

Cisco ISE Licensing Guide

January 2024

Contents

1. Overview of Cisco Identity Services Engine use cases	4
2. What you need for your Cisco ISE deployment	5
2.1. Appliances	5
2.2. Cisco ISE licensing	5
2.3. Services	6
3. Cisco ISE licenses	7
3.1. Understanding Cisco ISE licenses	7
3.2. ISE Subscription Licenses	9
3.3. Cisco ISE Device Admin license	13
3.4. Cisco ISE Virtual Machine licenses	13
4. How to order Cisco ISE licenses	13
4.1. Ordering ISE Subscription licenses a-la-carte	13
4.2. Changing existing orders or subscriptions	18
4.3. Other ISE License SKUs based on your deployment	18
5. Specific ISE Licensing Methods based on deployment	19
5.1. Licensing with persistent Internet connection	19
5.2. Licensing in an air-gapped network with SSM on-prem	19
5.3. Specific License Reservation (SLR)	20
6. Subscription Renewals, Cancellations or Modifications	24
6.1. Subscription renewals	24
6.2. Subscription cancellations	24
6.3. Subscription Modifications	24
7. Cisco ISE license migration	25
7.1 Cisco ISE Subscription license migration	27
7.2 Migrate to VM Common licenses	31
7.3 Migration of Device Admin licenses	33
8. Cisco Identity Services Engine use cases	34
8.1. Guest and secure wireless access	34
8.2. Asset visibility	36
8.3. Compliance (posture)	37
8.4. Secure Wired Access	38
8.5. Bring your own device (BYOD)	39
8.6. Rapid Threat Containment (RTC)	40
8.7. Segmentation	41



8.8. Security ecosystem integrations	43
8.9. Device Administration (TACACS+)	44
9. How to raise TAC case for Licensing requests	45

This guide provides information on how Cisco® ISE licensing works and how to calculate the quantity and types of licenses you need for your network.

1. Overview of Cisco Identity Services Engine use cases

Cisco Identity Services Engine (ISE) empowers you to solve a wide range of use cases.

To understand the types and quantities of Cisco ISE licenses you may need, you must first understand the capabilities of Cisco ISE. Cisco ISE is a product that supports a wide range of use cases. See the [Cisco ISE webpage](#) to understand the features of Cisco ISE and how it can address multiple use cases of network visibility, segmentation, and security.

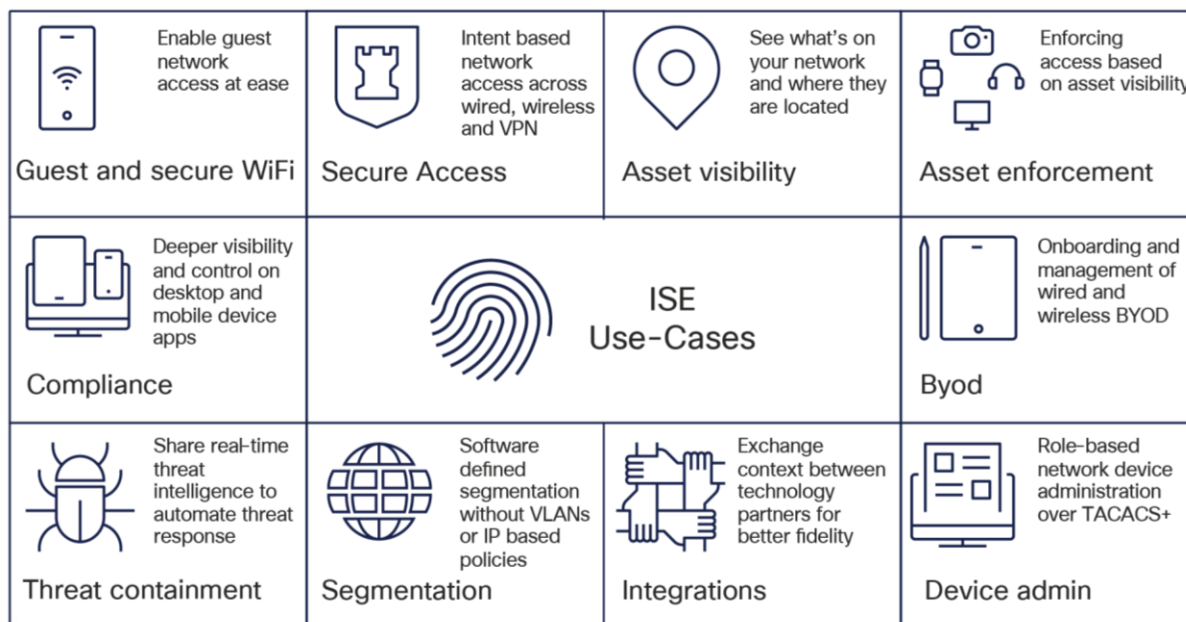


Figure 1.
Cisco ISE use cases

2. What you need for your Cisco ISE deployment

A Cisco ISE deployment consists of three primary components: Cisco ISE licenses, appliances, and services.

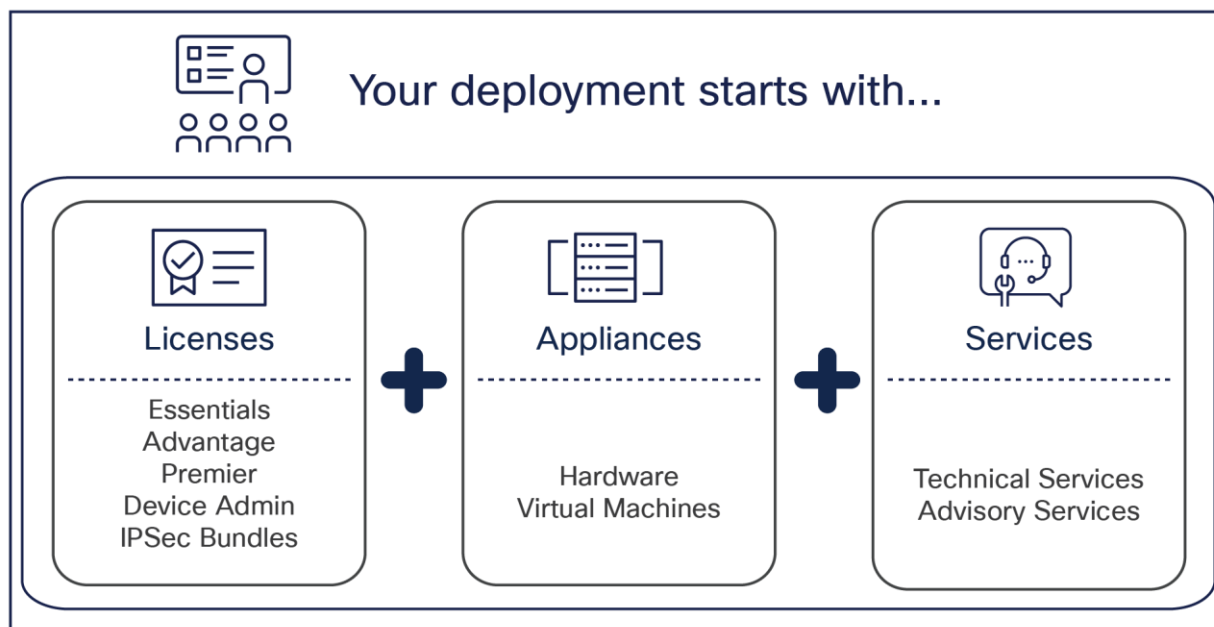


Figure 2.
Cisco ISE deployment

2.1. Appliances

Cisco ISE may be deployed on any combination of physical and virtual appliances, as well as infrastructure -as-a-service (IaaS) instances in AWS, Azure, and Oracle Cloud. For more details on Cisco ISE appliances, refer to the [Cisco Secure Network Server Data Sheet](#). For more details on virtual machine, refer to the section “Cisco ISE Virtual Machine licenses,” later in this guide. For detailed information about Cisco ISE on cloud platforms, please refer to [Deploy Cisco ISE Natively on Cloud Platforms](#).

For detailed information about performance and scalability, please refer to the [Performance and Scalability Guide](#).

2.2. Cisco ISE licensing

Cisco ISE licensing provides the ability to manage the application features and access, such as the number of concurrent active endpoints that can use Cisco ISE network resources at any time. Licensing in Cisco ISE is supplied as feature-based packages wherein different features are supported by each license type.

The types of Cisco ISE licensing are:

1. Tier-based Subscription licenses
2. Device Admin Licenses
3. Virtual Machine licenses
4. IPsec licenses
5. ISE-PIC Licenses

All licenses are managed in [Smart Licensing](#) format through Cisco Smart Software Manager (SSM). The Cisco Smart Software Manager is an intuitive portal where you can activate and manage all your Cisco licenses.

Smart Licensing is a new, flexible software licensing model that simplifies the way you can activate and manage licenses across your organization. Instead of using Product Activation Keys (PAKs), Smart Licenses establish a pool of software licenses in a customer-defined Smart Account that can be used across an enterprise. Smart Accounts are mandatory for any subscription. They help identify and connect the right customer accounts into which the license subscriptions purchased by a customer must be deposited. The combination of Smart Licensing and Smart Accounts delivers visibility into your license ownership and consumption (through a cloud portal) to help you reduce operational costs.

2.3. Services

2.3.1. Technical Services

Support for appliances and perpetual licenses

Customers can purchase Cisco Smart Net Total Care® for Cisco ISE physical appliances and Software Support (SWSS) contracts for Cisco ISE virtual machines or the ISE-PIC virtual machine, along with the option to upgrade support to Solution Support. The support for Cisco ISE physical or virtual appliances also covers Base license (for customers still on 2.x) and Device Admin deployments.

Support for subscription licenses

Cisco Software Support Basic (SWSS) is included for the duration of all Cisco ISE subscription licenses. Higher-value service levels, Solution Support and Software Support Enhanced and Premium, are available for all Cisco ISE subscription licenses.

Software Support Enhanced and Premium services provide everything included in Software Support Basic, but with a richer feature set, such as prioritized case handling, direct access to highly skilled engineers with solution-level expertise, and onboarding and technical adoption assistance. For additional information on Software Support for Cisco ISE, please see the [Cisco Support Services for Security Software At-a-Glance](#). Please note that Software Support Enhanced is the recommended support level for ISE subscription licenses.

2.3.2. Advisory Services

Cisco offers [Expert 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 help ensure the success of your segmentation initiative.

2.3.3. Cisco Talos Incident Response

The Cisco Talos Incident Response retainer provides a full suite of proactive and emergency services to help you prepare, respond, and recover from a cybersecurity breach. Cisco Talos Incident Response enables 24-hour emergency response capabilities and direct access to Cisco Talos®, the world's largest threat intelligence and research group.

You can order and transact Cisco Talos Incident Response when ordering Cisco ISE subscriptions. This will provide you yet another option to create a stronger security posture and stay protected in case of a security breach. Cisco Talos Incident Response will automatically attach with right sizing based on product order size. The auto-attached SKU can be removed and is not mandatory. Also, you can manually select from the available Cisco Talos Incident Response options in case of no auto-attach.

The table below shows the Cisco Talos Incident Response options available in a Cisco ISE configuration.

Table 1. Cisco Talos Incident Response SKUs

SKU	Description
SVS-CTIR-ISE-S	Cisco Talos Incident Response Retainer-Small, Attach with ISE
SVS-CTIR-ISE-M	Cisco Talos Incident Response Retainer-Medium, Attach with ISE
SVS-CTIR-ISE-L	Cisco Talos Incident Response Retainer-Large, Attach with ISE

To learn more about Cisco Talos Incident Response, see the [Incident Responses Services](#) webpage.

Note: If you have any further questions about services, reach out to your account manager.

3. Cisco ISE licenses

3.1. Understanding Cisco ISE licenses

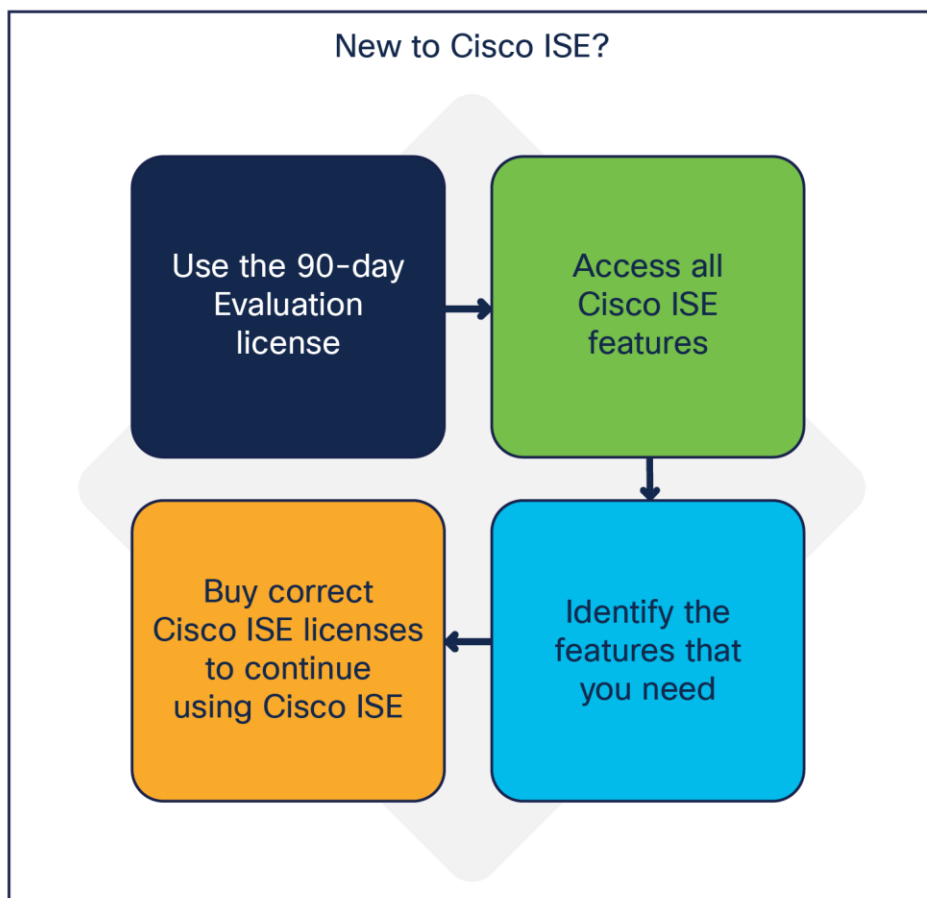


Figure 3. Evaluating Cisco ISE

Cisco ISE, upon installation, grants a 90-day Evaluation license that supports 100 endpoints and enables all Cisco ISE features. You can set up a limited deployment in Evaluation mode and explore all the capabilities and features within Cisco ISE.

A valid Cisco.com login is required to download the software. An existing Cisco ISE support contract may be required to download additional patches or packages.

For more information on your ISE release, please refer to the [Cisco ISE Administrator Guide, Release 3.1](#).

When Evaluation licenses expire at the 90-day mark, administrators can view only the Licensing window in the Cisco ISE administrator portal. No alarms are sent to administrators to notify them of Evaluation license expiration.

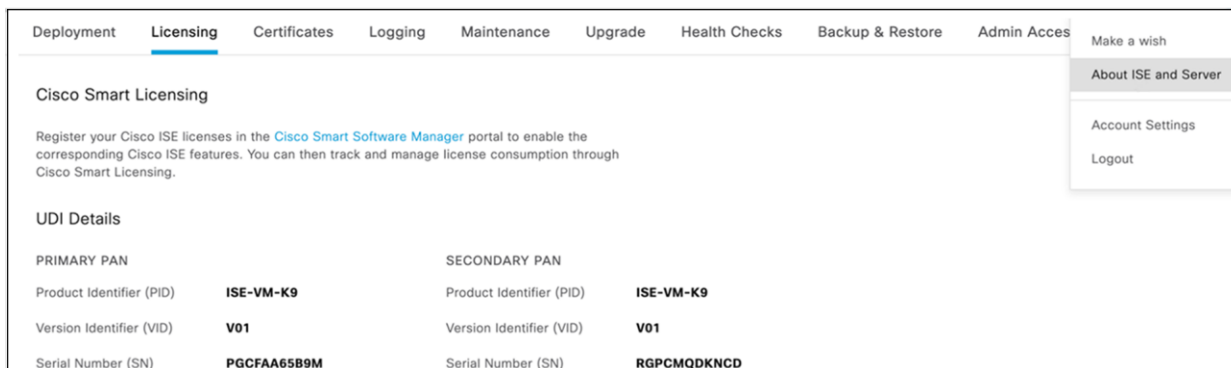
You may request an extension to your Evaluation licenses by adding another 90-day Evaluation license. You can also ask for your Evaluation license to support more than 100 endpoints. To increase endpoint support or to extend the Evaluation license duration, open a case via the [SCM tool](#) with your Unique Device Identifiers (UDIs), your license request, and a justification message.

Note that the UDI information for your Cisco ISE primary and secondary Policy Administration Nodes (PANs) is essential to modify your Evaluation license.

A UDI consists of:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

To view your Cisco ISE UDI, log in to your Cisco ISE administrator portal. From the main menu, choose **Administration > System > Licensing**. The UDI Details area contains the required information.



The screenshot shows the Cisco ISE administrator portal interface. The top navigation bar includes tabs for Deployment, Licensing (selected), Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, and Admin Access. A dropdown menu is open under Admin Access, showing options: Make a wish, About ISE and Server, Account Settings, and Logout. The main content area is titled 'Cisco Smart Licensing' and contains a paragraph about registering licenses. Below this is a 'UDI Details' section with a table showing information for Primary and Secondary PANs.

PRIMARY PAN		SECONDARY PAN	
Product Identifier (PID)	ISE-VM-K9	Product Identifier (PID)	ISE-VM-K9
Version Identifier (VID)	V01	Version Identifier (VID)	V01
Serial Number (SN)	PGCFAA65B9M	Serial Number (SN)	RGPCMQDKNCD

Alternatively, you can also see the **About Identity Services Engine** option in the Cisco ISE administrator portal:

About ISE and Server ✕

SERVER

Host:	sudhanss002	System Time:	Jul 18 2022 05:27:03 PM UTC
Personas:	Administration, Monitoring, Policy Service (SESSION,PROFILER)	FIPS Mode:	Disabled
		Version:	3.2.0.484
		Patch Information:	none
Role:	PRI(A), SEC(M)		

CISCO ISE

Product Identifier (PID)	ISE-VM-K9	Serial Number (SN)	PGCFAA65B9M
Version Identifier (VID)	V01	ADE-OS Version	3.2.0.219

To view the UDI details through the Cisco ISE command-line interface, use the **show udi** command:

Admin CLI

```
Positron-vm-3/admin#show udi
```

```
SPID: ISE-VM-K9
```

```
VPID: V01
```

```
Serial: TNEG8ID3JQ5
```

3.2. ISE Subscription Licenses

Subscription licenses refer to the licensing based on number of active endpoints you want to manage and secure within your network using ISE. These licenses are a crucial part of ISE deployment as they determine the number of active endpoints that can be authenticated, authorized, monitored or secured by ISE.

These are classified into three Tiers: Essentials, Advantage and Premier.

ISE Essentials:

ISE Essential is the base licensing tier that provides fundamental identity and access management features. It includes functionalities such as 802.1X-based network access, guest access management, posture assessment, and basic profiling capabilities. This tier is suitable for organizations looking for essential security features to control access to their network resources.

ISE Advantage:

ISE Advantage is the mid-tier licensing option that builds upon the features offered in the Essential tier. In addition to the functionalities provided in Essential, Advantage includes more advanced features such as Profiling, BYOD, Cisco pxGrid integration, and TrustSec Security Group Tagging (SGT) enforcement. This tier is appropriate for organizations requiring more extensive policy enforcement and advanced network access control capabilities.

ISE Premier:

Cisco ISE Premier is the highest licensing tier available for Cisco ISE. It encompasses all the features provided in the Essential and Advantage tiers and adds further enhancements like endpoint compliance and security automation integrations like MDM & Posture, as well as advanced threat containment and visibility capabilities TC-NAC. This tier is suitable for organizations with complex network environments and advanced security needs.

3.2.1. Feature mapping in Subscription Licenses

The following figure shows the mapping of features in ISE Subscription Tier licenses.

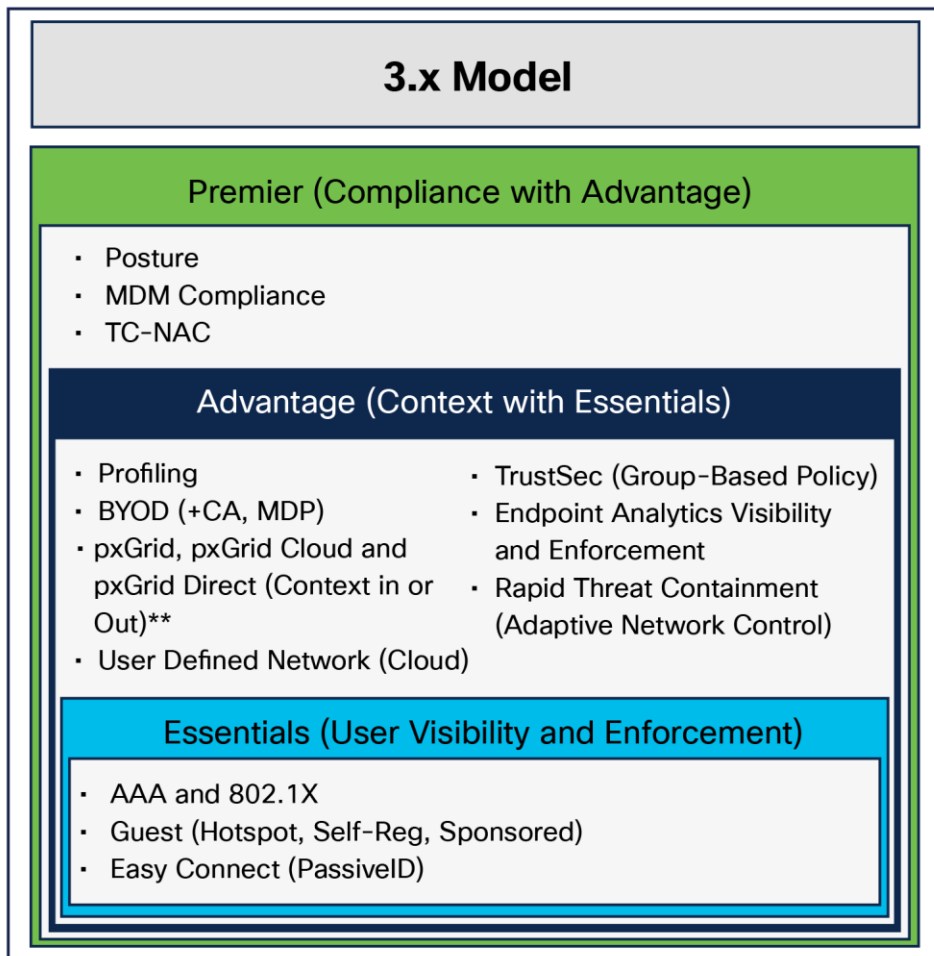


Figure 4.

Mapping of 3.x licensing model features

**For more information on pxGrid Cloud, please refer to the [Cisco pxGrid Cloud Solution Guide](#).

3.2.2. Cisco ISE Subscription license entitlement

When you purchase a license, you agree upon a quantity and duration for which you are purchasing the license. License entitlement refers to the monitoring and enforcement of license usage according to these terms.

A license is out of compliance when:

- The deployment uses more than 100 percent of active endpoints compared to the quantity purchased.
- The licenses have expired without renewal.

When a license is out of compliance or is nearing renewal:

- Alerts are displayed in your Cisco ISE GUI every day that the license is out of compliance.
- For term licenses that are nearing expiration, alerts are displayed at the 90-, 60-, and 30-day marks before expiration, and every day for the last 30 consecutive days before expiration.

During the time that the alerts are displayed, there is no impact to Cisco ISE usage. Existing configurations continue to operate without disruption.

If your Cisco ISE deployment is out of compliance for 30 days in a 60-day period, you will lose all administrative control of Cisco ISE until you purchase and activate the required licenses. Also, visibility and management of the features associated with an out-of-compliance license are affected. A Cisco ISE administrator has a limited read-only capability over the relevant features until the causes of noncompliance are fixed. **Authentications and features will continue to work as configured prior to license expiration.**

If you lose administrative access due to overconsumption and you then reduce the license consumption, the system recovers at the next synchronization with the Smart License Portal. Also, overconsumption for any amount of time during that day will count as a day (within a 24-hour period).

3.2.3. Subscription Tier License consumption

ISE license consumption is based on active endpoint counts measured through RADIUS sessions. In situations where RADIUS sessions are not present or cannot be correctly counted, then unique endpoint attributes may be used (example: PassivID etc). If you enable privacy/private MAC/MAC randomization/rotating and changing MAC in endpoints, the license consumption may be higher, as different sessions will be created for the same endpoint getting authenticated a second time with different MAC IDs.

The following table shows ISE licensing consumption.

Table 2. ISE licensing consumption

Feature	License tier	Dictionary/attribute	Trigger of license consumption	When license is released
AAA and 802.1X	Essentials		An endpoint establishes a RADIUS session	RADIUS session ends
Guest	Essentials		An endpoint with RADIUS session uses any Guest authorization	RADIUS session ends

Feature	License tier	Dictionary/attribute	Trigger of license consumption	When license is released
Easy Connect (PassiveID)	Essentials		An endpoint with a RADIUS session uses any Easy Connect functionality	RADIUS session ends
Profiling	Advantage	EndPoints.EndPointPolicy EndPoints.LogicalProfile	An endpoint with a RADIUS session uses profiling classification in an authorization policy	RADIUS session ends
BYOD (+CA, MDP)	Advantage	EndPoints.BYODRegistration	An endpoint with a RADIUS session uses its registration status in an authorization policy	RADIUS session ends
pxGrid, pxGrid Cloud, and pxGrid Direct (Context In or Out with Cisco and external third-party products)	Advantage		An endpoint with a RADIUS session connects over pxGrid	RADIUS session ends
Integrations (non-pxGrid)	Advantage		An endpoint establishes a RADIUS session	RADIUS session ends
Group-Based Policy (Cisco TrustSec[®])	Advantage		An endpoint establishes a RADIUS session	RADIUS session ends
Endpoint Analytics Visibility/ Enforcement	Advantage	CMDB_MODELCATEGORY CMDB_SERIAL_NUMBER CONCURRENT_MAC_ADDRESS EA_DEVICE_TYPE EA_HIERARCHY EA_MANUFACTURER EA_HW_MODEL CHANGE_IN_MFC_RESULT NAT_DETECTION_RESULT EA_OS	When you use these conditions, it's going to be under Enforcement. If not, it's just for visibility.	
Cisco AnyConnect[®] with Agent	Premier	Session.PostureStatus	An endpoint with a RADIUS session receives an authorization based on a posture status other than "Not applicable"	RADIUS session ends
Mobile device management (MDM)	Premier	MDM.DevicelsRegistered MDM.DeviceCompliantStatus	An endpoint uses an MDM attribute in an authorization policy	RADIUS session ends

Feature	License tier	Dictionary/attribute	Trigger of license consumption	When license is released
Threat-Centric Network Admission Control (TC-NAC)	Premier		An endpoint uses or triggers threat-based information or action as part of the authorization policy	RADIUS session ends
RTC (ANC)	Advantage	Session:ANCPolicy	An endpoint with a RADIUS session uses Adaptive Network Control (ANC) policy in an authorization policy	RADIUS session ends
User Defined Network	Advantage	UDN:Private-group-id UDN:Private-group-name UDN:Private-group-owner	An endpoint with RADIUS uses a UDN attribute in an authorization policy	RADIUS sessions ends

3.3. Cisco ISE Device Admin license

The Device Admin license (PID: L-ISE-TACACS-ND=) enables TACACS services on a Policy Service Node (PSN).

3.4. Cisco ISE Virtual Machine licenses

Cisco offers a single VM Common license (R-ISE-VMC-K9=) applicable across all VM and cloud platforms and irrespective of VM size. This license is needed when deploying ISE on non-Cisco hardware or Virtual machines.

4. How to order Cisco ISE licenses

All ISE licenses can be ordered from Cisco Commerce (CCW).

For the Subscription licenses, 3 methods of ordering are available:

1. A-la-carte purchase
2. [Cisco Enterprise Agreements](#)
3. ISE-Advantage licenses come embedded within [Catalyst Software Subscription for Switching](#)

4.1. Ordering ISE Subscription licenses a-la-carte

- Cisco ISE Subscription licenses are ordered from Cisco Commerce (CCW). These can be ordered in any quantity, starting with 50.
- Subscription-based licenses are available in 1-, 3-, and 5-year terms allowing the licenses to be co-terminated.
- The default start date is 3 days from the date of purchase. You can choose a different start date, up to 90 days from the date of purchase. However, you must specify the request to change the start date at the time of placing the order. The start date should be set based on the lead time of the hardware appliance. For example, if the appliance on which you will be installing ISE will not be available for 45 days, set the ISE subscription start date beyond 45 days. For longer lead times, consider buying ISE subscription licenses in a separate order once the hardware has been procured.

You can order three types of SKUs for ISE when buying the Subscription a-la-carte:

- Subscription SKU: Defines the subscription term and start date
- Product SKU: Defines the products and quantities that make up the subscription
- Support SKU: Defines the level of support for the subscription

The steps are given below.

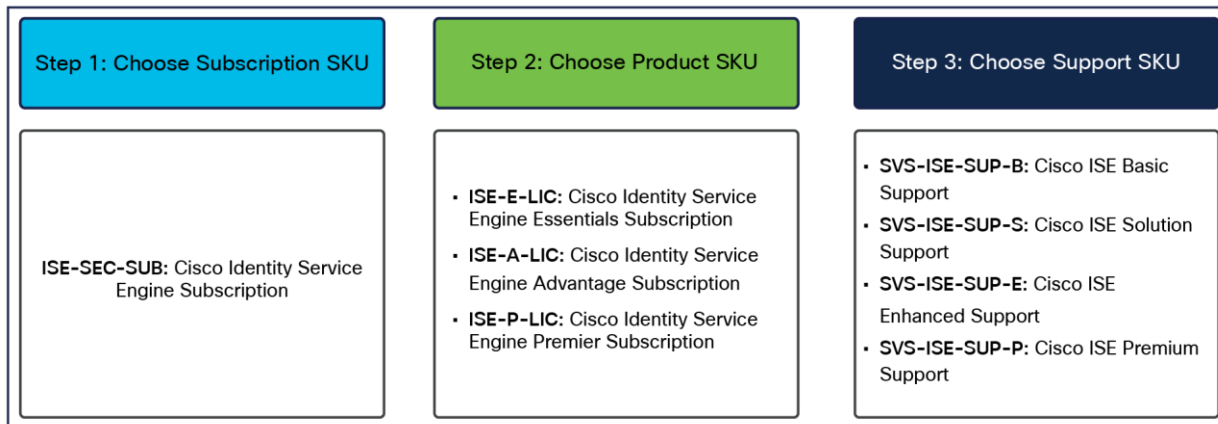


Figure 5.
Steps for ordering ISE licenses

Step 1: Selecting the subscription SKU.

There is one Cisco ISE subscription SKU (ISE-SEC-SUB). There is no price for this 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.

Purchase ISE-SEC-SUB Configuration

Requested Terms and Billing / Global Price List (USD)

Requested Start Date: 21-Aug-2020 | Requested For: 36 Months From 21-Aug-2020 To 20-Aug-2023 | Automatically Renews For: 12 Months On 21-Aug-2023 | Billing Frequency: Prepaid Term

Configuration Summary

Cisco Identity Service Engine Subscription

ISE Support

SKU	Qty	List Price
SYS-ISE-SUP-8	1	\$0.00
	Each	Per Each/Month

Subtotal: \$0.00

Restore Configuration | Cancel | Review Changes

ISE-SEC-SUB quantity 1 requires a minimum quantity of 100 from Cisco Identity Service Engine Subscription (CE100012)

Configuration is required. Please check the Configuration Summary window and configure the item(s) with warning icon image to the right.

ISE-SEC-SUB > Cisco Identity Service Engine Subscription

Cisco Identity Service Engine Subscription

License	SKU	Description	Unit List Price (USD)	Action
Qty	ISE-E-LIC	Cisco Identity Service Engine Essentials Subscription	Enter Qty to see List Price Per License/Month	
Qty	ISE-A-LIC	Cisco Identity Service Engine Advantage Subscription	Enter Qty to see List Price Per License/Month	
Qty	ISE-P-LIC	Cisco Identity Service Engine Premier Subscription	Enter Qty to see List Price Per License/Month	

The subscription term will default to 36 months (3 years). To change the term, see the screen shot below.

Purchase ISE-SEC-SUB Configuration

Current Requested Terms and Billing / Global Price List (USD)

Requested Start Date: 21-Aug-2020 | Requested For: 36 Months From 21-Aug-2020 To 20-Aug-2023 | Automatically Renews For: 12 Months On 21-Aug-2023 | Billing Frequency: Prepaid Term

Cisco will apply a standard lead time to your requested start date based on the selected product. If your start date is less than the lead time, Cisco may not be able to honor the requested start date. In some cases, our systems may require additional lead time to provision your services. (C0742)

REQUESTED FOR 36 Months | From 21-Aug-2020 To 20-Aug-2023

Requested Start Date

Day: 21 | Month: Aug | Year: 2020

Enter any date up between 18-Aug-2020 and 15-Nov-2020

End Date

Effective For: 36 Months

Enter any whole month value from 1-60

Co-Term to an End Date

Day: 20 | Month: Aug | Year: 2023

Enter any date up between 18-Nov-2020 and 20-Aug-2025

Automatically Renews For: 12 Months On 21-Aug-2023

Auto Renewal On

12 Months

Billing Frequency Prepaid Term

Prepaid Term | Annual Billing | Quarterly Billing | Monthly Billing

Cancel | Save Changes

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 shown 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.

Purchase ISE-SEC-SUB Configuration

Global Price List (USD)

Requested Start Date 21-Aug-2020	Requested For 36 Months From 21-Aug-2020 To 20-Aug-2023	Automatically Renews For 12 Months On 21-Aug-2023	Billing Frequency Prepaid Term
-------------------------------------	--	--	-----------------------------------

Configuration Summary

Cisco Identity Service Engine Subscription

ISE Support

SKU	Qty	List Price
SVS-ISE-SUP-B SA	1 Each	\$0.00 Per Each/Month

Subtotal: **\$0.00**

Restore Configuration Cancel Review Changes

ISE-SEC-SUB quantity 1 requires a minimum quantity of 100 from Cisco Identity Service Engine Subscription (CE100012)

Configuration is required. Please check the Configuration Summary window and configure the Item(s) with warning icon image to the right.

ISE-SEC-SUB > Cisco Identity Service Engine Subscription Key

Cisco Identity Service Engine Subscription

Cisco Identity Service Engine Subscription

License	SKU	Description	Unit List Price (USD)	Action
<input type="text" value="Qty"/>	ISE-E-LIC SA	Cisco Identity Service Engine Essentials Subscription	Enter Qty to see List Price Per License/Month	
<input type="text" value="Qty"/>	ISE-A-LIC SA	Cisco Identity Service Engine Advantage Subscription	Enter Qty to see List Price Per License/Month	
<input type="text" value="Qty"/>	ISE-P-LIC SA	Cisco Identity Service Engine Premier Subscription	Enter Qty to see List Price Per License/Month	

Pricing is determined dynamically according to the quantity ordered and the 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 screen shot below shows a 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.

Purchase ISE-SEC-SUB Configuration [Ordering Guide](#)

Requested Terms and Billing Global Price List (USD)

Requested Start Date: 24-Sep-2020 | Requested For: 36 Months From 24-Sep-2020 To 23-Sep-2023 | Automatically Renews For: 12 Months On 24-Sep-2023 | Billing Frequency: Prepaid Term

Configuration Summary

Cisco Identity Service Engine Subscription

SKU	Qty	List Price
ISE-E-LIC	100 License	\$0.18 Per License/Month
ISE-P-LIC	1500 License	\$1.59 Per License/Month

ISE Support

Subtotal: \$86,508.00

[Restore Configuration](#) [Cancel](#) [Review Changes](#)

Cisco Identity Service Engine Subscription

License	SKU	Description	Unit List Price (USD)	Action
100	ISE-E-LIC	Cisco Identity Service Engine Essentials Subscription	\$0.18 Per License/Month	
Qty	ISE-A-LIC	Cisco Identity Service Engine Advantage Subscription	Enter Qty to see List Price Per License/Month	
1500	ISE-P-LIC	Cisco Identity Service Engine Premier Subscription	\$1.59 Per License/Month	

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:

Cisco Software Support Basic is included for the duration of Cisco ISE subscription licenses. Higher-value service levels, Solution Support, or Software Support Enhanced or Premium Support may be purchased by selecting the appropriate level of support from the support options.

Prices for these higher-value services levels are calculated dynamically based on a percentage of the product cost and must meet annual minimum requirements, where needed. The support level must be consistent across all endpoints. Customers cannot purchase one support level for some endpoints and a different support level for others.

Purchase ISE-SEC-SUB Configuration

Requested Terms and Billing Global Price List (USD)

Requested Start Date: 21-Aug-2020 Requested For: 36 Months From 21-Aug-2020 To 20-Aug-2023 Automatically Renews For: 12 Months On 21-Aug-2023 Billing Frequency: Prepaid Term

Configuration Summary

Cisco Identity Service Engine Subscription

ISE Support

SKU	Qty	List Price
SVS-ISE-SUP-B	1 Each	\$0.00 Per EachMonth

Subtotal: **\$0.00**

Restore Configuration Cancel Review Changes

Configuration is required. Please check the Configuration Summary window and configure the item(s) with warning icon image to the right.

ISE-SEC-SUB > ISE Support

ISE Support

Subscriptions

Each	SKU	Description	Unit List Price (USD)	Action
1	SVS-ISE-SUP-B	Basic Support for Identity Service Engine Subscription	\$0.00 Per EachMonth	
Qty	SVS-ISE-SUP-E	Enhanced Support for Identity Service Engine Subscription	Enter Qty to see List Price Per EachMonth	
Qty	SVS-ISE-SUP-P	Premium Support for Identity Service Engine Subscription	Enter Qty to see List Price Per EachMonth	

Quoting and ordering help

For quoting or ordering questions, please contact cs-support@cisco.com.

4.2. Changing existing orders or subscriptions

Cisco Commerce (CCW) provides you the capability to modify, renew, and replace subscriptions for your active orders including changes to quantities or upgrading tiers.

For more information, refer to the [Change Subscription Job Aid](#).

4.3. Other ISE License SKUs based on your deployment

Apart from the subscription, product, and service SKUs, you also need to choose SKUs as required to cover the Cisco hardware appliances, virtual machines, and Device Admin nodes in your deployment. All the below licenses are perpetual in nature.

- **Cisco ISE Device Admin SKU (L-ISE-TACACS-ND=)**: Purchase one license for each PSN on which you wish to enable TACACS services.
- **Cisco ISE IPsec SKU (L-ISE-IPSEC)**: Purchase one license for each PSN that you use for IPsec VPN communication with network access devices. A maximum of 150 IPsec tunnels are supported on each PSN.
- **Cisco ISE VM License SKU (R-ISE-VMC-K9=)**: Purchase a license for each virtual machine or cloud-deployed ISE node in your deployment.
- **Cisco ISE VM License SKU (R-ISE-VMF-K9=)**: This is a special free VM license of 1 quantity available for eligible first-time ISE customers who receive ISE Subscription Tier licenses through the purchase of [Catalyst Advantage Subscription for Switching](#). Customers can contact their Channel Partners or Cisco Account teams to see if they would be eligible.

-
- **Cisco ISE-PIC License SKUs** (R-ISE-PIC-VM-K9= and L-ISE-PIC-UPG=): ISE-PIC is ISE with only the Passive Identity Connector (PIC) function. The SKU R-ISE-PIC-VM-K9= allows 3000 ISE-PIC sessions per ISE deployment. Purchasing the ISE-PIC-Upgrade SKU L-ISE-PIC-UPG= in addition to R-ISE-PIC-VM-K9= allows 300,000 ISE-PIC sessions. For more information on the ISE PIC, please refer to the [Cisco ISE Passive Identity Connector Data Sheet](#).

If an ISE-PIC node also has the ISE-PIC upgrade license, you can assign Essentials licenses to it, thereby making it an ISE server with full functionality. Please note that the features enabled in the 'full ISE' will depend on the available Subscription or other licenses. For example, enabling pxGrid requires Advantage licenses as stated in above sections.

5. Specific ISE Licensing Methods based on deployment

The Cisco ISE licenses that are available in your account are displayed in the SSM portal for you to monitor and manage.

You can configure Cisco ISE Smart Licensing through various methods, depending on the needs of your organization.

Choose a licensing method:

Smart Licensing for connected networks

Smart Licensing for air-gapped networks (SSM on-premises servers)

Specific License Reservation

5.1. Licensing with persistent Internet connection

Support notes: This licensing method is supported by Cisco ISE Release 2.4 and later.

If your Cisco ISE has a persistent internet connection, Smart Licensing is easily managed through consistent communication between Cisco ISE and the SSM. Direct internet connections and proxy servers are both supported by this Smart Licensing method.

5.2. Licensing in an air-gapped network with SSM on-prem

Cisco ISE Release 2.6 and later supports the use of SSM on-premises servers for Smart Licensing.

Cisco ISE Smart Licensing requires Cisco ISE to be connected to the SSM. If your network is air-gapped, Cisco ISE is unable to report license usage to SSM. This lack of reporting results in a loss of administrative access to Cisco ISE and restrictions in Cisco ISE features.

To avoid licensing issues in air-gapped networks and enable full Cisco ISE functionality, configure SSM On-Prem. This server takes over the role of Cisco SSM in your air-gapped network, releasing license entitlements as needed, and tracking usage metrics. The SSM on-premises server also sends notifications, alarms, and warning messages that are related to licensing consumption and validity.

5.3. Specific License Reservation (SLR)

Support note: Supported in Cisco ISE Release 3.1 and later.

Cisco ISE Smart Licensing requires Cisco ISE to be connected to the Cisco SSM. Cisco ISE Release 3.0 and later supports only Smart Licensing. If your network is air-gapped, Cisco ISE 3.x deployments are unable to report license usage to the SSM, and this results in a loss of administrative access to Cisco ISE and restrictions in Cisco ISE features.

Specific License Reservation enables you to deploy a software license on a device without communicating usage information to Cisco. This functionality is especially useful in highly secure networks, and it is supported on platforms that have Smart Licensing enabled.

Customers must be aware of following licensing processes while using SLR:

- A. Purchasing and reserving the right tiers and quantities for Primary PAN
- B. Purchasing and reserving the right tiers and quantities for Secondary PAN

Primary PAN:

While Cisco ISE Smart Licensing works as a nested model in which a higher-tier license includes all the lower-tier features, Specific License Reservation does not fully support such a model automatically. In Specific License Reservation, you must reserve and activate the required license count for each Cisco ISE license type. For example, if your deployment will consume Cisco ISE features enabled by Advantage and Premier licenses, you must reserve both Advantage and Premier licenses. If you reserve only Premier licenses, but your deployment has active endpoints which are only consuming Advantage tier feature and no Premier tier features, you receive error or non-authorized behavior notifications.

So, the reservation should be done based on the below criteria:

Premier Quantity to be reserved = Same as portion of peak active endpoints consuming Premier features. It does not matter whether the same endpoints consume Advantage or Essentials because premier already includes them.

Advantage Quantity to be reserved = Same as portion of peak active endpoints consuming Advantage features (but not Premier features). It does not matter whether the same endpoints consume Essentials because Advantage already includes them.

Essentials Quantity to be reserved = Same as portion of peak active endpoints consuming Essentials-only features (but no Advantage or Premier features)

Customers can change the reserved license tiers and quantities anytime.

Here is an example illustrating the SLR process for Subscription licenses:

Step 1: Purchase/Order:

Tier = Premier; Quantity = 100

Step 2: Smart Account display (after booking/invoicing)

Tier = Premier; Quantity = 100

Step 3: Generate SLR Reservation code in ISE

Step 4: Enter SLR Reservation Code in SSM

Step 5: SSM will show the following licenses to reserve (breaking Premier into lower tiers because of nested-doll model):

Tier = Premier; Purchase quantity = 100; Available to reserve quantity = 100

Tier = Advantage; Purchase quantity = 0; Available to reserve quantity = 100

Tier = Essentials; Purchase quantity = 0; Available to reserve quantity = 100

And this is where the customer must reserve each tier individually by adding quantities next to each tier. Please note that the total still needs to be 100 or less. So, the customer can do the following:

Premier Reserve quantity = 80

Advantage Reserve quantity = 10

Essentials Reserve quantity = 10

OR

Premier Reserve quantity = 30

Advantage Reserve quantity = 30

Essentials Reserve quantity = 10

Note the total is less than 100

Or

Any other combinations are possible where the total quantity across the tiers is 100 (same as the purchased quantity) or less.

Secondary PAN:

In a distributed deployment, you may need to enable Specific License Reservation on your primary and secondary PANs. If there are no Cisco ISE licenses registered on your secondary PAN, in the case of primary PAN failure, Cisco ISE access and services are impacted.

If Cisco ISE licenses are registered on the secondary PAN as well, in the event of a primary PAN failover, Cisco ISE will continue to be accessible through the newly promoted secondary PAN. You can then work on rejoining the primary PAN to its original state.

The following table explains two approaches to ensuring uninterrupted access to Cisco ISE if you require 100 tier licenses.

Table 3. License distribution for ISE licenses

Minimum license distribution that ensures Cisco ISE runs uninterrupted for certain period		What to expect in the event of a primary PAN failover	Maximum license distribution that ensures Cisco ISE runs uninterrupted, without noncompliance alarms		What to expect in the event of a primary PAN failover
Primary PAN	Secondary PAN		Primary PAN	Secondary PAN	
100	1	<p>Since the newly promoted primary PAN doesn't have sufficient licenses, your Cisco ISE goes out of compliance. Cisco ISE enters a 30-day grace period.</p> <p>Before the grace period expires, rejoin the original primary PAN with the higher license count.</p> <p>Alternatively, to continue working with the newly promoted primary PAN, release the licenses reserved on the original PAN and reserve the required licenses on the newly promoted PAN.</p>	100	100	<p>No impact on Cisco ISE services or operations.</p> <p>No remediation actions are required. You must only rejoin the original PAN to Cisco ISE.</p>

If there are zero licenses reserved on Secondary PAN, then it goes into 'Evaluation Mode' depending on the number of evaluation days left for the entire deployment since the first time ISE was deployed. For example, if ISE already used up 50 days in the initial eval period before purchased licenses were registered, then Secondary PAN (which becomes the newly promoted primary PAN on failover) would remain in evaluation period for 40 days in SLR scenarios. If there are zero evaluation days left, then the deployment becomes out-of-compliance until the customer releases the licenses reserved on the original PAN and reserves them on the newly promoted PAN.

You will not be able to use any license entitlements that are not part of your Specific License Reservation. Out-of-compliance alerts are shown in the Cisco ISE administration portal if license usage does not comply with the Specific License Reservation.

5.3.1. Licensing directives related to Specific License Reservation

- The number of licenses you can reserve through Specific License Reservation can be lower than or equal to the total number of licenses listed in the Purchased column, in the Licenses Inventory window of your Cisco SSM portal.
- You can reserve ISE-PIC licenses for Cisco ISE nodes that contain only the Passive Identity Connector (PIC) function. Each ISE-PIC license supports 3000 Cisco ISE-PIC sessions in a deployment. You can reserve only one ISE-PIC license per node. Hence, the number of available licenses decreases by 1. If you have purchased 5 ISE-PIC licenses and reserve 4 ISE-PIC licenses, then you have the following:

Table 4. ISE-PIC example

License	Purchased	In use	Balance
ISE-PIC	5	(4 reserved)	1

One ISE-PIC-UPG license supports 300,000 ISE-PIC sessions. To reserve an ISE-PIC-UPG license, you must also reserve an ISE-PIC license.

You cannot reserve tier licenses (ISE Essentials, ISE Advantage, or ISE Premier) in a Cisco ISE -PIC node.

You cannot reserve an ISE-PIC license on a Cisco ISE node. However, the License Reservation workflow in the Cisco SSM portal allows you to assign an ISE -PIC license to a Cisco ISE node. The SSM portal displays that the ISE-PIC license is reserved until you modify the reservation to remove the ISE-PIC license.

The License Reservation workflow in the Cisco SSM portal allows you to assign ISE Essentials licenses for an ISE-PIC node, even though the ISE-PIC node does not allow the use of these licenses. The SSM portal displays that the ISE Essentials licenses are reserved until you modify the reservation to remove the ISE Essentials licenses.

5.3.2. Specific License Reservation examples

Table 5. Specific License Reservation examples

Available licenses in your virtual account in SSM (*1)	Reserved licenses in ISE deployment	Licenses remaining in your virtual account in Cisco SSM (*1)
Rule 1. You can reserve as many licenses as you have in your virtual account.		
100 Essentials	300 Essentials (*2)	0 Essentials
100 Essentials		
100 Essentials		
Rule 2. You should reserve the right type of license that you are entitled to.		
100 Advantage	40 Advantage 40 Essentials (*3)	20 Advantage
Rule 3. You should reserve 1 ISE-PIC license (*4) per node.		
5 ISE-PIC licenses	1 ISE-PIC license	4 ISE-PIC licenses
Rule 4. If you reserve an ISE-PIC-UPG license, you must also reserve 1 ISE-PIC license.		
5 ISE-PIC licenses	1 ISE-PIC license	4 ISE-PIC licenses
3 ISE-PIC-UPG licenses	1 ISE-PIC-UPG license	2 ISE-PIC-UPG licenses
5 ISE-PIC licenses	1 ISE-PIC license (*5)	4 ISE-PIC licenses
3 ISE-PIC-UPG licenses		3 ISE-PIC-UPG licenses

Available licenses in your virtual account in SSM (*)	Reserved licenses in ISE deployment	Licenses remaining in your virtual account in Cisco SSM (*)
---	-------------------------------------	---

Rule 5. You shouldn't reserve Essentials, Advantage, and Premier licenses to the ISE-PIC node unless you are upgrading ISE-PIC to the ISE full version (*6).

- *1 This doesn't include licenses previously reserved and not returned.
- *2 You can reserve up to as many licenses as you are entitled to.
- *3 An Essentials license can be reserved if there are higher tier licenses available.
- *4 You should reserve only 1 ISE-PIC license per node. An ISE-PIC license should not be reserved to an ISE node. If you do it, then SSM will allow it even though it cannot be used in the deployment as these validations are not built into SSM.
- *5 You can reserve an ISE-PIC license only, which allows for up to 3000 ISE-PIC sessions per ISE-PIC deployment.
- *6 This is a rare case in which a customer has both an ISE-PIC deployment and an ISE deployment.

6. Subscription Renewals, Cancellations or Modifications

6.1. Subscription renewals

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 order 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 before the start date of the new term. If the subscription is not canceled 60 days before the start of the new term, the subscription will auto-renew. Midterm cancellations of subscriptions for credit are not allowed.

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.

6.2. Subscription cancellations

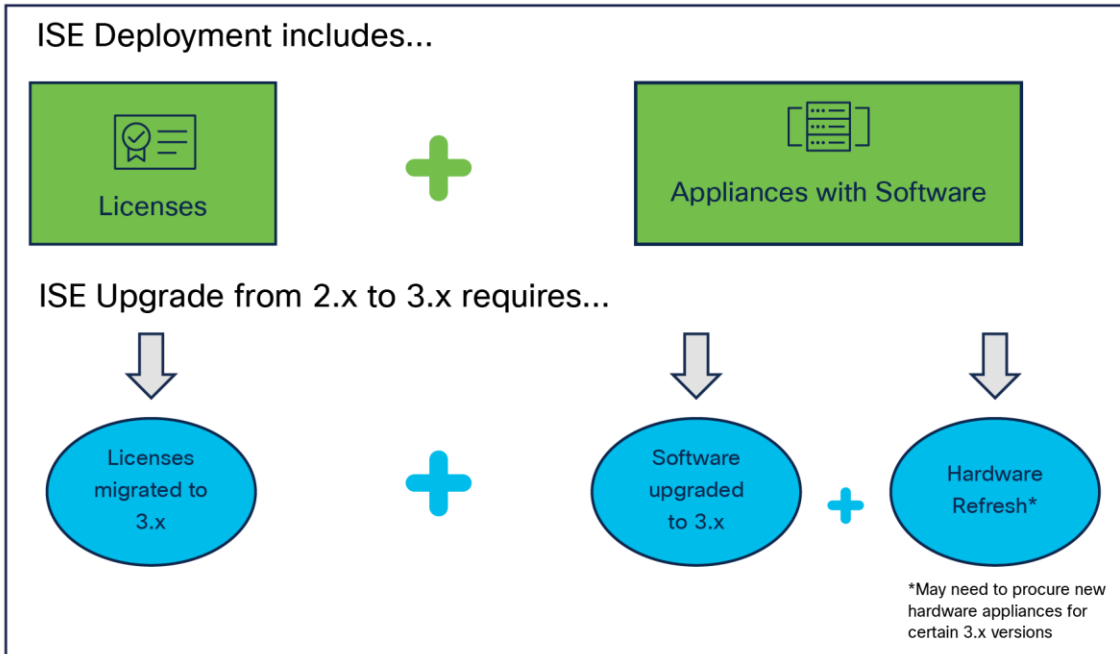
Renewals may be canceled up to 60 days before the start date of the new term. If the subscription is not canceled 60 days prior to the start of the new term, the subscription will automatically renew. Midterm cancellations of subscriptions for credit are not allowed.

6.3. Subscription Modifications

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 the [Cisco Commerce Change Subscription Job Aid](#). Attempting to add products or seats by creating a new subscription will result in an ordering error.

7. Cisco ISE license migration

An ISE Upgrade from 2.x to 3.x version may require multiple steps to be taken by the customer.



Planning the upgrade:

Step 1: Evaluate the features in 3.x versions to determine which version best works for your deployment

Step 2: Choose the upgrade path depending on where your current deployment is and which version you want to upgrade to

Executing the upgrade

Step 1: Procure additional hardware depending on the future 3.x version

Step 2: Migrate ISE Licenses from 2.x to 3.x (detailed later in this document)

Step 3: Upgrade the deployment to the decided 3.x version before 22-Sep-2024

Please refer to the [Cisco Upgrade guide](#) for details of the steps not covered in this document. Cisco highly recommends utilizing the free [Healthchecks and expert sessions](#) before performing the upgrade.

Get help from an expert

For an ISE health check or 1:1 consultation with a Cisco expert, please connect with your Cisco account team or attend the following Ask the Experts session below.

Featured session: ISE Upgrade

Cisco ISE licenses have undergone some changes to help streamline and optimize Cisco ISE purchasing and management.

New licenses introduced in Cisco ISE are typically Smart Licenses. Therefore, to migrate an existing 2.x license type to a new 3.x license type, you will need a Smart Account for Cisco Smart Licensing. [Here](#) is a video with instructions for creating a Smart Account.

The following figure shows the mapping of features between the 2.x and 3.x licenses.

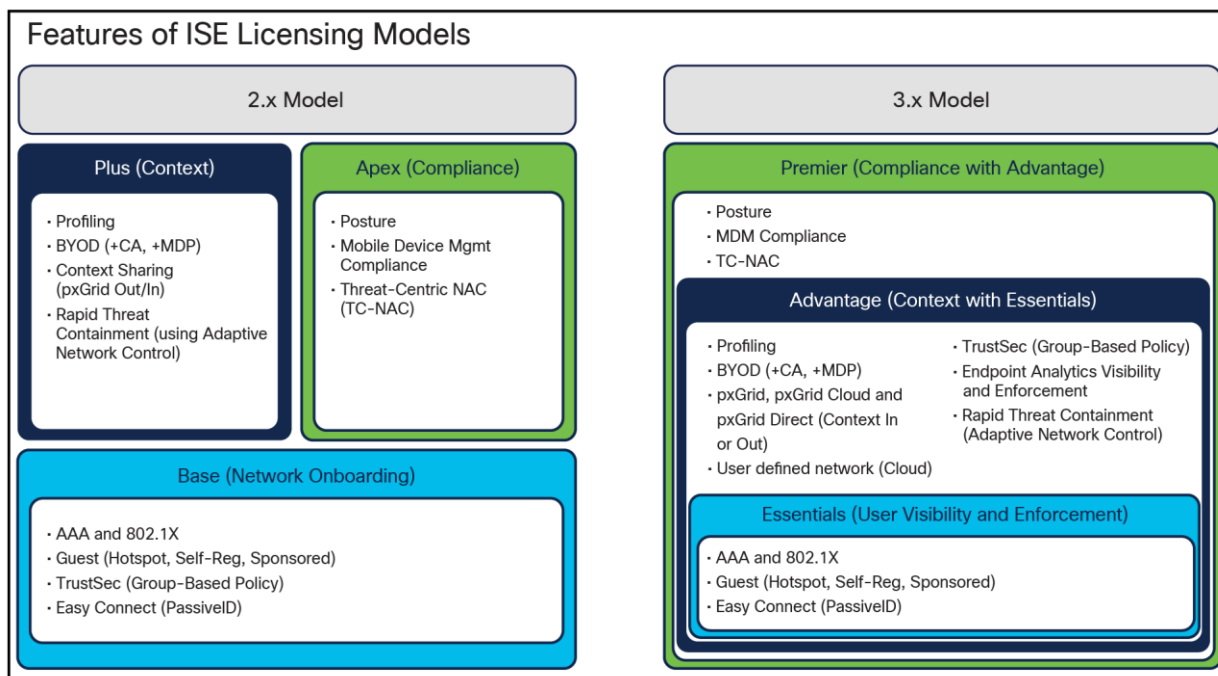


Figure 6. Mapping of 2.x and 3.x licensing model features

7.1 Cisco ISE Subscription license migration

Customers should migrate their licenses from ISE 2.x to 3.x using the **new ISE License Migration Offer** which is valid from Nov 1, 2023 until Sep 22, 2024

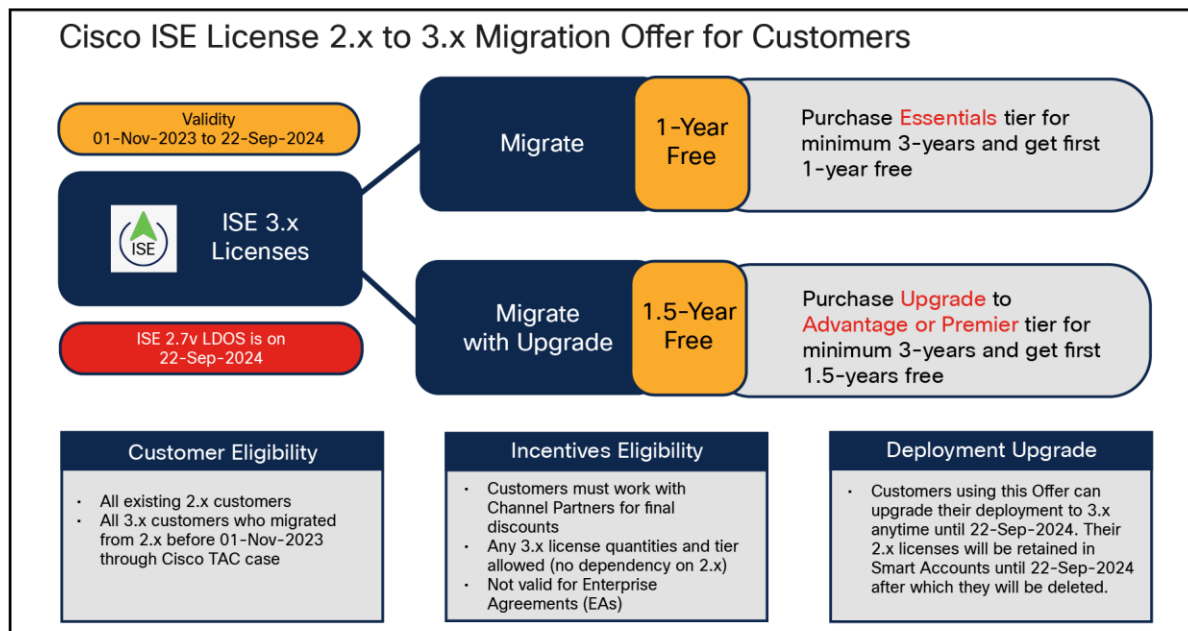


Figure 7.
Cisco ISE License Migration offer

7.1.1. Migrate from 2.x licenses to 3.x Subscription licenses using Migration Offer

Customers should work with their preferred Channel partners (where applicable) to place orders with Cisco for ISE 3.x licenses with a minimum 3-year Subscription duration. As part of this process, customers will receive the following incentives.

- A. First one year of Subscription free if they stay on lower Essentials tier.
- B. First one and half years of Subscription free on upgrading to higher tiers of Advantage or Premier

There is no dependency on tiers or quantities of current 2.x licenses. This Migration Offer allows choosing any 3.x tier or quantities as customers see fit. Cisco recommends using this opportunity to move to higher tiers to realize greater value and better network security from ISE 3.x versions.

All existing ISE 2.x customers who purchased 2.x through a-la-carte or DNA-Premier or Cisco One or other similar means can migrate to 3.x licenses using the above Offer.

For more information on this offer and specific terms, please refer to [ISE License Migration Offer - FY24](#). (Requires Cisco CCO login credentials)

Cisco Partners can refer to [ISE 2.x to 3.x License Migration Offer - Partners](#)

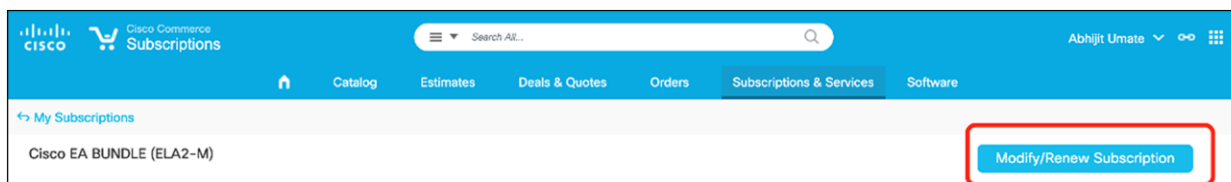
Cisco Sellers can refer to [ISE 2.x to 3.x License Migration Offer - Cisco INTERNAL ONLY](#)

Note: This new Migration Offer replaces the earlier 1-year-on-us promotion which was valid until Oct 31, 2023 and the manual TAC case process.

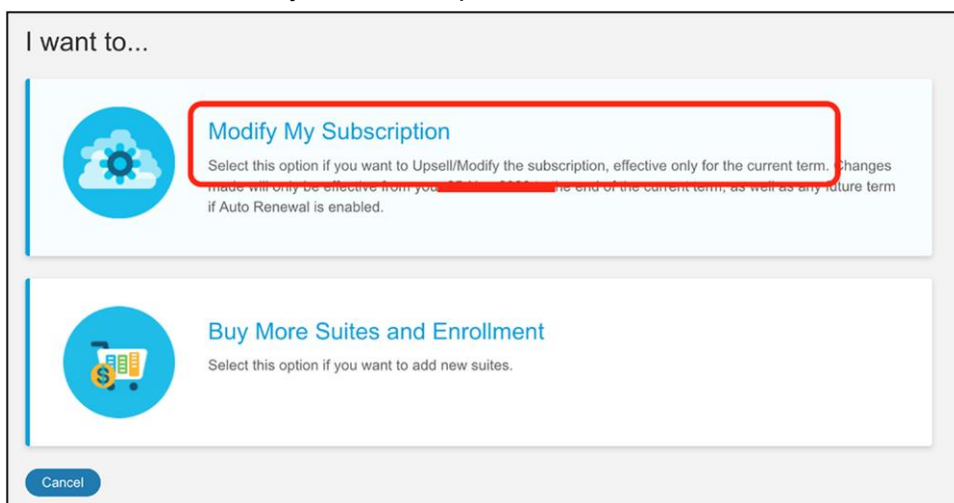
7.1.2 Migration for Enterprise Agreement customers

Cisco recommends all 2.x Enterprise Agreement (EA) customers to work with your Channel Partner or Account team to use the 'EA Change Subscription' process to replace 2.x with 3.x licenses. This ensures customers can continue to receive the benefits (example- Additional license generation, True Forwards etc) from the EA agreement for their 3.x licenses. Cisco Sales and Partners can follow these steps:

1. Open existing EA Subscription in [CCW](#) using Subscription ID
2. Click on 'Modify/Renew Subscription' button to start the Change Subscription process



3. Select to modify the Subscription



4. Click on 'Edit Options' link against the ISE Suite represented by E2F-SEC-ISE PID

Bundle Configuration
Modify ELA2-M Configuration ⓘ

Requested Terms and Billing ✎

Requested Change Date
██████████

SECURITY ENROLLMENT > 7 Selected (Min 0, Max 9999)

Product
E2F-SEC-NGFW Valid ⓘ Cisco EA 2.0 Choice - Security Suites- NGFW Add Custom Name Edit Options
E2F-SEC-ISE Valid ⓘ Cisco EA 2.0 Choice - Security Suites- ISE Add Custom Name Edit Options
E2SF-I-ISE-PLUS-10 Security EA 2.0 Choice ISE Plus License 10pk
E2SF-I-ISE-APEX-10 Security EA 2.0 Choice ISE Apex License 10pk
E2SF-I-ISE-BASE-10 Security EA 2.0 Choice ISE Base License 10pk
SVS-EA2-CISE-SUP-B BASIC SUPPORT FOR IDENTITY SERVICES E

5. Change quantities of existing Base, Plus and Apex licenses to 0

E2F-SEC-ISE > **Cisco Identity Services Engine Plus & Apex**

Cisco Identity Services Engine Plus & Apex

Cisco Identity Services Engine Plus & Apex

Each	SKU
<input type="text" value="0"/>	E2SF-I-ISE-PLUS-10
<input type="text" value="300"/>	E2SF-I-ISE-APEX-10

6. Enter desired quantities against the Essentials, Advantage or Premier licenses

Configuration Summary	E2F-SEC-ISE > Cisco Identity Services Engine 3.0																					
Cisco Identity Services Engine Plus & Apex Cisco Identity Services Engine Base & Device Admin Support Options <table border="1"> <thead> <tr> <th>SKU</th> <th>Qty</th> <th>List Price</th> </tr> </thead> <tbody> <tr> <td>SVS-EA2-CISE-SUP-B</td> <td>1</td> <td>\$0.00</td> </tr> <tr> <td></td> <td><i>Event</i></td> <td><i>Per Event/Month</i></td> </tr> </tbody> </table> Cisco Identity Services Engine 3.0 Cisco Identity Services Engine Device Admin 3.0	SKU	Qty	List Price	SVS-EA2-CISE-SUP-B	1	\$0.00		<i>Event</i>	<i>Per Event/Month</i>	Cisco Identity Services Engine 3.0 Cisco Identity Services Engine 3.0 <table border="1"> <thead> <tr> <th>License</th> <th>SKU</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="Qty"/></td> <td>E2SF-I-ISE-ESSM-10 SA</td> <td>Cisco Security EA 2.0 ISE Essentials Subscription 10pk</td> </tr> <tr> <td><input type="text" value="100"/></td> <td>E2SF-I-ISE-ADVM-10 SA</td> <td>Cisco Security EA 2.0 ISE Advantage Subscription 10pk</td> </tr> <tr> <td><input type="text" value="Qty"/></td> <td>E2SF-I-ISE-PRMM-10 SA</td> <td>Cisco Security EA 2.0 ISE Premier Subscription 10pk</td> </tr> </tbody> </table>	License	SKU	Description	<input type="text" value="Qty"/>	E2SF-I-ISE-ESSM-10 SA	Cisco Security EA 2.0 ISE Essentials Subscription 10pk	<input type="text" value="100"/>	E2SF-I-ISE-ADVM-10 SA	Cisco Security EA 2.0 ISE Advantage Subscription 10pk	<input type="text" value="Qty"/>	E2SF-I-ISE-PRMM-10 SA	Cisco Security EA 2.0 ISE Premier Subscription 10pk
SKU	Qty	List Price																				
SVS-EA2-CISE-SUP-B	1	\$0.00																				
	<i>Event</i>	<i>Per Event/Month</i>																				
License	SKU	Description																				
<input type="text" value="Qty"/>	E2SF-I-ISE-ESSM-10 SA	Cisco Security EA 2.0 ISE Essentials Subscription 10pk																				
<input type="text" value="100"/>	E2SF-I-ISE-ADVM-10 SA	Cisco Security EA 2.0 ISE Advantage Subscription 10pk																				
<input type="text" value="Qty"/>	E2SF-I-ISE-PRMM-10 SA	Cisco Security EA 2.0 ISE Premier Subscription 10pk																				

7. Complete rest of the Quoting process
8. Once the order is placed and changes begin, customer will have the new ISE 3.x licenses in their Smart Account

Alternatively 2.x Enterprise Agreement (EA) customers can use a manual process to migrate their licenses by raising a case with Cisco TAC. This process does **not** allow customers to receive the benefits (example - Additional license generation, True Forwards etc) from the EA agreement for their 3.x licenses.

In this manual migration process, following formulae will be used for determining the quantities and end date for the 3.x Subscription licenses:

- A. Premier license quantities = Same as Apex license quantities
- B. Advantage license quantities = Plus minus Apex license quantities
- C. Essentials license quantities = Base minus Plus minus Apex license quantities. Please note that if the Base licenses are outside of the EA Subscription, then they will have to use the Migration Offer described in the above section
- D. End date of all 3.x licenses = EA end date

All existing 2.x licenses from EA customer’s Smart Account will be removed upon completion of the manual license migration process.

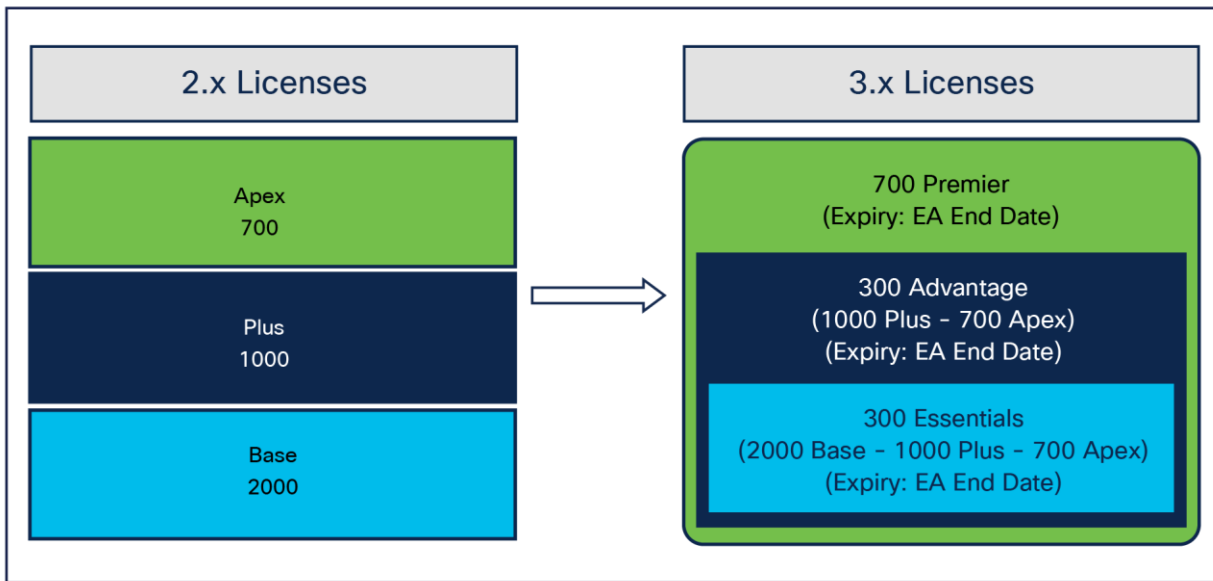


Figure 8.
Example: EA Conversion of 2.x licenses to 3.x subscription licenses through alternate manual process

7.1.3. Renew existing ISE Base, Plus, and/or Apex licenses

As per [Cisco EOL policy](#), the Base, Plus, and Apex licenses have reached end of life and will not be renewed. Customer needs to upgrade to Cisco ISE 3.x version and will be required to go through the migration process as specified above.

7.1.4. Roll back from 3.x Subscription licenses to 2.x licenses

Customers using the new Migration Offer specified above may retain their 2.x licenses until 22-Sep-2024. This approach provides ample time to upgrade the deployments to 3.x versions. Please note that the last date of Support for ISE 2.x version is 22-Sep-2024. For more information on this offer and specific terms, please refer to the [ISE License Migration Offer - FY24](#) (requires Cisco CCO login credentials)

EA customers may also be eligible to retain their 2.x licenses until 22-Sep-2024 if they use the 'EA Change Subscription' process. Please raise a Cisco TAC case with such a request which will be reviewed by Cisco ISE BU team.

7.2 Migrate to VM Common licenses

Each VM license—Small, Medium, or Large—is converted to a VM Common license. If you currently own 50 VM Small licenses, 30 VM Medium licenses, and 20 VM Large licenses, you will own 100 VM Common licenses after the migration process is complete.

Table 6. Migration to VM Common licenses

Upgrade from	Upgrade to	Ratio
R-ISE-VML-K9=	R-ISE-VMC-K9=	1:1
R-ISE-VMM-K9=	R-ISE-VMC-K9=	1:1
R-ISE-VMS-K9=	R-ISE-VMC-K9=	1:1

Customers can continue to use classic VM Small, Medium, and Large licenses as well as the VM Common license for ISE 2.4, 2.6, 2.7, and 3.0. However, note that the classic PAK VM licenses need to be converted to Smart Licenses in ISE 3.0. For a seamless customer experience, we have replaced all classic VM licenses (Small, Medium, and Large) in your Smart Account with new VM Common licenses, which cover the use of any Large, Medium, or Small VM Licenses. If you already had VM Small, Medium, and Large licenses in your Smart Account, no further action will be required for upgrade. However, if you do not have a Smart Account, please create a Smart Account by navigating to [Cisco Software Central](#), and then open a case with the Cisco Global License Operations Team to have your old or classic VM licenses converted to the new VM Common licenses in Smart Account.

Table 7. Virtual machine license use cases

License on release		Pre-2.4 release	Releases 2.4, 2.6, 2.7, and 3.0	Release 3.1 and later
VM license	New (VM Common: R-ISE-VMC-K9=)	Not supported	Licensed with Smart Licensing enforcement	
	Classic (VM Large: R-ISE-VML-K9=) (VM Medium: R-ISE-VMM-K9=) (VM Small: R-ISE-VMS-K9=)	Licensed without enforcement	Licensed with PAK and Smart Licensing enforcement	License migration to Common is not required if already using Smart Licensing. If not, please raise a case with the Global License Operations Team through Support Case Manager.
	Old (R-ISE-10VM-K9=) (R-ISE-5VM-K9=) (R-ISE-VM-K9=) (R-ISE-GST-BUN-K9=) (ISE-VM-M-K9=)	Licensed without enforcement	License migration to Classic or Common is required by raising a case with the Global License Operations Team. Please include all details from the original VM appliance purchase. Note: 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.	License migration to Common is required by raising a case with the Global License Operations Team. Please include all details from the original VM appliance purchase. Note: 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.

If you upgrade to ISE 2.4 prior to raising a case with the licensing team, the deployment displays the warning “Fewer VM Licenses installed than VM Resources/VM Nodes deployed.” While on ISE 2.4, this is only a warning message and does not disrupt any user’s ISE experience.

Customers who are on ISE 2.x and ISE 3.0 can continue to use the classic VM licenses until the [end-of-life](#) date of the licenses.

VM licenses use the license hierarchy, meaning that usage for a tier can be covered by any available licenses in a higher tier at a 1:1 ratio.

VM Common (Smart only) > VM Large > VM Medium > VM Small.

7.2.1 Downgrade from the VM Common license to the classic VM licenses

A downgrade is not recommended. You can use the VM Common license in any Cisco ISE release with Smart Licensing enforcement. Once you have the VM Common license (which works as the VM Large license does), you can use it even if you roll back to a Cisco ISE Release 3.0 or earlier (Cisco ISE Release 2.4 and later) that has Smart Licensing enabled. The VM Common license covers VM Small, VM Medium, and VM Large licenses.

If you purchased VM Common but are still in an ISE release earlier than 2.4, you will not be able to use the VM Common license.

7.2.2. Support associated with the classic VM licenses

When you migrate your PAK classic VM licenses to the VM Common license, you continue to receive support based on the support contract purchased with the classic VM license product ID (PID). The support can be renewed until the classic VM license PID is EOL and reaches the last date of service renewal per the [End-of-life notices](#). There is no support migration required. Therefore, for seamless support in such cases, customers should open a case with [Cisco Customer Service](#) and request the End-of-Life PID to be replaced with the desired PID in order to renew and receive support.

If you need to renew support, please follow the steps in the next section.

7.2.3 How to renew expired support on the old VM PID

Customers who are using PAK classic VM licenses can renew support for their VM licenses until the classic VM license PID reaches [End of Life](#) and last date of service renewal per the [End-of-Life](#) bulletin. However, customers who purchased old or classic VM licenses but are now using VM Common licenses should follow the steps below to request a PID swap in order to renew support.

1. Log in to <https://customerservice.cloudapps.cisco.com/>
2. Search for RMA Issues and click Open a case.
3. Fill in the Case title field with a relevant title (Example: PID Swap for Customer XXX).
4. Select Product ID Upgrade or Change as the Type of Request.
5. Select the appropriate Business Justification.
6. Download the Excel template, fill in all the required sections, and upload or update the attributes in the UI itself.

Old product ID	Old instance number	New product ID	Contract number
Ex: R-ISE-VM-K9	Ex: 1310418043	R-ISE-VMC-K9=	204831740

7. Click Next and create the case.

This PID swap request is processed by the Customer Service team, which shares the newly created instance number with the customer. Subsequently, the customer can continue to renew support on the new VM Common PID.

7.3 Migration of Device Admin licenses

Cisco ISE Release 2.4 and earlier also supports a classic Device Admin license, which is no longer available for purchase. The classic Device Admin license was a cluster license that allowed TACACS services on all the PSNs in a deployment. Releases 2.6 and later require the Node license.

Classic Device Admin licenses are grandfathered. If you are migrating from a 2.x release to a 3.x release, your Device Admin license must be migrated to a Smart Account.

The classic Device Admin license entitled an entire deployment of ISE to TACACS+ feature usage. This meant that up to all 50 ISE PSNs could be enabled with TACACS+ capabilities. This license works up to and including ISE Release 2.4.

At the time of the release of 2.4, a new Device Admin license was introduced that enables TACACS+ feature usage on a per-node basis. This new license is required for ISE Release 2.6 and later.

Customers with the classic Device Admin license who are upgrading to Release 2.4 or later are entitled to upgrade and receive the number of new Device Admin licenses equivalent to the number of PSNs in their deployment.

Table 8. Device Admin license use cases

License on release		Pre-2.4 release	Release 2.4 and later
Device Admin license	New	Not applicable	Is identified and enables consumption of 1 ISE TACACS+ Policy Service Node
	Classic	Is identified and consumed as uncounted (unlimited number of ISE TACACS+ appliances within the deployment)	Is identified and enables consumption of up to 50 ISE TACACS+ Policy Service Nodes

Note: Classic Device Admin and Node licenses are perpetual.

8. Cisco Identity Services Engine use cases

8.1. Guest and secure wireless access

8.1.1. Why provide Guest access?

Many organizations provide free internet access to guests visiting their organization for a short period. These guests include vendors, retail customers, short-term vendors or contractors, and so on. Cisco ISE provides the ability to create accounts for these visitors and authenticate them for audit purposes. There are three ways in which Cisco ISE can provide Guest access: via a hotspot (immediate noncredentialed access), self-registration, or sponsored Guest access. Cisco 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, and so on to match the look and feel of the customer’s brand.

8.1.2. How does Guest access work?

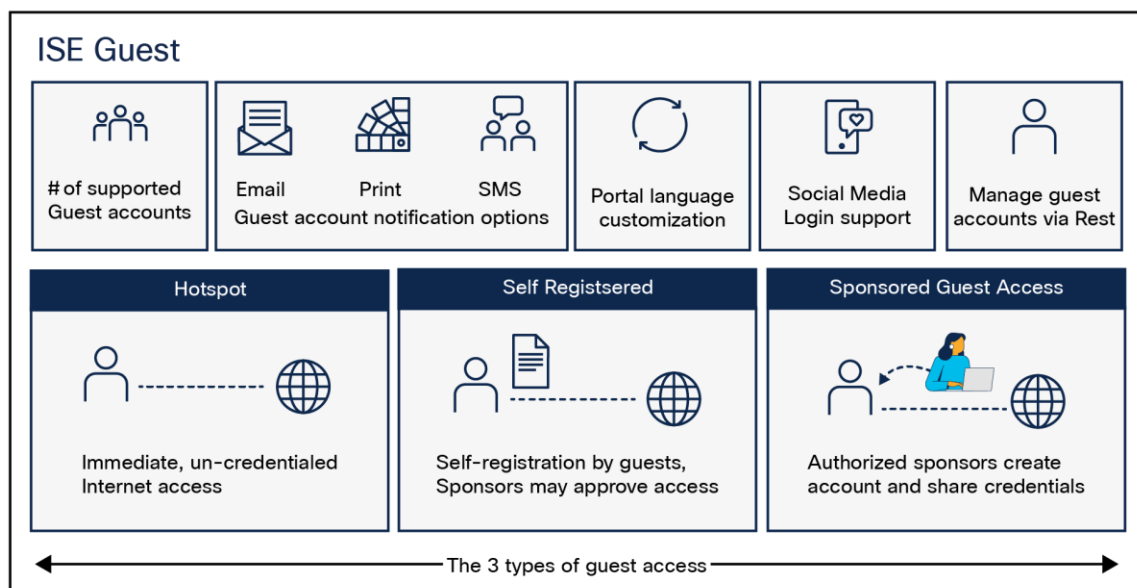


Figure 9. Cisco ISE Guest use case

Cisco ISE creates local accounts for guests. These accounts can be created either by an employee hosting the guest (the sponsor) using a built-in portal or by the guests themselves by providing some basic information. The guest can receive credentials via email or SMS and use them to authenticate themselves to the network and thereby get network access. The administrator can define what level of access to provide to such users.

Required license: ISE Essentials

8.1.3. Why provide secure wireless access?

Most organizations start by securing their wireless network. Securing the wireless network is the most basic need for every organization. Using Cisco 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 devices to connect to the network and then later enforcing different security policies. Authentication and authorization are core functionalities of Cisco ISE. Every Cisco ISE session begins with authentication, whether to a user or to a device. Authentication can be active or passive (not including 802.1X sessions): An active authentication is done using 802.1X when Cisco ISE authenticates the user against an identity source, while in passive authentication (used in Easy Connect) Cisco ISE learns about the user after the user authenticates against an identity source such as Microsoft’s Active Directory (AD) and the AD notifies ISE.

8.1.4. How does secure wireless access work?

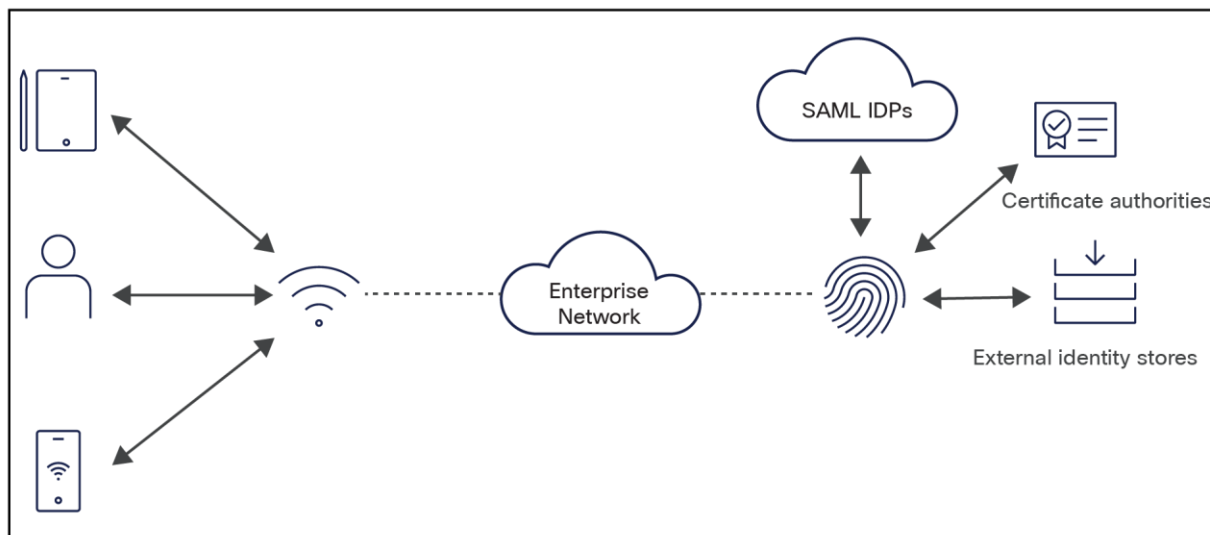


Figure 10.
Cisco ISE secure wireless use case

After successful authentication, based on the group’s information, Cisco ISE provides the right access to the wireless connection, whether the connection is a passive identity session (Easy Connect), MAC Address Bypass (MAB), or 802.1X. This can be achieved by assigning the user to a VLAN, discretionary access control list (DACL), or access control list (ACL) or to a security group tag (SGT) or security group access control list (SGACL).

Required license: ISE Essentials (SGT or SGACL will require ISE Advantage).

8.2. Asset visibility

8.2.1. Why asset visibility?

Understanding the device type is often 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 the 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 into most of your network, especially your traditional devices (printers, mobile phones, etc.), advanced asset visibility will provide you with visibility into more vertical-specific and IoT-types of devices.

8.2.2. How does Basic Visibility (Cisco ISE Profiling Visibility) work?

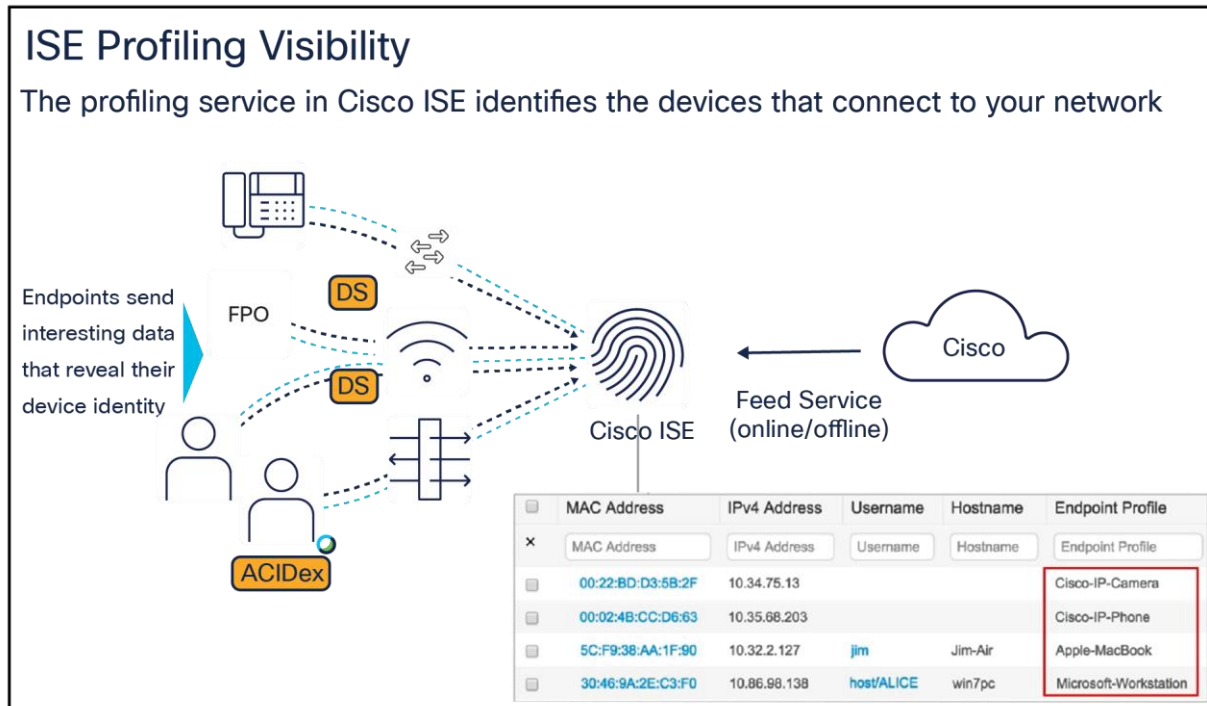


Figure 11.
Cisco ISE Basic Visibility use case

Basic asset visibility in Cisco 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.

It uses artificial intelligence and machine learning to intuitively group endpoints that have common attributes and helps IT administrators by providing suggestions for the right endpoint profiling labels. Multifactor classification classifies endpoints using label categories for flexible profiling.

Based on an asset’s profile, the next step in 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 helps ensure that, based on the visibility learned for an endpoint, it will be given only the network permissions for its profile. Printers will be able to receive access only to printing servers or anyone needing printing services, and mobile personal devices will be able to receive access only to internet services and low-risk internal systems.

Required license: ISE Advantage

8.3. Compliance (posture)

8.3.1. Why provide 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 would have been simple to remediate but were overlooked. Compliance Visibility allows organizations to view how user endpoints comply with corporate policy through the use of posture and/or integration with mobile device management (MDM) and enterprise mobility management (EMM) systems (supported MDM/EMM systems can be found in [Cisco ISE Network Component Compatibility](#)). Using either Cisco 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.

8.3.2. How does Compliance Visibility work?

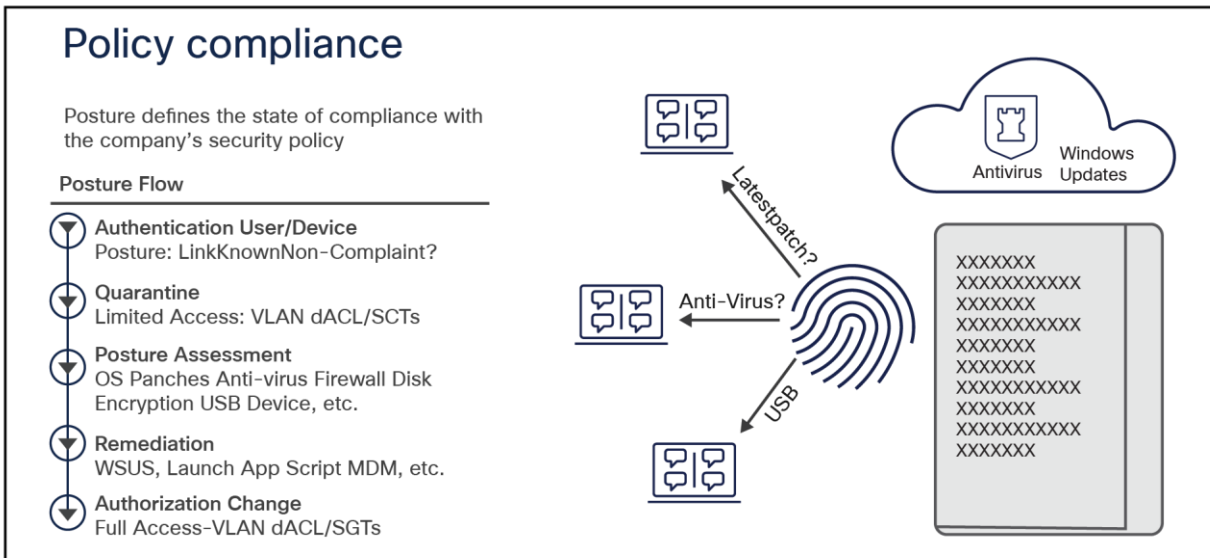


Figure 12.
Cisco ISE Compliance Visibility use case

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.

Having good visibility into what endpoints comply with the corporate software policy is usually not enough. A customer might want to enable differentiated access to endpoints based on their compliance level. Compliance enforcement allows the customer to take an overall compliance status, derived either through Cisco ISE's own Posture engine or through said MDM/EMM integrations, and using it in an access policy. Combined with other attributes (such as identity), this powerful capability helps lower the organizational risks and shrink the overall threat surface created by noncompliant, 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 only to remediation systems, help desk systems, and/or low-risk services by endpoints found noncompliant. Using either Cisco ISE's Posture engine or an MDM, an organization can evaluate how many endpoints are compliant and ensure that noncompliant endpoints with outdated and/or unsupported software cannot access critical resources.

Required license: ISE Premier (with Cisco AnyConnect Apex if using AnyConnect or AnyConnect Stealth).

8.4. Secure Wired Access

8.4.1. Why provide Secure Wired Access?

Securing the wired network is essential to prevent unauthorized users from connecting their devices to the network. Using Cisco ISE, network administrators can provide secure wired network access by authenticating and authorizing users and devices. Authentication can be active or passive. An active authentication is done using 802.1X when Cisco ISE authenticates the user against an identity source. Passive authentication involves Cisco ISE learning the user's identity via Active Directory 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 a dynamic VLAN, a downloadable ACL, or other segmentation methods.

8.4.2. How does Secure Wired Access work?

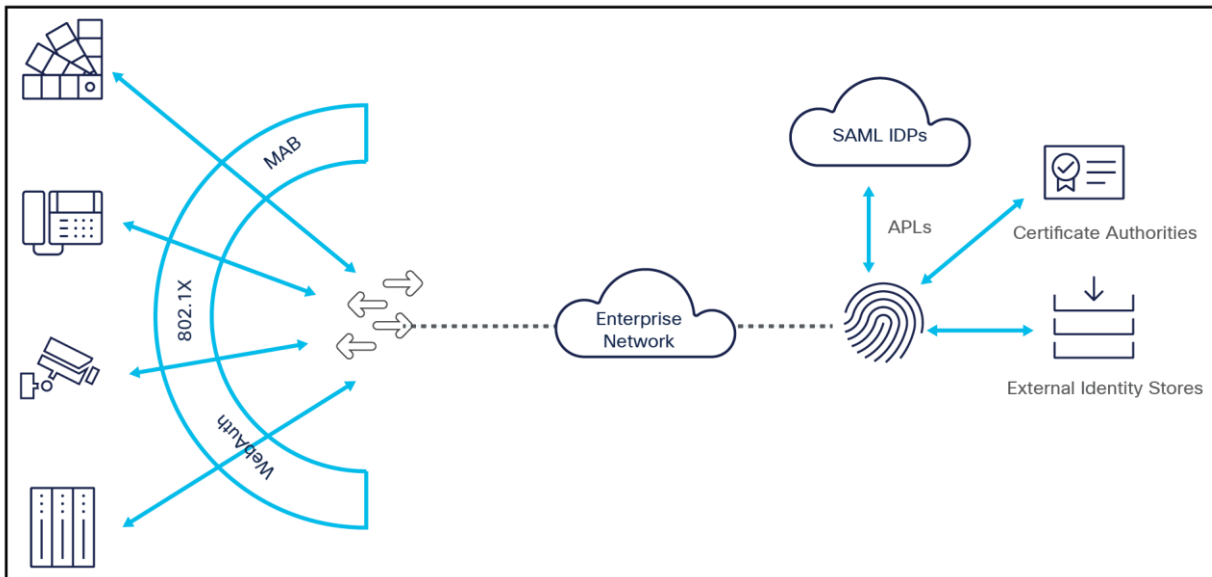


Figure 13.
Cisco ISE Secure Wired Access use case

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

Required license: ISE Essentials

8.5. Bring your own device (BYOD)

8.5.1. Why support BYOD?

Many organizations have instituted a policy that allows 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 a 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, Cisco ISE provides a very streamlined method to automate the entire BYOD onboarding process, from device registration and supplicant provisioning to certificate installation. This can be done on devices across various OS platforms such as iOS, Android, Windows, macOS, and ChromeOS. The Cisco ISE My Devices Portal, which is completely customizable, allows end users to onboard and manage various devices.

8.5.2. How does BYOD work?

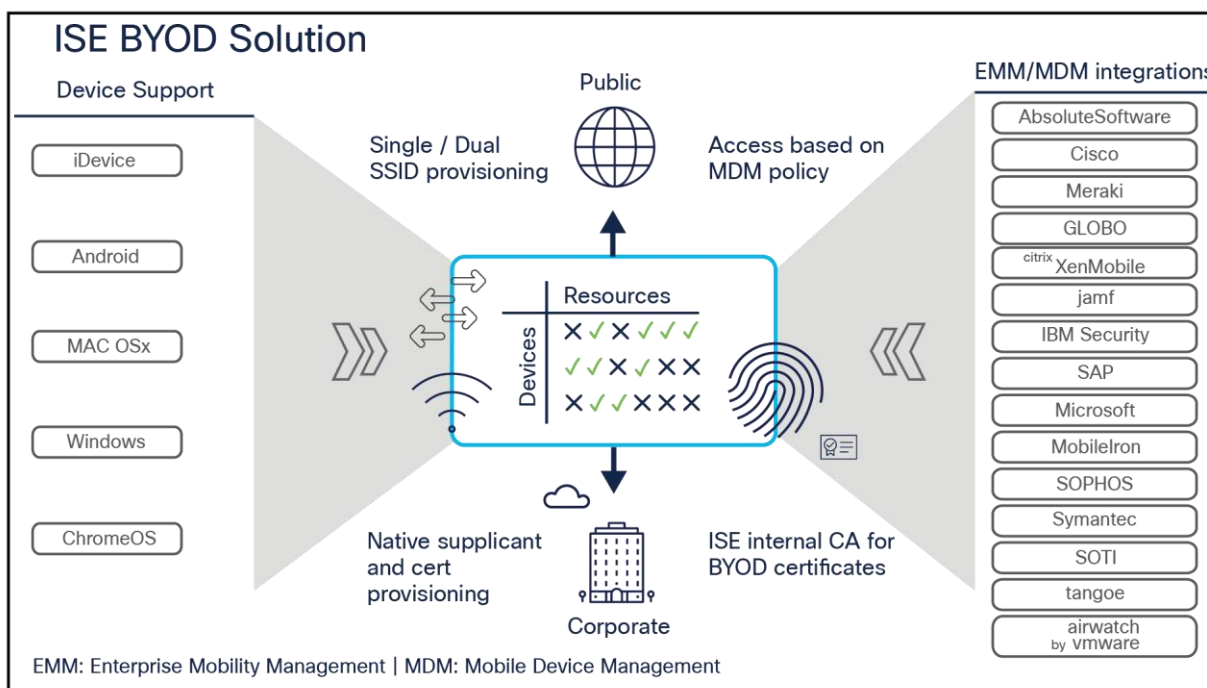


Figure 14.
Cisco ISE BYOD use case

Cisco 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. Cisco 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 and block it from the network. BYOD onboarding can be accomplished either through a single-SSID or dual-SSID approach. In the single-SSID approach, the same SSID is used to onboard and connect the end user's device, while in the dual-SSID approach, an open SSID is used to onboard 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.

For a list of enterprise and mobility management partners that integrate with Cisco ISE, see the [Cisco Secure Technical Alliance](#) Partners page and filter by Market Segment: EMM/MDM.

Required license: ISE Advantage

8.6. Rapid Threat Containment (RTC)

8.6.1. Why Rapid 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.

8.6.2. How does RTC work?

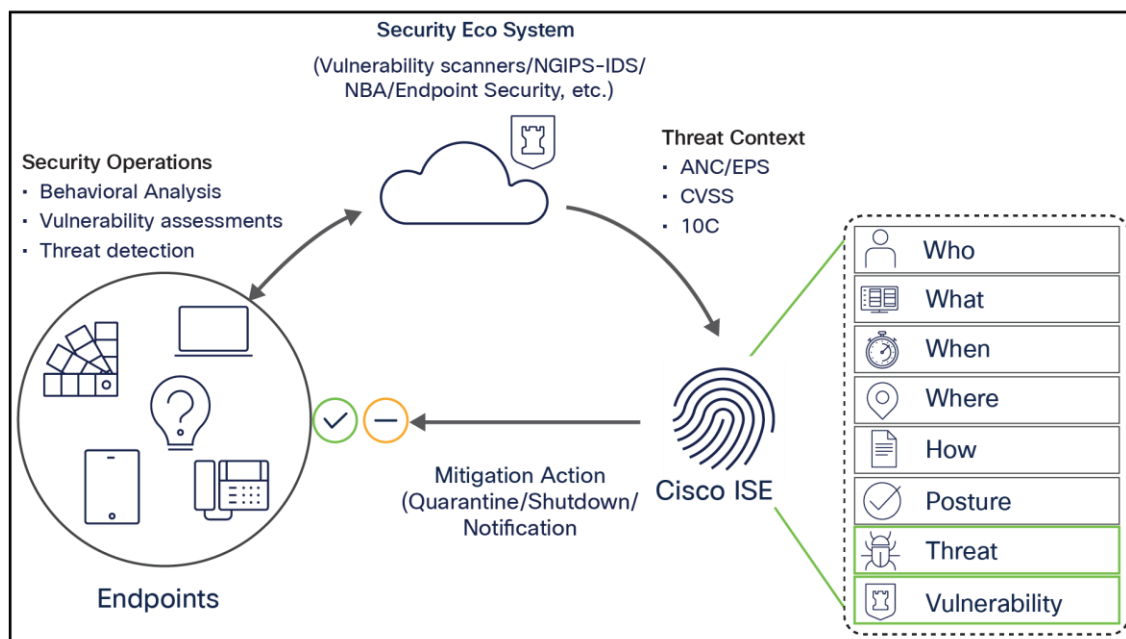


Figure 15.
Cisco ISE RTC use case

Upon detecting a flagrant threat on an endpoint, a pxGrid ecosystem 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 can be made based on their security score.

Cisco ISE integrates with more than 75 ecosystem partners over pxGrid to implement several use cases. Technical details about Cisco ISE integrations can be found in the [ISE Security Ecosystem Integration Guides](#).

For a list of enterprise and mobility management partners that integrate with Cisco ISE, see the [Cisco Secure Technical Alliance Partners](#) page and filter by Market Segment: EMM/MDM.

Required license: ISE Advantage

8.7. Segmentation

8.7.1. Why segmentation?

Network segmentation is a proven concept 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 concept in IETF, available within Open Daylight, and supported on third-party and Cisco platforms. Cisco ISE is the segmentation controller, which simplifies the management of switch, router, wireless, and firewall rules. Group-Based Policy/TrustSec segmentation provides better security at a 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.

8.7.2. How does segmentation work?

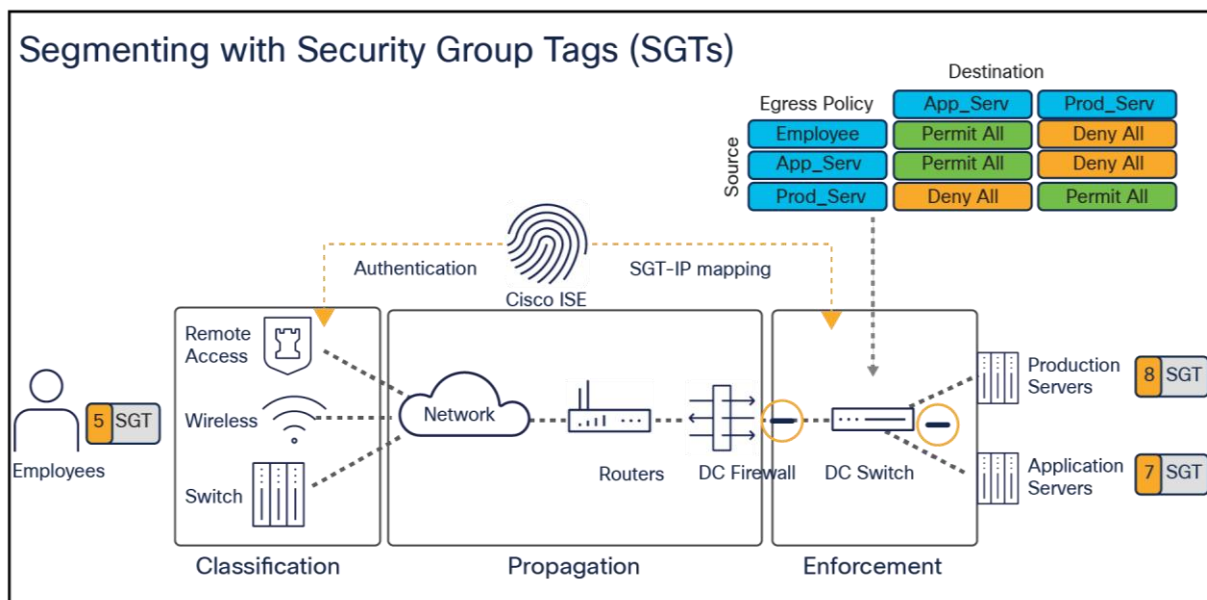


Figure 16.
Cisco ISE segmentation use case

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

8.7.3. Software-Defined Access

Segmentation is a key element of Cisco Software-Defined Access (SDA). Together, the Cisco DNA Center controller and Cisco ISE automate network segmentation and group-based policy. Identity-based policy and Segmentation decouples security policy definition from VLAN and IP addresses. The [SD-Access Design and Deployment](#) guides detail the configuration and deployment of Group-Based Policy.

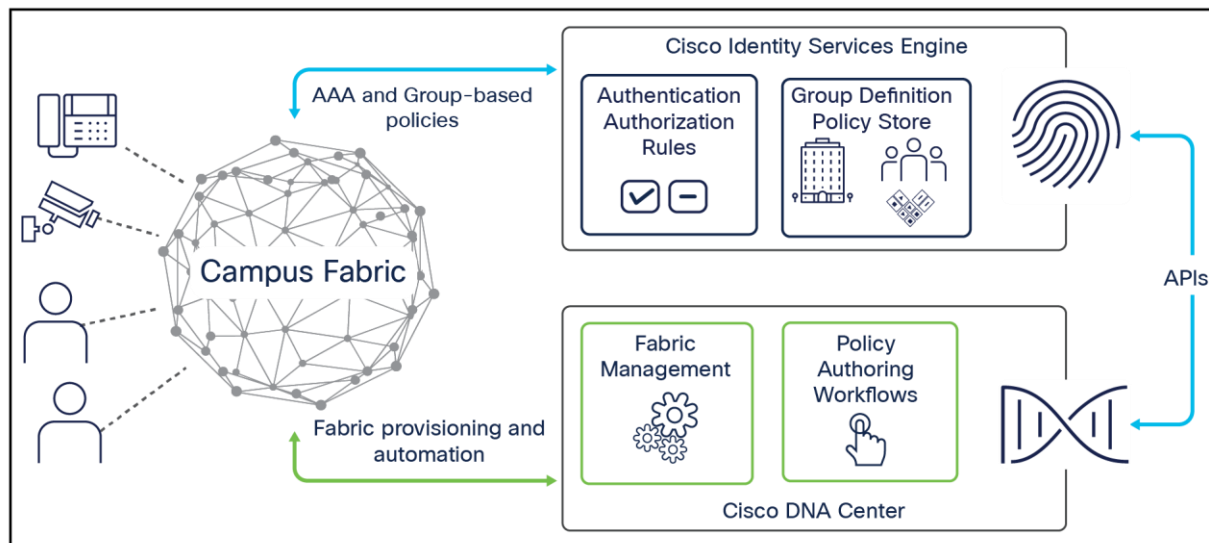


Figure 17.
Cisco ISE SD-Access integration use case

To extend segmentation across the enterprise network, Cisco ISE interfaces with the Cisco Application Centric Infrastructure (ACI) Controller, which is also called Application Policy Infrastructure Controller - Data Center (APIC- DC), to learn endpoint group (EPG) names and share software group (SG) names and corresponding EPG values, SGT values, and the Virtual Routing and Forwarding (VRF) name. This allows Cisco ISE to create and populate SG-to-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 Configuration 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. Cisco ISE acts as the policy controller for routers, switches, wireless, and security products. Details about product TrustSec capabilities are provided in the Cisco Group Based Policy [Platform and Capability Matrix](#). The Cisco TrustSec [Quick Start Configuration Guide](#) illustrates a typical TrustSec network deployment with step-by-step configuration of a sample environment. For more options, please refer to the [Design Guides](#).

Required license: ISE Advantage

Note: The following licenses enable segmentation via SD-Access: Advantage or Premier on Cisco ISE, and Cisco DNA Premier/Cisco DNA Advantage. For more information, see the [SD-Access Ordering Guide](#).

8.8. Security ecosystem integrations

8.8.1. Why security ecosystem integrations?

Cisco ISE builds contextual data about endpoints in terms of their device type, location, time of access, posture, user(s) associated to that asset, and much more. Endpoints can be tagged with 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 ecosystem partners to enrich their services. For example, in the Cisco Next-Generation Firewalls (NGFW), policies can be written based on the identity context, such as device type, location, user groups, and others, received from Cisco ISE. Inversely, specific context from third-party systems can be fed into the Cisco ISE to enrich its sensing and profiling capabilities, and for threat containment. The context exchange between the platforms can be done via Cisco pxGrid (including pxGrid Cloud and pxGrid Direct) or REST APIs.

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

8.8.2. How do security ecosystem integrations work?

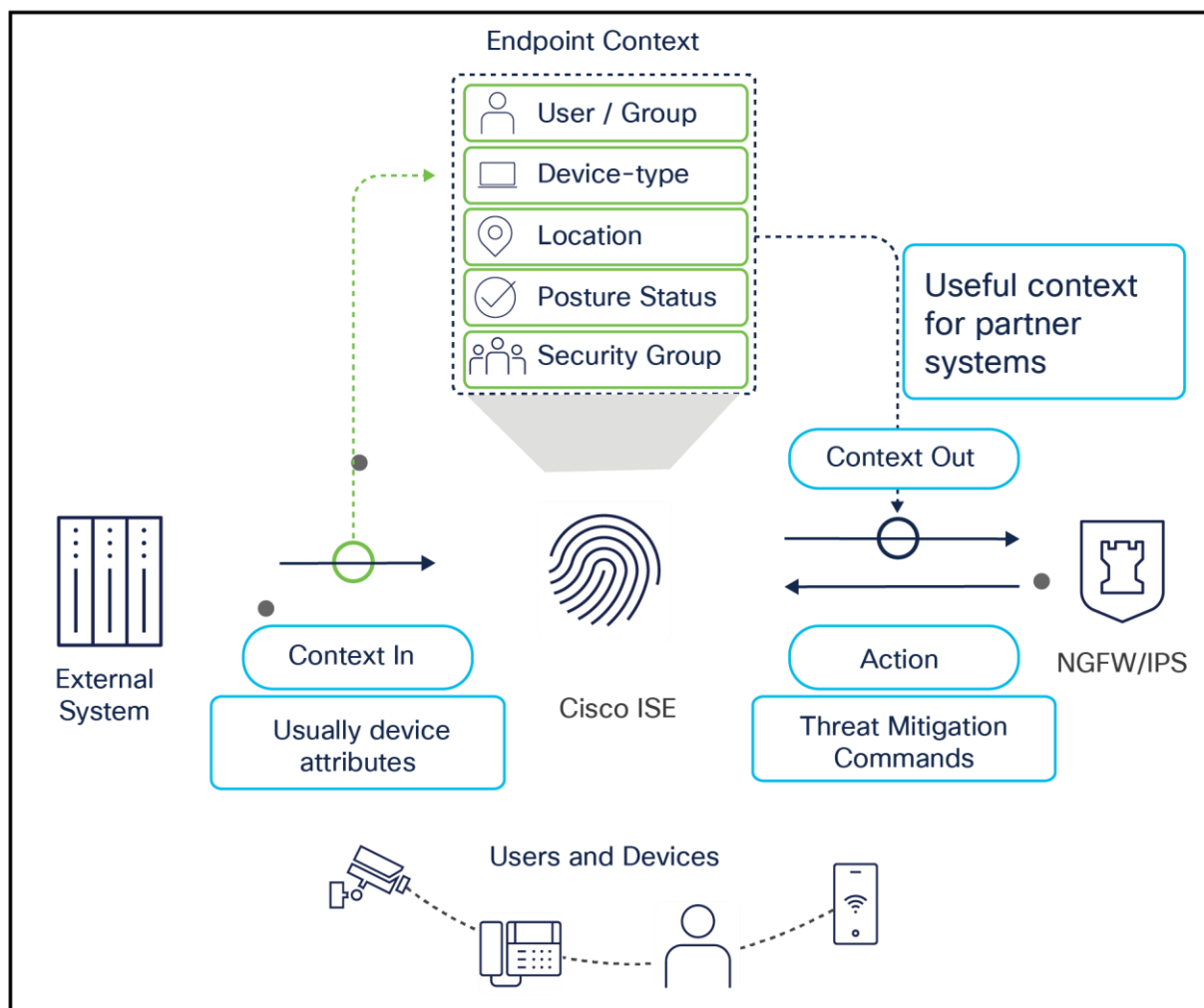


Figure 18.
Cisco ISE security ecosystem integration

Cisco ISE integrates with more than 75 ecosystem partners over pxGrid to implement technology partners. The technical details about integrations can be found in the [ISE Security Ecosystem Integration Guides](#).

A complete list of ecosystem partners can be found at the [Cisco Secure Technical Alliance Partners page](#).

Required license: ISE Advantage

8.9. Device Administration (TACACS+)

8.9.1. 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 a limited number of devices, keeping track of admin users, privileges, or changes in configuration can be easy. However, as the network grows to tens, hundreds, or even thousands of devices, it becomes exceedingly complex to manage devices without automation and a smooth workflow. Cisco ISE provides the capability to automate device administration tasks with clean workflows and monitoring capabilities with TACACS+ within a controlled space in the UI.

8.9.2. How does Device Administration work?

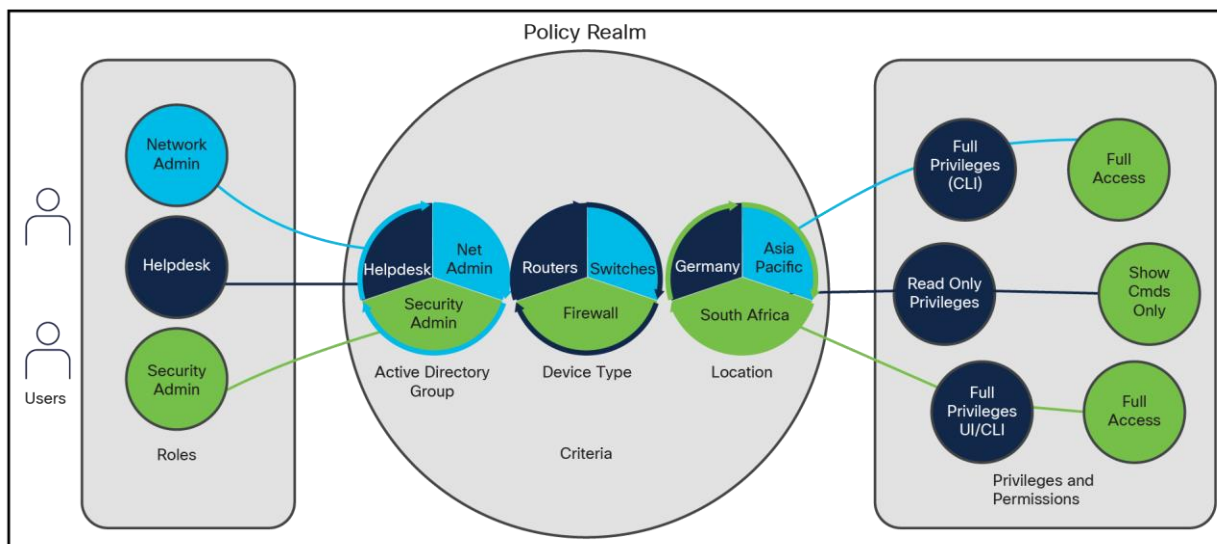


Figure 19.

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 Cisco ISE, and Cisco ISE asks for their credentials. Credentials are verified against an identity source.

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

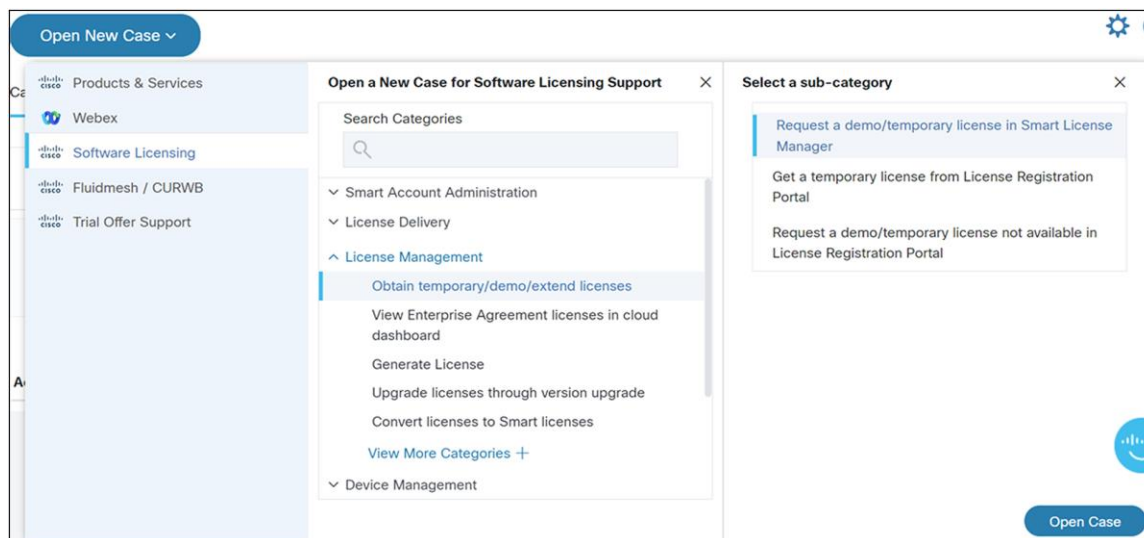
8.9.3. How to license Device Administration

- License that enables Device Administration: Device Admin license
- License consumption: Device Admin licenses are consumed per Policy Service Node (PSN). You must have a Device Admin license for each of the PSNs 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 an Essentials license.

9. How to raise TAC case for Licensing requests

Customer should follow the steps below to raise a TAC case for Software licensing support.

1. Login to [Support Case Manager](#)
2. Click "Open new case"
3. Select "Software Licensing"
4. Select the appropriate category under "License Management"
5. Select the appropriate "Sub-category" and click "Open Case"



6. Select product "ISE" under Security tab
7. Fill in the details (Title, problem description, Telephone, Email) and click "submit case"

This TAC case is handled by Global Licensing operations Team and fulfilled with ISE BU approval.

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>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)