

Cisco Identity Services Engine

The Cisco[®] Identity Services Engine (ISE) allows you to see and control users and devices connecting to the corporate network. It does all this from a central location.

Product Overview

A different approach is required to both manage and secure the evolving mobile enterprise. With superior user and device visibility, Cisco ISE simplifies the mobility experience for enterprises. It also shares vital contextual data with integrated technology partner solutions. With the integration, consolidation, and automation that Cisco ISE provides, you can identify, contain, and remediate threats faster.

The Customer Advantages

Cisco ISE offers a holistic approach to network access security. You gain many advantages when it is deployed, including:

Highly secure business and context-based access based on your business policies. ISE can match endpoints with attributes, such as user, time, location, threat, vulnerability, or access type, to create an all-encompassing contextual identity. This identity can be used to enforce a highly secure access policy that matches the identity's business role. IT administrators can apply precise controls over who, what, when, where, and how endpoints are allowed on the network. ISE uses multiple mechanisms to enforce policy, including [Cisco TrustSec[®]](#) software-defined segmentation.

Streamline network visibility through a simple, flexible, and highly consumable interface. ISE now stores a detailed attribute history of all the endpoints that connect to the network. The streamlined Visibility Wizard can quickly deploy the feature to get a complete picture of all the endpoints on a given network. This picture includes visibility of guest users on the network, all the way down to endpoint application details and firewall status.

Extensive policy enforcement that defines easy, flexible access rules that meet your ever-changing business requirements. All this is controlled from a central location that distributes enforcement across the entire network and security infrastructure. IT administrators can centrally define a policy that differentiates guests from registered users and devices. Regardless of the access location, users and endpoints are allowed access based on role and policy.

Robust guest experiences that provide multiple levels of access to your network. Guests can use a coffee-shop hotspot, self-service registered access, or sponsored access to specific resources. Dynamic visual tools offer a real-time preview of the portal screen and the experience a user would have connecting. You can see how changes affect the settings in sponsored, self-registration, and access confirmation for both SMS and email. Deployment is quick and easy with the [ISE Wireless Guest Setup Guide](#).

Self-service device onboarding for the enterprise's bring-your-own-device (BYOD) or guest policies. Users can manage devices according to the business policies defined by IT administrators. The IT staff will have the automated device provisioning, profiling, and posturing needed to comply with security policies. At the same time, employees can get their devices onto the network without requiring IT assistance.

Software-Defined Access (SDA). Part of Cisco’s Digital Network Architecture (DNA), Cisco SDA provides consistent policy from the edge to the cloud. User access policy is automated across a single network fabric with highly secure end-to-end segmentation. Cisco SDA is simpler to enable than other segmentation mechanisms such as VLANs, and policies stay consistent on the network regardless of the underlying infrastructure. The consistency in policy across the network simplifies segmentation, optimizes the use of resources, and fosters a more secure network.

DNA is powered by three pillars. DNA Center centralizes network automation using an overlay fabric that is separate from the physical underlay. ISE serves as the security policy for the entire fabric. And the Network Data Platform (NDP) provides assurance of network operations and performance. With Cisco SDA, organizations will see a significant reduction in OpEx and complexity while increasing capability.

Automated device-compliance checks for device-posture and remediation options using the Cisco AnyConnect® Unified Agent. The AnyConnect agent also provides advanced VPN services for desktop and laptop checks. ISE integrates with market-leading mobile device management/enterprise mobility management (MDM/EMM) vendors. This integration helps ensure that the mobile device is both secure and policy compliant before it is given access to the network.

Sharing of user and device details throughout the network. Cisco [pxGrid technology](#) is a robust platform that you can use to share a deep level of contextual data about connected users and devices with Cisco and [Cisco Security Technical Alliance](#) solutions. ISE’s network and security partners use this data to improve their own network access capabilities and accelerate third-party capabilities to identify, mitigate, and rapidly contain threats.

Features and Benefits

Cisco ISE empowers organizations in a number of ways (Table 1).

Table 1. Features and Benefits

Feature	Benefit
Centralized management	<ul style="list-style-type: none"> Helps administrators centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console. Simplifies administration by providing integrated management services from a single pane of glass.
Business-policy enforcement	<ul style="list-style-type: none"> Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. Provides the ability to create detailed policies by pulling attributes from predefined dictionaries. Includes attributes such as user and endpoint identity, posture validation, authentication protocols, profiling identity, and other external attributes. These can be created dynamically and saved for later use. Integrates with multiple external identity repositories such as the Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA one-time password (OTP), certificate authorities for both authentication and authorization, and Open Database Connectivity (ODBC).
Access control	<ul style="list-style-type: none"> Provides a range of access control options, including downloadable access control lists (dACLs), virtual LAN (VLAN) assignments, URL redirections, named ACLs, and security groups (SGs) with Cisco TrustSec technology.
Secure supplicant-less network access with Easy Connect	<ul style="list-style-type: none"> Provides the ability to swiftly roll out highly secure network access without configuring endpoints for 802.1X authentication. Derives authentication and authorization from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
Security group tag exchange protocol (SXP) support	<ul style="list-style-type: none"> Uses SXP as a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets with security group tags (SGTs). Allows security services on switches, routers, or firewalls to learn identity information from access devices.
Guest lifecycle management	<ul style="list-style-type: none"> Provides a streamlined experience for implementing and customizing guest network access. Creates corporate-branded guest experiences with advertisements and promotions in minutes. Support is built in for hotspot, sponsored, self-service, and numerous other access workflows. Provides the administration with real-time visual flows that bring the effects of the guest flow design to life. Tracks access across the network for security, compliance, and full guest auditing. Time limits, account expirations, and SMS verification offer additional security controls. Streamlines access so guests can use their social media credentials to connect.

Feature	Benefit
Streamlined device onboarding	<ul style="list-style-type: none"> • Provides automatic supplicant provision and certificate enrollment for standard PC and mobile computing platforms. Provides more secure access, reduces IT help desk tickets, and delivers a better experience to users. • Enables end users to add and manage their devices with self-service portals and supports SAML 2.0 for web portals. • Integrates with MDM/EMM vendors for mobile device compliancy and enrollment.
Built-in AAA services	<ul style="list-style-type: none"> • Uses standard RADIUS protocol for authentication, authorization, and accounting (AAA). • Supports a wide range of authentication protocols, including, but not limited to PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS), and EAP-Tunneled Transport Layer Security (TTLS).
Device administration access control and auditing	<ul style="list-style-type: none"> • Supports the TACACS+ protocol • Grants users access based on credentials, group, location, and executable commands. • Provides access to device configuration on a need-to-know and need-to-act basis while keeping audit trails for every change in the network.
Internal certificate authority	<ul style="list-style-type: none"> • Offers an easy-to-deploy internal certificate authority. • Provides a single console to manage endpoints and certificates. Certificate status is checked through the standards-based Online Certificate Status Protocol (OCSP). Certificate revocation is automatic. • Supports standalone deployments, products integrated on pxGrid, and subordinate ones (that is, ones in which the certificate authority is integrated with your existing enterprise public key infrastructure, or PKI). • Facilitates the manual creation of bulk or single certificates and key pairs to connect devices to the network with a high degree of security.
Device profiling	<ul style="list-style-type: none"> • Ships with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones, tablets, and more than 250 medical devices. • Creates custom device templates to automatically detect, classify, and associate administration-defined identities when endpoints connect to the network. • Associates endpoint-specific authorization policies based on device type. • Collects endpoint attribute data with passive network monitoring and telemetry.
Device-profile feed service	<ul style="list-style-type: none"> • Delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. Simplifies the task of keeping an up-to-date library of the newest IP-enabled devices. • Partners and customers can share customized profile information to be vetted by Cisco and redistributed.
Endpoint posture service	<ul style="list-style-type: none"> • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispymware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, and USB -attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect® 4.x agent for posture assessment on these OS platforms: <ul style="list-style-type: none"> ◦ Windows 10, 8.1, 8, and 7 ◦ Mac OS X 10.8 and later
Extensive multi-forest Active Directory support	<ul style="list-style-type: none"> • Provides comprehensive authentication and authorization against multiforest Microsoft Active Directory domains. • Groups multiple disjointed domains into logical groups. • Includes flexible identity rewriting rules to smooth the solution's transition and integration. • Supports Microsoft Active Directory 2003, 2008, 2008R2, 2012, and 2012R2.
<u>Cisco Rapid Threat Containment</u>	<ul style="list-style-type: none"> • Takes manual or automated network mitigation and investigation actions in response to security events. • Integrates Cisco ISE and Cisco <u>security technology partner</u> solutions in a broad variety of technology areas. • Changes user access based on the Common Vulnerability Scoring System (CVSS) and Structured Threat Information Expression (STIX) threat scores. • Uses <u>Cisco pxGrid</u> as a highly scalable IT clearinghouse for multiple security tools to communicate automatically with each other in real time.
Monitoring and troubleshooting	<ul style="list-style-type: none"> • Offers a built-in help desk web console for monitoring, reporting, and troubleshooting. • Provides robust historical and real-time reporting for all services. Logs all activity and offers real-time dashboard metrics of all users and endpoints connecting to the network.

Feature	Benefit
Certifications	<ul style="list-style-type: none"> • Meets the requirements of Federal Information Processing Standard (FIPS) 140-2, Common Criteria, and Unified Capabilities Approved Product List. • IPv6 ready. • Note: Certifications may not be available on all releases or they may be in varying states of approval. Current certifications and releases can be found at Global Government Certifications.

Platform Support and Compatibility

ISE is available as a [physical](#) or virtual appliance. Both physical and virtual deployments can be used to create ISE clusters to serve larger organizations and to provide the scale, redundancy, and failover requirements of a critical enterprise business system.

ISE virtual appliances are supported on VMware ESXi 5.x and 6.x or KVM on Red Hat 7.x. A production deployment should be run on hardware that equals or exceeds the configurations of the current physical ISE platforms. For lab or testing environments that provide no product services, the solution can be run on virtual targets that have at least 4 GB of memory and at least 200 GB of hard-drive space available.

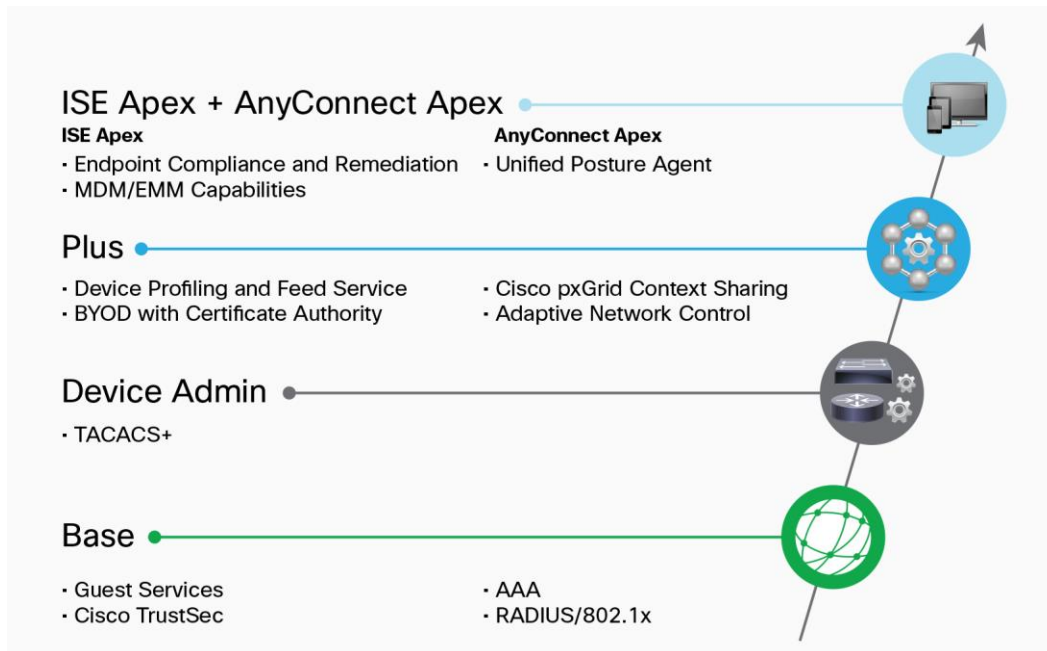
For physical platform support of ISE, please refer to the [Cisco Secure Network Server data sheet](#).

Licensing Overview

Currently, seven license packages are available (see Figure 1). Cisco support services for Base licenses are tied to Cisco Smart Net Total Care™ Software Application Support plus Upgrades contracts. Cisco support services for the various term-based licenses are included in the individual term license for the duration of the license.

As seen in Figure 1, four primary ISE licenses are available. With this flexible model, you can select the number and combination of licenses to get the set of services you want.

Figure 1. ISE License Packages



Ordering Information

The Cisco ISE [Ordering Guide](#) will help you understand the different models and licensing types that will make the best use of your ISE deployment. To place an order, visit the [Cisco ordering homepage](#). To download the ISE software, visit the [Cisco Software Center](#).

Service and Support

Cisco offers a wide range of service programs. These innovative programs are delivered through a combination of people, processes, tools, and partners that results in high levels of customer satisfaction. Cisco Services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see [Cisco Technical Support Services](#) or [Cisco Security Services](#).

Warranty information is found at: <http://www.cisco.com/go/warranty>. Licensing information is available at: <http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-licensing-information-listing.html>.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital[®] financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [Learn more](#).

For More Information

For more information about the Cisco ISE solution, visit <http://www.cisco.com/go/ise> or contact your local account representative.



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)