Cisco ISE Meets Azure Cloud

Deploy, Automate, Integrate with Entra ID and Intune

Eugene Korneychuk - Security Technical Leader

BRKSEC-2416

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

Webex App

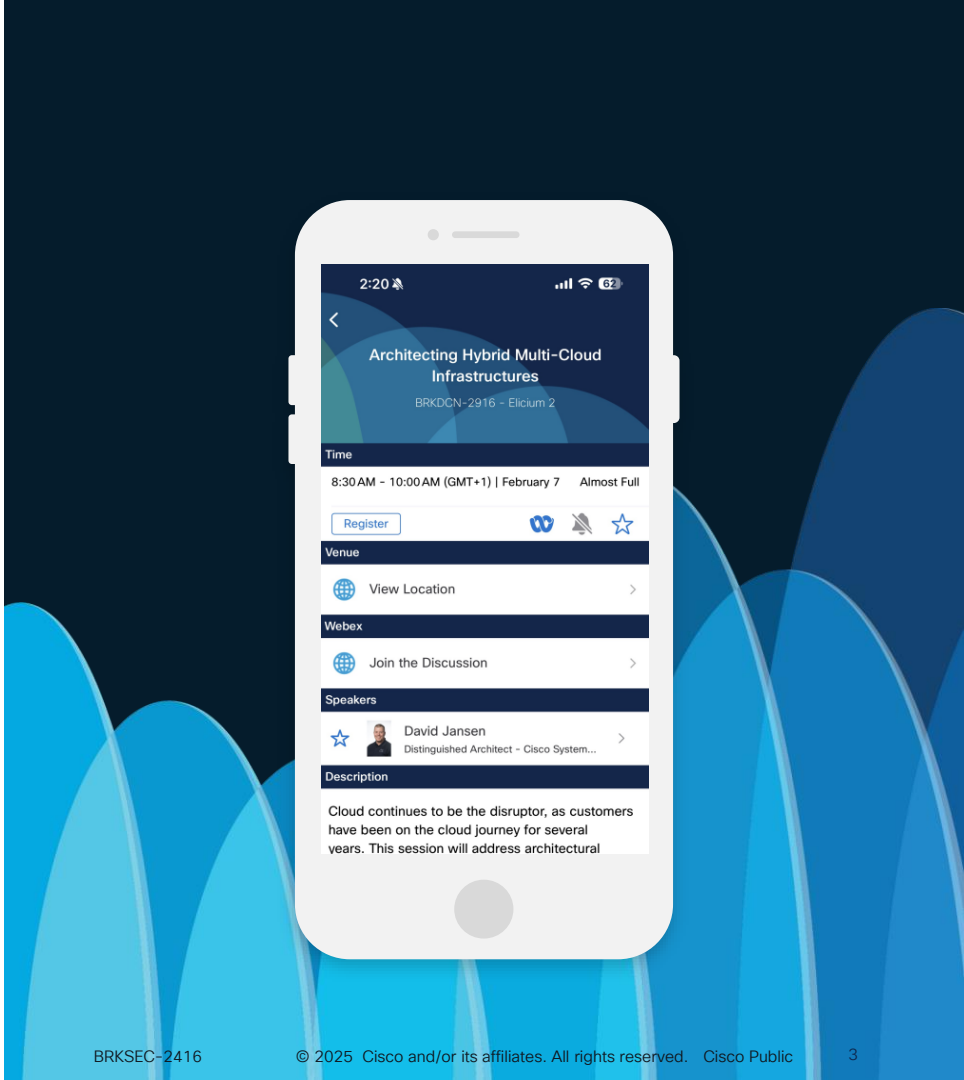
Questions?

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

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

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



Session Objective

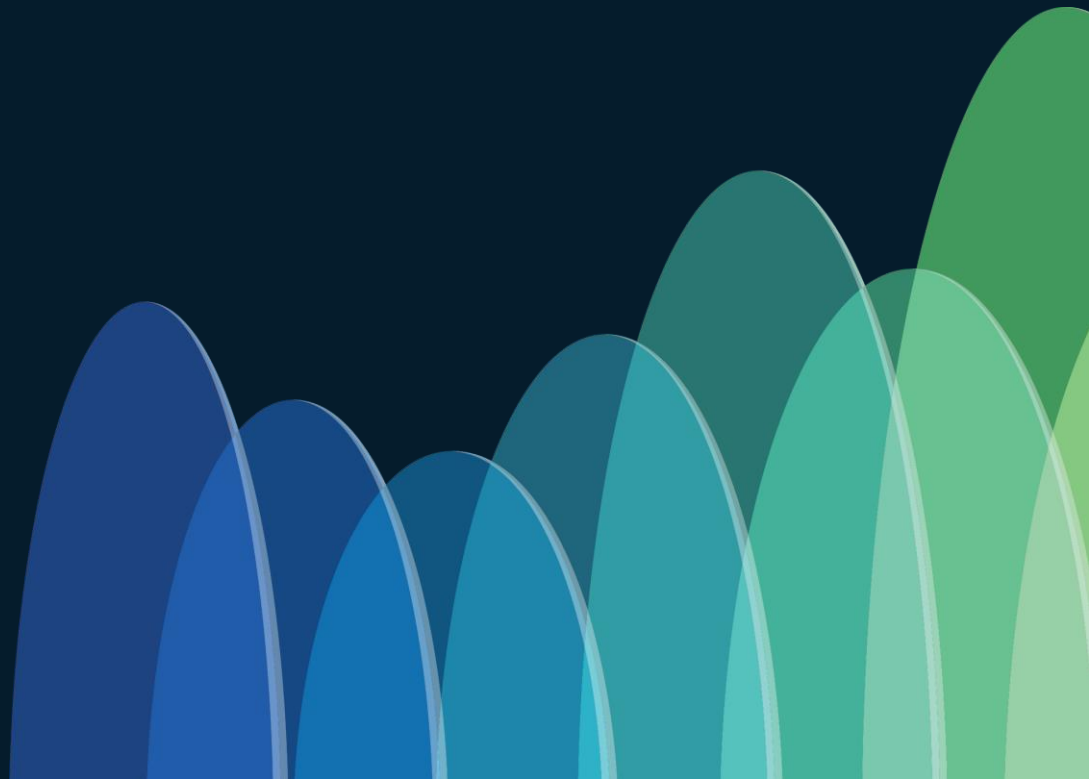
The Goal of this session is to:

- 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

Agenda

- ISE Architecture Concepts
- ISE in Azure Cloud
- ISE SAML SSO
- Entra ID Authentications
- Intune Integration
- Conclusion

ISE Architecture Concepts



cisco Live!

ISE Design Concepts

Policy Administration Node (PAN)
- Single plane of glass for ISE admin
- Owns ISE database and replicates it to other nodes

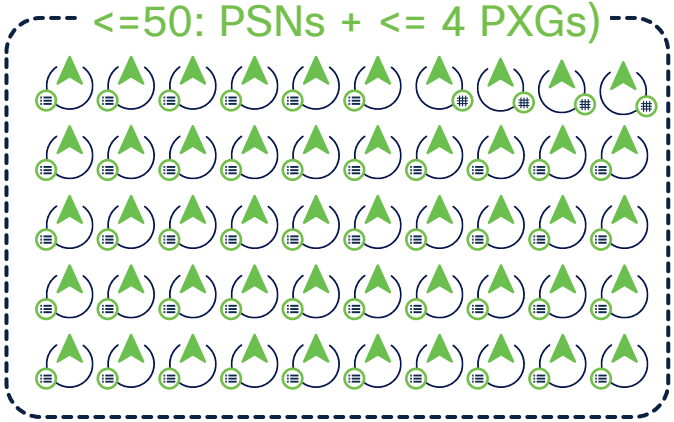
Monitoring & Troubleshooting Node (MnT)
- Reporting and logging node
- Collects health and log information from other nodes

Policy Services Node (PSN)
- Makes policy decisions
- RADIUS / TACACS+ Servers

pxGrid Controller
- Facilitates sharing of context

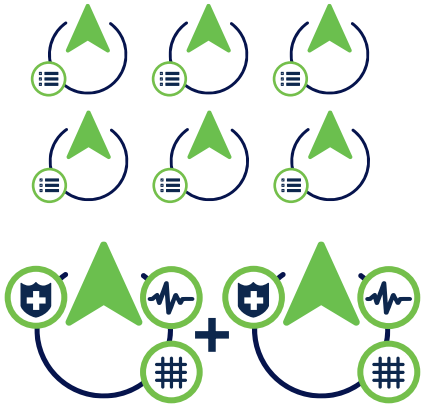
ISE Scaling

Lab and Evaluation



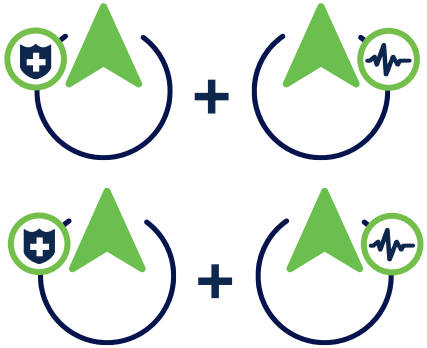
Small HA Deployment

2 x (PAN+MNT+PSN)+ Extra PSN



Medium Multi-node Deployment

2 x (PAN+MNT+PXG), <= 6 PSN



Large Deployment

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

Total Maximum Concurrent Active Sessions

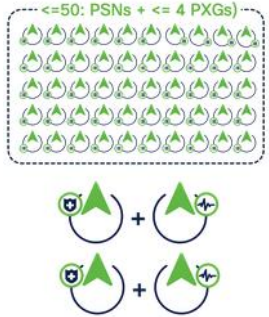
Cisco ISE

Deployment Type	SNS 3615	SNS 3715	SNS 3595	SNS 3655	SNS 3755	SNS 3695	SNS 3795
Large deployment	Unsupported	Unsupported	500,000	500,000	750,000	2,000,000	2,000,000
Medium deployment	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

Large Deployment



cisco Live!

PSN Maximum Concurrent Active Sessions

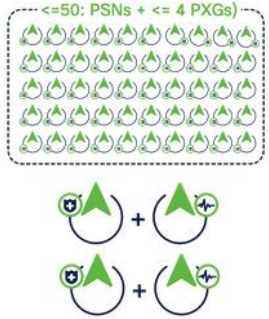
Cisco ISE

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

Small Deployment

Medium Deployment

Large Deployment

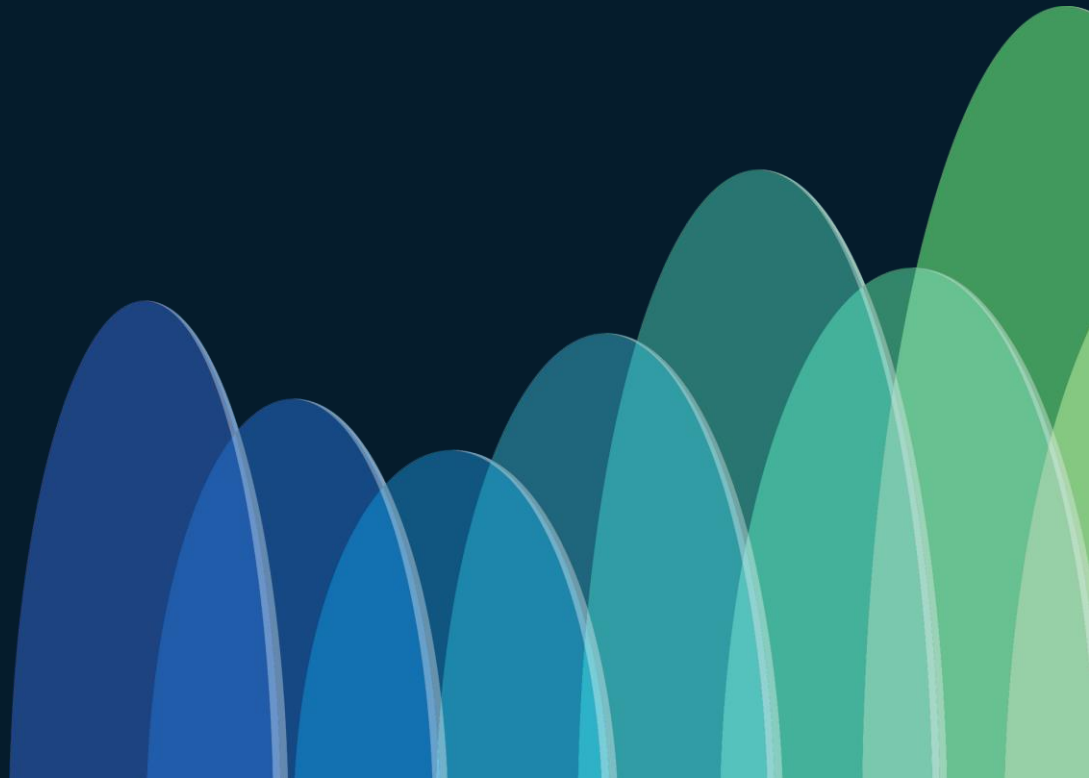


Cisco Cloud Platforms Sizing

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
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)

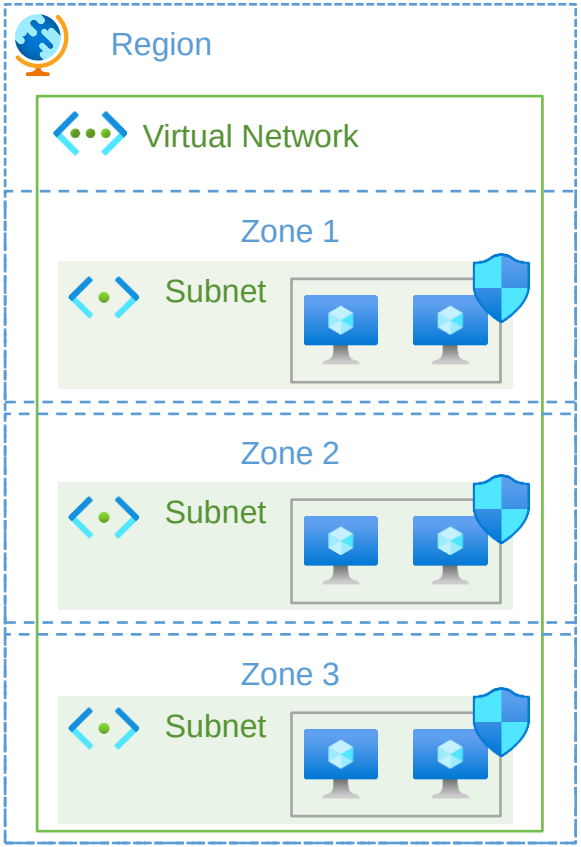
* This instance is compute-optimized and provides better performance compared to the general purpose instances.
** In OCI, you choose CPU in terms of Oracle CPU (OCPU). Each OCPU equals two hardware execution threads known as vCPUs.

ISE in Azure Cloud



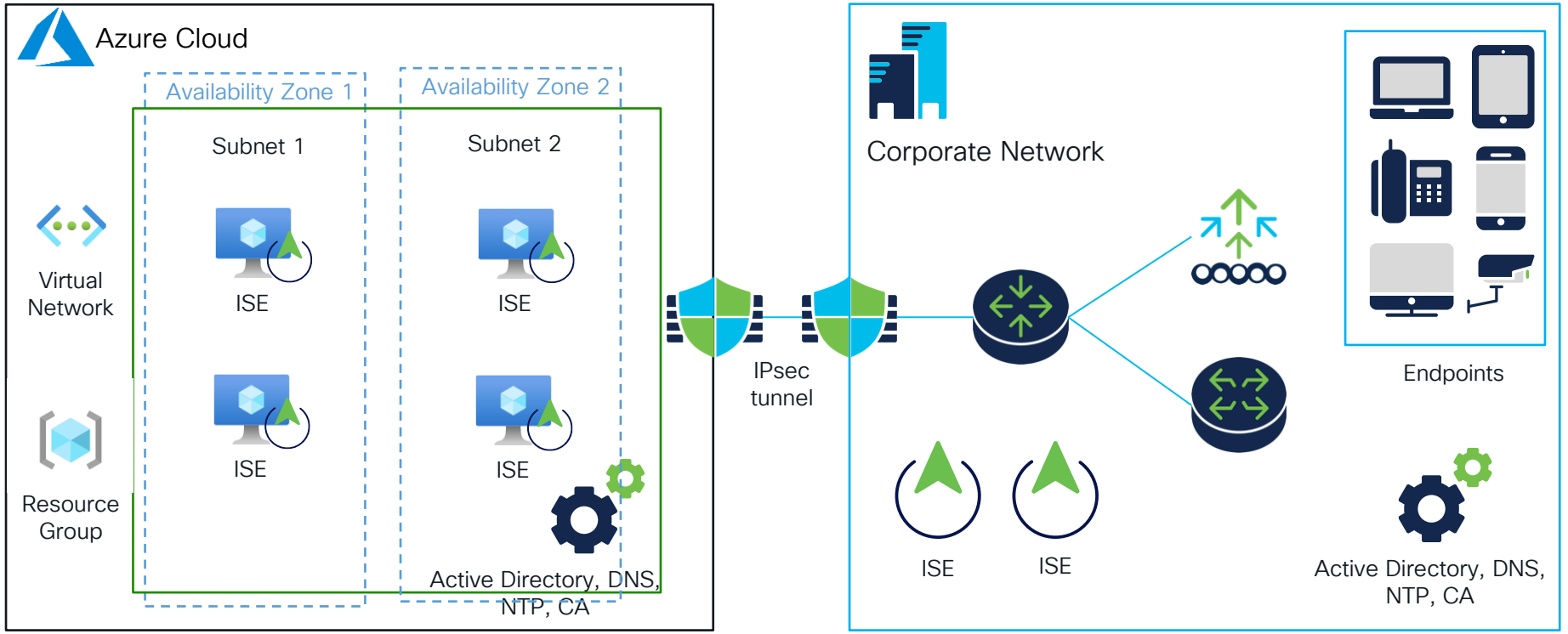
cisco Live!

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 and Solution:

There is a bug in the Azure fragmentation reassembly code. While Microsoft plans to address this issue, a temporary solution has been proposed for Cisco ISE customers utilizing Azure instances.

To implement the short-term fix, ISE customers are advised to raise an Azure support ticket. Microsoft has committed to:

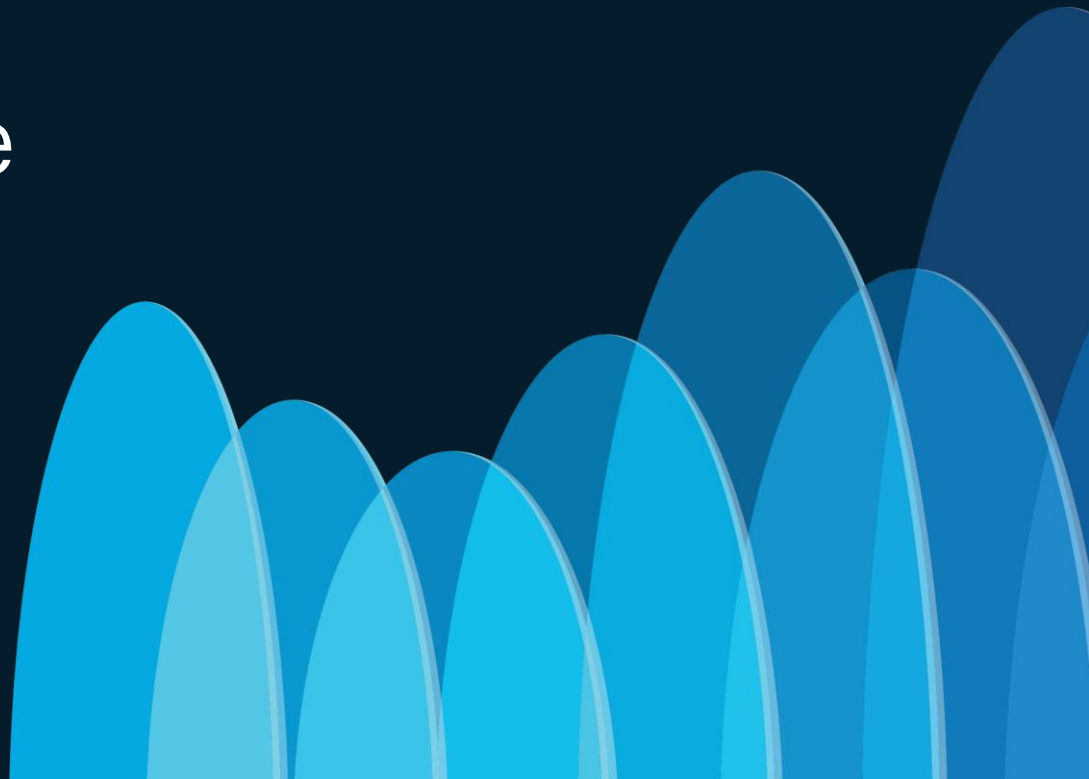
1. Pinning the subscription to ensure that all instances within that subscription are deployed on Gen7 hardware.

2. Allowing out-of-order fragments to pass to the destination instead of being dropped.

Latest Update:

Regions where Azure Cloud has already implemented the fixes: **East Asia** (eastasia) and **West Central US** (westcentralus)

Demo. ISE Azure Application Deployment



cisco Live!

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

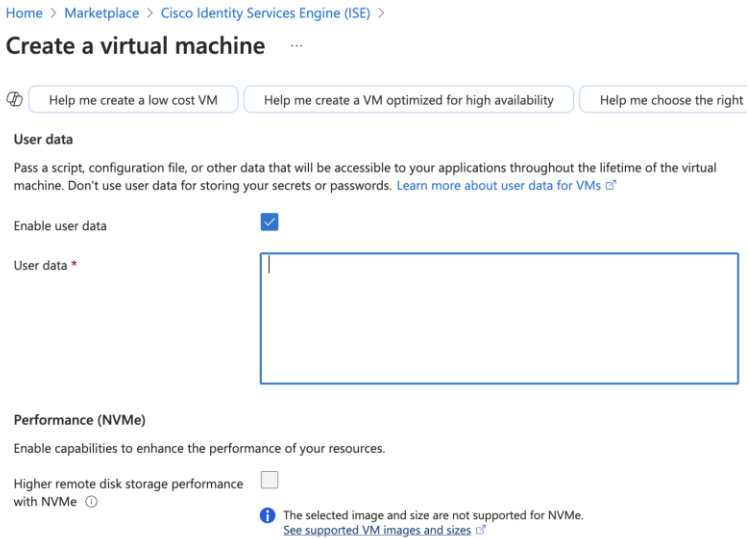
Resources

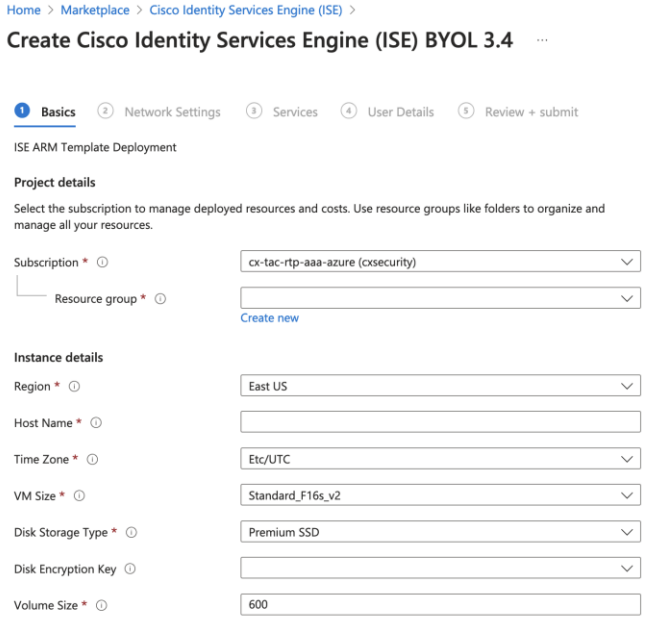
Recent | Favorite

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

Create ISE Instance using Azure Virtual Machine / Application





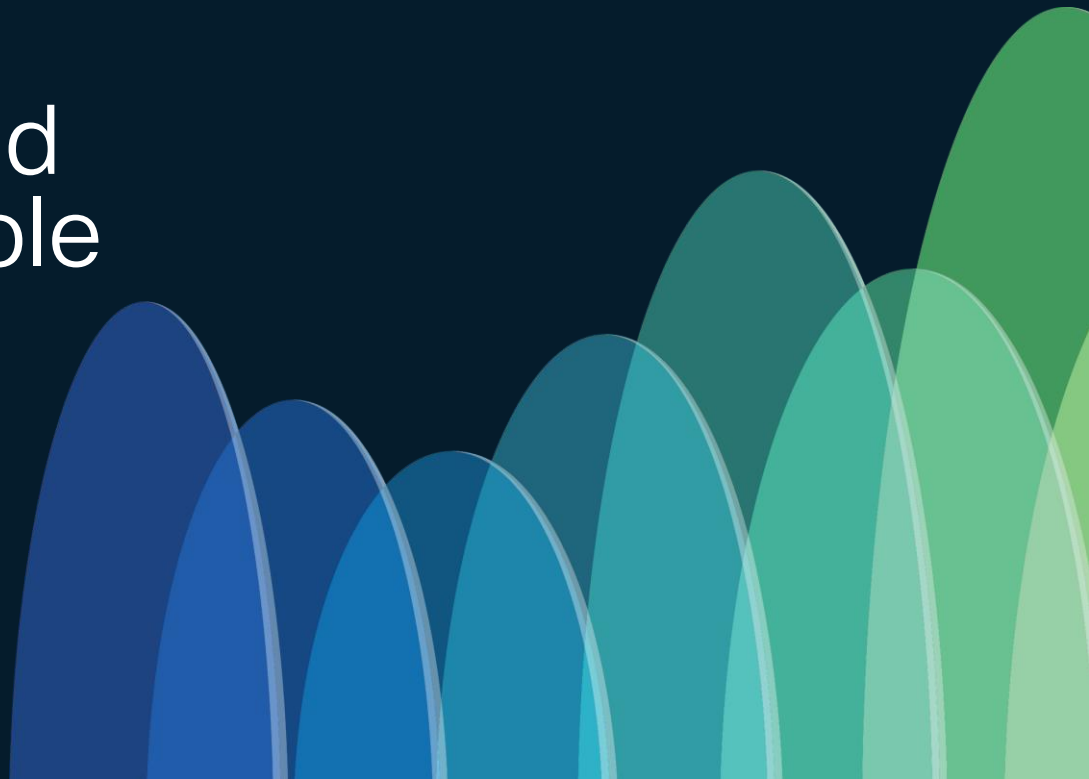
ISE as Azure Virtual Machine

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

ISE as Azure Application

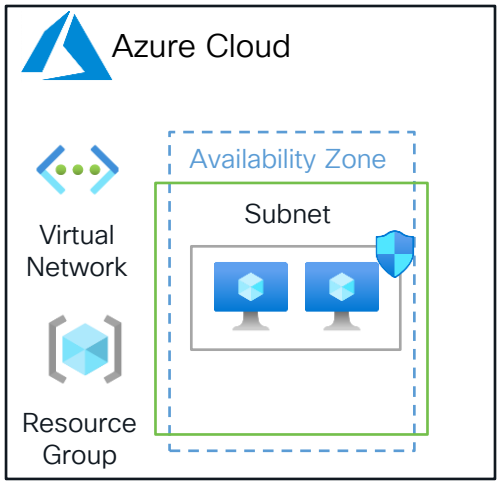
- ARM Template helps to setup ISE with menu prompts

What if you would like to install whole infrastructure?



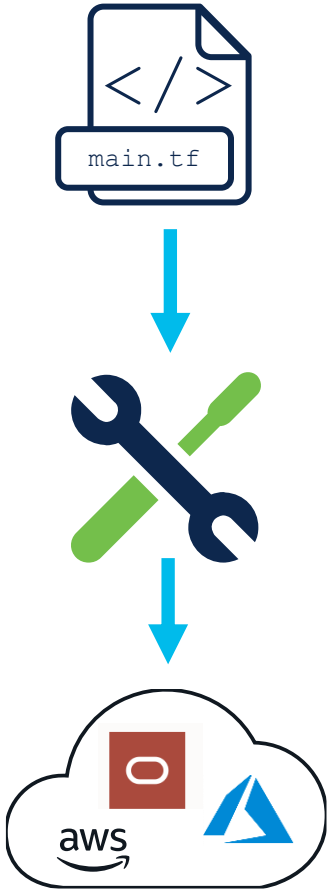
Terraform

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

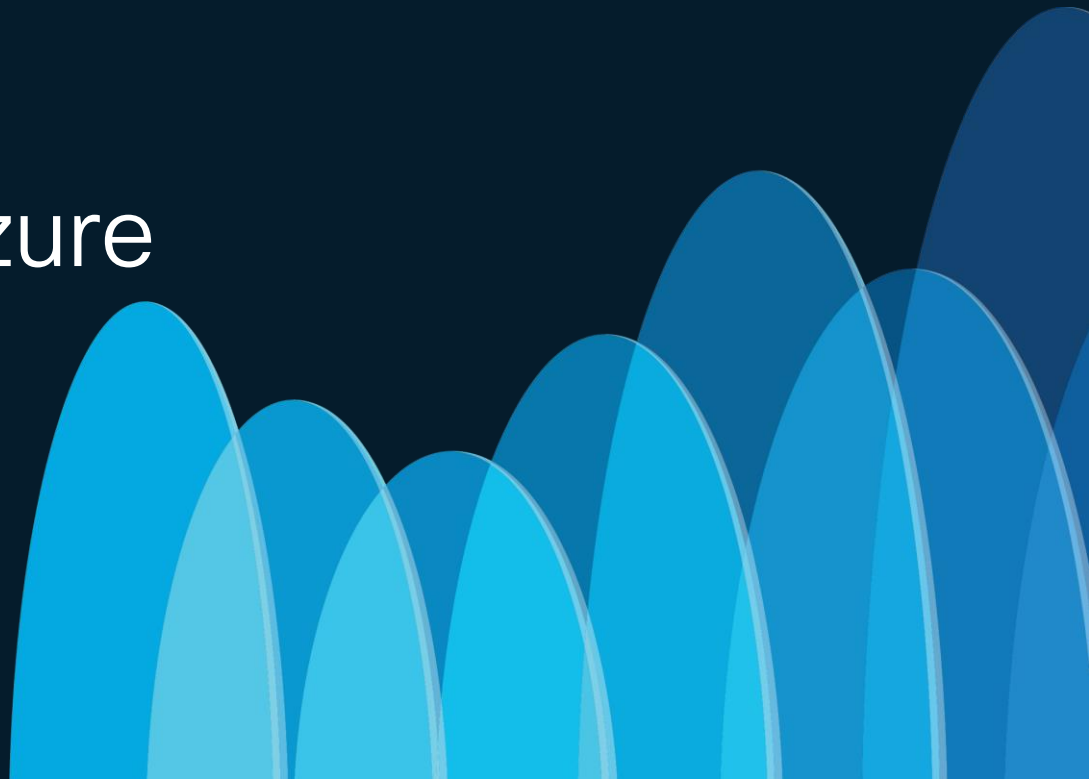


- Create Network Interface
- Create Network Security Group
- Create Virtual Machine
- Create Resource Group

- 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

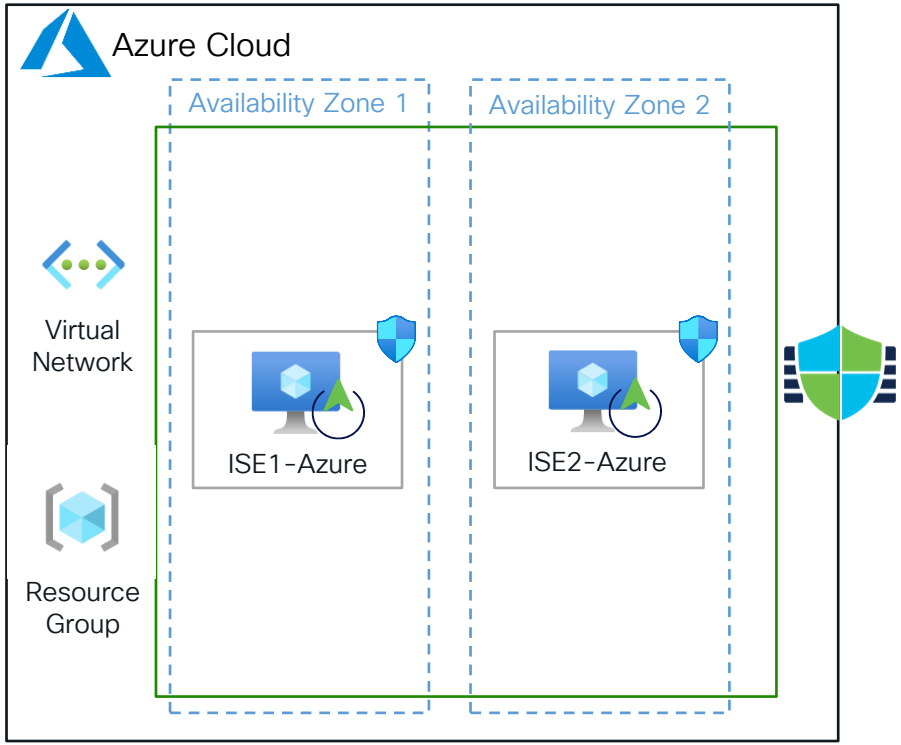


Demo. ISE installation on Azure using Terraform



cisco Live!

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="OSProvis
ioningTimedOut" 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 o
f 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="OSProvis
ioningTimedOut" 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 o
f 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" {


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

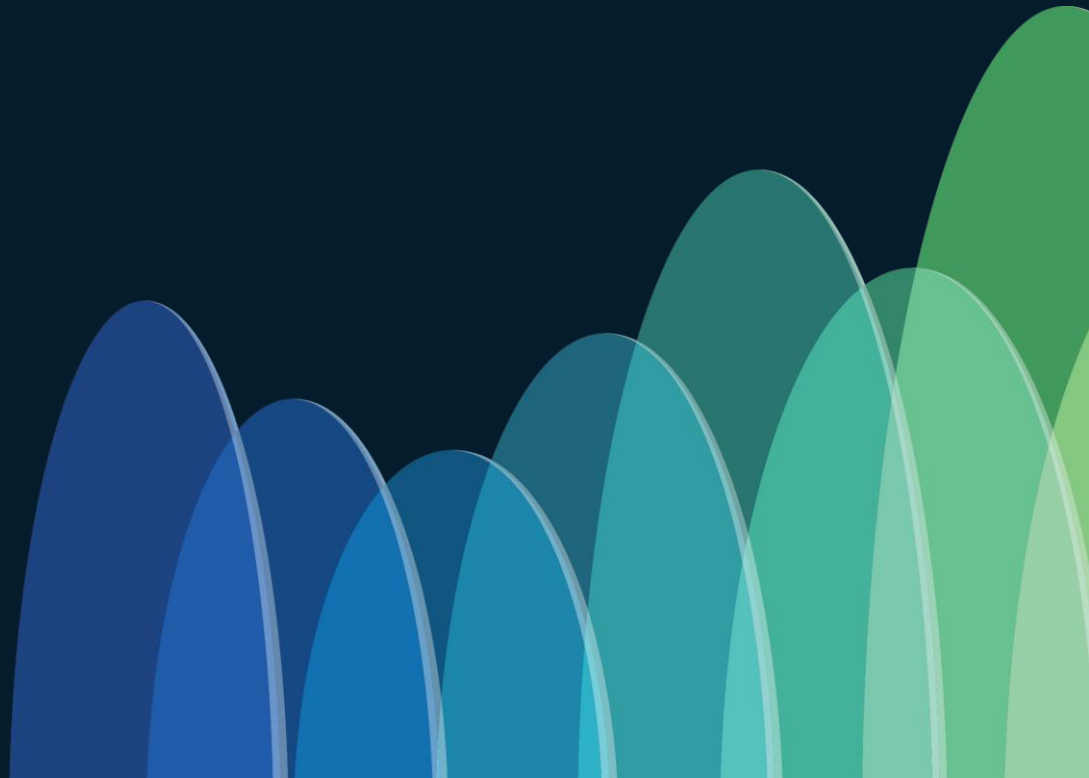
ISE1-Azure | Serial console

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:
```

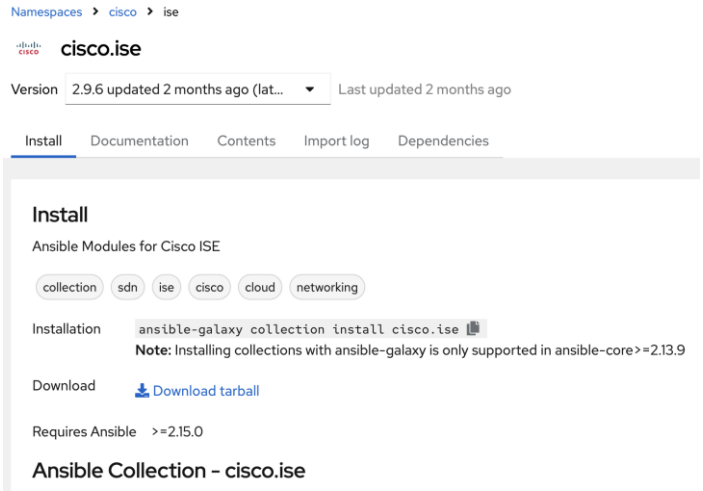
That’s not it, you need to configure things...



Ansible

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

galaxy.ansible.com



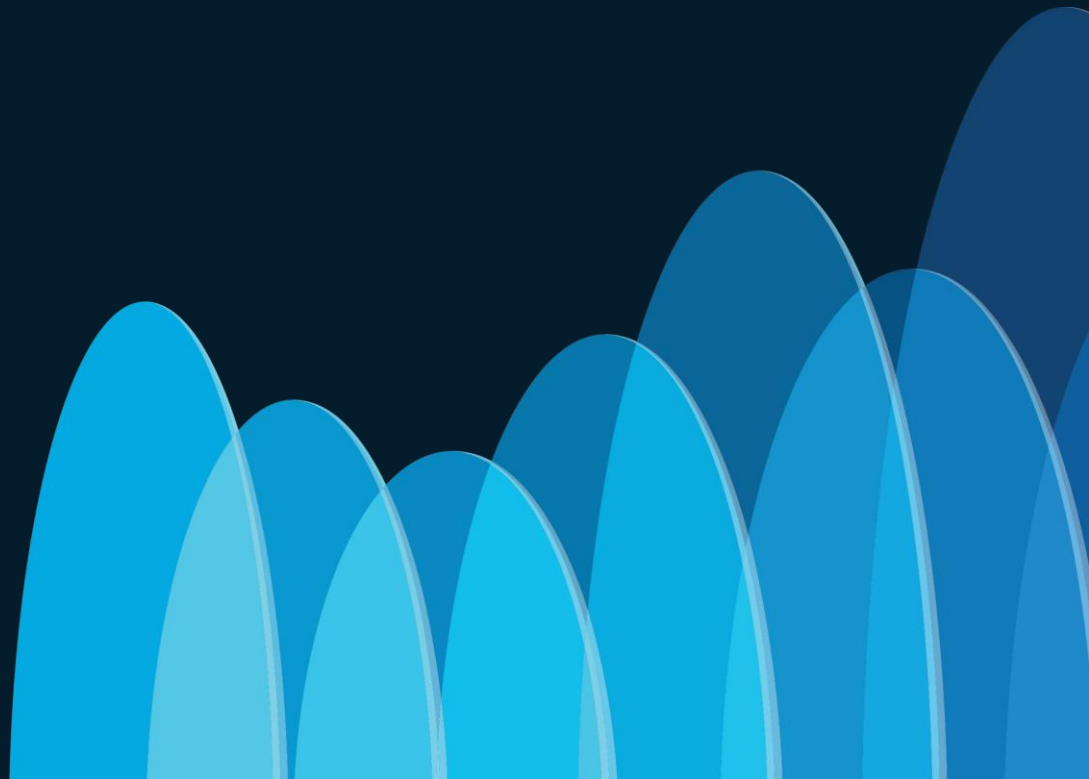
Play (set of tasks)

Task

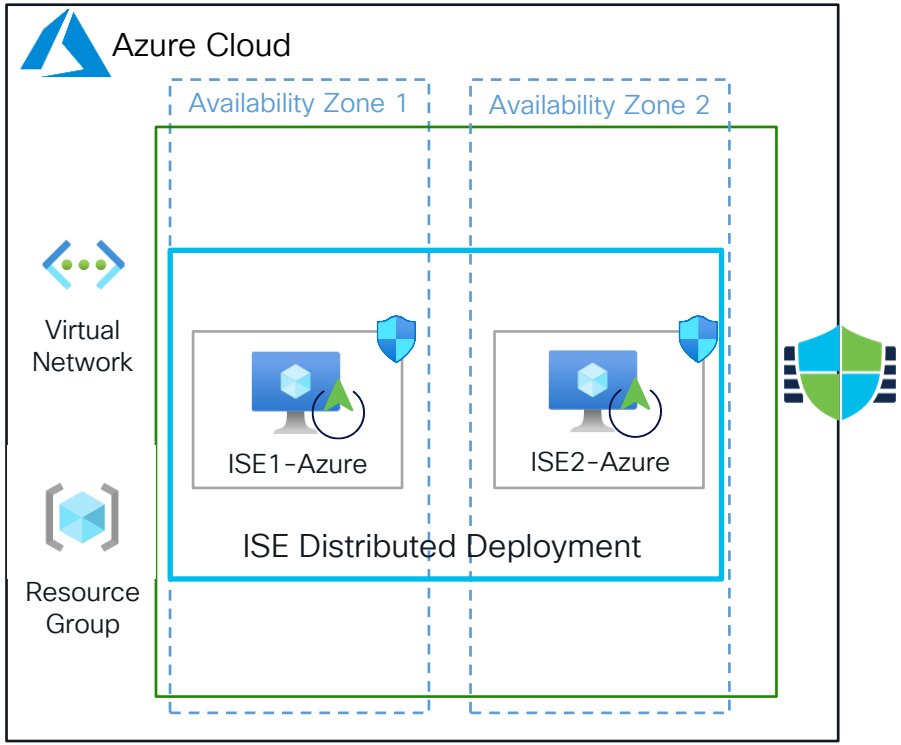
```yaml
- hosts: ise_servers
  vars_files:
    - credentials_emea.yml
  gather_facts: no
  tasks:

  - 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

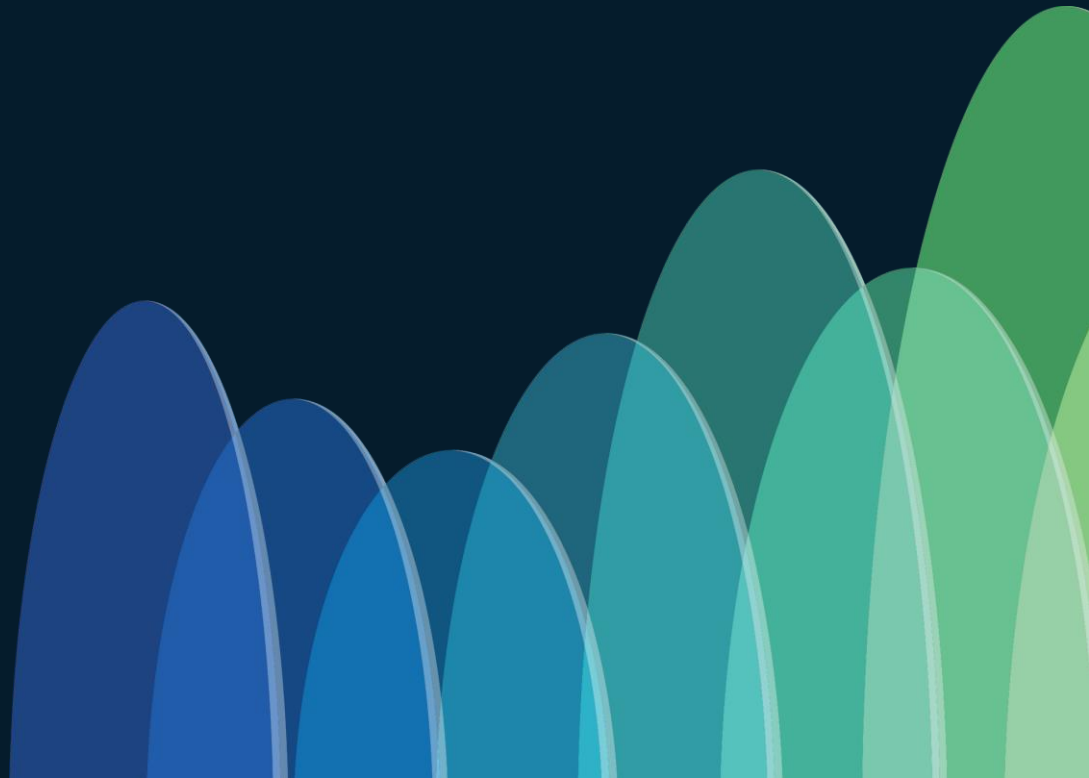
```
(CL) ekorneyc@EKORNEYC-M-CW9R Ansible % ansible-playbook -i hosts cl-ise-playbook.yaml
```

ISE in the Cloud. Licensing

Cisco ISE leverages the Bring Your Own License (BYOL)

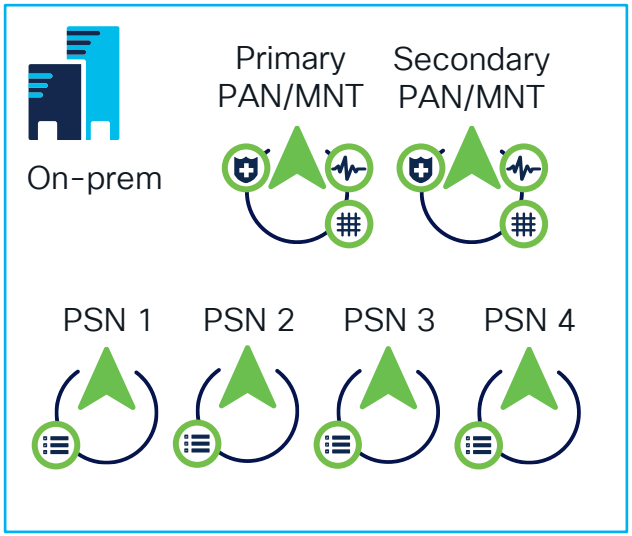
- ISE Comes with 90-days Evaluation License
- Use the Common VM License to enable Cisco ISE on cloud platforms, in addition to the other Cisco ISE licenses that you need for the Cisco ISE features you want to use.

Migration and Upgrades



cisco Live!

Migration



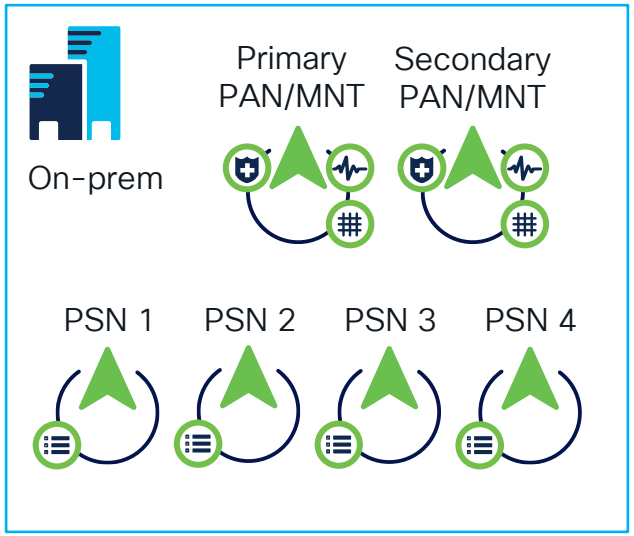
Scenario: ISE 3.3 patch 4 Medium Deployment Migration to Cloud Infrastructure

--- === 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

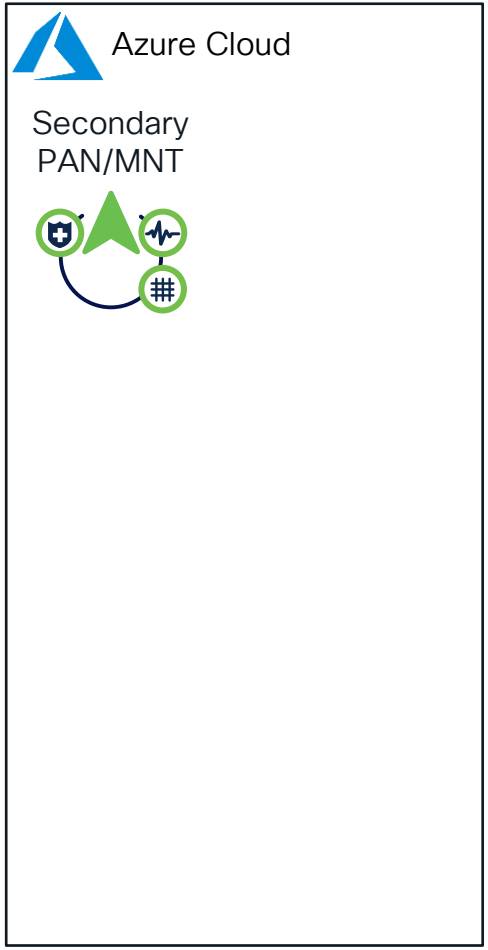
Azure Cloud

Migration



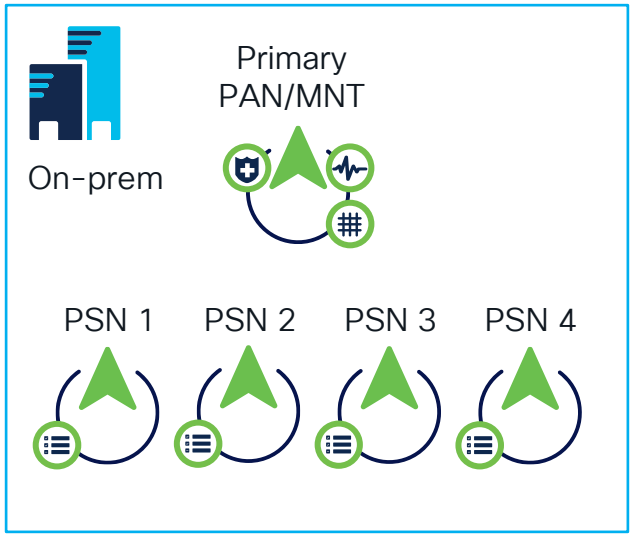
--- === Phase 1 === ---

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



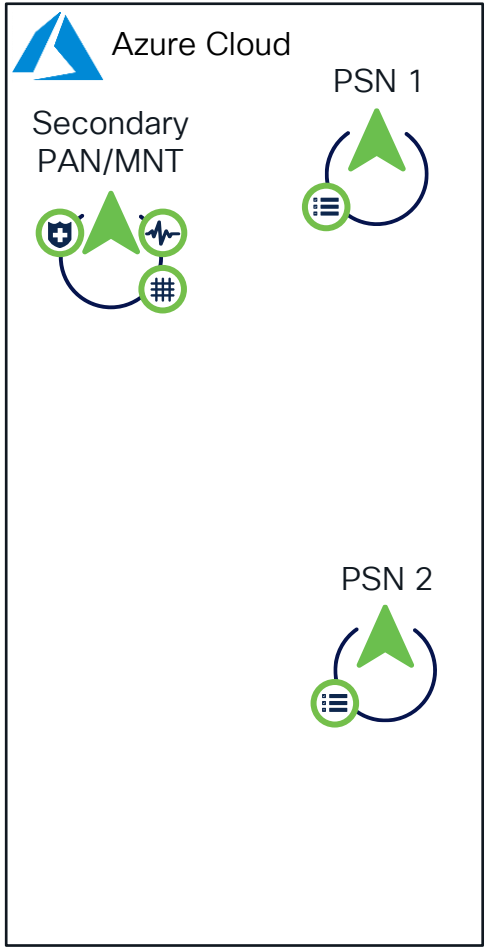
Considerations:
- (Optional) Certificates to be exported prior Deregistration of Secondary PAN, imported before adding Node to the Deployment

Migration



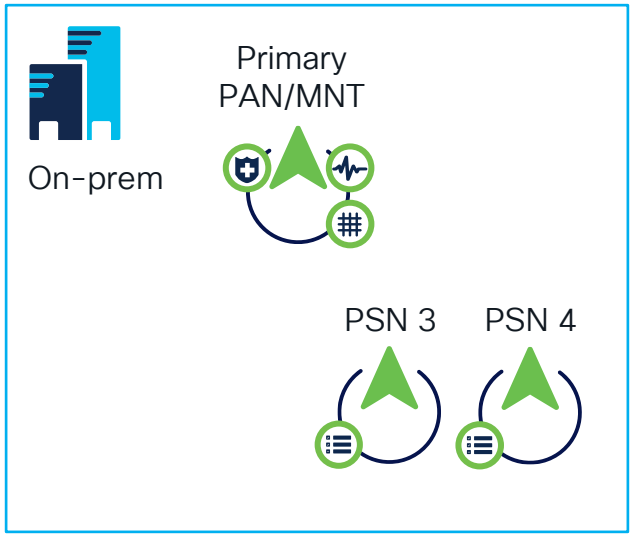
--- === Phase 2 === ---

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



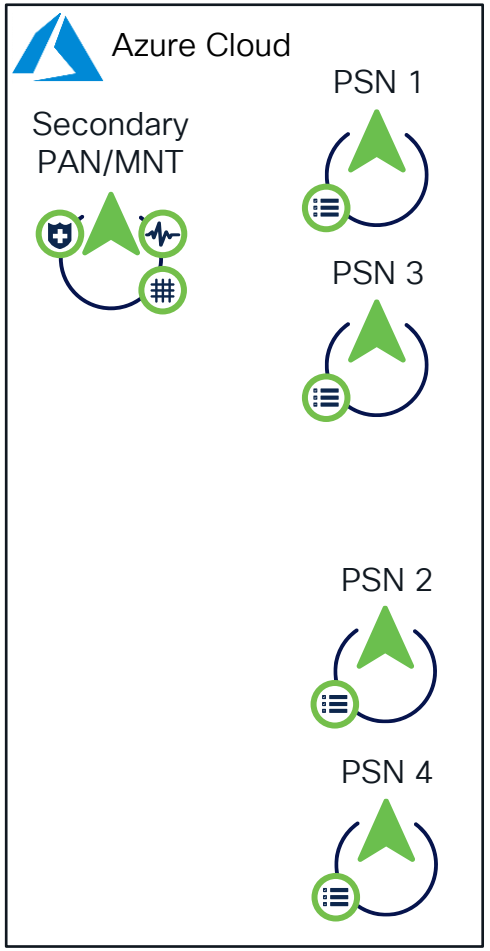
Considerations:
- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 2. Exclude PSN1 and PSN2 from LB Groups or ensure that high availability configuration includes PSN3 and PSN4

Migration



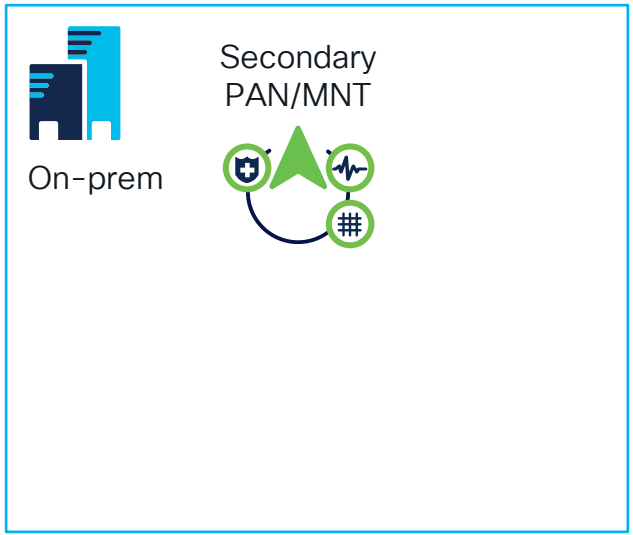
--- === Phase 3 === ---

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



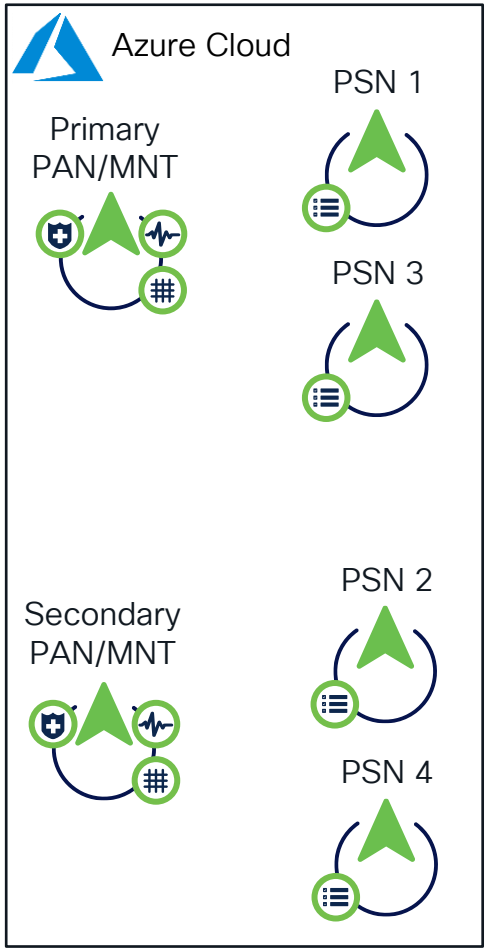
Considerations:
- (Optional) Certificates to be exported prior Deregistration, imported before adding Nodes to the Deployment
- NAD's configuration should be evaluated prior to Phase 3. Exclude PSN3 and PSN4 from LB Groups or ensure that high availability configuration includes PSN1 and PSN2

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



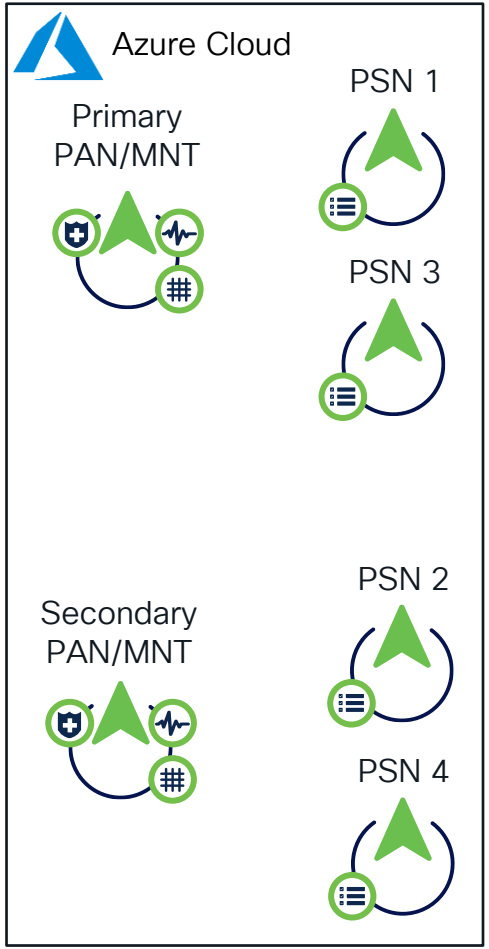
Considerations:
- (Optional) Certificates to be exported prior Removal of PAN, imported before adding Node to the Deployment

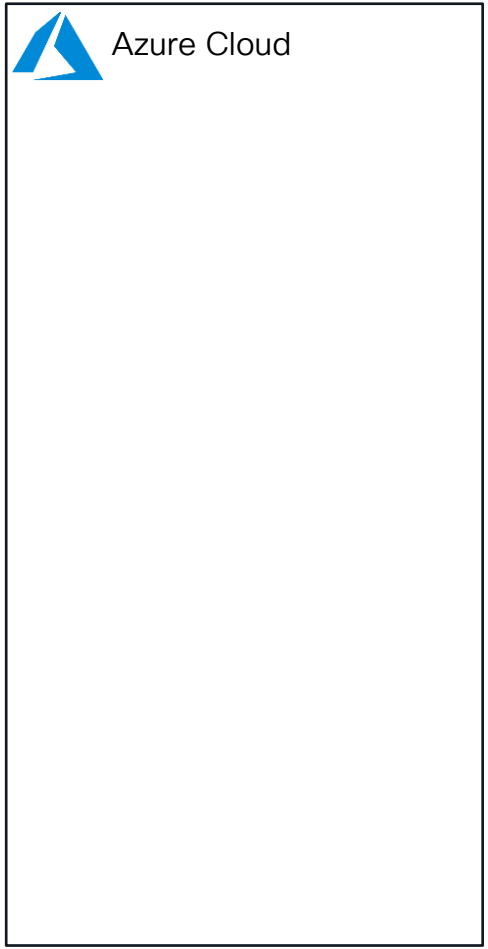
Upgrade

--- === 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



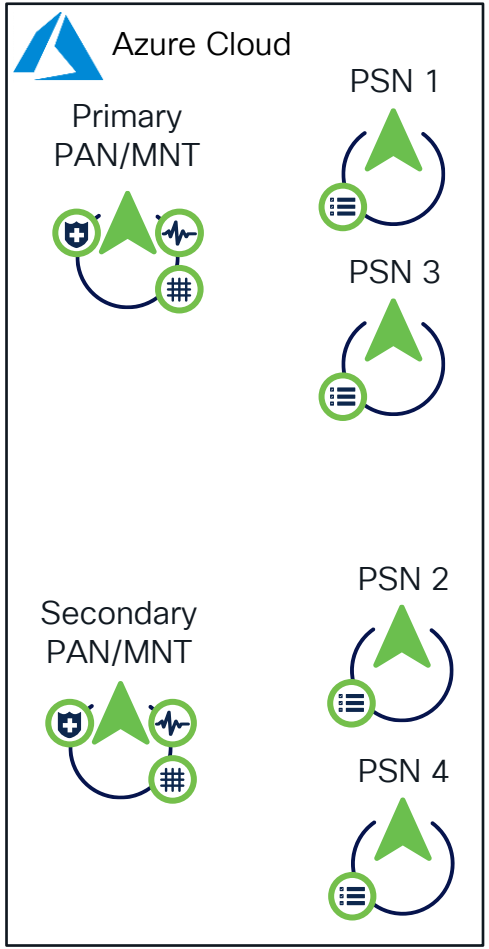


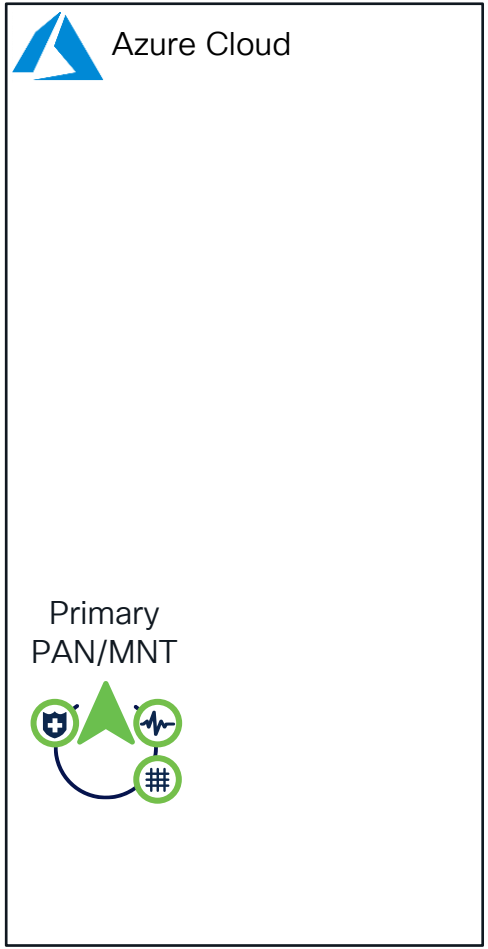
Upgrade

--- === 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



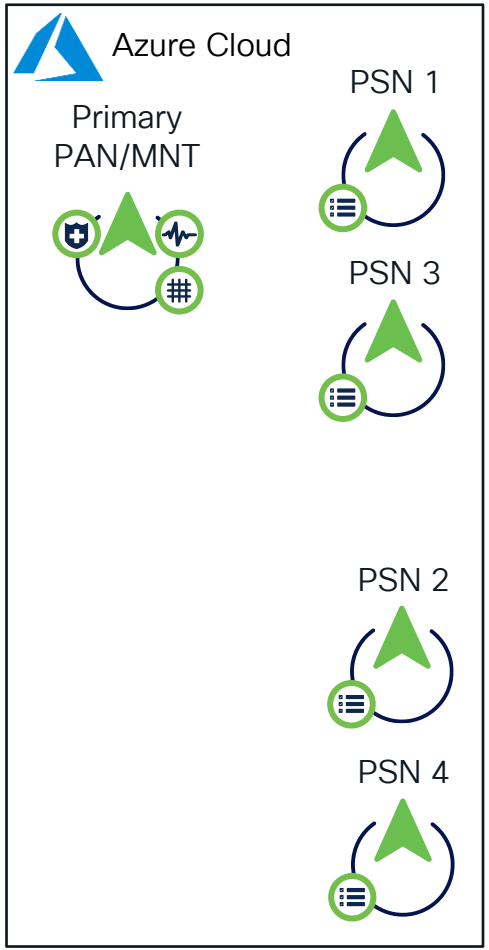


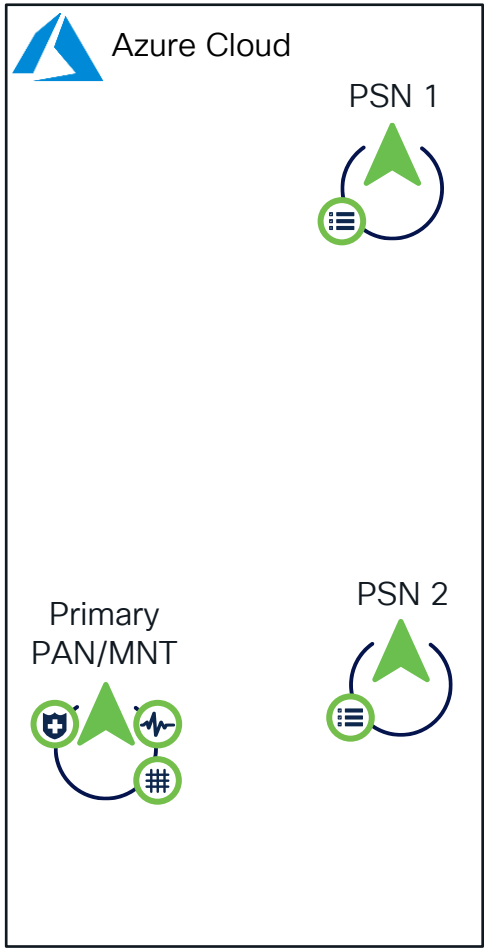
Upgrade

--- === 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



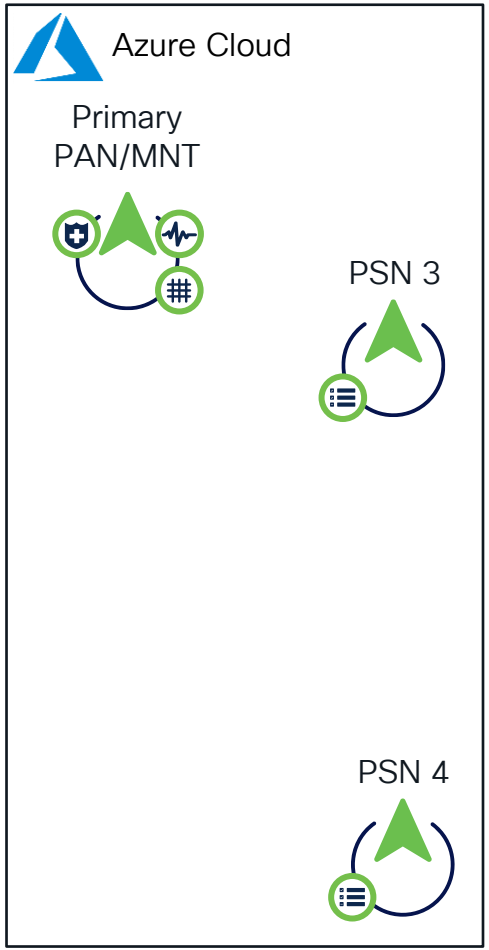


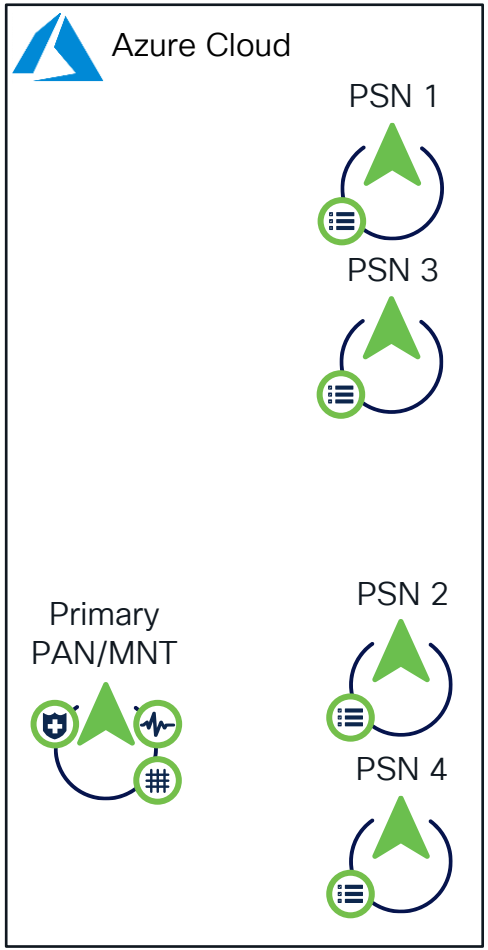
Upgrade

--- === 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



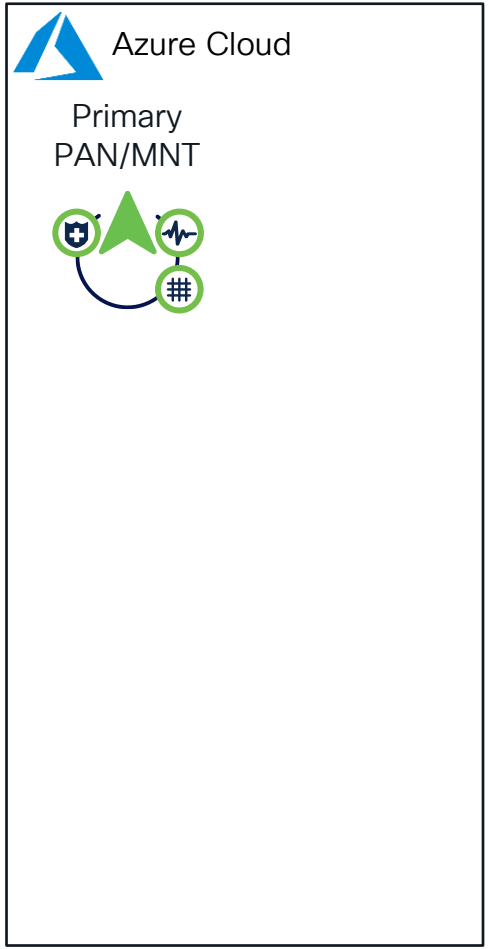


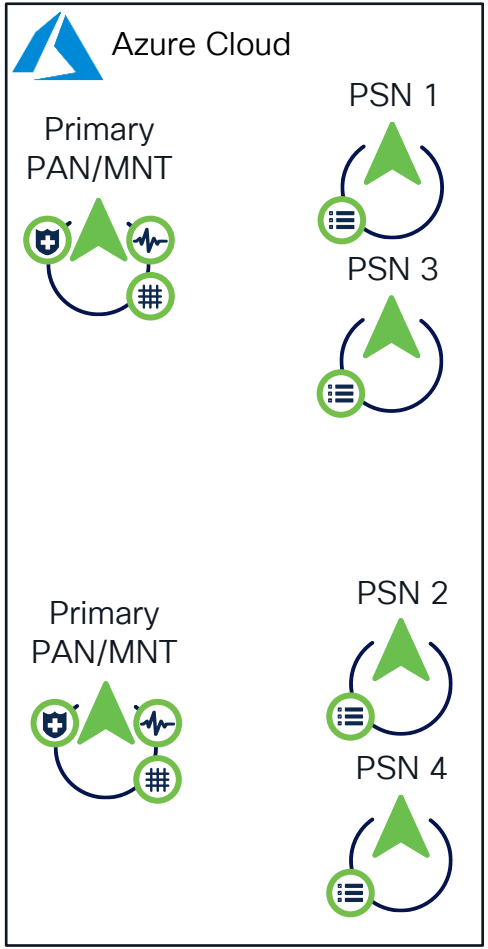
Upgrade

--- === 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

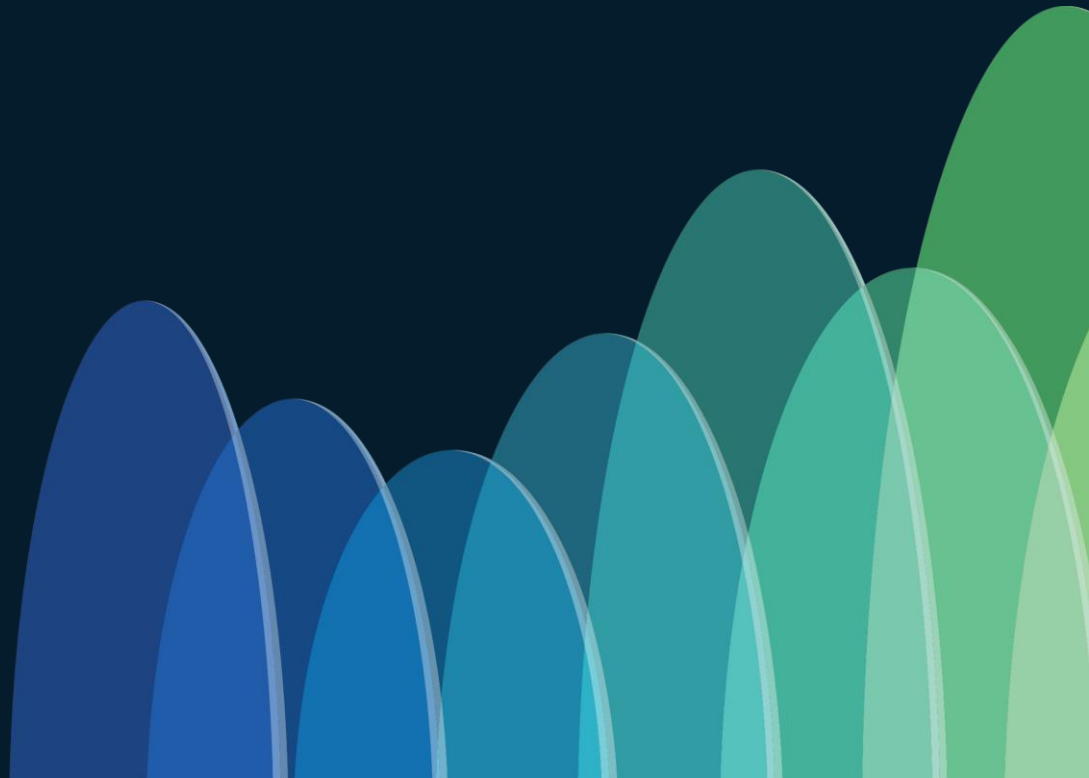
- Inline upgrade workflow is not supported. Only fresh installs are supported. However, you can carry out backup and restore of configuration data

- 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

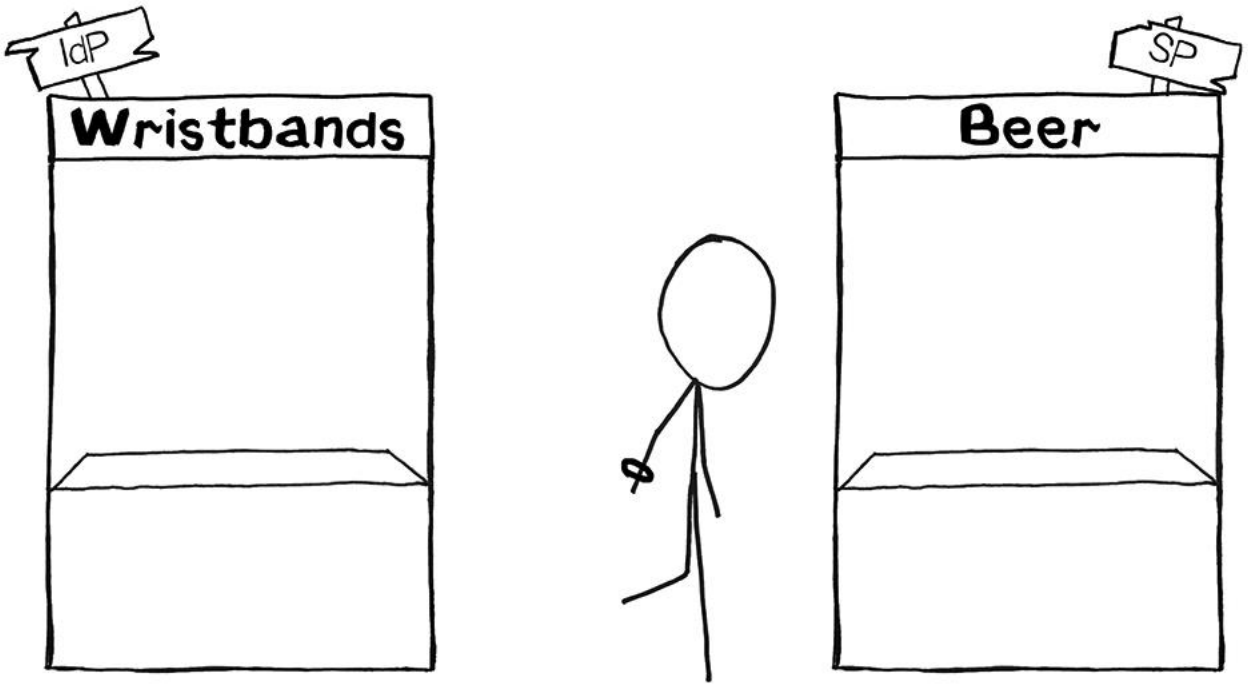
- Starting ISE 3.2 default GUI username is “iseadmin”

ISE SAML SSO



cisco Live!

What is SAML?



The Beer Drinker's Guide to SAML

Web Browser

ISE

Entra ID

1 User opens admin portal webpage

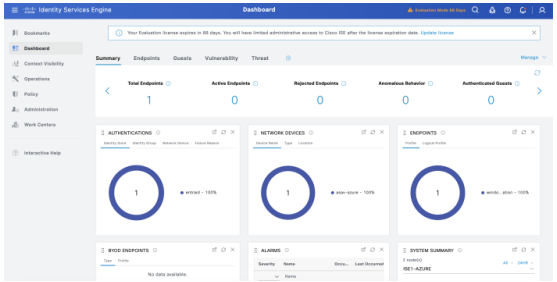
2 Internal Redirection to Azure
https://login.microsoftonline.com/

3 SAML Request, Identity Provider (Entra ID) authenticates the user

4 Encoded SAML Response is returned along with assertion data

5 SAML Response is sent to Service Provider
(ISE)

6 ISE confirms successful authentication as a result of SAML Response parsing, browser is redirected to the next page in the flow



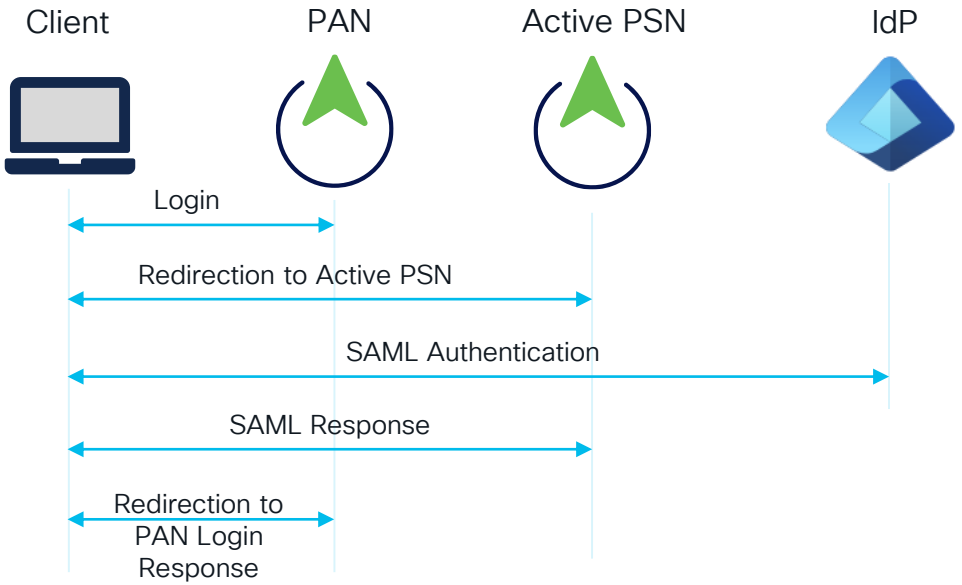
CSCwh49351 SAML request PSN exclusion

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

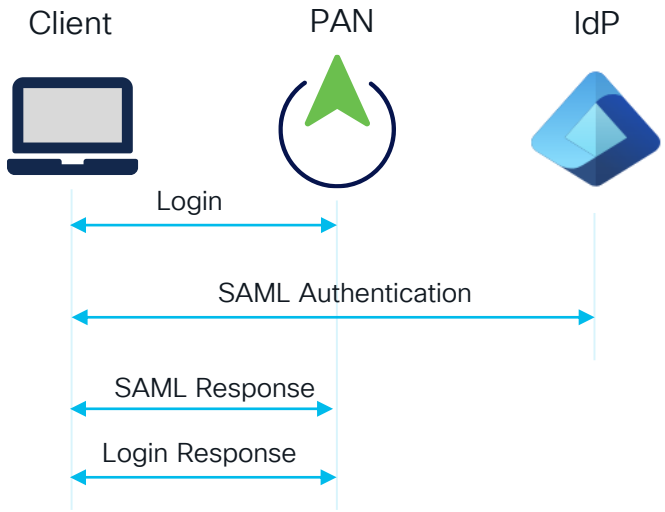


CSCwh49351 SAML request PSN exclusion

Solution:

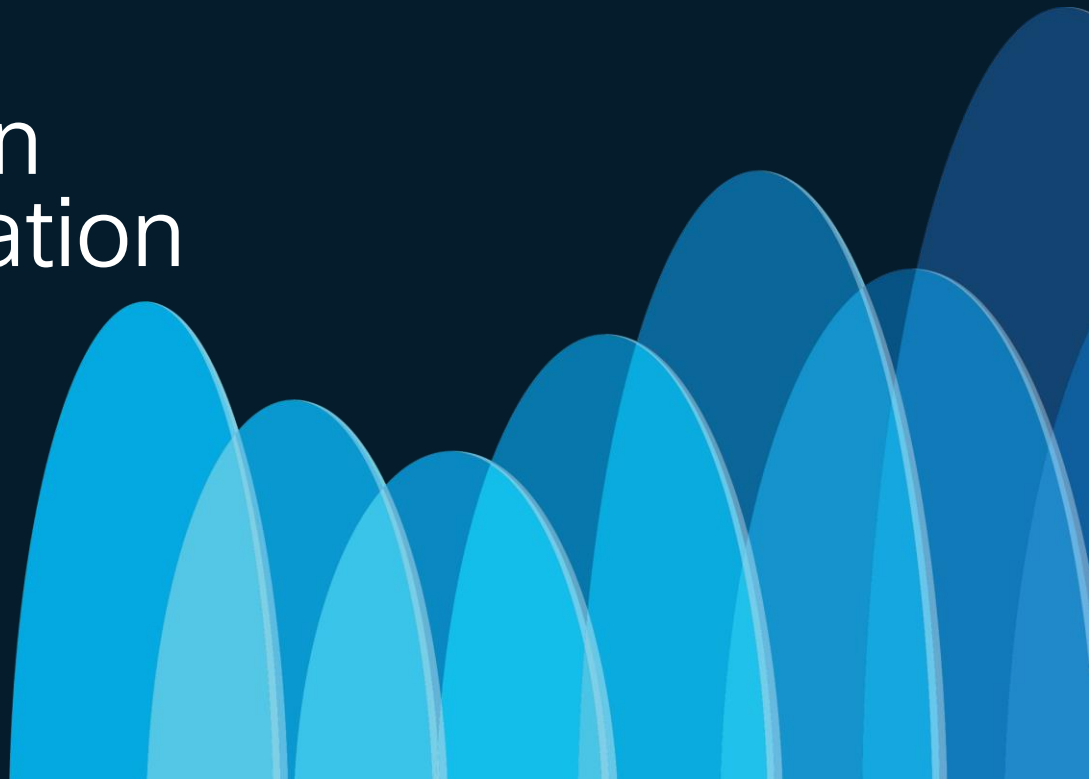
- No dependency with any other node
- Entire flow gets executed with ISE node (where admin user logs in)

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



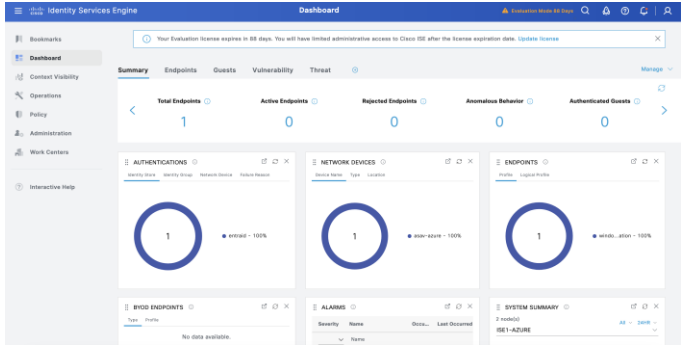
Known Fixed Releases:
ISE 3.2 patch 7
ISE 3.3 patch 4
ISE 3.4

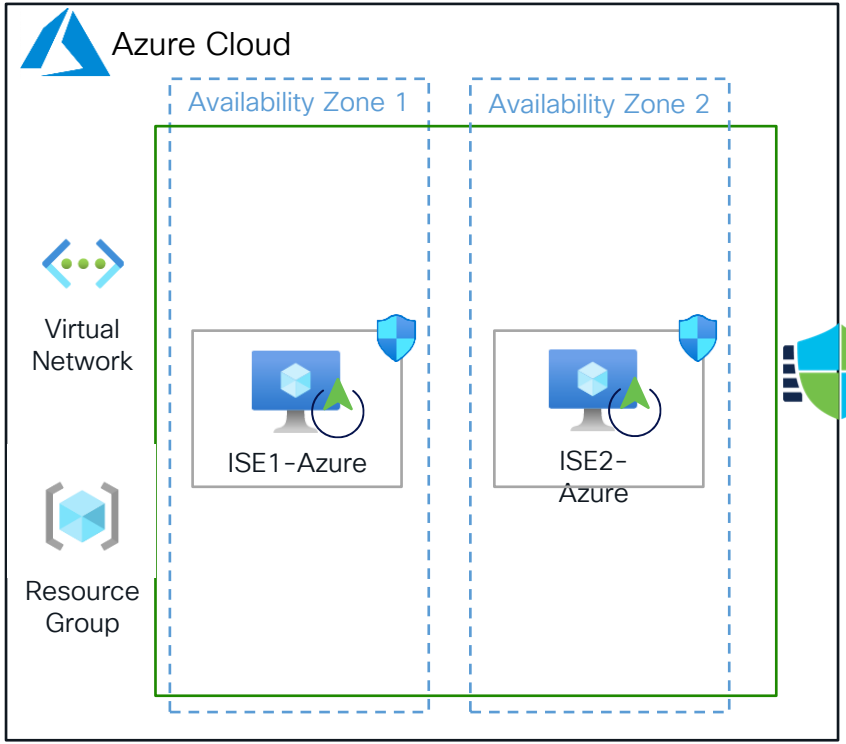
Demo. ISE Admin Portal Authentication with SAML SSO



cisco Live!

Demo Topology





Site to Site VPN Tunnel

Entra ID SAML Identity Provider

[Configure SAML SSO with Entra ID for Admin Access]

https://ise1-azure.example.com/admin/#

Identity Services Engine

Dashboard

Evaluation Mode 88 Days

- 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

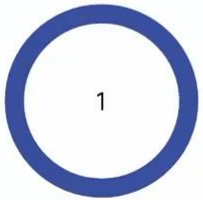
Summary | Endpoints | Guests | Vulnerability | Threat

Manage

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests
1	0	0	0	0

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason



entraid - 100%

NETWORK DEVICES

Device Name | Type | Location

asav-azure - 100%

ENDPOINTS

Profile | Logical Profile

windo...ation - 100%

BYOD ENDPOINTS

Type | Profile

No data available.

ALARMS

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

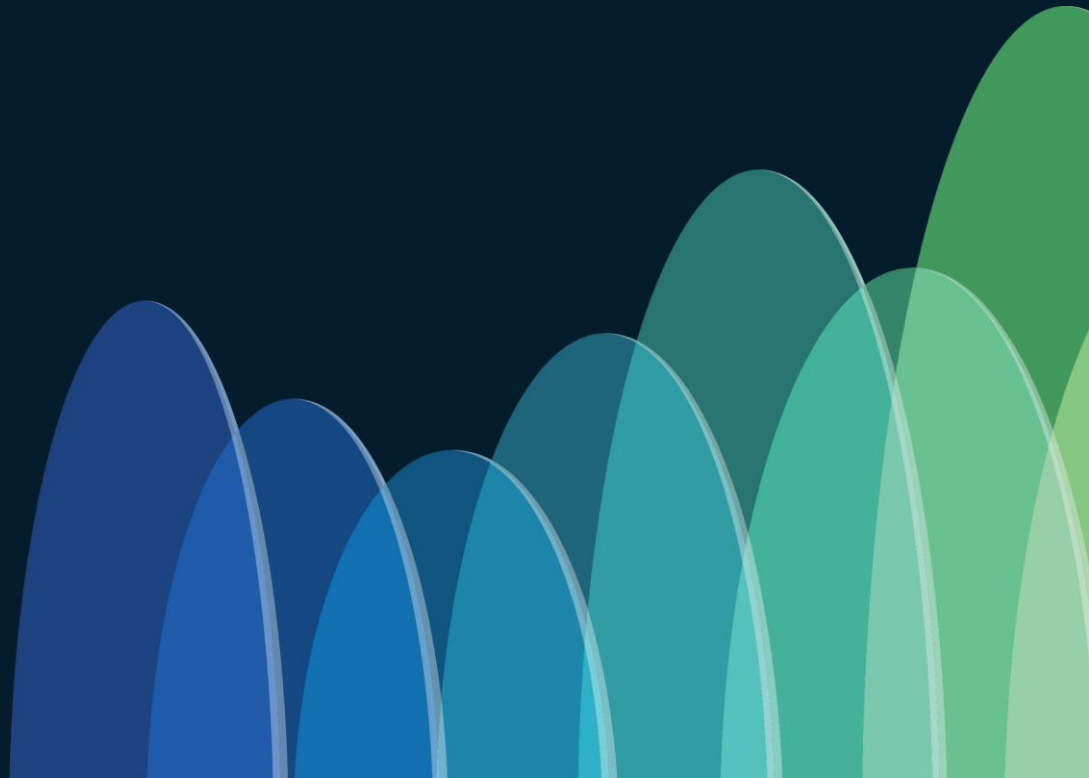
SYSTEM SUMMARY

2 node(s)

All | 24HR

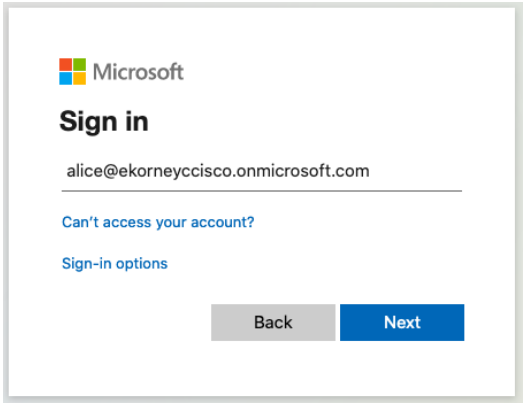
ISE1-AZURE

Entra ID Authentications



cisco Live!

802.1x Authentication Problem with SAML



Endpoint

Entra ID

SAML

802.1x

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

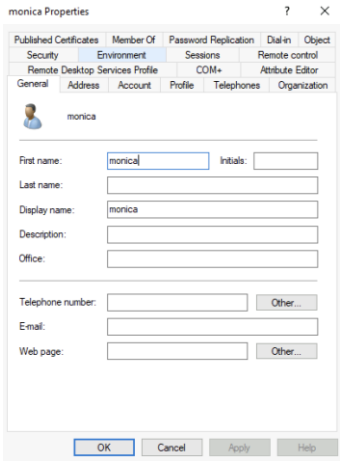
802.1x being a Layer 2 authentication protocol, will grants Network Access after Authentication is completed

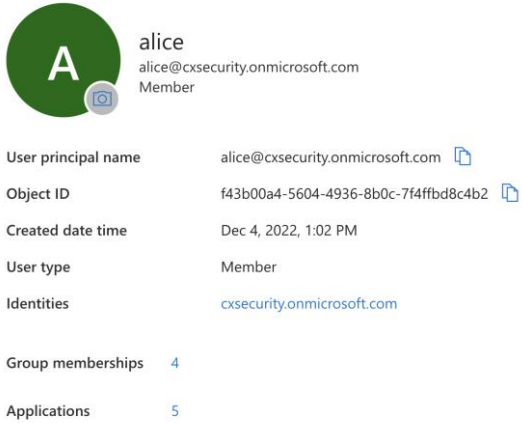
No Access Before Authentication

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

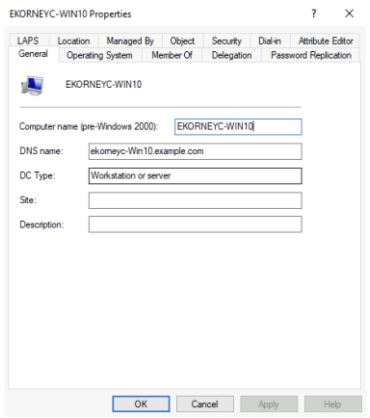
Active Directory User vs Entra ID User





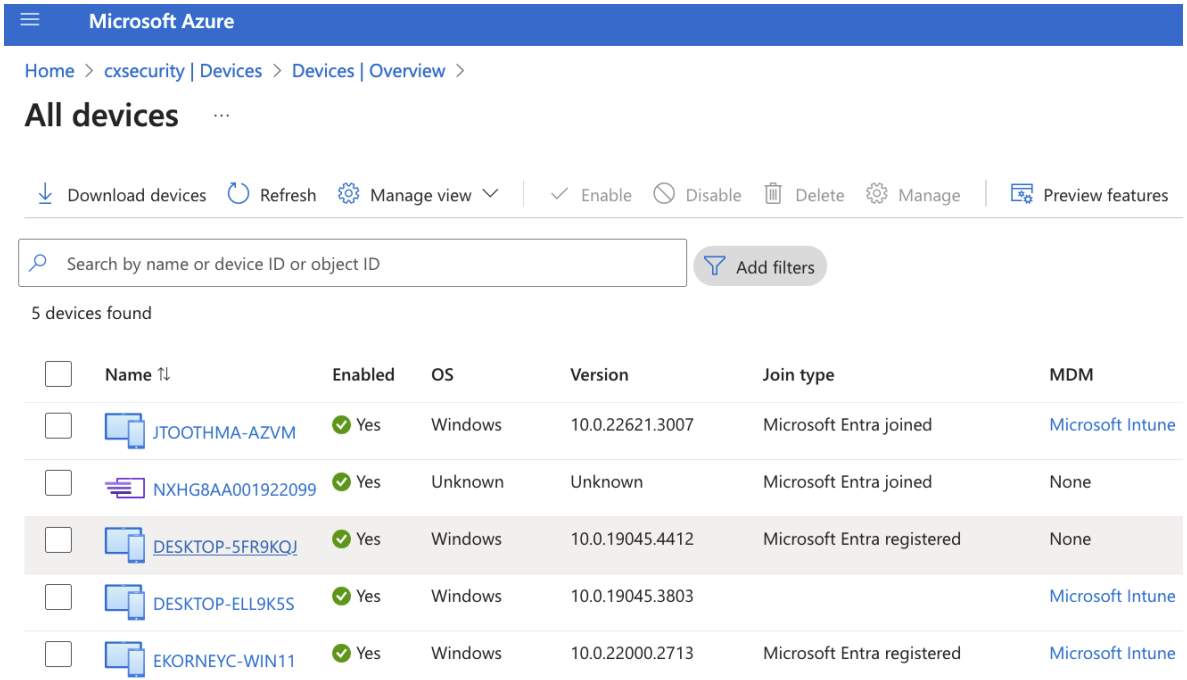
Aspect	Active Directory User	Entra ID User
Purpose	Represent User Identity	
Identifier	User Principle Name (UPN), Distinguished Name (DN), SID, sAMAccountName	User Principle Name (UPN), Object ID
Management	Active Directory, Group Policy (GPO)	Entra ID, Intune
Source	Manual Creation	Manual Creation,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

Active Directory Computer vs Entra ID Device



Aspect	Active Directory Computer	Entra ID Device
Purpose	Represent Computer/Device Identity	
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



Registered Device:

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

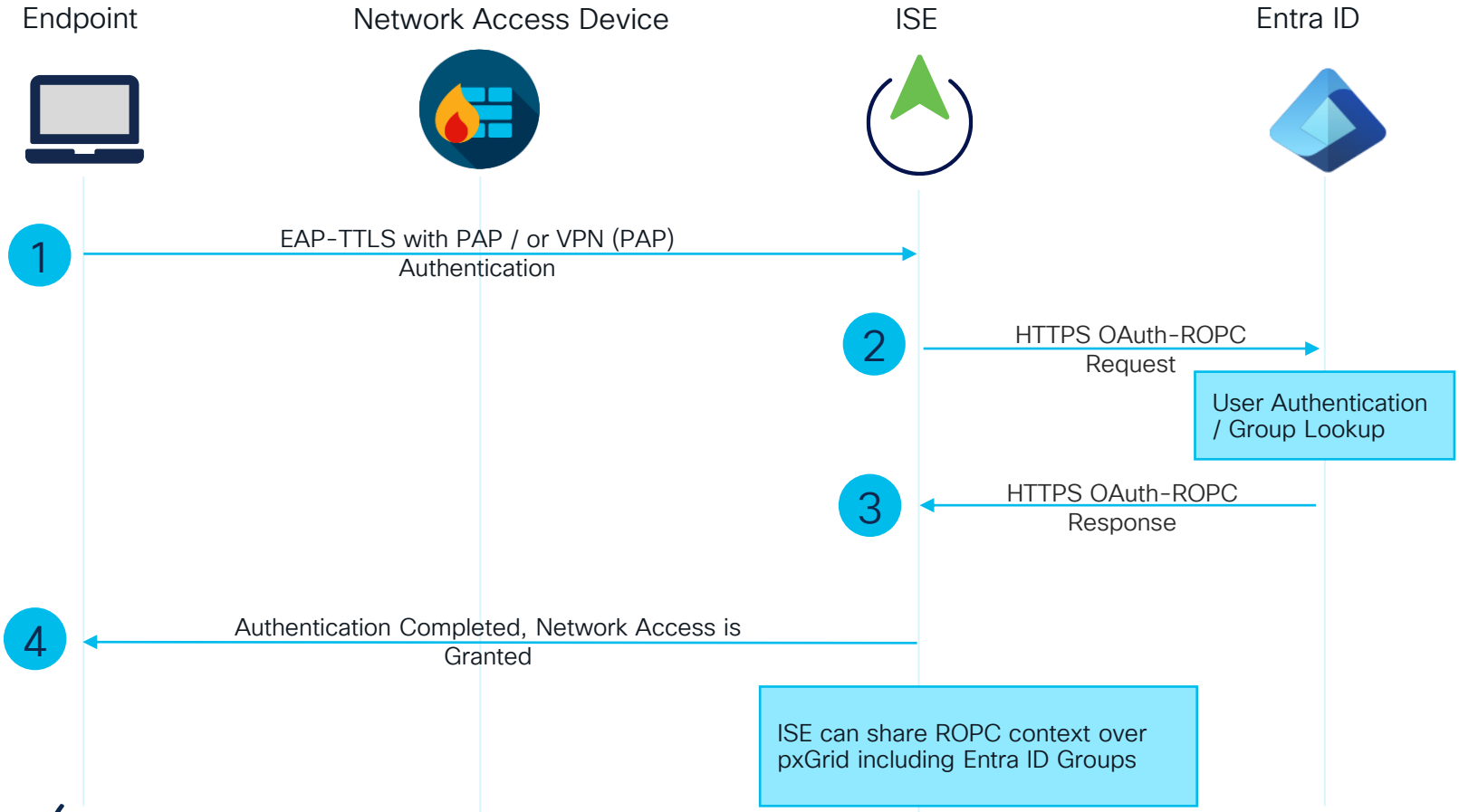
Joined Device:

- 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

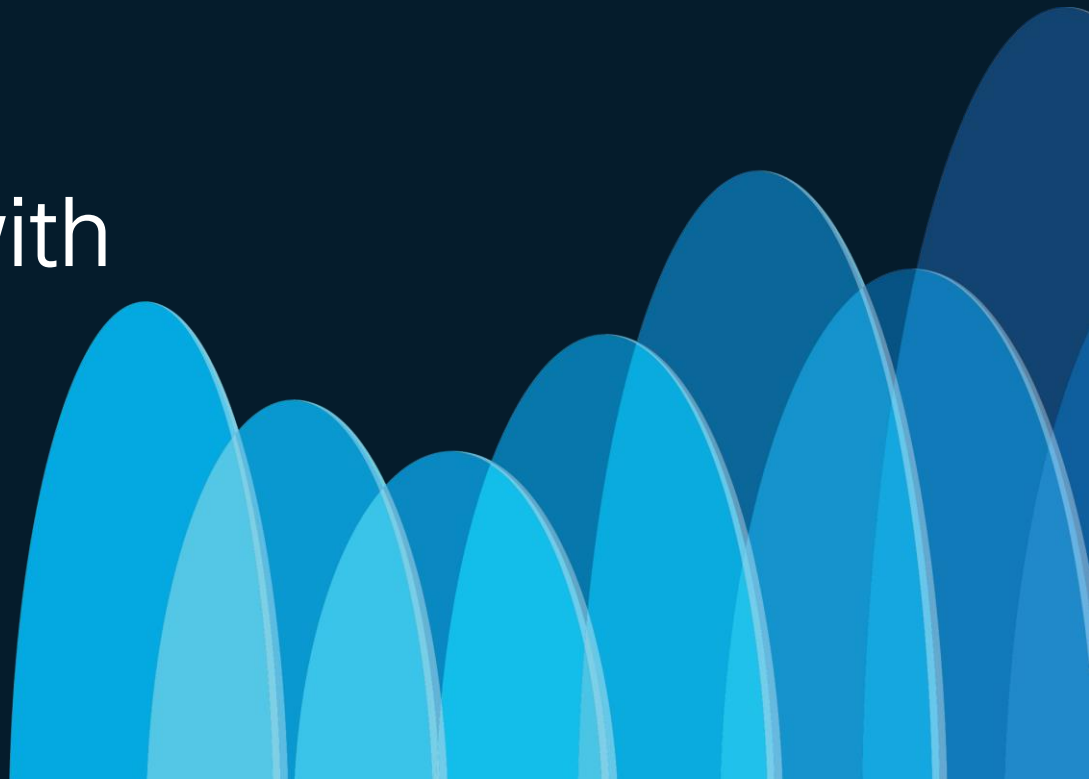
ROPC Flow Diagram



ROPC Limitations

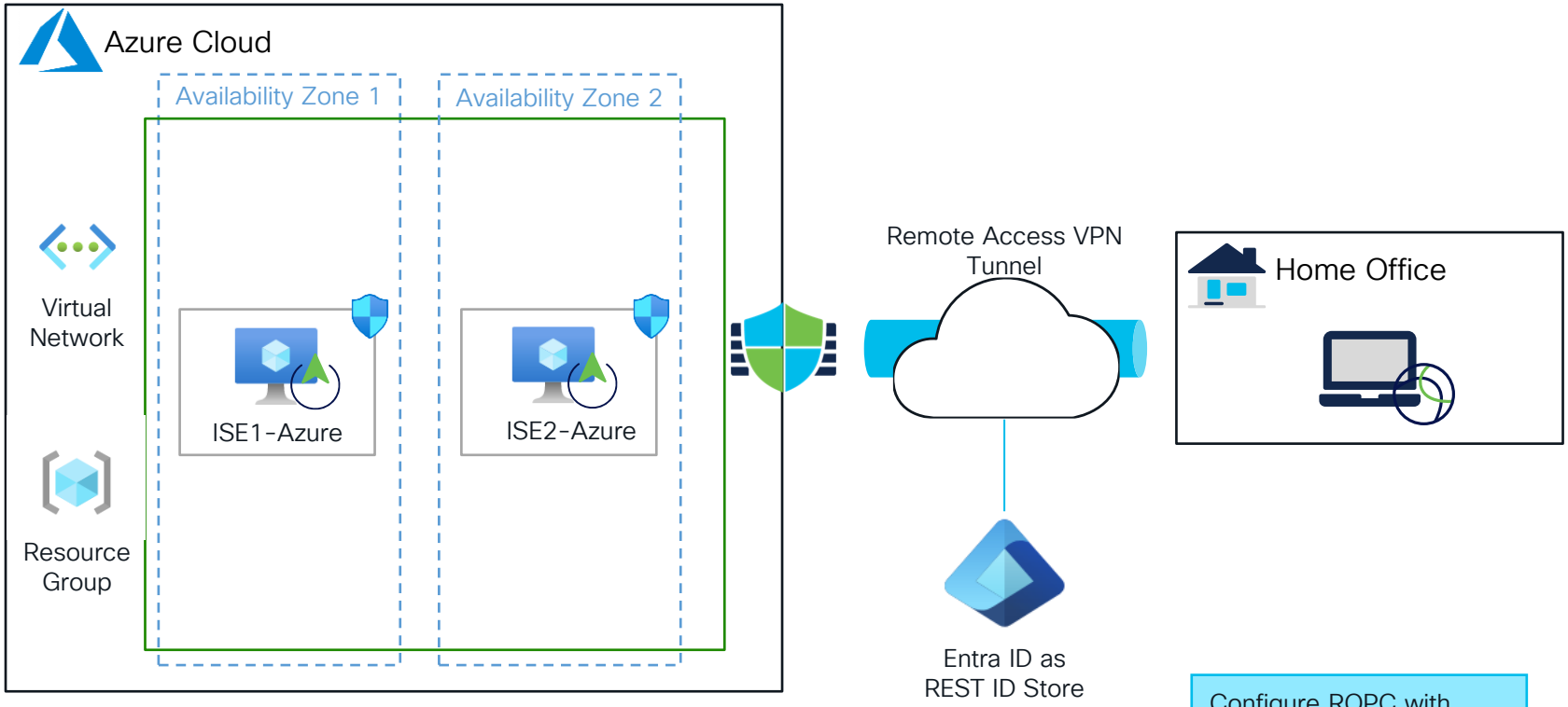
- No user interactions allowed for password changes, MFA, or AUPs
- No new accounts that have not yet changed the default password
- Only user authentication is supported

Demo. ROPC Authentication with VPN Use Case



cisco Live!

Demo Topology



Configure ROPC with Entra ID

https://ise1-azure.example.com/admin/#home

Identity Services Engine

Dashboard

Evaluation Mode 87 Days

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

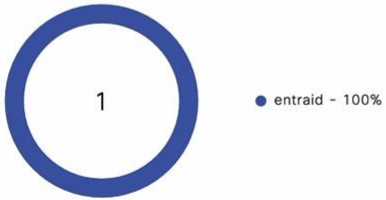
Your Evaluation license expires in 87 days. You will have limited administrative access to Cisco ISE after the license expiration date. Update license

Summary | Endpoints | Guests | Vulnerability | Threat | Manage

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests
1	0	0	0	0

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

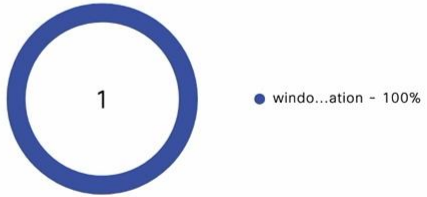


NETWORK DEVICES

Device Name | Type | Location

ENDPOINTS

Profile | Logical Profile



BYOD ENDPOINTS

Type | Profile

No data available.

ALARMS

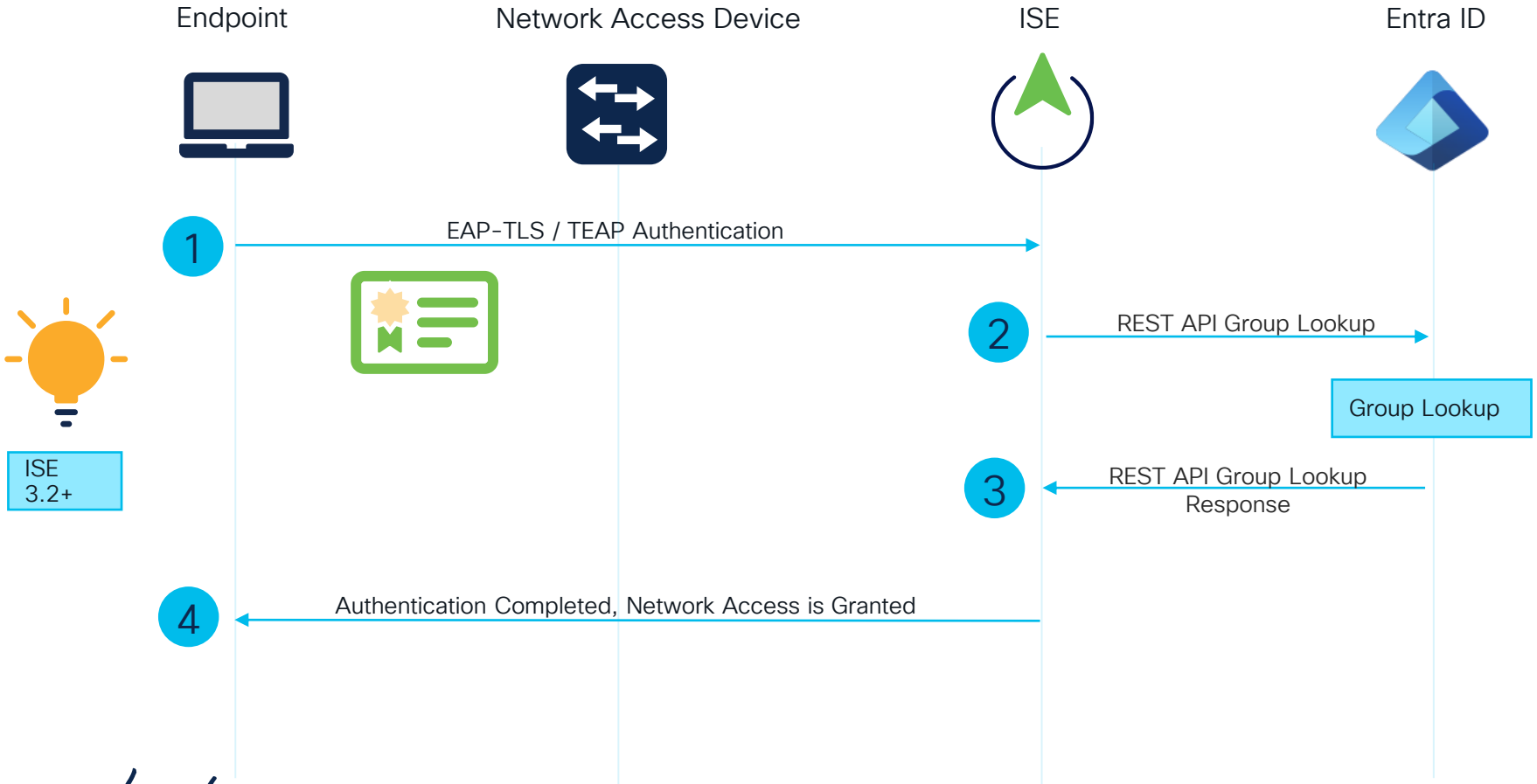
Severity	Name	Occu...	Last Occurred
	Name		
	Configuration Changed	9516	less than 1 min

SYSTEM SUMMARY

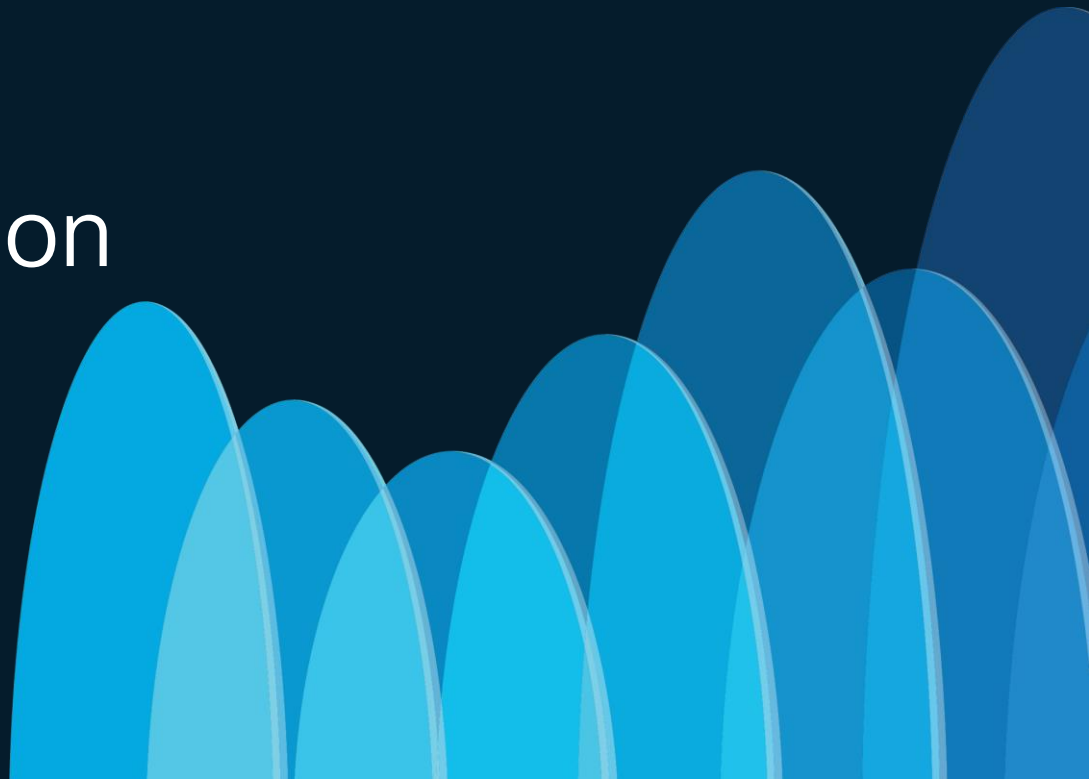
2 node(s) — All — 24HR

ISE1-AZURE

EAP-TLS Authorization with Entra ID

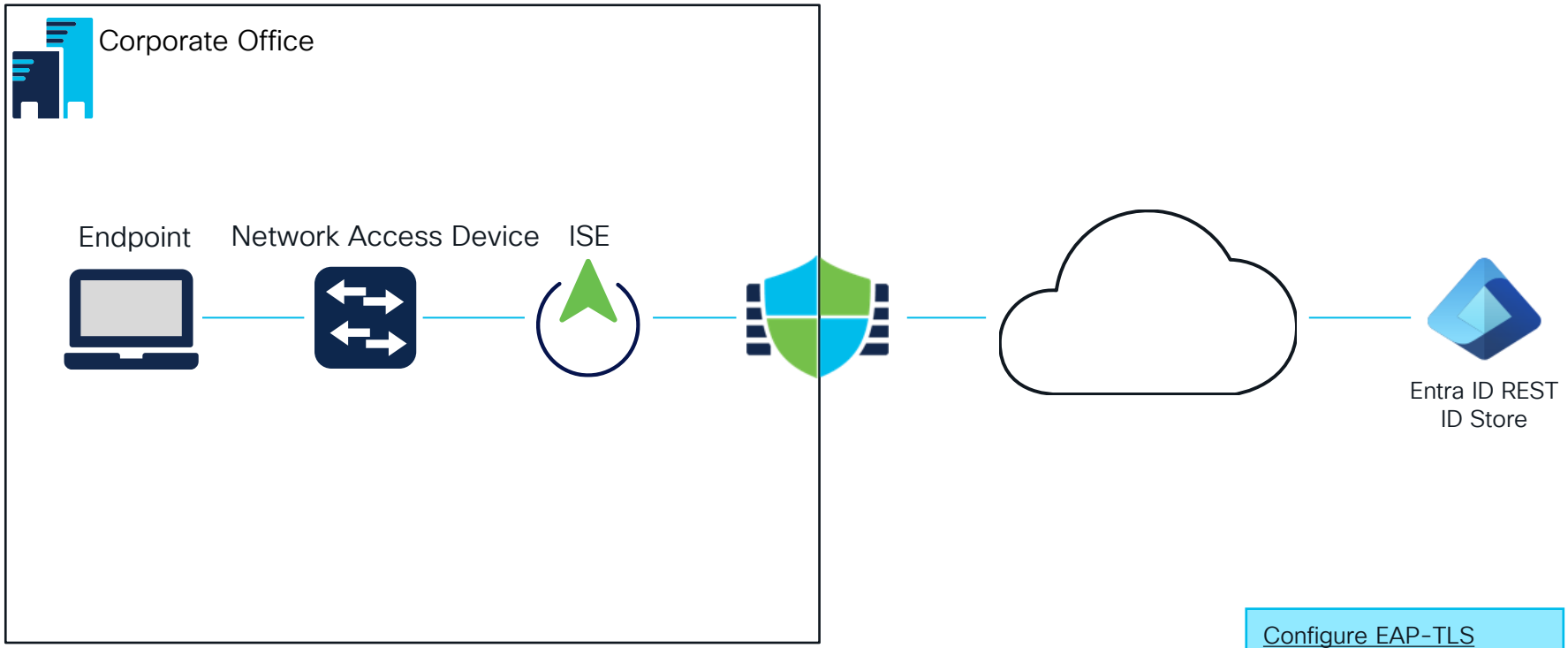


Demo. REST ID Store Authorization with EAP-TLS

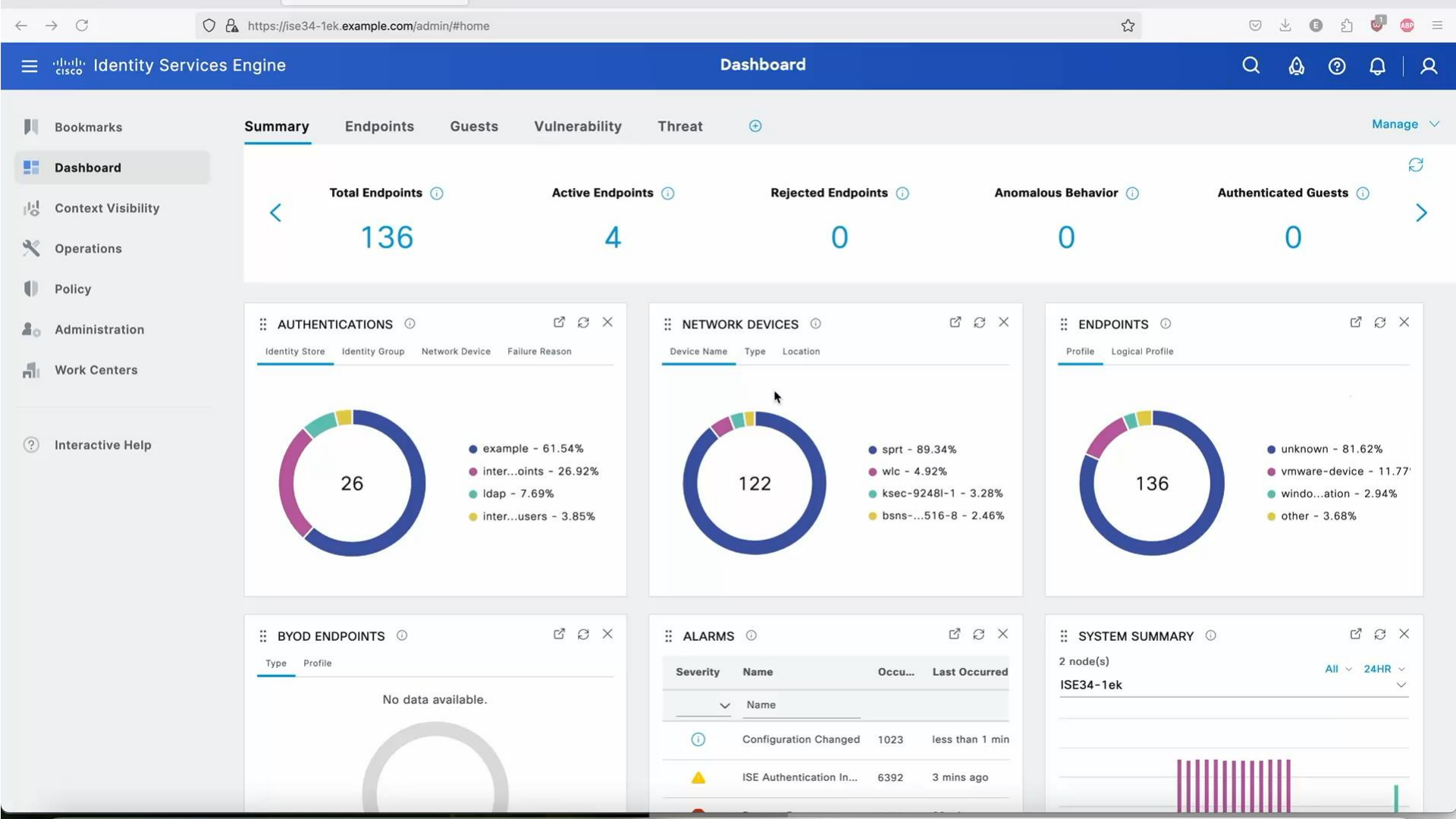


cisco Live!

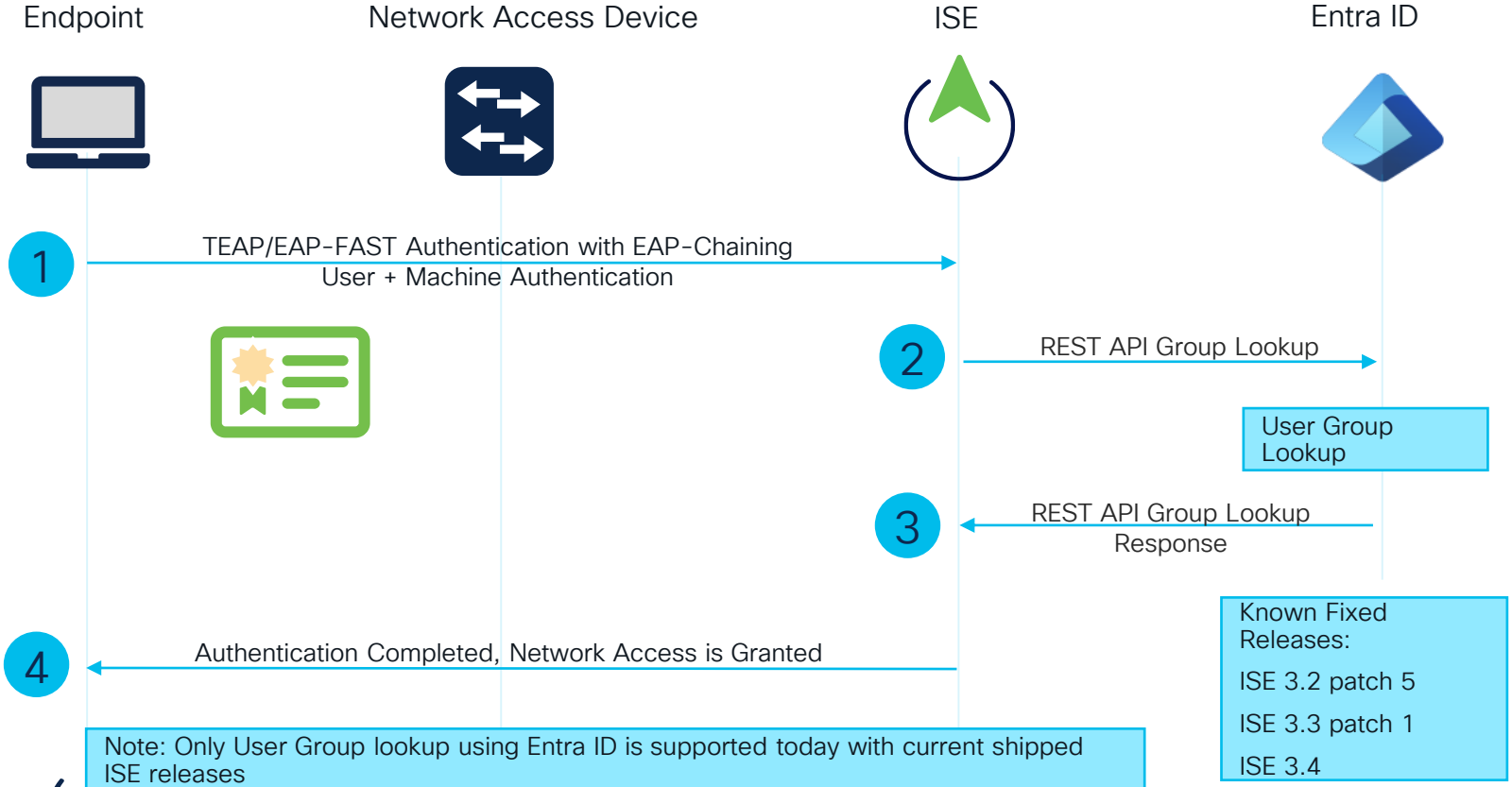
Demo Topology



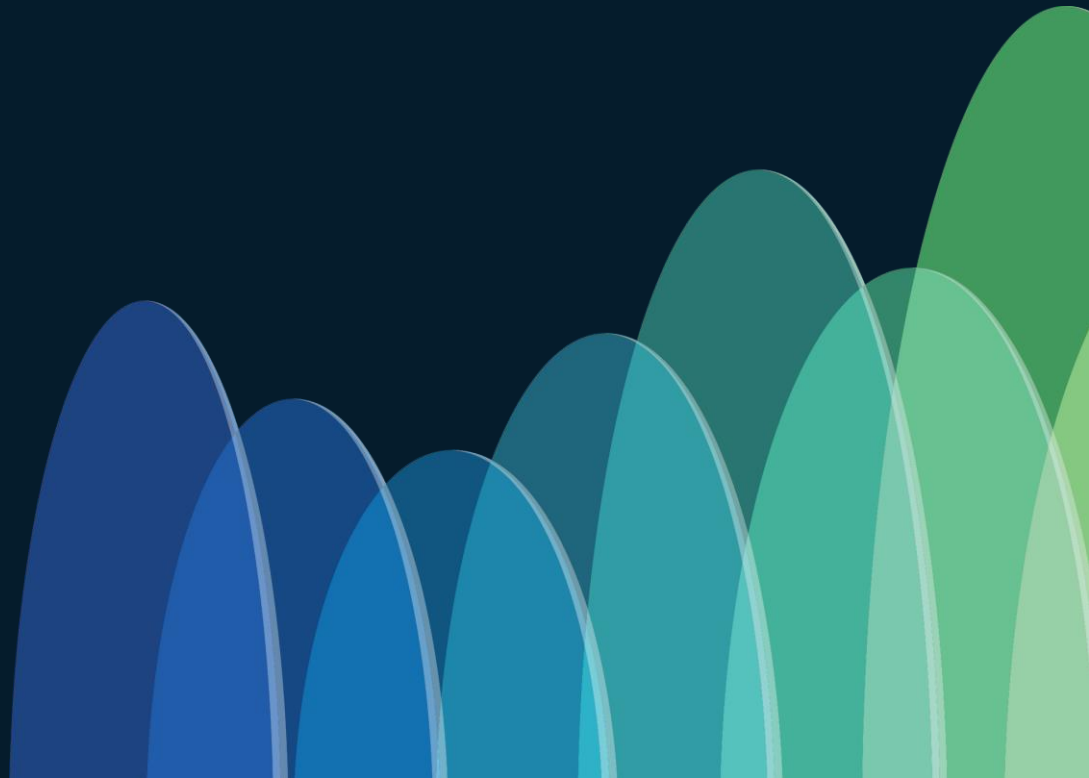
Configure EAP-TLS Authorization with Entra ID


https://ise34-1ek.example.com/admin/#home
Identity Services Engine
Dashboard
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
136
Active Endpoints
4
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
26
example - 61.54%
inter...oints - 26.92%
ldap - 7.69%
inter...users - 3.85%
NETWORK DEVICES
Device Name
Type
Location
122
sprt - 89.34%
wlc - 4.92%
ksec-9248l-1 - 3.28%
bsns-...516-8 - 2.46%
ENDPOINTS
Profile
Logical Profile
136
unknown - 81.62%
vmware-device - 11.77
windo...ation - 2.94%
other - 3.68%
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Occu...
Last Occurred
Name
Configuration Changed
1023
less than 1 min
ISE Authentication In...
6392
3 mins ago
SYSTEM SUMMARY
2 node(s)
All
24HR
ISE34-1ek

CSCwd34467 ISE Authz rule evaluation broken for attempts using eap-chaining and Azure AD groups

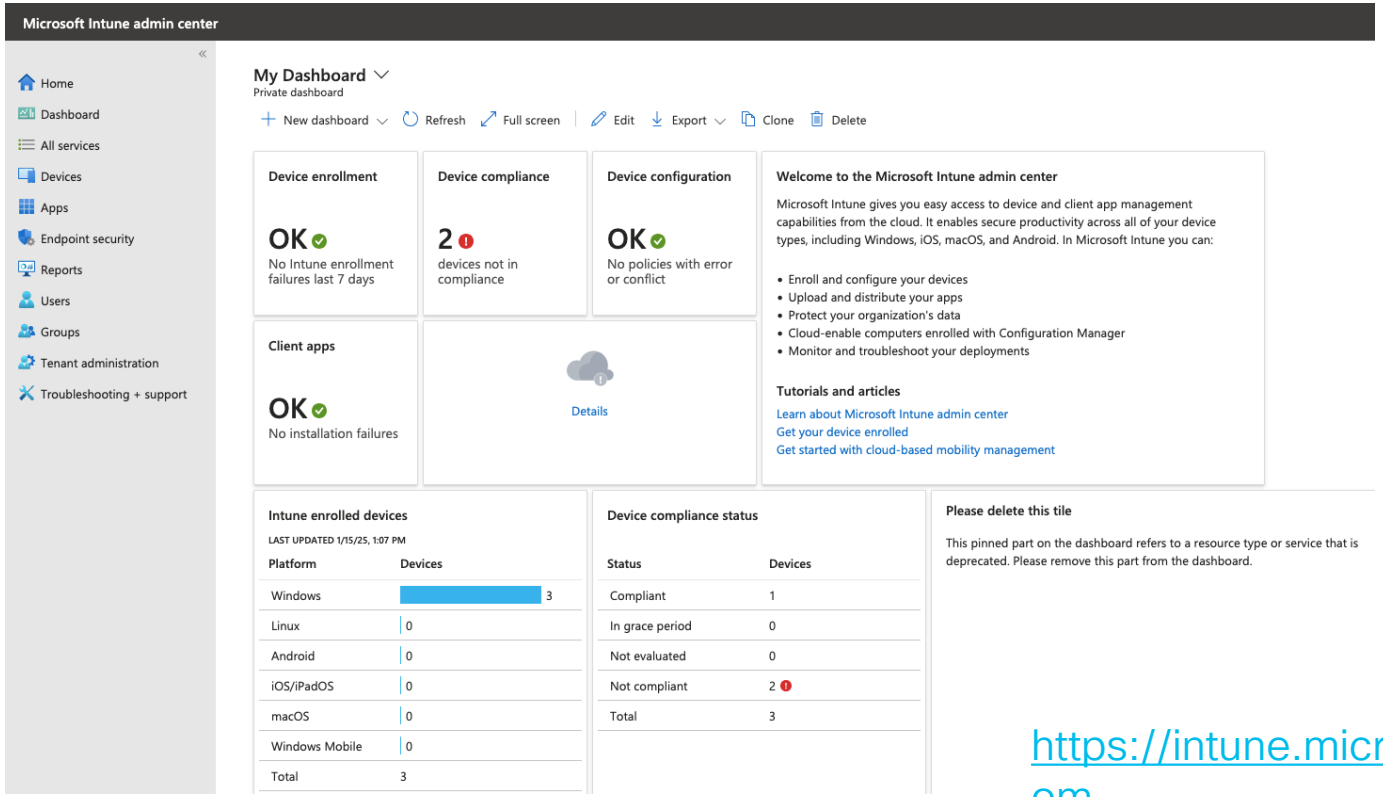


Intune Integration



cisco Live!

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



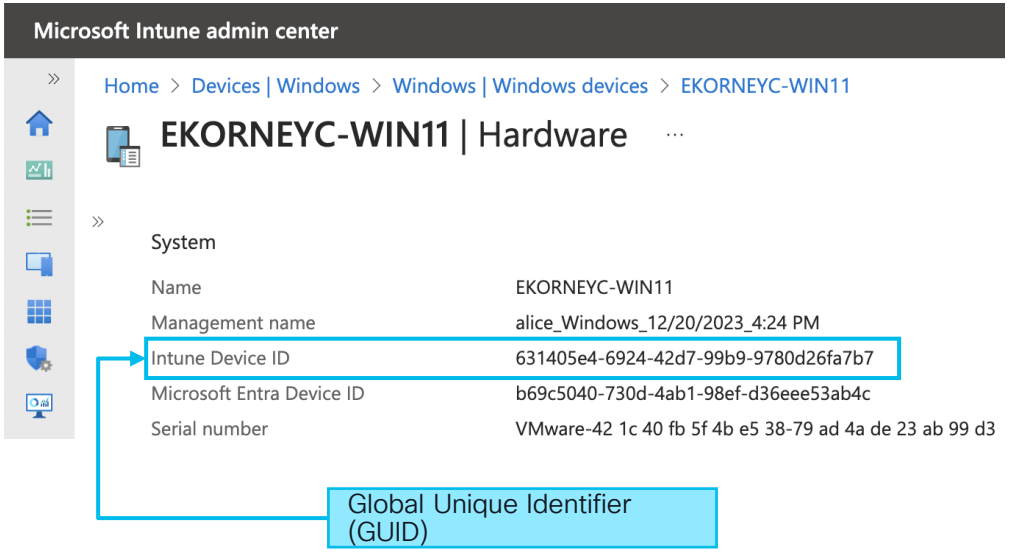
https://intune.microsoft.com

Problem with MAC address MDM Lookup

1. Docking Station / Dongles

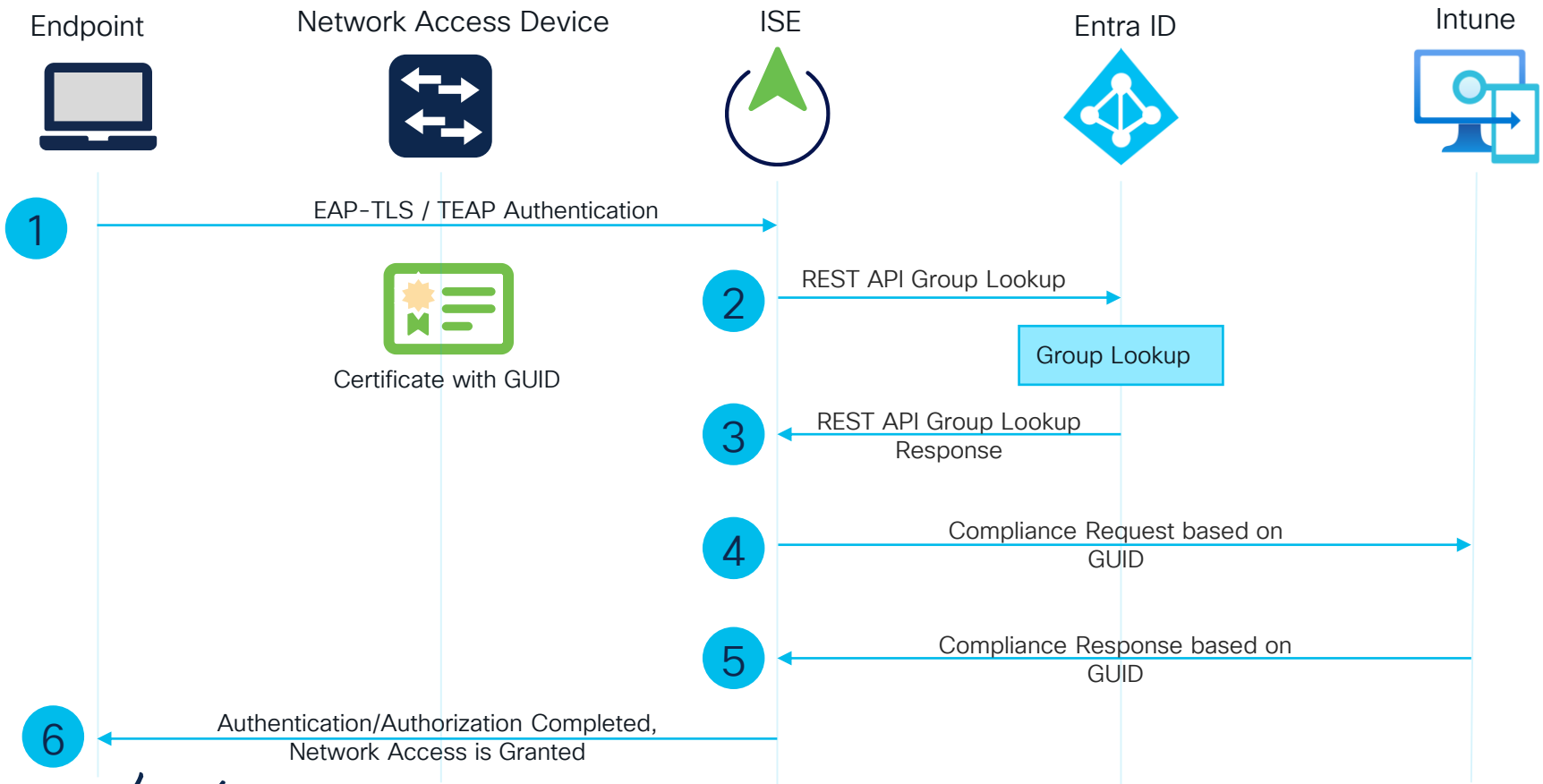
2. Wired vs Wireless

3. Random MAC address

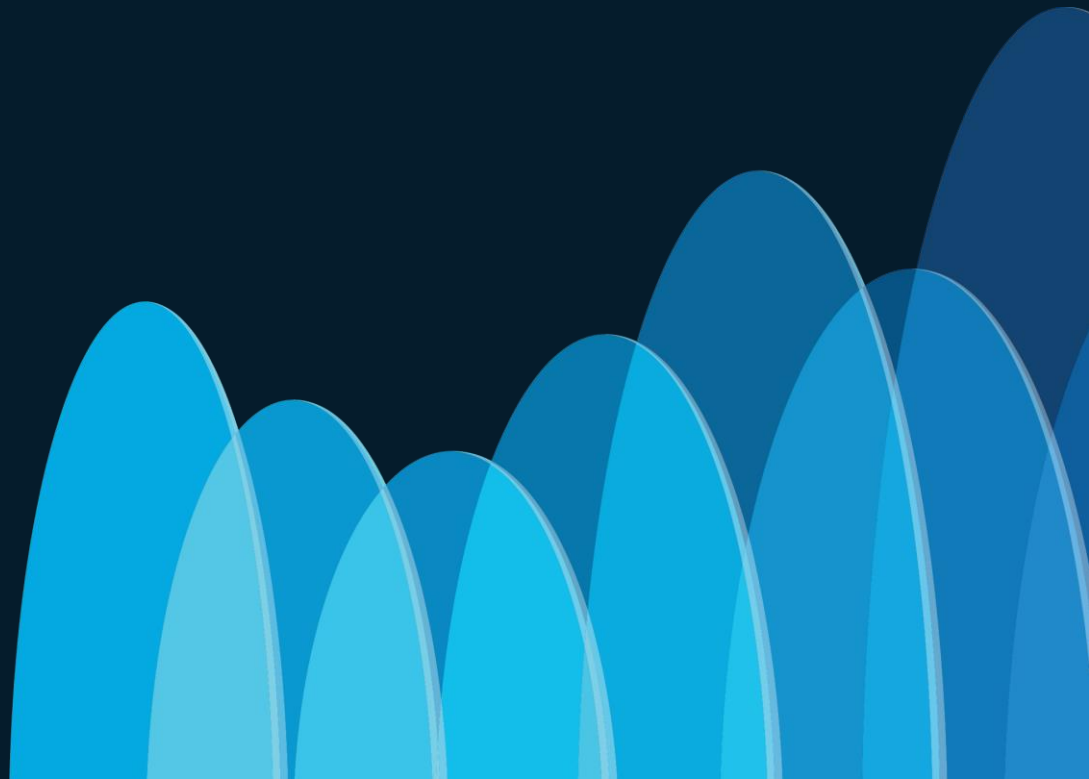


Certificate with GUID

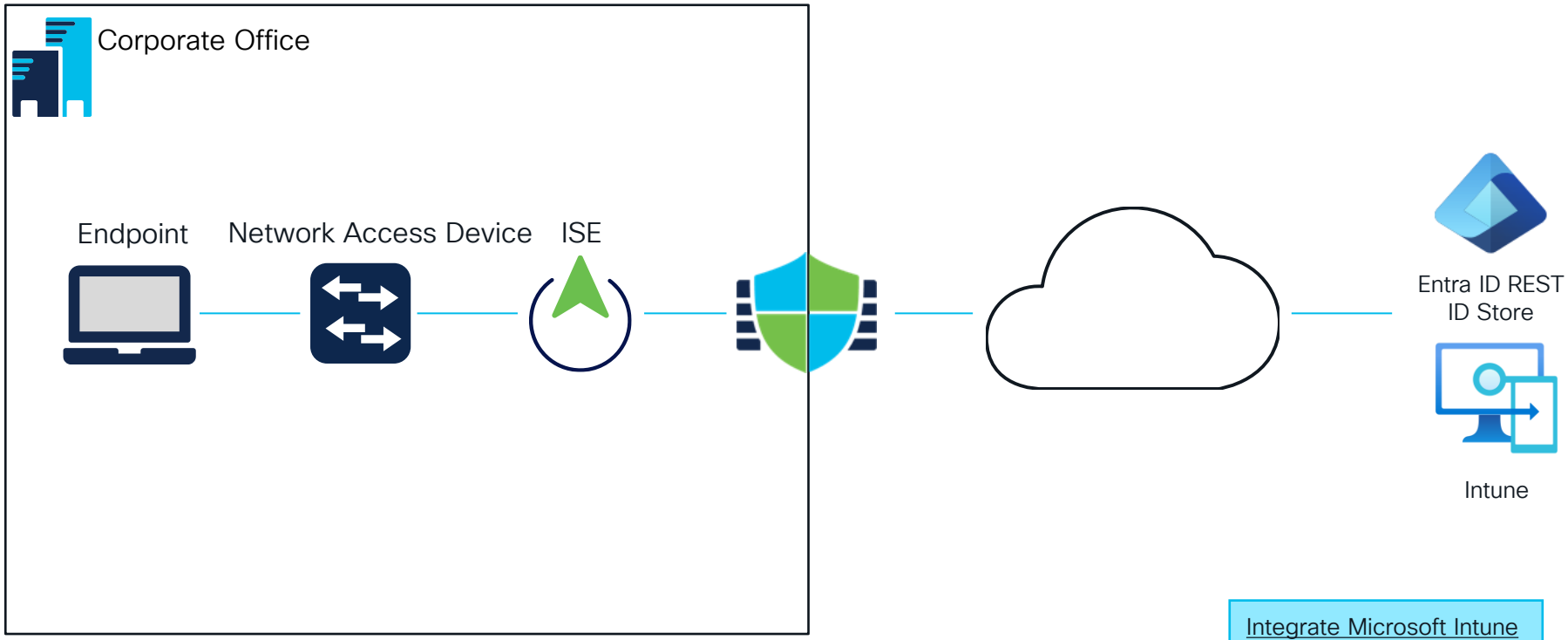
EAP-TLS with Azure Entra ID and Intune MDM



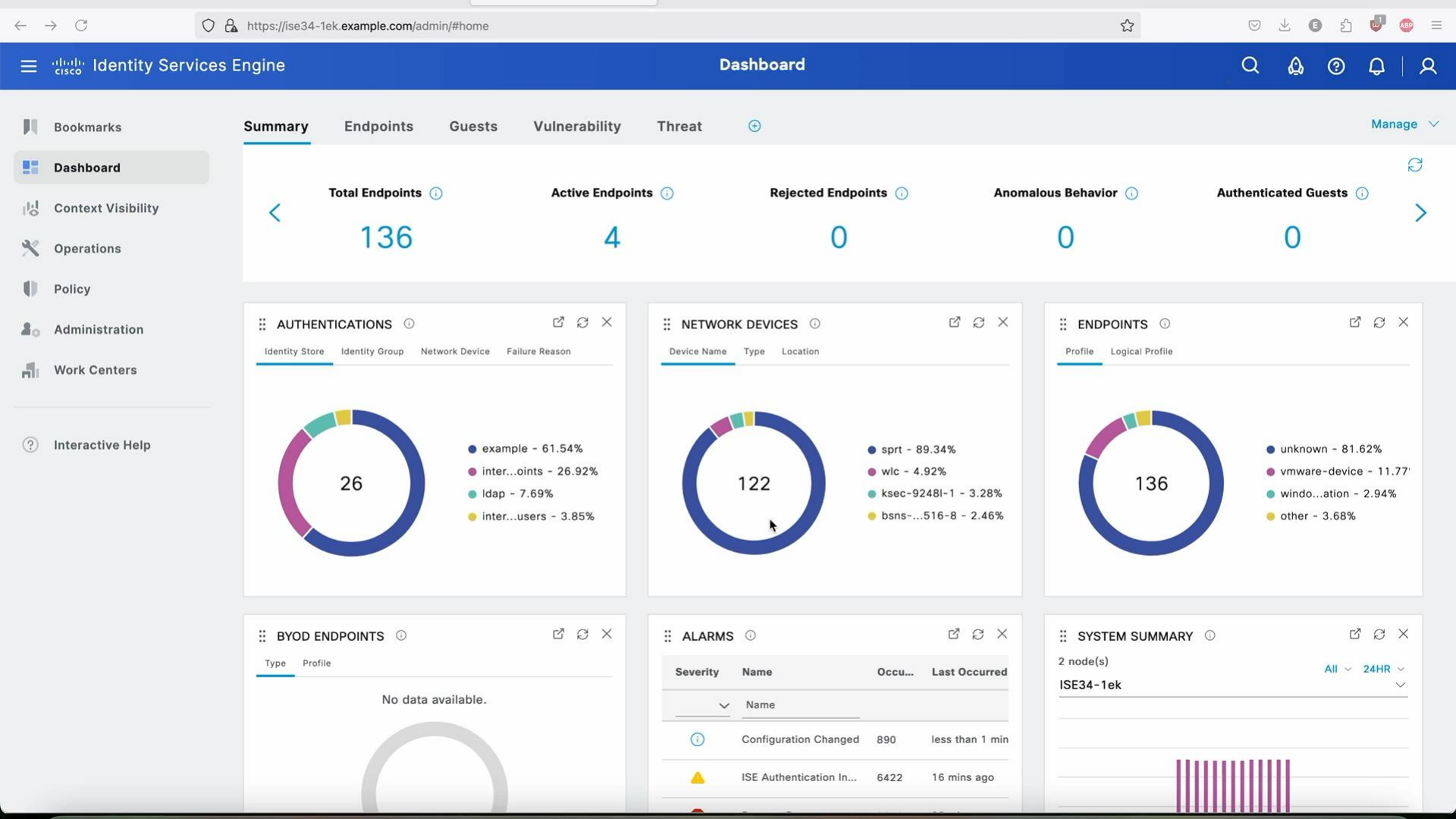
Demo. Intune MDM Integration



Deployment Topology



Integrate Microsoft Intune with Cisco ISE


https://ise34-1ek.example.com/admin/#home
Identity Services Engine
Dashboard
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Summary
Endpoints
Guests
Vulnerability
Threat
Manage
Total Endpoints
136
Active Endpoints
4
Rejected Endpoints
0
Anomalous Behavior
0
Authenticated Guests
0
AUTHENTICATIONS
Identity Store
Identity Group
Network Device
Failure Reason
26
example - 61.54%
inter...oints - 26.92%
ldap - 7.69%
inter...users - 3.85%
NETWORK DEVICES
Device Name
Type
Location
122
sprt - 89.34%
wlc - 4.92%
ksec-9248l-1 - 3.28%
bsns-...516-8 - 2.46%
ENDPOINTS
Profile
Logical Profile
136
unknown - 81.62%
vmware-device - 11.77
windo...ation - 2.94%
other - 3.68%
BYOD ENDPOINTS
Type
Profile
No data available.
ALARMS
Severity
Name
Occu...
Last Occurred
Name
Configuration Changed
890
less than 1 min
ISE Authentication In...
6422
16 mins ago
SYSTEM SUMMARY
2 node(s)
All
24HR
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.

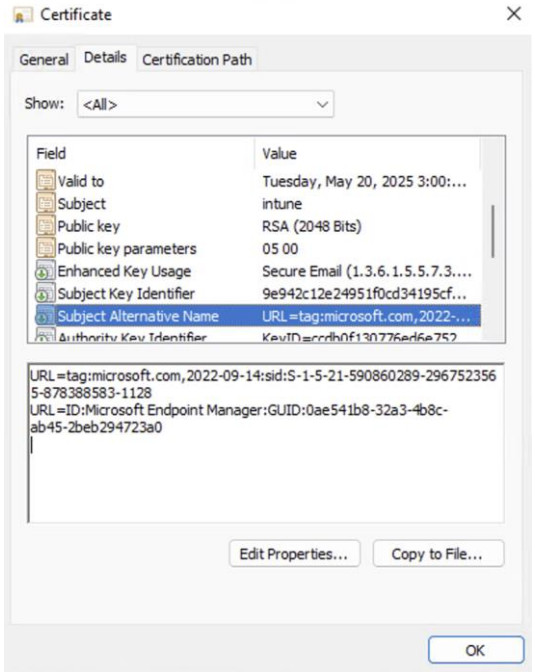
Known Fixed Releases:

ISE 3.1 patch 10

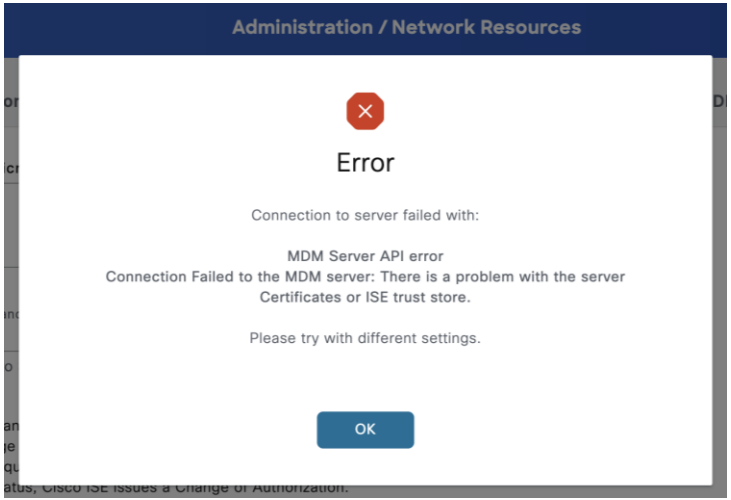
ISE 3.2 patch 7

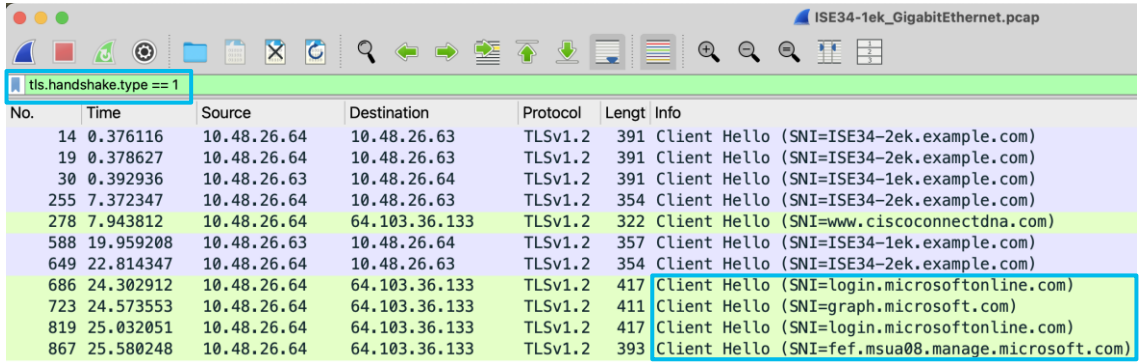
ISE 3.3 patch 4

ISE 3.4 patch 1

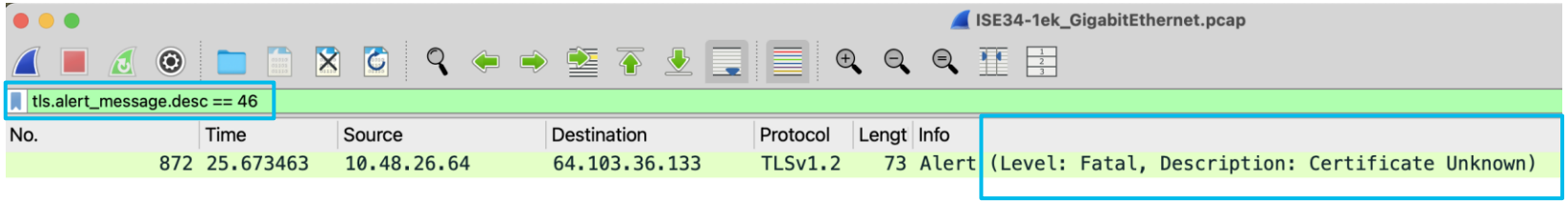


Intune Integration Troubleshooting



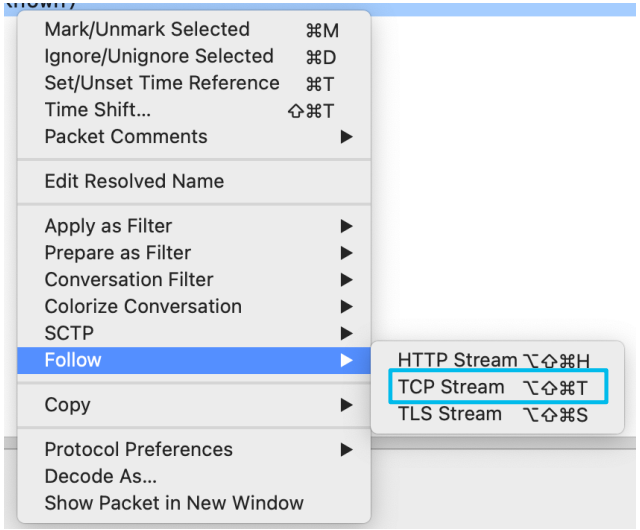


1 Wireshark filter: tls.handshake.type == 1, to filter Client Hello messages

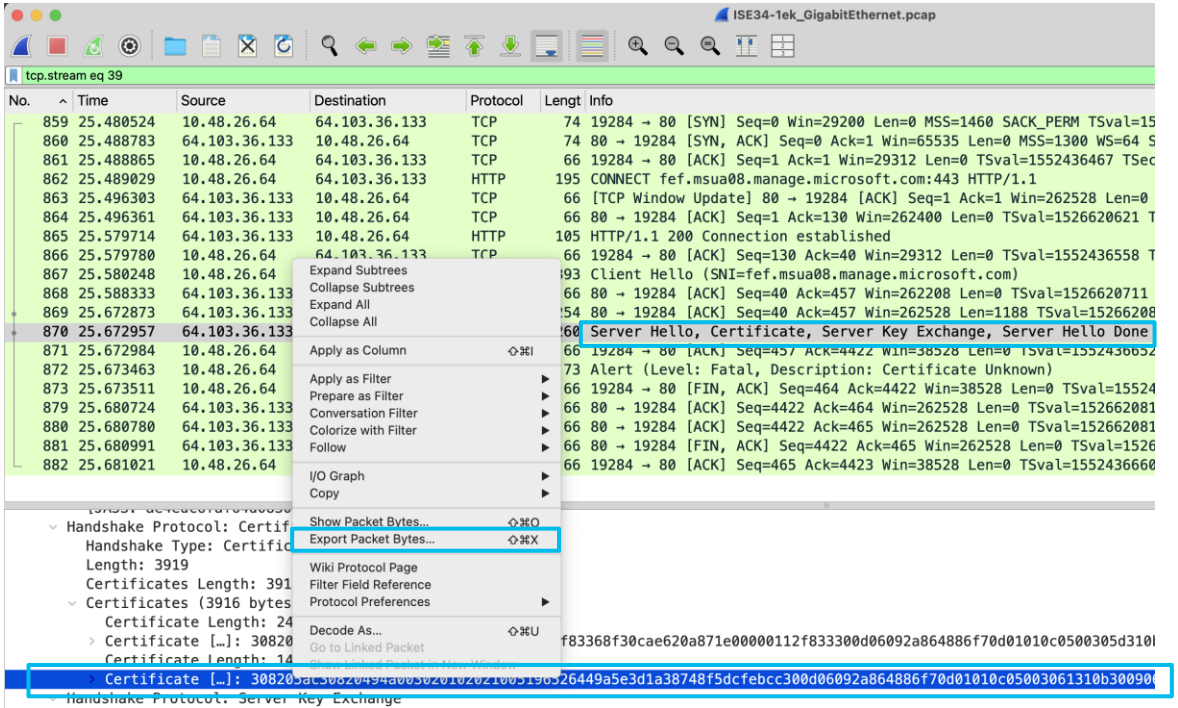


2 Wireshark filter: tls.alert_message.desc == 46, to filter Certificate Unknown TLS Alerts

Intune Integration Troubleshooting



3 Wireshark: Right Click > Follow > TCP Stream

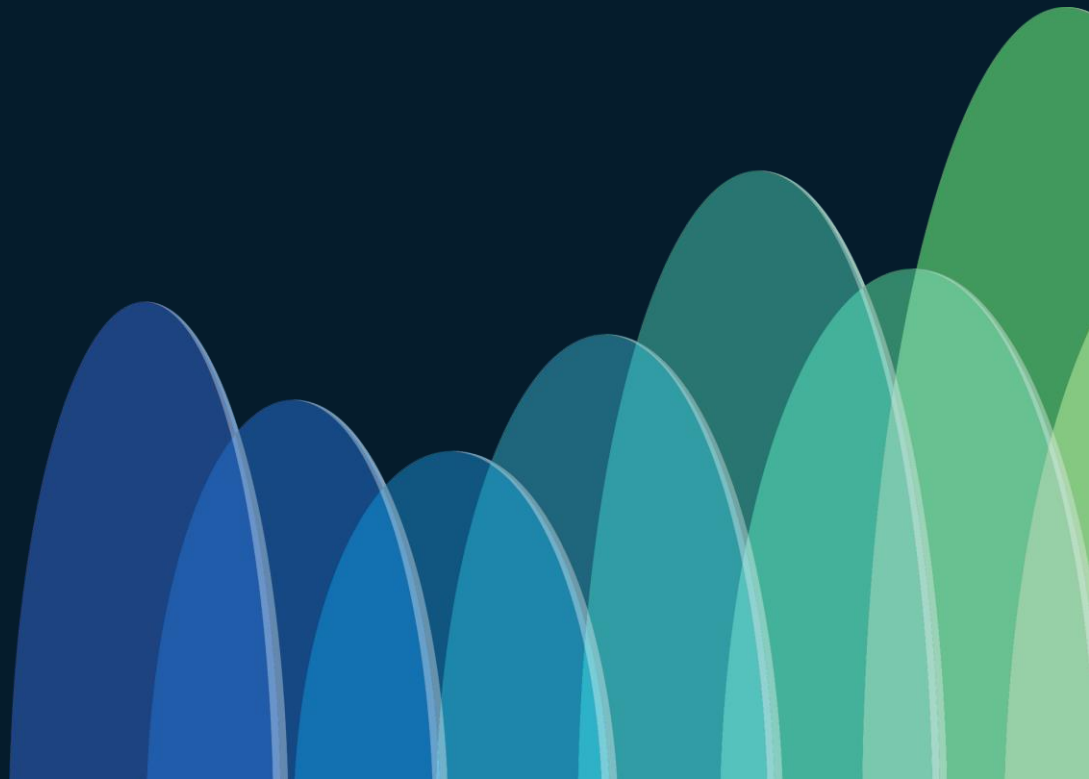


5 Import Certificate into ISE Trusted Store

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 are possible with Entra ID as an External Identity Store
- ISE MDM integration allows more granular network access based on the Compliance Status

Webex App

Questions?

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

How

1. Find this session in the Cisco Events mobile app
2. Click “Join the Discussion”
3. Install the Webex app or go directly to the Webex space
4. Enter messages/questions in the Webex space

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

Fill Out Your Session Surveys

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

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

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

Content Catalog

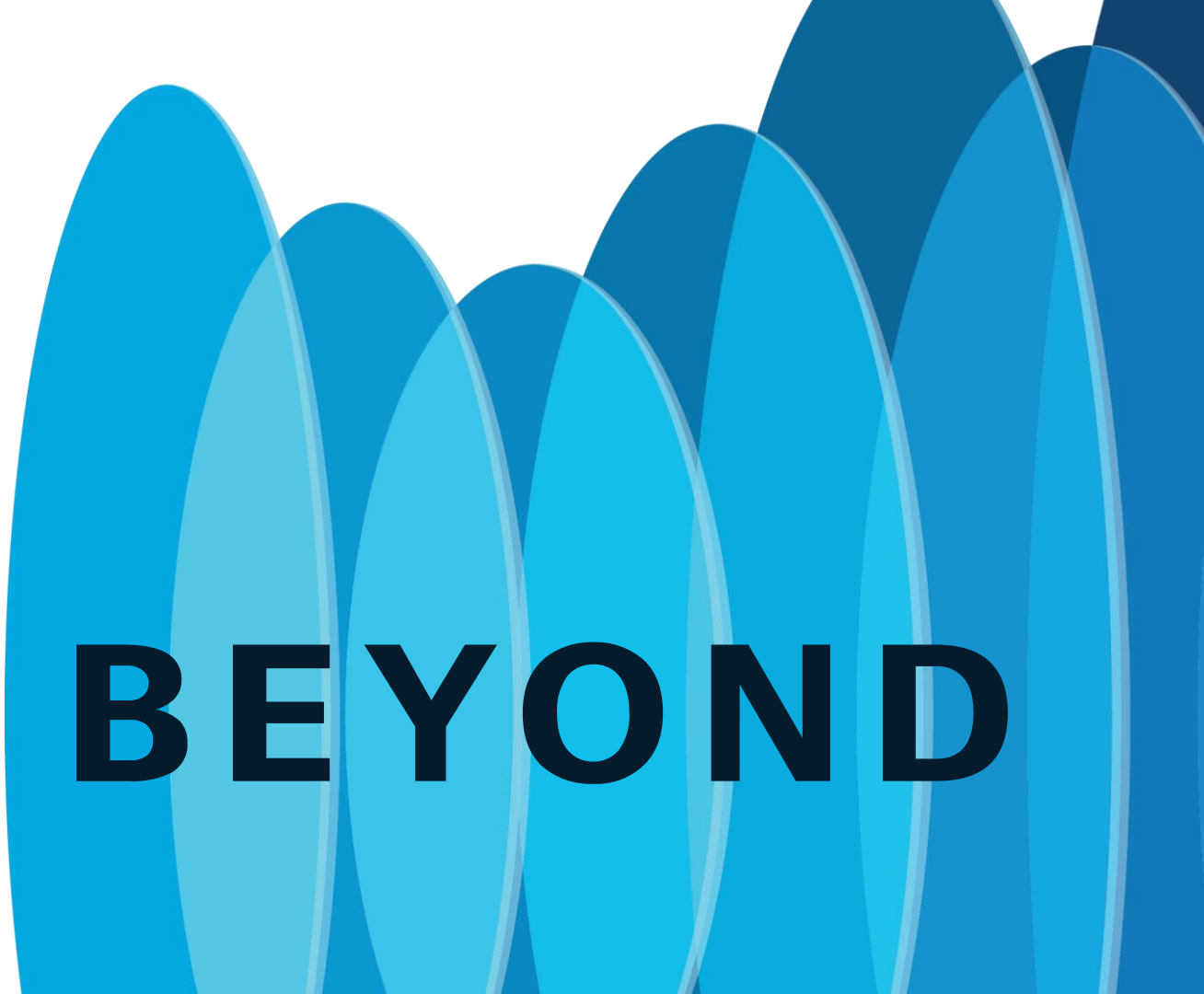
Continue your education

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

Contact me at: ekorneyc@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND