Cisco Identity Services Engine

September 2020

Contents

1. Understanding the Cisco Identity Services Engine use cases

This section is to help you understand the various use cases that the Cisco Identity Services Engine (ISE) can empower you to solve. This is a great place to start if you are looking to understand the use cases, see what fits your needs and understand the quantity and types of licenses needed. You may choose to implement multiple use cases.
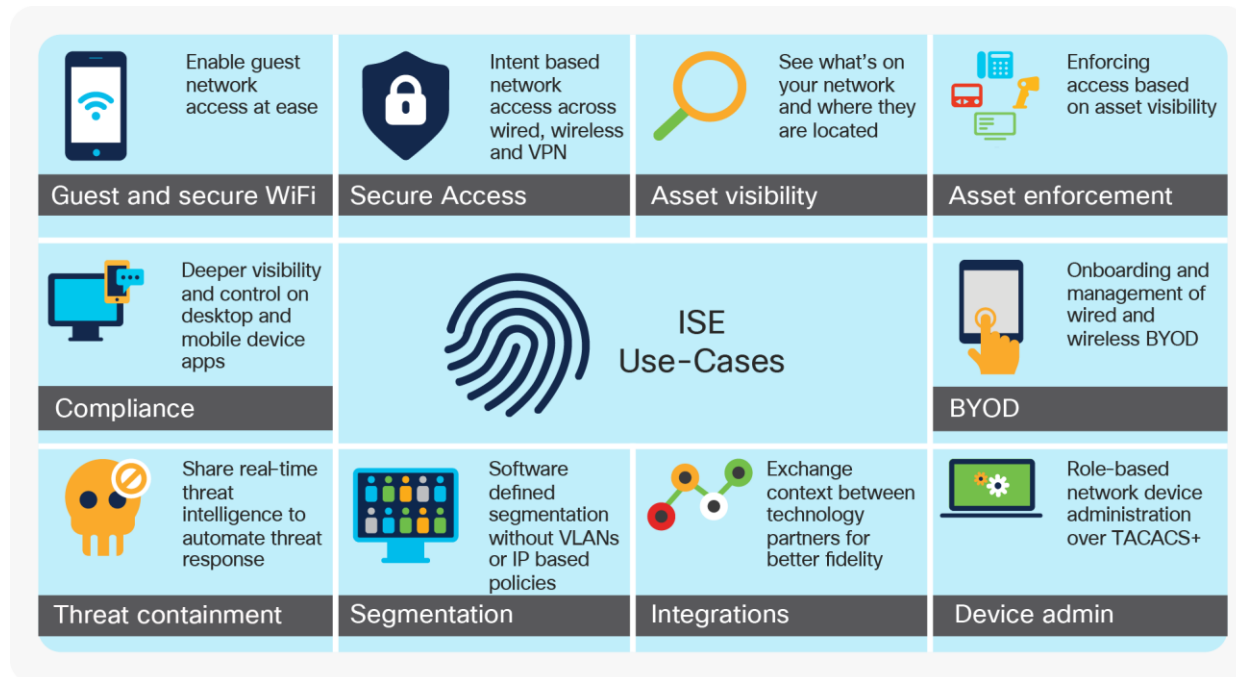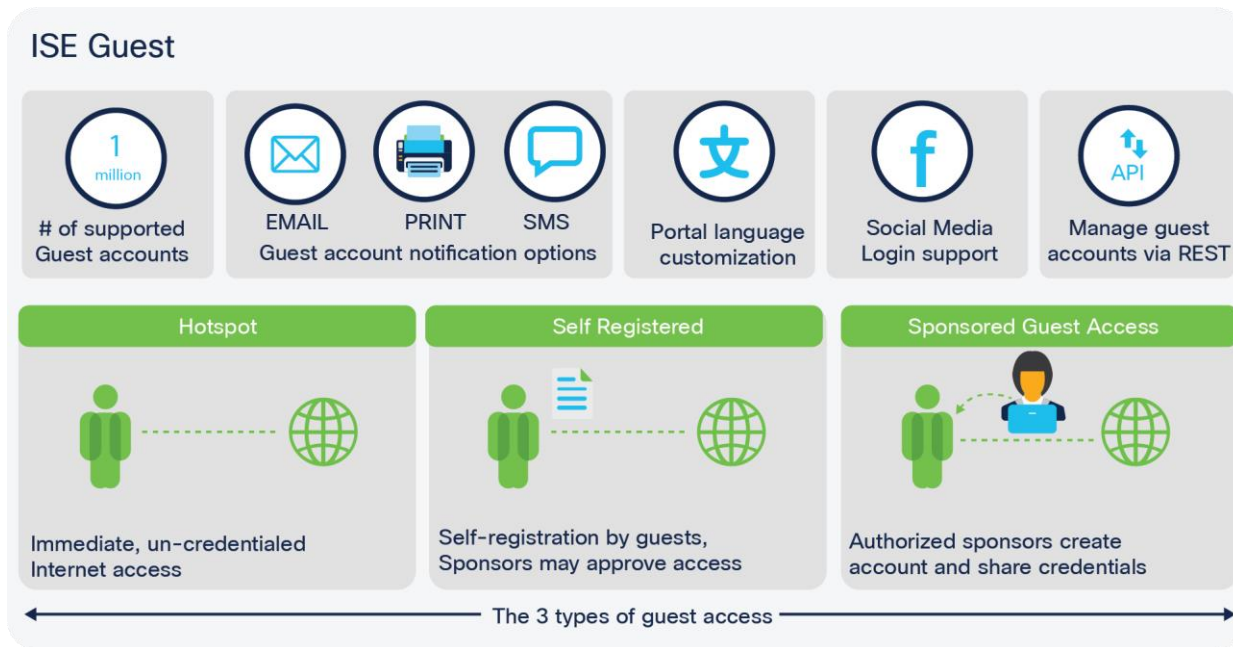

Figure 1.
Cisco Identity Services Use-cases

1.1 Guest and Secure Wireless Access

1.1.1 Why Guest

Many organizations provide free Internet access to guests visiting their organization for a short period. These guests include vendors, retail customers, short-term vendors/contractors, etc. ISE provides the ability to create accounts for these visitors and authenticate them for audit purposes. There are three ways in which ISE can provide Guest access: Hotspot (immediate non-credentialed access), Self-Registration and Sponsored Guest access. ISE also provides a rich set of APIs to integrate with other systems such as vendor management systems to create, edit and delete Guest accounts. Further, the various portals that the end user sees can be completely customized with the right font, color, themes, etc. to match the look and feel of the customer's brand.
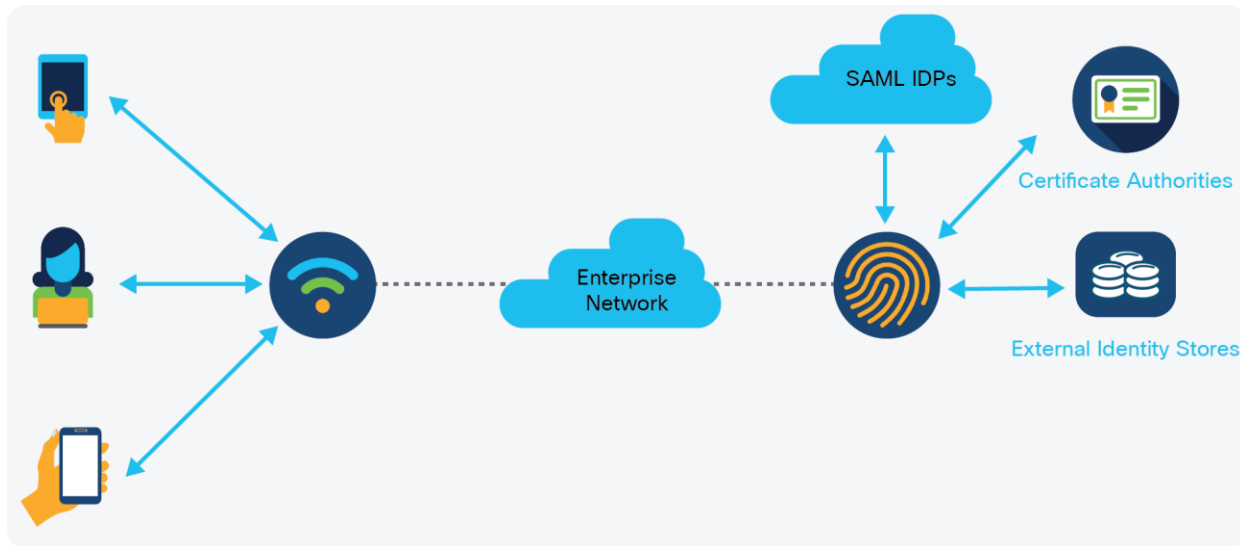
Figure 2.
Cisco ISE Guest Use-Case

ISE creates local accounts for Guests. These accounts can be created by an employee hosting the Guest (the Sponsor) using a built-in portal or created by the Guest themselves by providing some basic info. The Guest can receive credentials via email/SMS and use that to authenticate themselves to the network and thereby get network access. The admin can define what level of access to provide to such users.

Required license: ISE Essentials

1.1.3 Why Secure Wireless Access

Most organizations start securing their wireless network first. Securing the wireless network is the most basic needs for every organization. Using ISE, network administrators can secure access to the network by allowing only authorized users and wireless devices, such as mobile phones, tablets or laptops – BYOD or organization owned and other wireless "things" to connect to the network and later enforce different security policies. Authentication and Authorization are core functionalities of ISE. Every ISE session begins with authentication, whether to a user or to a device. Authentication can be active authentication or passive authentication (not including 802.1x session): An authentication is done using 802.1x when ISE authenticates the user against an Identity Source, while in passive authentication (used in Easy Connect) ISE learns about the user after the user authenticates against the Identity Source like Microsoft's Active Directory (AD) and the AD notifies ISE.

1.1.4 How does Secure Wireless Access work

Figure 3.
Cisco ISE Secure Wireless Use-case

After successful authentication, based on group's information ISE provides the right access the wireless connection, whether the connection is a Passive Identity session (Easy Connect), MAB (MAC Address Bypass) or 802.1x. This can be achieved by assigning the user to a VLAN, DACL, ACL, or assign an SGT or SGACL.

Required license: ISE Essentials or ISE Advantage (for SGT or SGACL only)

1.2 Asset Visibility

1.2.1 Why Asset Visibility

Understanding the device type is many times a critical element in determining the type of network access that should be granted to the device. For example, a building management system such as an IP camera or an elevator should be given access to a specific part of the network (such as the building management services network) while a printer should be given access to another part of the network (such as IT services). Having visibility helps the IT administrator determine the types of devices on their network and how to provide them with the right level of permissions. Basic asset visibility profiles endpoints by matching their network attributes to known profiles. Advanced asset visibility performs deeper analysis of the different conversations that applications on these devices have with other endpoints and servers on the network through Deep Packet Inspection (DPI). While basic asset visibility will provide you with visibility to most of your network, especially to your traditional devices (printers, mobile phones, etc.), advanced asset visibility will provide you with visibility into more vertical-specific and IoT-type of devices.
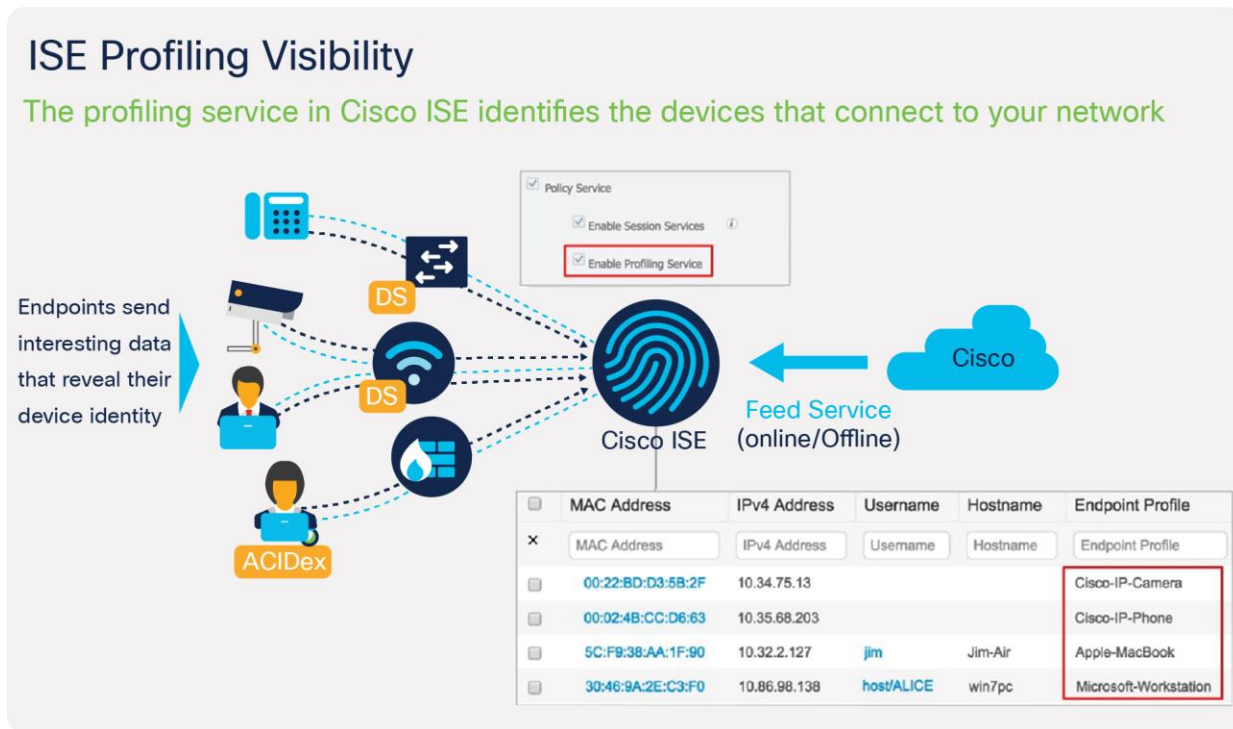
Figure 4.
Cisco ISE Basic Visibility Use-case

Basic asset visibility in ISE is accomplished through the Profiler service, which gathers information about a device by listening to its network communication. The likely device type is determined by weighing the information from most definitive to least definitive attributes.

Based on the asset's visibility, the next step on securing your network asset continuum is to **enforce** access. Basic Asset Enforcement allows you to use the categorization of endpoints by profiles and in your network access policy. This ensures that based on the visibility learnt for an endpoint, it will be given only the network permissions for its profile. Printers will be able to only receive access to printing servers or anyone needing printing services, and mobile BYODs will be able to receive access only for internet services and low-risk internal systems.

Required license: ISE Advantage

1.2.4 How Advanced Asset Visibility (Endpoint Analytics visibility) works

Endpoint Analytics is designed to improve endpoint profiling fidelity. It provides fine-grained endpoint identification and assigns labels to a variety of endpoints. This is done by analyzing endpoint attributes through Deep Packet Inspection (DPI) and other probes aggregated from different sources such as SD-AVC, Cisco ISE, and other third-party components.

It uses Artificial Intelligence (AI) and machine learning to intuitively group endpoints that have common attributes and helps IT admins in providing suggestions to choose the right endpoint profiling labels. Multifactor classification classifies endpoints using label categories for flexible profiling. These endpoint labels can then be used in Cisco ISE to create custom profiles that form the basis of providing the right set of access privileges to endpoints/endpoint groups via an authorization policy.
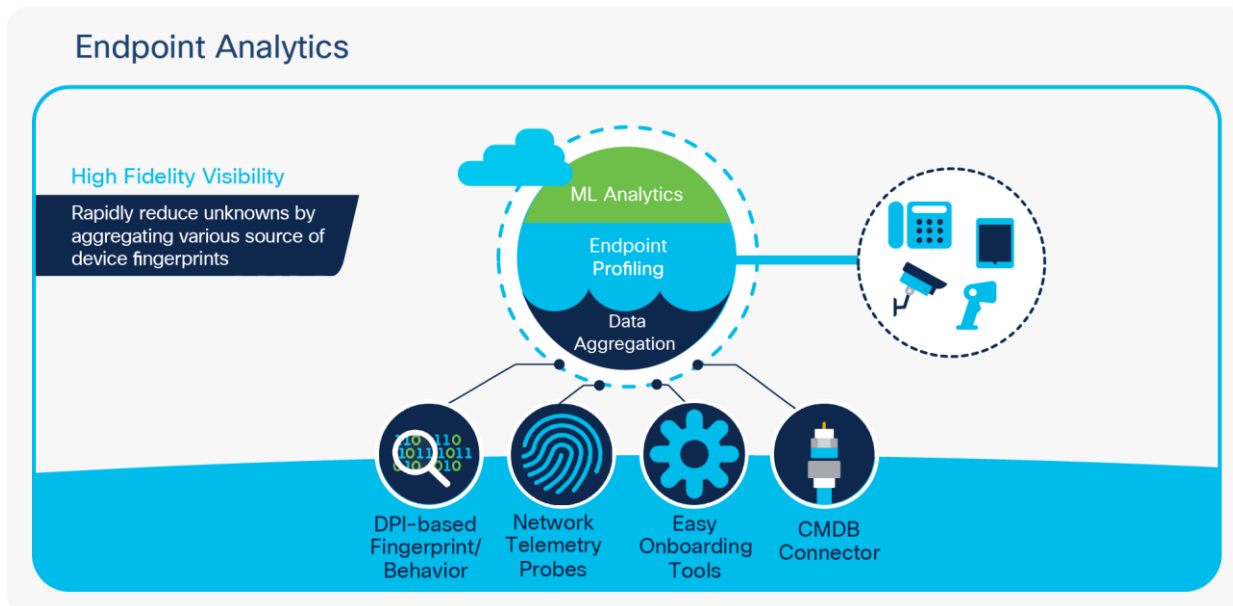
Figure 5.
Cisco ISE Advance Asset Visibility Use-case

Required license:

Basic Asset Visibility and Enforcement - ISE Advantage

Endpoint Analytics Visibility – ISE Advantage

Endpoint Analytics Enforcement – ISE Premier

1.3 Compliance (Posture)

1.3.1 Why Compliance Visibility

Saboteurs focus on intentional data corruption (ransomware) and data exfiltration which compromises endpoints on a network. The most effective and well-publicized compromises take advantage of known issues that could be simply remediated but were overlooked. Compliance Visibility allows organizations to view how user endpoints comply with corporate policy through the use of both Posture and/or integration through Mobile Device Management (MDM) and Enterprise Mobility Management (EMM) systems (supported MDM/EMM systems can be found here). Using either ISE's Posture engine or an MDM, an organization can evaluate how many endpoints are compliant, and ensure that noncompliant software is not installed and/or running.

1.3.2 How does Compliance work
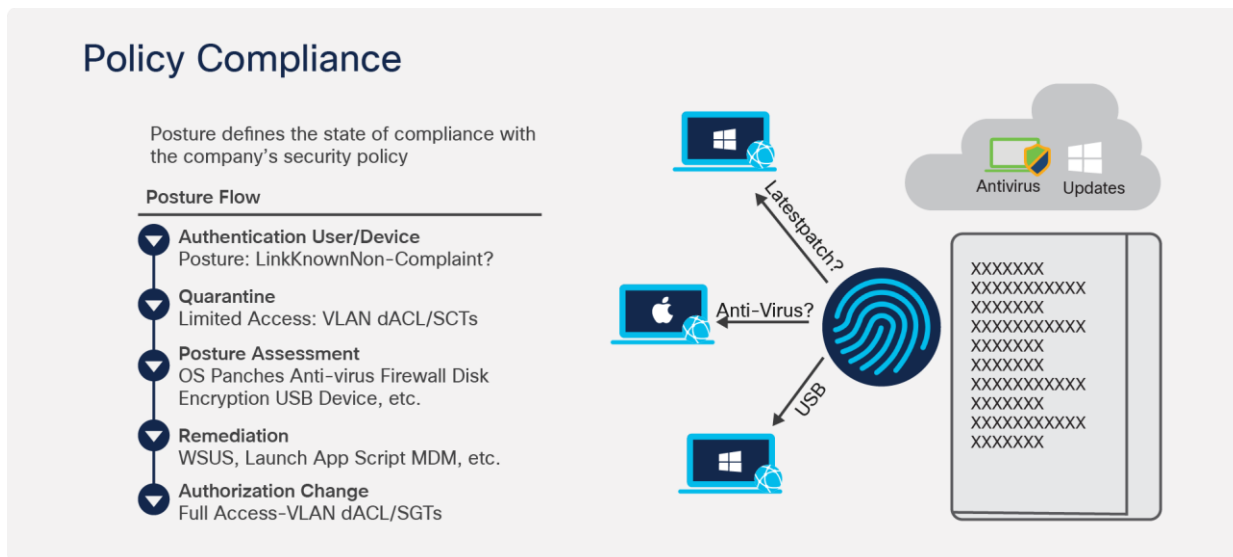
Figure 6.
Cisco ISE Compliance Visibility Use-case

Posture leverages installed and temporal agents looking inside the endpoint to provide assurance that operating system patches, antimalware, firewall, and more are installed, enabled, and up to date before authorizing the device onto the network.
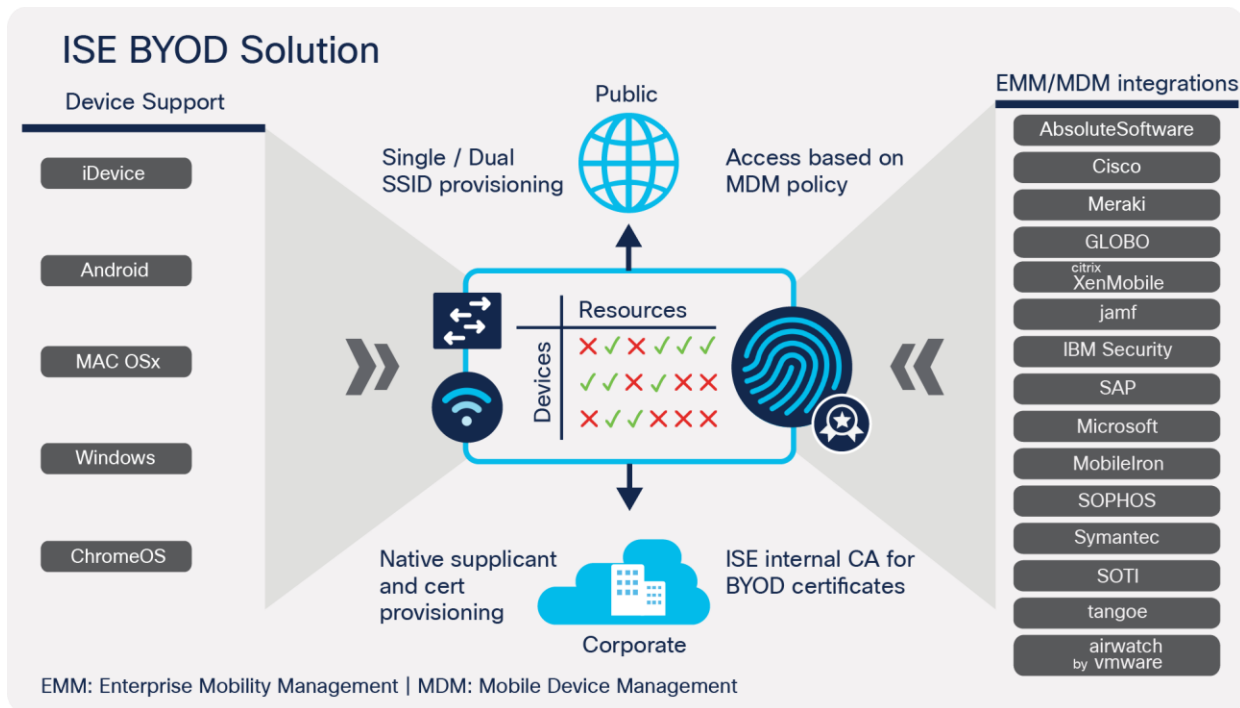
Having good visibility into what endpoints comply with the corporate software policy is usually not enough – customer might want to enable differentiated access to endpoints based on their compliance level. Compliance Enforcement allows taking an overall compliance status, derived through either ISE's own Posture engine or through said MDM/EMM integrations, and use it in an access policy. Combined with other attributes, e.g. identity, this enables a powerful capability that lowers the organizational risks and shrinks the overall threat surface created by non-compliant, unhygienic endpoints trying to connect to the network. Such policy can allow fully compliant endpoints to have full access to required resources by the user using it, while allowing access to only remediation systems, help-desk systems and/or low-risk services by endpoints found non-compliant. Using either ISE's Posture engine or an MDM, an organization can evaluate how many endpoints are compliant, and ensure that non-compliant endpoint with outdated and/or unsupported software cannot access critical resources.

Required license: ISE Premier

1.4 Secure Wired Access

1.4.1 Why Secure Wired Access

Securing the wired network is essential to prevent unauthorized users from connecting their devices to the network. Using ISE, network administrators can provide secure network access by authenticating and authorizing users and devices. Authentication can be active or passive. An active authentication is done using 802.1x when ISE authenticates the user against an Identity Source. Passive authentication involves ISE learning the user's identity via Active Directory (AD) domain logins or other indirect means. Once the user or device authenticates successfully, authorization takes place. Authorization can be achieved by assigning the endpoint's network access session with a dynamic VLAN, downloadable ACL, or other segmentation methods.

1.4.2 How does Secure Wired Access work

Figure 7.
Cisco ISE Secure Wired Access Use-case

ISE authenticates the users and endpoints via 802.1X, Web Authentication, MAB and other means. ISE can query external identity sources for identity resolutions and apply appropriate network policies by instructing the network devices.

Required license: ISE Essentials

1.5 Bring Your Own Device (BYOD)

1.5.1 Why BYOD

Many organizations have instituted a policy that allows the employees to connect their personal devices such as smartphones to the corporate wireless network and use it for business purposes. This is referred to as the Bring Your Own Device (BYOD) policy. However, since these devices are owned by the individuals, they don't like to install management software that allows organizations to "manage" the endpoint. In such situations, ISE provides a very streamlined method to automate the entire BYOD onboarding process – from device registration, supplicant provisioning to certificate installation. This can be done on devices across various OS platforms like iOS, Android, Windows, macOS and ChromeOS. The ISE My Devices Portal, that is completely customizable, allows the end users to onboard and manage various devices.

1.5.2 How does BYOD work

ISE BYOD Solution

Device Support: iDevice, Android, MAC OSx, Windows, ChromeOS

Public — Single / Dual SSID provisioning — Access based on MDM policy

Resources / Devices

Native supplicant and cert provisioning — ISE internal CA for BYOD certificates — Corporate

EMM/MDM integrations: AbsoluteSoftware, Cisco, Meraki, GLOBO, citrix XenMobile, jamf, IBM Security, SAP, Microsoft, MobileIron, SOPHOS, Symantec, SOTI, tangoe, airwatch by vmware

EMM: Enterprise Mobility Management | MDM: Mobile Device Management

https://cisco.com/go/csta

Figure 8.
Cisco ISE BYOD Use-case

ISE provides multiple elements that help automate the entire onboarding aspect for BYOD. This includes a built-in Certificate Authority (CA) to create and help distribute certificates to different types of devices. The built-in CA provides a complete certificate lifecycle management. ISE also provides a My Devices Portal, an end user facing portal, that allows the end user to register their BYOD endpoint as well as mark it as being lost to blacklist it from the network. BYOD on boarding can be accomplished either through a single SSID or through a dual SSID approach. In a single SSID approach, the same SSID is used to onboard and connect the end user's device while in a Dual SSID approach a different open SSID is used to on board the devices but the device connects to a different more secure SSID after the onboarding process. For customers that want to provide a more complete management policy, BYOD can be used to connect the end user to the MDM onboarding page as well.

Required license: ISE Advantage

1.6 Rapid Threat Containment (RTC)

1.6.1 Why Threat Containment

Cisco RTC makes it easy to get fast answers about threats on your network and to stop them even faster. It uses an open integration of Cisco security products, technologies from Cisco partners, and the extensive network control of Cisco ISE.

With integrated network access control technology, you can manually or automatically change your users' access privileges when there's suspicious activity, a threat or vulnerabilities discovered. Devices that are suspected of being infected can be denied access to critical data while their users can keep working on less critical applications.

1.6.2 How does Rapid Threat Containment work
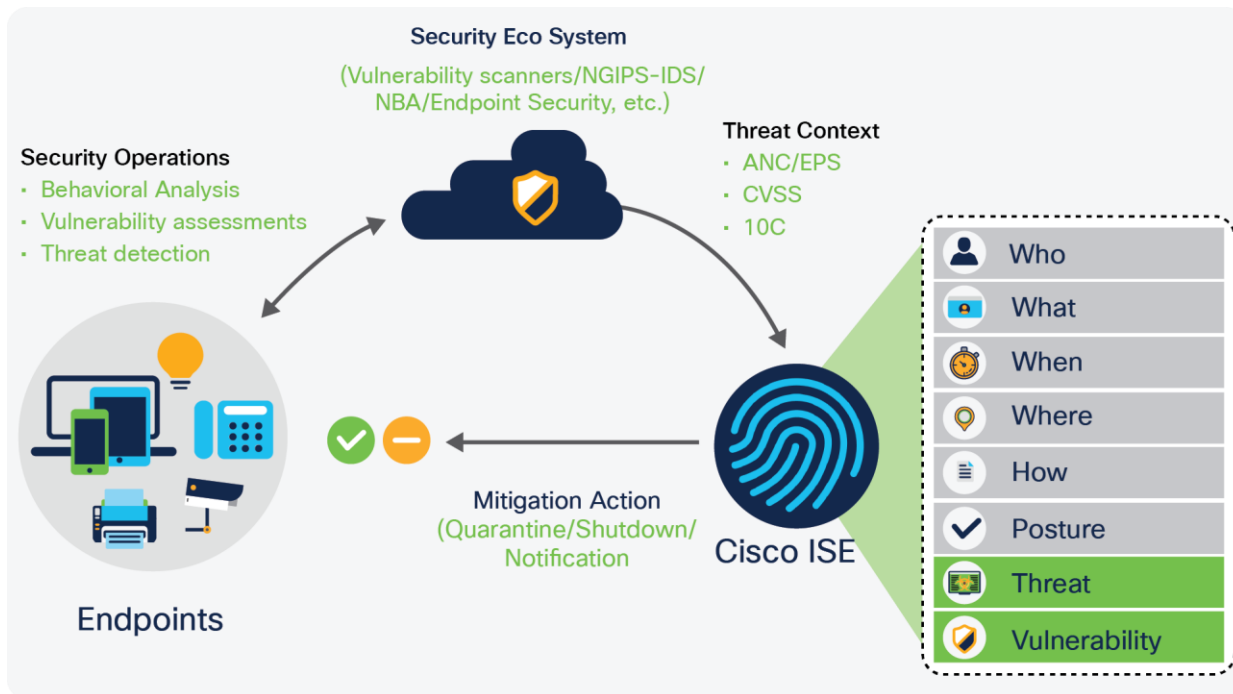
Figure 9.
Cisco ISE RTC Use-case

Cisco ISE integrates with security eco-system partners over pxGrid and/or Application Programming Interfaces (APIs) to learn threat level of the endpoints to take mitigation actions.

Upon detecting a flagrant threat on an endpoint, a pxGrid eco-system partner can instruct ISE to contain the infected endpoint either manually or automatically. The containment can involve moving the device to a sandbox for observation, moving it to a remediation domain for repair, or removing it completely. ISE can also receive the standardized Common Vulnerability Scoring System (CVSS) classifications and the Structured Threat Information Expression (STIX) threat classifications, so that graceful manual or automatic changes to a user's access privileges based on their security score can be made.

Cisco ISE integrates with more than 75 eco-system partners over pxGrid to implement several use cases. All the technology partners and the technical details about integrations can be found here:
https://community.cisco.com/t5/security-documents/ise-design-amp-integration-guides/ta-p/3621164

A complete list of eco-system partners can be found here: https://cisco.com/go/csta

Required license: ISE Premier

1.7 Segmentation

1.7.1 Why Segmentation

Network segmentation is a proven technology to protect critical business assets, but traditional approaches are complex. Cisco Group Based Policy/TrustSec software-defined segmentation is simpler to enable than VLAN-based segmentation. Policy is defined through security groups. It is an open technology in IETF, available within Open Daylight, and supported on third-party and Cisco platforms. ISE is the Segmentation controller, which simplifies the management of switch, router, wireless, and firewall rules. Group Based Policy / TrustSec Segmentation provides better security for lower cost compared to traditional segmentation. Forrester Consulting found in an analysis of customers that operational costs are reduced by 80% and policy changes are 98% faster.

1.7.2 How does Segmentation works
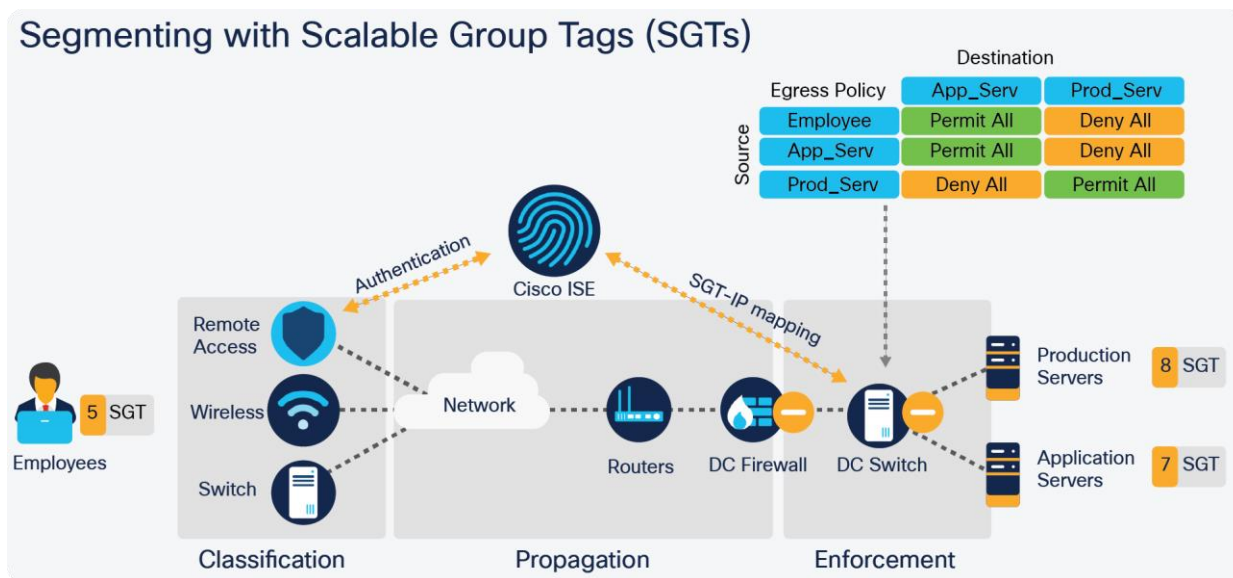
Figure 10.
Cisco ISE Segmentation Use-case

The illustration above show users and devices are assigned to security groups and consequently their group membership is known throughout the network so any enforcement device along the path can evaluate policy based on the group-to-group approved communication.

Software Defined Access

Segmentation is a key element of Software Defined Access (SDA). Together Cisco Digital Network Architecture (DNA) Controller and ISE automate network segmentation and group-based policy. Identity based Policy and Segmentation decouples security policy definition from VLAN and IP addresses. The Software Defined (SD) Access Design and Deployment guides detail the configuration and deployment of Group Based Policy.
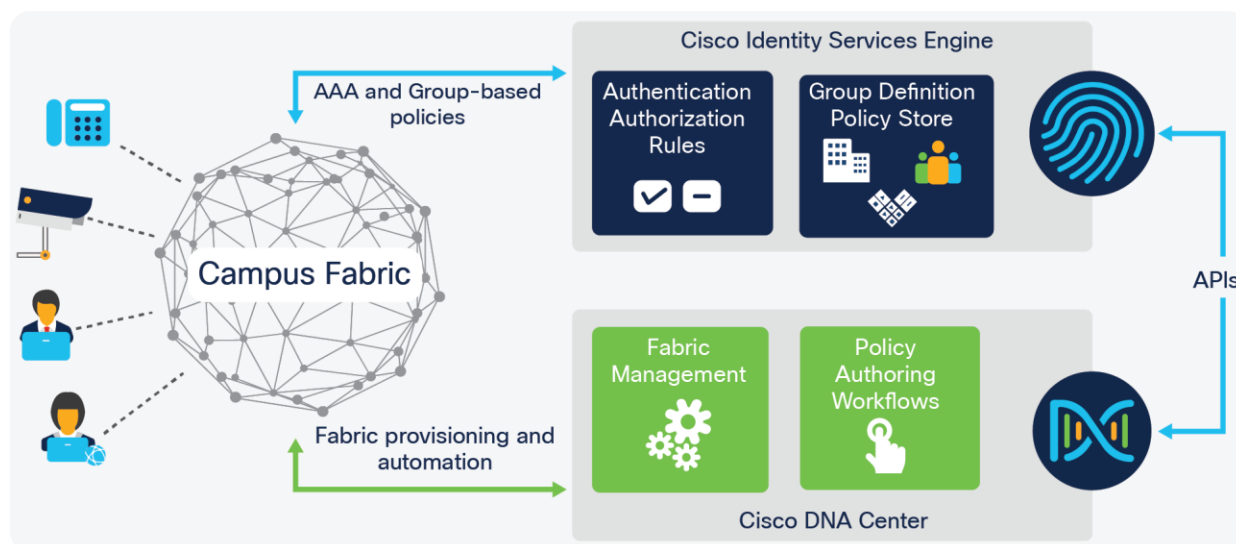
Figure 11.
Cisco ISE SDA Integration Use-case

To extend segmentation across the enterprise network, ISE interfaces with the Cisco Application Centric Infrastructure (ACI) Controller, which is also called Application Policy Infrastructure Controller – Data Center (APIC- DC), to learn EPG names, share Software Group (SG) names and corresponding EPG value, SGT value and Virtual Routing and Forwarding (VRF) Name. This allows Cisco ISE to create and populate SG-EPG translation tables, which are obtained by the border device to translate TrustSec-ACI identifiers as traffic passes across the domains. The TrustSec – ACI Policy Plane integration guide gives an overview of ACI and the configuration of the policy plane integration.

TrustSec technology is supported in over 50 Cisco product families and works with open source and third-party products. ISE acts as the policy controller for routers, switches, wireless, and security products. Details about product TrustSec capabilities are provided in the Platform Capability Matrix. The Quick Start Config Guide illustrates a typical TrustSec network deployment with step by step configuration of a sample environment. More design guides are also provided here.

Required license: ISE Advantage

Note: Licenses that enable Segmentation via SDA: Advantage or Premier on ISE, and Cisco DNA Premier / Cisco DNA Advantage. Please find more information in the SDA Ordering Guide

1.8 Security Ecosystem Integrations

1.8.1 Why Security Ecosystem Integrations

ISE builds contextual data about endpoints in terms of its device type, location, time of access, posture, user(s) associated to that asset and much more. Endpoints can be tagged with Scalable Group Tags (SGTs) based on these attributes. This rich contextual insight can be used to enforce effective network access control policies and can also be shared with eco-system partners to enrich their services. For example, in the Cisco Next Generation Firewall (NGFW), policies can be written based on the identity context such as device-type, location, user groups and others, received from ISE. Inversely, specific context from 3rd party systems can be fed in to the ISE to enrich its sensing and profiling capabilities, and for Threat Containment. The context exchange between the platforms can be done via Cisco® pxGrid or REST APIs.

External RESTful Services (ERS) on ISE serves both the purpose of context sharing (in and out) and management of ISE for specific set of use cases over REST APIs.

1.8.2 How do Security Ecosystem Integrations work?
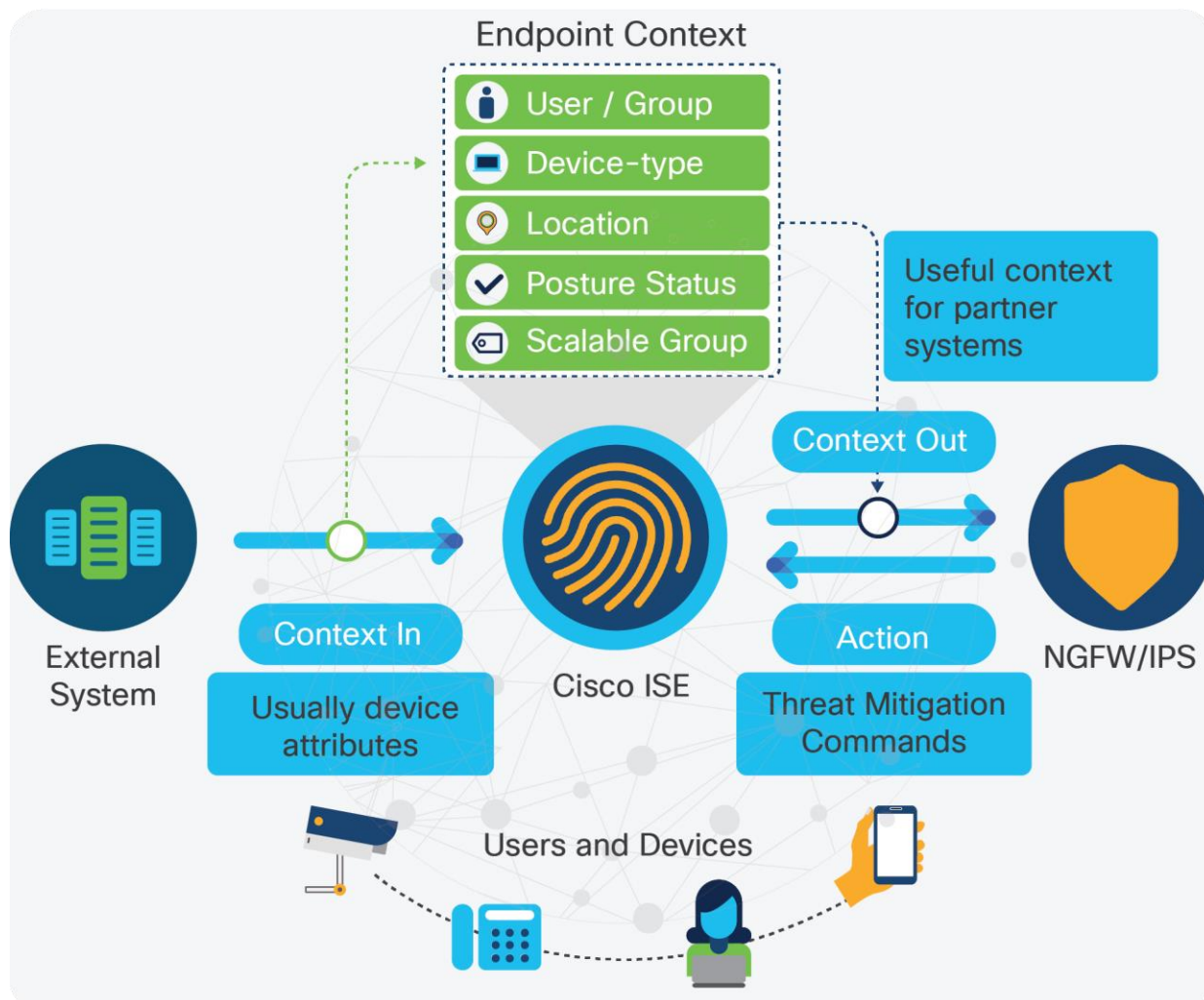
Figure 12.
Cisco ISE Security Integration

The context exchange between the platforms can be done via Cisco® pxGrid or REST APIs.

Cisco ISE integrates with more than 75 eco-system partners over pxGrid to implement technology partners and the technical details about integrations can be found here: https://community.cisco.com/t5/security-documents/ise-design-amp-integration-guides/ta-p/3621164

A complete list of eco-system partners can be found here: https://cisco.com/go/csta

Required license: ISE Advantage

1.9 Device Administration (TACACS+)

1.9.1 Why Device Administration

Network and security administrators typically own the task of administering and monitoring network and security devices in an enterprise. When there are only a handful of devices, keeping track of the admin users, privileges, and changes to configuration is not very difficult. However, when the network grows to tens, hundreds, and thousands of devices, it would be a nightmare to manage the devices without automation and smooth workflow. ISE provides the capability to automate device administration tasks with clean workflows and monitoring capabilities within a controlled space in the UI using TACACS+ protocol, which allows for providing different permissions to network operators.

1.9.2 How does Device Administration work
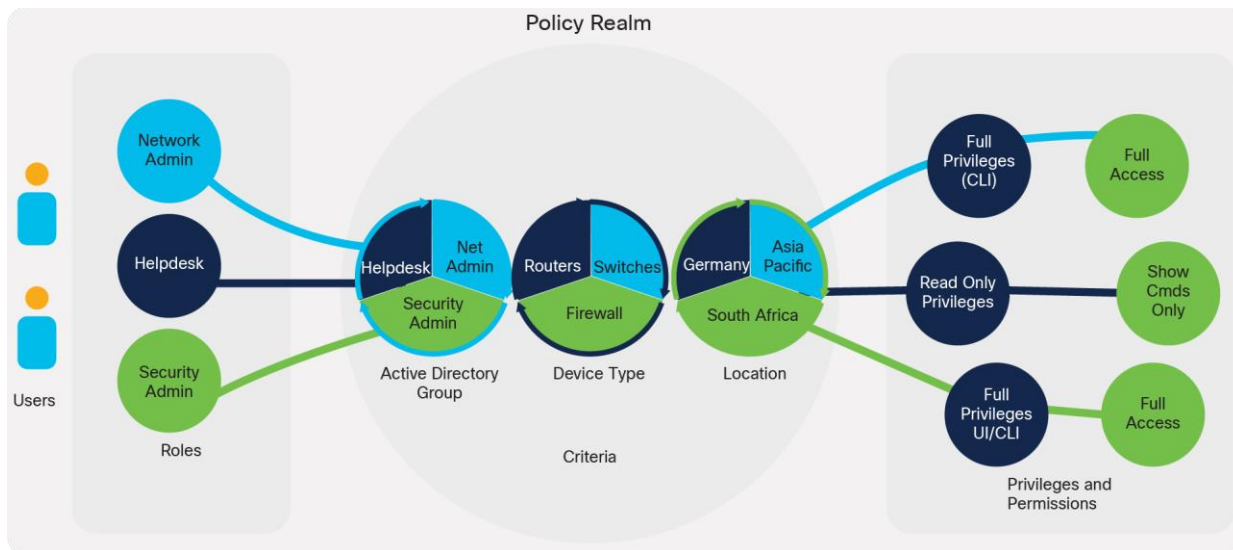
Figure 13.
Cisco ISE Device Administration Use-case

When a network administrator tries to connect to a network device, the device sends out a "request for connection" to ISE, and ISE asks for their credentials. Credentials are verified against an identity source.

Next, the network device asks ISE to authorize the network administrator. Once they get access to the shell prompt, the network administrator can start executing commands. ISE can be configured to authorize individual commands as well.

1.9.3 How do I license Device Administration

- License that enables Device Administration: Device Admin License

- License consumption: Device Administration licenses are consumed per policy service node. You must have Device Administration license for each of the policy service nodes that you enable TACACS+ service on. Device Administration using TACACS+ does not consume endpoints, and there is no limit on network devices for Device Administration. The user does not require a legacy base license.

- Find the SKU here.

2. What you need for your ISE deployment

This section helps new customers understand the primary components needed in order to start the deployment. This is a great place to start if you're looking to understand the ISE licenses, appliances and services offered.
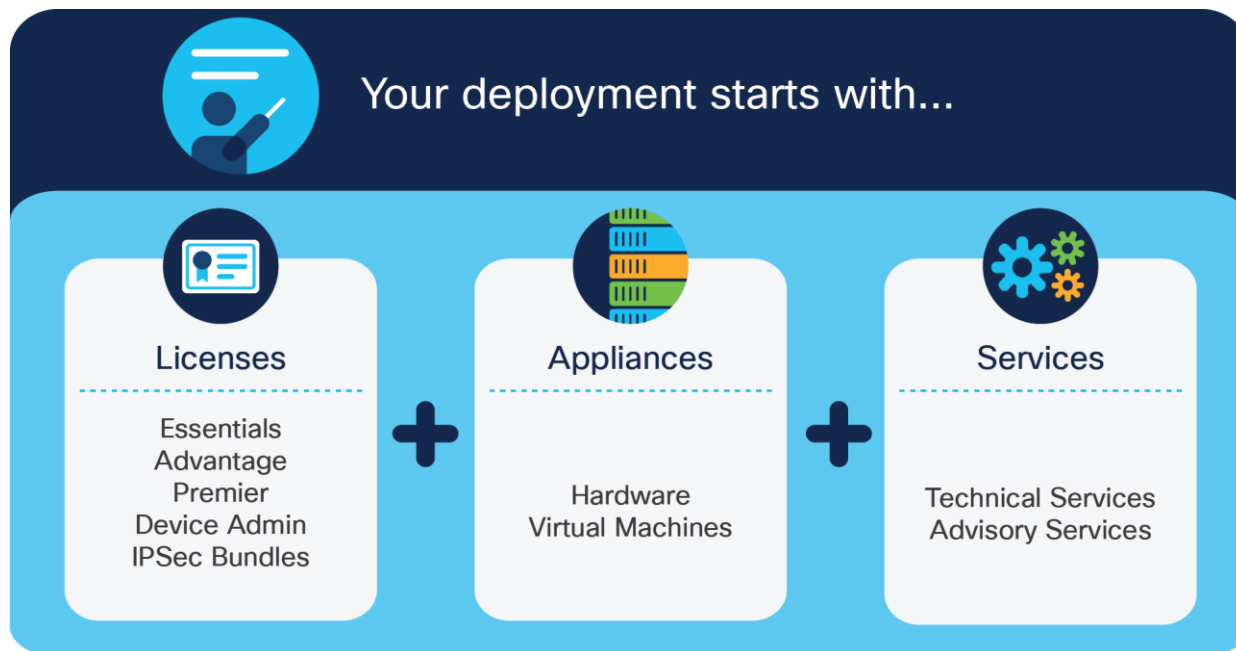
Figure 14.
Cisco ISE Deployment

2.1 Licenses

2.1.1 Understanding the License model

Subscriptions Overview

Cisco ISE licenses are licensed on a subscription basis. Subscriptions are available for standard term lengths of 1, 3, and 5 years. Following the completion of the term, the subscription will be automatically renewed for an additional 1-year term unless the renewal is canceled.

Existing subscriptions may be changed during the term of the subscription. Changes may be made to products and/or quantities ordered. Additional quantities may be added to the subscription at any time during the subscription term by placing a "change-subscription" order. Quantities added through a Change-Subscription order will co-terminate with the existing subscription. Quantities may be decreased for a subscription renewal, but not mid-term for a current subscription. Click here for more information on the change-subscription transaction.

Cisco ISE Licensing

Cisco ISE licensing provides the ability to manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources. Licensing in Cisco ISE is supplied as feature-based packages with different features supported in each of the Essentials, Advantage, or Premier license. Full details on features support is listed in Table 1.

Session Bands

The session-based license follows a tiered pricing model where pricing depends on the session count and the term of the subscription. Sales and partner representatives should determine the correct sizing for each customer deployment so that the appropriate session count is selected (the minimum is 100 sessions). Cisco Commerce (CCW) will dynamically determine the correct price associated with the session count that is entered.

Session Bands
100 – 999 Sessions
1000 – 2499 Sessions
2500 – 4999 Sessions
5000 – 9999 Sessions
10,000 – 24,999 Sessions
25,000 – 49,999 Sessions
50,000 – 99,999 Sessions
100,000+ Sessions

2.1.1 Overall feature view

Below is a list of ISE licenses offered. Features under the licenses are mutually exclusive.

Cisco ISE License Package	Focus	Perpetual or Subscription (Terms Available)	Notes
Essentials	Provides AAA and guest services for user-based visibility and enforcement.	Subscription (1, 3, or 5 years)	
Advantage	Provides complete IoT and user device visibility, basic IoT device enforcement, and context sharing about sessions. Includes functionality in the Essentials license.	Subscription (1, 3, or 5 years)	
Premier	Provides advanced IoT device enforcement, user device enforcement, and cloud services. Includes functionality in the Advantage license.	Subscription (1, 3, or 5 years)	
Device Administration (DA)	Enables Device Administration/TACA CS+ support for networking devices	Perpetual	One license per ISE Policy Service Node (PSN) with TACACS+ Persona enabled.

Cisco ISE License Package	Focus	Perpetual or Subscription (Terms Available)	Notes
IPSec	Enables VPN communication between Cisco ISE PSNs and Cisco Network Access Devices	Perpetual	One license per ISE PSN used for IPsec VPN communication to NADs with up to 150 IPsec tunnels per ISE PSN

Table 1.   Cisco ISE features and licenses mapping

	Cisco ISE Feature or Service	License			
		Essentials	Advantage	Premier	DA
Access to the Network	Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass and Easy Connect, and Web authentication	✓	✓	✓	X
	MACsec (all)	✓	✓	✓	X
	SSO, SAML, ODBC–based authentication	✓	✓	✓	X
	Guest portal and sponsor services	✓	✓	✓	X
	Representational state transfer (monitoring) APIs	✓	✓	✓	X
	External RESTful services (CRUD)–capable APIs	✓	✓	✓	X
	PassiveID (Cisco Subscribers)	✓	✓	✓	X
	PassiveID (Non–Cisco Subscribers)	X	✓	✓	X
	Secure Wired and Wireless Access	✓	✓	✓	X
	Device registration (My Devices portal) and provisioning for Bring Your Own Device (BYOD) with built-in Certificate Authority (CA)	X	✓	✓	X
Segmentation	Security Group Tagging (Cisco TrustSec® SGT) and ACI integration	X	✓	✓	X

	Cisco ISE Feature or Service	License			
		Essentials	**Advantage**	**Premier**	**DA**
Asset Visibility	Basic Asset Visibility and Enforcement (Profiling)	X	✓	✓	X
	Basic Asset Feed Service	X	✓	✓	X
	Advanced Asset Visibility (Endpoint Analytics)	X	✓	✓	X
	Advanced Asset Enforcement (Endpoint Analytics)	X	X	✓	X
	Visibility and Enforcement based on Location-based integration	X	✓	✓	X
Context Sharing and Response	Context Sharing and Security Ecosystem Integrations	X	✓	✓	X
	Endpoint Protection Services (EPS)	X	X	✓	X
	Rapid Threat Containment (RTC) (using Adaptive Network Control and context sharing)	X	X	✓	X
Compliance	Posture Visibility and Enforcement	X	X	✓	X
	Visibility and Enforcement through Enterprise Mobility Management and Mobile Device Management (EMM and MDM) integration	X	X	✓	X
	Threat-centric NAC	X	X	✓	X
Device Administration	Device Administration (TACACS+)	X	X	X	✓

2.1.2 Features and exceptions to consumption of license

Mostly all the features irrespective of ISE license result in consumption of a license session except for the ones listed in the table below:

Cisco ISE Feature or Service	Description	License consumed
PassiveID (Cisco-only Subscribers)	Gathering, collating, and caching authentication data (username, IP address and MAC) from other servers in the data center and distributing the authentication data to subscribing systems	No
PassiveID (Non-Cisco Subscribers)	Gathering, collating, and caching authentication data (username, IP address, and MAC) from other servers in the data center and distributing the authentication data to subscribing systems	No
Profiler feed service	Dynamic downloading of endpoint classification rules	No
My Devices portal* and NSP	Self-service web portal for users to add and manage their sessions with automatic Network Supplicant Provisioning (NSP)	No
Context sharing	User and endpoint contextual attribute (who, what, where, when, etc.) data exchange between Cisco ISE and third- party system through pxGrid	No
Endpoint Protection Services (EPS)	APIs for delivering dynamic network controls of active network sessions	No
Cisco TrustSec and ACI integration	The ACI TrustSec integration provides a solution interconnecting the administrative domains of Cisco TrustSec and Application Centric Infrastructure (ACI) to provide a consistent end-to-end policy segmentation.	No

Take me to the Cisco ISE License SKUs

Note: For all features that do not directly consume sessions, it is required to still match the number of licenses with the number of devices in the deployment.

Table 2. 2.1.3 Context exchange licensing requirements

Authentication Mechanism	Context Shared With	License Requirement
Cisco ISE	Cisco platforms	Advantage 1:1 Number of endpoints
Cisco ISE	Third-party platforms	Advantage 1:1 Number of endpoints
Non-ISE Authentication (e.g., AD)	Cisco platforms	Essentials
Non-ISE Authentication (e.g., AD)	Third-party platforms	Advantage 1:1 Number of endpoints

Note: Each active endpoint's context shared with an external system will consume an Advantage license. Each active endpoint session information shared with an external system will need a 1:1 Advantage license. For example, when a Windows laptop authenticates via 802.1X, one Essentials license is consumed. If this endpoint's context is shared with Cisco Stealthwatch or NGFW, one additional Advantage license will be consumed.

2.1.5 Device Admin license and corresponding features

To manage administrative access to network devices.

[Take me to the Cisco ISE Device Admin SKUs](#)

2.1.6 IPSec license and corresponding features

Allow s VPN communication between Cisco ISE PSNs and Cisco Network Access Devices.

[Take me to the Cisco ISE IPSec SKUs](#)

2.1.7 Product and solution bundle offerings

ISE licenses are also available as part of Cisco's many product and solution bundle offerings.

- [Software Volume Purchasing](#)
- [Enterprise Agreement](#)
- [Enterprise License Agreement](#)
- [Cisco One](#)

2.2 Appliances

Cisco ISE supports both physical and virtual appliances. You can find more details on Cisco ISE appliances [here](#).

2.2.1 Hardware

These are physical appliances delivered by Cisco that reside in your deployment.

Please note that ISE appliances always ship with the latest version of software, but the software version can be changed manually. This would be in the form of a fresh installation. Please refer to the release notes and administrator guide of the ISE release you plan to install.

2.2.2 Virtual Machine

Cisco ISE virtual appliances are supported on VMware ESX/ESXi 5.x and 6.x and KVM on RedHat Enterprise Linux (RHEL) 7. Virtual appliances should be run on hardware that equals or exceeds the configurations of the physical platforms listed in the Cisco ISE [datasheet](#). Cisco ISEvirtual target should comply with the required memory and disk space requirements which can be found in the installation guide here: [Cisco Identity Service Installation Guide](#)

2.3 Services

2.3.1 Technical Services

Smart Net Total Care® or SWSS contracts for Cisco ISE physical and virtual appliances are available. Smart Net Total Care and SWSS contracts for Cisco ISE physical and virtual appliances cover Base and Device Admin deployments as well. Cisco Software Support Service (SWSS) Basic is included for the duration of all Cisco ISE subscription licenses however, Smartnet SNT or another level of service must be purchased to activate that SWSS.

Higher-value service levels, Software Support Enhanced and Premium, are available for Cisco Base license and all Cisco ISE subscription licenses. These service levels provide everything included in Software Support Basic with a richer feature set such as software configuration guidance, direct access to experts with faster response time and technical adoption support. Software Support Enhanced and Premium is available on two billing platforms: Subscription Billing Platform (SBP) and Term and Content. For the ISE 3.0 purchase on SBP, support options will be available in the product ordering configuration. For the product purchase on term and content platform, the support is available via a top-level ATO PID in CCW: CISE-SW-SUPP.

2.3.2 Advisory Services

Cisco offers Advisory Services to address your business objectives with the technology we offer. For example, the Cisco Security Segmentation Service provides a strategic infrastructure segmentation approach to ensure the success of your Segmentation initiative.

3. What's new

This section helps existing customers of ISE understand the latest SKUs available for ISE, information directing to end of life announcements of ISE SKUs and the comparison of legacy vs latest SKUs.

3.1 Highlights

We are introducing a new model for ISE Licensing, which is a subscription-only model with Smart License SKUs. In the new model, three subscription-based license tiers exist, namely ISE Essentials, ISE Advantage, and ISE Premier. This new model is referred to as a nested-doll model, which means that the higher tier license already includes all lower-tier features. For example, the ISE Premier license includes all ISE Advantage and ISE Essential features. Similarly, the ISE Advantage license includes all ISE Essential features. The subscription term for each tier is 1, 3, and 5 years.
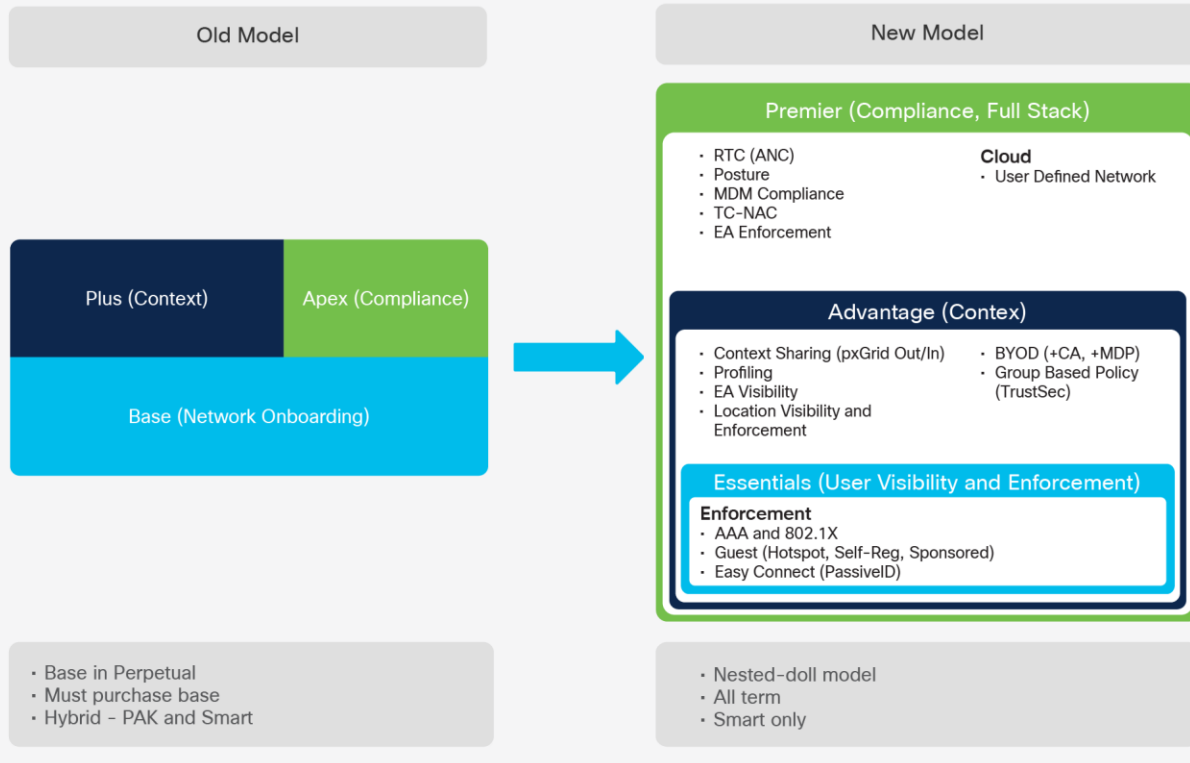
3.2 End-of-life notices

Please find all end-of-life notices announced for various ISE licenses and appliances here.

3.3 Virtual Machine and Device Administration License behavior

With both the legacy and current format of license being consumed today, it is useful to understand how the licenses are enforced on ISE pre-2.4 and post-2.4 releases.

The table below explains the same.

License on release	Pre-2.4 release	Release 2.4 and Beyond
New VM license	Licensed with no enforcement	Licensed with PAK and smart licensing enforcement
Legacy VM license	Licensed with no enforcement	Licensed with PAK and smart licensing enforcement
New Device Admin license	Is identified and consumed as uncounted (unlimited number of ISE TACACS+ nodes within the deployment)	Is identified and enables consumption of 1 ISE TACACS+ node
Legacy Device Admin license		Is identified and enables consumption of up to 50 ISE TACACS+ nodes

For Essentials, Advantage, and Premier licenses, there is no change in the license identification or consumption behavior.

3.4 What to expect during upgrade to version 2.4 and greater

3.4.1 ISE Virtual Machine (VM) Nodes

Customers who purchased the Legacy VM licenses will need to obtain a Product Authorization Key (PAK) for each VM licenses purchased when upgrading to ISE 2.4 and beyond. To obtain a PAK, email ise-vm-license@cisco.com. Include the Sales Order numbers that reflect the ISE VM purchase, and your Cisco ID in your email. Cisco will, in return, provide a medium VM PAK which is reflective of the VM specifications prior to the introduction of small, medium, and large VM licenses with ISE 2.4. A medium VM PAK can be used with small and medium VM installations.

If you upgrade to ISE 2.4 prior to obtaining a PAK, the deployment displays a warning, at which point you may start using the new license procured. While on ISE 2.4, this is only a warning message and does not disrupt any user's ISE experience.

With ISE 3.0, the VM licenses need to be converted to Smart Licenses.

If you are unable to locate the sales order number pertaining to your past purchase of ISE VM, please reach out to your Cisco sales representative or partner.

3.4.2 Appliance ISE nodes

No action is needed. ISE appliances with valid support period can be upgraded to the latest software with no additional license action for the appliance.

3.4.3 Device Admin

No action is needed. Legacy Device Admin licenses are grandfathered.

The legacy Device Admin license entitles an entire deployment of ISE to TACACS+ feature usage. This means that all 50 ISE Policy Service Nodes (PSNs) can be enabled with TACACS+ capabilities.

Upon upgrade to ISE Release 2.4, the same legacy Device Admin license continues to entitle the deployment with a total count of 50 PSNs that could be enabled with TACACS+ capabilities.

Upon upgrade to the ISE 3.0 release, the Device Admin license must be converted to a Smart License.

3.4.4 Base, Plus, and Apex

These licenses have been migrated to the new ISE Essentials, Advantage, and Premier licenses starting in the ISE 3.0 release.

For complete behavior of these licenses upon upgrade to ISE Release 3.0, please refer to the section on Migration below.

4. Migration from other older licenses to today

Starting with the 3.0 release, you are required to have Smart Licensing, which further requires you to have a Smart Account created and configured before you upgrade or migrate the ISE licenses. Cisco Smart Software Licensing helps you to procure, deploy, and manage licenses easily where devices self-register and report license consumption, removing the need for Product Activation Keys (PAKs). This licensing uses Cisco Smart Software Manager (CSSM) to obtain the necessary authorization.

If you purchased one of the older licenses in the past (Base, Plus, or Apex) and would like to understand how to migrate to today's licenses, please go here.

End-of-life announcement for all these licenses can be found here.

Customers experiencing an issue with licensing and migration may open a case via Cisco Support Case Manager (SCM) at https://cs.co/scmswl (choose 'licensing' option in SCM) with the Cisco sales order number reflecting the ISE purchase.

4.6 ISE Base Licenses

This license is only valid for releases prior to ISE 3.0. Features included were: Authentication, Authorization, Accounting, Guest, PassiveID, and Security Group Tags. The Cisco ISE Base license offered a similar feature set to what is in Essentials today.

Table 3.   Cisco ISE Base licenses

Part Number (SKU)	Description
L-ISE-BSE-P1	Cisco ISE Base License - Sessions 100 to 249
L-ISE-BSE-P2	Cisco ISE Base License - Sessions 250 to 499
L-ISE-BSE-P3	Cisco ISE Base License - Sessions 500 to 999
L-ISE-BSE-P4	Cisco ISE Base License - Sessions 1000 to 2499
L-ISE-BSE-P5	Cisco ISE Base License - Sessions 2500 to 4999
L-ISE-BSE-P6	Cisco ISE Base License - Sessions 5000 to 9999
L-ISE-BSE-P7	Cisco ISE Base License - Sessions 10,000 to 24,999
L-ISE-BSE-P8	Cisco ISE Base License - Sessions 25,000 to 49,999
L-ISE-BSE-P9	Cisco ISE Base License - Sessions 50,000 to 99,999
L-ISE-BSE-P10	Cisco ISE Base License - Sessions 100,000 to 249,999
L-ISE-BSE-P11	Cisco ISE Base License - Sessions 250,000 and above

4.7 ISE Plus Licenses

This license is only valid for releases prior to ISE 3.0. Features included were: Profiling, Context Sharing, BYOD (including the My Devices Portal), and Rapid Threat Containment.

Table 4.   Cisco ISE Plus subscription licenses

Description	5-Year Subscription Licenses	3-Year Subscription Licenses	1-Year Subscription Licenses
100 – 249 Sessions	L–ISE–PLS–5Y–S1	L–ISE–PLS–3Y–S1	L–ISE–PLS–1Y–S1
250 – 499 Sessions	L–ISE–PLS–5Y–S2	L–ISE–PLS–3Y–S2	L–ISE–PLS–1Y–S2
500 – 999 Sessions	L–ISE–PLS–5Y–S3	L–ISE–PLS–3Y–S3	L–ISE–PLS–1Y–S3
1000 – 2499 Sessions	L–ISE–PLS–5Y–S4	L–ISE–PLS–3Y–S4	L–ISE–PLS–1Y–S4
2500 – 4999 Sessions	L–ISE–PLS–5Y–S5	L–ISE–PLS–3Y–S5	L–ISE–PLS–1Y–S5
5000 – 9999 Sessions	L–ISE–PLS–5Y–S6	L–ISE–PLS–3Y–S6	L–ISE–PLS–1Y–S6
10,000 – 24,999 Sessions	L–ISE–PLS–5Y–S7	L–ISE–PLS–3Y–S7	L–ISE–PLS–1Y–S7
25,000 – 49,999 Sessions	L–ISE–PLS–5Y–S8	L–ISE–PLS–3Y–S8	L–ISE–PLS–1Y–S8
50,000 – 99,999 Sessions	L–ISE–PLS–5Y–S9	L–ISE–PLS–3Y–S9	L–ISE–PLS–1Y–S9
100,000–249,999 Sessions	L–ISE–PLS–5Y–S10	L–ISE–PLS–3Y–S10	L–ISE–PLS–1Y–S10
250,000+ Sessions	L–ISE–PLS–5Y–S11	L–ISE–PLS–3Y–S11	L–ISE–PLS–1Y–S11

4.8 ISE Apex Licenses

This license is only valid for releases prior to ISE 3.0. Features included were: Posture, Enterprise Mobility Device Management Integration, and TC–NAC.

Table 5.   Cisco ISE Apex subscription licenses

Description	5-Year Subscription Licenses	3-Year Subscription Licenses	1-Year Subscription Licenses
100 – 249 Sessions	L–ISE–APX–5Y–S1	L–ISE–APX–3Y–S1	L–ISE–APX–1Y–S1
250 – 499 Sessions	L–ISE–APX–5Y–S2	L–ISE–APX–3Y–S2	L–ISE–APX–1Y–S2
500 – 999 Sessions	L–ISE–APX–5Y–S3	L–ISE–APX–3Y–S3	L–ISE–APX–1Y–S3
1000 – 2499 Sessions	L–ISE–APX–5Y–S4	L–ISE–APX–3Y–S4	L–ISE–APX–1Y–S4
2500 – 4999 Sessions	L–ISE–APX–5Y–S5	L–ISE–APX–3Y–S5	L–ISE–APX–1Y–S5
5000 – 9999 Sessions	L–ISE–APX–5Y–S6	L–ISE–APX–3Y–S6	L–ISE–APX–1Y–S6
10,000 – 24,999 Sessions	L–ISE–APX–5Y–S7	L–ISE–APX–3Y–S7	L–ISE–APX–1Y–S7

Description	5-Year Subscription Licenses	3-Year Subscription Licenses	1-Year Subscription Licenses
25,000 – 49,999 Sessions	L-ISE-APX-5Y-S8	L-ISE-APX-3Y-S8	L-ISE-APX-1Y-S8
50,000 – 99,999 Sessions	L-ISE-APX-5Y-S9	L-ISE-APX-3Y-S9	L-ISE-APX-1Y-S9
100,000–249,999 Sessions	L-ISE-APX-5Y-S10	L-ISE-APX-3Y-S10	L-ISE-APX-1Y-S10
250,000+ Sessions	L-ISE-APX-5Y-S11	L-ISE-APX-3Y-S11	L-ISE-APX-1Y-S11

5. Cisco ISE ordering (SKUs) and entitlement information

5.1 Cisco ISE License Ordering

- All Cisco ISE licenses are orderable in the Cisco Commerce Workspace (CCW) and are listed on the Global Price List (GPL)

- Cisco ISE endpoint session-based licenses can be ordered in any quantity starting with 100 sessions

- Please note for Subscription licenses:

  ○ These can be ordered with 1-, 3(default)-, or 5-year terms

  ○ Support contracts on all the Cisco ISE appliances (physical or virtual) in a deployment are a prerequisite to purchasing and using ISE term-based licenses

  ○ Default start of license usage is immediate. At the time of ordering, this start date can be adjusted up to 60 days out from the current date. This calculation can be performed by CCW for you by counting backwards from the end date the duration of the license or forward from the start date

  ○ The term can be between 12 and 60 months, allowing the licenses to be co-termed

5.1.1 Cisco ISE License Entitlement

Customers are entitled to utilize the quantity and duration of the license per terms and conditions agreed upon at the time of purchase.

Relevant ISE releases: 2.2 and later

Out of compliance: A license is out of compliance when

(a) the deployment uses more than 125% (to account for a temporary burst of usage) sessions compared to the quantity purchased; or

(b) the licenses have expired without renewal.

Compliance enforcement: The impact described below is experienced after a deployment is out of compliance for 45 out of 60 consecutive days.

Alerts will be provided every day that a license is out of compliance. For term licenses, alerts are provided, 90, 60 and 30 days before expiry and also for the last 30 consecutive days before expiry.

Impact: There will be no impact to end users. Existing configuration continues to operate without disruption.

However, visibility and management of the features associated with an out-of-compliance license will be affected.

This means the ISE deployment administrator encounters limited read-only capability over the relevant features until the out-of-compliance is fixed.

These enforcement actions are subject to change in the future and will be conveyed in relevant release material.

5.1.2 Cisco ISE SKU Overview

Orders for Cisco ISE license subscription involves three SKU types:

- The subscription SKU, which is used to define the subscription term and start date
- The product SKUs, which are used to define the products and quantities that make up the subscription
- The support SKUs, which define the level of support for the subscription

Orders start with the selection of the Umbrella subscription SKU, which is followed by the configuration of the subscription by selecting the product and support SKUs that will constitute the subscription.

SKU Type	SKU	Description
Subscription	ISE-SEC-SUB	Cisco Identity Service Engine Subscription

Product SKUs: ISE Essentials, ISE Advantage, ISE Premier

There is one SKU each for ISE Essentials, ISE Advantage, and ISE Premier. Pricing follows a tiered pricing model and is calculated dynamically based on the seat count and term of the subscription.

SKU Type	SKU	Description
Billing	ISE-E-LIC	Cisco Identity Service Engine Essentials Subscription
	ISE-A-LIC	Cisco Identity Service Engine Advantage Subscription
	ISE-P-LIC	Cisco Identity Service Engine Premier Subscription

Cisco ISE Support

SKU Type	SKU	Description
Support	SVS-ISE-SUP-B	Cisco ISE Basic Support
	SVS-ISE-SUP-E	Cisco ISE Enhanced Support
	SVS-ISE-SUP-P	Cisco ISE Premium Support

Step 1.

Selecting the Subscription SKU. There is one Cisco ISE subscription SKU (ISE-SEC-SUB). There is no price for the subscription SKU. Pricing is determined when product SKUs are added and configured. A quantity of 1 should be selected because each end customer may have one, and only one, subscription. Product quantities will be entered when the product SKUs are added to the subscription.

After selecting the subscription SKU, choose "Select Options" to edit the subscription term and the requested start date.

Figure 15.
Subscription SKU selection on CCW

The subscription term will default to a 36-month term.

Figure 16.
Changing Subscription term on CCW

The requested start date may also be changed at this time.

The service is provisioned and the subscription starts on the service start date. The provisioning of the service may take up to 72 hours, assuming the order information is complete and correct.

Step 2. Selecting the Product SKU

When the subscription terms have been set, the next step is to add products to the subscription. The term for the product is defined by the subscription term. Start by selecting the appropriate product in the subscription configuration summary. The guidance below uses ISE-P-LIC as an example. Having chosen to configure the subscription for the product, you then enter the quantity based on the number of sessions.

Figure 17.
Selecting Billing SKUs on CCW

Pricing is determined dynamically according to the quantity ordered and term, and is based on a tiered pricing model. Per-month prices are displayed for the selected SKU. However, billing is prepaid for the term of the subscription, and the term amount is shown in the subtotal. The figure below shows an sample of dynamic pricing based on 100 sessions of ISE-E-LIC and 1500 sessions of ISE-P-LIC selected for a term of 3 years.

Figure 18.
Selecting Billing SKU quantity on CCW to view dynamic pricing

Step 3. Selecting the Support SKU

After the products have been added, the next step is to define the support level desired for the subscription. There are three Cisco ISE support SKUs, corresponding to the three levels of support. To configure support for the subscription, start by selecting "Cisco ISE Support Options" in the subscription configuration summary:

Basic Support is the standard support model and is selected by default. Enhanced or Premium Support may be purchased by selecting the appropriate level of support from the support options. Enhanced and Premium Support prices are calculated dynamically based on a percentage of the product cost and must meet annual minimum requirements.

Figure 19.
Service SKU selection on CCW

Quoting and Ordering Help

For Quoting or Ordering questions, please contact cs-support@cisco.com or open a case at <TBD>.

5.1.5 Cisco ISE Device Admin SKU

One ISE Device Administration license is required per Policy Service Node that operates on Device Administration transactions.

Table 6.   Cisco ISE Device Administration license

Part Number (SKU)	Description
L-ISE-TACACS-ND=	Cisco ISE Device Admin Node License

5.1.6 Cisco ISE IPSec SKU

One Cisco ISE IPsec license is required for every Policy Services Node used for IPsec VPN communication to the NADs. There is a maximum of 150 IPsec tunnels per Policy Services Node.

Table 7.   Cisco ISE IPsec licenses

Part Number (SKU)	Description
L-ISE-IPSEC	Cisco Identity Services Engine IPsec License

5.2 Cisco ISE Appliance SKUs

When selecting either the SNS-3515 or SNS-3595 Secure Network Server for a Cisco ISE deployment be sure to select the appropriate software option:

- SW-3515-ISE-K9 for the Cisco Secure Network Server 3515
- SW-3595-ISE-K9 for the Cisco Secure Network Server 3595

Table 8.   Cisco ISE Hardware Appliance licenses

Server Part Number	Product Description	Comments
SNS-3515-K9	Small Secure Network Server for ISE Applications	Customer must choose either upgrade or new purchase
SNS-3595-K9	Large Secure Server for ISE Applications	Customer must choose either upgrade or new purchase
SNS-3615-K9	Small Secure Network Server for ISE Applications	Customer must choose software option
SNS-3655-K9	Medium Secure Network Server for ISE Applications	Customer must choose software option
SNS-3695-K9	Large Secure Network Server for ISE Applications	Customer must choose software option

Table 9.   Spare components for the Cisco Secure Network Server

Secure Network Server	Component Part Number	Component Description
3515/3595	UCS-HD600G10K12G	600-GB 12-Gb SAS 10K RPM SFF hard disk; hot pluggable; drive sled mounted
3615/3655/3695	UCS-HD600G10K12N	600-GB 12-Gb SAS 10K RPM SFF hard disk; hot pluggable; drive sled mounted
3515/3595/3615/3655/3695	UCSC-PSU1-770W=	770W power supply
3515/3595/3615/3655/3695	N20-BKVM=	KVM cable
3515/3595/3615/3655/3695	UCSC-RAILB-M4=	Rail kit

Table 10. Cisco ISE Virtual Machine licenses

Service Part No	Product Description	VM Appliance Specifications
R-ISE-VMS-K9=	Cisco ISE Virtual Machine Small	Min 16GB RAM and 12 CPU cores for SNS-3515 equivalent
		Min 32GB RAM and 16 CPU cores for SNS-3615 equivalent
R-ISE-VMM-K9=	Cisco ISE Virtual Machine Medium	Min 64GB RAM and 16 CPU cores for SNS-3595 equivalent
		Min 96GB RAM and 24 CPU cores for SNS-3655 equivalent
R-ISE-VML-K9=	Cisco ISE Virtual Machine Large	Min 256GB RAM and 16 CPU cores for MnT in clusters supporting more than 500,000 concurrent sessions
		Min 256GB RAM and 24 CPU cores for SNS-3695 equivalent

6. Subscription renewals, cancellations, and changes

Cisco ISE subscriptions automatically renew for an additional 12-month term by default unless auto-renewal was deselected at the time of initial order. No quoting or ordering is required. Starting 120 days before the end of the initial term, renewal notices will be sent to the customer or partner. The customer or partner will receive an invoice at the start of the new term.

You can cancel a renewal up to 60 days prior to the start date of the new term. If the subscription is not cancelled 60 days prior to the start of the new term, the subscription will auto-renew. Mid-term cancellations of subscriptions for credit are not allowed.

Manual renewal

Any subscription can be manually renewed if the customer or partner desires, with standard terms of 12, 36, or 60 months. For manual renewals, quotes are created using the same process as the Change-Subscription process outlined below. This process will create a new quote. After a quote is approved, it can be converted to an order following the standard process.

Subscription cancellations

Renewals may be cancelled up to 60 days before the start date of the new term. If the subscription is not cancelled 60 days prior to the start of the new term, the subscription will automatically renew. Mid-term cancellations of subscriptions for credit are not allowed.

Subscription changes (Change-Subscription)

Changes to the products, quantities, or terms of a subscription may be made at any time during the term of the subscription. To change the subscription, please refer to this Cisco Commerce Change-Subscription Job Aide. Attempting to add products or seats by creating a new subscription will result in an ordering error.

7. License management

Starting with the ISE 3.0 release, ISE Licenses are Smart Licenses only. If you're on any prior release, the licenses can be used as either traditional Product Authorization Key based or as Smart Licenses. In the former case, the license file is imported into the deployment. For more details on how to convert ISE licenses purchased into Smart licenses, please take a look at the Cisco Smart Software Licensing details.

Cisco offers a variety of license management tools at the License Registration Portal. A valid Cisco.com user name and a password are required to access the portal. Key features of the Cisco License Registration portal include:

- Simplified asset management: identifies PAKs registered to a customer and the devices with installed licenses

- Automated software activation: quickly processes PAK registration and license file distribution

- License transfers: rehosts existing licenses to new Cisco ISE Administration nodes

- Replacement of devices: uses the "return materials authorization" to request replacement PAKs and licenses

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA

C07-656177-44   11/20