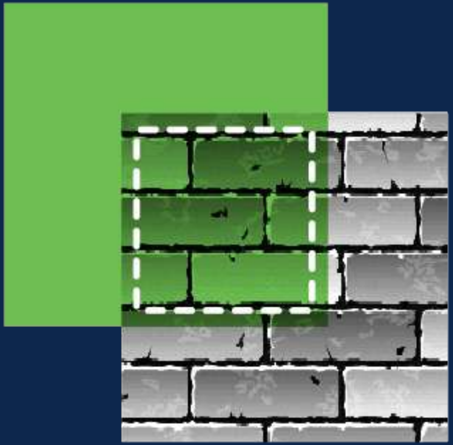
CISCO SECURE

CISCO The bridge to possible

Cisco ISE - Update

Tech Club



Jiří Tesař

TSA, jitesar@cisco.com

31.1.2023

Cisco Secure Zero Trust

A comprehensive approach to securing all access across your people, applications, and environments.

Workforce

Ensure only the right users and secure devices can access applications.

Workplace

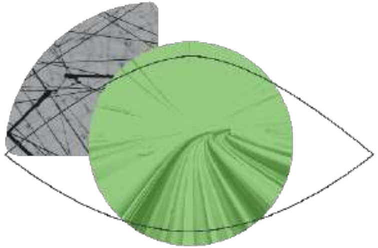
Secure all user and device connections across your network, including IoT.

Workloads

Secure all connections within your apps, across multi-cloud.

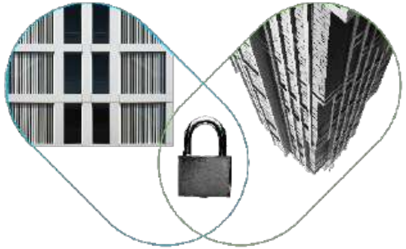
The Foundations of Zero Trust in Your Workplace

Visibility



Grant the right level of network access to users across domains

Segmentation



Shrink zones of trust and grant access based on least privilege

Containment

Automate containment of infected endpoints and revoke network access

ISE Provides Zero Trust for the Workplace

Enterprise

Security

Endpoints

- Users
- Devices
- Things

Network Devices

- Switches
- WLCs / APs
- VPN

Cisco ISE

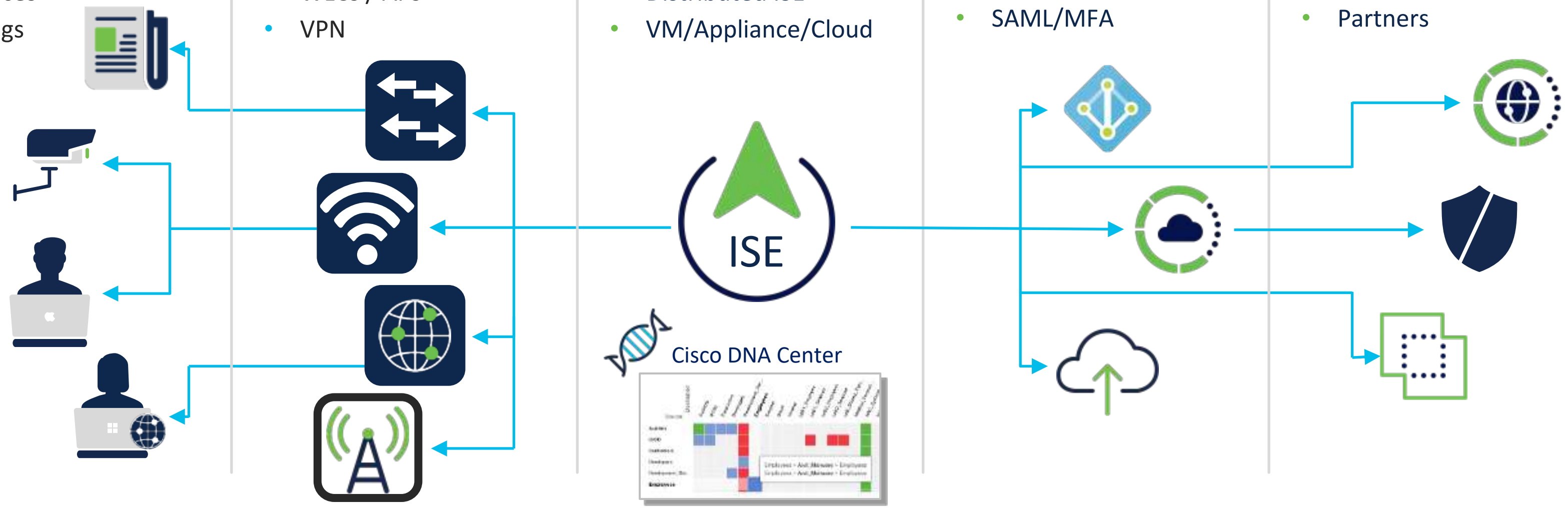
- Single ISE Evaluation
- Distributed ISE
- VM/Appliance/Cloud

Identity Services

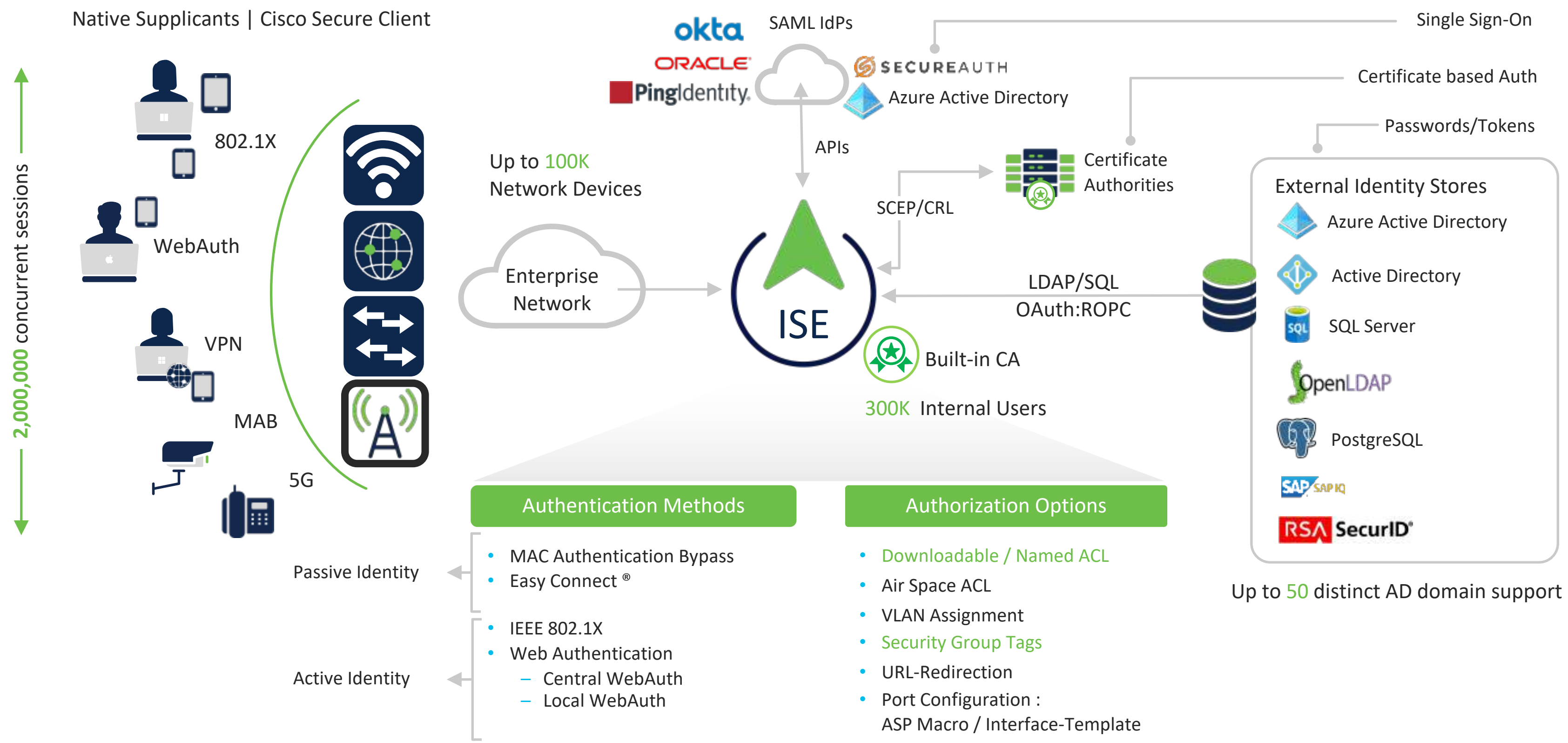
- Azure/AD/LDAP
- MDM
- SAML/MFA

Security Services

- Cloud Analytics
- Secure Firewall
- Partners



ISE Secure Access Control Options



Native Supplicants | Cisco Secure Client

2,000,000 concurrent sessions

802.1X

WebAuth

VPN

MAB

5G

okta

ORACLE

PingIdentity

SAML IdPs

SECUREAUTH

Azure Active Directory

Single Sign-On

Certificate based Auth

Passwords/Tokens

APIs

Up to 100K Network Devices

Enterprise Network

SCEP/CRL

Certificate Authorities

ISE

LDAP/SQL

OAuth:ROPC

Built-in CA

300K Internal Users

External Identity Stores

- Azure Active Directory
- Active Directory
- SQL Server
- OpenLDAP
- PostgreSQL
- SAP SAP IQ
- RSA SecurID

Up to 50 distinct AD domain support

Authentication Methods

Passive Identity

- MAC Authentication Bypass
- Easy Connect ®

Active Identity

- IEEE 802.1X
- Web Authentication
  - Central WebAuth
  - Local WebAuth

Authorization Options

- Downloadable / Named ACL
- Air Space ACL
- VLAN Assignment
- Security Group Tags
- URL-Redirection
- Port Configuration :
  ASP Macro / Interface-Template

Why Customers Buy ISE

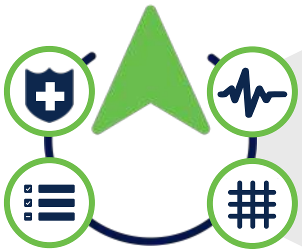
ISE

Device Administration	TACACS+ Migrating from Cisco Secure ACS or building a new Device Administration Policy Server, this allows for secure, identity-based access to the network devices
Secure Access	Allow wired, wireless, or VPN access to network resources based upon the identity of the user and/or endpoint. Use RADIUS with 802.1X, MAB, Easy Connect, or Passive ID
Guest Access	Differentiate between Corporate and Guest users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options
Asset Visibility	Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with Device Profiling. Automate access for many different IoT devices
Compliance & Posture	Use agentless posture, Cisco Secure Client, MDM, or EMM to check endpoints to verify compliance with policies (Patches, AV, AM, USB, etc.) before allowing network access
Context Exchange	pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase Network Visibility and facilitate automated Enforcement.
Segmentation	Group-based Policy allows for segmentation of the network through the use of Security Group Tags (SGT) and Security Group ACLs (SGACL) instead of VLAN/ACL segmentation.
Cisco SDA/DNAC	ISE integrates with DNA Center to automate the network fabric and enforces the policies throughout the entire network infrastructure using Software-Defined Access (SDA)
BYOD	Allow employees to use their own devices to access network resources by registering their device and downloading certificates for authentication through a simple onboarding process
Threat Containment	Using a Threat Analysis tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results

ISE Architecture

cs.co/ise-scale

Standalone ISE



Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes

Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes

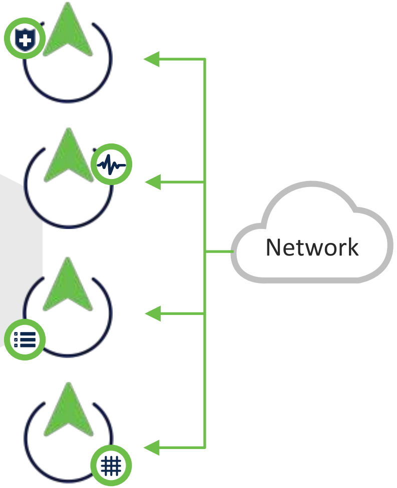
Policy Services Node (PSN)

- Makes policy decisions
- RADIUS / TACACS+ Servers

pxGrid Controller (PXG)

- Facilitates sharing of context

Distributed ISE



Single Node (Virtual/Appliance)	|||||	Multiple Nodes (Virtual/Appliance)
Up to **20,000** concurrent endpoints	3500	Up to **500,000** concurrent endpoints
Up to **50,000** concurrent endpoints	3600	Up to **2,000,000** concurrent endpoints

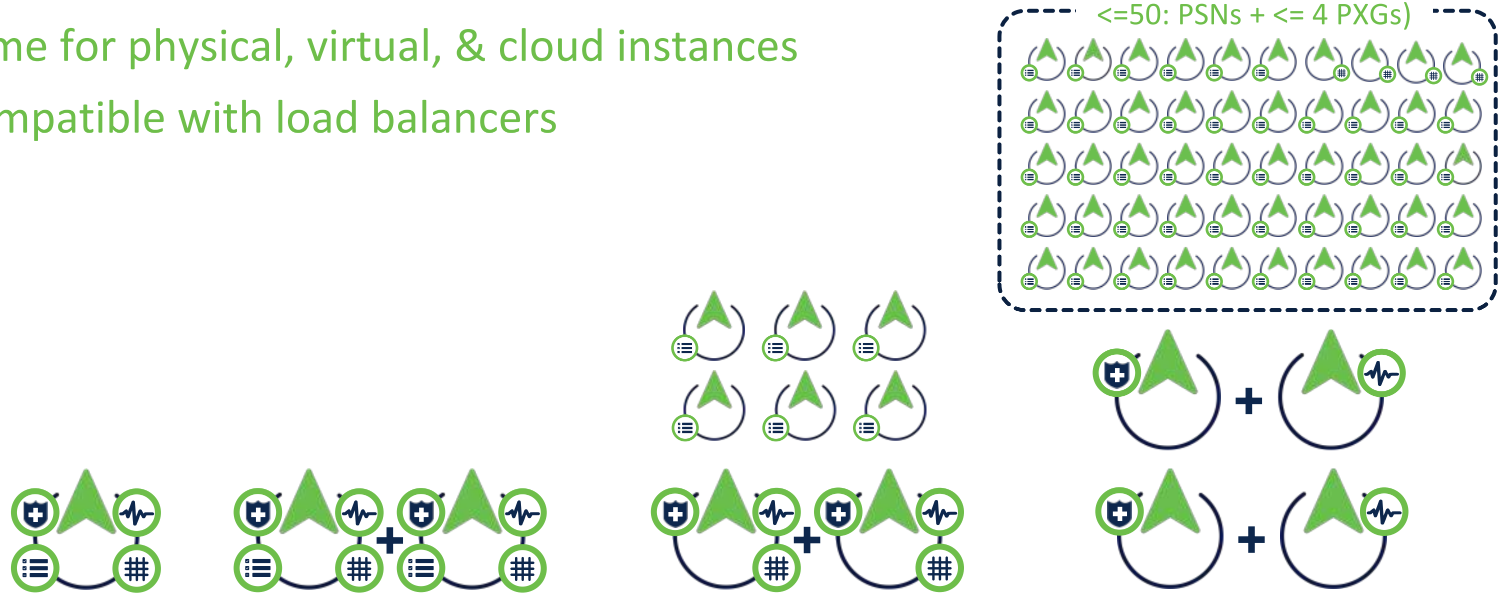
ISE Deployment Scale

cs.co/ise-scale

2.6+

Same for physical, virtual, & cloud instances

Compatible with load balancers



Lab and Evaluation

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

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

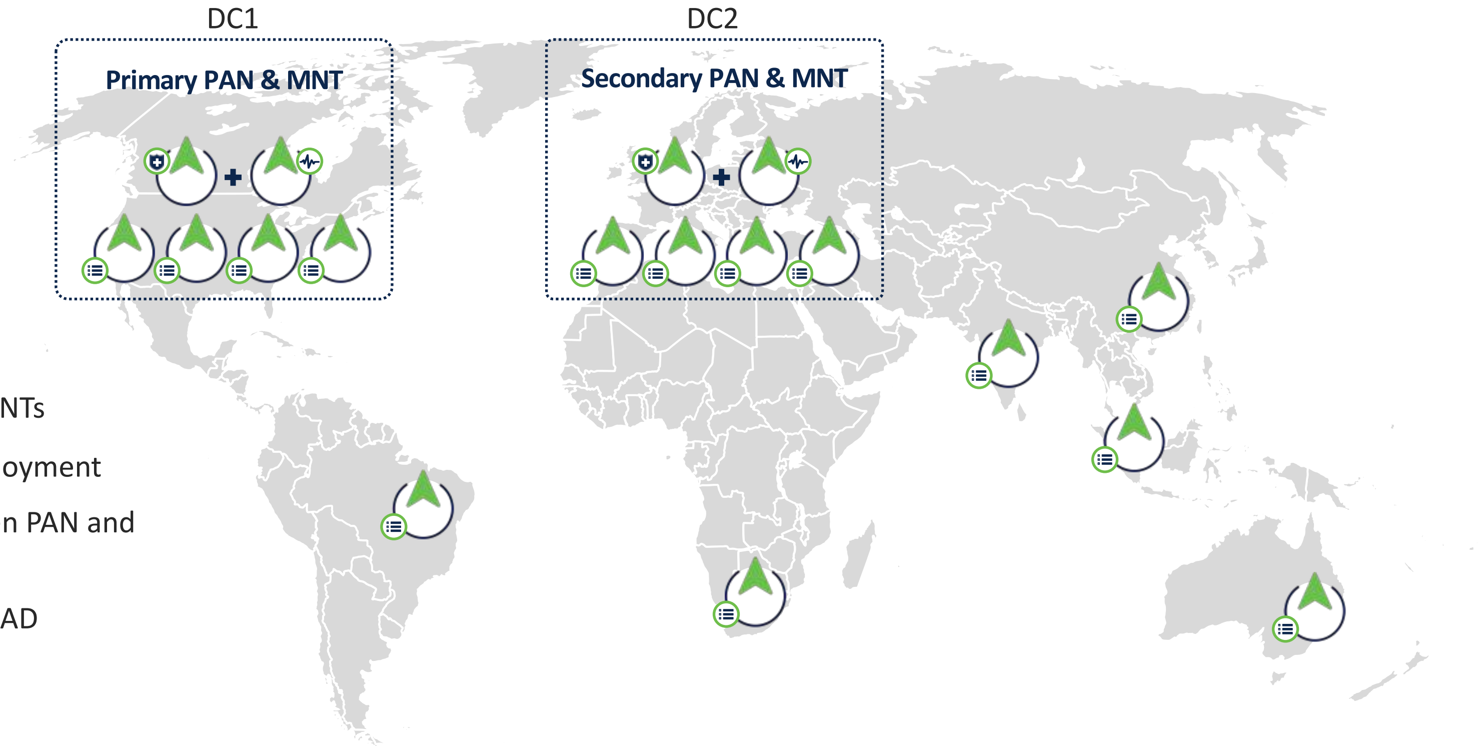
Large Deployment
2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

100 Endpoints	Up to 20,000 Endpoints	Up to 500,000 Endpoints	3500
100 Endpoints	Up to 50,000 Endpoints	Up to 2,000,000 Endpoints	3600

cisco SECURE

ISE Fully Distributed Architecture

- Centralize in DCs…or Distribute PSNs across Geographies



- Separate PAN and MNTs
- 50 PSN max per deployment
- 300ms delay between PAN and other ISE nodes
- Co-locate PSNs with AD

ISE Nodes – Mix and Match

Physical Appliances

SNS-3695
SNS-3655
SNS-3615
SNS-3595
SNS-3515

Virtual Machines

KVM

Microsoft

NUTANIX

vmware®

Cloud Instances

aws

Azure

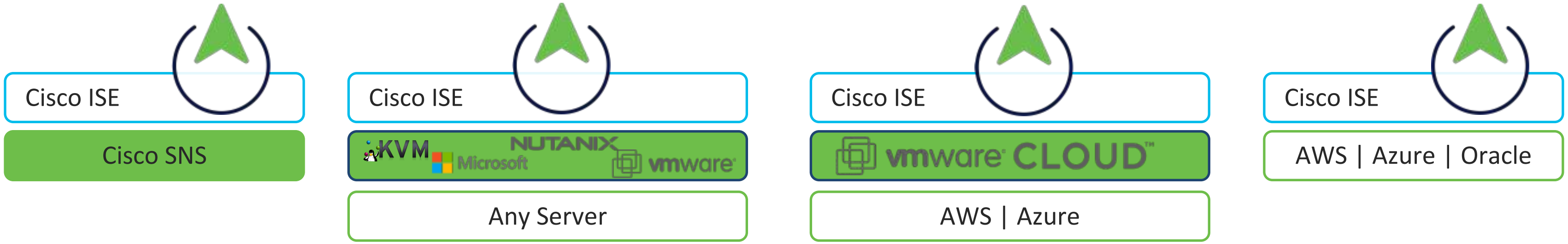
ORACLE

Future

Google

ISE 3.2 Supported Platforms

See Deploy Cisco ISE Natively on Cloud Platforms for provider instance types and XS/S/M/L node sizing



	Appliances	Standalone Sessions	PSN Sessions	Processor	Cores	Memory	Disk	RAID	Network Interfaces
	SNS-3615	10,000	10,000	1- intel Xeon 2.10 GHz 4110	8	32 GB (2 x 16 GB)	1 (600GB)	No	2x10Gbase-T 4x1GBase-T
	SNS-3655	25,000	50,000	1 – Intel Xeon 2.10 GHz 4116	12	96 GB (6 x 16 GB)	4 (600 GB)	10	2x10Gbase-T 4x1GBase-T
	SNS-3695	50,000	100,000	1 – Intel Xeon 2.10 GHz 4116	12	256 GB (8 x 32 GB)	8 (600 GB)	10	2x10Gbase-T 4x1GBase-T
EOL	~~SNS-3515~~	~~7500~~	~~7500~~	~~1 – Intel Xeon 2.40GHz E5-2620~~	~~6~~	~~16 GB~~ ~~(2 x 8 GB)~~	~~1 (600 GB)~~	~~NO~~	~~6x1GBase-T~~
	SNS-3595	20,000	40,000	1 – Intel Xeon 2.60 GHz E5-2640	8	64 GB (4 x 16 GB)	4 (600 GB)	10	6x1GBase-T

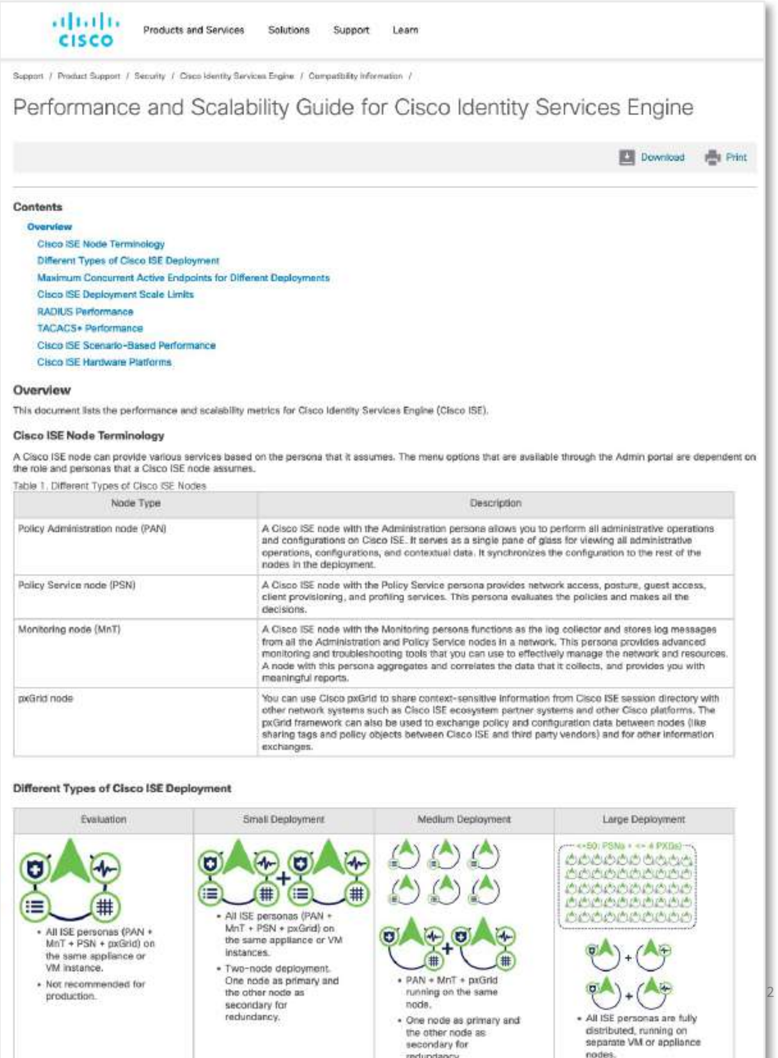
* SNS-3515 no longer supported with ISE 3.1

* VMWare version 6.5+ required

ISE Performance & Scale

cs.co/ise-scale

- Deployment Architectures: S / M / L
- Maximum Concurrent Active Sessions
- Deployment Scale Limits
- Protocol Performance
- Scenario Performance



Support / Product Support / Security / Cisco Identity Services Engine / Compatibility Information /

Performance and Scalability Guide for Cisco Identity Services Engine

Contents

Overview

This document lists the performance and scalability metrics for Cisco Identity Services Engine (Cisco ISE).

Cisco ISE Node Terminology

A Cisco ISE node can provide various services based on the persona that it assumes. The menu options that are available through the Admin portal are dependent on the role and personas that a Cisco ISE node assumes.

Table 1. Different Types of Cisco ISE Nodes

Node Type	Description
Policy Administration node (PAN)	A Cisco ISE node with the Administration persona allows you to perform all administrative operations and configurations on Cisco ISE. It serves as a single pane of glass for viewing all administrative operations, configurations, and contextual data. It synchronizes the configuration to the rest of the nodes in the deployment.
Policy Service node (PSN)	A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions.
Monitoring node (MnT)	A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service nodes in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage the network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports.
pxGrid node	You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as Cisco ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes (like sharing tags and policy objects between Cisco ISE and third party vendors) and for other information exchanges.

Different Types of Cisco ISE Deployment

Evaluation	Small Deployment	Medium Deployment	Large Deployment
• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM instance. • Not recommended for production.	• All ISE personas (PAN + MnT + PSN + pxGrid) on the same appliance or VM instances. • Two-node deployment. One node as primary and the other node as secondary for redundancy.	• PAN + MnT + pxGrid running on the same node. • One node as primary and the other node as secondary for redundancy.	<=50: PSNs + <= 4 PXGs • All ISE personas are fully distributed, running on separate VM or appliance nodes.

ISE 3.0

- Platform Support: VMware Cloud on AWS
- New Interface Look and Feel
- SAML SSO with Azure AD (ISE web portals)
- 802.1X with Azure AD (using EAP-TTLS (PAP) + OAuth/ROPC)
- Agentless Posture on Windows & macOS
- Endpoint Visibility with Custom Scripts
- ODBC Multiple Attributes Lookup
- Certificate Pinning for Multiple CAs
- PassiveID with Windows Eventing APIs (WMI => MS RPC API)
- Device Identifier Changes for Windows Devices (MDM, MAC)
- Baselines Policies with Microsoft SCCM (MDM, & baseline pol.)
- Posture AV/AM Minimum Version
- Posture Session Status Sharing
- Health Checks (usage case: prior to upgrade)
- Make a Wish
- Debug Wizard by Function (debug profile for more ISE nodes)
- TCP Dump Improvements (file size, number of files,..)
- License Changes

Agentless Posture on Windows & macOS

3.0

Problem

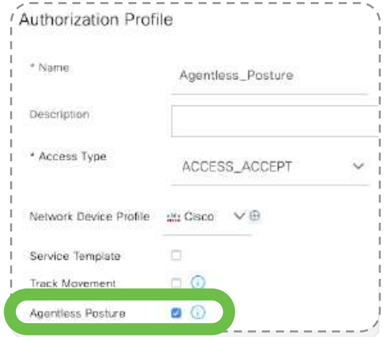
While endpoint compliance is the basis for endpoint trust, customers have to rely on persistent agent for endpoint compliance

Solution

ISE provides an option to get endpoint compliance based on a plugin which doesn't require installation of persistent agent on endpoints

Caveats / Prerequisites

Requires administrator credentials.
No support for remediation, grace period, re-assessment, or AUP



Authorization Profile

* Name: Agentless_Posture

Description:

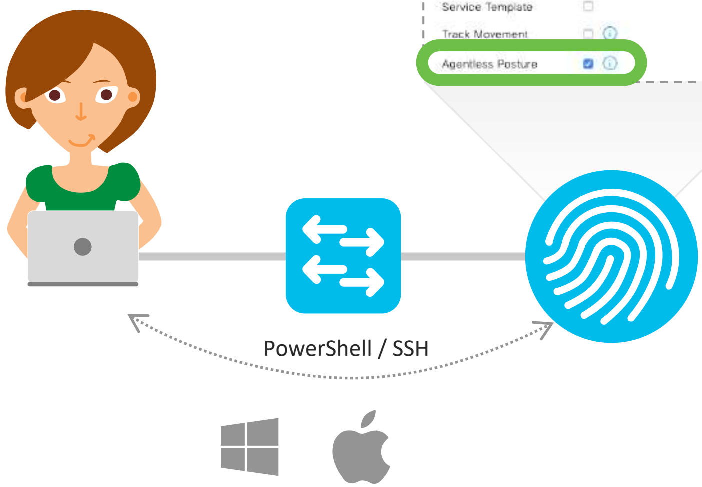
* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template □

Track Movement □

Agentless Posture ☑



Linux Support added in ISE 3.1

Posture Deployment Options

✓ Supported
! Limitations
✗ Not Supported

Capability	AnyConnect			AC Stealth		Temporal		Agentless	
	🪟	🍎	🐧	🪟	🍎	🪟	🍎	🪟	🍎
Anti-Malware Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Firewall Installation Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
Application Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Hardware Inventory	✓	✓	✗	✓	✓	✓	✓	✓	✓
Process Checks	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dictionary Conditions	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application Checks	✓	✓	✗	✓	✓	✓	✓	✓	✓
File Checks	✓	✓	!	✓	✓	✓	✓	!	✓
Service Checks	✓	✓	✗	✓	✓	✓	!	✓	!
Disk Encryption	✓	✓	✗	✓	✓	!	!	!	!
Patch Management	✓	✓	!	✓	✓	!	!	!	!
Registry Checks	✓	N/A	N/A	✓	N/A	✓	N/A	!	N/A
USB Checks	✓	✗	✗	✓	✗	✓	✗	✓	✗
WSUS remediation (legacy)	✓	N/A	N/A	✓	N/A	✗	✗	✗	✗
Remediation	Auto, Manual	Partial	Partial	Part Auto	Partial	Text	Text	✗	✗
Reassessment	✓	✓	✓	✓	✓	✗	✗	✗	✗

Visibility (Less Effort)

Experience (Less Time)

Security (More Protection)

Cisco pxGrid 2.0

ISE 3.1 Deprecates pxGrid 1.0

	pxGrid 1.0	pxGrid 2.0
Protocol	XMPP	WebSockets & REST
Ports	Two (TCP 5222 & 7400)	One (TCP 8910)
Service redundancy	No (No HA)	Yes
Scale and performance	Low – Limited integrations (5,000 KB/s for 4 subscribers)	High – Scalable integrations (100,000 KB/s agg. for 150 subscribers)
Client-side development	Java or C	Any language
Support	From ISE 1.3	From ISE 2.4
	Not supported in 3.1	

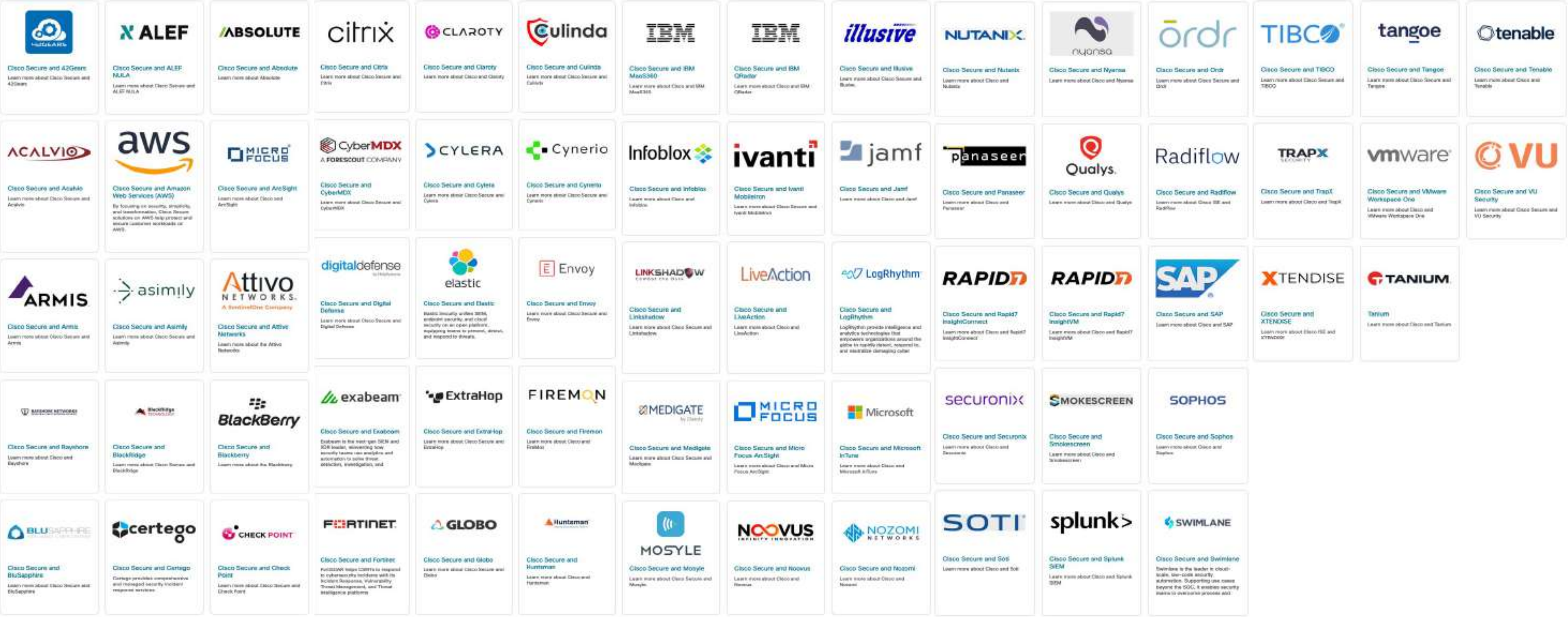
More at http://bit.ly/pxgrid2-0

All Cisco products now support pxGrid 2.0!

Product	Min Version
Cisco Firepower	6.0
Cisco Stealthwatch Enterprise	7.3.2
Cisco Cyber Vision	3.1.0
Cisco Web Security Appliance	11.7
Cisco Industrial Network Director	1.3
Cisco DNA Center	2.1.0

Cisco ISE Security Technical Alliance Partners

Sep 2022



Cisco Secure and 42Gears
Learn more about Cisco Secure and 42Gears

Cisco Secure and ALEF NULA
Learn more about Cisco Secure and ALEF NULA

Cisco Secure and Absolute
Learn more about Absolute

Cisco Secure and Citrix
Learn more about Cisco Secure and Citrix

Cisco Secure and Claroty
Learn more about Cisco and Claroty

Cisco Secure and Culinda
Learn more about Cisco Secure and Culinda

Cisco Secure and IBM MaaS360
Learn more about Cisco and IBM MaaS360

Cisco Secure and IBM QRadar
Learn more about Cisco and IBM QRadar

Cisco Secure and Illusive
Learn more about Cisco Secure and Illusive

Cisco Secure and Nutanix
Learn more about Cisco and Nutanix

Cisco Secure and Nyansa
Learn more about Cisco and Nyansa

Cisco Secure and Ordr
Learn more about Cisco Secure and Ordr

Cisco Secure and TIBCO
Learn more about Cisco Secure and TIBCO

Cisco Secure and Tangoe
Learn more about Cisco Secure and Tangoe

Cisco Secure and Tenable
Learn more about Cisco and Tenable

Cisco Secure and Acalvio
Learn more about Cisco Secure and Acalvio

Cisco Secure and Amazon Web Services (AWS)
By focusing on security, simplicity, and transformation, Cisco Secure solutions on AWS help protect and secure customer workloads on AWS.

Cisco Secure and ArcSight
Learn more about Cisco and ArcSight

Cisco Secure and CyberMDX
Learn more about Cisco Secure and CyberMDX

Cisco Secure and Cylera
Learn more about Cisco Secure and Cylera

Cisco Secure and Cynerio
Learn more about Cisco Secure and Cynerio

Cisco Secure and Infoblox
Learn more about Cisco and Infoblox

Cisco Secure and Ivanti MobileIron
Learn more about Cisco Secure and Ivanti MobileIron

Cisco Secure and Jamf
Learn more about Cisco and Jamf

Cisco Secure and Panaseer
Learn more about Cisco and Panaseer

Cisco Secure and Qualys
Learn more about Cisco and Qualys

Cisco Secure and Radiflow
Learn more about Cisco ISE and Radiflow

Cisco Secure and TrapX
Learn more about Cisco and TrapX

Cisco Secure and VMware Workspace One
Learn more about Cisco and VMware Workspace One

Cisco Secure and VU Security
Learn more about Cisco Secure and VU Security

Cisco Secure and Armis
Learn more about Cisco Secure and Armis

Cisco Secure and Asimily
Learn more about Cisco Secure and Asimily

Cisco Secure and Attivo Networks
Learn more about the Attivo Networks

Cisco Secure and Digital Defense
Learn more about Cisco Secure and Digital Defense

Cisco Secure and Elastic
Elastic Security unifies SIEM, endpoint security, and cloud security on an open platform, equipping teams to prevent, detect, and respond to threats.

Cisco Secure and Envoy
Learn more about Cisco Secure and Envoy

Cisco Secure and Linkshadow
Learn more about Cisco Secure and Linkshadow

Cisco Secure and LiveAction
Learn more about Cisco and LiveAction

Cisco Secure and LogRhythm
LogRhythm provide intelligence and analytics technologies that empowers organizations around the globe to rapidly detect, respond to, and neutralize damaging cyber

Cisco Secure and Rapid7 InsightConnect
Learn more about Cisco and Rapid7 InsightConnect

Cisco Secure and Rapid7 InsightVM
Learn more about Cisco and Rapid7 InsightVM

Cisco Secure and SAP
Learn more about Cisco and SAP

Cisco Secure and XTENDISE
Learn more about Cisco ISE and XTENDISE

Tanium
Learn more about Cisco and Tanium

Cisco Secure and Rayshore
Learn more about Cisco and Bayshore

Cisco Secure and BlackRidge
Learn more about Cisco Secure and BlackRidge

Cisco Secure and Blackberry
Learn more about the Blackberry

Cisco Secure and Exabeam
Exabeam is the next-gen SIEM and XDR leader, reinventing how security teams use analytics and automation to solve threat detection, investigation, and

Cisco Secure and ExtraHop
Learn more about Cisco Secure and ExtraHop

Cisco Secure and Firemon
Learn more about Cisco and Firemon

Cisco Secure and Medigate
Learn more about Cisco Secure and Medigate

Cisco Secure and Micro Focus ArcSight
Learn more about Cisco and Micro Focus ArcSight

Cisco Secure and Microsoft InTune
Learn more about Cisco and Microsoft InTune

Cisco Secure and Securonix
Learn more about Cisco and Securonix

Cisco Secure and Smokescreen
Learn more about Cisco and Smokescreen

Cisco Secure and Sophos
Learn more about Cisco and Sophos

Cisco Secure and BluSapphire
Learn more about Cisco Secure and BluSapphire

Cisco Secure and Certego
Certego provides comprehensive and managed security incident response services.

Cisco Secure and Check Point
Learn more about Cisco Secure and Check Point

Cisco Secure and Fortinet
FortiSOAR helps CSIRTs to respond to cybersecurity incidents with its Incident Response, Vulnerability Threat Management, and Threat Intelligence platforms

Cisco Secure and Globo
Learn more about Cisco Secure and Globo

Cisco Secure and Huntsman
Learn more about Cisco and Huntsman

Cisco Secure and Mosyle
Learn more about Cisco Secure and Mosyle

Cisco Secure and Noovus
Learn more about Cisco and Noovus

Cisco Secure and Nozomi
Learn more about Cisco and Nozomi

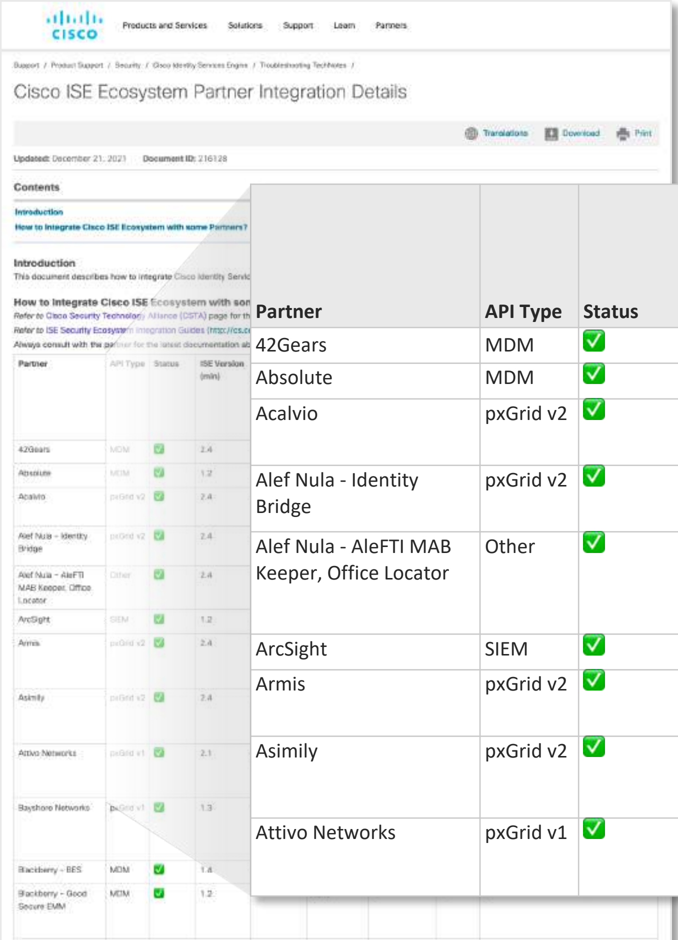
Cisco Secure and Soti
Learn more about Cisco and Soti

Cisco Secure and Splunk SIEM
Learn more about Cisco and Splunk SIEM

Cisco Secure and Swimlane
Swimlane is the leader in cloud-scale, low-code security automation. Supporting use cases beyond the SOC, it enables security teams to overcome process and

cisco.com/go/csta

Cisco ISE Ecosystem Partner Integration Details



cisco
Products and Services
Solutions
Support
Learn
Partners
Support / Product Support / Security / Cisco Identity Services Engine / Troubleshooting TechNotes /
Translations
Download
Print

Cisco ISE Ecosystem Partner Integration Details

Updated: December 21, 2021 **Document ID:** 216128

Contents

Introduction
How to Integrate Cisco ISE Ecosystem with some Partners?

Introduction

This document describes how to integrate Cisco Identity Servic

How to Integrate Cisco ISE Ecosystem with son

Refer to Cisco Security Technology Alliance (CSTA) page for th

Refer to ISE Security Ecosystem Integration Guides (http://cs.c

Always consult with the partner for the latest documentation ab

Partner	API Type	Status	ISE Version (min)
42Gears	MDM	✓	2.4
Absolute	MDM	✓	1.2
Acalvio	pxGrid v2	✓	2.4
Alef Nula – Identity Bridge	pxGrid v2	✓	2.4
Alef Nula – AleFTI MAB Keeper, Office Locator	Other	✓	2.4
ArcSight	SIEM	✓	1.2
Armis	pxGrid v2	✓	2.4
Asimily	pxGrid v2	✓	2.4
Attivo Networks	pxGrid v1	✓	2.1
Bayshore Networks	pxGrid v1	✓	1.3
Blackberry – BES	MDM	✓	1.4
Blackberry – Good Secure EMM	MDM	✓	1.2

cs.co/ise-ecosystem-partners

Partner	API Type	Status	ISE Version (min)	Partner Version (min)	RTC Type	RTC Action (pxGrid)	ISE Authz Policy (EPS, ANC)	pxGrid Topics/Attributes
42Gears	MDM	✓	2.4	-	None	-	-	-
Absolute	MDM	✓	1.2	-	None	-	-	-
Acalvio	pxGrid v2	✓	2.4	4.0	pxGrid	Automated via policy	ANC	-
Alef Nula - Identity Bridge	pxGrid v2	✓	2.4	-	None	-	-	Session - Identity Bridge (replaces CDA type functionality with ASA)
Alef Nula - AleFTI MAB Keeper, Office Locator	Other	✓	2.4	-	None	-	-	-
ArcSight	SIEM	✓	1.2	-	EPS REST	-	-	-
Armis	pxGrid v2	✓	2.4	-	pxGrid	Manual via GUI	ANC	Topic Subscribes: ANC
Asimily	pxGrid v2	✓	2.4	20.10	pxGrid	Manual via GUI (or automatic)	ANC	Session ERS API calls to configure ACL
Attivo Networks	pxGrid v1	✓	2.1	ATV Botsink 4.0	pxGrid	Manual via GUI	EPS	Topic Subscribes: EndpointProtectionService

ISE Security Ecosystem Integration Guides

Sep 2022

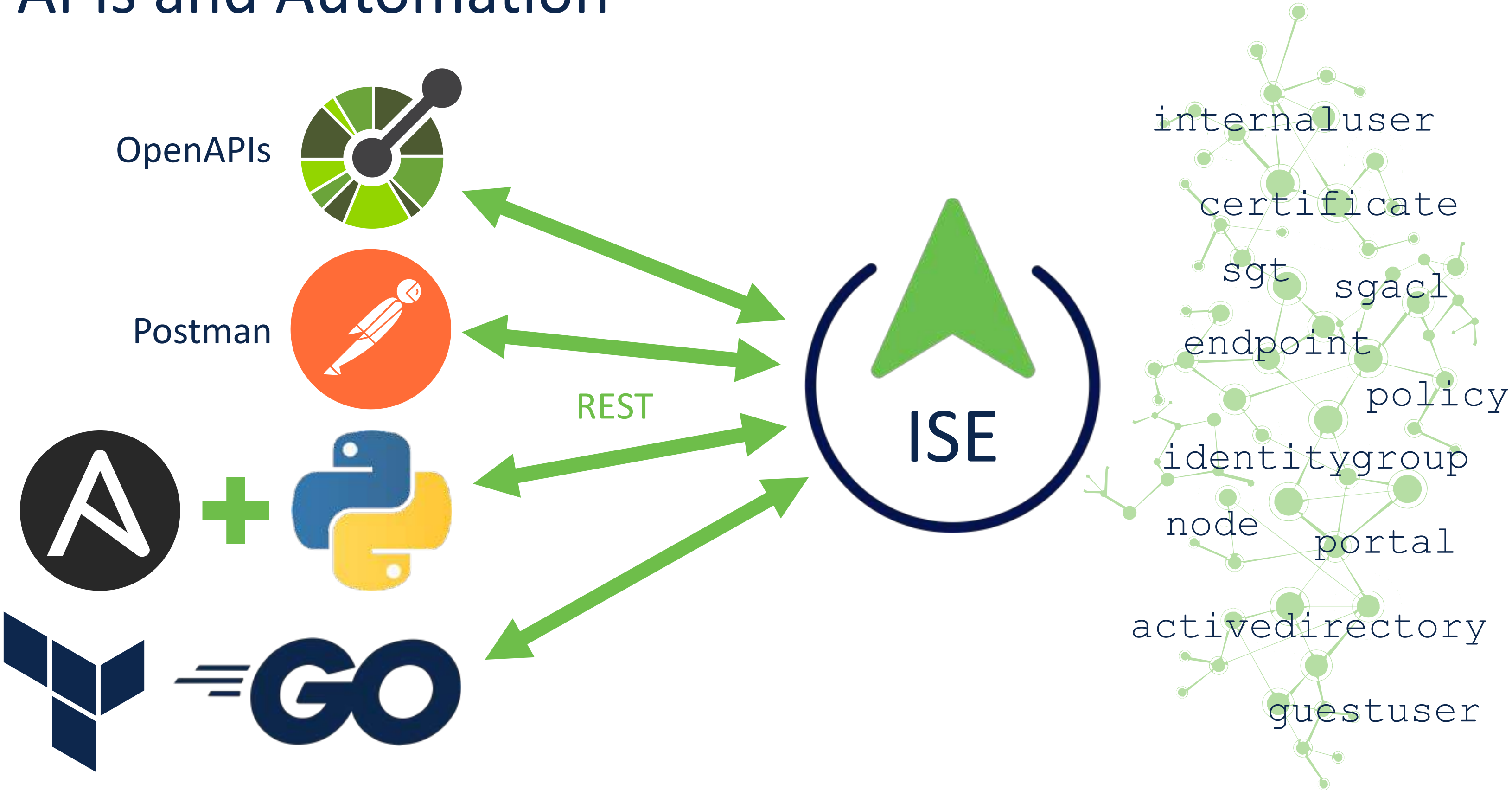
Configuration guides for all ISE integrations, sorted by **Vendor** and **Product**!

cs.co/ise-guides

- AirWatch
- Acalvio (pxGrid, ANC)
- Alef (pxGrid)
- Amazon Web Services (AWS)
- Ansible
- Arista
- Armis (pxGrid - ERS API)
- Aruba
- Asimily
- Avaya
- Bayshore
- Blusapphire (pxGrid)
- Brocade
- Certego
- Certificates / Private Key Infrastructure (PKI)
- Checkpoint
- Cisco
- Cisco Adaptive Security Appliance (ASA)
- Cisco AI Endpoint Analytics
- Cisco Secure Client (formerly AnyConnect)
- Cisco Catalyst Wireless
- Cisco Cognitive Threat Analytics (CTA)
- Cisco CyberVision
- Cisco DNA Center (DNAC)
- Cisco Industrial Network Director (IND)
- Cisco IP Phones
- Cisco Meraki
- Cisco pxGrid (Platform Exchange Grid)
- Cisco pxGrid Cloud
- Cisco Prime Infrastructure
- Cisco Secure Access by Duo - formerly Cisco Duo
- Cisco Secure Endpoint - formerly Advanced Malware Protection (AMP)
- Cisco Secure Firewall - formerly NGFW or Firepower Management Center (FMC)
- Cisco Secure Network Analytics - formerly Cisco Stealthwatch
- Cisco Secure Workload - formerly Cisco Tetration
- Cisco Security Manager (CSM)
- Cisco Catalyst Switches
- Cisco TrustSec
- Cisco UCS / Cisco Integrated Management Center (CIMC)
- Cisco Umbrella
- Cisco Web Security Appliance (WSA)
- Cisco Webex Room Navigator
- Citrix XenMobile
- Compliance
- CyberArk (API)
- Cyber Observer (API)
- Cylera (pxGrid)
- Cynerio (pxGrid)
- Digital Defense by Help Systems
- DFLabs - Incman - (SOAR)
- EAP (Extensible Authentication Protocol)
- Envoy (Guest)
- ExtraHop (pxGrid)
- Extreme Networks
- F5
- Forescout
- Fortinet FortiManager/FortiGate - pxGrid
- Good (MDM)
- Google
- Google Android
- Google Chromebook
- HashiCorp
- Terraform
- HP
- Huawei
- IBM
- IBM MaaS360
- IBM QRadar (Syslog & pxGrid)
- InfoBlox (pxGrid)
- Ivanti (formerly MobileIron)
- Juniper
- KVM (Hypervisor)
- Lightweight Directory Access Protocol (LDAP)
- LinkShadow (pxGrid)
- Live Action (pxGrid)
- Logzilla (syslog)
- McAfee (pxGrid)
- Microsoft
- Microsoft Active Directory
- Microsoft Azure
- Microsoft Azure Active Directory
- Microsoft Endpoint Manager (MEM)
- Microsoft Hyper-V
- Microsoft Intune
- Microsoft System Center Configuration Manager (SCCM)
- Microsoft WSUS
- MicroTik (TACACs)
- Mobile Device Management (MDM)
- Motorola
- MySQL
- Nozomi (pxGrid)
- Nutanix
- Okta
- Open DataBase Connect (ODBC)
- Oracle
- Oracle Cloud Infrastructure (OCI)
- ORDR (formerly CloudPost)
- Palo Alto Networks
- IoT Security ISE Integration (ERS)
- IoT ISE pxGrid Integration
- Other Documents
- Ping Federate
- Postman
- Qualys (TC-NAC)
- RADIUS Servers
- Radiflow (pxGrid-ERS)
- Rapid7 (TC-NAC)
- REST (Representational State Transfer APIs)
- Rockwell
- RSA
- Ruckus
- Securonix (Syslog)
- ServiceNow (ERS API)
- Smokescreen - CarbonBlack now Zscaler (pxGrid)
- SMTP (Simple Mail Transfer Protocol)
- SMS
- Splunk (syslog, SOAR)
- Symantec
- TACACS (Terminal Access Controller Access-Control System) Protocol
- Tanium (pxGrid)
- Tenable Nessus (TC-NAC)
- ThreatConnect (SOAR)
- TrapX Labs DeceptionGrid (pxGrid)
- VMware
- vCenter
- XTENDISE

ISE APIs and Automation

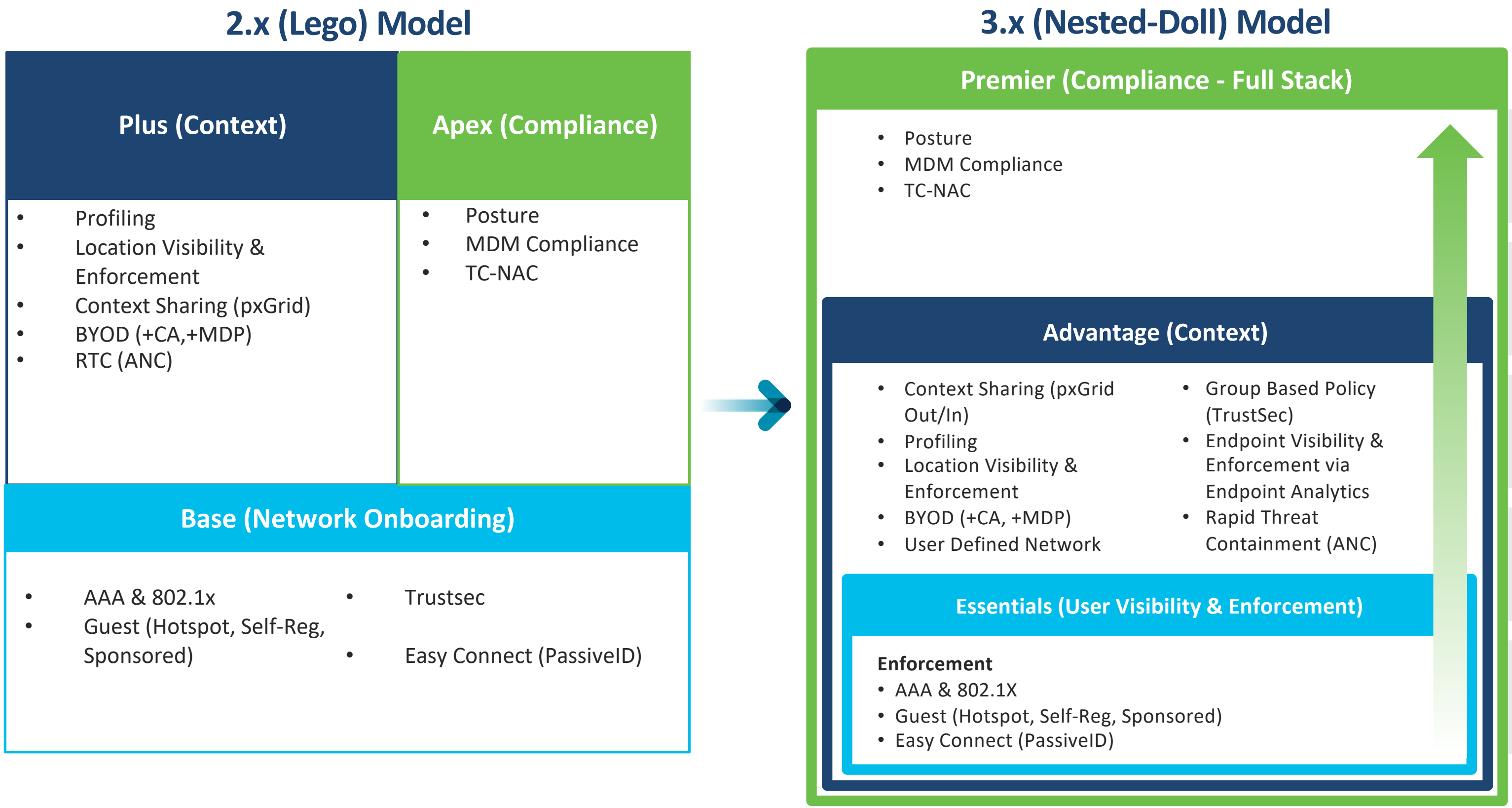
3.1



github.com/CiscoISE

ISE 3.x Licensing Model

cs.co/ise-licensing



2.x (Lego) Model

Plus (Context)

- Profiling
- Location Visibility & Enforcement
- Context Sharing (pxGrid)
- BYOD (+CA,+MDP)
- RTC (ANC)

Apex (Compliance)

- Posture
- MDM Compliance
- TC-NAC

Base (Network Onboarding)

- AAA & 802.1x
- Guest (Hotspot, Self-Reg, Sponsored)
- Trustsec
- Easy Connect (PassiveID)

3.x (Nested-Doll) Model

Premier (Compliance - Full Stack)

- Posture
- MDM Compliance
- TC-NAC

Advantage (Context)

- Context Sharing (pxGrid Out/In)
- Profiling
- Location Visibility & Enforcement
- BYOD (+CA, +MDP)
- User Defined Network
- Group Based Policy (TrustSec)
- Endpoint Visibility & Enforcement via Endpoint Analytics
- Rapid Threat Containment (ANC)

Essentials (User Visibility & Enforcement)

Enforcement

- AAA & 802.1X
- Guest (Hotspot, Self-Reg, Sponsored)
- Easy Connect (PassiveID)

Smart licensing only (Satellite, SLR available)

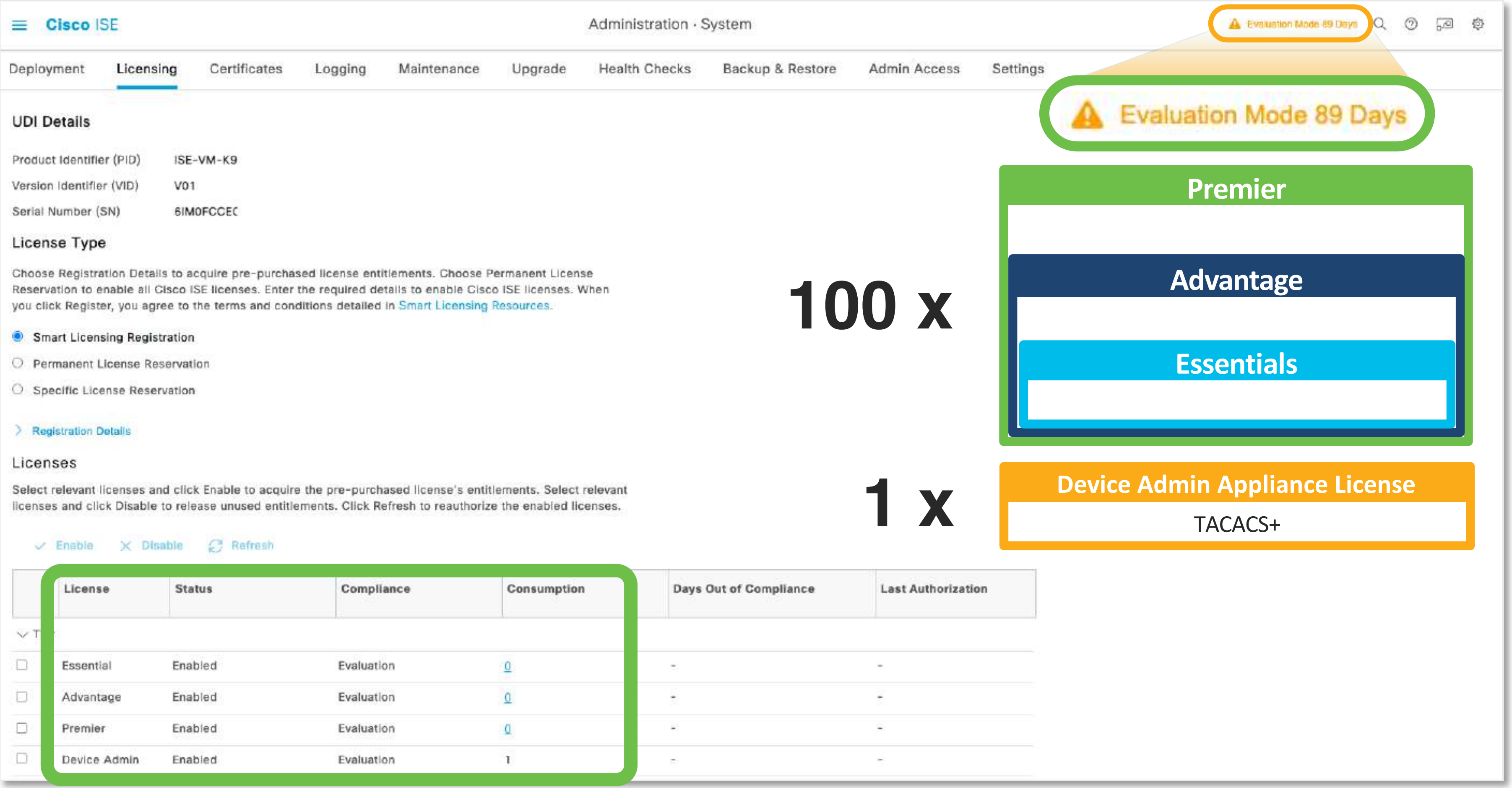
All Endpoint licenses are term-based

Single 'common' VM license (across all sizes & platforms/clouds)

Device Admin does not need endpoint licenses

Base → Essentials, term fixed for Oct 2023 expiry

Try ISE 3 for Free!   90-day Eval Licenses on Install!



UDI Details

Product Identifier (PID)	ISE-VM-K9
Version Identifier (VID)	V01
Serial Number (SN)	6IMOFCCEC

License Type

Choose Registration Details to acquire pre-purchased license entitlements. Choose Permanent License Reservation to enable all Cisco ISE licenses. Enter the required details to enable Cisco ISE licenses. When you click Register, you agree to the terms and conditions detailed in Smart Licensing Resources.

● Smart Licensing Registration

○ Permanent License Reservation

○ Specific License Reservation

> Registration Details

Licenses

Select relevant licenses and click Enable to acquire the pre-purchased license's entitlements. Select relevant licenses and click Disable to release unused entitlements. Click Refresh to reauthorize the enabled licenses.

✓ Enable   ✕ Disable   Refresh

	License	Status	Compliance	Consumption	Days Out of Compliance	Last Authorization
□	Essential	Enabled	Evaluation	0	-	-
□	Advantage	Enabled	Evaluation	0	-	-
□	Premier	Enabled	Evaluation	0	-	-
□	Device Admin	Enabled	Evaluation	1	-	-

⚠ Evaluation Mode 89 Days

100 x

Premier

Advantage

Essentials

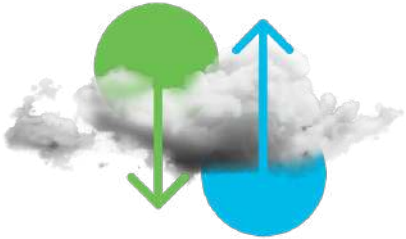
1 x

Device Admin Appliance License

TACACS+

ISE 3.2 Update

Cisco ISE 3.2 delivers:

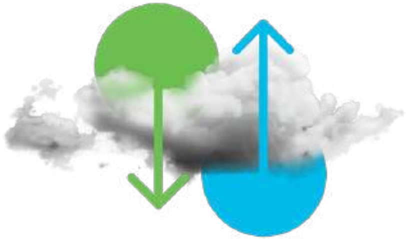


1. Cloud Ready, with Increased Flexibility

2. Infinitely Flexible Compliance

3. Flexible and Efficient Operations

Cisco ISE 3.2 delivers:



1. Cloud Ready, with Increased Flexibility

2. Infinitely Flexible Compliance

3. Flexible and Efficient Operations

ISE deployment on more public cloud platforms

Bring Your Own Licensing
Same license for VMs & Cloud instances
(R-ISE-VMC-K9=)

Expand as you grow
S/M/L instance sizes

Flexible deployment
ISE nodes on-prem and in cloud

Faster deployment
< 20 minutes (with Templates)

Reduced TCO
(Total Cost of Ownership)

amazon web services™
NEW
Microsoft Azure
NEW
ORACLE CLOUD

EAP-TLS & TEAP Authorization with Azure AD

Problem

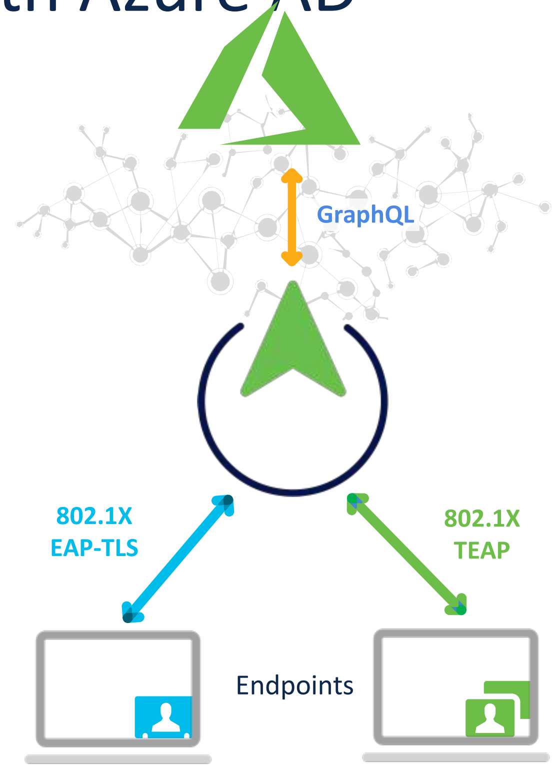
As organizations migrate their on-prem AD infrastructure to Azure, they need business continuity with network access control

Solution

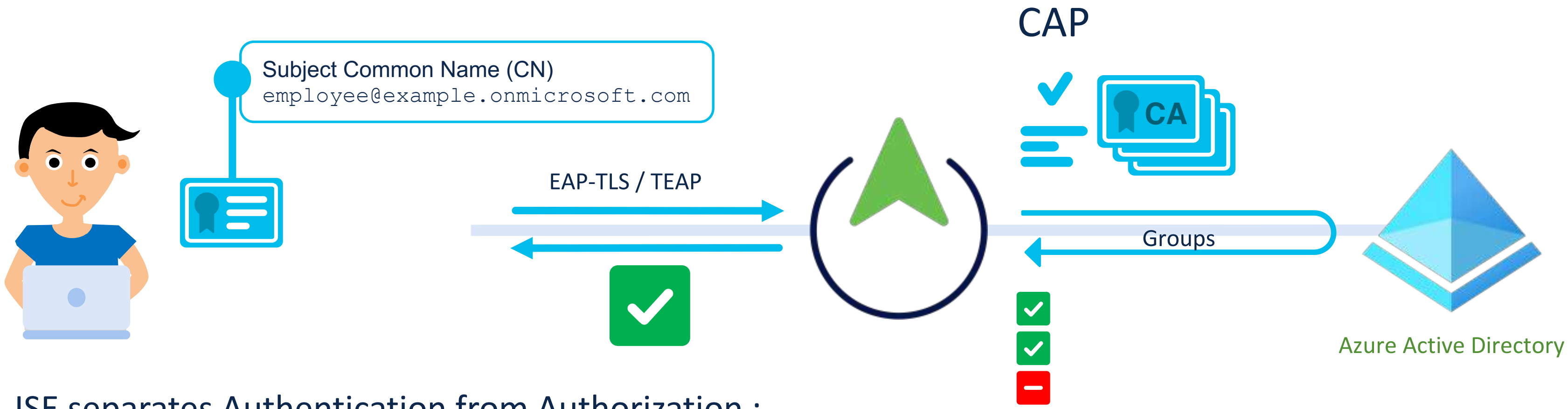
ISE extends Azure AD integration introduced in ISE 3.0, to secure authentication methods like EAP-TLS and Tunnel EAP

Caveats / Prerequisites

Privileged admin account is required to query MS Azure Graph APIs



802.1X with EAP-TLS or TEAP to Azure AD



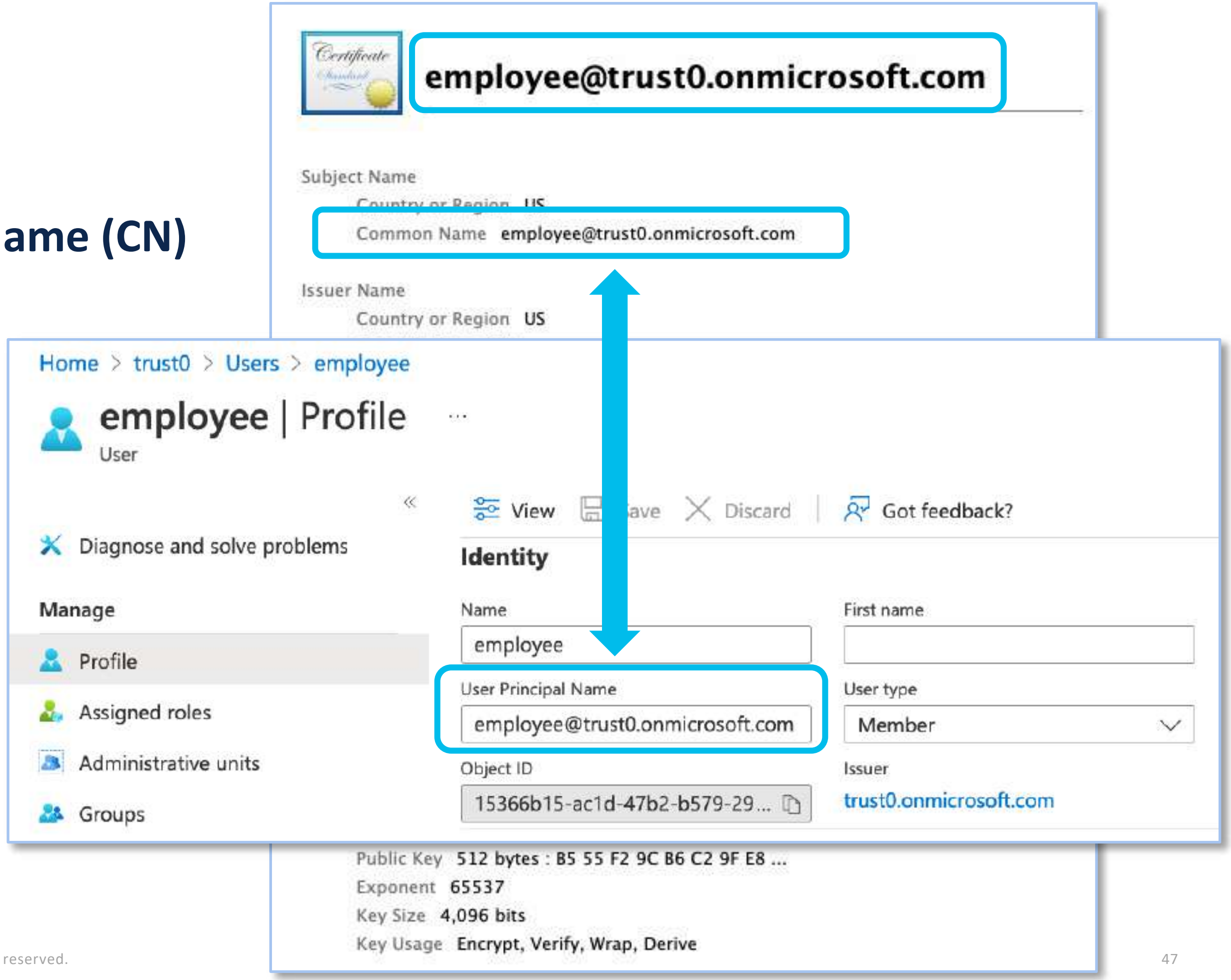
ISE separates Authentication from Authorization :

1. Authentication Using Certificate (user OR machine (EAP-TLS)| user AND machine (TEAP))
2. ISE fetches groups & attributes for certificate CN using Azure Graph API
3. Authorization based on Azure AD group membership and attributes

Digital Certificate

Subject Common Name (CN)

Known as the ***User Principal Name (UPN)***
In Azure Active Directory



employee@trust0.onmicrosoft.com

Subject Name
Country or Region US
Common Name employee@trust0.onmicrosoft.com

Issuer Name
Country or Region US

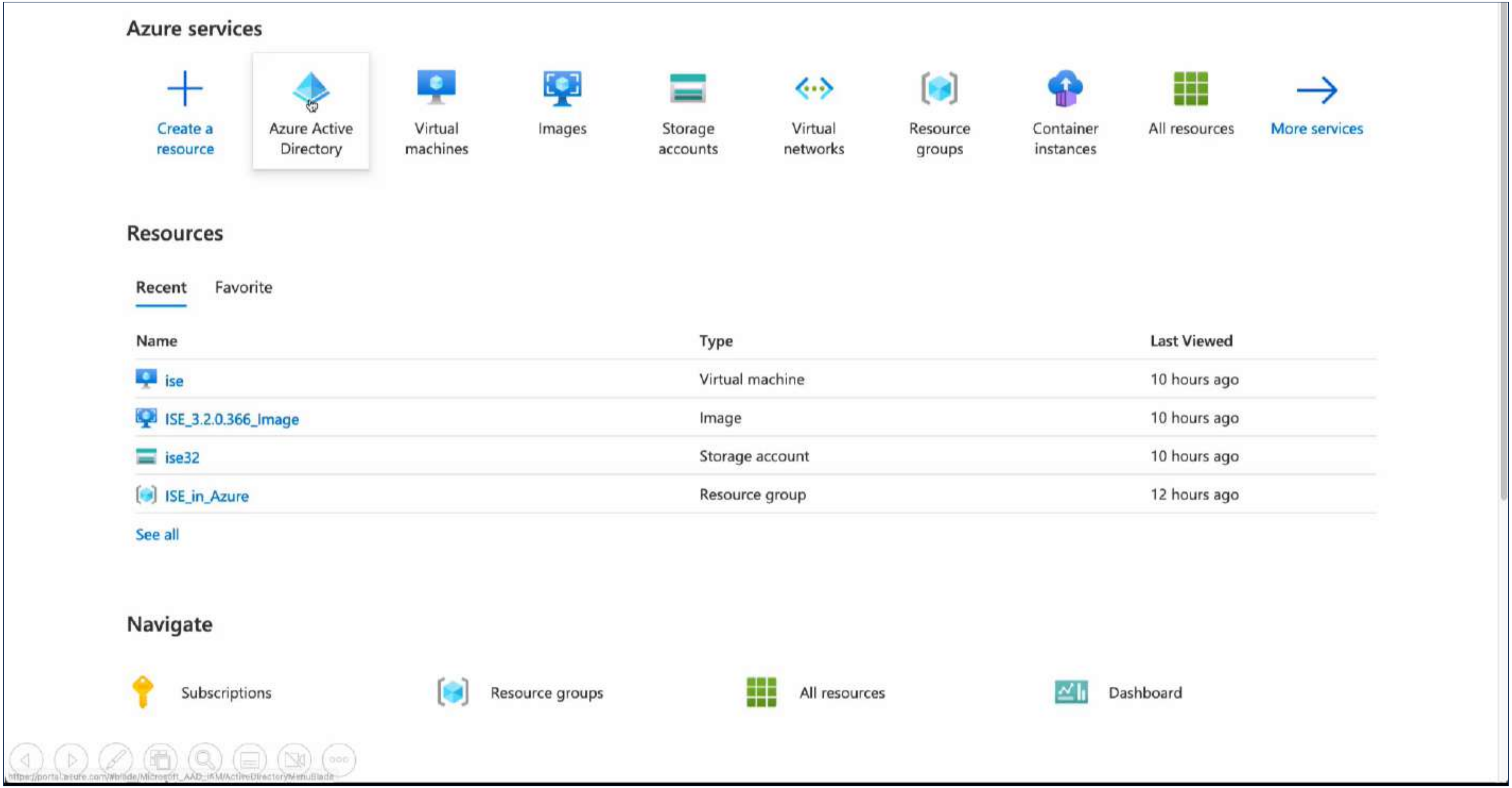
Home > trust0 > Users > employee

employee | Profile ...
User

Identity

Name: employee	First name:
User Principal Name: employee@trust0.onmicrosoft.com	User type: Member
Object ID: 15366b15-ac1d-47b2-b579-29...	Issuer: trust0.onmicrosoft.com

Public Key 512 bytes : B5 55 F2 9C B6 C2 9F E8 ...
Exponent 65537
Key Size 4,096 bits
Key Usage Encrypt, Verify, Wrap, Derive



Name	Type	Last Viewed
ise	Virtual machine	10 hours ago
ISE_3.2.0.366_Image	Image	10 hours ago
ise32	Storage account	10 hours ago
ISE_in_Azure	Resource group	12 hours ago

See all
Navigate
Subscriptions
Resource groups
All resources
Dashboard
https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade

Extra Small Virtual Machine

Problem

Certain remote sites have a low endpoint footprint which warranties a **low scale ISE policy services node** for AAA services

Solution

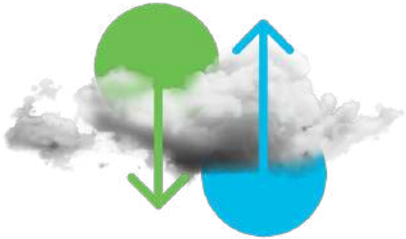
Introducing **PSN Lite, a small factor PSN that supports up to 12K sessions**

Caveats / Prerequisites

Supported on VMs only for PSN persona. Not supported on Public Cloud platforms

VM Sizes	CPUs	Memory	Storage
PSN Lite (Extra Small)	8	32	300 GB
Small	16	32	600 GB
Medium	24	96	600 GB
Large	24	256	2 TB

Cisco ISE 3.2 delivers:



1. Cloud Ready, with Increased Flexibility

2. Infinitely Flexible Compliance

3. Flexible and Efficient Operations

Cisco Secure Client 5.0 (formerly AnyConnect)

Problem

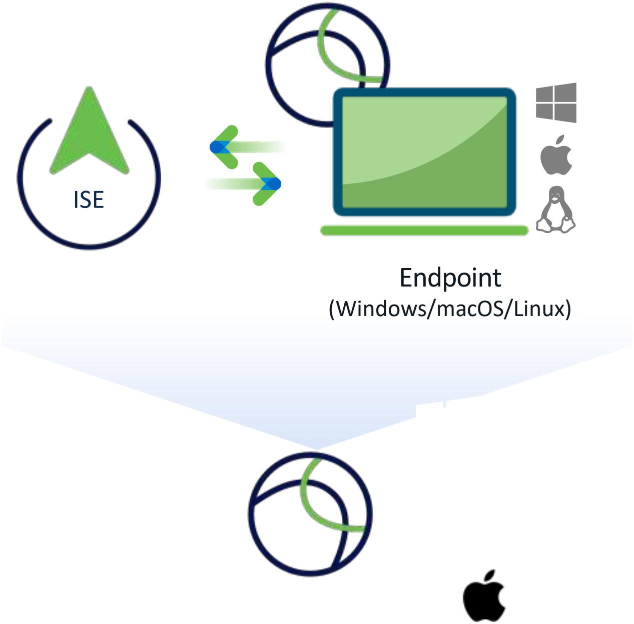
Customers are looking for **unified modular client across all Cisco secure products**

Solution

Cisco Secure Client is a **unified & truly modular client across all cisco security products which gives consistent user experience**

Caveats / Prerequisites

None



Posture compliance your way

Problem

Compliance based authorization is a necessary tenet of Zero Trust, but what if your security policy requires a condition check that is not pre-built by Cisco?

Solution

Custom PowerShell (Windows) and shell (MacOS & Linux) scripts can be written to perform any arbitrary compliance check on endpoints.
None, supported with persistent Agent, Stealth Agent, Agentless and Temporal Agent

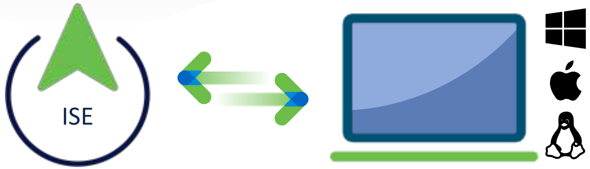
Caveats / Prerequisites

In order to establish trust and be able to execute the scripts on endpoints, you need to configure the SHA-256 fingerprint of any certificate in the certificate chain in the AnyConnectLocalPolicy.xml

- ✓ Is swap space configured as per corporate policy?
- ✓ Are all corporate CA certs, and no rogue CA certs installed?

⋮

- ✓ Has the user over-written network config to use public DNS servers?



Single Entry for Endpoints with GUID Context Visibility Endpoint Window

Problem

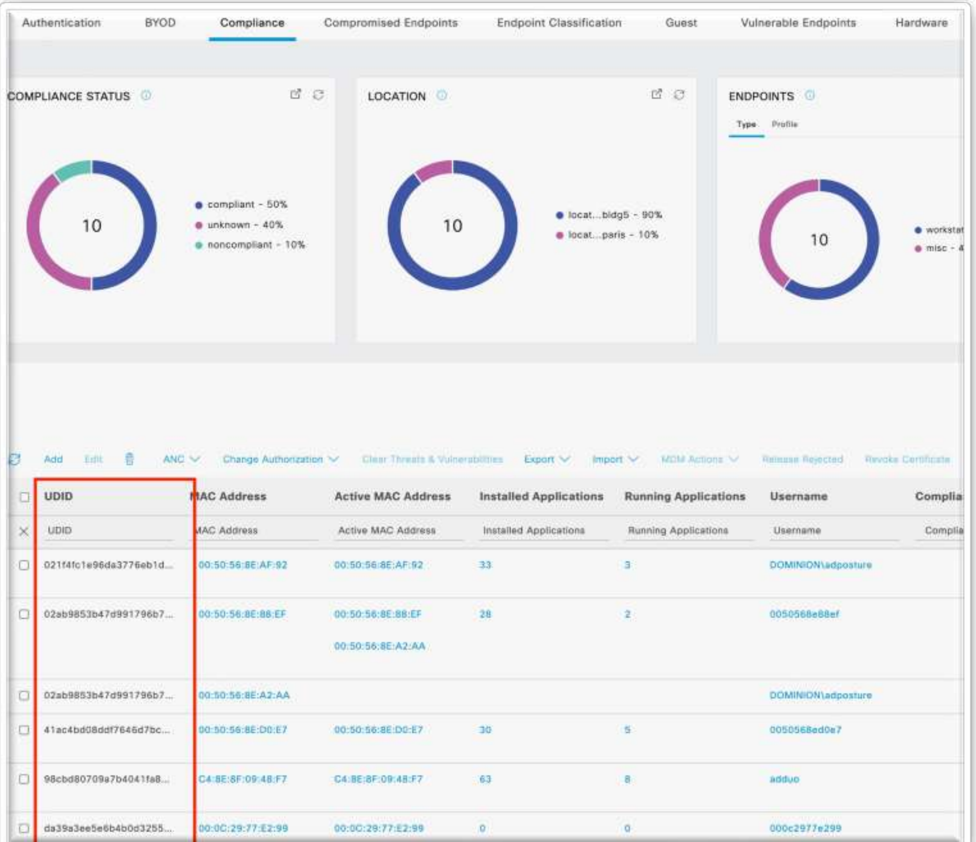
When MAC address randomized, how do you **manage endpoints uniqueness**?

Solution

ISE context visibility now gives uniqueness based on UDID onboarded through MDM/BYOD solutions

Caveats / Prerequisites

UDID imprinted under certificates is the the key for uniqueness



□	UDID	MAC Address	Active MAC Address	Installed Applications	Running Applications	Username	Complia
✕	UDID	MAC Address	Active MAC Address	Installed Applications	Running Applications	Username	Complia
□	021f4fc1e96da3776eb1d...	00:50:56:8E:AF:92	00:50:56:8E:AF:92	33	3	DOMINION\adposture	
□	02ab9853b47d991796b7...	00:50:56:8E:88:EF	00:50:56:8E:88:EF 00:50:56:8E:A2:AA	28	2	0050568e88ef	
□	02ab9853b47d991796b7...	00:50:56:8E:A2:AA				DOMINION\adposture	
□	41ac4bd08ddf7646d7bc...	00:50:56:8E:D0:E7	00:50:56:8E:D0:E7	30	5	0050568ed0e7	
□	98cbd80709a7b4041fa8...	C4:8E:8F:09:48:F7	C4:8E:8F:09:48:F7	63	8	adduo	
□	da39a3ee5e6b4b0d3255...	00:0C:29:77:E2:99	00:0C:29:77:E2:99	0	0	000c2977e299	

SECURE

Multi-UEM Authorization

Problem

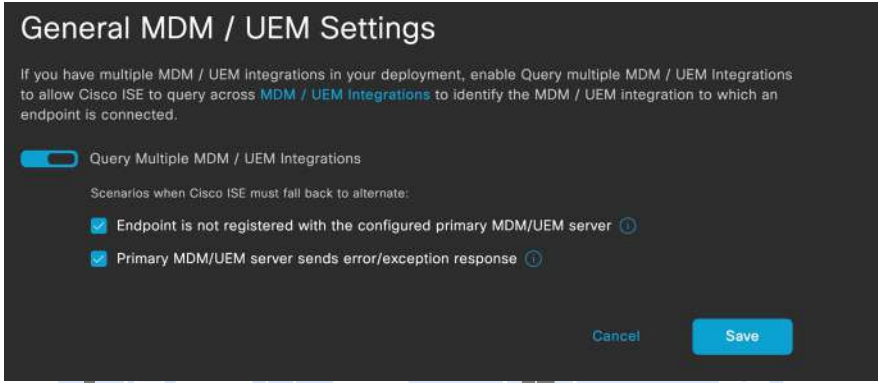
Policies define which UEM ISE queries for each endpoint. But what if multiple UEMs are in use (e.g., during a transition from one vendor to another) and **you have no way to differentiate which UEM manages which endpoint**?

Solution

Define a list of UEM integrations to fall back on if communication with the selected UEM fails or if the endpoint is not registered with it.

Caveats / Prerequisites

None



General MDM / UEM Settings

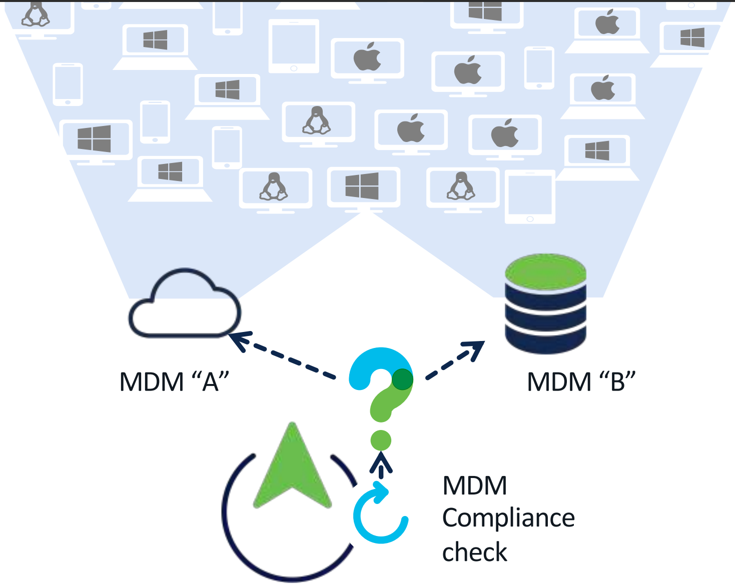
If you have multiple MDM / UEM integrations in your deployment, enable Query multiple MDM / UEM Integrations to allow Cisco ISE to query across MDM / UEM Integrations to identify the MDM / UEM integration to which an endpoint is connected.

● Query Multiple MDM / UEM Integrations

Scenarios when Cisco ISE must fall back to alternate:

☑ Endpoint is not registered with the configured primary MDM/UEM server

☑ Primary MDM/UEM server sends error/exception response



PassiveID Enhancements

Problem

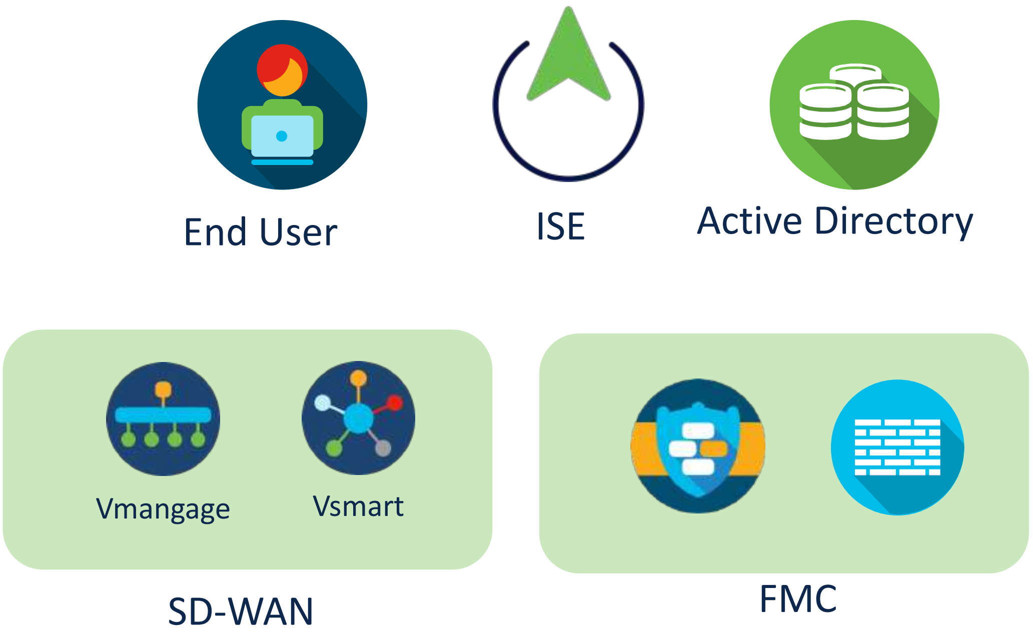
How can you authorize endpoints based on PassiveID?

Solution

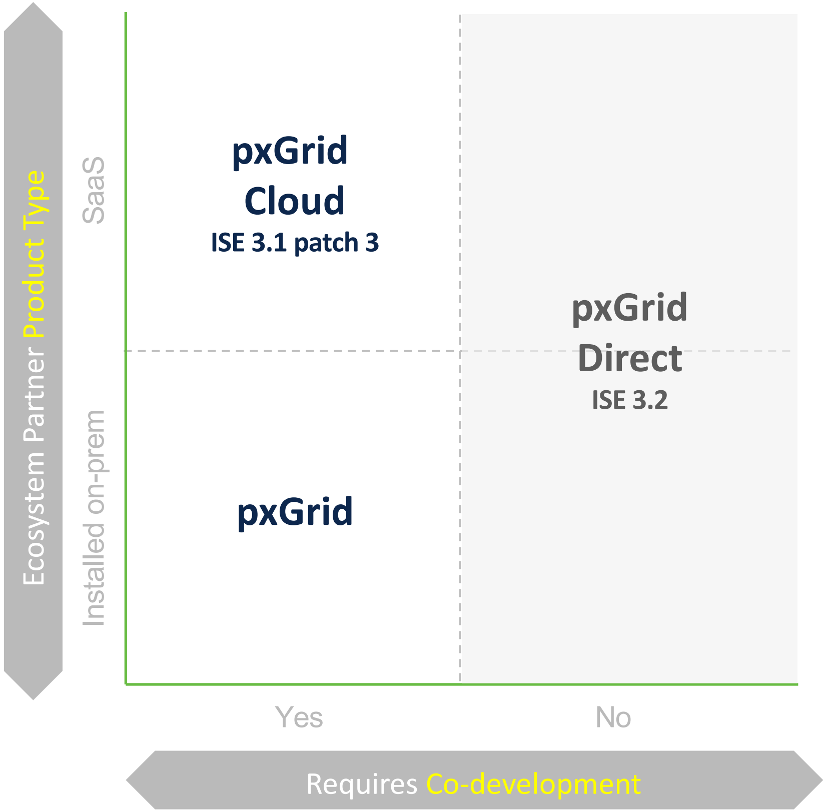
ISE can use authorization policy to assign an SGT to PassiveID endpoints and share group membership, making ISE/ISE-PIC a single connector to AD.
PassiveID also checks if the user is still on the network and shares updates with SD-WAN, FMC and any other integrated system.

Caveats / Prerequisites

n/a



Flexible new methods for ISE integrations



Co-dev essential for integrations involving real-time context exchange and unsolicited requests to ISE such as Adaptive Network Control (ANC)

‘pxGrid Direct’ explained

Problem

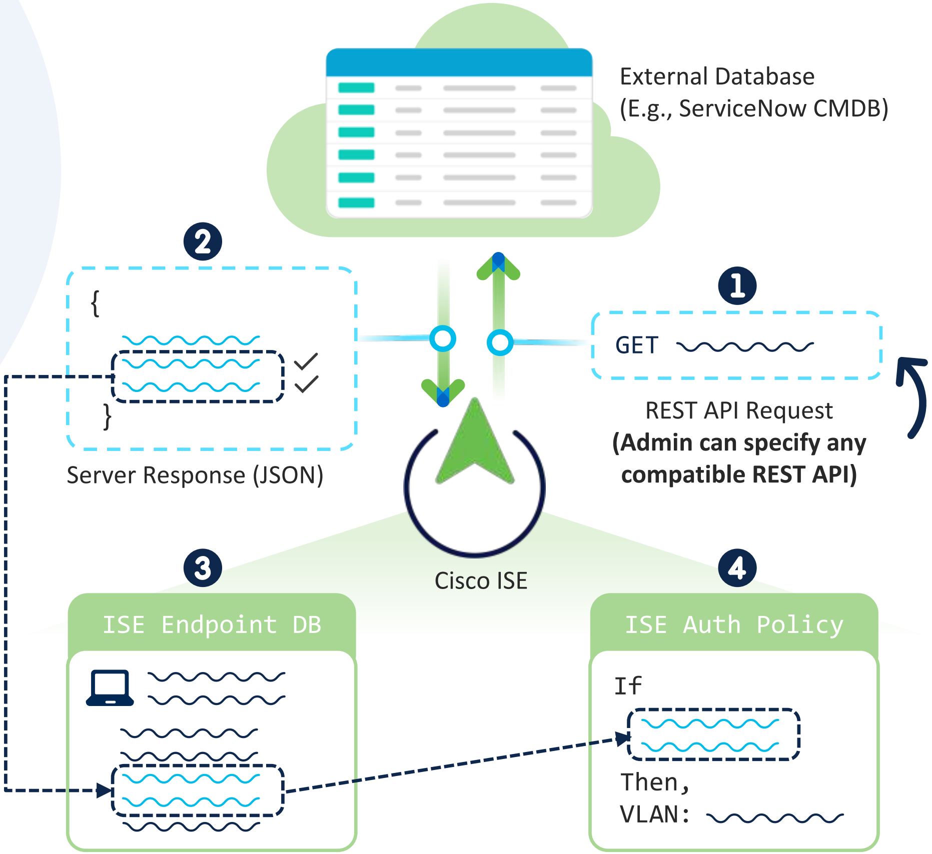
Ingesting endpoint data from external systems into ISE only works if there are pre-built integrations between the two systems.

Solution

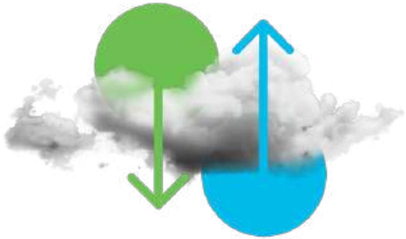
pxGrid Direct, an open integrations framework, enables syncing endpoint data from any external system using REST APIs or other standard methods without requiring ISE-specific code development on the partner end.

Caveats / Prerequisites

Works for REST APIs and JSON formatted data only (in the first phase)



Cisco ISE 3.2 delivers:



1. Cloud Ready, with Increased Flexibility

2. Infinitely Flexible Compliance

3. Flexible and Efficient Operations

View Cisco ISE in Dark Mode

Problem

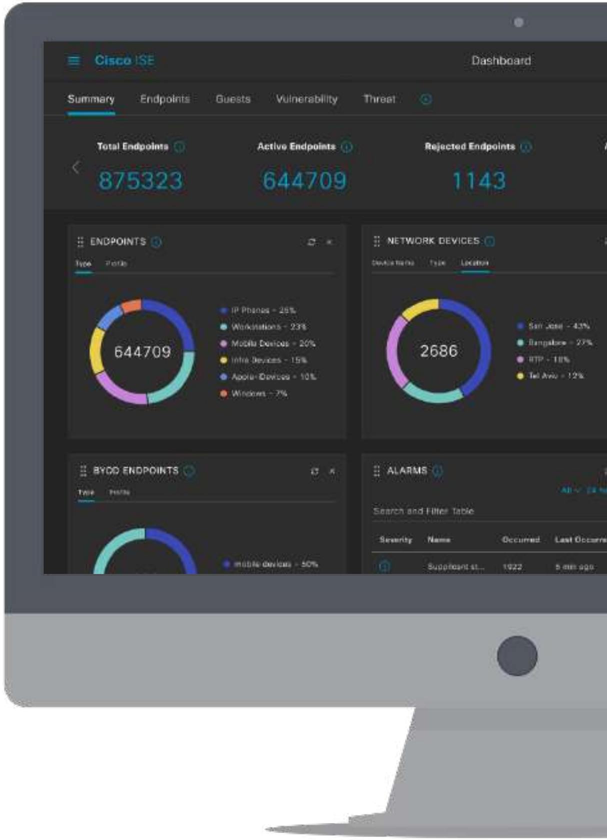
Most requested theme to view ISE UI in Dark Mode

Solution

Set your preference from Account settings

Caveats / Prerequisites

Default theme is ”Light”



Custom reports & dashboards with “Data Connect”

Problem

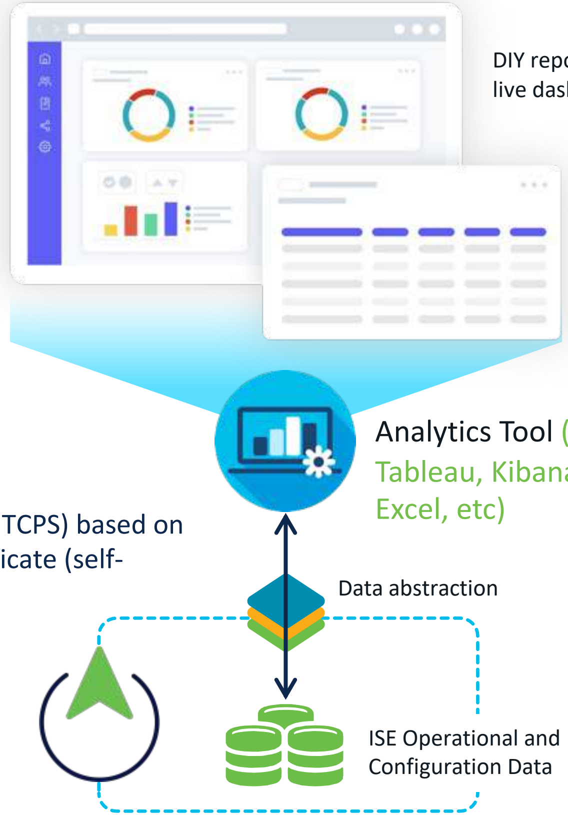
Reports and dashboards are pre-defined capabilities in terms of report type, columns available and other customization options. **How can you create a live dashboard or report based on ISE data that isn’t available in a pre-defined report?**

Solution

ISE exposes configuration, endpoint, session and other operational data for use within 3rd party reporting tools such as PowerBI, Tableau, Kibana or Excel.

Caveats / Prerequisites

Read only access to MnT data, recommended to run queries on secondary MnT node.



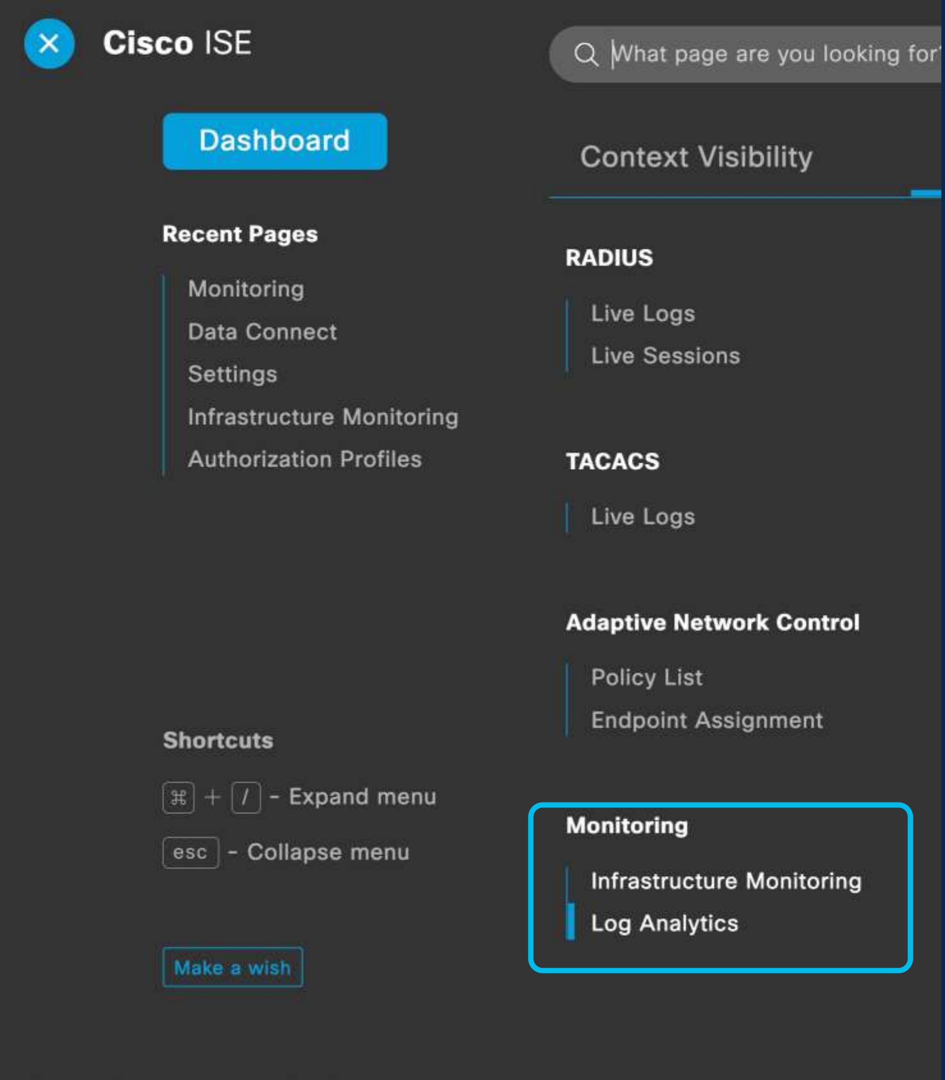
DIY reports, & live dashboards

Analytics Tool (PowerBI, Tableau, Kibana, MS Excel, etc)

Secure connection (TCPS) based on Data Connect Certificate (self-signed cert)

Data abstraction

ISE Operational and Configuration Data



Cisco ISE

What page are you looking for

Dashboard

Context Visibility

Recent Pages

- Monitoring
- Data Connect
- Settings
- Infrastructure Monitoring
- Authorization Profiles

RADIUS

- Live Logs
- Live Sessions

TACACS

- Live Logs

Adaptive Network Control

- Policy List
- Endpoint Assignment

Monitoring

- Infrastructure Monitoring
- Log Analytics

Shortcuts

⌘ + / - Expand menu

esc - Collapse menu

Make a wish

- Radical new ways to monitor ISE infrastructure and perform log analysis

Infrastructure Monitoring

Reporting. Unleashed.

Problem

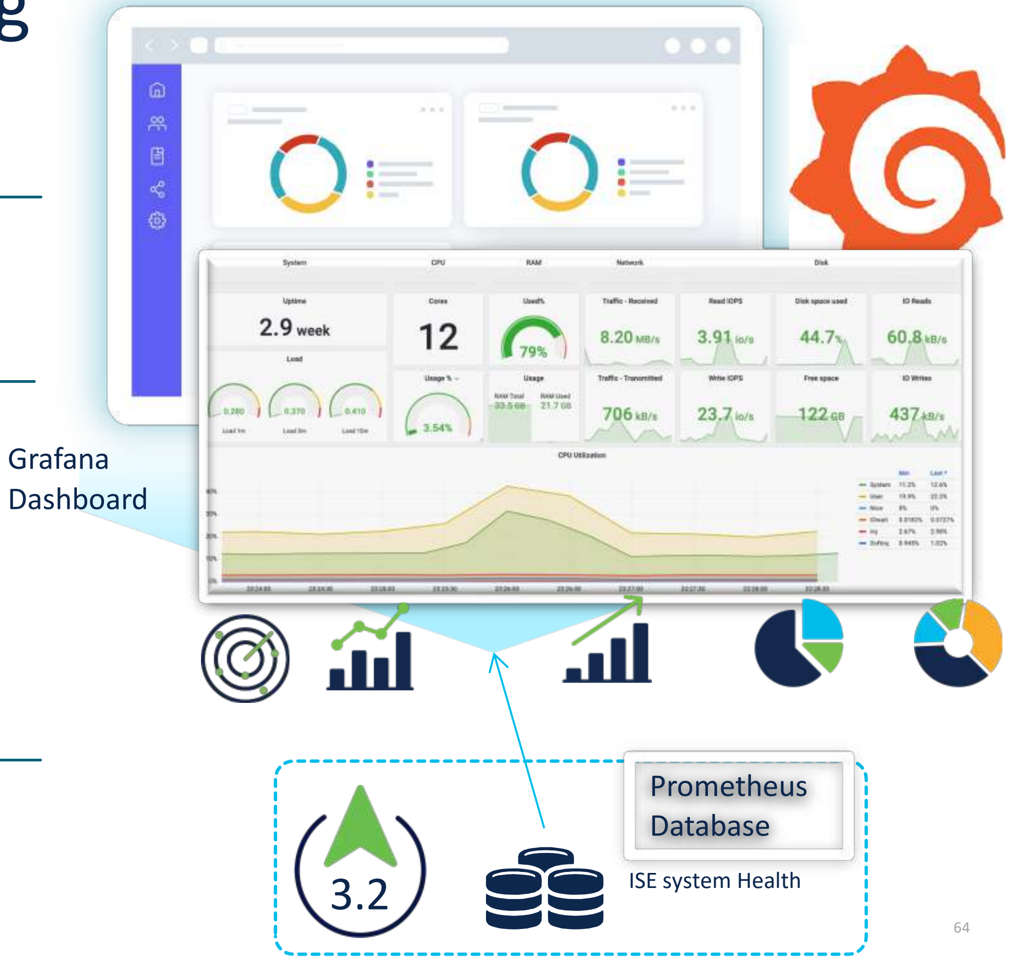
How can you monitor **ISE system health in real time?**

Solution

ISE is now equipped with **Grafana for creating dashboards based on ISE System Health, applications & KPIs**(Process, CPU, Memory, Disk utilization, IO, Network..) stored in Prometheus timeseries database

Caveats / Prerequisite

Enabled by default

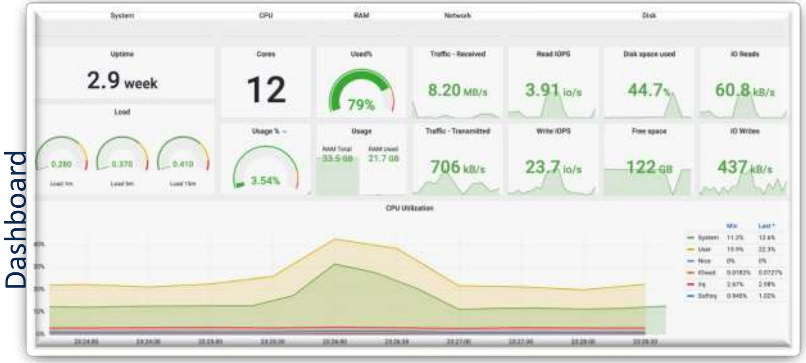


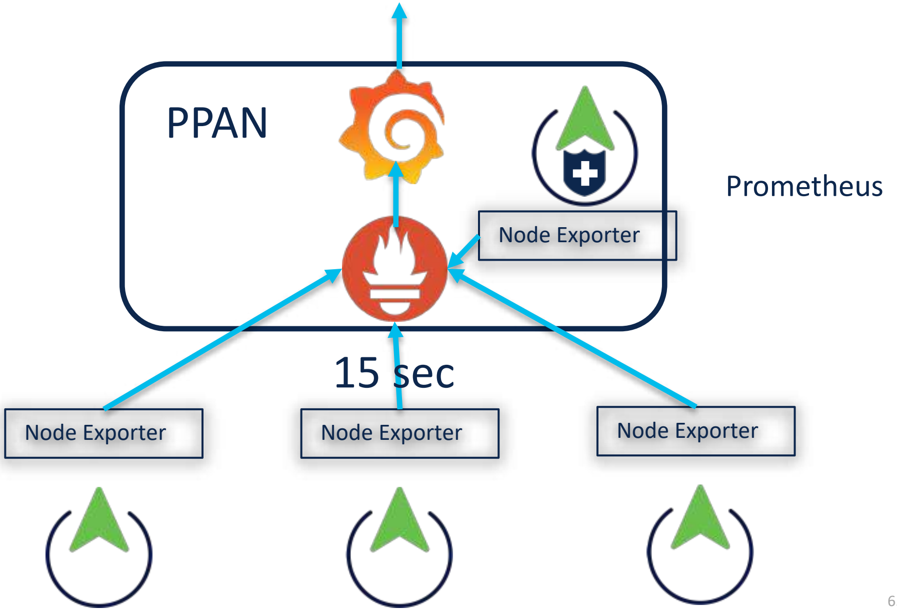
Infrastructure Monitoring

- Node Exporter runs on each ISE node which collects the system health KPIs
- Prometheus collects the information and stores in Timeseries database
- Grafana(front-end)gives you capability to view ISE system health & create your own Dashboards
- Use it for Timeseries Grafana dashboards for System Health

https://prometheus.io/docs/prometheus/latest/querying/basics/

Grafana Dashboard





Log Analytics

Reporting. Unleashed.

Problem

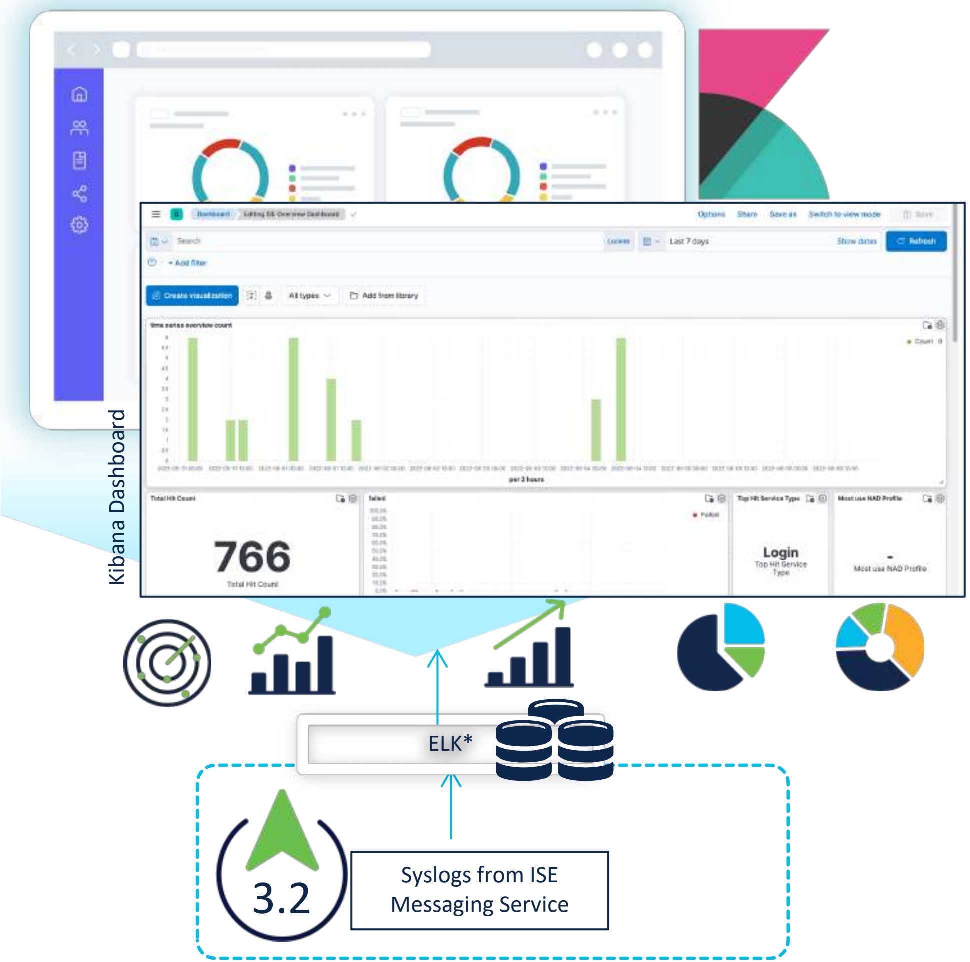
How can you analyze ISE operational data and create your own Dashboards?

Solution

ISE is now equipped with **Kibana for log analytics and creating dashboards based on Syslogs**

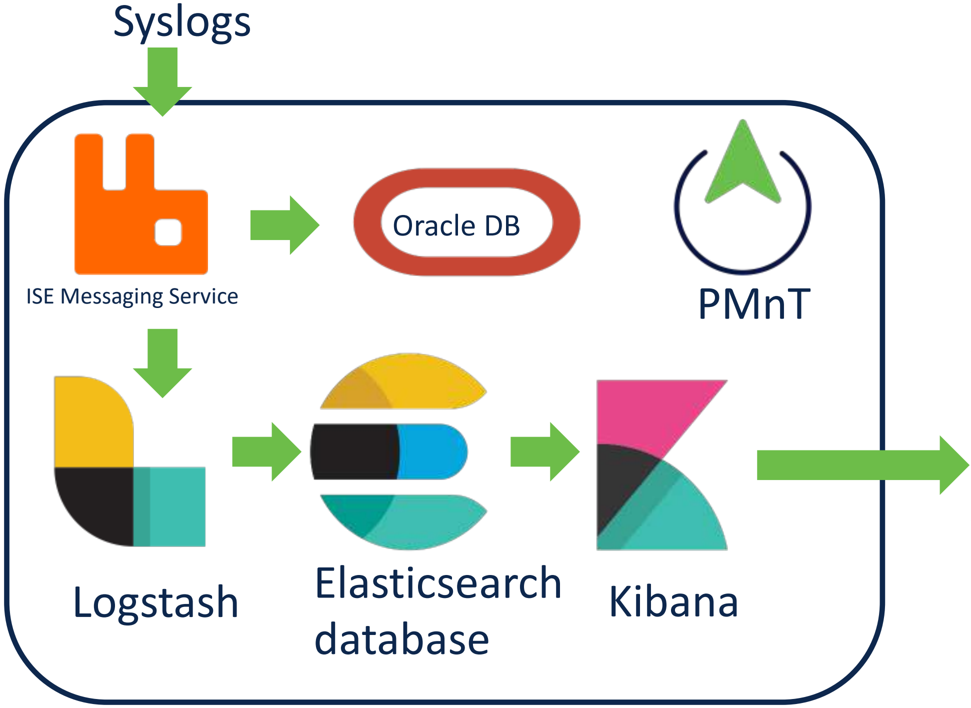
Caveats / Prerequisite

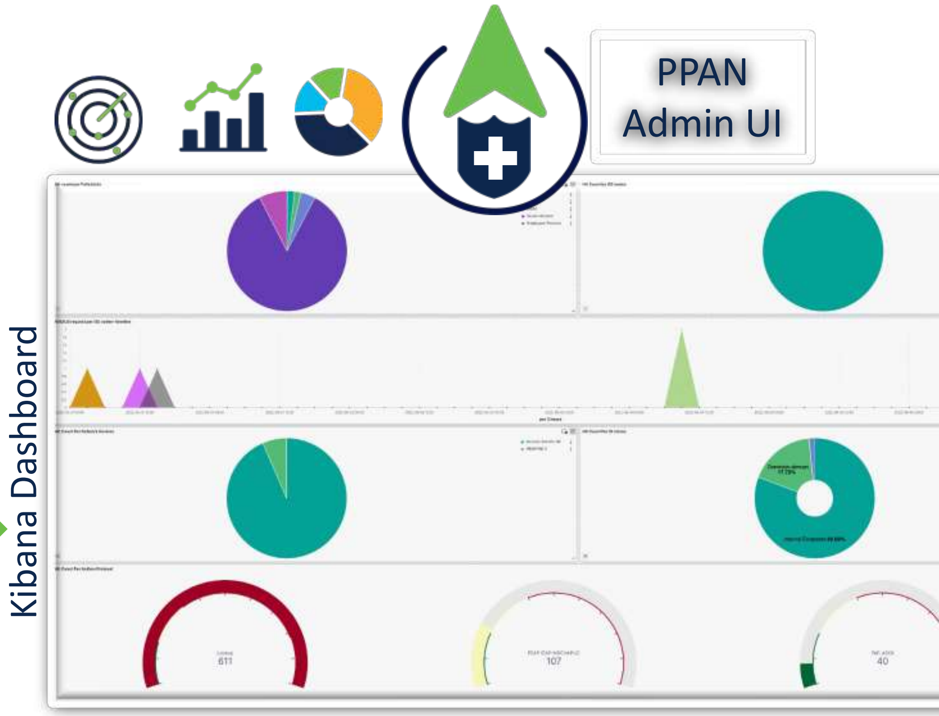
Disabled by default and runs on MnT



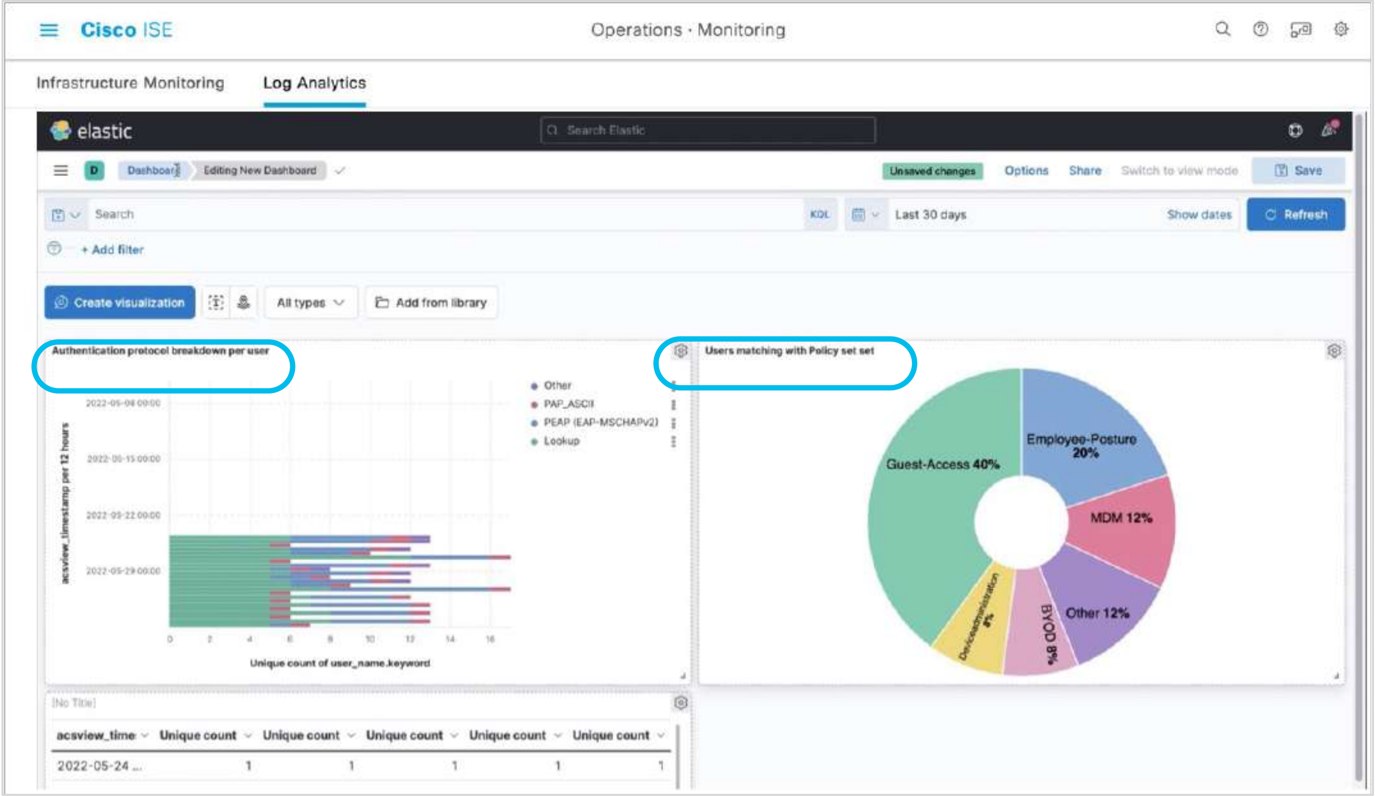
*Elasticsearch, Logstash & Kibana

Log Analytics - details





Create your own dashboard to analyze ISE logs



acsview_time	Unique count	Unique count	Unique count	Unique count	Unique count
2022-05-24 ...	1	1	1	1	1

Simplified API operations with the ‘PATCH’ method

Problem

To update resources on ISE via the REST API ‘PUT’ method requires passing of all the attributes making it hard to scale the API use in production environments.

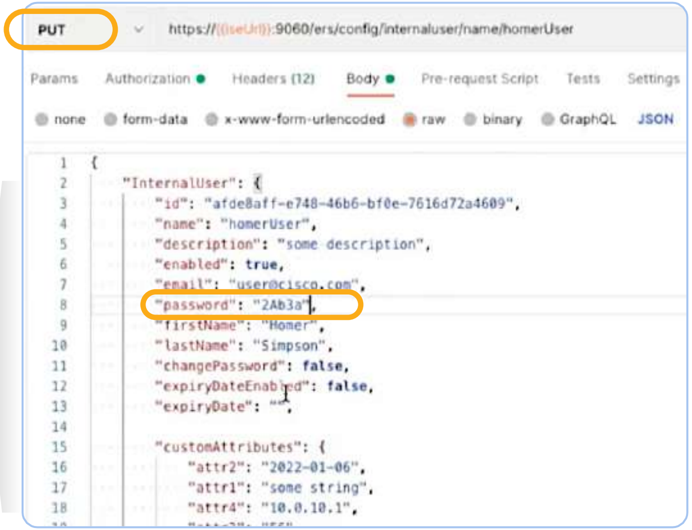
Solution

ISE 3.2 introduces the API ‘PATCH’ method allowing external applications to update specific attributes to update on ISE.

Caveats / Prerequisites

Works for JSON format only

Before: Updating a resource required passing all attributes

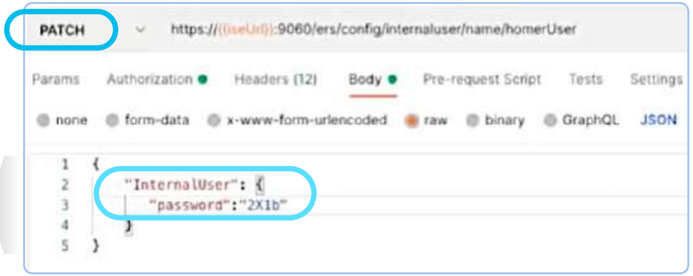


PUT https://{{iseUrl}}:9060/ers/config/internaluser/name/homerUser

```
{
    "InternalUser": {
        "id": "afde8aff-e748-46b6-bf0e-7616d72a4609",
        "name": "homerUser",
        "description": "some description",
        "enabled": true,
        "email": "user@cisco.com",
        "password": "2Ab3a",
        "firstName": "Homer",
        "lastName": "Simpson",
        "changePassword": false,
        "expiryDateEnabled": false,
        "expiryDate": "",

        "customAttributes": {
            "attr2": "2022-01-06",
            "attr1": "some string",
            "attr4": "10.0.10.1",
```

Now: Update resources with specific set of attributes



PATCH https://{{iseUrl}}:9060/ers/config/internaluser/name/homerUser

```
{
    "InternalUser": {
      "password":"2X1b"
    }
}
```

SECURE

Meraki integration

Group-based Policy Sync with Meraki dashboard

Problem

1. Hybrid customers using on-premise ISE and cloud-managed Meraki
2. Inconsistencies between ISE and Meraki policies
3. Personas differ across orgs and applications

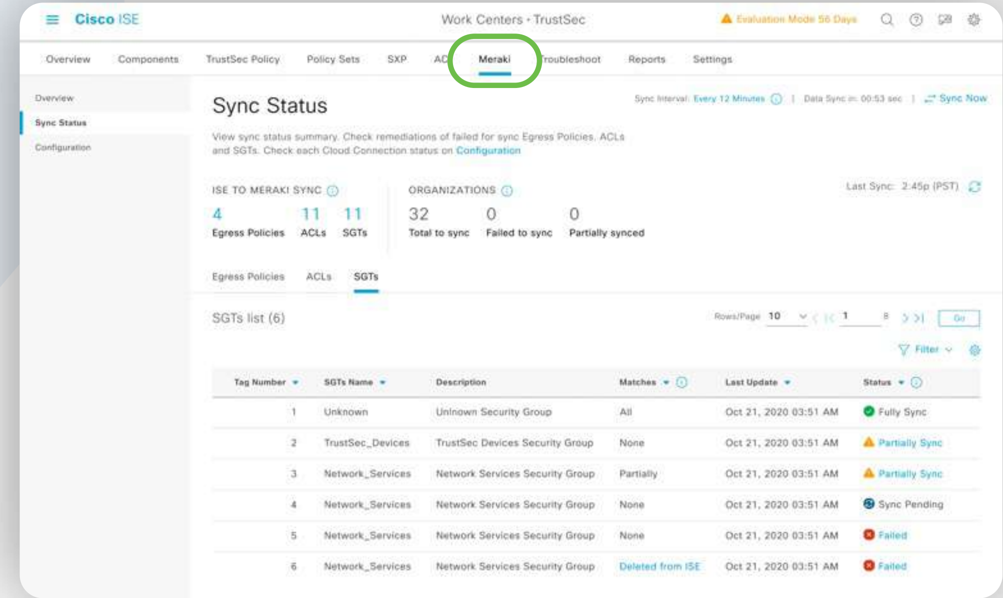
How might we sync TrustSec policy in an organization with hybrid networks?

Solution

Automated TrustSec policy sync via UI in ISE which removes redundant policy settings and management. Provide the ability to sync from one ISE to many Meraki orgs.

Caveats / Prerequisites

Solution Targeted for ISE 3.2 P1. Sync limited to 60 SGTs per org (based on Meraki constraints)



Sync Status

View sync status summary. Check remediations of failed for sync Egress Policies, ACLs and SGTs. Check each Cloud Connection status on Configuration

ISE TO MERAKI SYNC

4	11	11
Egress Policies	ACLs	SGTs

ORGANIZATIONS

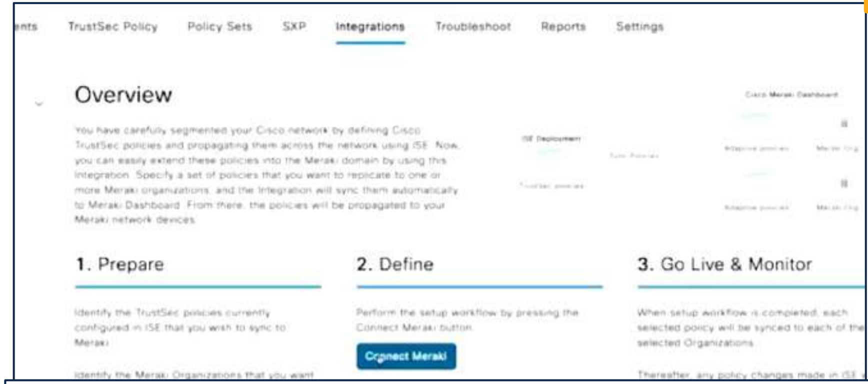
32	0	0
Total to sync	Failed to sync	Partially synced

SGTs list (6)

Tag Number	SGTs Name	Description	Matches	Last Update	Status
1	Unknown	Uninown Security Group	All	Oct 21, 2020 03:51 AM	Fully Sync
2	TrustSec_Devices	TrustSec Devices Security Group	None	Oct 21, 2020 03:51 AM	Partially Sync
3	Network_Services	Network Services Security Group	Partially	Oct 21, 2020 03:51 AM	Partially Sync
4	Network_Services	Network Services Security Group	None	Oct 21, 2020 03:51 AM	Sync Pending
5	Network_Services	Network Services Security Group	None	Oct 21, 2020 03:51 AM	Failed
6	Network_Services	Network Services Security Group	Deleted from ISE	Oct 21, 2020 03:51 AM	Failed

Use the ‘Sync Status’ page to monitor and take action on policies that are selected for sync with Meraki.

Meraki integration wizard



ents TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Overview

You have carefully segmented your Cisco network by defining Cisco TrustSec policies and propagating them across the network using ISE. Now, you can easily extend these policies into the Meraki domain by using this integration. Specify a set of policies that you want to replicate to one or more Meraki organizations, and the integration will sync them automatically to Meraki Dashboard. From there, the policies will be propagated to your Meraki network devices.

1. Prepare

Identify the TrustSec policies currently configured in ISE that you wish to sync to Meraki.

Identify the Meraki Organizations that you want

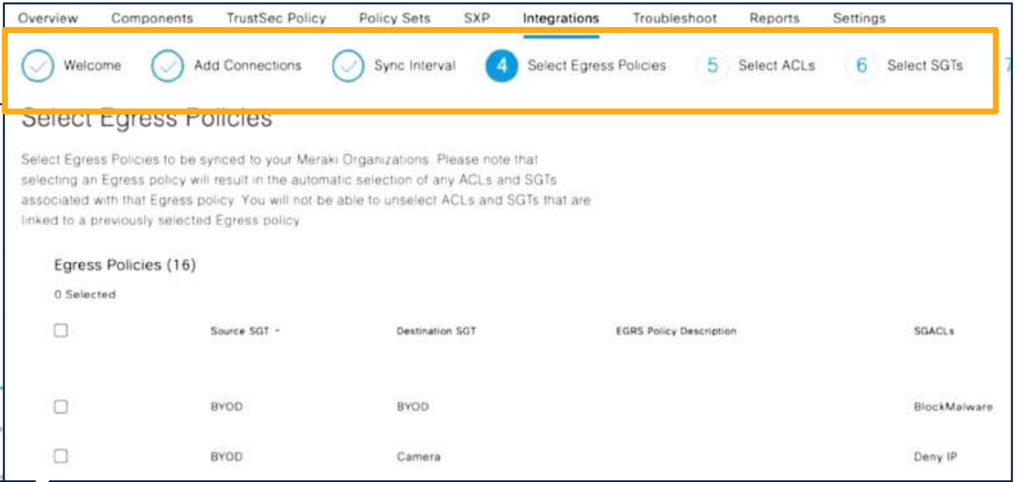
2. Define

Perform the setup workflow by pressing the Connect Meraki button.

3. Go Live & Monitor

When setup workflow is completed, each selected policy will be synced to each of the selected Organizations.

Thereafter, any policy changes made in ISE



Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

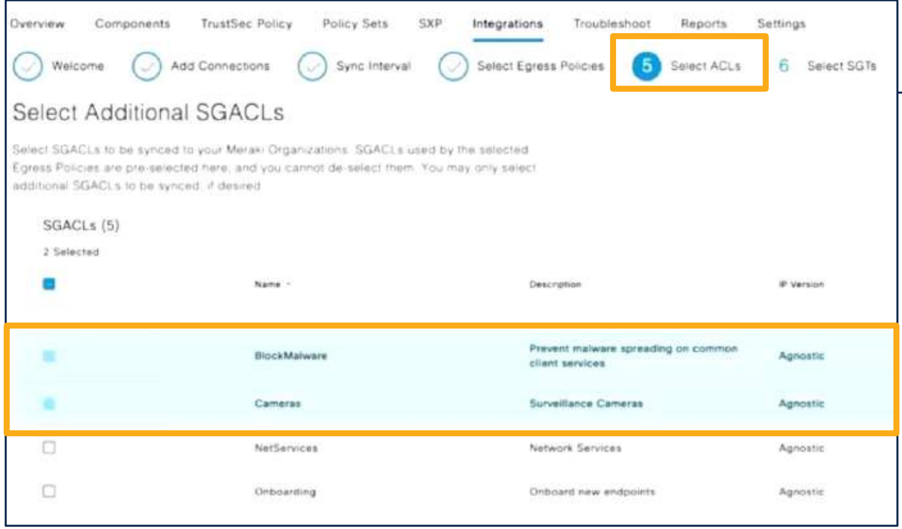
Select Egress Policies

Select Egress Policies to be synced to your Meraki Organizations. Please note that selecting an Egress policy will result in the automatic selection of any ACLs and SGTs associated with that Egress policy. You will not be able to unselect ACLs and SGTs that are linked to a previously selected Egress policy.

Egress Policies (16)

0 Selected

□	Source SGT ˄	Destination SGT	EGRS Policy Description	SGACLs
□	BYOD	BYOD		BlockMalware
□	BYOD	Camera		Deny IP



Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

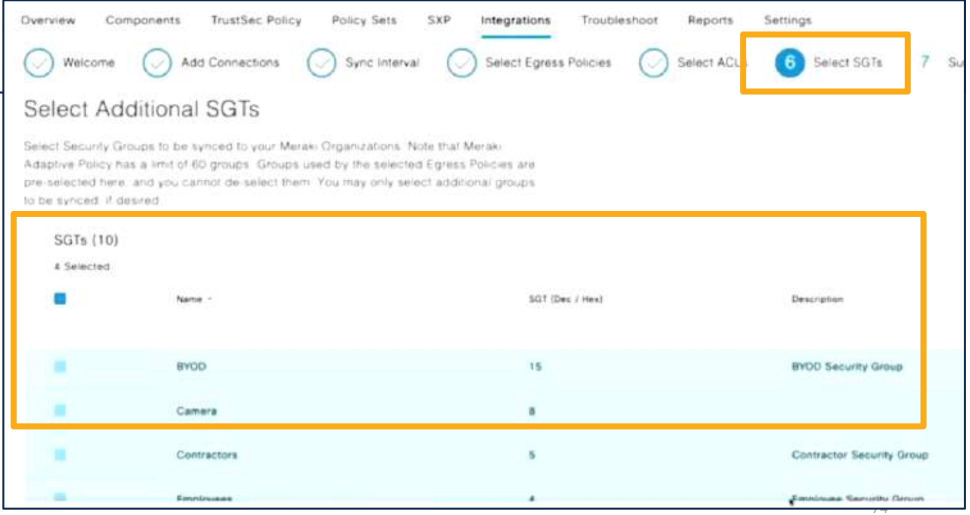
Select Additional SGACLs

Select SGACLs to be synced to your Meraki Organizations. SGACLs used by the selected Egress Policies are pre-selected here, and you cannot de-select them. You may only select additional SGACLs to be synced, if desired.

SGACLs (5)

2 Selected

■	Name ˄	Description	IP Version
■	BlockMalware	Prevent malware spreading on common client services	Agnostic
■	Cameras	Surveillance Cameras	Agnostic
□	NetServices	Network Services	Agnostic
□	Onboarding	Onboard new endpoints	Agnostic



Overview Components TrustSec Policy Policy Sets SXP Integrations Troubleshoot Reports Settings

Select Additional SGTs

Select Security Groups to be synced to your Meraki Organizations. Note that Meraki Adaptive Policy has a limit of 60 groups. Groups used by the selected Egress Policies are pre-selected here, and you cannot de-select them. You may only select additional groups to be synced, if desired.

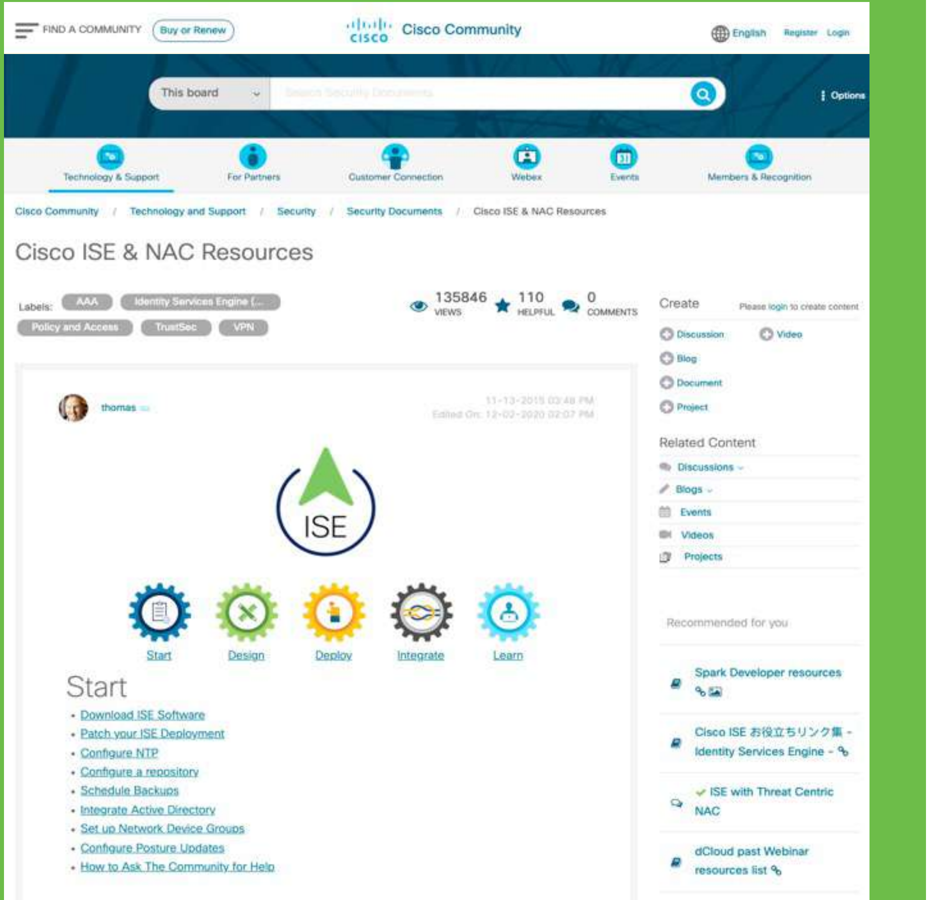
SGTs (10)

4 Selected

■	Name ˄	SGT (Dec / Hex)	Description
■	BYOD	15	BYOD Security Group
■	Camera	8	
■	Contractors	5	Contractor Security Group
■	Employees	4	Employee Security Group

End of Life Announcement for ISE 2.7

Milestone	Definition	Date
End of Life Notice	Announcement of end-of-life of the product posted on cisco.com.	**March 22, 2022**
Software Maintenance	From this date, Cisco will only publish fixes for security vulnerabilities and severity 1 issues pertaining to the release as determined by the Cisco ISE team.	**September 22, 2022**
End of Software Maintenance	The last date on which Cisco Engineering may release the final software maintenance releases or bug fixes, if any. After this date, Cisco Engineering will no longer develop, repair, maintain, or test the product software including Sev 1 and security vulnerabilities.	**September 22, 2023**
End of Support	The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product will become unavailable, and the product becomes obsolete.	**September 22, 2024**



Cisco Community / Technology and Support / Security / Security Documents / Cisco ISE & NAC Resources

Cisco ISE & NAC Resources

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

135846 VIEWS 110 HELPFUL 0 COMMENTS

thomas

11-13-2015 03:48 PM
Edited On: 12-02-2020 02:07 PM

Start

- Download ISE Software
- Patch your ISE Deployment
- Configure NTP
- Configure a repository
- Schedule Backups
- Integrate Active Directory
- Set up Network Device Groups
- Configure Posture Updates
- How to Ask The Community for Help

Create Please login to create content

Discussion Video
Blog
Document
Project

Related Content

Discussions
Blogs
Events
Videos
Projects

Recommended for you

Spark Developer resources

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

ISE with Threat Centric NAC

dCloud past Webinar resources list

- Consolidated list of resources
  cs.co/ise-resources
- Community Q&A
  cs.co/ise-community
- Recorded webinars and other videos
  cs.co/ise-videos
- Evaluations
  cs.co/ise-eval
- Integration Guides
  cs.co/ise-guides
- Sellers – Start Here!
  cs.co/selling-ise
- Licensing Guide
  cs.co/ise-licensing

CISCO SECURE