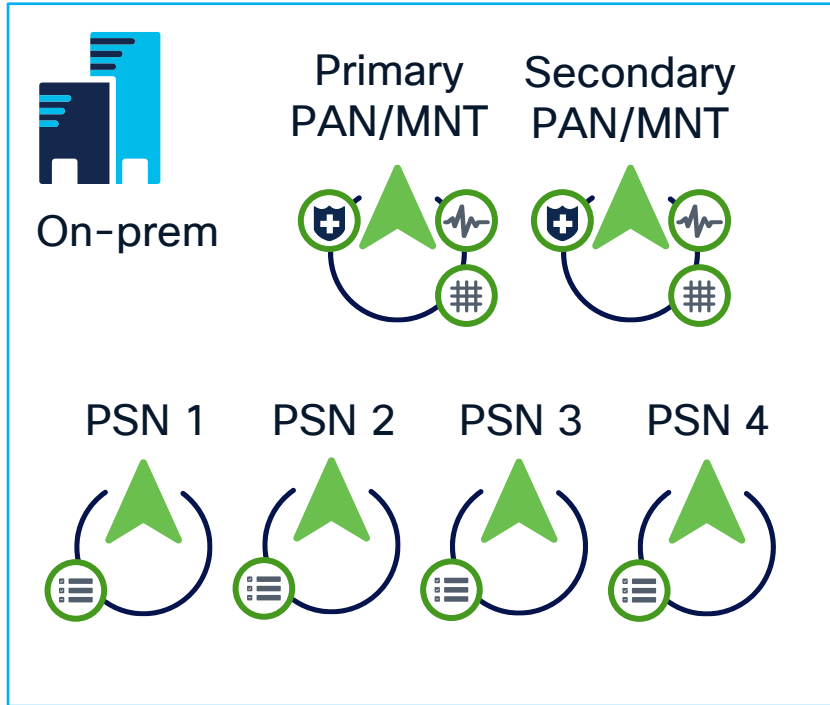


Scenario: ISE 3.3 patch 4 Medium Deployment Migration to Cloud Infrastructure

--- === Phase 0 === ---

- Plan
 - Take a Backup
 - Run Health Checks
 - FQDN's of ISE Nodes to be used
 - IP addresses of ISE Nodes to be used
 - End to End connectivity with the Cloud Providers
 - Test Infrastructure
 - Time and Date for MW

Migration



--- === Phase 1 === ---

1. Deregister Secondary PAN/MNT
2. Deploy Cloud Instance
3. Install Patch
4. Add Node to the existing Deployment



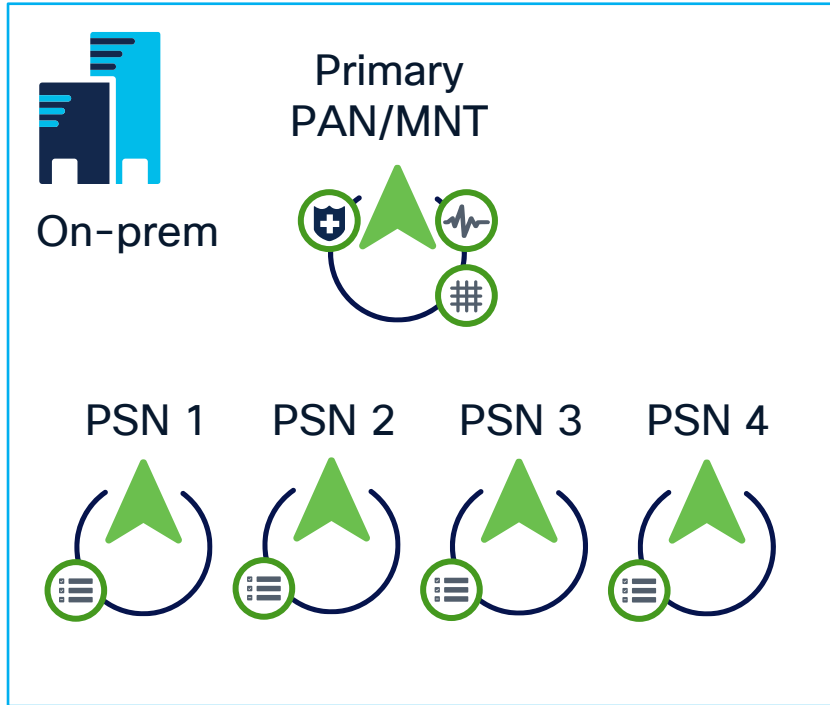
Secondary
PAN/MNT



Considerations:

- (Optional) Certificates to be exported prior Deregistration of Secondary PAN, imported before adding Node to the Deployment

Migration

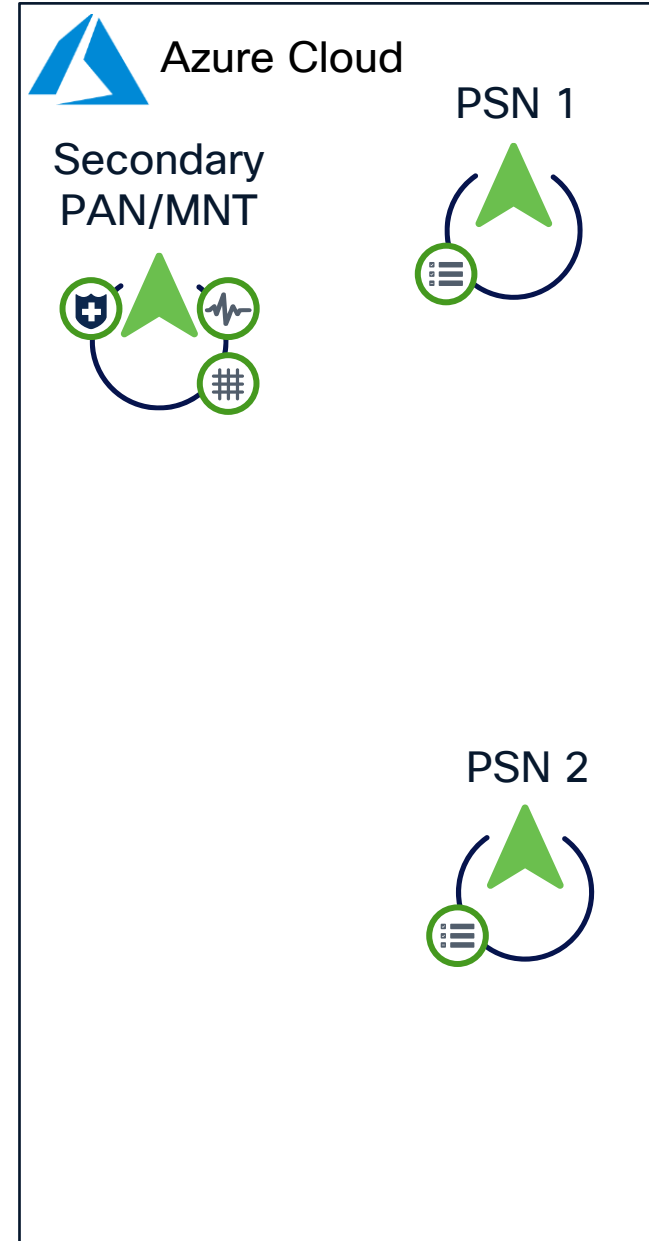


--- === Phase 2 === ---

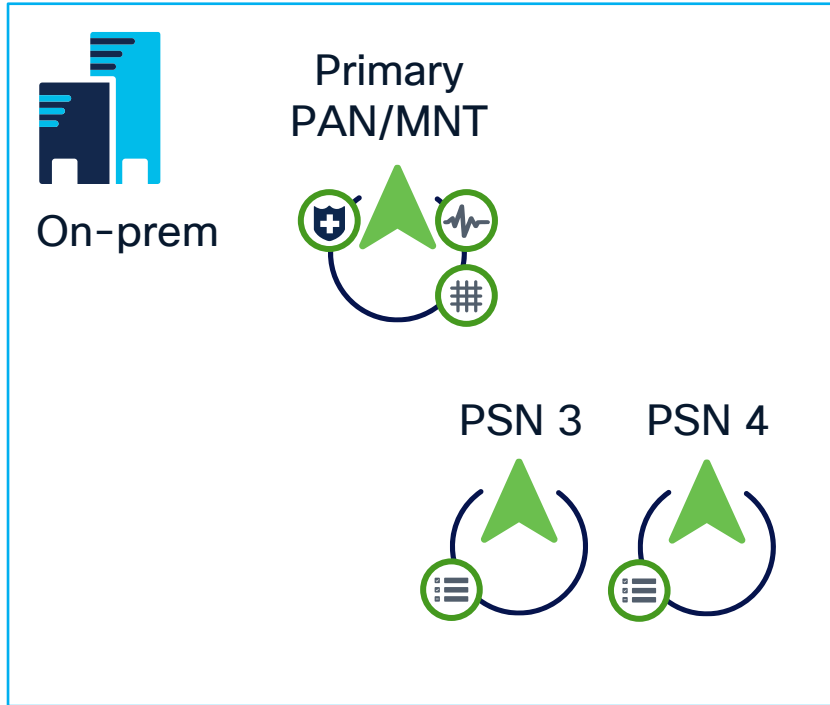
1. Deregister PSN1, PSN2
2. Deploy Cloud Instances
3. Install Patch
4. Add Nodes to the Deployment
5. Test

Considerations:

- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 2. Exclude PSN1 and PSN2 from LB Groups or ensure that high availability configuration includes PSN3 and PSN4



Migration

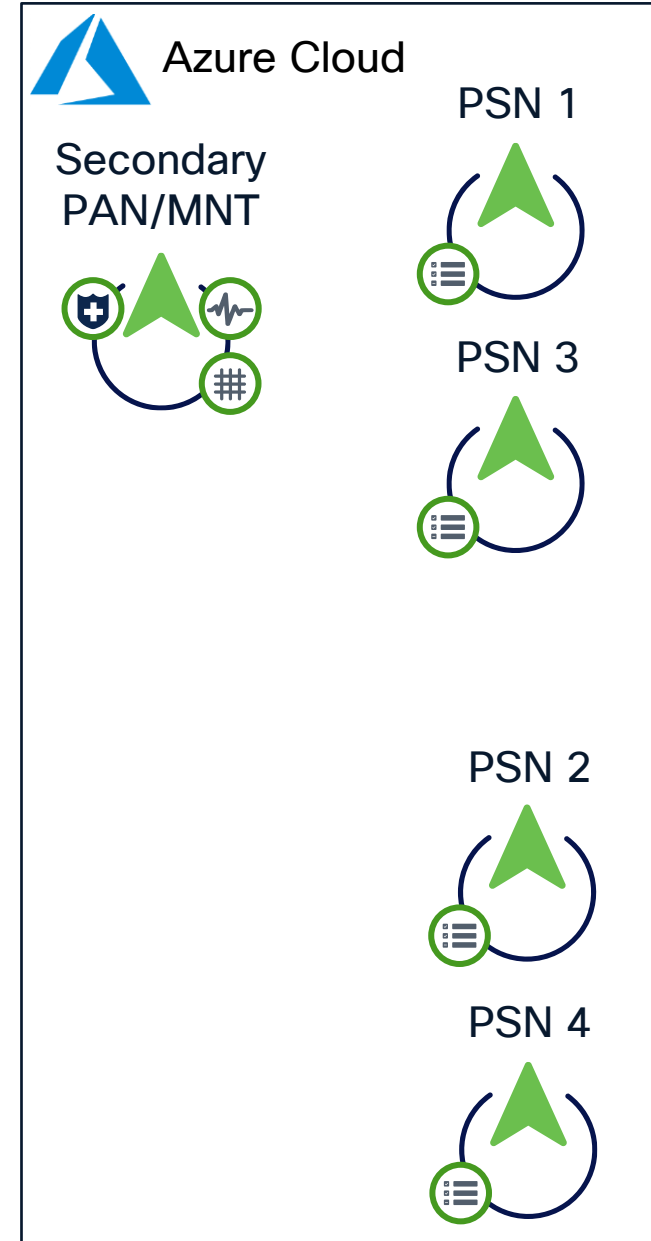


--- === Phase 3 === ---

1. Deregister PSN3, PSN4
2. Deploy Cloud Instances
3. Install Patch
4. Add Nodes to the Deployment
5. Test

Considerations:

- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 3. Exclude PSN3 and PSN4 from LB Groups or ensure that high availability configuration includes PSN1 and PSN2



Migration

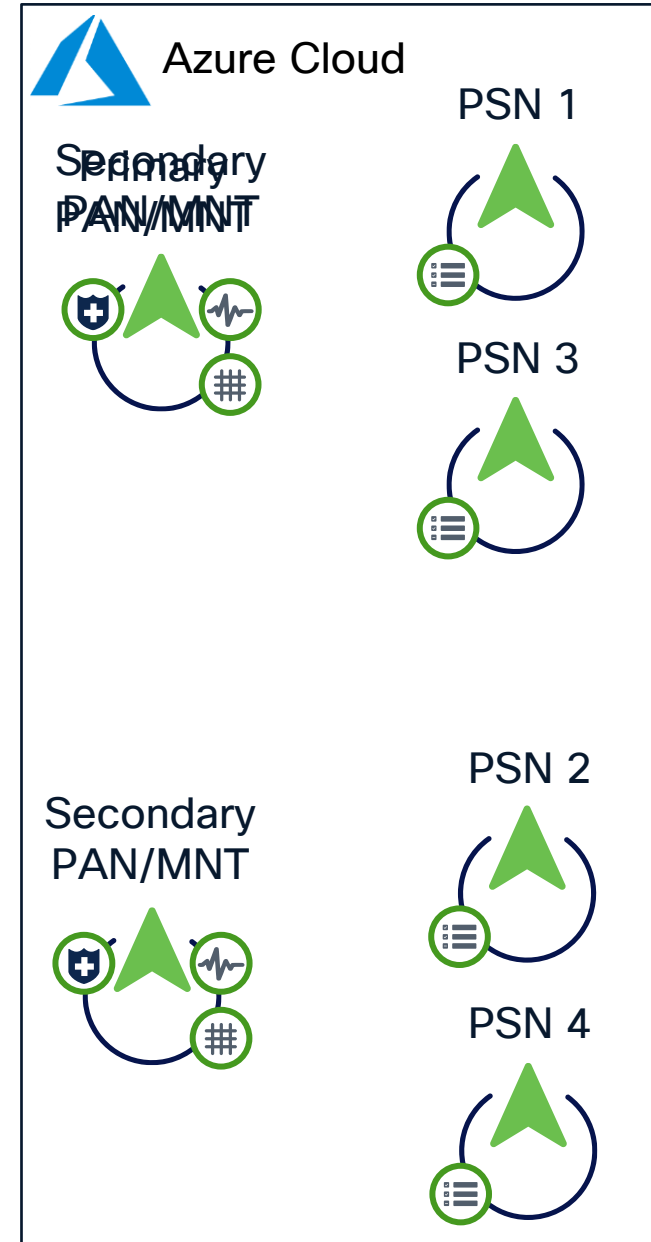


--- == Phase 4 == ---

1. Promote Secondary PAN/MNT to Primary
2. Remove Secondary PAN/MNT
3. Deploy Cloud Instance
4. Install Patch
5. Add Node to the Deployment

Considerations:

- (Optional) Certificates to be exported prior Removal of PAN, imported before adding Node to the Deployment



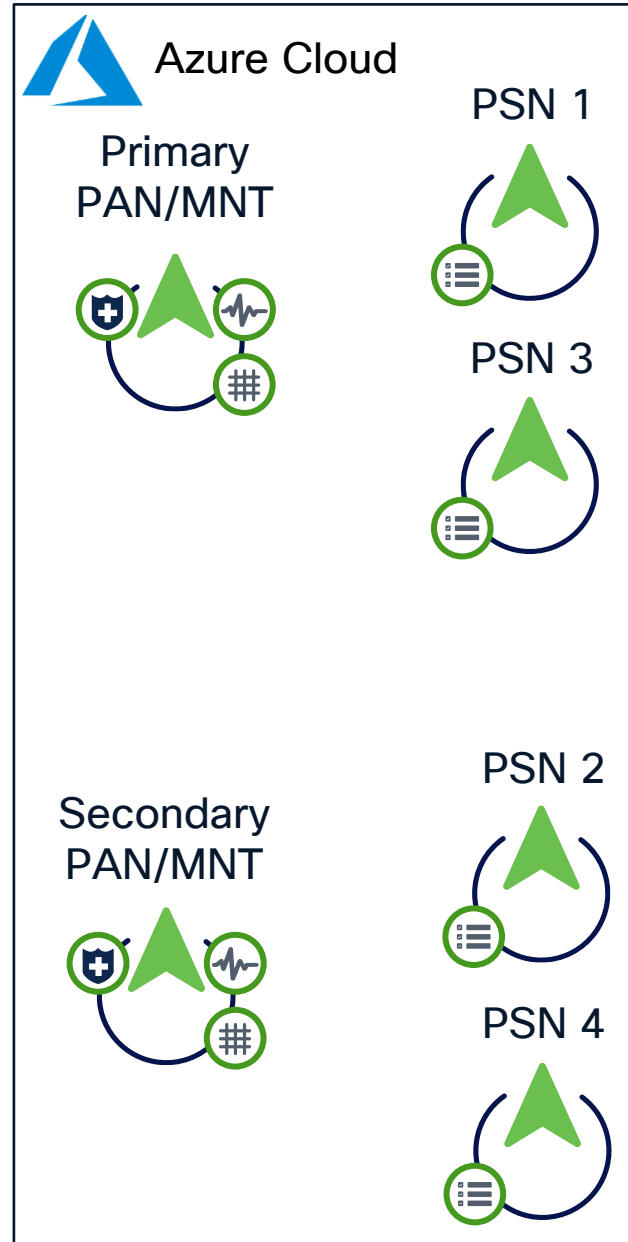
Upgrade



--- === Phase 0 === ---

- Plan
 - Review the Upgrade Guide
 - Take a Backup
 - Test Infrastructure
 - Time and Date for MW
 - Run Health Checks

Scenario: ISE 3.2 patch 4 Medium
Deployment Upgrade to ISE 3.3 patch 4



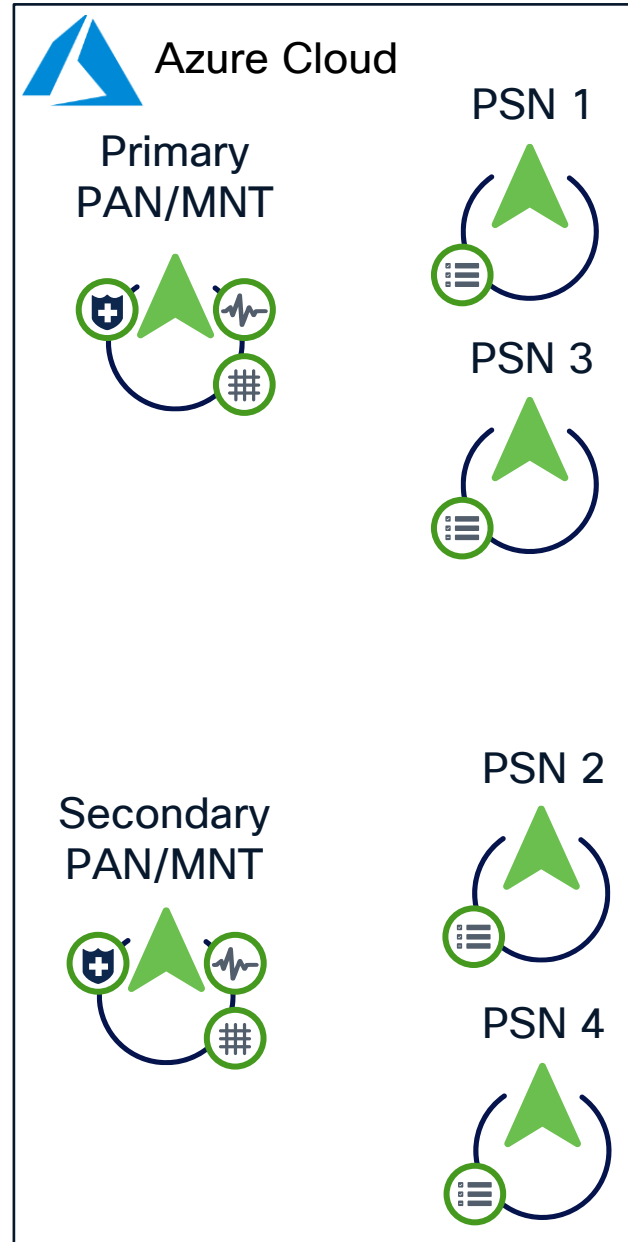
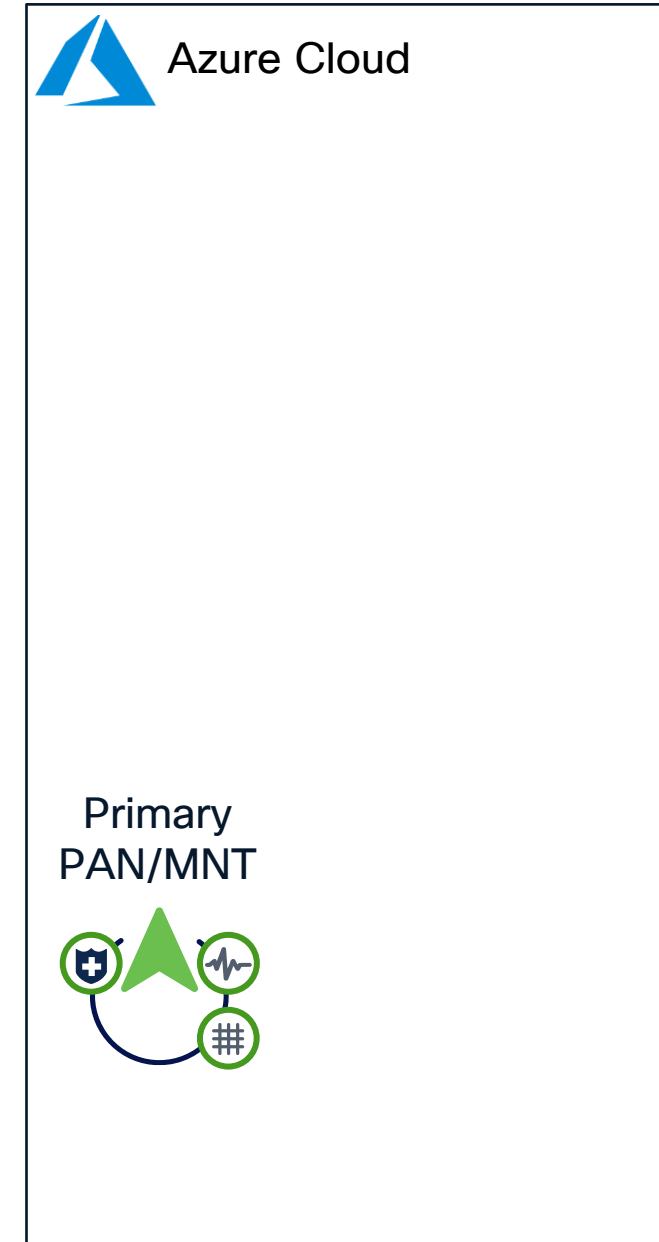
Upgrade

--- === Phase 1 === ---

- Deregister Secondary PAN/MNT and delete the instance
- Deploy the new instance to destination ISE release.
- Install the patch
- Restore the Backup
- Promote the Standalone Node to Primary PAN/MNT

Considerations:

- (Optional) Certificates to be exported prior Deregistration of Secondary PAN, imported after the Backup Restore



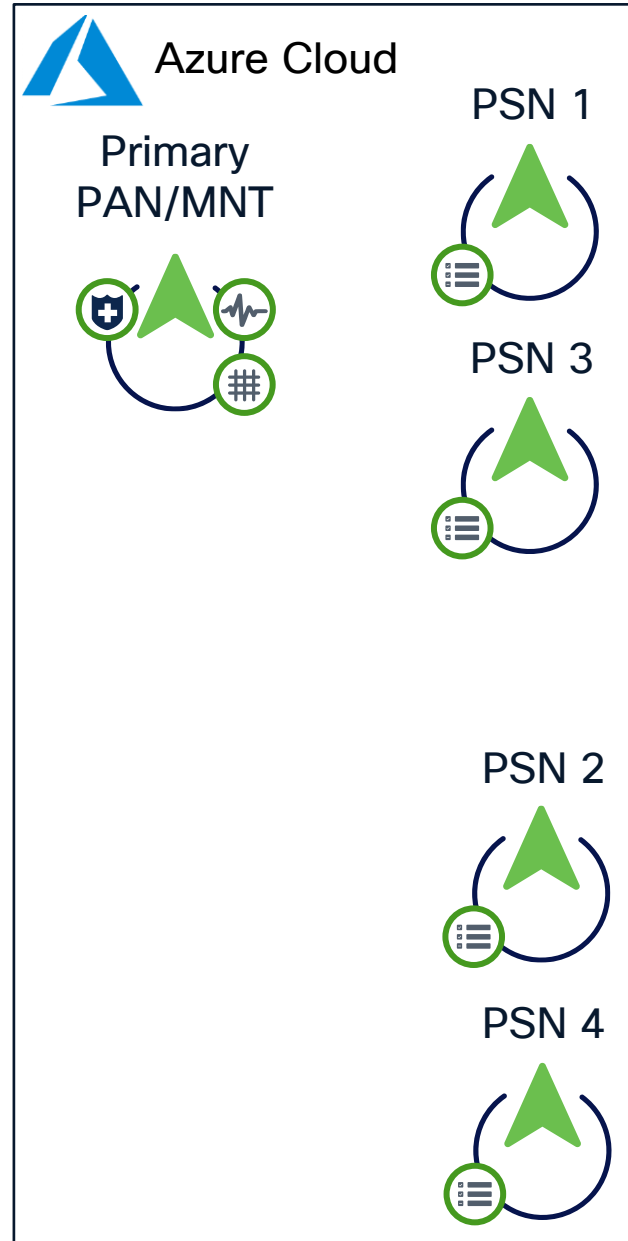
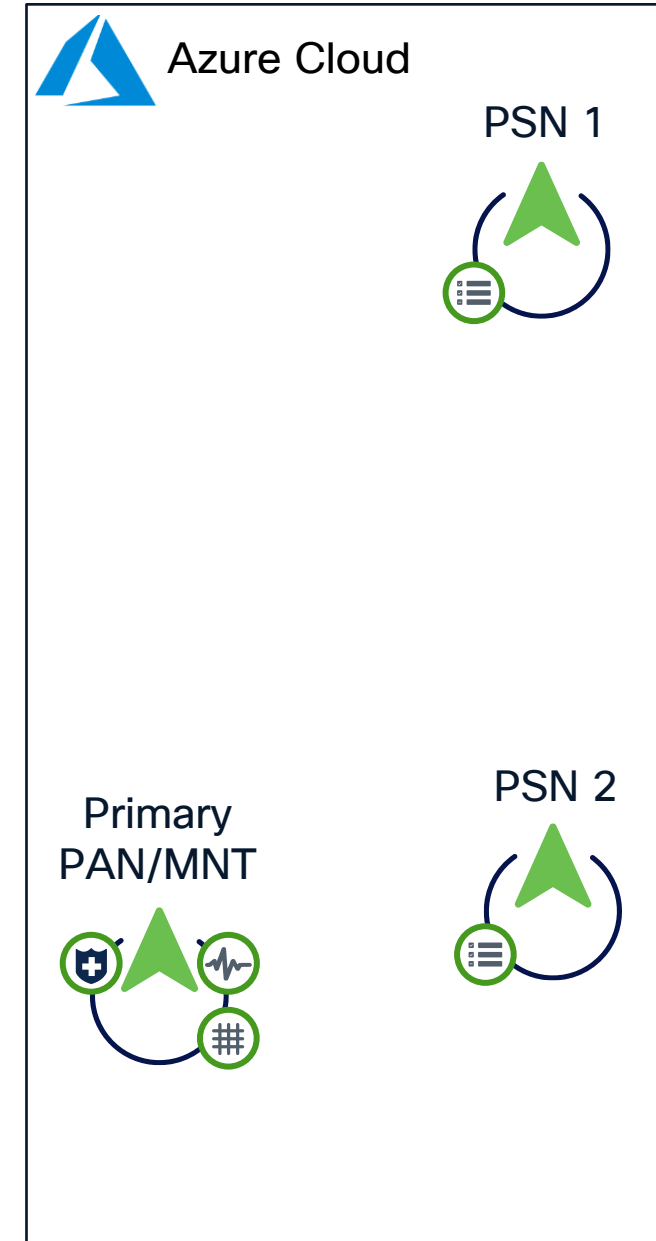
Upgrade

--- === Phase 2 === ---

- Deregister PSN1 and PSN2 and delete the instances
- Deploy the new instances to destination ISE release.
- Install the patch
- Join the new deployment
- Test

Considerations:

- (Optional) Certificates to be exported prior Deregistration of PSN1 and PSN2, imported before Joining the Deployment
- NAD's configuration should be evaluated prior Deregistration. Exclude PSN1 and PSN2 from LB Groups or ensure that high availability configuration includes PSN3 and PSN4



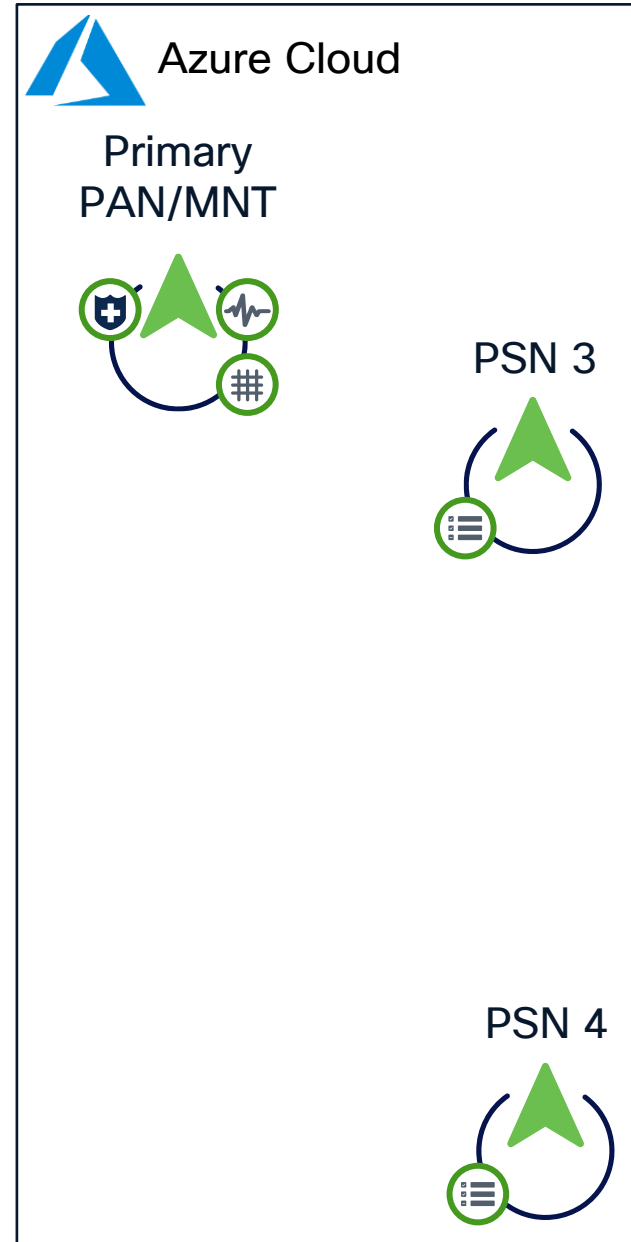
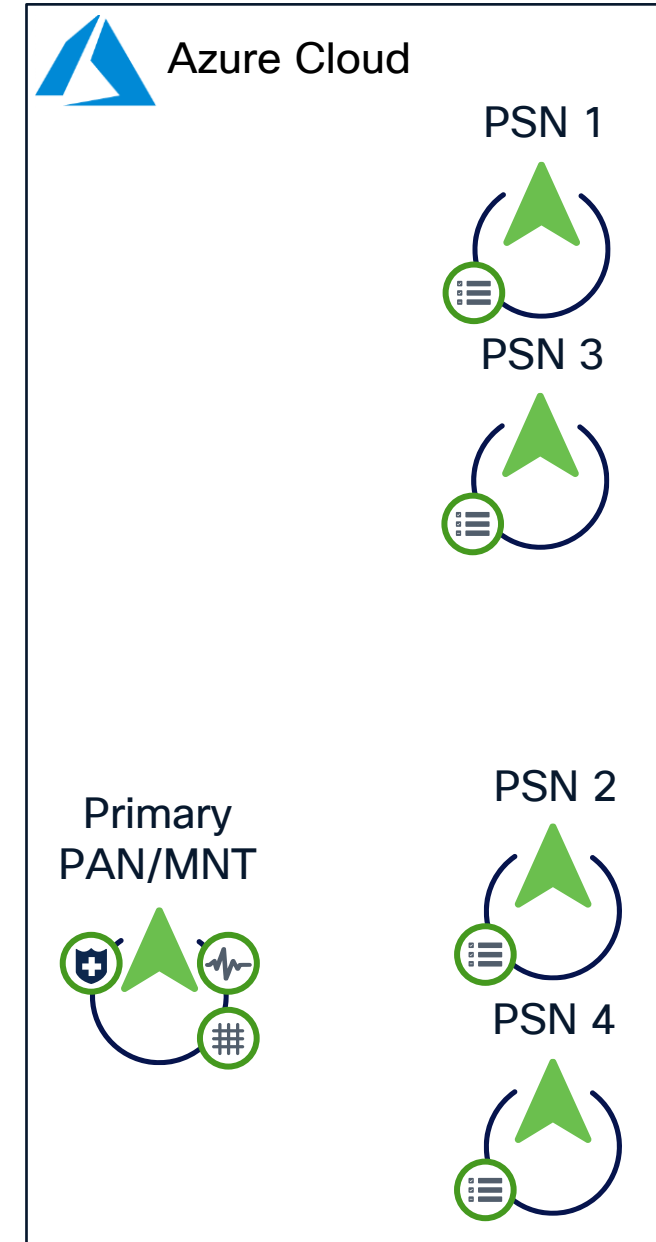
Upgrade

--- === Phase 3 === ---

- Deregister PSN3 and PSN4 and delete the instances
- Deploy the new instances to destination ISE release.
- Install the patch
- Join the new deployment
- Test

Considerations:

- (Optional) Certificates to be exported prior Deregistration of PSN3 and PSN4, imported before Joining the Deployment
- NAD's configuration should be evaluated prior Deregistration. Exclude PSN3 and PSN4 from LB Groups or ensure that high availability configuration includes PSN1 and PSN2



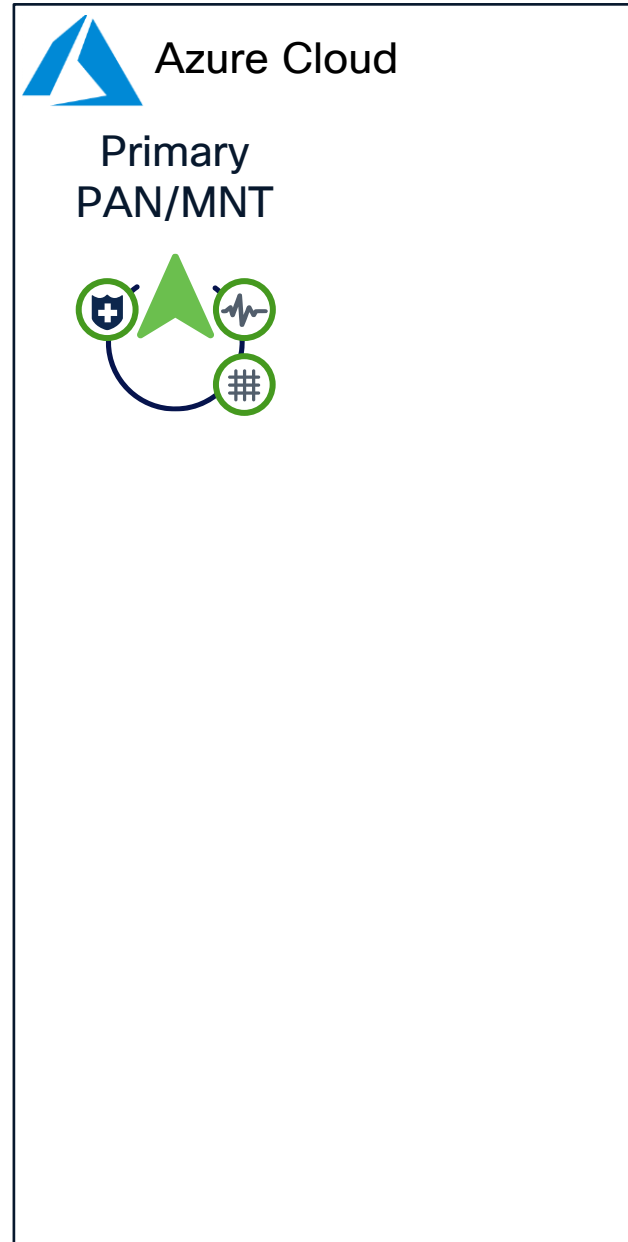
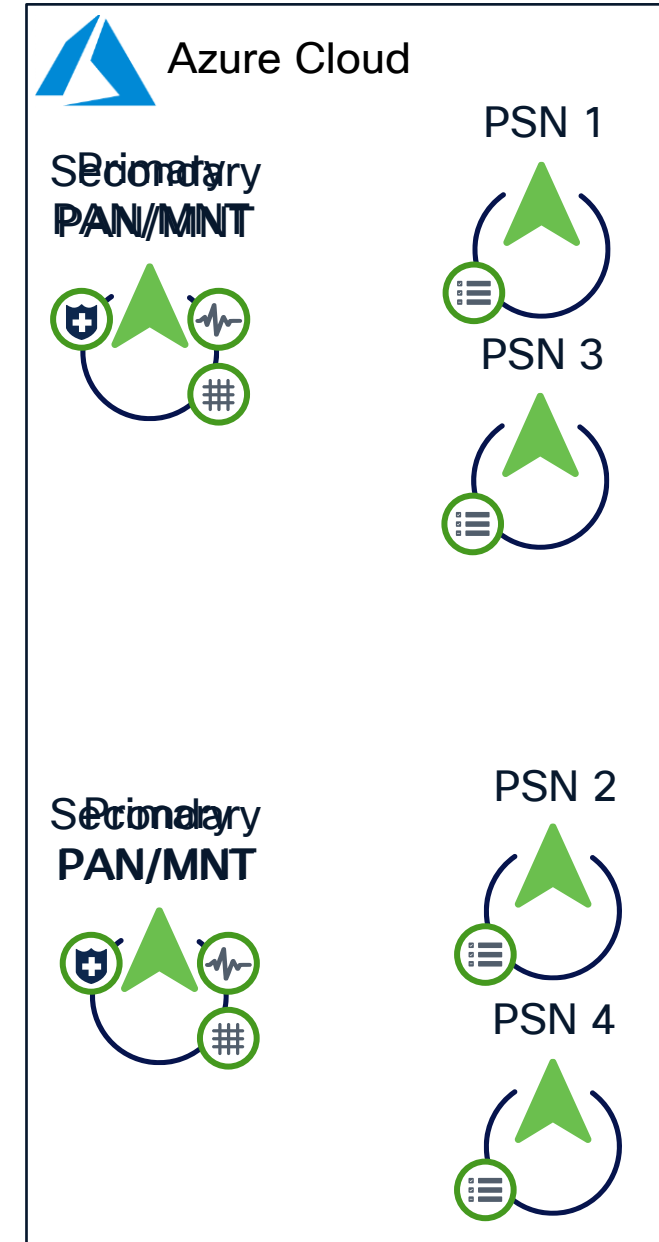
Upgrade

--- === Phase 4 === ---

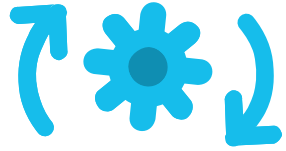
- Delete Primary PAN/MNT of old deployment
- Deploy the new instance to destination ISE release.
- Install the patch
- Join the new deployment
- Promote Secondary PAN/MNT to Primary PAN/MNT
- Test

Considerations:

- (Optional) Certificates to be exported prior Deregistration of Primary PAN, imported before joining the deployment



ISE in the Cloud. Design Considerations



- Inline upgrade workflow is not supported. Only fresh installs are supported. However, you can carry out backup and restore of configuration data



- SSH access to Cisco ISE CLI using password-based authentication is not supported. You can only access the Cisco ISE CLI through a key pair



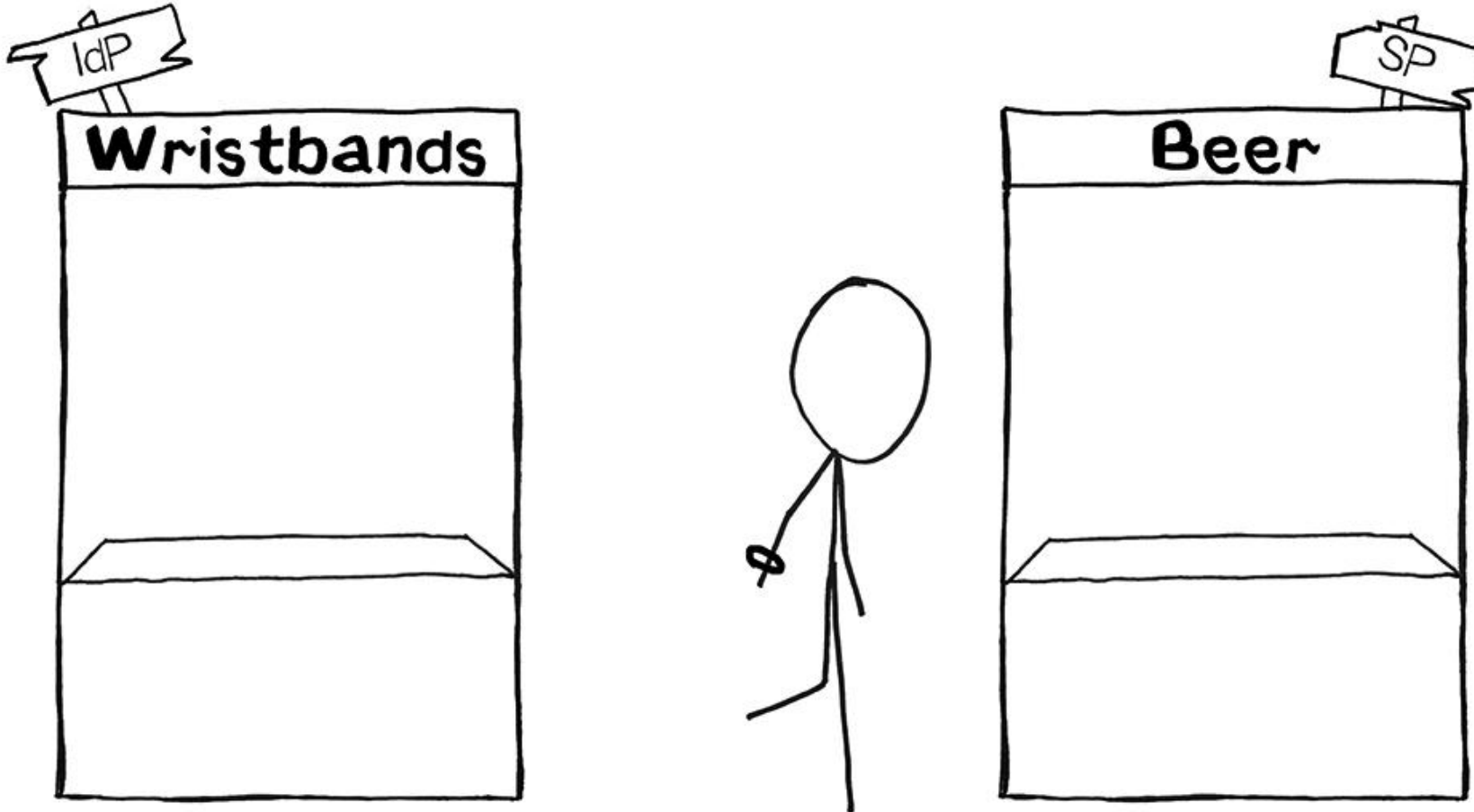
- Latency should be below 300 msec



- Starting ISE 3.2 default GUI username is “iseadmin”

ISE SAML SSO

What is SAML?



[The Beer Drinker's Guide to SAML](#)

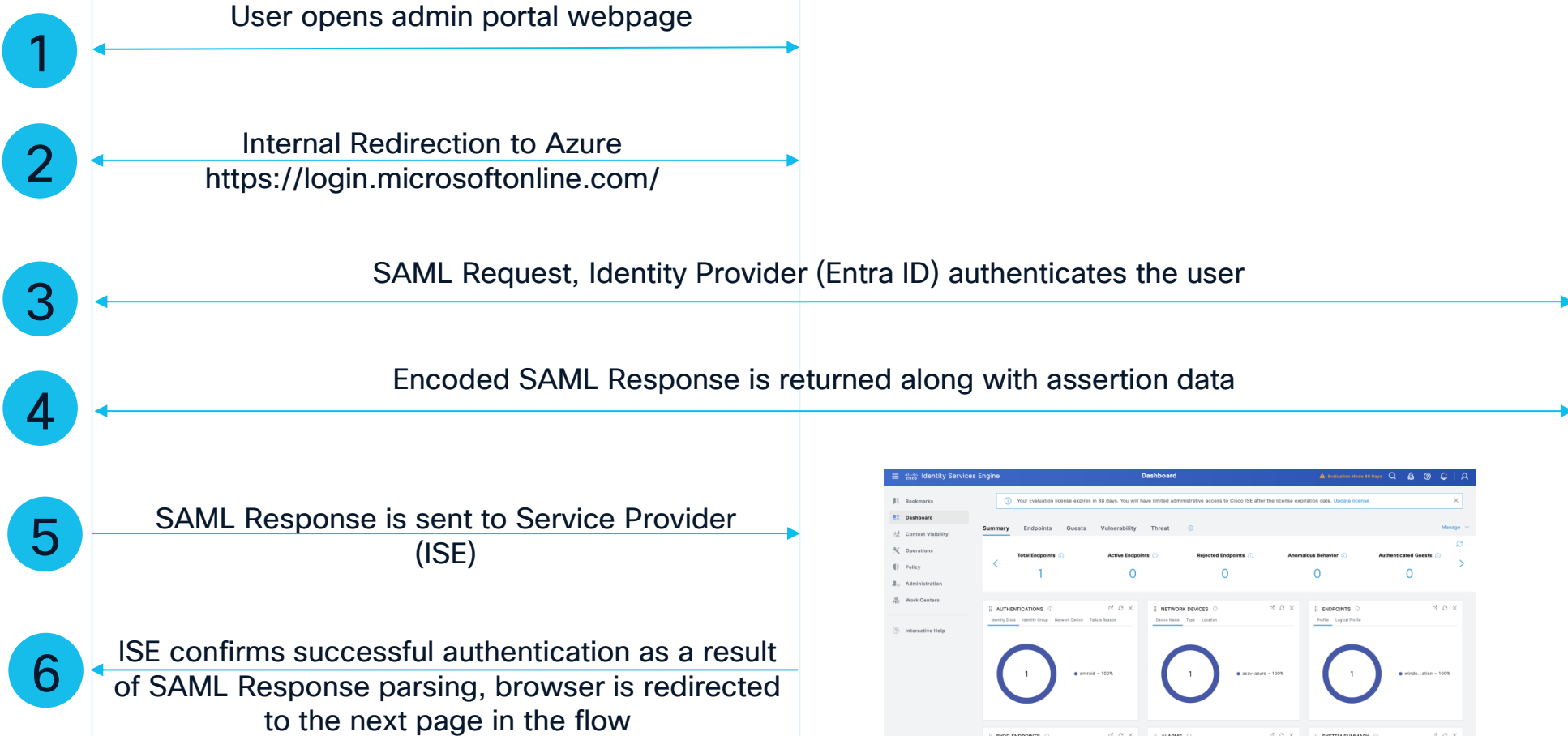
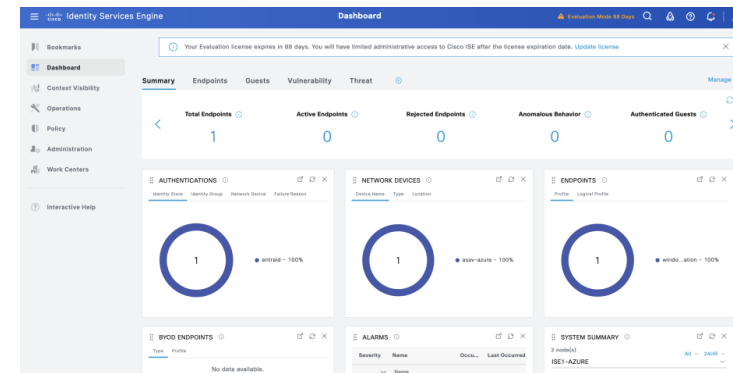
Web Browser



ISE



Entra ID

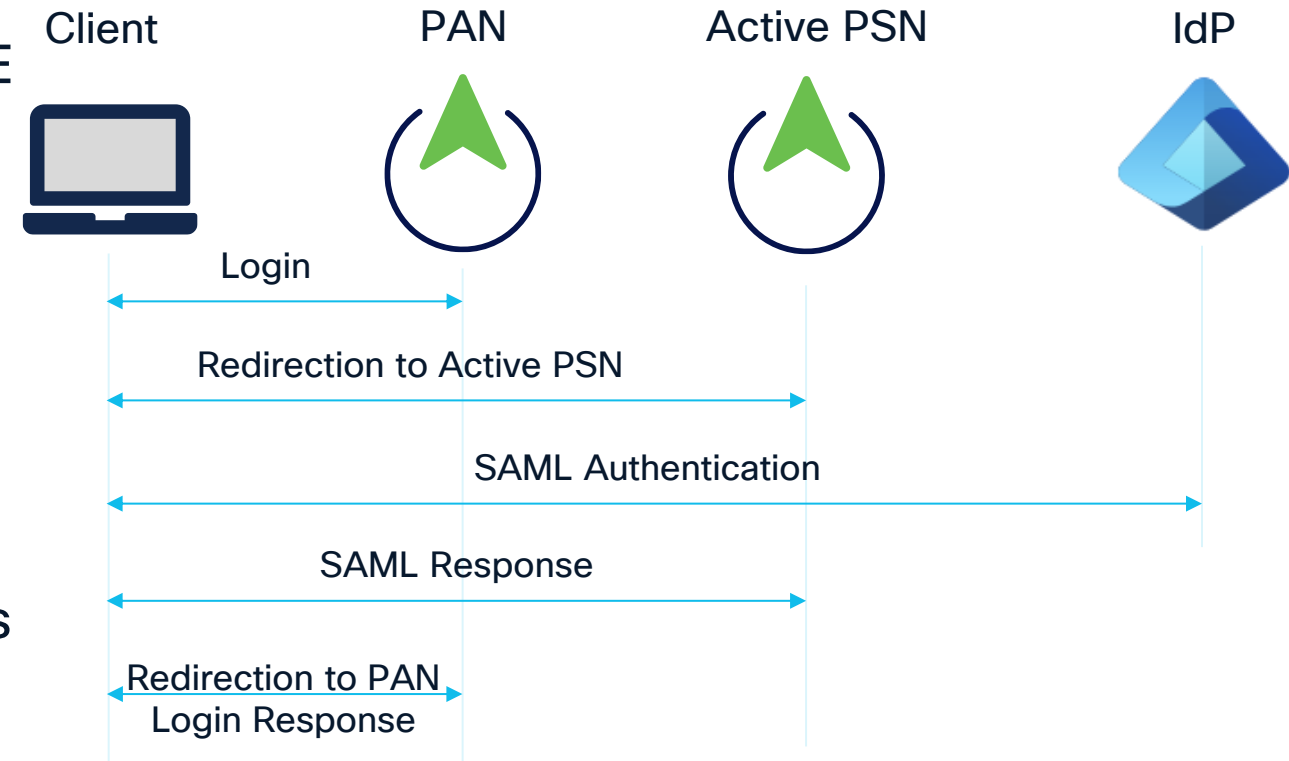


CSCwh49351 SAML request PSN exclusion



Problem:

- ISE Deployment has a dependency on PSN node (we call it “Active PSN”)
- Active PSN is automatically selected by ISE Administrator has no control over it
- Admin SAML authentication doesn't work if:
 - Active PSN is not reachable from client
 - Active PSN is down
 - Active PSN domain is not the same as the ISE node where admin logging in



CSCwh49351 SAML request PSN exclusion



Solution:

- No dependency with any other node
- Entire flow gets executed with ISE node (where admin user logs in)

Action: None (if all Assertion Consumer Services URL's are already present in IdP as Reply URL's)

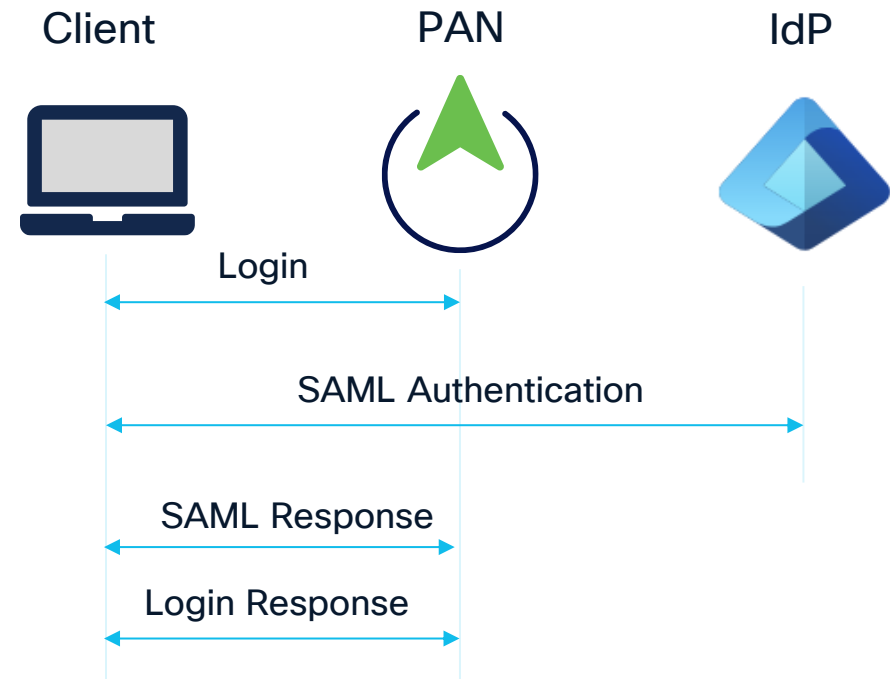
Known Fixed Releases:

ISE 3.1 patch 10

ISE 3.2 patch 7

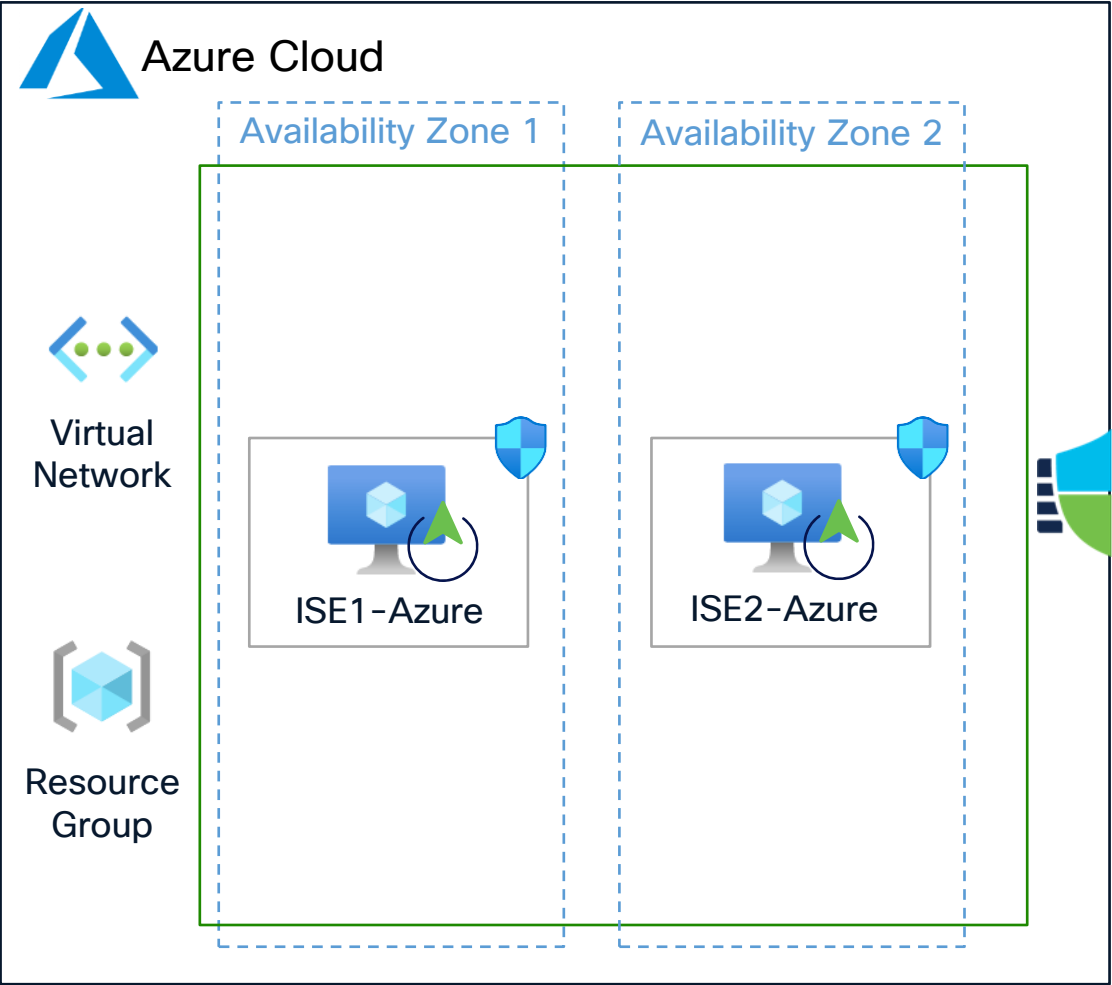
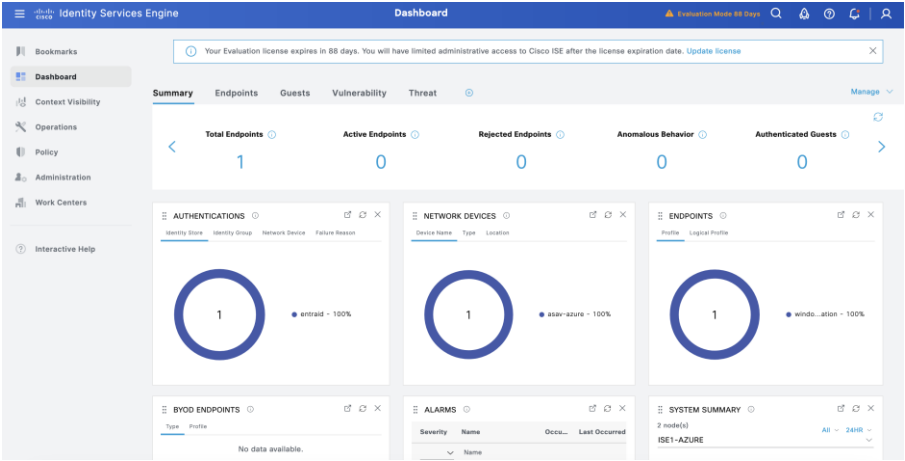
ISE 3.3 patch 4

ISE 3.4

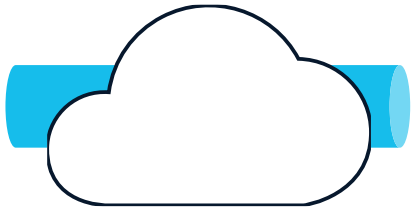


Demo. ISE Admin Portal Authentication with SAML SSO

Demo Topology



Site to Site VPN Tunnel



Entra ID SAML
Identity Provider



Configure SAML SSO with
Entra ID for Admin Access

- 🔖 Bookmarks
- 🏠 Dashboard
- 📊 Context Visibility
- 🔧 Operations
- 🛡️ Policy
- 👤 Administration
- 🏢 Work Centers
- ❓ Interactive Help

❗ Your Evaluation license expires in 88 days. You will have limited administrative access to Cisco ISE after the license expiration date. [Update license](#)

✕

Summary

Endpoints

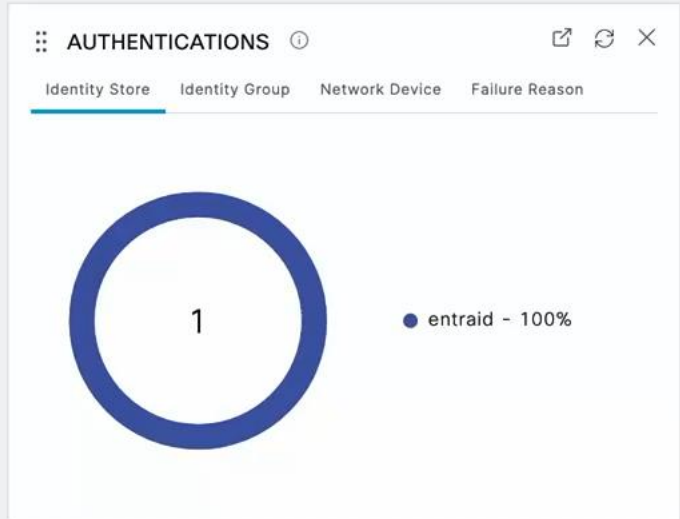
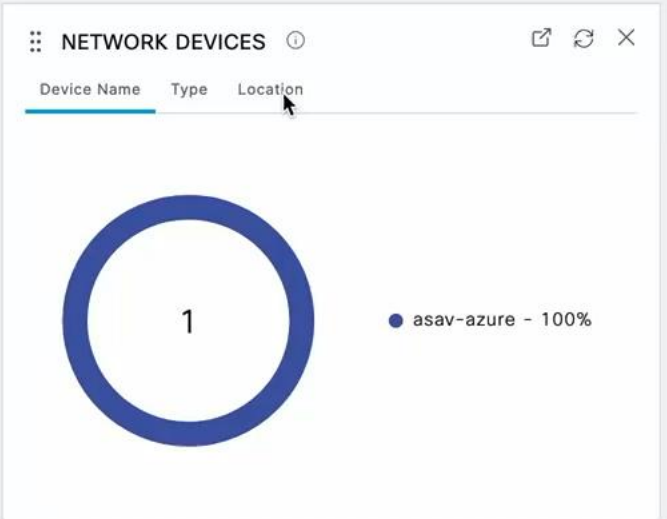
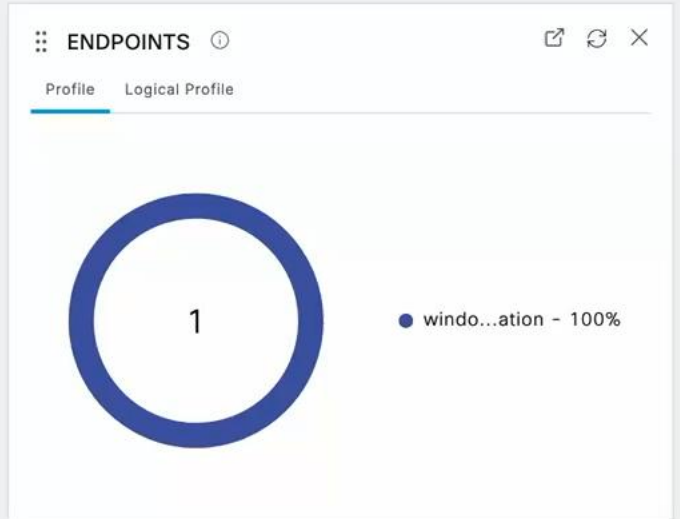
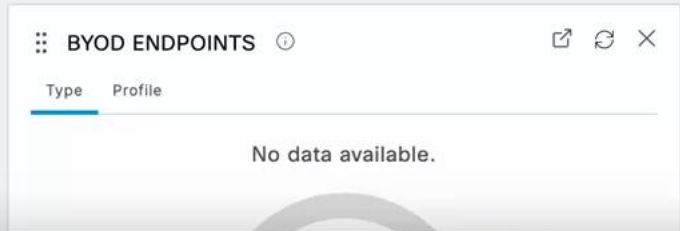
Guests

Vulnerability

Threat

⊕

Manage ▾



ALARMS ⓘ

Severity	Name	Occu...	Last Occurred
▼	Name		
❗	Configuration Changed	9507	less than 1 min

SYSTEM SUMMARY ⓘ

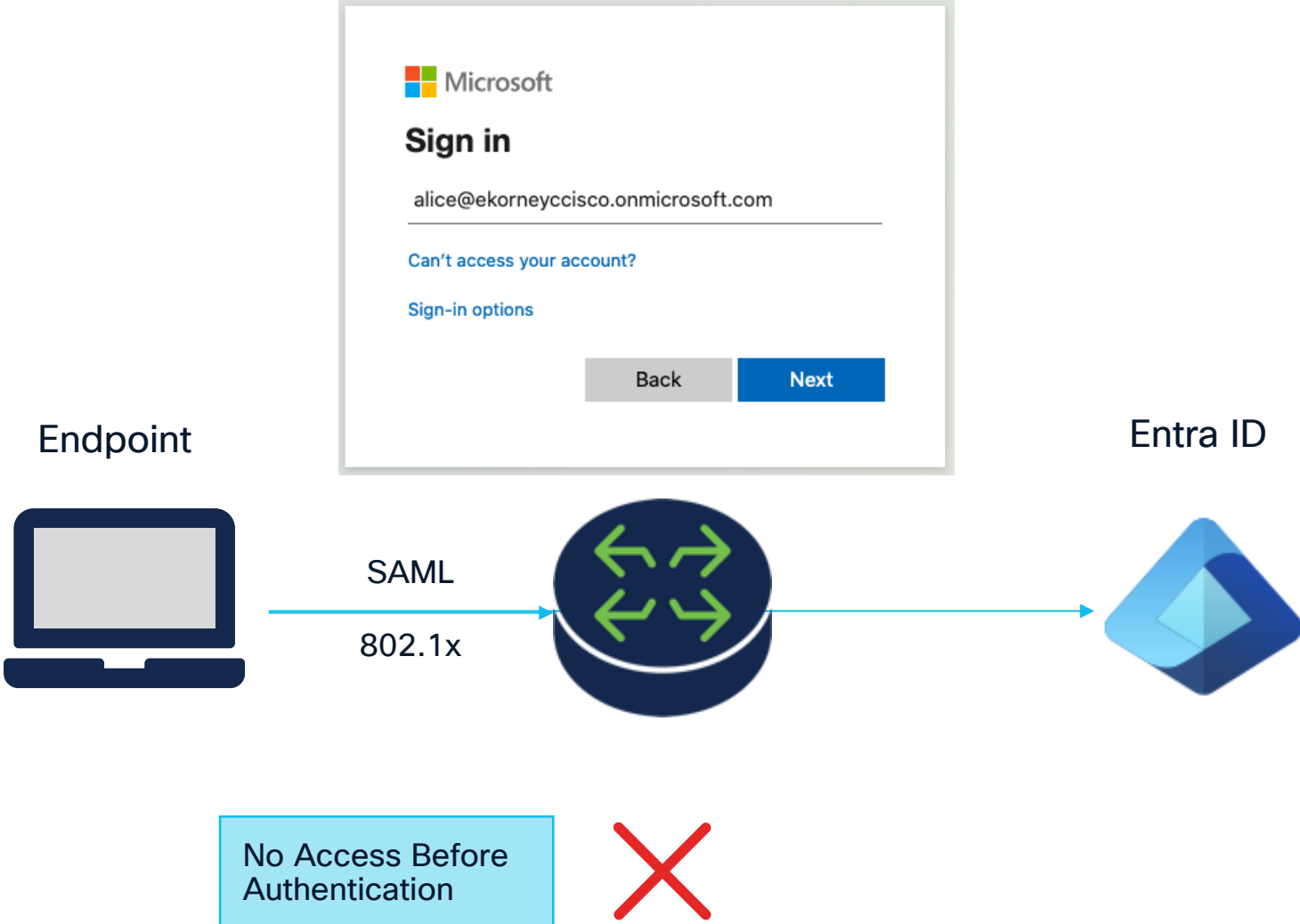
2 node(s)

ISE1-AZURE

All ▾ 24HR ▾

Entra ID Authentications

802.1x Authentication Problem with SAML



SAML assumes network connectivity, so the Endpoint can reach Identity Provider

802.1x being a Layer 2 authentication protocol, will grants Network Access after Authentication is completed

Microsoft Active Directory vs Entra ID



Aspect	Active Directory	Entra ID
Purpose	Centralized management for users and groups Validating identity of the users and devices Granting permissions to the resources based on the roles	
Architecture	On-premises infrastructure	Cloud Native
Authentication Protocols	Kerberos and NTLM for on-prem authentication	OAuth, OpenID, SAML for cloud-based apps
Device Management	Manages on-prem devices via GPO	Manages variety of devices via Intune

Active Directory User vs Entra ID User

monica Properties

Published Certificates Member Of Password Replication Dial-in Object
Security Environment Sessions Remote control
Remote Desktop Services Profile COM+ Attribute Editor

General Address Account Profile Telephones Organization

monica

First name: monica Initials:

Last name:

Display name: monica

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help



alice

alice@cxsecurity.onmicrosoft.com

Member

User principal name

alice@cxsecurity.onmicrosoft.com

Object ID

f43b00a4-5604-4936-8b0c-7f4ffbd8c4b2

Created date time

Dec 4, 2022, 1:02 PM

User type

Member

Identities

[cxsecurity.onmicrosoft.com](#)

Group memberships

4

Applications

5



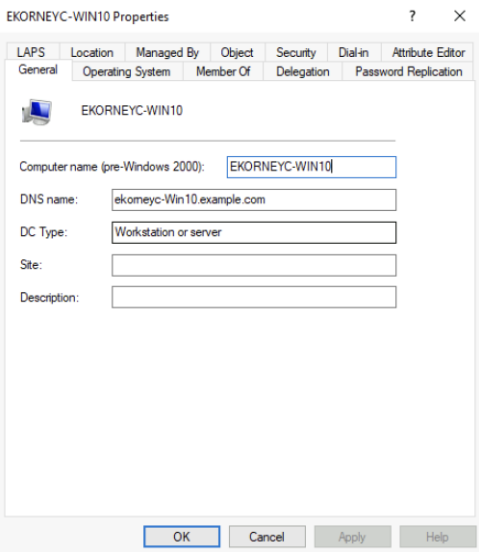
Active Directory User



Entra ID User

Aspect	Represent User Identity	
Purpose		
Identifier	User Principle Name (UPN), Distinguished Name (DN), SID, sAMAccountName	User Principle Name (UPN), Object ID
Management	Active Directory, Group Policy (GPO)	Entra ID, Intune
Source	Manual Creation	Manual Creation, Synchronized via Entra Connect

Active Directory Computer vs Entra ID Device



Active Directory Computer



Entra ID Device

Aspect	Represent Computer/Device Identity	
Purpose		
Identifier	SID, sAMAccountName	Device ID, Object ID
Management	Active Directory, Group Policy (GPO)	Entra ID, Intune
Source	Automatic Creation	Automatic Creation, Synchronized via Entra Connect

Entra ID Device Join Types

Microsoft Azure

[Home](#) > [cxsecurity | Devices](#) > [Devices | Overview](#) >

All devices

Download devices

Refresh

Manage view

Enable

Disable

Delete

Manage

Preview features

Search by name or device ID or object ID

Add filters

5 devices found

☐	Name ↕	Enabled	OS	Version	Join type	MDM
☐	 JTOOTHMA-AZVM	 Yes	Windows	10.0.22621.3007	Microsoft Entra joined	Microsoft Intune
☐	 NXHG8AA001922099	 Yes	Unknown	Unknown	Microsoft Entra joined	None
☐	 DESKTOP-5FR9KQJ	 Yes	Windows	10.0.19045.4412	Microsoft Entra registered	None
☐	 DESKTOP-ELL9K55	 Yes	Windows	10.0.19045.3803		Microsoft Intune
☐	 EKORNEYC-WIN11	 Yes	Windows	10.0.22000.2713	Microsoft Entra registered	Microsoft Intune

Registered Device:

- BYOD Device
- Login with personal credentials
- Corporate credentials when registering
- Register via Settings

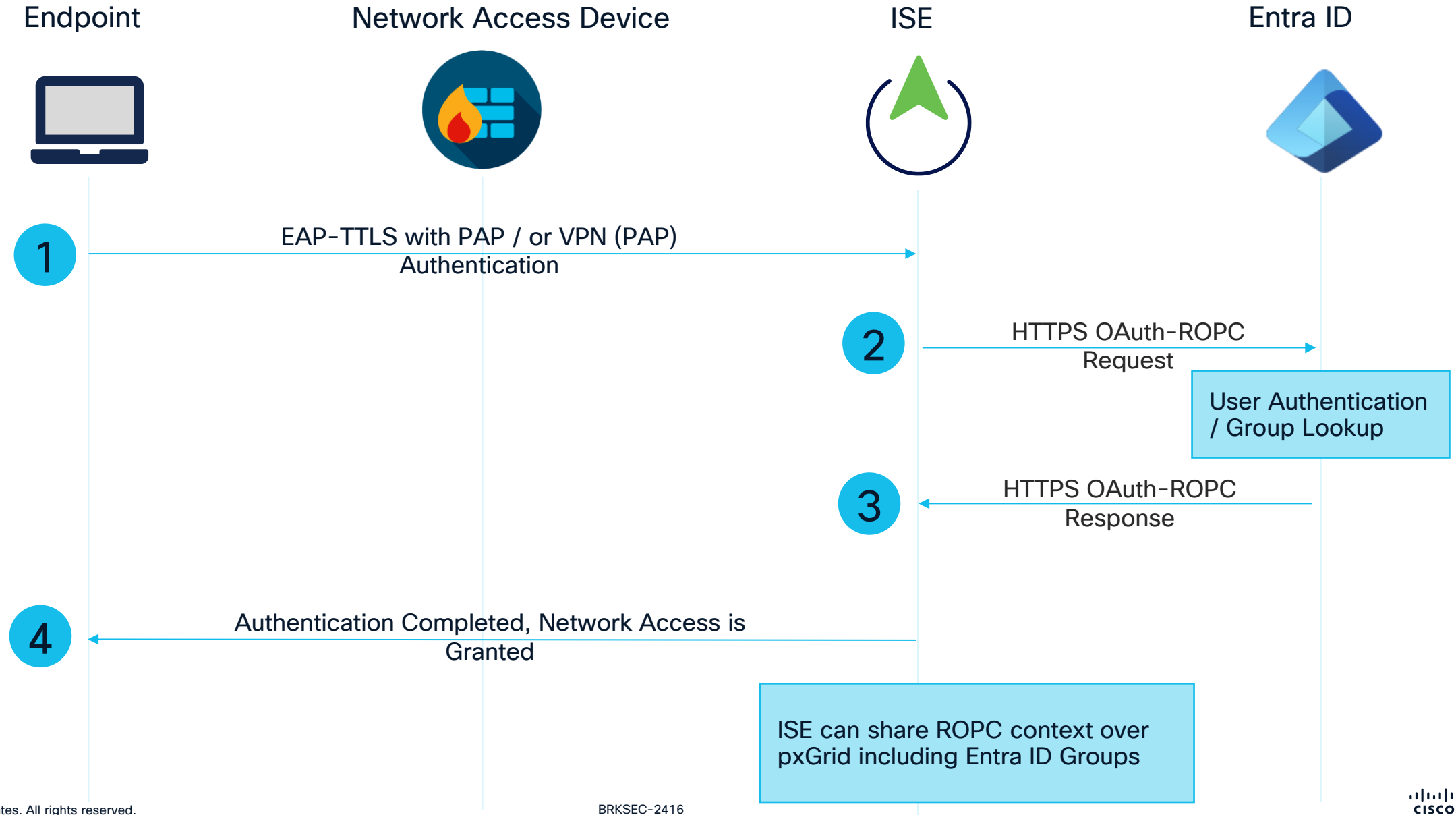
Joined Device:

- Generally, Company Owned Device
- Login with Entra ID credentials
- Autopilot, Out Of Box Experience
- Full control over the Device

Hybrid Joined Device:

- Joined to on-premises Active Directory and Microsoft Entra ID
- Login with corporate credentials
- Synchronized via Entra Connect

ROPC Flow Diagram



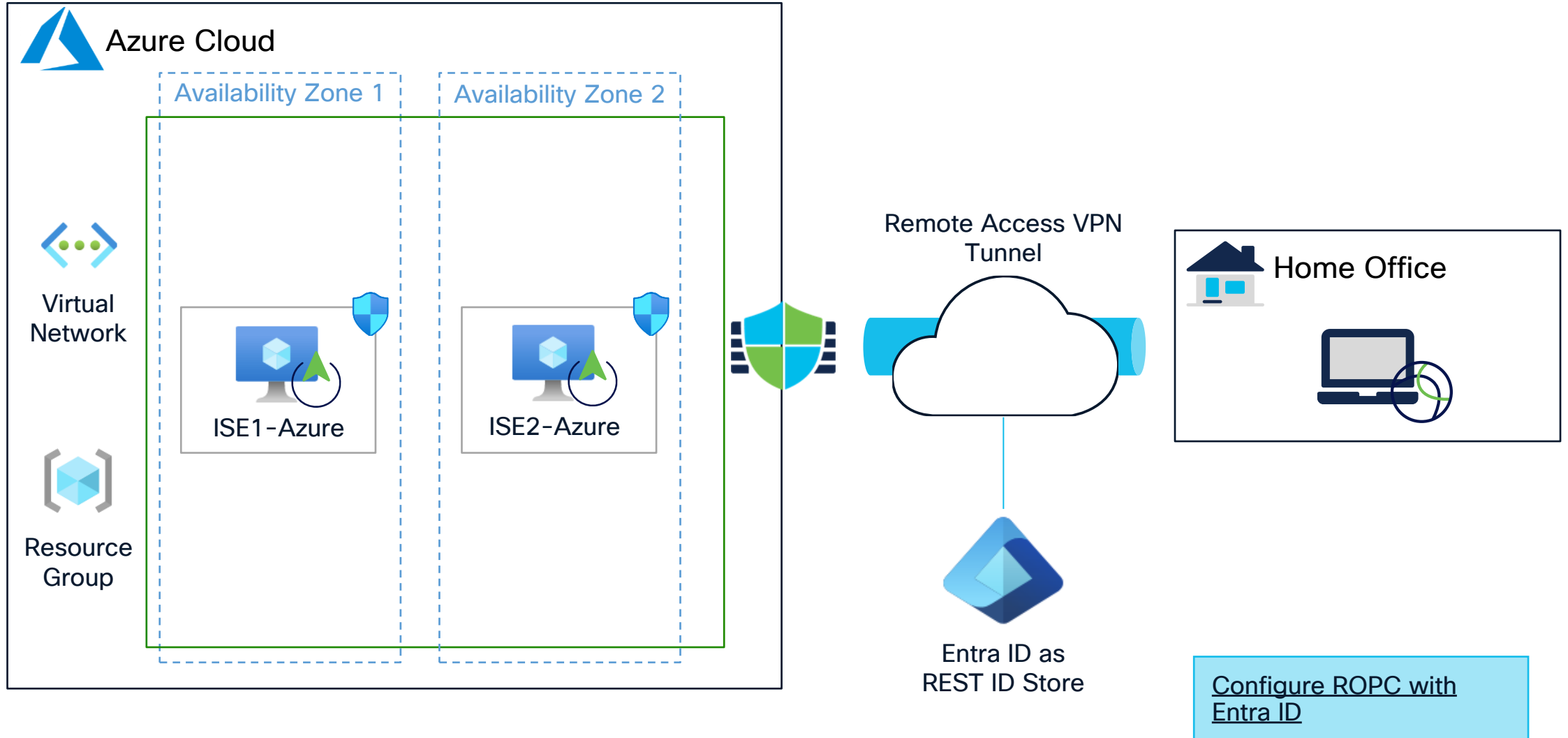
ROPC Limitations



- No user interactions allowed for password changes, MFA, or AUPs
- No new accounts that have not yet changed the default password
- Only user authentication is supported

Demo. ROPC Authentication with VPN Use Case

Demo Topology



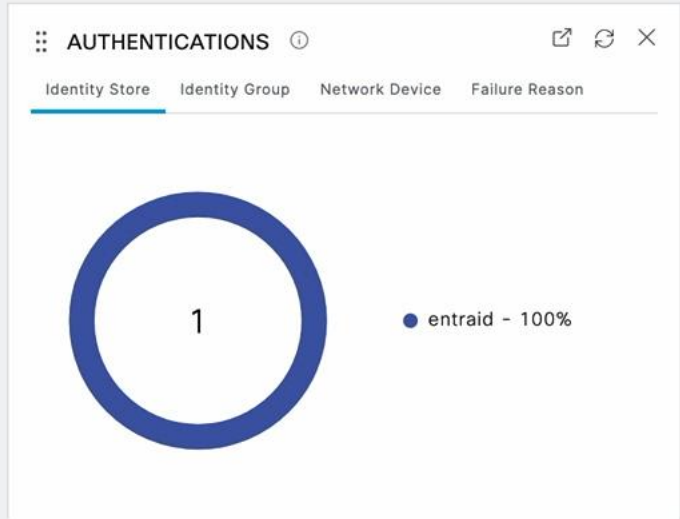
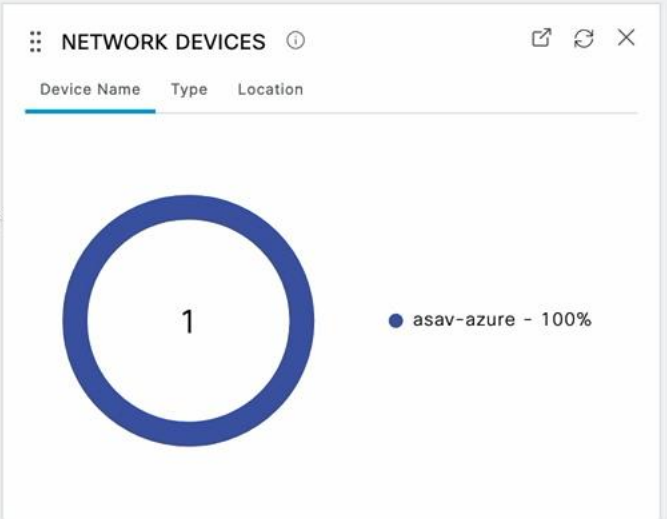
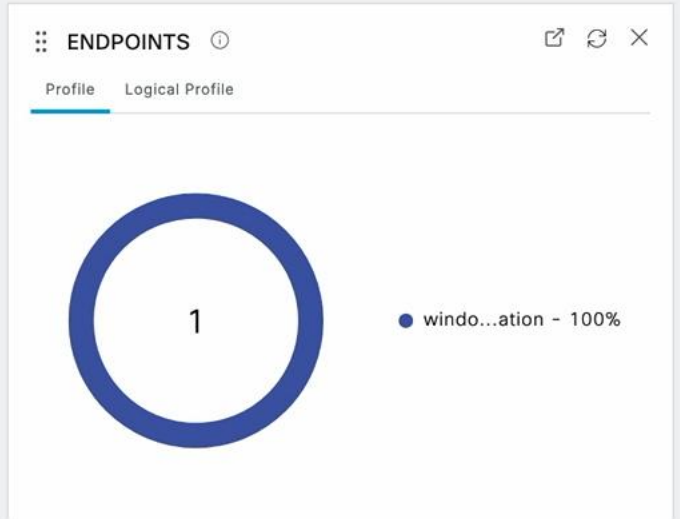
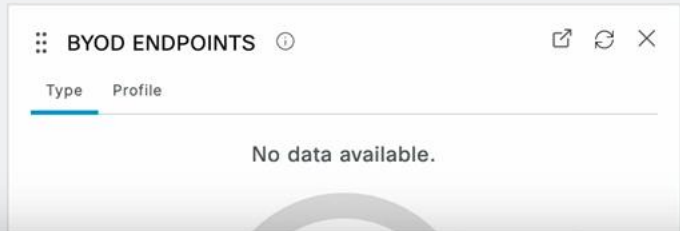
- [🔖 Bookmarks](#)
- [🏠 Dashboard](#)
- [📊 Context Visibility](#)
- [🔧 Operations](#)
- [🛡️ Policy](#)
- [👤 Administration](#)
- [🏢 Work Centers](#)
- [❓ Interactive Help](#)

[❓](#) Your Evaluation license expires in 87 days. You will have limited administrative access to Cisco ISE after the license expiration date. [Update license](#)

[✕](#)

Summary Endpoints Guests Vulnerability Threat [+](#)

[Manage](#) [▼](#)



[☰](#) ALARMS [❓](#)

[🔗](#) [🔄](#) [✕](#)

Severity	Name	Occu...	Last Occurred
▼	Name		
❓	Configuration Changed	9516	less than 1 min

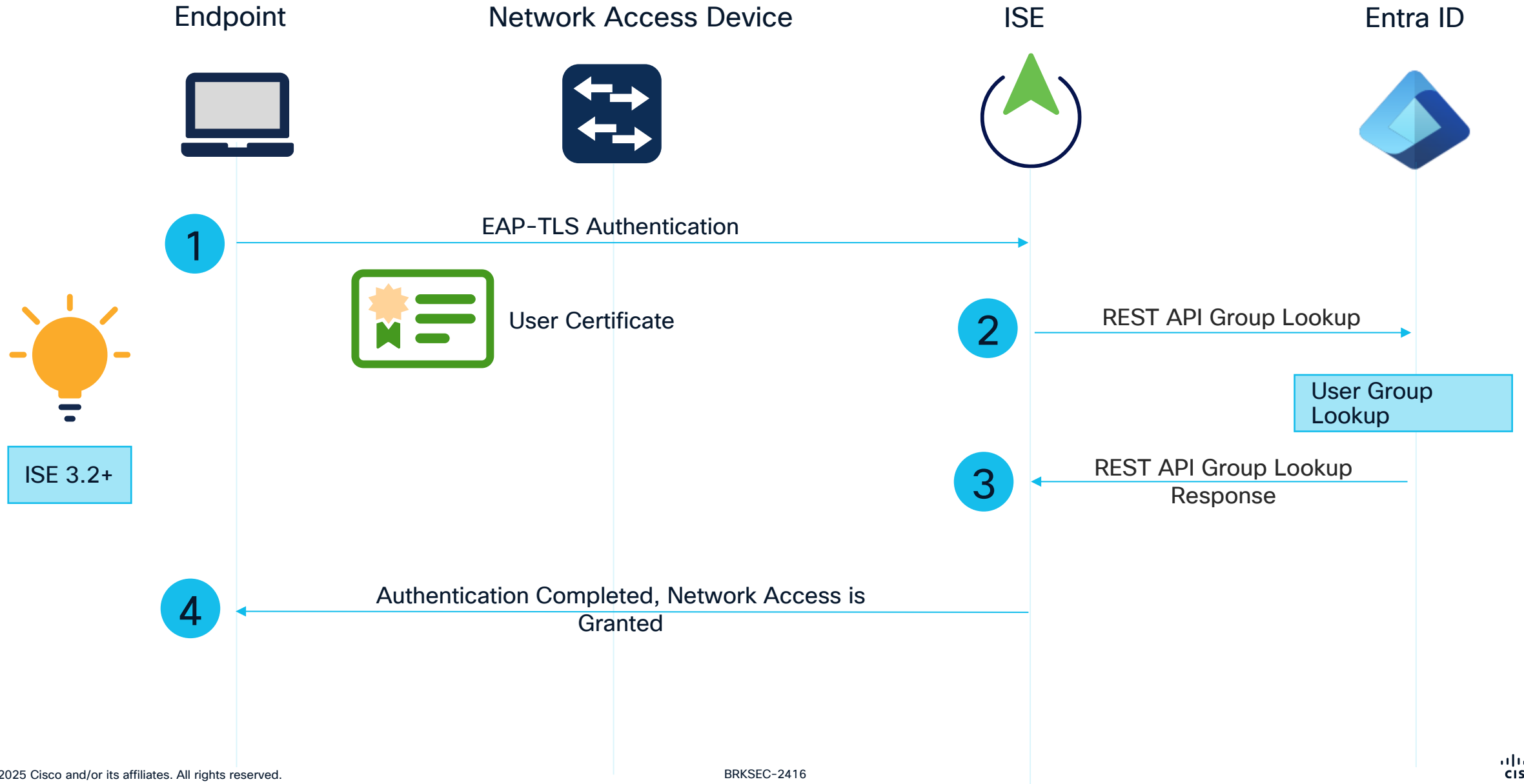
[☰](#) SYSTEM SUMMARY [❓](#)

[🔗](#) [🔄](#) [✕](#)

2 node(s) [All](#) [24HR](#)

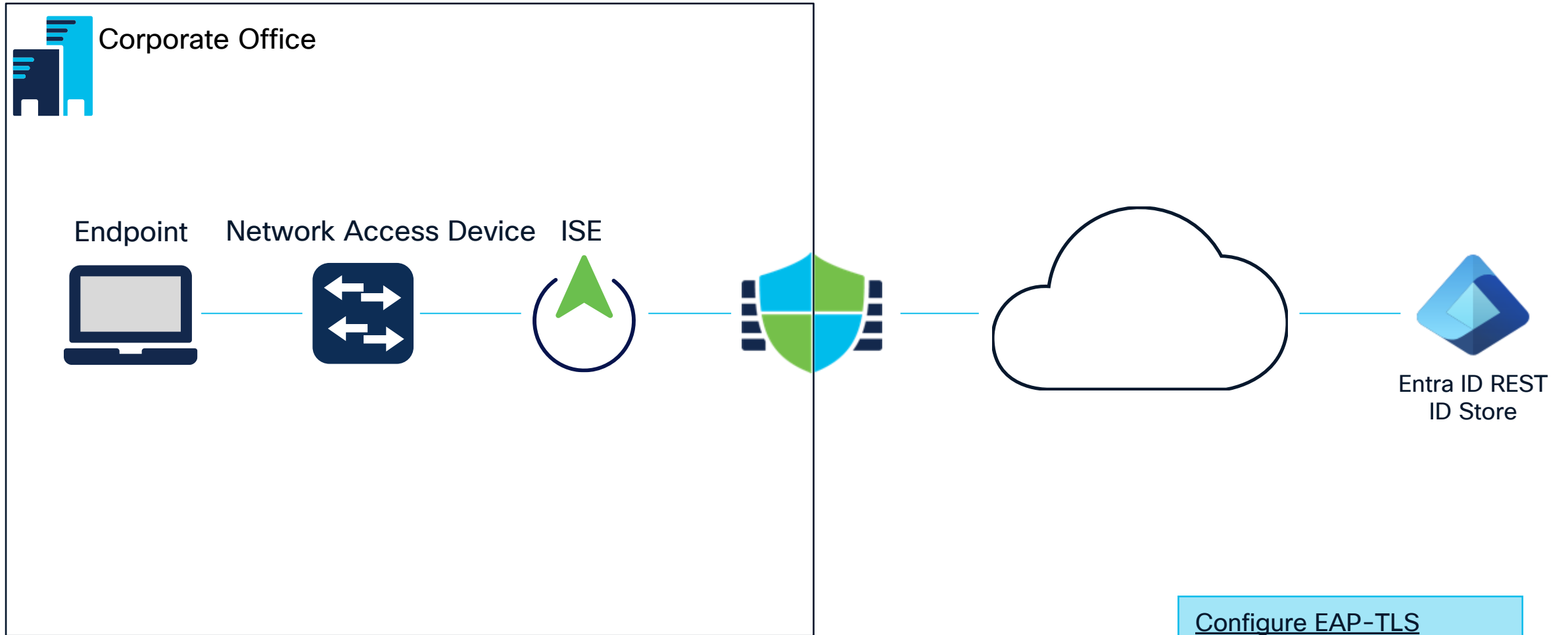
ISE1-AZURE

EAP-TLS User Authorization with Entra ID



Demo. REST ID Store Authorization with EAP-TLS

Demo Topology



Configure EAP-TLS
Authorization with Entra ID

-  Bookmarks
-  Dashboard
-  Context Visibility
-  Operations
-  Policy
-  Administration
-  Work Centers
- 

 Interactive Help

SummaryEndpointsGuestsVulnerabilityThreat+

Manage ▾

<

Total Endpoints ⓘ

136

Active Endpoints ⓘ

4

Rejected Endpoints ⓘ

0

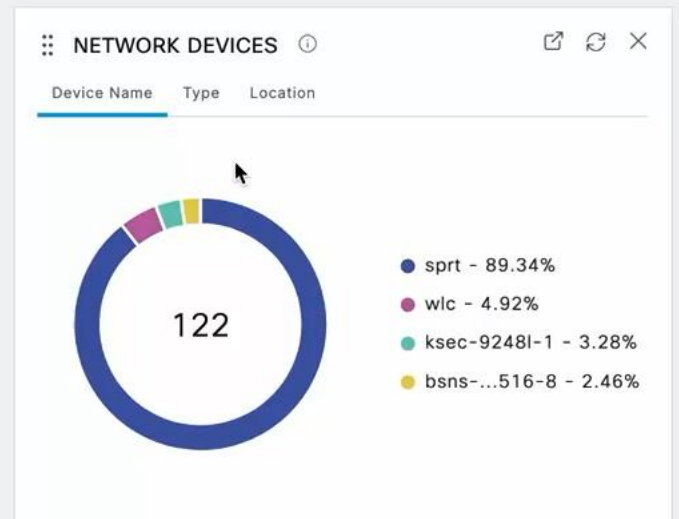
Anomalous Behavior ⓘ

0

Authenticated Guests ⓘ

0

>



⌵ BYOD ENDPOINTS ⓘ

Type

Profile

No data available.

⌵ ALARMS ⓘ

Severity

Name

Occu...

Last Occurred

Severity	Name	Occu...	Last Occurred
ⓘ	Configuration Changed	1023	less than 1 min
⚠	ISE Authentication In...	6392	3 mins ago

⌵ SYSTEM SUMMARY ⓘ

2 node(s)

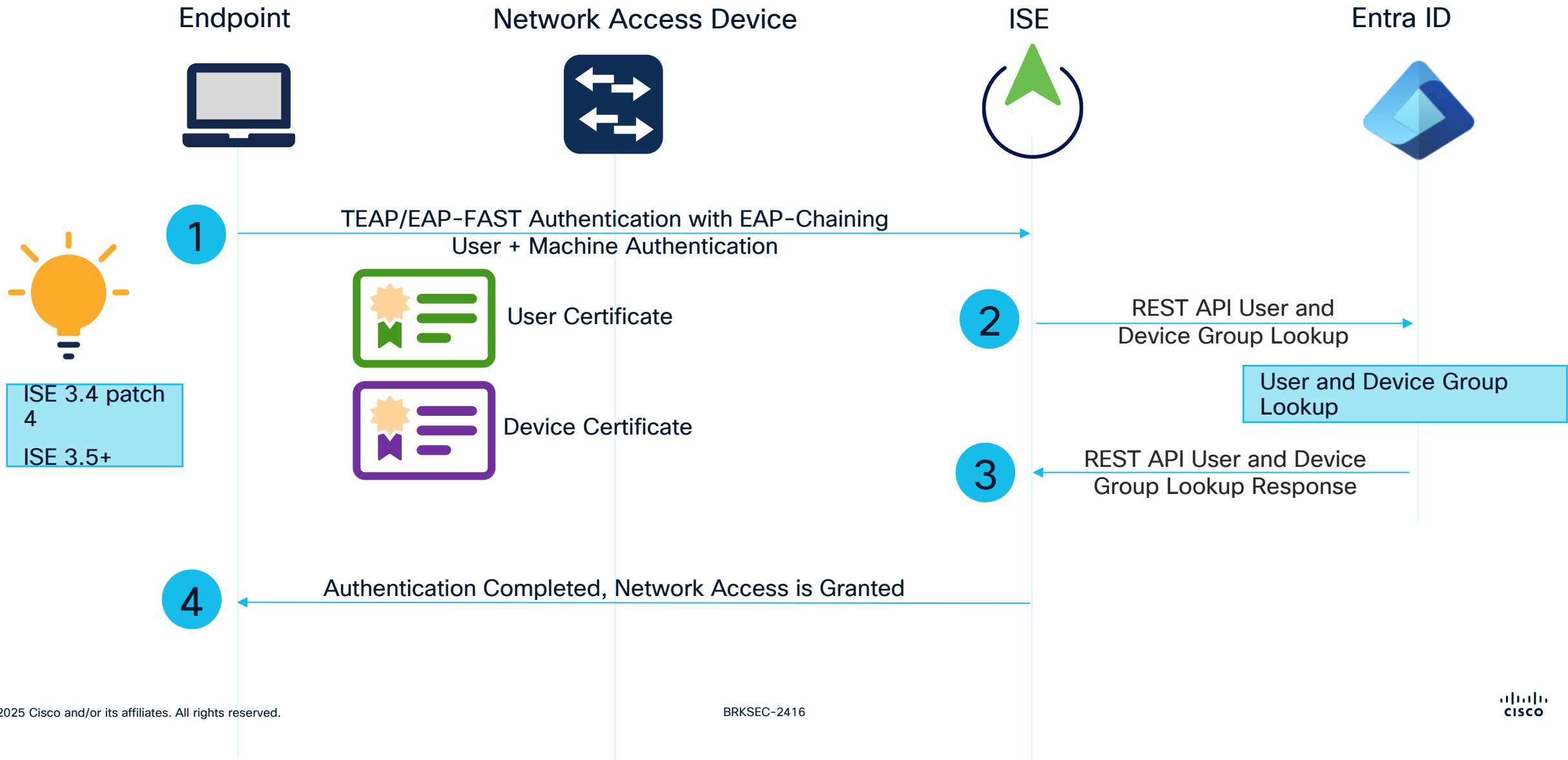
ISE34-1ek

All ▾

24HR ▾



TEAP User and Device Authorization with Entra ID



Demo. REST ID Store Authorization with TEAP

[◀](#)

Total Endpoints ⓘ
62

Active Endpoints ⓘ
2

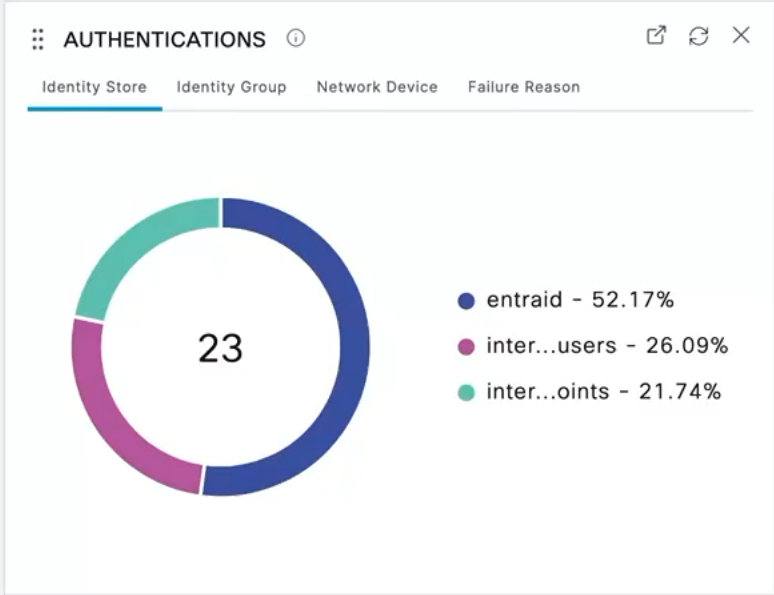
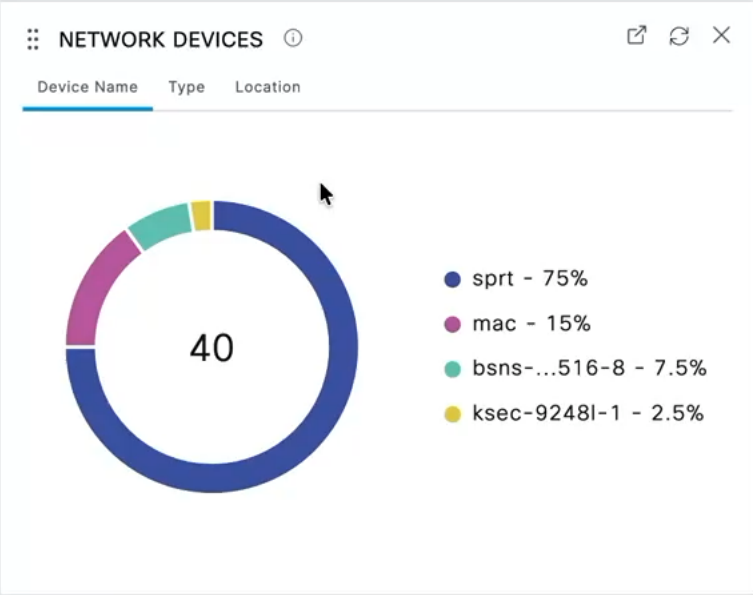
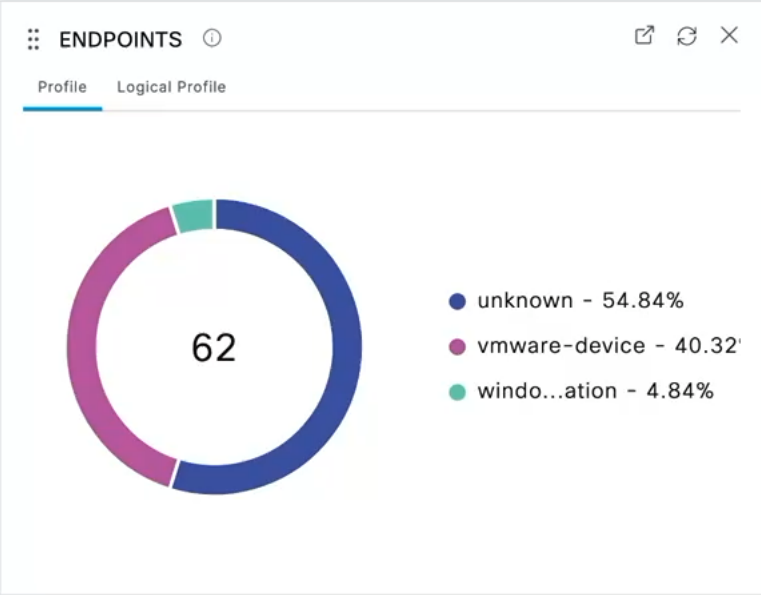
Rejected Endpoints ⓘ
0

Chatty Endpoints ⓘ
0

Anomalous Behavior ⓘ
0

Authenticated Guests ⓘ
0

[▶](#) [🔄](#)



[⋮](#) BYOD ENDPOINTS ⓘ [🔗](#) [🔄](#) [✕](#)

[Type](#) [Profile](#)

No data available.

[⋮](#) ALARMS ⓘ [🔗](#) [🔄](#) [✕](#)

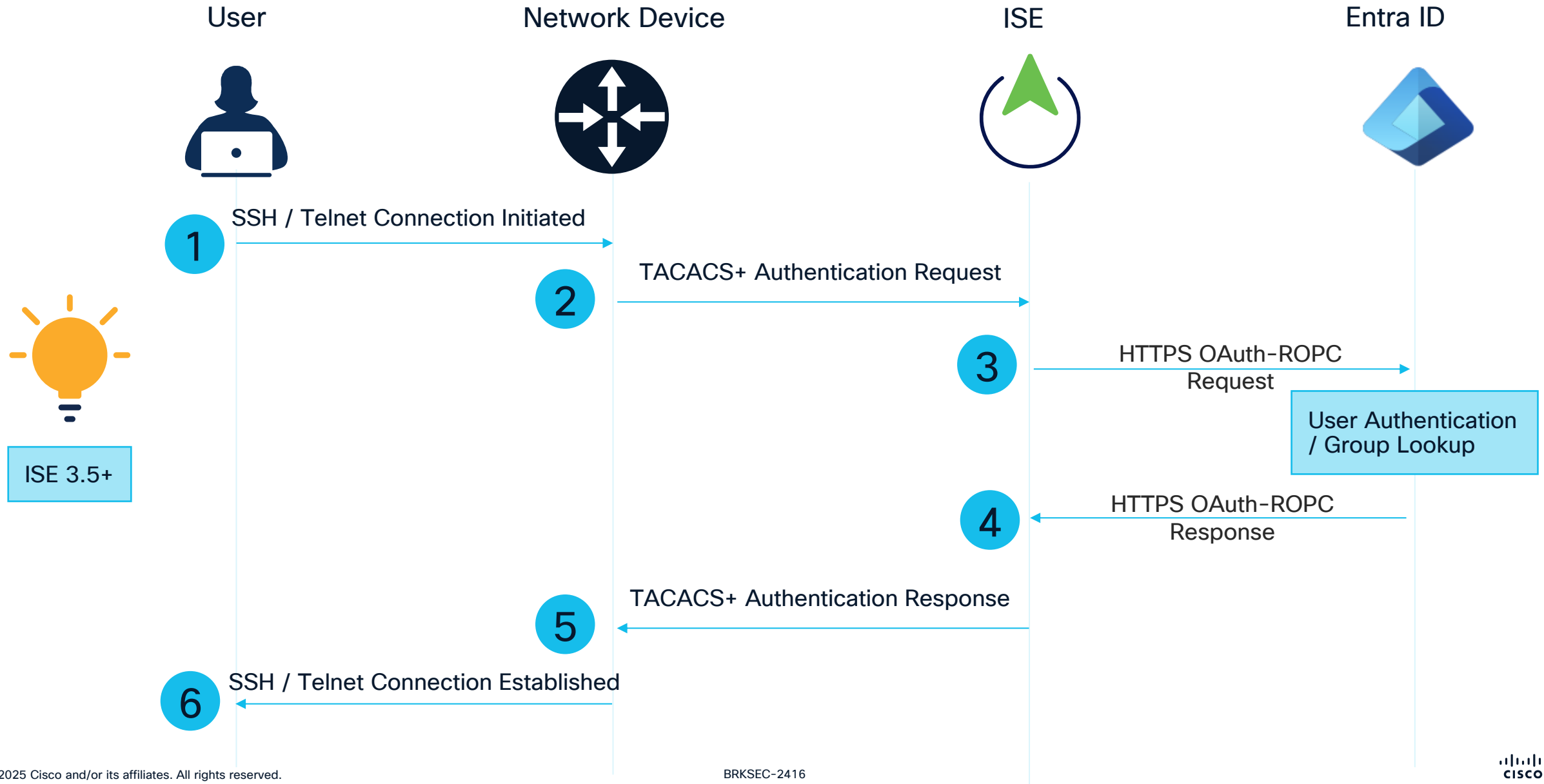
Severity	Name	Occu...	Last Occurred
▼	Name		
ⓘ	Configuration Changed	11198	12 mins ago

[⋮](#) SYSTEM SUMMARY ⓘ [🔗](#) [🔄](#) [✕](#)

2 node(s) [All](#) [24HR](#) [▼](#)

ISE35-1ek [▼](#)

Device Administration with Entra ID Authentication



Demo. Device Administration with Entra ID

```
ekorneyc@EKORNEYC-M-CW9R ~ % ssh joe@10.48.23.70
```

I

Intune Integration

Intune – Mobile Device Manager (MDM) / Mobile Application Manager (MAM)

Microsoft Intune admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

My Dashboard

Private dashboard

New dashboard

Refresh

Full screen

Edit

Export

Clone

Delete

Device enrollment

OK

No Intune enrollment failures last 7 days

Device compliance

2

devices not in compliance

Device configuration

OK

No policies with error or conflict

Client apps

OK

No installation failures

Details

Welcome to the Microsoft Intune admin center

Microsoft Intune gives you easy access to device and client app management capabilities from the cloud. It enables secure productivity across all of your device types, including Windows, iOS, macOS, and Android. In Microsoft Intune you can:

Enroll and configure your devices

Upload and distribute your apps

Protect your organization's data

Cloud-enable computers enrolled with Configuration Manager

Monitor and troubleshoot your deployments

Tutorials and articles

Learn about Microsoft Intune admin center

Get your device enrolled

Get started with cloud-based mobility management

Intune enrolled devices

LAST UPDATED 1/15/25, 1:07 PM

Platform	Devices
Windows	3
Linux	0
Android	0
iOS/iPadOS	0
macOS	0
Windows Mobile	0
Total	3

Device compliance status

Status	Devices
Compliant	1
In grace period	0
Not evaluated	0
Not compliant	2
Total	3

Please delete this tile

This pinned part on the dashboard refers to a resource type or service that is deprecated. Please remove this part from the dashboard.

<https://intune.microsoft.com>

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

BRKSEC-2416

CISCO

Problem with MAC address MDM Lookup

1 Docking Station / Dongles



2 Wired vs Wireless



3 Random MAC address



Microsoft Intune admin center

Home > Devices | Windows > Windows | Windows devices > EKORNEYC-WIN11

EKORNEYC-WIN11 | Hardware ...

System

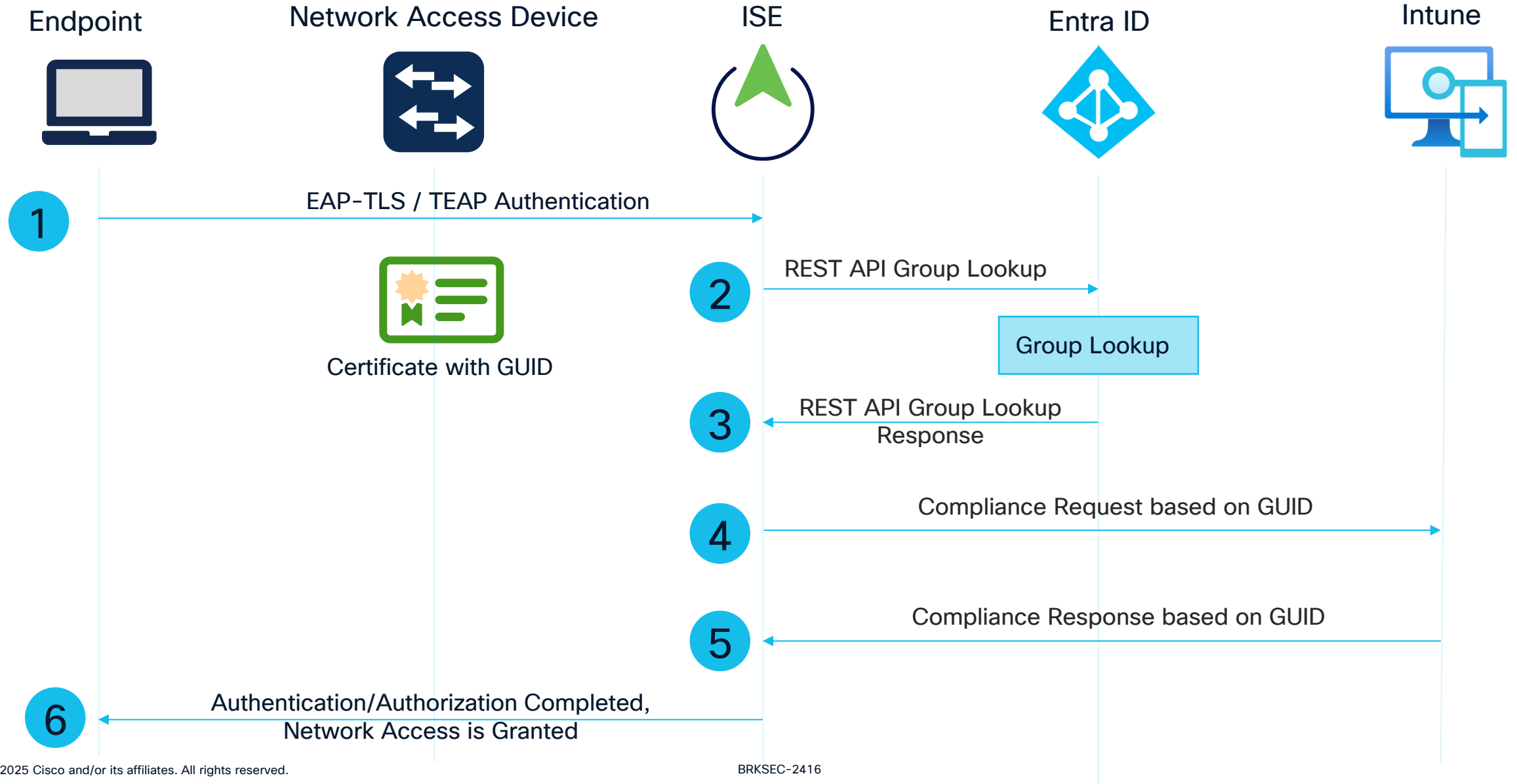
Name	EKORNEYC-WIN11
Management name	alice_Windows_12/20/2023_4:24 PM
Intune Device ID	631405e4-6924-42d7-99b9-9780d26fa7b7
Microsoft Entra Device ID	b69c5040-730d-4ab1-98ef-d36eee53ab4c
Serial number	VMware-42 1c 40 fb 5f 4b e5 38-79 ad 4a de 23 ab 99 d3

Global Unique Identifier (GUID)



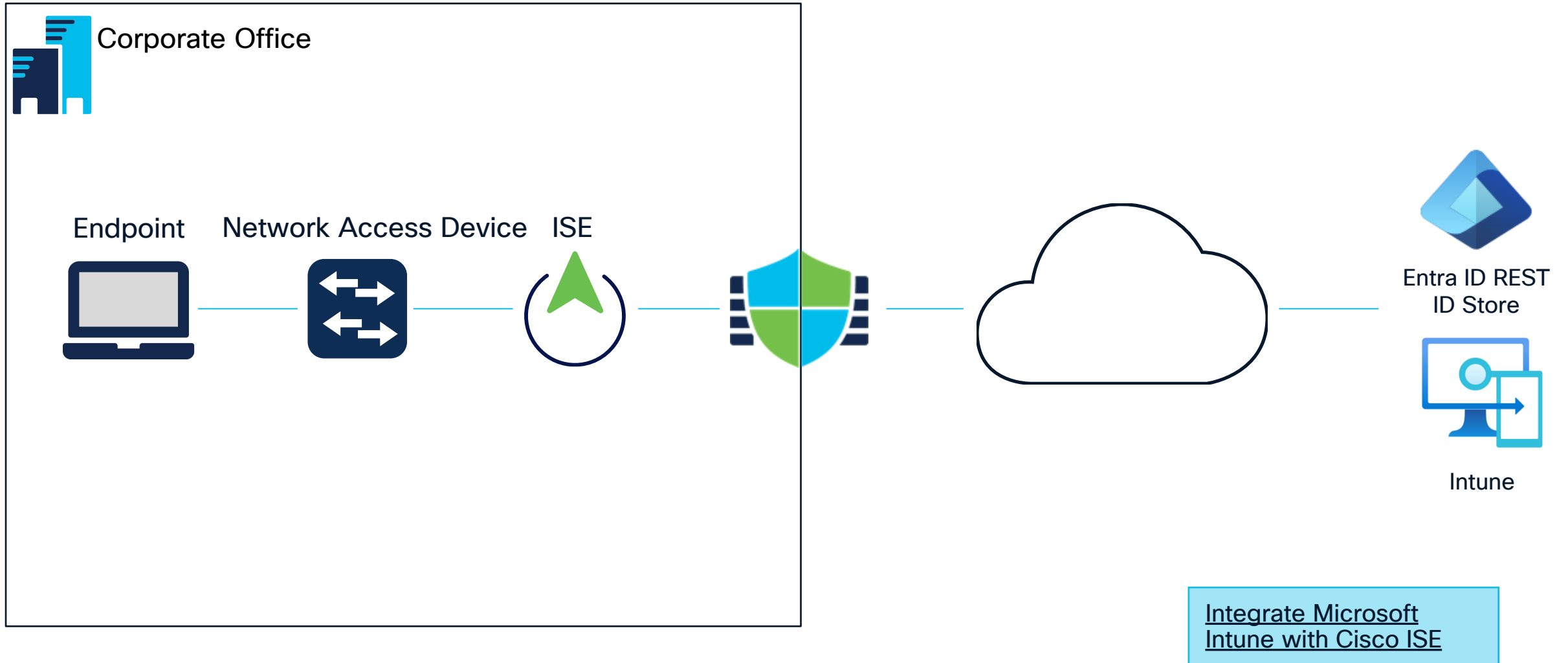
Certificate with GUID

EAP-TLS with Azure Entra ID and Intune MDM



Demo. Intune MDM Integration

Deployment Topology



- 🔖 Bookmarks
- 🏠 Dashboard
- 📊 Context Visibility
- 🔧 Operations
- 🛡 Policy
- 👤 Administration
- 🏢 Work Centers
- ❓ Interactive Help

SummaryEndpointsGuestsVulnerabilityThreat

Manage

<

Total Endpoints ⓘ

136

Active Endpoints ⓘ

4

Rejected Endpoints ⓘ

0

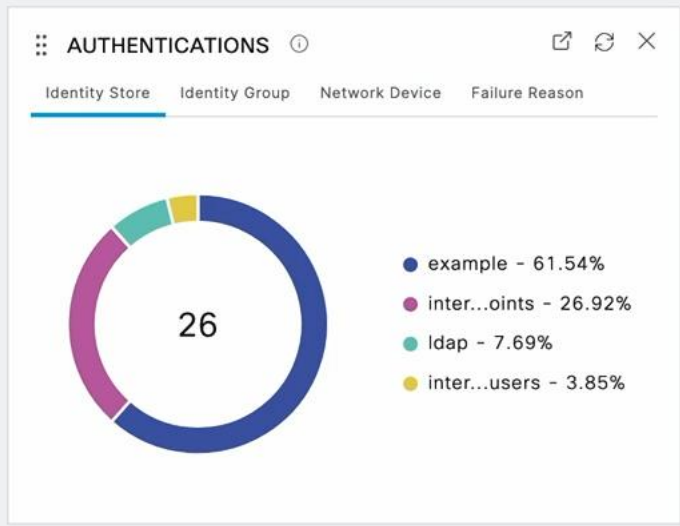
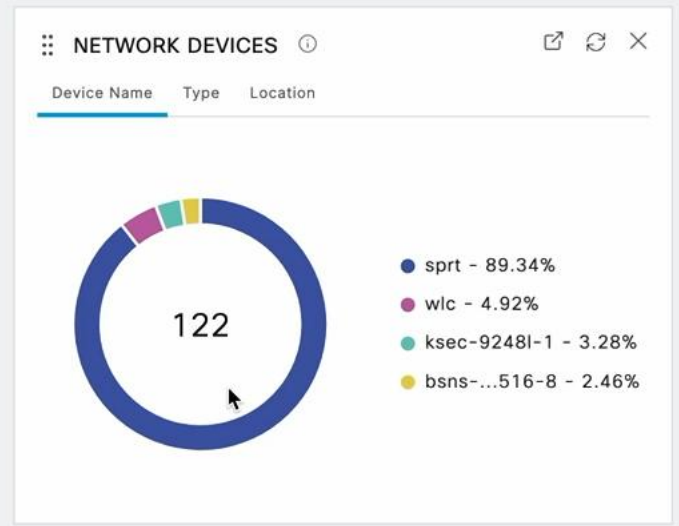
Anomalous Behavior ⓘ

0

Authenticated Guests ⓘ

0

>



BYOD ENDPOINTS ⓘ

TypeProfile

No data available.

ALARMS ⓘ

Severity	Name	Occu...	Last Occurred
ⓘ	Configuration Changed	890	less than 1 min
⚠	ISE Authentication In...	6422	16 mins ago

SYSTEM SUMMARY ⓘ

2 node(s)

ISE34-1ek

📊

ISE Intune Integration Field Notices



[Field Notice: FN74227 - Cisco Identity Services Engine: Authentication and Certificate-Based Logins Will Fail Due to Microsoft Intune Security Identifier Changes - Software Upgrade Recommended](#)

Problem:

As part of Windows update May 10, 2022 ([KB5014754: Certificate-based authentication changes on Windows domain controllers](#)) requires certificates for users or computers to be strongly mapped to Active Directory. To do this Microsoft Intune adds Security Identifiers (SIDs) to Uniform Resource Identifier (URI) of certificate using {{ OnPremisesSecurityIdentifier }} variable.

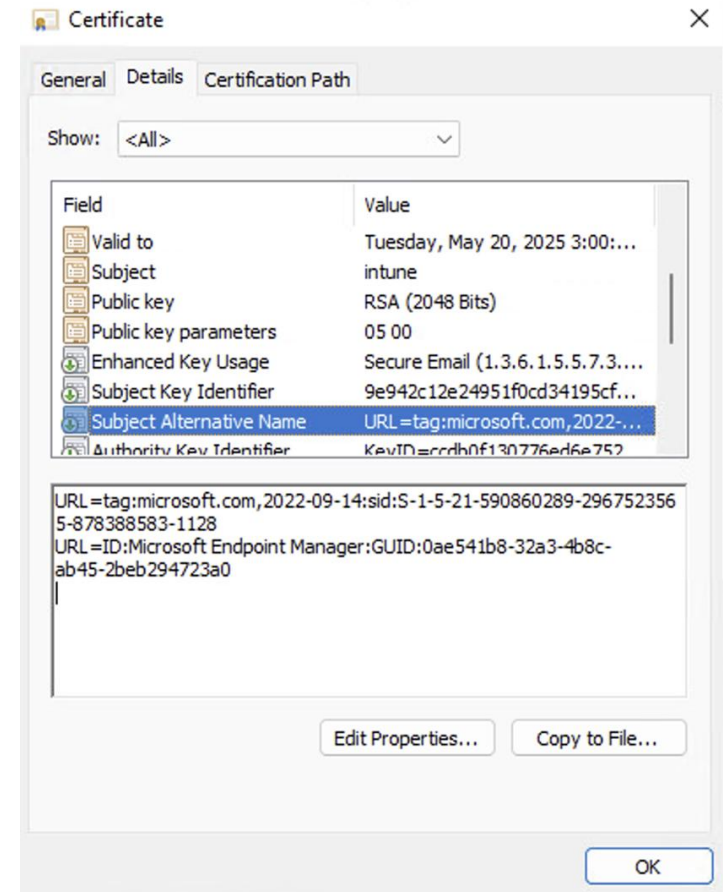
Known Fixed Releases:

ISE 3.1 patch 10

ISE 3.2 patch 7

ISE 3.3 patch 4

ISE 3.4 patch 1



Intune Integration Troubleshooting



Administration / Network Resources

Error

Connection to server failed with:

MDM Server API error
Connection Failed to the MDM server: There is a problem with the server
Certificates or ISE trust store.

Please try with different settings.

OK

ISE34-1ek_GigabitEthernet.pcap						
tls.handshake.type == 1						
No.	Time	Source	Destination	Protocol	Lengt	Info
14	0.376116	10.48.26.64	10.48.26.63	TLSv1.2	391	Client Hello (SNI=ISE34-2ek.example.com)
19	0.378627	10.48.26.64	10.48.26.63	TLSv1.2	391	Client Hello (SNI=ISE34-2ek.example.com)
30	0.392936	10.48.26.63	10.48.26.64	TLSv1.2	391	Client Hello (SNI=ISE34-1ek.example.com)
255	7.372347	10.48.26.64	10.48.26.63	TLSv1.2	354	Client Hello (SNI=ISE34-2ek.example.com)
278	7.943812	10.48.26.64	64.103.36.133	TLSv1.2	322	Client Hello (SNI=www.ciscoconnectdna.com)
588	19.959208	10.48.26.63	10.48.26.64	TLSv1.2	357	Client Hello (SNI=ISE34-1ek.example.com)
649	22.814347	10.48.26.64	10.48.26.63	TLSv1.2	354	Client Hello (SNI=ISE34-2ek.example.com)
686	24.302912	10.48.26.64	64.103.36.133	TLSv1.2	417	Client Hello (SNI=login.microsoftonline.com)
723	24.573553	10.48.26.64	64.103.36.133	TLSv1.2	411	Client Hello (SNI=graph.microsoft.com)
819	25.032051	10.48.26.64	64.103.36.133	TLSv1.2	417	Client Hello (SNI=login.microsoftonline.com)
867	25.580248	10.48.26.64	64.103.36.133	TLSv1.2	393	Client Hello (SNI=fef.msua08.manage.microsoft.com)

1

Wireshark filter: tls.handshake.type == 1, to filter Client Hello messages

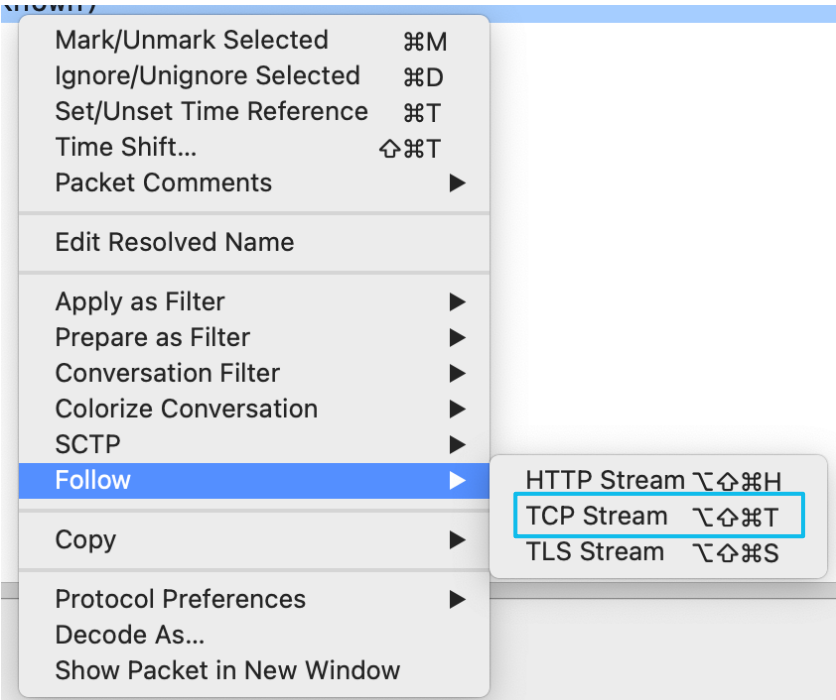
ISE34-1ek_GigabitEthernet.pcap						
tls.alert_message.desc == 46						
No.	Time	Source	Destination	Protocol	Lengt	Info
872	25.673463	10.48.26.64	64.103.36.133	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)

2

Wireshark filter: tls.alert_message.desc == 46, to filter Certificate Unknown TLS Alerts

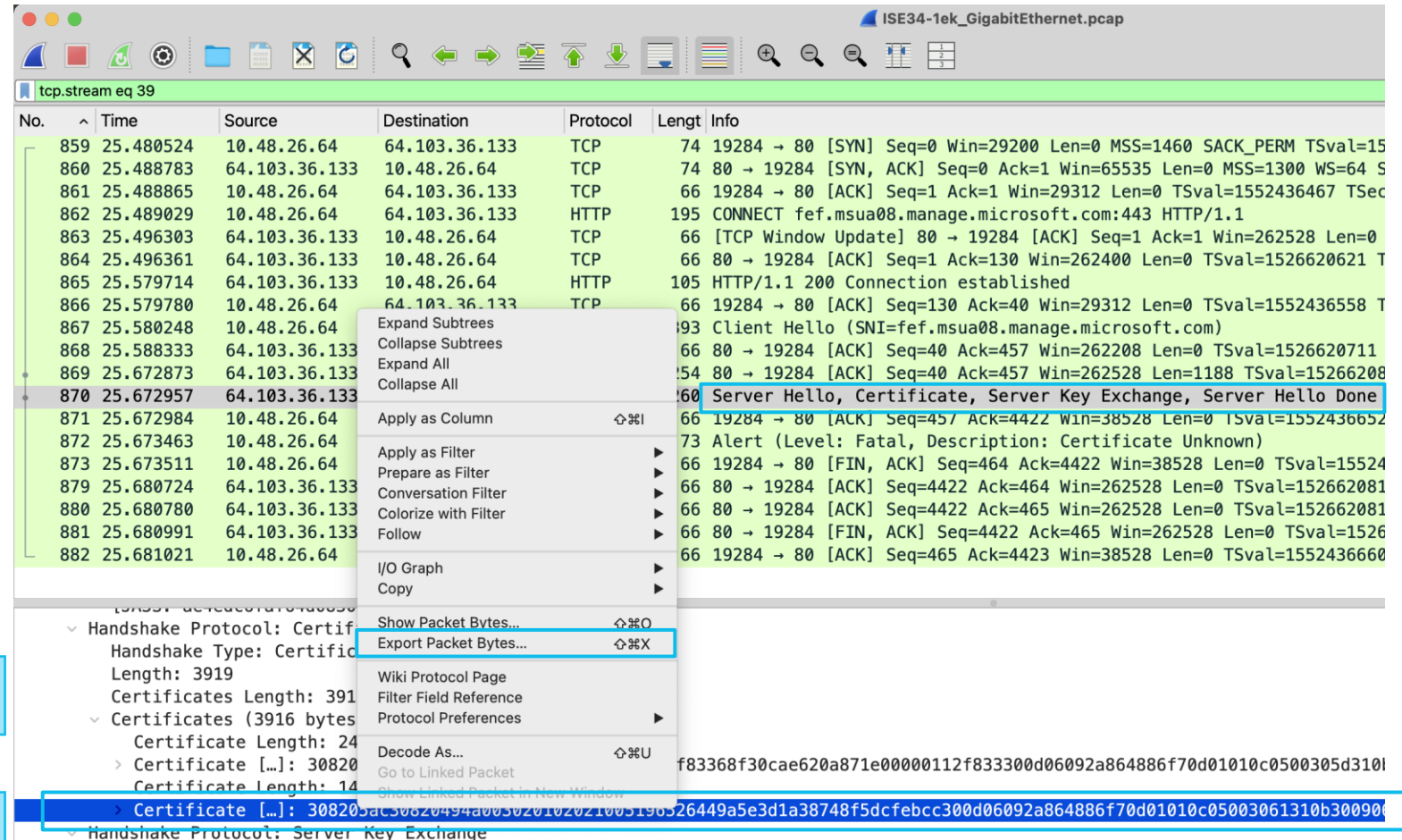


Intune Integration Troubleshooting



3 Wireshark: Right Click > Follow > TCP Stream

5 Import Certificate into ISE Trusted Store
Administration > System > Certificates > Trusted Certificates > Import



4

- Locate Server Hello, Certificate message
- Locate Certificates under Packet Details
- Right Click > Export Packet Bytes

Conclusion

Key Takeaways

- ISE can be deployed natively on Azure as Virtual Machine or Application, installation and configuration can be automated with IaC tools like Terraform and Ansible
- SAML SSO is available on ISE for Portals (Admin, Guest, Sponsor, etc.)
- 802.1X authentications, RA VPN authentications, Device Administration with TACACS+ are possible with Entra ID as an External Identity Store
- ISE MDM integration allows more granular network access based on the Compliance Status

Complete Your Session Evaluations



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



Earn 800 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco Stand for related demos



Book your one-on-one Meet the Expert meeting



Attend the interactive education with Capture the Flag, and Walk-in Labs



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

Contact me at: ekorneyc@cisco.com

Thank you

CISCO Live !

