Cisco Identity Services Engine

The Cisco® Identity Services Engine (ISE) is your one-stop solution to streamline security policy management and reduce operating costs. With ISE, you can see users and devices controlling access across wired, wireless, and VPN connections to the corporate network.

Product overview

Cisco ISE allows you to provide highly secure network access to users and devices. It helps you gain visibility into what is happening in your network, such as who is connected, which applications are installed and running, and much more. It also shares vital contextual data, such as user and device identities, threats, and vulnerabilities with integrated solutions from Cisco technology partners, so you can identify, contain, and remediate threats faster.

Customer advantages

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

Highly secure business and context-based access based on your company policies. ISE works with network devices to create an all-encompassing contextual identity with attributes such as user, time, location, threat, vulnerability, and access type. This identity can be used to enforce a highly secure access policies 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. Cisco TrustSec security groups are based on business rules and not IP addresses or network hierarchy. These security groups give users access that is constantly maintained as resources move across domains. Managing switch, router, and firewall rules becomes easier.

Streamlined network visibility through a simple, flexible, and highly consumable interface. ISE stores a detailed attribute history of all the endpoints that connect to the network as well as users (including types such as guest, employee, and contractors) 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 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 their location, users and endpoints are allowed access based on role and policy.

Robust guest experiences that provide multiple levels of access to your network. You can provide guest access through a coffee-shop-type hotspot access, self-service registered access, or sponsored access. ISE provides you with the ability to highly customize various guest portals through an on-box or cloud-delivered portal editor that provides dynamic visual tools. You can see real-time previews of the portal screen and the experience a guest would have connecting to the network.

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.

DNA Center

DNA Center is the foundational controller and analytics platform at the heart of Cisco's Intent based Network. DNA Center simplifies network management and allows one to quickly set up various ISE services such as Guest and BYOD quickly and easily throughout the network, DNA Center also makes it easy to design, provision, and apply policy in minutes, not days across the network. Analytics and assurance use network insights to optimize network performance. DNA Center integrates with ISE 2.3 or later using pxGrid to deploy group based secure access and network segmentation based on business needs. With Cisco DNA Center and ISE, policy can be applied to users and applications instead of to the network devices. TrustSec technology provides software-defined segmentation to control network access, enforce security policies, and meet compliance requirements.

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 also integrates with market-leading Mobile Device Management/Enterprise Mobility Management (MDM/EMM) vendors. MDM integration helps ensure that a mobile device is both secure and policy compliant before it is given access to the network.

The ability to share user and device details throughout the network. Cisco pxGrid (Platform Exchange Grid) 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 their ability to identify, mitigate, and rapidly contain threats.

Central network device management using TACACS+. Cisco ISE allows you to manage network devices using the TACACS+ security protocol to control and audit the configuration of network devices. ISE facilitates granular control of who can access which network device and change the associated network settings.

Features and benefits

Cisco ISE empowers organizations in a number of ways, as shown in Table 1.

Table 1. Features and benefits

Feature	Benefit
Centralized management	• 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.
Rich contextual identity and business-policy enforcement	• 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 attributes can be created dynamically and saved for later use. • Integrates with multiple external identity repositories such as 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	• 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.

Feature	Benefit
Secure supplicant-less network access with Easy Connect	• 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	• Propagates 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	• 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.
Streamlined device onboarding	• Automates 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	• 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). Note: Cisco ISE is the only RADIUS server to support EAP chaining of machine and user credentials.
Device administration access control and auditing	• Supports the TACACS+ protocol • Grants users access based on credentials, group, location, and 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	• 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	• Populated with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets. with additional device templates available for specialized devices such as medical, manufacturing, and building automation. • 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	• 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. • Gives partners and customers the ability to share customized profile information to be vetted by Cisco and redistributed.
Endpoint posture service	• 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 antispyware 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: ◦ Windows 10, 8.1, 8, and 7 ◦ Mac OS X 10.8 and later

Feature	Benefit
Extensive multiforest Active Directory support	• 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, 2012R2, and 2016.
Monitoring and troubleshooting	• 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.
Certifications	• 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.

Integrated solutions

Cisco pxGrid is a highly scalable IT clearinghouse for multiple security tools to communicate automatically with each other in real time. With Cisco ISE 2.4 we introduce pxGrid 2.0, which provides a new WebSockets client and removes dependencies on underlying operating systems and languages. More than 50 integrations are available from Cisco and third-party vendors, notably Cisco Industrial Network Director (IND), which uses pxGrid to provide OT endpoint information to ISE.

Cisco Rapid Threat Containment simplifies and automates network mitigation and investigation actions in response to security events. It integrates Cisco ISE and Cisco security technology partner solutions in a broad variety of technology areas. With Threat-Centric Network Access Control (TC-NAC), it can change user access based on CVSS vulnerability and STIX threat scores. With the Cisco pxGrid Adaptive Network Control (ANC), it gives you the ability to reset the network access status of an endpoint to quarantine, unquarantine, bounce, or shut down a port.

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 that can provide the scale, redundancy, and failover requirements of a critical enterprise business system.

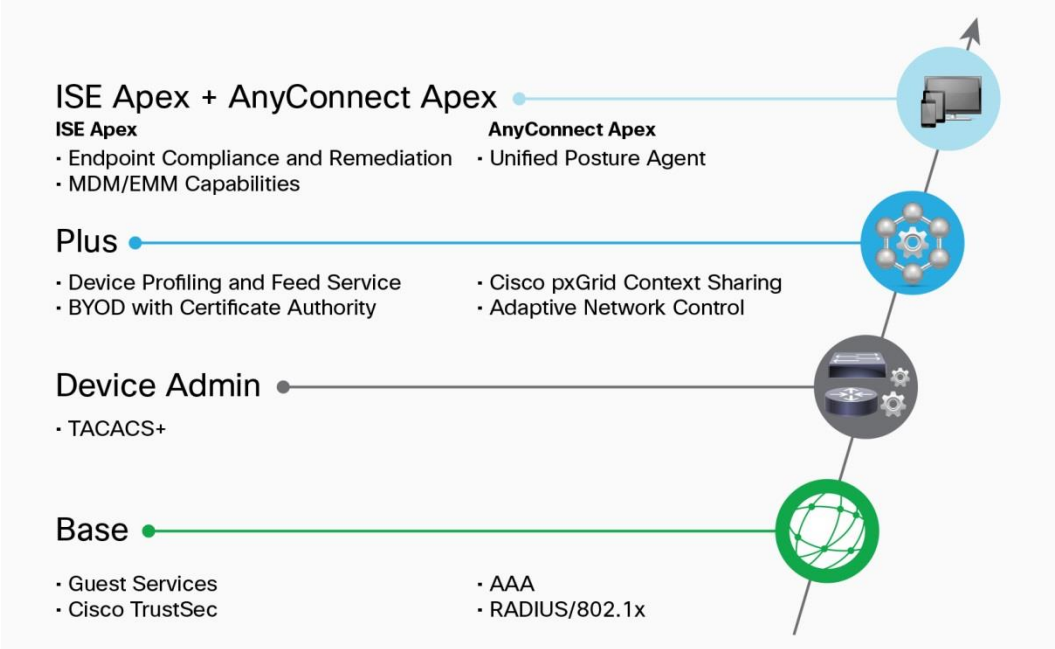
ISE virtual appliances are supported on VMware ESXi 5.x and 6.x, KVM on Red Hat 7.x, and Microsoft Hyper-V on Microsoft Windows Server 2012R2 and later. A production deployment should be run on hardware that equals or exceeds the configurations of the current physical ISE platforms. For lab or testing 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 ISE physical appliance details please refer to the Cisco Secure Network Server data sheet.

Licensing overview

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 features you want.

Figure 1. Cisco ISE license packages



Ordering information

The Cisco ISE ordering guide will help you understand the different models and licensing types to 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 can be found here.

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, and 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 https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html 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 **https://www.cisco.com/go/offices**.

Printed in USA C78-656174-16 03/18