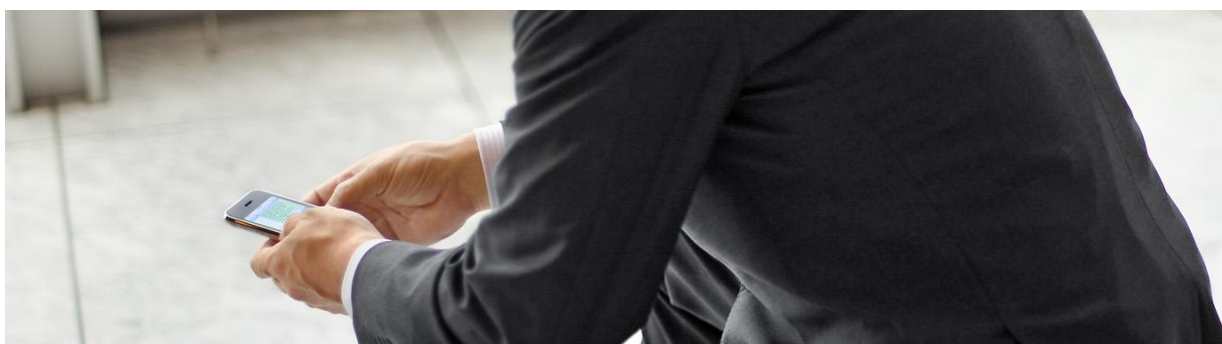


Cisco Identity Services Engine Software 1.2



- Q.** What new features and capabilities are delivered in Cisco® Identity Services Engine Software Release 1.2?
- A.** Cisco Identity Services Engine Software Release 1.2 delivers important enhancements to the Identity Services Engine in several areas, including scalability and usability. New ISE Release 1.2 features include:
- **MDM integration** ensures all mobile devices comply with security policy.
 - **Solution ecosystem** enables platforms such as MDM and Threat Management to address more use-cases and undertake their functions more effectively.
 - **Device feed service** supports the latest devices, making it hassle-free for users and IT.
 - **Doubling of scale and performance** allows IT to handle the continuous influx of new devices.
 - **Bootstrap wizards** provide IT deployment automation and simplification when testing the ISE in a proof-of-concept network.
- Q.** What is being released with ISE Release 1.2?
- A.** Two new hardware platforms called the Cisco Secure Network Servers. These new servers are based on the powerful Cisco UCS® C220 Rack Server platform and are configured to support the Cisco Identity Services Engine (ISE), Network Admission Control (NAC), and Secure Access Control System (ACS) security applications. The multiuse Cisco Secure Network Servers offer many improvements over current ISE, ACS, and NAC appliances and are the platform recommended to deploy newer versions of these applications. During ordering, customers can specify which security application they would like to have installed. See the Product Details section for more information.
- Q.** If I am an existing Identity Services Engine customer, will I need to buy a new Cisco Secure Network Server in order to upgrade to ISE Release 1.2?
- A.** There is no need to buy new hardware; the current IBM servers will support ISE Release 1.2 through manual software upgrade. However, the new Cisco Secure Network Servers can only run ISE Release 1.2 and subsequent versions.
- Q.** Can I mix hardware in my Identity Services Engine deployment?
- A.** Yes. You can use different hardware in your environment, but all software versions need to be the same.

Q. What are the scalability enhancements?

A. The Identity Services Engine was previously able to scale to 100,000 concurrent connected endpoints. ISE Release 1.2 enables the Identity Services Engine to handle up to 250,000 concurrent connected endpoints. Additionally, the new Cisco Secure Network Servers increase endpoint support over the Cisco Identity Services Engine 3300 Series appliances. For example, the Cisco Secure Network Server 3415 supports 5000 endpoints compared to 3000 for the Cisco Identity Services Engine 3315, and the Secure Network Server 3495 supports 20,000 endpoints compared to 10,000 for the Cisco Identity Services Engine 3395.

Q. What are the usability enhancements?

A. ISE Release 1.2 delivers simplified product configuration capabilities. The bootstrap wizards aid in the configuration of the authentication, authorization, profiler, posture, compliance, and guest capabilities so it's easier and faster to deploy ISE services across an organization's networks.

Q. How does MDM integration add value to the solution?

A. ISE Release 1.2 delivers integration between Identity Services Engine and MDM platforms, which can ensure that all mobile devices are compliant with security policy before they are allowed to access the network. This feature enables posture compliance assessment and network access control of mobile endpoints attempting to access the network. The solution also performs ongoing posture checks to ensure that devices remain compliant and that the correct network access level is maintained. The specific posture attributes collected by MDM partner platforms for compliance and access policy enforcement in the Identity Services Engine are:

- Is the mobile device registered with MDM?
- Does the mobile device have disk encryption enabled?
- Does the device have PIN-Lock enabled?
- Has the device been jail-broken/rooted?

In terms of global compliance, posture compliance decisions may be made by the MDM platform instead of the Identity Services Engine. In this scenario, additional attributes such as blacklisted applications or presence of an enterprise data container may be checked. The MDM platform simply informs the Identity Services Engine if a device is in compliance, then the Identity Services Engine enforces the appropriate network access policy.

This integration brings great value to MDM customers as it automates the device registration process. As MDM solutions are network-blind, they can't detect a new device when it connects to the wireless network, so the administrator needs to send a notification to the users who wish to enroll their devices. With ISE integration, device enrollment is done automatically when users connect their device to the Wi-Fi network.

Q. What MDM platforms are supported with ISE Release 1.2?

A. Presently, the following seven MDM platforms are supported with ISE Release 1.2: AirWatch, Good Technology, Fiberlink, IBM, MobileIron, SAP/Afaria, and Citrix/Zenprise.

Q. What technology areas does the ISE ecosystem cover?

A. Currently, MDM and SIEM/TD (Security information and event management/threat defense). Cisco has also introduced a framework for multiplatform context sharing called Platform Exchange Grid (pxGrid). The Identity Services Engine is the first Cisco platform to adopt pxGrid for the purpose of growing the ISE ecosystem. We will continue to expand it based on use case areas (like MDM and SIEM/TD) in coming months and years.

- Q.** What is the value of the ISE SIEM/TD ecosystem?
- A.** ISE integration with leading SIEM/TD platforms brings together a networkwide view of security events supplemented with relevant identity and device context from the Identity Services Engine. This gives security analysts the context they need to quickly assess the significance of security events by being able to answer questions like “Who is this security event associated with and what level of access do they have on the network?” and “What type of device is it coming from?” - all within the SIEM/TD system. Providing ISE user and device context to SIEM/TD platforms also enables a new suite of security monitoring capabilities, such as mobility-aware analytics. SIEM/TD platforms may utilize ISE to take remediation actions in the Cisco network infrastructure. This suite of capabilities helps IT organizations increase the speed of threat detection and simplifies threat response.

- Q.** What is the new device feed service, and what are the benefits?
- A.** With ISE Release 1.2, Cisco is delivering a unique feed service that provides new and updated profiles for various IP-enabled devices when vendors release new devices. ISE customers will be able to recognize new devices, in addition to a multitude of other network-attached devices such as printers, video cameras, and specialized mobile computing devices.

Cisco works with various vendors, partners, and customers to profile the multitude of IP-enabled devices that are expected to be deployed in various customer environments and then create profiles for the devices. These profiles are made available through the device feed service. An ISE server that is configured to connect to the feed service establishes a secure connection with the cloud-based service. The various profiles on the feed service are automatically downloaded to the ISE server, providing ISE customers the ability to detect the IP-enabled devices that connect to their network. The feed service will be available with ISE Release 1.2 and is part of the Advanced license.

- Q.** Given the new capabilities introduced in ISE Release 1.2, is there any change to the Identity Services Engine product packaging and licensing?
- A.** The current Base, Advanced, and Wireless licenses remain the same. In order to benefit from the MDM integration or the profiler feed service, Advanced licenses will need to be purchased.
- Q.** Are there any enhancements to Identity Services Engine license management?
- A.** Yes. Beginning with ISE Release 1.2, customers will be able to register an ISE PAK for Primary and Secondary Administration nodes by entering the Unique Device Identifier (UDI) of both nodes. This allows the resulting Identity Services Engine license file to be installed on both nodes, which is a significant enhancement for failover and upgrade processes. Also, enhancements to the [Cisco License Administration Portal](#) allow the customer to re-host their existing Identity Services Engine licenses to another node or two nodes.
- Q.** What new languages are supported in ISE Release 1.2?
- A.** Czech, Dutch (Netherland Dialect), Hungarian, and Polish are now supported.
- Q.** What features of Cisco ISE are translated into localized languages?
- A.** Cisco ISE allows end-user-facing portal content to be localized in a supported language. This capability means that the Cisco ISE Guest, Sponsor, and MyDevices portals allow their displayed text strings to be translated into a supported language. These portals and the Client Provisioning portal are pretranslated into 15 languages in Release 1.2. The supported languages are also mapped to popular browser locale settings.
- Q.** Will there be any price increases associated with ISE Release 1.2?
- A.** No. Prices will not be increased for any Identity Services Engine product.

- Q.** Can I run ISE Release 1.2 on my existing Identity Services Engine hardware appliances?
- A.** Yes. ISE Release 1.2 will work with the Identity Services Engine 3315, 3355, and 3395 hardware appliances in their default configurations.

General Overview

- Q.** What is the Identity Services Engine?
- A.** The Identity Services Engine is a single policy control point for identity, access control, and device security across wired, wireless, and VPN networks. Through complete, automated features for BYOD and guest access, employees and guests can use the device of their choice while integrating with MDM solutions to ensure device security before allowing access to work resources. IT can assure identity and account for all network-attached devices, including printers, surveillance cameras, servers, and unique mobile computing devices used in retail, healthcare, and manufacturing. And resources are protected by strong access control that's already embedded in the Cisco network.
- Q.** What are the key features of the Identity Services Engine?
- A.** The core ISE features stem from the tight integration of identity services in a single RADIUS-based Cisco product. This includes:
- **Rigorous identity enforcement:** Extensive device profiling and asset visibility with automatic feed service
 - **Extensive policy enforcement:** Contextual identity access control on wired, wireless, and VPN networks
 - **Automated onboarding:** Supports IT, BYOD, and guest devices
 - **Solution ecosystem:** Technology partner platform integration ISE provides IT organizations a consistent method of making their IT platforms identity, device and policy aware. This awareness enables platforms such as MDM and Threat Management to address more use-cases and undertake their functions more effectively. Integration with ISE also enables partner platforms to reach into the Cisco network infrastructure to execute network actions on users and devices - such as quarantine and blocking access.
 - **Dependable anywhere access:** Consistent resource availability for workers
 - **Operational efficiencies:** ISE automation reduces IT and helpdesk burden and improves accuracy
 - **Embedded enforcement:** Device sensing and enforcement already present in Cisco networks reduces equipment costs
 - **Next-generation policy networking:** Ends the difficulties of VLAN, ACL, and firewall rule administration
- The Identity Services Engine starts with rigorous identity enforcement, with an industry-first, automatic device feed service to keep the device profiler current with the latest smartphones, tablets, mobile computing devices, printers, and video surveillance cameras, as well as specialized devices used in the retail and healthcare industries. The product identifies a device, the user ID, location and time of access, and type of media, then creates a contextual identity, applies the policy, and dynamically provisions the network so workers get dependable access to their resources from virtually anywhere.
- Q.** What role does the Identity Services Engine play in the Cisco SecureX solution?
- A.** As a core component of the SecureX framework, the Identity Services Engine provides a unified policy platform that ties organizational security policies to business components such as security and network infrastructure, user identity, resources, and IT operational processes. The Identity Services Engine allows customers to create and manage centralized policies, while Cisco TrustSec® delivers policies and enforcement through the network.

- Q.** What role does the Identity Services Engine play in the Cisco Unified Access™ solution?
- A.** The Identity Services Engine is the “One Policy” in the Unified Access solution, which also includes “One Management” and “One Network.” The Identity Services Engine provides central policy management across all Cisco wired, wireless, and remote networks. Cisco Unified Access is an intelligent network platform comprised of ISE policy management, Cisco Prime™ network management, Cisco Catalyst® switches, and Cisco wireless controllers, access points, and mobility services managers. This platform enables IT to intelligently connect people, processes, data, and things with greater intelligence, security, and efficiency than ever before.
- Q.** What customer challenges does the Identity Services Engine solve?
- A.** The Identity Services Engine solves four customer challenges:
- Secure access: Provides authenticated and authorized access to the network based on who is accessing the network, the types of devices being used, and the location and health status of each device.
 - BYOD automation: Provides easy onboarding of employee-owned devices while ensuring that the right level of security is in place.
 - Guest lifecycle management: Allows provisioning, notification, management, and reporting of guest user accounts.
 - Next-generation network control: Acts as the policy control point for next-generation TrustSec networking, which is secure access policy embedded in the network infrastructure to ensure consistent and efficient enforcement.
- Q.** What types of customers can benefit from deploying the Identity Services Engine?
- A.** All customers requiring identity and network access services across their wired, wireless, and VPN networks will benefit from deploying the Identity Services Engine.
- Q.** Are there customer references?
- A.** Yes. Cisco currently has thousands of ISE customers in industries such as financial services, manufacturing, healthcare, public sector, education, and more. There are written case studies and video on some of these customers [here](#).
- Q.** How does the identity Services Engine compare to other solutions in the industry?
- A.** While the Identity Services Engine offers so many capabilities in one integrated product that it may drive a new classification for secure access, the most relevant comparison is the Gartner Magic Quadrant for NAC, where it is named the market leader.
- Q.** Will the Identity Services Engine replace Cisco Secure Access Control Server (ACS) and Cisco Network Access Control (NAC)?
- A.** Not at this time. The Cisco Secure ACS and Cisco NAC product lines are viable products, and they will continue to be sold.
- Q.** Should existing Cisco NAC Appliance, Cisco NAC Profiler, or Cisco NAC Guest Server customers migrate to the Identity Services Engine platform?
- A.** Cisco NAC customers can migrate to the Identity Services Engine platform if they so desire. However, it is highly recommended that customers consult with their sales representatives and Cisco Certified Partners to determine the best course of action.

- Q.** Should existing Cisco Secure ACS customers migrate to the Identity Services Engine platform?
- A.** Existing Cisco Secure ACS customers using network access can easily migrate to the Cisco Identity Services Engine platform using migration part numbers and tools. However, existing Cisco Secure ACS customers using TACACS functions will not be able to migrate to the current version of ISE for network device identity management, which is often acceptable for customers who prefer to keep user and network identity on separate systems.
- Q.** Does the Identity Services Engine support older Cisco Secure ACS and Cisco NAC deployments?
- A.** ISE Release 1.2 does not interoperate with Cisco Secure ACS deployments. The Identity Services Engine can work in tandem with Cisco NAC Manager to provide the same profiling service as the NAC Profiler, which has reached end-of-sale status. Please speak to your local Security Sales Specialist to verify applicability in your environment.

Product Details

- Q.** What are the Identity Services Engine product components?
- A.** The Identity Services Engine has three components: appliances, software application, and software licenses. Appliances include physical and virtual options. The entire software application is installed on each appliance when it is shipped. To enable specific software functionality, you must order a separate software license. The Base license is perpetual, and the Advanced and Wireless licenses are term-based (1-, 3-, and 5-year terms). The Wireless Upgrade license adds the ability to support wired and VPN use cases to Wireless licenses. The Wireless Upgrade license enables one Wireless license to be equal to one Base and one Advanced license. The Wireless Upgrade license can be purchased in 1-, 3-, or 5-year terms. The number of Wireless Upgrade licenses ordered must be equal to the Wireless license quantity the customer has deployed. Tables 1 and 2 list the platforms and options available.

Table 1. Platforms and Options

Platforms	Options
Appliances	Cisco Identity Services Engine 3315 (small); 3000-endpoint target Cisco Identity Services Engine 3355 (medium); 6000-endpoint target Cisco Identity Services Engine 3395 (large); 10,000-endpoint target
Servers	Cisco Secure Network Server 3415 (small), 5000-endpoint target Cisco Secure Network Server 3495 (large), 20,000-endpoint target
Software or Virtual Machine	1, 5, or 10 virtual machines

Table 2. Software Packages and Options

Software Packages	Options
Base	Capabilities: Basic network access and guest access Network deployment support: Wired, wireless, and VPN License prerequisite: None Perpetual license Licenses are available for 100, 250, 500, 1000, 1500, 2500, 3500, 5000, 10,000, 25,000, 50,000, and 100,000 endpoints
Advanced	Capabilities: Profiler and feed service, posture, MDM integration, automated endpoint onboarding, and Security Group Access (SGA) Network deployment support: Wired, wireless, and VPN License prerequisite: Base license Term license: 1, 3- and 5-year terms Licenses are available for 100, 250, 500, 1000, 1500, 2500, 3500, 5000, 10,000, 25,000, 50,000, and 100,000 endpoints

Software Packages	Options
Wireless	Capabilities: Basic network access, guest access, profiler, posture, and SGA Network deployment support: Wireless License prerequisite: None Term license: 1, 3- and 5-year terms Licenses are available for 100, 250, 500, 1000, 1500, 2500, 3500, 5000, 10,000, 25,000, 50,000, and 100,000 endpoints
Wireless Upgrade	Capabilities: Basic network access, guest access, profiler, posture, and SGA Network deployment support: Wired, wireless, and VPN License prerequisite: Wireless license Term license: 1, 3- and 5-year terms Upgrade licenses are available for 100, 250, 500, 1000, 1500, 2500, 3500, 5000, 10,000, 25,000, 50,000, and 100,000 endpoints

Q. How does the Cisco Secure Network Server 3415 compare to the Cisco Identity Services Engine 3315 Appliance?

A. A high-level configuration comparison is shown in Table 3.

Table 3.

	Cisco Secure Network Server 3415 (Small) - New	Cisco Identity Services Engine 3315 (Small)
Processor	1 x Intel Xenon Quad-Core 2.4 GHz E5-2609	2 x QuadCore Intel Xeon CPU E5504 @ 2.00 GHz
Memory	16 GB	4 GB
Hard disk	1 x 600-GB 6-GB SAS 10K RPM	2 x 250-GB SATA HDD
RAID	No	No
CD/DVD-ROM drive	No	Yes
Ethernet NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs
Endpoints supported	5000	3000
Available for Sale	Yes	No. It has been removed from all price lists.

Q. Can I still order the Cisco ISE 3315 Appliance?

A. No. Because of material shortages, the Cisco ISE 3315 is no longer orderable. Please order the Cisco Secure Network Server 3415 (product ID SNS-3415-K9) instead.

Q. Can I still order the Cisco ISE 3355 Appliance?

A. No. Because of material shortages, the Cisco ISE 3355 is no longer orderable. Please order the Cisco Secure Network Server 3495 (product ID SNS-3495-K9) instead.

Q. How does the Cisco Secure Network Server 3495 compare to the Cisco Identity Services Engine 3395 Appliance?

A. A high-level configuration comparison is shown in Table 4.

Table 4.

	Cisco Secure Network Server 3495 (Large) - New	Cisco Identity Services Engine 3395 (Large) - New
Processor	2 x Intel Xenon Quad-Core 2.4 GHz E5-2609	2 x Intel Xenon Quad-Core 2.4 GHz E5-2609
Memory	32 GB	4 GB
Hard disk	2 x 600-GB 6-GB SAS 10K RPM	4 x 300-GB SFF SAS drives
RAID	Yes (RAID 0+1)	Yes (RAID 0+1)
CD/DVD-ROM drive	No	Yes
Ethernet NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs
Endpoints supported	20,000	10,000

- Q.** Why aren't Cisco Secure Network Servers referred to as "appliances"?
- A.** Appliances are generally specific-purpose devices. Servers are generally considered to be multipurpose devices. Because the new hardware platforms support multiple applications with the same configuration(s), labeling them as "servers" is more appropriate.
- Q.** What is the default Identity Services Engine software release for the different appliances and servers?
- A.** The default Identity Services Engine software release installed during manufacturing is as follows:
- Cisco Secure Network Servers (3415 and 3495): ISE Release 1.2
 - Cisco ISE Appliances (3315, 3355, 3395): ISE Release 1.1.1
 - Cisco ISE VM Appliances: ISE Release 1.2
- Q.** Can I select the version of ISE software that is installed on appliances and servers when ordering?
- A.** No. The most currently available version of ISE software is always installed.
- Q.** Can I upgrade the version of ISE software installed on the appliance and servers after deployment?
- A.** Yes. Software upgrade procedures are annotated in the User Guide.
- Q.** What ISE software versions are supported on ISE appliances and servers?
- A.** ISE 3300 Series appliances and VM appliances support all versions (ISE Release 1.0, 1.1, and 1.2); Cisco Secure Network Servers support ISE Release 1.1.4 and 1.2.
- Q.** Do the new Cisco Secure Network Servers offer any components as spares and FRUs?
- A.** Yes. Customers can order power supplies, hard disk drives, KVM cables, and rail kits as spares.
- Q.** With the release of the new Cisco Secure Network Servers, will end-of-sale (EOS) status for the Cisco Identity Services Engine 3300 Series be announced soon?
- A.** The end-of-sale announcement for the Cisco ISE 3300 Series was posted on June 25, 2013. Please refer to the announcement at http://www.cisco.com/en/US/prod/collateral/vpndev/ps5712/ps11640/eol_C51-728424.html. The ISE-3315-K9 and ISE-3355-K9 appliances are no longer orderable due to material shortages.
- Q.** When does the term begin for a Cisco Identity Services Engine license?
- A.** Consistent with Cisco policy, the Identity Services Engine license term starts 24 hours after dispatch. All Identity Services Engine licenses are electronically delivered and are typically dispatched within 48 hours after order processing.
- Q.** Can I order multiple licenses?
- A.** Yes. You can order multiple licenses to increase the number of endpoints supported. Identity Services Engine licenses are cumulative across the entire Identity Services Engine deployment and apply only to concurrent, active sessions. This is different from the Cisco NAC Appliance or NAC Profiler, where licenses are applied per appliance.
- Q.** Can I order Identity Services Engine licenses as options to the appliances and servers?
- A.** No. Identity Services Engine licenses are defined as spares and must be ordered separately.
- Q.** Can I consolidate multiple license terms with different start and end dates to allow synchronization of the renewal contracts?
- A.** No. License terms cannot be synchronized (e.g., co-term) at this time.

- Q.** Does the Identity Services Engine include an evaluation license?
- A.** Yes. The Identity Services Engine includes a free 90-day evaluation license that can support up to 100 devices. The evaluation license supports Identity Services Engine Base and Advanced software packages.
- Q.** How do I purchase technical support for the Identity Services Engine?
- A.** For Identity Services Engine hardware appliances, you have the option to purchase Cisco SMARTnet® service contracts. For Identity Services Engine “virtual” appliances, you have the option to purchase Cisco Software Application Support plus Upgrades (SASU) service contracts. A valid Cisco SMARTnet or SASU contract covers advanced hardware replacement, Cisco Technical Assistance Center (TAC) support, and major and minor software upgrades and bug fixes for all Identity Services Engine products. You do not need to purchase separate service contracts for the Base or Advanced licenses.
- Q.** What are the new “R” type ISE VM PIDs?
- A.** The new “R” PIDS (R-ISE-VM-K9=, R-ISE-5VM-K9=, R-ISE-10VM-K9=, R-ISE-VM-M-K9=, R-ISE-5VM-M-K9=, R-ISE-10VM-M-K9=) use Cisco’s eDelivery system to deliver ISE VM software. There is no change to pricing or to the physical version of the ISE VM products; this is simply a more automated process. The “R” ISE VM PIDs are the recommended type of ISE eDelivery VM product to order. Please refer to the product bulletin at http://www.cisco.com/en/US/products/ps11640/prod_bulletins_list.html.
- Q.** Will the end-of-sale status be announced for the older “L” versions of the eDelivery ISE VM PIDs?
- A.** Yes. An end-of-sale announcement for the “L” PIDs (L-ISE-VM-K9=, L-ISE-5VM-K9=, L-ISE-10VM-K9=, L-ISE-VM-M-K9=, L-ISE-5VM-M-K9=, L-ISE-10VM-M-K9=) is expected to be made in July 2013. Please use the new “R” versions of the ISE VM PIDs for all orders. There is no change to the physical version of the ISE VM products.
- Q.** What is the new ISE Evaluation Software “R” Product?
- A.** The new ISE Evaluation Software “R” Product (R-ISE-EVAL-K9=) is a free version of ISE software that can be installed as an ISE VM appliance and deployed for evaluation purposes only. It includes a 90-day evaluation license and can support up to 100 endpoints. Like other “R” type products, this is an eDelivery product.
- Q.** Are there changes to accessing ISE software on CCO with the ISE 1.2 software release?
- A.** Yes. In accordance with Cisco policy, ISE 1.2 and subsequent images posted to CCO Software Download Center will require a Cisco support contract (e.g. SmartNet or SASU) number along with a user name and password to access and download the software. ISE 1.x.x software images will continue to require only user name and password for access and download.

Product Comparisons

- Q.** What are the primary differences between Cisco NAC, Cisco Secure ACS, and Cisco Identity Services Engine?
- A.** Cisco NAC and Cisco Identity Services Engine differences are listed in Table 5, and Cisco Secure ACS and Cisco Identity Services Engine differences are listed in Table 6.

Table 5. Differences Between Cisco NAC and Cisco Identity Services Engine

	Cisco NAC	Cisco Identity Services Engine
Control plane for wired out-of-band deployment	Simple Network Management Protocol (SNMP)	RADIUS
Support for in-band mode at network aggregation points	Yes	No
Support for wireless	Yes	Yes
Support for posture on an 802.1X-enabled wired network	No	Yes

Table 6. Differences Between Cisco Secure ACS and Cisco Identity Services Engine

	Cisco Secure ACS	Cisco Identity Services Engine
Support for TACACS+ (device administrator use cases)	Yes	No
User or device authentication and authorization	Yes	Yes
Integrated profiling	No	Yes
Integrated guest services	No	Yes
Security Group Access (SGA)	Yes	Yes

- Q.** When deployed with a NAC Appliance, the NAC Agent supports a feature called Active Directory Single Sign-On (SSO), which provides automatic network authentication based on successful Windows login to AD. The Identity Services Engine also uses the NAC Agent, so does it offer this same functionality?
- A.** Yes. Unlike a NAC Appliance that uses the NAC Agent for authentication and posture, in an Identity Services Engine deployment, the NAC Agent performs only posture assessment functions. SSO support for Identity Services Engine users is provided through supplicants that support transparent 802.1X user authentication based on a user's Windows login credentials. 802.1X supplicants, including Cisco AnyConnect® Network Access Manager and the Microsoft native OS supplicant for Windows XP, Vista, and Windows 7, support this capability. Identity Services Engine customers that deploy certificate-based authentication will also experience transparent network login.
- Q.** The NAC Appliance supports a feature called VPN SSO that provides automatic network authentication based on successful login to a RADIUS gateway. Does the Identity Services Engine offer this same functionality?
- A.** Yes. Unlike a NAC Appliance that requires a separate network authentication following login to a VPN concentrator or wireless LAN controller, the Identity Services Engine authenticates users at the point of access to the VPN or wireless network since it is the RADIUS server for these access devices. No additional network login is required.

Cisco Identity Services Engine Licensing

Q. How do I license the Identity Services Engine, and how does it work?

A. Cisco offers three packages:

- Base package includes authentication, authorization, guest, and MAC security services.
- Advanced package includes Base package offerings, plus posture, profiler, feed service, MDM integration, automated endpoint onboarding, and SGA services.
- Wireless package includes all services (for wireless endpoints only).

Every package is licensed based on the total number of concurrent endpoints that use the services in the package. The total number of endpoints includes all the endpoints connecting to the Cisco Identity Services Engine within a deployment. Every time an endpoint connects to the Identity Services Engine, it consumes one license from one or more packages (depending on what services it uses); when the endpoint disconnects from the network, it releases that license from the Identity Services Engine (after the Identity Services Engine receives a RADIUS stop message).

Q. Should I configure RADIUS accounting on my network access devices (NADs)?

A. Yes. The Cisco ISE uses RADIUS accounting messages to help determine when endpoints start or stop network sessions.

Q. How can I upgrade from one package to another?

A. License upgrades can be implemented in two ways: Base license with Advanced License and Wireless with Wireless Upgrade license. These are shown in Table 7.

Table 7.

Upgrade Method	Order Process	Effect	License Treatment	Term Consideration
Base with Advanced	Customer orders Advanced License	Enables new features (e.g. Posture, Profiling, SGA)	Advanced license quantity cannot exceed Base license quantity	Advanced license have 3- and 5-year terms: No effect on Base licenses
Wireless with Wireless Upgrade		Enabled Wired and VPN Access	Wireless Upgrade License quantity must equal Wireless license quantity	Both Wireless and Wireless Upgrade licenses have 3- and 5-year terms. Wireless and Wireless Upgrade terms do not have to match

Q. How and when does an endpoint in the Identity Services Engine consume an endpoint license?

A. An endpoint consumes a license in the Identity Services Engine when it uses services that belong to specific packages. Table 8 depicts how licenses are consumed in the Identity Services Engine.

Table 8. How Licenses Are Consumed in Cisco ISE Software

Use Case	ISE Release 1.0 Licenses Used		ISE Release 1.1 and Later Licenses Used	
	Base	Advanced	Base	Advanced
Endpoint authenticates and authorizes and uses VLAN, ACL enforcement.	Yes	No	Yes	No
Endpoint authenticates and authorizes and uses SGA enforcement.	Yes	Yes	Yes	Yes
Endpoint authenticates and authorizes with posture assessment.	Yes	Yes	Yes	Yes
Endpoint is added manually to Identity Services Engine and statically assigned an endpoint identity group, with Identity Services Engine probes enabled.	Yes	No	Yes	No
Endpoint is dynamically profiled and assigned to an endpoint identity group. This endpoint identity group is used in authorization policy.	Yes	Yes	Yes	Yes

Q. If I want to use profiling for automated network authorization on a subset of my endpoints, can I buy a smaller number of Advanced licenses than Base licenses?

A. Yes. Having some Advanced licenses (even as few as 100) will enable the Identity Services Engine to collect contextual information for all the endpoints on the network up to the total number of Base licenses. Only when the profile information is used in an authorization decision is the Advanced license consumed. This allows IT administrators to have visibility into the endpoints on the network and then use this information to determine which endpoint categories can be put into a static white list of MAC addresses and which need the full profiler functionality for automated discovery and network services enablement.

Q. What are the prerequisites for deploying any software package?

A. Prerequisites are as follows:

- Base package: There are no prerequisites for deploying the Base software package.
- Advanced package: A Base license must be preinstalled in order to install the Advanced software package. The endpoint count for the Advanced license should be equal to or less than that of the Base license.
- Wireless package: There are no prerequisites for deploying the Wireless software package.

- Wireless Upgrade package: A Wireless license must be preinstalled in order to install the Wireless Upgrade software package. The endpoint count for the Wireless Upgrade license should be equal to that of the Wireless license.

Q. What is the term of the Wireless Upgrade license?

A. Wireless Upgrade licenses can be ordered in 1-, 3-, and 5-year terms and must match the term of the wireless license ordered.

Q. What are the differences between the various licenses available for the Cisco Identity Services Engine?

A. Table 9 lists the differences.

Table 9. Differences Between Cisco Identity Services Engine Licenses

License Type	Features Supported	Deployment Type Supported	License Term	License Prerequisite	ATP Required
Base	Authentication/authorization Guest provisioning Link encryption policies	Wired Wireless VPN	Perpetual	-	Yes
Advanced	Device onboarding/provisioning Device profiling Feed service MDM integration Host posture SGA	Wired Wireless VPN	1-, 3-, or 5-year terms	Base license	Yes
Wireless	Device onboarding/provisioning Authentication/authorization Guest provisioning Link encryption policies Device profiling Feed service MDM integration Host posture SGA	Wireless	1-, 3-, or 5-year terms	-	No
Wireless Upgrade	Authentication/authorization Guest provisioning Link encryption policies Device profiling Feed service MDM integration Host posture SGA	Wireless	1-, 3-, or 5-year terms	Wireless license	Yes

Q. What is an ISE Migration license?

A. ISE Migration licenses are specially priced licenses intended to help existing ACS and NAC customers to migrate to the Identity Services Engine. The ISE Base Migration license is for ACS customers and provides an ISE Base license specific to the quantity ordered. The ISE Advanced Migration license is a license bundle for NAC customers and provides an ISE Base license and a 3-year ISE Advanced license in the quantities ordered.

- Q.** What are the new Identity Services Engine subscription licenses?
- A.** The new ISE subscription licenses are a series of new license PIDs for ISE Advanced, Wireless, and Wireless Upgrade licenses. They can be identified by an “S” in the PID (e.g., L-ISE-ADV-S-10K=, L-ISE-W-S-10K=, L-ISE-WU-S-10K=) and are only orderable via CCW. The new ISE subscription licenses do not impose any pricing change; they are priced exactly as the older ISE term licenses. The benefit of the new ISE subscription licenses is that they deliver new capabilities such as co-termining and renewal management. The new licenses will be orderable in July 2013 and are recommended over the older ISE term licenses.

Deployments

- Q.** What is the maximum number of concurrent endpoints that an Identity Services Engine deployment can support?
- A.** An Identity Services Engine deployment using ISE Release 1.2 can control up to 250,000 endpoints. Deployments using ISE Release 1.x can support a maximum of 100,000 endpoints.
- Q.** Can I deploy Identity Services Engine appliances and servers using different versions of ISE software?
- A.** No.
- Q.** Which reports can the Identity Services Engine generate?
- A.** ISE Release 1.2 has a comprehensive reporting mechanism that shows detailed current and historical information related to authentication, accounting, posture, profiler, guest access, and session directory.
- Q.** Can the Identity Services Engine provide data to external reporting systems?
- A.** Yes. In addition to log data that can be sent to an external log/report server, the Identity Services Engine provides session directory APIs so that you can query the data directly.
- Q.** Does the Identity Services Engine provide mechanisms to transport the reports to any external or central reporting system?
- A.** The Identity Services Engine has the capability, through APIs, to tie into central reporting solutions.
- Q.** What kind of high-availability and redundancy scheme does the solution offer?
- A.** ISE Release 1.2 offers service redundancy through redundant appliances and supports integration with external load balancers to eliminate single points of failure. For details about high availability and redundancy, please refer to the Cisco Identity Services Engine user guide.
- Q.** Can I deploy the Identity Services Engine solution for wireless networks only?
- A.** Yes. You can deploy the Identity Services Engine solution with Wireless licenses for wireless-only deployments (e.g., BYOD or guest network services).
- Q.** Is there an equivalent of the Base license for wireless networks only?
- A.** No. The Base license supports wired, wireless, and VPN endpoints. Customers can deploy the Base license for wireless endpoints only. The Wireless license enables all the features offered by the Base and Advanced licenses (basic network access, guest access, profiler, posture, and SGA) for wireless endpoints only.
- Q.** If I'm using Wireless licenses, what is the recommended way to add support for wired and VPN devices?
- A.** The recommended approach is to order and install a Wireless Upgrade license. The Wireless Upgrade license must be ordered in the same quantity as the existing Wireless license. It is strongly suggested not to add Base or Advanced licenses to deployments where Wireless licenses are already in use.

- Q.** If I order Wireless Upgrade licenses, will this quantity account specifically for wired and VPN devices?
- A.** No. Adding a Wireless Upgrade license does not add to the count of supported endpoints. For example, if a customer has 500 Wireless licenses installed and then purchases and installs 500 Wireless Upgrade licenses, their Identity Services Engine deployment can support a maximum of 500 concurrent endpoints (wired, wireless, VPN devices combined).
- Q.** If I'm using Wireless licenses, can I install Base licenses for wired or VPN device support?
- A.** No. It is strongly suggested not to add Base or Advanced licenses to deployments where Wireless licenses are already in use.
- Q.** Are all Cisco ISE software releases available for download from the Cisco Software Download Center?
- A.** No. Beginning in October 2013, old Cisco ISE software images will begin to be deferred on the Cisco Software Download Center. They are being deferred because of their age and the availability of newer, more stable images. Once deferred, these images will be placed in a specific Deferral Folder on the Cisco Software Download Center and will not be available for download. Please download a more current version of Cisco ISE software. Deferred Cisco ISE software images will still be supported by Cisco Technical Support (TAC).

The initial Cisco ISE software image release and the related patches are: 1.0, 1.0MR, and 1.1.

Cisco ISE software releases 1.1.1, 1.1.2, 1.3.3, 1.1.4, and 1.2 will still be available for standard downloading from Cisco Software Download Center.

Please consult the Cisco ISE 1.1.x Release Notes for the list of resolved defects in available software releases.

Ordering and Purchasing

- Q.** How can I purchase the Cisco Identity Services Engine?
- A.** Cisco Identity Services Engine Advanced, Base, and Wireless Upgrade licenses can be purchased through Cisco Authorized Technology Provider (ATP) Partners, through Cisco Advanced Services, or through a fully trained business-unit-sponsored professional services partner.
- Note:** Cisco Identity Services Engine platforms (both physical and virtual) and Wireless licenses are generally available for purchase through any Cisco Certified Partner.
- Q.** What is an Authorized Technology Provider (ATP) Partner?
- A.** Cisco ATP Partners have demonstrated expert levels of training and knowledge in specific advanced technologies. The ATP Program for the Identity Services Engine was designed to ensure customer success in solving complex security challenges related to their Identity Services Engine deployments.
- Q.** What if an ATP Partner cannot address a customer's deployment needs in a timely manner?
- A.** If an ATP Partner does not have immediate resources, assistance can be requested from Cisco Advanced Services or from a business-unit-sponsored professional services partner who has been fully trained, has authored HLD documents, and has worked at Cisco as a Technical Marketing Engineer, such as SecurView.

Additional Information

- Q.** Whom should I contact for additional information?
- A.** Please contact your local Cisco sales representative or Cisco Certified Partner.
- Q.** Where can I go for additional information?
- A.** To learn more about the Cisco Identity Services Engine, please visit <http://www.cisco.com/go/ise>.



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 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: 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)