Cisco Identity Services Engine

June 2020

Contents

1. Understanding the Cisco Identity Services Engine Use Cases

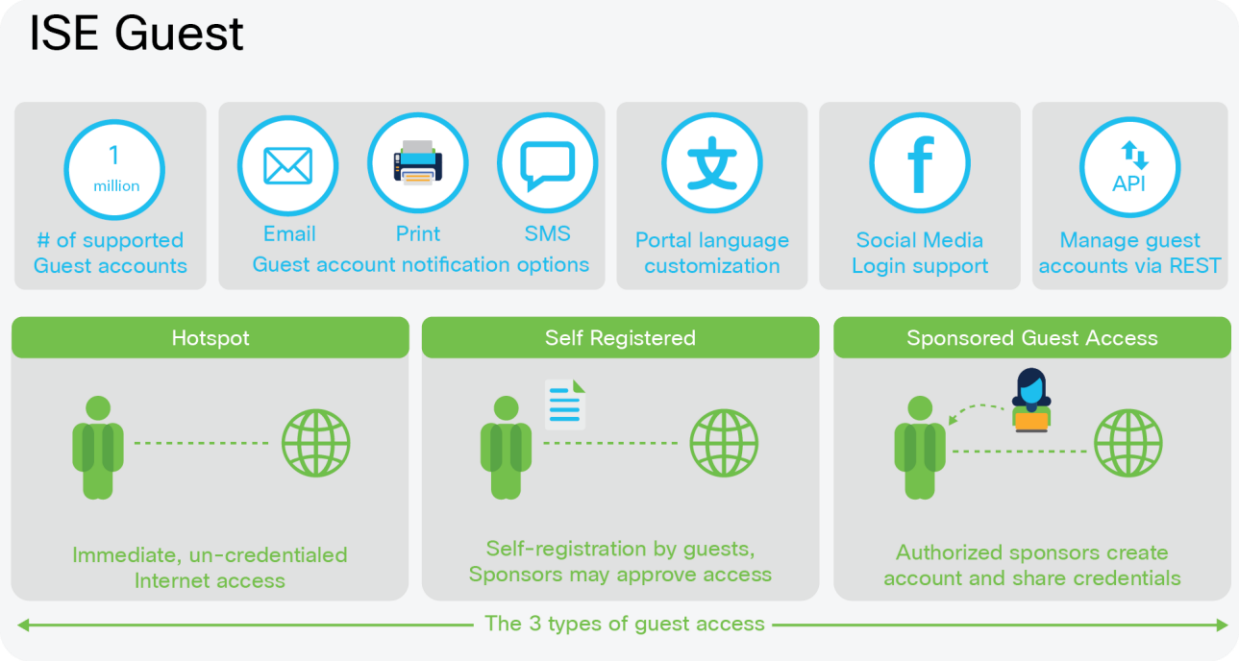
This section is to help you understand the various use cases that the Cisco Identity Services Engine (ISE) can empower you to solve. This is a great place to start if you are looking to understand the use cases, see what fits your needs and understand the quantity and types of licenses needed. You may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

1.1 Guest and Secure Wireless Access

1.1.1.1 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.

1.1.1.2 How does Guest work



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.

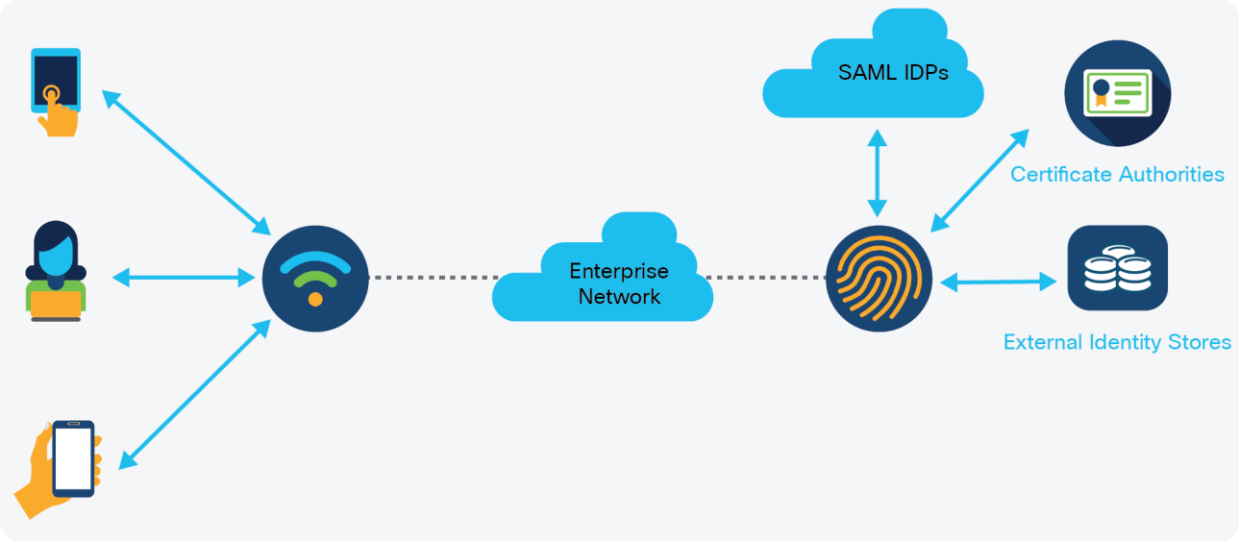
1.1.1.3 How do I license Guest

- License that enables Guest: Base
- License consumption: A Base license is needed for each active session (Session: a single connection between a user/device to a network device)
- Find the list of SKUs here

1.1.2.1 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.

1.1.2.2 How does Secure Wireless Access work



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, assign an SGT or SGACL.

1.1.2.3 How do I license Secure Wireless Access

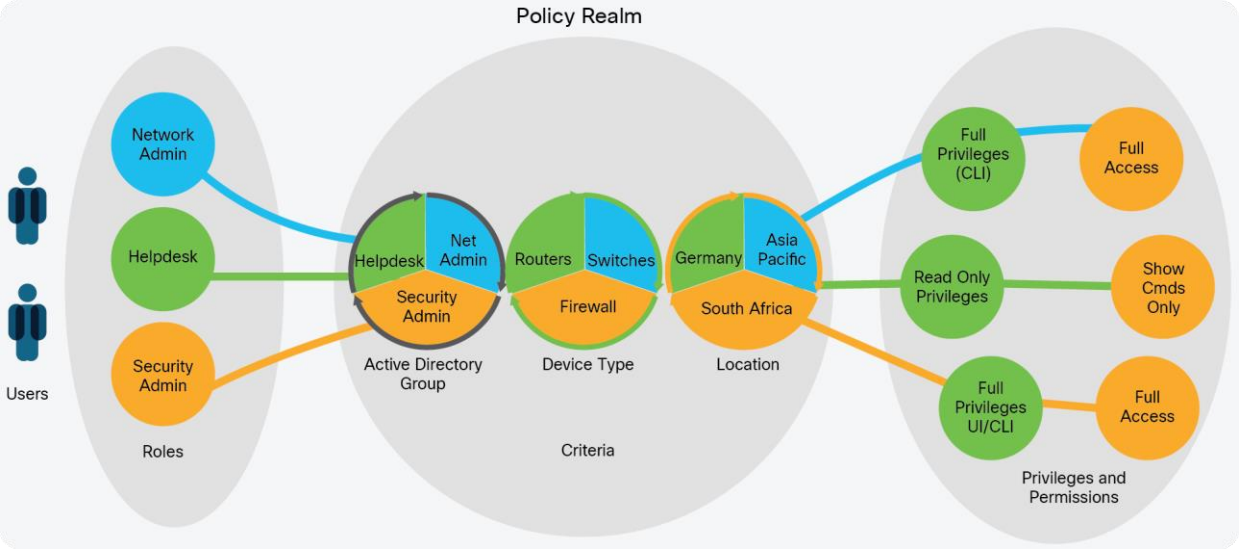
- License that enables Secure access: Base
- License consumption: A Base license is needed for each active session
- Find the list of SKUs here

1.2 Device Administration (TACACS+)

1.2.1 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 providing different permissions network operators.

1.2.2 How does Device Administration work



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.

1.2.3 How do I license Device Administration

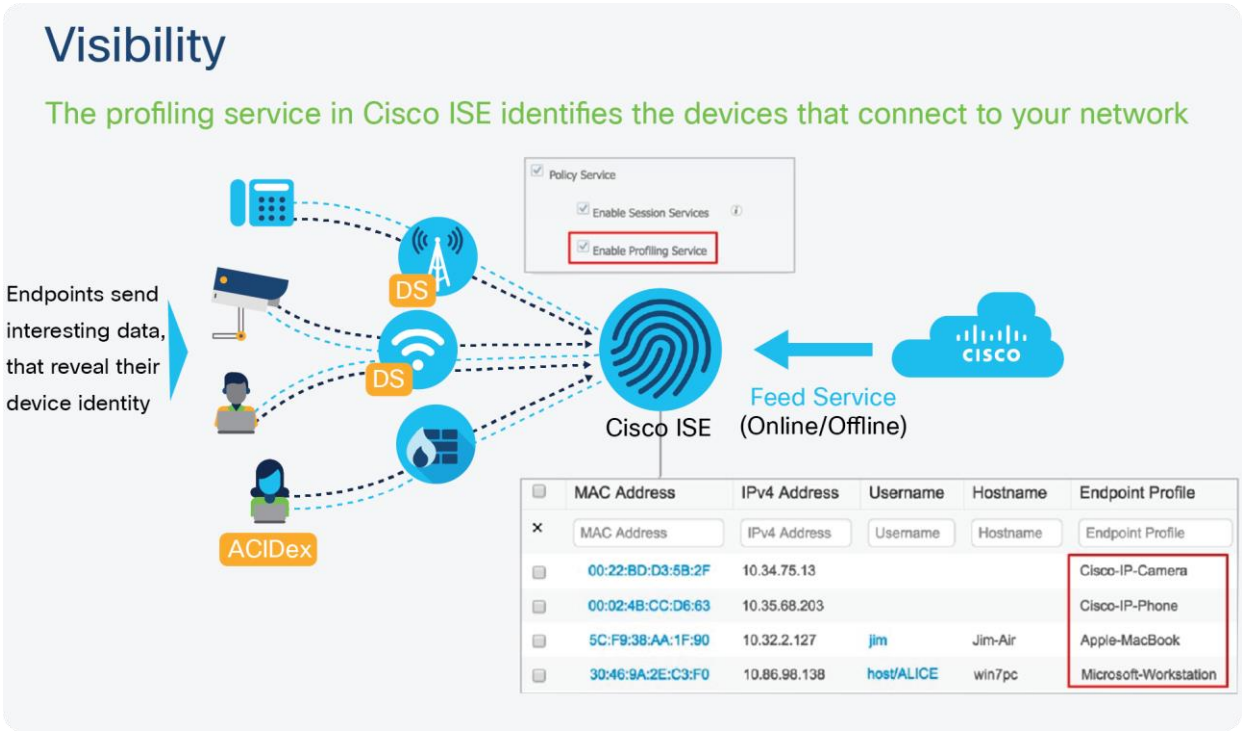
- License that enables Device Administration: Device Admin License
- License Consumption: Device Administration licenses are consumed per policy service node. Each policy service node that is setup to support Device Administration must have a Device Administration license. Device Administration using TACACS+ does not consume endpoint sessions but an ISE installation must have a minimum of 100 Base licenses. There is no limit on network devices for Device Administration.
- Find the SKU here. Please review table to understand prerequisite licenses

1.3 Asset visibility (Profiling)

1.3.1 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 laptop that belongs to the enterprise may be given full network access where a smartphone associated with the same user may only be given internet access or no access at all. Profiling helps the IT administrator determine the types of devices on their network.

1.3.2 How does asset visibility work



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

1.3.3 How do I license asset visibility

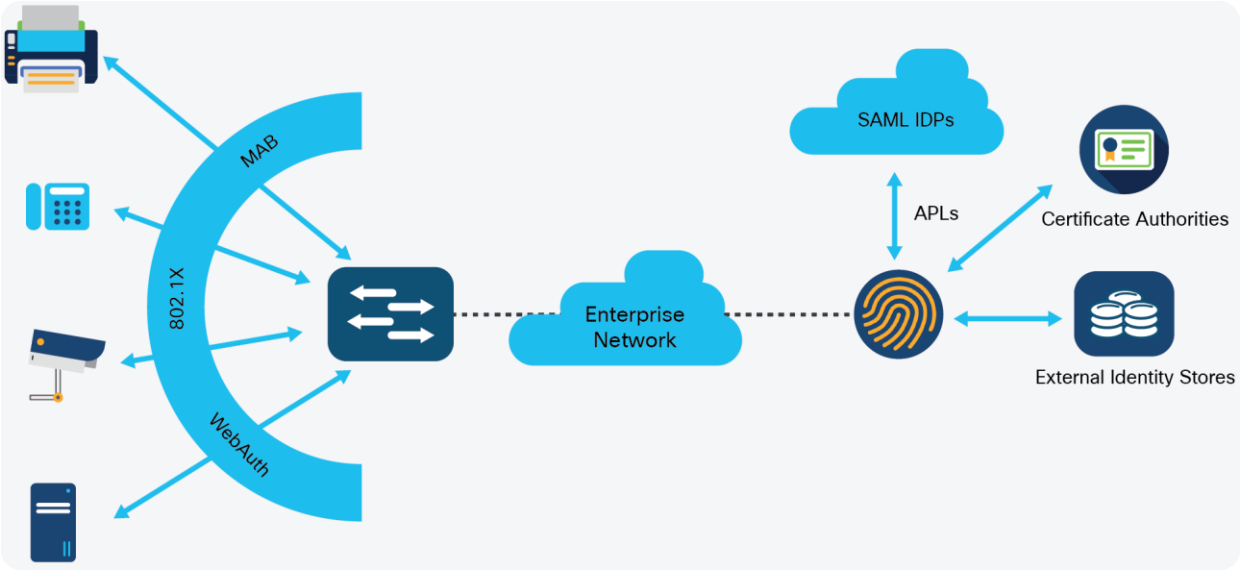
- Licenses that enable asset visibility: Plus
- License consumption: One Plus license is consumed per active endpoint session if there is an authorization policy built on the profile identified
- Find the list of SKUs for Plus here. Please review table to understand prerequisite licenses

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, Security Group Tag (SGT) or other segmentation methods.

1.4.2 How does Secure Wired Access work



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.

1.4.3 How do I license Secure Wired Access

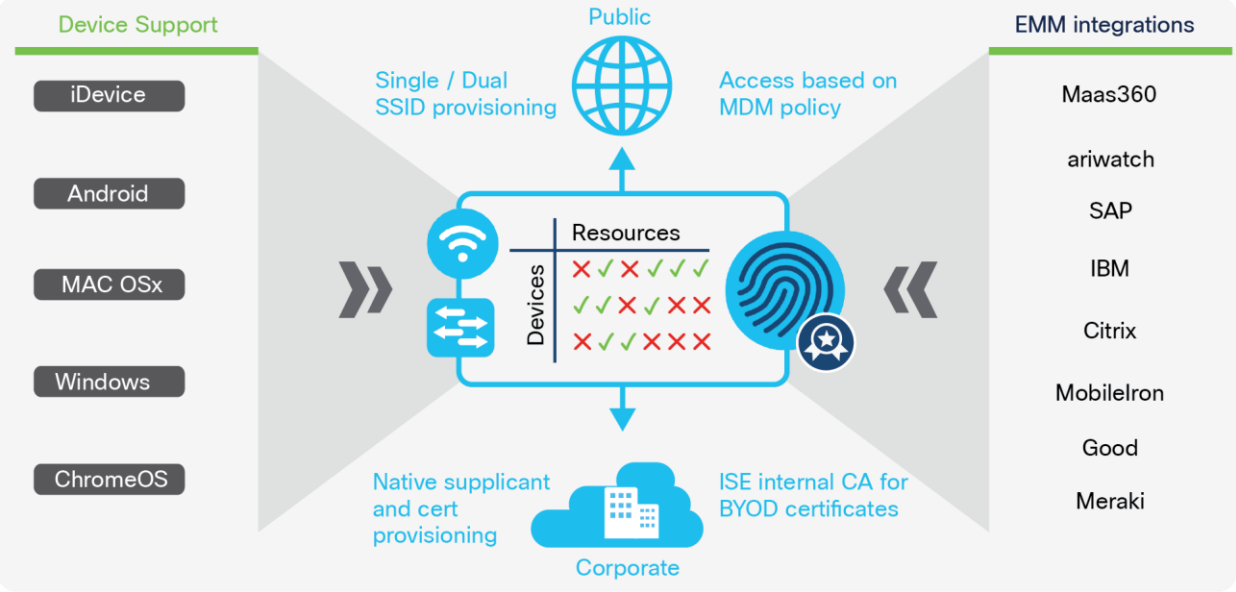
- License that enables Secure access: Base
- License Session consumption: A Base license is consumed for each active session
- Find the list of SKUs here

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 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.

1.5.3 How do I license BYOD

- License that enables BYOD: Plus
- License consumption: Each BYOD device connected to the network will consume a Plus license
- Find the SKUs for Plus licenses here

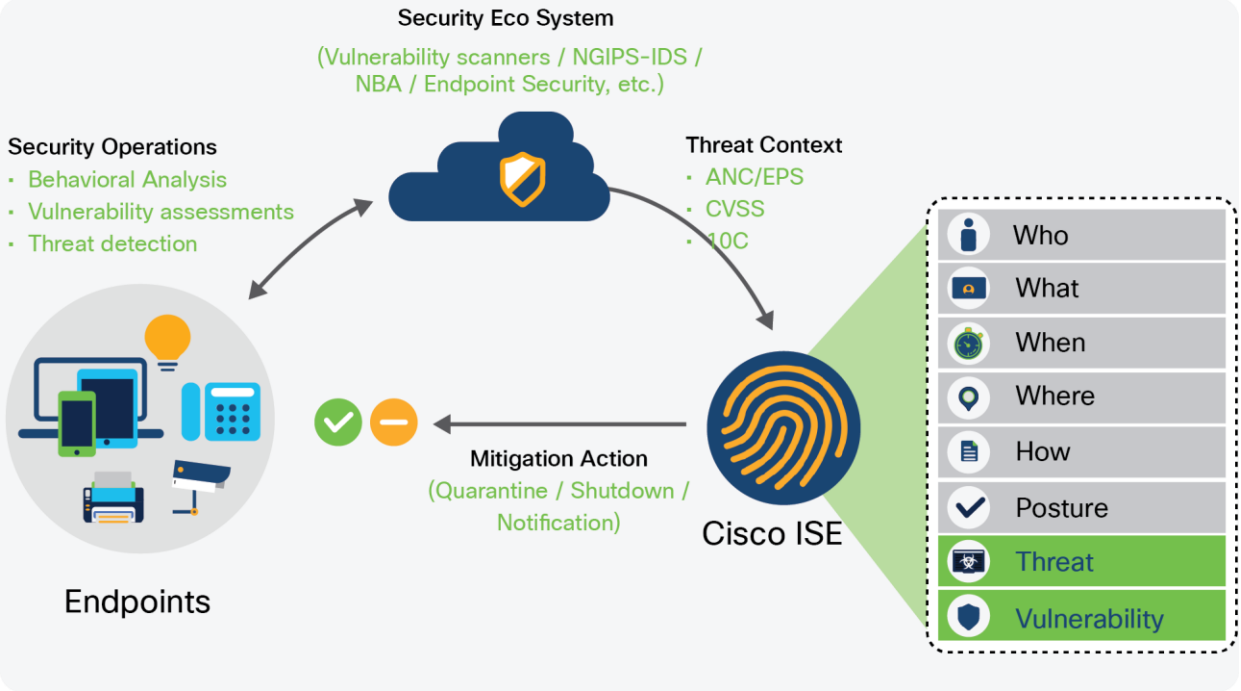
1.6 Rapid Threat Containment (RTC)

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



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.

1.6.3 How do I license Threat Containment

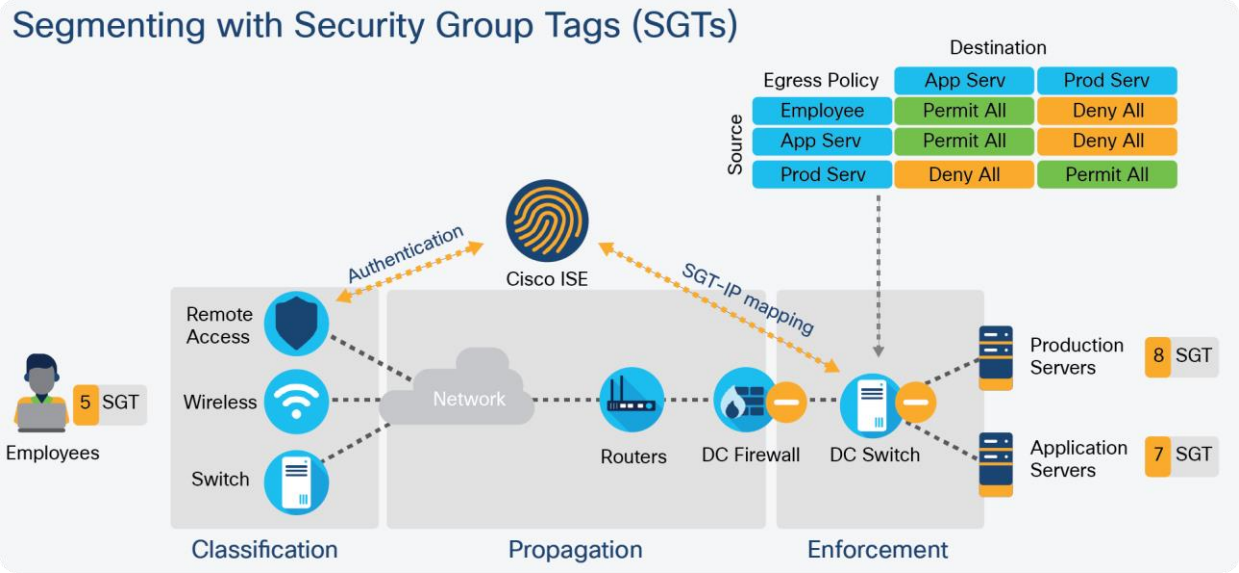
- License that enables Threat Containment: Base, Plus and Apex
- Threat Centric NAC (TC NAC) service enablement on ISE needs at least one Apex license. Further, an Apex license is consumed when an endpoint uses or triggers threat-based information or action as part of the authorization policy. Use of pxGrid for Adaptive Network Control (ANC) actions will consume a Plus license each per endpoint
- Find the SKUs for Base licenses here, Plus licenses here and for Apex licenses here
- Cisco ISE integrates with more than 50 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

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.

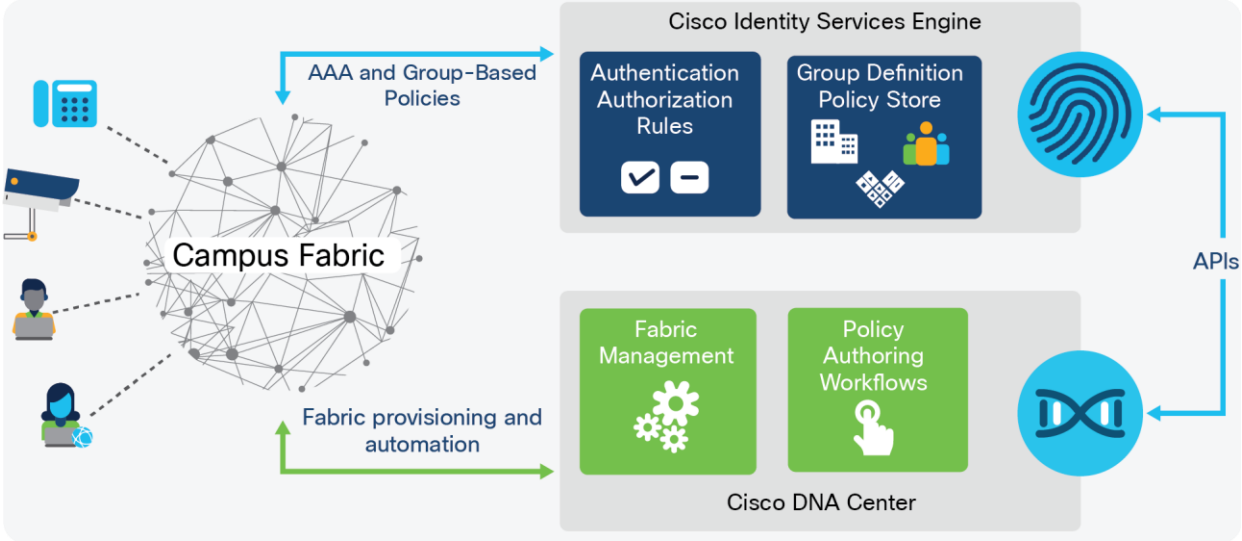
1.7.2 How does Segmentation works



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.



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.

1.7.3 How do I license Segmentation (TrustSec)

- License that enables Segmentation: Base
- License Session consumption: Segmentation itself does not consume sessions
- Find the list of SKUs here
- Licenses that enable Segmentation via SDA: Cisco DNA Premier / Cisco DNA Advantage. Please find more information in the SDA Ordering Guide

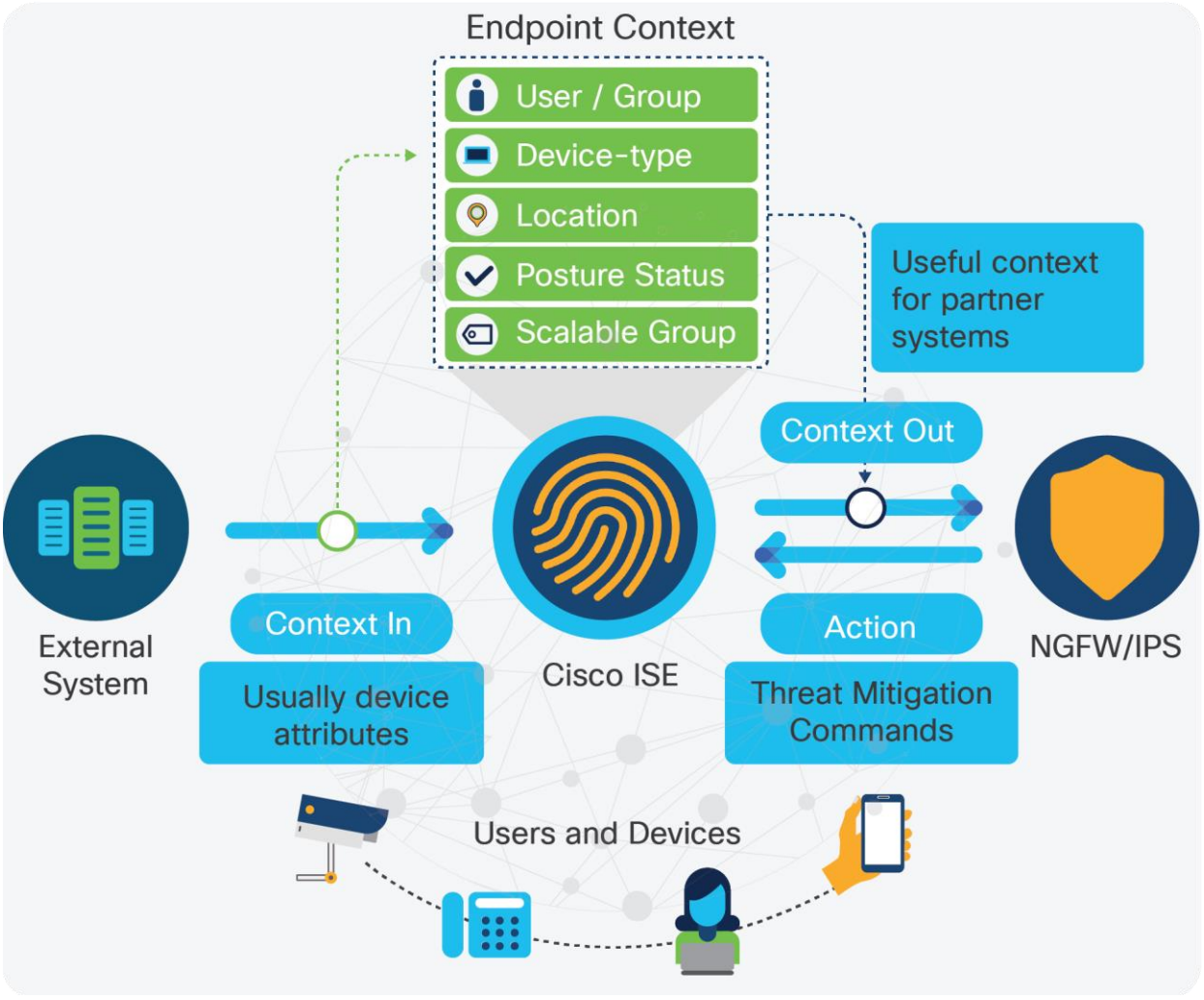
1.8 Security Ecosystem Integrations

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?



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

Cisco ISE integrates with more than 50 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

1.8.3 How do I license Security Ecosystem Integrations

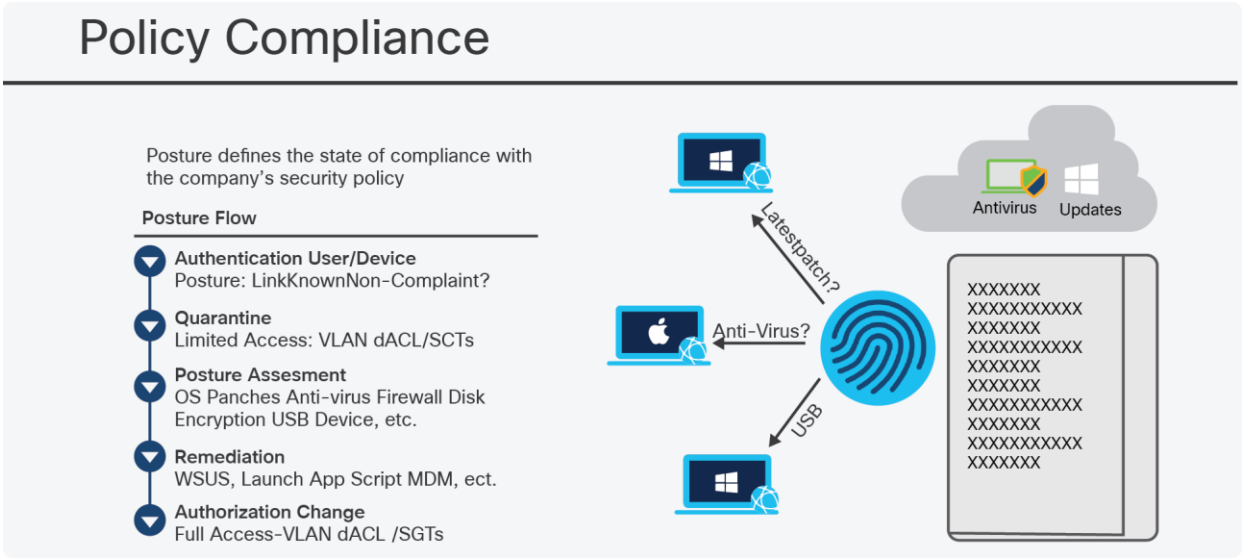
- License that enables Context Services: Base and Plus
- License Session consumption: Each active endpoint's context shared with an external system will consume a Plus license pxGrid and ERS service enablement needs a Plus license. Each active endpoint session information shared with an external system will need 1:1 Base to Plus licenses. For example, when a Windows laptop authenticates via 802.1X one Base license is consumed, if this endpoint's context is shared with Cisco Stealthwatch or NGFW, one additional Plus license will be consumed
- Find the SKUs for Base licenses here and Plus licenses here

1.9 Compliance (Posture)

1.9.1 Why Compliance

Saboteurs focus on intentional data corruption (ransomware) and data exfiltration compromising endpoints as a means to that end. The most effective and well-publicized compromises take advantage of known issues that could be simply remediated but were overlooked. Posture checks the endpoint making sure the overlooked or simply ignored are fixed before authorizing the device on the network. Posture also looks to make sure that software that is outside policy, such as peer-to-peer is not installed.

1.9.2 How does Compliance work



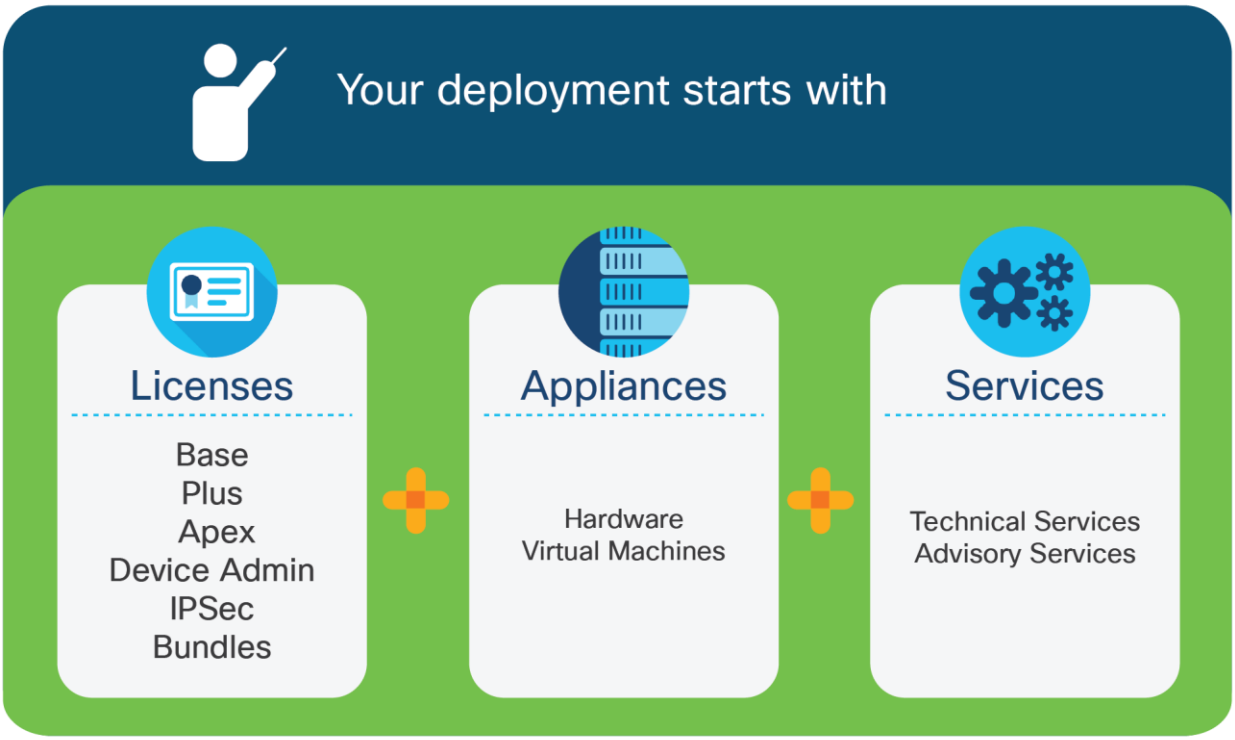
Posture leverages installed and temporal agents looking inside the endpoint to provide assurance that operating system patches, anti-malware, firewall, and more are installed, enabled, and up to date before authorizing the device onto the network.

1.9.3 How do I license Compliance

- License that enables Compliance: Apex
- License Session consumption: An Apex license is consumed for each active endpoint session postured
- Find the list of SKUs here. Please review table to understand prerequisite licenses
- AnyConnect Apex licenses together with ISE licenses mentioned above are required to fulfill this solution

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.



2.1 Licenses

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
Base	Provides highly secure endpoint and user access	Perpetual	Required before installing any further licenses
Plus	Provides context about sessions for more detailed access policies	Subscription (1, 3, or 5 years)	
Apex	Provides compliance details about sessions for more detailed access policies	Subscription (1, 3, or 5 years)	For posture/compliance use case, Cisco AnyConnect® Apex user licenses are required. The Cisco AnyConnect Apex licenses must be ordered as a separate line item with a count equal to the total number of possible users that will make use of Cisco AnyConnect services within the Cisco ISE deployment.

Cisco ISE License Package	Focus	Perpetual or Subscription (Terms Available)	Notes
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.
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			
	Base	DA	Plus	Apex
Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass and Easy Connect	Yes	No	No	No
Web authentication (local, central, device registration)	Yes	No	No	No
MACsec (all)	Yes	No	No	No
SSO, SAML, ODBC-based authentication	Yes	No	No	No
Guest portal and sponsor services	Yes	No	No	No
Representational state transfer (monitoring) APIs	Yes	No	No	No
External RESTful services (CRUD)-capable APIs	Yes	No	No	No
Security Group Tagging (Cisco TrustSec® SGT)	Yes	No	No	No
PassiveID (Cisco Subscribers)	[1]	No	Yes	No
PassiveID (Non-Cisco Subscribers)	[1]	No	Yes	No
Profiling	[1]	No	Yes	No
Profiler feed service	[1]	No	Yes	No
Device registration (My Devices portal) and provisioning for Bring Your Own Device (BYOD) with built-in Certificate Authority (CA)	[1]	No	Yes	No
Context sharing	[1]	No	Yes	No
Endpoint Protection Services (EPS)	[1]	No	Yes	No
Cisco TrustSec and ACI integration	[1]	No	Yes	No
Location-based integration Cisco Mobility Services Engine (MSE)	[1]	No	Yes	No

Cisco ISE Feature or Service	License			
Rapid Threat Containment (RTC) (using Adaptive Network Control and context sharing)	[1]	No	Yes	No
Posture (endpoint compliance and remediation)	[1]	No	No	Yes
Enterprise Mobility Management and Mobile Device Management (EMM and MDM) integration	[1]	No	No	Yes
Threat Centric NAC	[1]	No	No	Yes
Cisco AnyConnect Unified Agent (requires Cisco AnyConnect Apex license; see "Ordering information" section)	[1]	No	No	Yes
Secure Wired Access	Yes	No	No	No
Secure Wireless Access	Yes	No	No	No
Device Administration (TACACS+)	[1]	Yes	No	No

[1] Base license is prerequisite for Plus/Apex/DA licenses. Please refer table for more details

2.1.2 Base license and corresponding features

Features including but not limited to Authentication, Authorization, Accounting, Guest, PassiveID, and Security Group Tags.

While ISE Base license is pre-requisite to leveraging features from the rest of the ISE licenses, it is important to note the features Base has to offer.

Cisco ISE Feature or Service	Description	License consumed
Basic RADIUS authentication, authorization, and accounting, including 802.1x, MAC Authentication Bypass and Easy Connect	A Base license is consumed when an endpoint establishes an active network session	Yes
Web authentication (local, central, device registration)		Yes
MACsec (all)		Yes
SAML, ODBC-based authentication		Yes
Guest portal and sponsor services		Yes
Representational state transfer (monitoring) APIs		Yes
External RESTful services (CRUD)-capable APIs		Yes
Scalable group tagging (Cisco TrustSec® SGT)	Use of SGTs as part of authorization policy	No

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
Wired access control		Yes

Take me to the Cisco ISE Base SKUs

2.1.3 Plus license and corresponding features

Features including but not limited to Profiling, Context Sharing, and Rapid Threat Containment.

Cisco ISE Feature or Service	Description	License consumed
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
Profiling	A Plus license is consumed when an endpoint with an active session uses profiling classification in an authorization policy	Yes
Profiler feed service	Dynamic downloading of endpoint classification rules	No
BYOD client provisioning and enablement	A Plus license is consumed when an endpoint with an active session uses its registration status in an authorization policy	Yes
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 ISE Feature or Service	Description	License consumed
Cisco TrustSec and ACI integration		No
Location-based integration using Cisco Mobility Services Engine (MSE)		Yes
Rapid Threat Containment (RTC) (using Adaptive Network Control and pxGrid)		Yes

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

Table 2. Context exchange licensing requirements

Authentication Mechanism	Context Shared With	License Requirement
Cisco ISE	Cisco platforms	Plus 1:1 Base
Cisco ISE	Third-party platforms	Plus 1:1 Base
Non-ISE Authentication (e.g., AD)	Cisco platforms	Base
Non-ISE Authentication (e.g., AD)	Third-party platforms	Plus 1:1 Base

Take me to the Cisco ISE Plus SKUs

2.1.4 Apex license and corresponding features

Features including but not limited to Posture, and Integration with Enterprise Mobility Device Management.

Cisco ISE Feature or Service	Description	Apex
Posture (endpoint compliance and remediation)	An Apex license is consumed when an endpoint with an active session receives an authorization based on a posture status other than “Not applicable” (for example, Compliant, Not compliant, Pending, or Unknown)	Yes
Enterprise Mobility Management and Mobile Device Management (EMM and MDM) integration		Yes
Threat Centric NAC		Yes
Cisco AnyConnect Unified Agent (requires Cisco AnyConnect Apex license; see “Ordering information” section)		Yes

Take me to the Cisco ISE Apex SKUs

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 data center.

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 data sheet. Cisco ISE requires the virtual target to have at least 16 GB of memory and at least 200 GB of hard drive space available.

2.3 Services

2.3.1 Technical Services

Cisco Software Support Service (SWSS) is included for the duration of all Cisco ISE subscription licenses.

Higher-value service levels, Software Support Enhanced and Premium, are available for Cisco ISE Base, Plus and Apex 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. The Enhanced and Premium Software Support is based on the number of concurrent sessions, and can be ordered via the top-level ATO PID in CCW: CISE-SW-SUPP.

Please note that Smart Net Total Care® or SWSS contracts for Cisco ISE physical and virtual appliances must be purchased separately and are required to consume any ISE subscription licenses. Smart Net Total Care and SWSS contracts for Cisco ISE physical and virtual appliances cover Base and Device Admin deployments as well. Please also note that Cisco does not offer standalone ISE software upgrade service SKUs or separate support SKUs for subscription licenses.

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

In April 2018, a new format of ISE SKUs was introduced to make purchase and consumption easier.

1. ISE Base, Plus, and Apex licenses are band priced. This means customers have the flexibility to choose the quantity of purchase now since each PID has a range of quantities.
2. Device Admin licenses are based on number of ISE nodes used for TACACS+.
3. Virtual Machine (VM) licenses are categorized as small scale-, medium scale-, or large scale-based licenses.

Note: ISE Base continues to be a perpetual offering, and ISE Plus and Apex continue to be subscription licenses.

3.2 End-of-life notices

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

3.3 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 Base, Plus, and Apex 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.

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 2.4 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.

3.4.4 Base, Plus, and Apex

There is no change in license behavior. No action is required.

Whether using legacy or today's licenses, the behavior of these licenses does not change upon upgrade to ISE Release 2.4.

4. Migration from other older licenses to today

If you purchased one of the following licenses in the past and would like to understand how to migrate to today's licenses, please click on the relevant links below. End of life announcement for all these licenses can be found here.

4.1 ISE Mobility and Wireless Licenses

Cisco ISE Wireless and Mobility licenses are term-based licenses that support wireless and remote access.

Cisco ISE Wireless and Mobility licenses appear in the ISE user interface adding Base, Plus, and Apex capacity with expirations on all three that match the term of the ISE Wireless or Mobility license.

Existing customers with Wireless licenses that migrate to 2.0 or later releases will see a Wireless to Mobility name change in the administrative console, but they will have the same functionality, plus the ability to provide VPN access control.

A Mobility license is consumed when a wireless or VPN endpoint establishes an active network session

4.1.2 ISE Wireless and Mobility Upgrade Licenses

Cisco ISE Mobility Upgrade licenses are term-based licenses that add wired capability to existing ISE Wireless and Mobility licenses. Cisco ISE Mobility Upgrade licenses do not add to the number of licensed endpoints or change the term of the Cisco ISE Wireless or Mobility license.

The number of Cisco ISE Mobility Upgrade licenses purchased should be no more than the number of Wireless or Mobility licenses. Cisco ISE Mobility Upgrade licenses should be co-termed to the ISE Wireless or Mobility licenses.

Adding endpoints to existing ISE Wireless or Mobility clusters requires a purchase of Base, Plus, and Apex licenses because the ISE Wireless and ISE Mobility licenses are no longer for sale. Purchasing Mobility Upgrade licenses in equal quantity and co-terminating is a prerequisite to this approach.

Alternatively, the ISE Wireless or Mobility licenses can be replaced by current Base, Plus and Apex licenses based on use cases addressed. This is a preferable approach considering the announcement of end of life of Mobility Upgrade licenses. In rare cases, customers may choose to wait until expiry of the ISE Wireless or Mobility licenses before expanding.

When the number of ISE Mobility Upgrade licenses installed is less than the number of ISE Wireless or Mobility licenses, traditional Base, Plus and Apex licenses cannot be added. Earlier versions of Cisco ISE allowed a difference between the Mobility and Mobility Upgrade count due to issues with RADIUS intermediaries (for example, load balancers), but Cisco ISE 2.0 addresses these issues.

4.2 ISE Express License

Cisco ISE Express is a bundle of 1 virtual ISE appliance and 150 Base licenses.

Additional ISE endpoint licenses (Base, Plus and Apex) can be added to the existing 150 Base licenses via the normal a la carte process described in this ordering guide. The maximum number of Base, Plus or Apex licenses in an ISE Express deployment is 5000, meaning that ISE Express supports up to 5000 Base licenses, up to 5000 Base and Plus licenses, up to 5000 Base and Apex licenses or up to 5000 Base, Plus and Apex licenses. Please note that AnyConnect Apex licenses can be used in an ISE Express deployment as long as it has Apex licenses.

Also note ISE Device Administration license is not supported with ISE Express.

The virtual appliance included in ISE Express is for a single-site deployment only, and cannot participate in a larger ISE deployment nor can it be paired with another ISE appliance for high availability.

Customers who would like to expand beyond the constraints of ISE Express (say, add additional ISE nodes, or go beyond 5000 sessions), have the opportunity to purchase the ISE Express Upgrade, to convert their ISE Express node to a 'normal' ISE base license. Please consider the timelines for such a purchase since the end of life of this upgrade license has also been announced.

4.3 ISE Advanced License

Cisco ISE Advanced license offered the entire feature set of what lies in Plus and Apex today.

At the time of renewal, customers have the opportunity to right-size their license consumption to either Plus or Apex based on their use cases.

Existing Advanced customers that migrate to Cisco ISE 2.0 or a later release will see the Advanced name decomposed into Plus and Apex in the administrative console, but they too will have same functionality.

4.4 ISE Advanced Migration Licenses

This license offered a combination of Base as perpetual, Plus and Apex as subscription licenses of duration 3 yrs. This license was originally intended to provision a transition path for customer of the legacy Cisco Clean Access product to Cisco ISE.

While the license is meant to provision a perpetual Base license, there has been a technical limitation identified with this particular license where it provides only 3 years of Base functionality. Customers experiencing this limitation may open a case via Cisco Support Case Manager (SCM) at http://cs.co/scmswl (choose 'licensing' option in SCM) with the Cisco sales order number reflecting the ISE Advanced Migration purchase in order to procure functional Base perpetual licenses.

After expiry of the Plus and Apex licenses, customer may choose to purchase new Plus and Apex licenses based on the ISE use cases they wish to continue to utilize or explore.

4.5 ISE Base Migration Licenses

This license has attained End-of-Life (EOL). It offered perpetual Base licenses at a discounted price as a limited period offer to provision a transition path for customers of the legacy Cisco Secure Access Control System product to Cisco ISE.

In case of expanding such a deployment, customer would follow the same steps as expanding an existing ISE deployment with a regular Base license.

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 Base SKUs

Start by choosing L-ISE-BSE- PLIC=. From here choose one of the following SKUs that fits your quantity requirement. The Cisco ISE Base license options are listed in the table below.

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 10000 to 24999
L-ISE-BSE-P8	Cisco ISE Base License - Sessions 25000 to 49999
L-ISE-BSE-P9	Cisco ISE Base License - Sessions 50000 to 99999

Part Number (SKU)	Description
L-ISE-BSE-P10	Cisco ISE Base License - Sessions 100000 to 249999
L-ISE-BSE-P11	Cisco ISE Base License - Sessions 250000 and above

5.1.3 Cisco ISE Plus SKUs

Start by choosing L-ISE-PLS-LIC= and click on Select Service. From here enter the sessions count to pick the subscription SKU that fits your quantity and duration requirement.

Table 4. Cisco ISE Plus 5-year subscription licenses

Term Subscription	Description
L-ISE-PLS-5Y-S1	Cisco ISE Plus License, 5Y, 100 - 249 Sessions
L-ISE-PLS-5Y-S2	Cisco ISE Plus License, 5Y, 250 - 499 Sessions
L-ISE-PLS-5Y-S3	Cisco ISE Plus License, 5Y, 500 - 999 Sessions
L-ISE-PLS-5Y-S4	Cisco ISE Plus License, 5Y, 1000 - 2499 Sessions
L-ISE-PLS-5Y-S5	Cisco ISE Plus License, 5Y, 2500 - 4999 Sessions
L-ISE-PLS-5Y-S6	Cisco ISE Plus License, 5Y, 5000 - 9999 Sessions
L-ISE-PLS-5Y-S7	Cisco ISE Plus License, 5Y, 10000 - 24999 Sessions
L-ISE-PLS-5Y-S8	Cisco ISE Plus License, 5Y, 25000 - 49999 Sessions
L-ISE-PLS-5Y-S9	Cisco ISE Plus License, 5Y, 50000 - 99999 Sessions
L-ISE-PLS-5Y-S10	Cisco ISE Plus License, 5Y, 100000 - 249999 Sessions
L-ISE-PLS-5Y-S11	Cisco ISE Plus License, 5Y, 250000+ Sessions

Table 5. Cisco ISE Plus 3-year subscription licenses

Term Subscription	Description
L-ISE-PLS-3Y-S1	Cisco ISE Plus License, 3Y, 100 - 249 Sessions
L-ISE-PLS-3Y-S2	Cisco ISE Plus License, 3Y, 250 - 499 Sessions
L-ISE-PLS-3Y-S3	Cisco ISE Plus License, 3Y, 500 - 999 Sessions
L-ISE-PLS-3Y-S4	Cisco ISE Plus License, 3Y, 1000 - 2499 Sessions
L-ISE-PLS-3Y-S5	Cisco ISE Plus License, 3Y, 2500 - 4999 Sessions
L-ISE-PLS-3Y-S6	Cisco ISE Plus License, 3Y, 5000 - 9999 Sessions
L-ISE-PLS-3Y-S7	Cisco ISE Plus License, 3Y, 10000 - 24999 Sessions

Term Subscription	Description
L-ISE-PLS-3Y-S8	Cisco ISE Plus License, 3Y, 25000 - 49999 Sessions
L-ISE-PLS-3Y-S9	Cisco ISE Plus License, 3Y, 50000 - 99999 Sessions
L-ISE-PLS-3Y-S10	Cisco ISE Plus License, 3Y, 100000 - 249999 Sessions
L-ISE-PLS-3Y-S11	Cisco ISE Plus License, 3Y, 250000+ Sessions

Table 6. Cisco ISE Plus 1-Year subscription licenses

Term Subscription	Description
L-ISE-PLS-1Y-S1	Cisco ISE Plus License, 1Y, 100 - 249 Sessions
L-ISE-PLS-1Y-S2	Cisco ISE Plus License, 1Y, 250 - 499 Sessions
L-ISE-PLS-1Y-S3	Cisco ISE Plus License, 1Y, 500 - 999 Sessions
L-ISE-PLS-1Y-S4	Cisco ISE Plus License, 1Y, 1000 - 2499 Sessions
L-ISE-PLS-1Y-S5	Cisco ISE Plus License, 1Y, 2500 - 4999 Sessions
L-ISE-PLS-1Y-S6	Cisco ISE Plus License, 1Y, 5000 - 9999 Sessions
L-ISE-PLS-1Y-S7	Cisco ISE Plus License, 1Y, 10000 - 24999 Sessions
L-ISE-PLS-1Y-S8	Cisco ISE Plus License, 1Y, 25000 - 49999 Sessions
L-ISE-PLS-1Y-S9	Cisco ISE Plus License, 1Y, 50000 - 99999 Sessions
L-ISE-PLS-1Y-S10	Cisco ISE Plus License, 1Y, 100000 - 249999 Sessions
L-ISE-PLS-1Y-S11	Cisco ISE Plus License, 1Y, 250000+ Sessions

5.1.4 Cisco ISE Apex SKUs

Start by choosing L-ISE-APX-LIC= and click on Select Service. From here enter the sessions count to pick the subscription SKU that fits your quantity and duration requirement.

Table 7. Cisco ISE Apex 5-year subscription licenses

Term Subscription	Description
L-ISE-APX-5Y-S1	Cisco ISE Apex License, 5Y, 100 - 249 Sessions
L-ISE-APX-5Y-S2	Cisco ISE Apex License, 5Y, 250 - 499 Sessions
L-ISE-APX-5Y-S3	Cisco ISE Apex License, 5Y, 500 - 999 Sessions
L-ISE-APX-5Y-S4	Cisco ISE Apex License, 5Y, 1000 - 2499 Sessions
L-ISE-APX-5Y-S5	Cisco ISE Apex License, 5Y, 2500 - 4999 Sessions

Term Subscription	Description
L-ISE-APX-5Y-S6	Cisco ISE Apex License, 5Y, 5000 - 9999 Sessions
L-ISE-APX-5Y-S7	Cisco ISE Apex License, 5Y, 10000 - 24999 Sessions
L-ISE-APX-5Y-S8	Cisco ISE Apex License, 5Y, 25000 - 49999 Sessions
L-ISE-APX-5Y-S9	Cisco ISE Apex License, 5Y, 50000 - 99999 Sessions
L-ISE-APX-5Y-S10	Cisco ISE Apex License, 5Y, 100000 - 249999 Sessions
L-ISE-APX-5Y-S11	Cisco ISE Apex License, 5Y, 250000+ Sessions

Table 8. Cisco ISE Apex 3-year subscription licenses

Term Subscription	Description
L-ISE-APX-3Y-S1	Cisco ISE Apex License, 3Y, 100 - 249 Sessions
L-ISE-APX-3Y-S2	Cisco ISE Apex License, 3Y, 250 - 499 Sessions
L-ISE-APX-3Y-S3	Cisco ISE Apex License, 3Y, 500 - 999 Sessions
L-ISE-APX-3Y-S4	Cisco ISE Apex License, 3Y, 1000 - 2499 Sessions
L-ISE-APX-3Y-S5	Cisco ISE Apex License, 3Y, 2500 - 4999 Sessions
L-ISE-APX-3Y-S6	Cisco ISE Apex License, 3Y, 5000 - 9999 Sessions
L-ISE-APX-3Y-S7	Cisco ISE Apex License, 3Y, 10000 - 24999 Sessions
L-ISE-APX-3Y-S8	Cisco ISE Apex License, 3Y, 25000 - 49999 Sessions
L-ISE-APX-3Y-S9	Cisco ISE Apex License, 3Y, 50000 - 99999 Sessions
L-ISE-APX-3Y-S10	Cisco ISE Apex License, 3Y, 100000 - 249999 Sessions
L-ISE-APX-3Y-S11	Cisco ISE Apex License, 3Y, 250000+ Sessions

Table 9. Cisco ISE Apex 1-year subscription licenses

Term Subscription	Description
L-ISE-APX-1Y-S1	Cisco ISE Apex License, 1Y, 100 - 249 Sessions
L-ISE-APX-1Y-S2	Cisco ISE Apex License, 1Y, 250 - 499 Sessions
L-ISE-APX-1Y-S3	Cisco ISE Apex License, 1Y, 500 - 999 Sessions
L-ISE-APX-1Y-S4	Cisco ISE Apex License, 1Y, 1000 - 2499 Sessions
L-ISE-APX-1Y-S5	Cisco ISE Apex License, 1Y, 2500 - 4999 Sessions
L-ISE-APX-1Y-S6	Cisco ISE Apex License, 1Y, 5000 - 9999 Sessions

Term Subscription	Description
L-ISE-APX-1Y-S7	Cisco ISE Apex License, 1Y, 10000 - 24999 Sessions
L-ISE-APX-1Y-S8	Cisco ISE Apex License, 1Y, 25000 - 49999 Sessions
L-ISE-APX-1Y-S9	Cisco ISE Apex License, 1Y, 50000 - 99999 Sessions
L-ISE-APX-1Y-S10	Cisco ISE Apex License, 1Y, 100000 - 249999 Sessions
L-ISE-APX-1Y-S11	Cisco ISE Apex License, 1Y, 250000+ Sessions

5.1.5 Cisco ISE Device Admin SKU

Please note that at least 100 ISE Base session licenses are needed in the deployment prior to adding an ISE Device Administration license. One ISE Device Administration license is required per Policy Service Node that operates on Device Administration transactions.

Table 10. 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 11. 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 12. 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

Server Part Number	Product Description	Comments
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 13. 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 14. 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. License management

ISE 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 C07-656177-41 06/20