

Cisco ISE Meets Azure Cloud Deploy, Automate, Integrate with Entra ID and Intune

Eugene Korneychuk - Security Technical Leader BRKSEC-2416

cisco /

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



cisco / ille

Webex App

Questions?

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

How

- 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
- Enter messages/questions in the Webex space

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

cisco / illa



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













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

CISCO

Total Maximum Concurrent Active Sessions

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



cisco

Medium Deployment



Large Deployment

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	Medium Deployment			rge Deploym මෙන්නකර්ත මෙන්තකර්ත මෙන්තකර්ත මෙන්තකර මෙන්ත මෙන් + (කිලි මෙන් + (කිලි	ent

cisco Ne!

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_v 2* 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



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



cisco ive!

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 <u>implemented</u> the fixes: **East Asia** (eastasia) and **West Central** US (westcentralus)

Demo. ISE Azure Application Deployment

cisco ive!

C O A	https://portal.azure.cor	n/#home					150% 公	○ 6 约 6
Microsoft Azure		ources, services,	and docs (G+/)		💋 Cop	pilot 📐	Q 🕸 🛈	ନ୍ମ ekorneyc@cisco.c cxsɛcı
Azure services	5							
+		•		•••	DNS	DNS		♦
Create a resource	Network security groups	Virtual machines	Marketplace	Public IP addresses	Private DNS zones	DNS zones	Network security grou	Microsoft Entra ID
\rightarrow								
More services								
Resources <u> Recent</u> Favori	te							
Name				Туре			Last	Viewed
ISE1-Azure				Virtual mac	hine		11 n	ninutes ago
SAv-ekorney	/C			Virtual mac	hine		40 n	ninutes ago
间 ekorneyc-RG				Resource g	roup		41 n	ninutes ago
ASAv-Outside	-NSG			Network se	curity group		2 da	ys ago
ASAv-ekornev	c-SecurityGroup			Network se	curity group		2 da	vs 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 da machine. Don't use user data for storing y	ata that will be accessible to your applications throughout our secrets or passwords. Learn more about user data for '	the lifetime of the virtual VMs ♂
Enable user data	\checkmark	
User data *		
Performance (NVMe)		
Enable capabilities to enhance the perform	nance of your resources.	
Higher remote disk storage performance with NVMe \bigcirc	The selected image and size are not supported for NVMe See supported VM images and sizes C	a.

ISE as Azure Virtual Machine

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

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

Create Cisco Identity Services Engine (ISE) BYOL 3.4

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

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 * ①	cx-tac-rtp-aaa-azure (cxsecurity)	\sim
Resource group * ①		\sim
	Create new	
Instance details		
Region * ①	East US	\sim
Host Name * ①		
Time Zone * 🕕	Etc/UTC	\sim
VM Size * ()	Standard_F16s_v2	\sim
Disk Storage Type * ①	Premium SSD	\sim
Disk Encryption Key ①		\checkmark
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?

cisco ile!

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



cisco live!

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:

+ resource_group_name

#	azuı	rerm_linux_virtual_machine.ise-a	zur	re-1 will be created	
+	reso	ource "azurerm_linux_virtual_mack	nir	ne" "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)	

= "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





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="0SProvis ioningTimedOut" Message="0S Provisioning for W '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/LinuxMMLifecycle."

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="0SProvis ioningTimedOut" Message="0S 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 %



Virtual machine

> ? Feedback 🔼 ් හූ 🕛 🎛

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...

cisco ive!

Ansible

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

tasks)

of

(set

Play

ask



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

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

VM Common

 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 ive!



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



32



--- === 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



- --- === 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





PSN 2



--- === 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



--- === 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


- --- === 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







- --- === 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





cisco live!

- --- === 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



- --- === 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



- --- === Phase 4 === ---
 - Delete Primary PAN/MNT of old ۲ deployment
- Deploy the new instance to • destination ISF 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



PSN 2

PSN 4

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

>_
99
cisco Live!

- 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

cisco live!

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!

Entra ID Authentications

cisco live!

802.1x Authentication Problem with SAML

cisco / ile !

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				

cisco ive!

Active Directory User vs Entra ID User

	Published Certificate Member Of Password Replication Dal-in Object Security Environment Sessions Remote control General Address Account Profile Telephones Organization monica m		User principal name Object ID Created date time User type	ecurity.onmicrosoft.com alice@cxsecurity.onmicrosoft.com f43b00a4-5604-4936-8b0c-7f4ffbd8c4b2 Dec 4, 2022, 1:02 PM Member
Aspect		r	Identities Group memberships 4 Applications 5 E	cxsecurity.onmicrosoft.com
Purpose		Represent U	ser Identity	
Identifier	User Principle Name (UPN), Distingu (DN), SID, sAMAccountName	uished Name	User Principle Name	e (UPN), Object ID
Management	Active Directory, Group Policy (GPO)	Entra ID, Intune	
Source	Manual Creation		Manual Creation, Sy	nchronized via Entra Connect

cisco live!

Active Directory Computer vs Entra ID Device

	EXDRNEYC-WIN10 Properties ? × LAPS Location General Operating System Weiber OD Delegation Password Replacation W EXORNEYC-WIN10 Computer name (size-Windows 2000) EXORNEYC-WIN10 DNS name: ekorneyc-Win10 example com DC Type: Workstation or server Size:	Image: > Devices Windows > Windows devices > EKORNEYC-WIN11 Image: Provide Windows Windo		
Aspect	ctive Directory Computer	Entra ID Device		
Purpose	Represent Comput	er/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		

cisco live

Entra ID Device Join Types

Microsoft Azure

Home > cxsecurity | Devices > Devices | Overview >

All devices

$\overline{\uparrow}$	Download devices	🕐 Refresh	🔅 Manage view	\sim	\checkmark	Enable	\bigcirc	Disable	🗓 Delete	🔅 Manage	Preview features
Q	Search by name or de	evice ID or ob	ject ID						dd filters		

5 devices found

Name ↑↓	Enabled	OS	Version	Join type	MDM
ЈТООТНМА-АΖУМ	🕑 Yes	Windows	10.0.22621.3007	Microsoft Entra joined	Microsoft Intune
E NXHG8AA001922099	🕑 Yes	Unknown	Unknown	Microsoft Entra joined	None
DESKTOP-5FR9KQJ	🕑 Yes	Windows	10.0.19045.4412	Microsoft Entra registered	None
DESKTOP-ELL9K5S	🕑 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

cisco live!

Demo Topology

EAP-TLS Authorization with Entra ID

Demo. REST ID Store Authorization with EAP-TLS

cisco live!

Demo Topology

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

Intune Integration

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

Microsoft Intune admin center						
 ≪ ☆ Home ☑ Dashboard ☑ All spaces 	$\frac{\text{My Dashboard}}{\text{Private dashboard}} \sim \\ + \text{New dashboard} \sim \zeta$) Refresh 🛛 Z Full screen	🖉 Edit 🞍 Export 🗸 🗓	Clone 📋 Delete		
All services All services Device enrollment Apps Endpoint security Reports Users Device enrollment failures last 7 days		Device compliance	Device configuration OK © No policies with error or conflict	Welcome to the Microso Microsoft Intune gives you capabilities from the cloud, types, including Windows, i • Enroll and configure you • Upload and distribute yo • Protect your organizatior		
 Groups Tenant administration Troubleshooting + support 	Client apps	De	etails	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 De	vices	Device compliance statu Status	IS Devices	Please delete this tile This pinned part on the dashboard refers to a resource typ deprecated. Please remove this part from the dashboard.	be or service that is
	Windows	3	Compliant	1		
	Linux 0		In grace period	0		
	Android 0		Not evaluated	0		
	iOS/iPadOS 0		Not compliant	2 🕕		
	macOS 0		Total	3		
	Windows Mobile 0				<u>https://intur</u>	<u>e.microsoft.c</u>
	Total 3				om	

cisco ile

Problem with MAC address MDM Lookup

Micro	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						
் க		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 Uniqu	e Identifier						

(GUID)

Certificate with GUID

EAP-TLS with Azure Entra ID and Intune MDM

Demo. Intune MDM Integration

cisco live!

Deployment Topology



ISE Intune Integration Field Notices



<u>Field Notice: FN74227 - Cisco Identity Services Engine: Authentication and Certificate-Based Logins Will Fail</u> <u>Due to Microsoft Intune Security Identifier Changes - Software Upgrade Recommended</u>

Problem:

As part of Windows update May 10, 2022 (<u>KB5014754</u>: <u>Certificate-based authentication changes on Windows</u> <u>domain controllers</u>) 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 {{

> 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		•				ISE34-1ek_GigabitEthernet.pcap
			I 🙆 🗴 📕	🗋 ี 🔁 🚺	९ 🔶 🛸 警	T 🕹	_ = @ , Q , Q , !! !
		📕 tls.h	andshake.type == 1				
or		No.	Time	Source	Destination	Protocol	Lengt Info
	_		14 0.376116	10.48.26.64	10.48.26.63	TLSv1.2	<pre>391 Client Hello (SNI=ISE34-2ek.example.com)</pre>
CI.	Error		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)
	Connection to server failed with:	2	255 7.372347	10.48.26.64	10.48.26.63	TLSv1.2	354 Client Hello (SNI=ISE34-2ek.example.com)
		2	278 7.943812	10.48.26.64	64.103.36.133	TLSv1.2	322 Client Hello (SNI=www.ciscoconnectdna.com)
	MDM Server API error	5	588 19.959208	10.48.26.63	10.48.26.64	TLSv1.2	357 Client Hello (SNI=ISE34-1ek.example.com)
	Connection Failed to the MDM server: There is a problem with the server	6	549 22.814347	10.48.26.64	10.48.26.63	TLSv1.2	354 Client Hello (SNI=ISE34-2ek.example.com)
	Certificates or ISE trust store	6	586 24.302912	10.48.26.64	64.103.36.133	TLSv1.2	<pre>417 Client Hello (SNI=login.microsoftonline.com)</pre>
inc	Gentineates of ISE trust store.	7	23 24.573553	10.48.26.64	64.103.36.133	TLSv1.2	<pre>411 Client Hello (SNI=graph.microsoft.com)</pre>
	Please try with different settings	8	319 25.032051	10.48.26.64	64.103.36.133	TLSv1.2	<pre>417 Client Hello (SNI=login.microsoftonline.com)</pre>
	risdoo ay maranoione ootango.	8	367 25.580248	10.48.26.64	64.103.36.133	TLSv1.2	393 Client Hello (SNI=fef.msua08.manage.microsoft.com)
0							
an	ОК		1 V	Vireshark fill	ter: tis.handsha	ake.type	e == 1, to filter Client Hello
e			n l	nessages			
qu							
atus. Us	CO ISE ISSUES A CHANGE OF AUTIONZATION.						



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



2

Intune Integration Troubleshooting



NUN	W117							
	Mark/Upmark Salastad		•	•				ISE34-1ek_GigabitEthernet.pcap
	Ignore/Unignore Selected #D			i 🧶 🖲	S 🕺 🗋	۹ 🔶 😫	T 👱	💶 🔳 @, @, @, 🎚 🗄
	Set/Unset Time Reference #T		📕 tcp	stream eq 39.				
			No.	∧ Time	Source	Destination	Protocol	Lengt Info
	Time Shift 公本1		- 1	859 25,480524	10,48,26,64	64,103,36,133	TCP	74 19284 → 80 [SYN] Seg=0 Win=29200 Len=0 MSS=1460 SACK PERM TSval=1
	Packet Comments		1	860 25.488783	64.103.36.133	10.48.26.64	TCP	74 80 → 19284 [SYN, ACK] Seg=0 Ack=1 Win=65535 Len=0 MSS=1300 WS=64 5
-				861 25.488865	10.48.26.64	64.103.36.133	TCP	66 19284 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1552436467 TSec
	Edit Resolved Name		1	862 25.489029	10.48.26.64	64.103.36.133	HTTP	195 CONNECT fef.msua08.manage.microsoft.com:443 HTTP/1.1
			1	863 25.496303	64.103.36.133	10.48.26.64	TCP	66 [TCP Window Update] 80 → 19284 [ACK] Seq=1 Ack=1 Win=262528 Len=0
	Apply as Filter		1	864 25.496361	64.103.36.133	10.48.26.64	TCP	66 80 → 19284 [ACK] Seq=1 Ack=130 Win=262400 Len=0 TSval=1526620621
			1	865 25.579714	64.103.36.133	10.48.26.64	HTTP	105 HTTP/1.1 200 Connection established
	Prepare as Filter		1	866 25.579780	10.48.26.64	64.103.36.133	TCP	66 19284 → 80 [ACK] Seq=130 Ack=40 Win=29312 Len=0 TSval=1552436558
	Conversation Filter		1	867 25.580248	10.48.26.64	Expand Subtrees		93 Client Hello (SNI=fef.msua08.manage.microsoft.com)
			1	868 25.588333	64.103.36.133	Collapse Subtrees		66 80 → 19284 [ACK] Seq=40 Ack=457 Win=262208 Len=0 TSval=1526620711
	Colonze Conversation		+ 3	869 25.672873	64.103.36.133	Collapse All		154 80 → 19284 [ACK] Seq=40 Ack=457 Win=262528 Len=1188 TSval=15266208
	SCTP		+ 1	870 25.672957	64.103.36.133			160 Server Hello, Certificate, Server Key Exchange, Server Hello Done
	Follow ►	HTTP Stream て介出日		871 25.672984	10.48.26.64	Apply as Column	ራቹ	66 19284 → 80 [ACK] Seq=457 ACK=4422 W1n=38528 Len=0 ISVal=1552430652
				872 25.673463	10.48.26.64	Apply as Filter		73 Alert (Level: Fatal, Description: Certificate Unknown)
	Conv	TCP Stream 【公策】		8/3 25.6/3511	10.48.26.64	Prepare as Filter		66 19284 → 80 [FIN, ACK] Seq=464 Ack=4422 Win=38528 Len=0 ISval=15524
	Сору	TLS Stream て企業S		8/9 25.680/24	64.103.36.133	Conversation Filter		66 80 → 19284 [ACK] Seq=4422 ACK=464 Win=262528 Len=0 TSVal=15266208.
	- · · · · · · · · · · · · · · · · · · ·			880 25.680/80	64.103.36.133	Colorize with Filter		▶ 66 80 → 19284 [ALK] Seq=4422 ACK=465 W1n=262528 Len=0 ISVal=15266208.
	Protocol Preferences				04.103.30.133	Follow		► 00 80 → 19284 [FIN, ACK] Seq=4422 ACK=403 Win=202528 Len=0 ISVal=1520
	Decode As			582 23.081021	10.48.20.04	I/O Graph		00 19284 → 80 [ACK] Seq=405 ACK=4423 W1n=38528 Len=0 TSVal=1552430000
	Show Packet in New Window					Сору		•
	Show Facket III New Window			Londoholio D		Show Packet Bytes	۵¥	0
				V Handshake Pi	Turner Contifie	Export Packet Bytes	0% 0%	x
				Handshake	Type: Certific			
つ	Wiresnark: Right Click >	· FOIIOW > TCP		Cortifica:	tos Longth, 201	Wiki Protocol Page		
J,	Stream				tes (3016 bytes	Protocol Preferences		
	ououn			Certifi	cate Length: 24	1101000111010101000		
				> Certifi	cate []: 30820	Decode As	ዕ ዝ	U f83368f30cae620a871e00000112f833300d06092a864886f70d01010c0500305d310
				Certifi	cate Length: 14	Go to Linked Packet	and the state of t	105501500000112105550000052004000520040001010050050505050505050505050505050
				> Certifi	cate []: 30820	07105106204947005020		26449a5e3d1a38748f5dcfebcc300d06092a864886f70d01010c05003061310b30090
	Import Certificate into IS	SF Trusted Store		· Handshake Pi	rotocol. Server	Key Exchange		
-								
5	Administration > System	n > Certificates >				Locate	Server	Hello, Certificate message

4

Administration > System > Certificates > Trusted Certificates > Import

cisco live!

BRKSEC-2416 © 2025 Cisco and/or its affiliates. All rights reserved. Cisco Public 76

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

- 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
- Enter messages/questions in the Webex space

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

cisco / illa



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'





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 <u>ciscolive.com/on-demand</u>.
 Sessions from this event will be available from March 3.

Contact me at: ekorneyc@cisco.com



Thank you

cisco Live!



GO BEYOND