Cisco Identity Services Engine

The Cisco® Identity Services Engine (ISE) helps IT professionals meet enterprise mobility challenges and protect the evolving network across the attack continuum. The market-leading platform for security-policy management, it unifies and automates access control to enforce compliance-driven role-based access to networks and network resources.

Product Overview

The enterprise network no longer sits within four secure walls. It extends to wherever employees are and wherever data goes. Employees today want access to work resources from more devices and through more non-enterprise networks than ever before. Mobility and the Internet of Everything (IoE) are changing the way we live and work. As a result, enterprises must support a massive proliferation of new network-enabled devices. However, a myriad of security threats and highly publicized data breaches clearly demonstrate the importance of protecting this evolving enterprise network.

As the modern network expands, the complexity of marshaling resources, managing disparate security solutions, and controlling risk grows as well. Factor in the ubiquitous connectivity of IoE with already constrained IT resources, and the potential impact of failing to identify and remediate security threats becomes very large indeed.

A different approach is required for both the management and the security of the evolving mobile enterprise. With superior user and device visibility, Cisco ISE delivers simplified mobility experiences to enterprises. It also shares vital contextual data with integrated ecosystem partner solutions using Cisco Platform Exchange Grid (pxGrid) technology. The identification, mitigation, and remediation of threats are all accelerated.

Features and Benefits

Cisco ISE offers a holistic approach to network access security. It provides:

- Accurate identification of every user and device
- Easy provisioning of all devices
- Centralized, context-aware policy management to control user access: whoever, wherever, and from whatever device
- Rich contextual data about connected users and devices to rapidly detect, mitigate, and remediate threats

When deployed in a network, customers gain many advantages (Table 1).

Table 1. Major Customer Advantages

Advantage	Description
Highly secure business and context-based access	With ISE, organizations can deliver what is defined in their business policies. It can match users and endpoints and other attributes such as time, location, and access type or method to create an encompassing contextual identity. This identity is used to enforce a secure-access policy that matches the identity's business role. IT administrators can apply precise controls over who and what are allowed on the network. They can use multiple mechanisms to enforce the policy, including the Cisco TrustSec® solution' security group tags.

Advantage	Description
Extensive policy enforcement	ISE is the industry's first software-defined security controller. Organizations can define access policy rules easily and with great flexibility to meet their ever-changing business needs. They can do this all from a centralized location that distributes enforcement across the entire network and security infrastructures. For example, IT administrators can centrally define a policy that differentiates guest users and devices from registered users and devices. Regardless of the access location, users and endpoints are allowed access based on their context.
Streamlined guest experiences	With the solution's out-of-the-box simplicity, organizations can provide multiple levels of guest access to their networks. Guests can use a coffee-shop hotspot or self-service registered access or sponsored access to specific resources (internal or external). Dynamic visual tools offer real-time previews of the portal screens and the steps that a user experiences. You can test how changes will affect settings in sponsored guest accounts, self-registrations, and SMS and email confirmations of access.
Self-service device onboarding	The IT staff can decide how to implement an enterprise's bring-your-own-device (BYOD) or guest policies. With a self-service portal, users can register and provision new devices according to the business policies defined by the IT administrators. The IT staff can get the automated device provisioning, profiling, and posturing it needs to comply with security policies, while employees can get their devices onto the network without requiring IT assistance.
Security compliance	A single management console simplifies policy creation, visibility, and reporting across all company networks. The IT staff can easily validate compliance for audits, regulatory requirements, and mandated federal guidelines for IEEE 802.1X standards.
Automated device-compliance checks	ISE delivers device-posture check and remediation options using the Cisco AnyConnect® Unified Agent, which also provides advanced VPN services for desktop and laptop checks. ISE can also be integrated with market-leading enterprise mobility management (EMM) solutions for mobile devices. IT staff can thus make sure that a user's device is both highly secure and policy compliant before giving it access to the network.
Multivendor-infrastructure support	ISE supports third-party network access devices, depending on the device's capabilities[1]. ISE interoperates with a multivendor infrastructure (for example, switches and wireless access points). It is compliant with RADIUS and IEEE 802.1X standards, but does not require IEEE 802.1X in order to fully operate. Cisco and its partners offer best-practice guidelines as well as detailed, hands-on design guidance. Enterprise customers use ISE with a network infrastructure designed by Cisco along with Cisco TrustSec technology to get even greater intelligence and visibility from their networks.
pxGrid context sharing	ISE collects dynamic contextual data from throughout the network and uses pxGrid technology, a robust context-sharing platform, to share that deeper level of contextual data about connected users and devices with external and internal ecosystem partner solutions. Through the use of a single framework, ISE's network and security partners use this data to improve their own network access capabilities and accelerate their own solutions' capabilities to identify, mitigate, and remediate network threats.
Broad, integrated partner ecosystem	ISE boasts one of the largest Cisco partner ecosystems. Partners use pxGrid to improve endpoint vulnerability remediation, network forensics, and web single sign-on (SSO). Integrated technology partners for EMM, security information and event management (SIEM), and threat defense all take advantage of the deep contextual identity awareness that ISE provides. With ISE, partner platforms can reach deep into the Cisco network infrastructure and implement network actions for users and devices (for example, quarantining smartphones or laptops and blocking network access).

[1] For standard access control with dynamic authorization (including the integration of profiling into the access decision), a network access device must support CoA as defined in RFC 5176. For the guest, BYOD on boarding, and posture flows, a network access device must support URL redirection with media access control (MAC) address notification.

ISE empowers organizations by providing comprehensive policy management, streamlined device onboarding, rich contextual data that can be shared with partner network solutions, and dynamic enforcement to help ensure highly secure wired, wireless, and VPN access. Features and benefits are shown in Table 2.

Table 2. Features and Benefits

Feature	Benefit
Business-policy enforcement	Provides a rule-based, attribute-driven policy model for creating flexible and business-relevant access control policies. Provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries that include information about user and endpoint identity, posture validation, authentication protocols, profiling identity, or other external attribute sources. Attributes can also be created dynamically and saved for later use. Offers the ability to integrate with multiple external identity repositories, such as Microsoft Active Directory, Lightweight Directory Access Protocol (LDAP), RADIUS, RSA one-time password (OTP), and certificate authorities for both authentication and authorization.
Access control	Provides a range of access control options, including downloadable access control lists (dACLs), VLAN assignments, URL redirections, named ACLs, and security group tags (SGTs) using the advanced capabilities of Cisco TrustSec technology-enabled network devices.

Feature	Benefit
Highly secure supplicant-less network access	Provides organizations with the ability to swiftly roll out highly secure network access without configuring endpoints for authentication and authorization. Authentication and authorization are derived from login information across application layers and used to allow user access without requiring a 802.1X supplicant to exist on the endpoint.
Source-Group Exchange Protocol (SXP) Support	Can act as an SXP speaker or listener as defined in the Source-Group Tag Exchange Protocol (SXP) draft and as the network's source of truth for source-group tag information. Organizations can use ISE to bridge over the segments that are not compliant with Cisco TrustSec policies. At the same time, they can make sure that differentiated role-based access is provided across the entire network.
Guest lifecycle management	Provides a streamlined experience for implementing and customizing guest network access. With built-in support for hotspot, sponsored, self-service, and numerous other access workflows, the solution makes it easy to create corporate-branded guest experiences, with advertisements and promotions, in minutes. The new guest administration Work Center provides real-time visual flows that bring the effects of your design to life right before your eyes. Time limits, account expirations, and SMS verification offer additional security controls, and full guest auditing can track access across your network for security and compliance demands.
Streamlined on- and off-premises device onboarding	Delivers fully customizable and branded user experiences with themes. Offers out-of-the-box workflows that walk users through the onboarding process and provides end users with their own self-service portals to add and manage their devices. Provides automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. This streamlined device onboarding creates fewer IT help desk cases along with more secure access and an easier, more transparent experience for users. ISE can be integrated with mobile device management/enterprise mobility management (MDM/EMM) solutions to help ensure that the mobile device is compliant with the MDM/EMM policy. It can also redirect the user to the MDM/EMM registration system to connect the registration flow with the overall mobile device onboarding flow.
AAA protocols	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). ISE is the only RADIUS server to support EAP chaining of machine and user credentials.
Device administration access control and auditing	Uses the TACACS+ protocol so that an organization can authenticate, authorize, and audit users when they access devices that support the TACACS+ protocol, such as network devices and servers. Users can be granted fine-grained access to commands on every device based on their credentials, the group they belong to, where they connect from, and what action they are trying to take on the device. Organizations can provide 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 organizations an easy-to-deploy internal certificate authority to simplify certificate management for personal devices without adding the significant complexity of an external certificate authority application. ISE offers a single console to manage endpoints and their certificates with the capability to check certificate status through the standards-based Online Certificate Status Protocol (OCSP) and provide automatic certificate revocation when a device is stolen. The internal certificate authority supports standalone deployments as well as subordinate ones (that is, ones in which the certificate authority is integrated with your existing enterprise public key infrastructure, or PKI). For Internet of Things (IoT) devices, a certificate provisioning portal is provided to facilitate the manual creation of bulk or single certificates and key pairs, so that these devices can be connected to the network with a high degree of security.
Device profiling	Ships with predefined device templates for many types of endpoints, such as IP phones, printers, IP cameras, smartphones, and tablets. Administrators can also create their own device templates. These templates can be used to automatically detect, classify, and associate administration-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type. The solution collects endpoint attribute data with passive network monitoring and telemetry, querying the actual endpoints, or alternatively from the Cisco infrastructure by means of device sensors on Cisco Catalyst® switches. The infrastructure-driven endpoint-sensing capability on Catalyst switches is a subset of ISE's sensing technology. This capability allows the switch to quickly collect endpoint-attribute information and then, using standard RADIUS, pass this information to ISE for endpoint classification and policy-based enforcement. This switch-based sensing promotes the efficient and distributed collection of endpoint information for increased scalability, deployability, and time to classification.
Device-profile feed service	Supports ISE's out-of-the-box profiling technology with an industry-first device-profile feed service. The service delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. It also offers a mechanism where partners and customers can share their own customized profile information to be vetted by Cisco and redistributed. With these automatic updates, enterprises have the ability to detect all of the newest devices when their users try to connect them to the network. This simplifies the task of keeping up with the multitude of new devices coming out every week and reduces a significant amount of support that IT administrators need to provide.
Endpoint posture	Verifies endpoint posture assessment for PCs and mobile devices connecting to the network. Works through a persistent client-based agent, a temporary web agent, or a query to an external MDM/EMM system to validate that an endpoint conforms to a company's posture policies. Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patches, antivirus and antispyware software packages with current definition file variables (version, date, etc.), registries (key, value, etc.), patch management, disk encryption, mobile PIN-lock or rooted or jailbroken status, application presence, and so on. Also supports the 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. Can now use the endpoint state from an external MDM/EMM system to apply different policies to mobile platforms.

Feature	Benefit
Ecosystem with pxGrid	Accelerates partner solutions' capabilities across the network. pxGrid is a robust context-sharing platform that takes the deep level of contextual data collected by ISE and delivers it to external and internal ecosystem partner solutions. From endpoint vulnerability assessment to web single sign-on, the list of ecosystem partners who are taking advantage of this simple unified framework continues to expand. Visit our partner security ecosystem page for information about how ISE can integrate through pxGrid with SIEM and threat defense solutions, web security solutions, and operational technology control (including supervisory control and data acquisition, or SCADA, operational and security policy integration). You will also find information about ISE and simplified network troubleshooting and forensics, endpoint vulnerability remediation, network and application performance management, cloud security access brokers, firewall and access control, rapid threat containment, and risk-based, adaptive authentication single sign-on.
Extensive multiforest Active Directory support	Provides comprehensive authentication and authorization against multiforest Microsoft Active Directory domains. Can group multiple disjointed domains into logical groups for simplified configuration of complex Active Directory topologies to support ever-changing business environments. Also supports flexible identity rewriting rules to smooth the solution's transition and integration. Supports Microsoft Active Directory 2003, 2008, 2008R2, 2012, and 2012R2.
Endpoint protection service	Helps administrators quickly take corrective action (quarantine, un-quarantine, or shut down) on risk-compromised endpoints within the network. This service helps reduce risk and increase security in the network.
Centralized management	Helps administrators centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console. Greatly simplifies administration by providing integrated management services from a single pane of glass.
Monitoring and troubleshooting	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist help desk and network operators in quickly identifying and resolving issues. Offers robust historical and real-time reporting for all services, logging of all activities, and real-time dashboard metrics of all users and endpoints connecting to the network.
Platform options	Available as a physical or virtual appliance. There are two physical platforms as well as a VMware ESXi- or KVM-based virtual appliance. Both physical and virtual form factors can be used to create ISE clusters to serve larger organizations and provide the necessary scale, redundancy, and failover required of a critical enterprise business system.
Certifications	Meets requirements of Federal Information Processing Standard (FIPS) 140-2, Common Criteria, and Unified Capabilities Approved Product List. Also 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 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.

Posture Assessment System Requirements

System requirements for the AnyConnect® 4.x agent, used for posture assessment, are the following:

- Microsoft Windows 7, 8, or 8.1 (32-bit or 64-bit) Mac OS X 10.7, 10.8, or 10.9

Licensing

Currently, six license packages are available (see Table 3). Cisco support services for the 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.

Table 3. License Packages

License Package or Bundle	Focus	Perpetual or Subscription (Terms Available)	Notes
Base	Provides highly secure access	Perpetual	-
Plus	Provides context about endpoints for more detailed access policies	Subscription (1, 3, or 5 years)	Does not include Base services; Base licenses are required to install Plus licenses
Apex	Provides context and compliance details about endpoints for more detailed access policies	Subscription (1, 3, or 5 years)	Does not include Base or Plus services; Base licenses are required to install Apex licenses. Please note that AnyConnect Apex user licenses are required in addition to ISE Apex licenses when making use of AnyConnect unified agent services across wired, wireless, and VPN.
Device Management	Allows device administration tasks to be performed through the TACACS+ and RADIUS protocol	Perpetual	Requires one license per deployment
Mobility	Delivers complete ISE services for wireless and VPN endpoints only	Subscription (1, 3, or 5 years)	Please note that AnyConnect Apex user licenses are required in addition to ISE Mobility licenses when making use of AnyConnect unified agent services.
Mobility Upgrade	Helps enable wired endpoint support for wireless license deployments	Subscription (1, 3, or 5 years)	See the ISE License Ordering Guidelines section for quantity requirements.
Express	Entry-level VM license bundle for small guest deployments	Perpetual	Bundle includes 1 ISE virtual appliance and 150 Base licenses for guest services. The virtual appliance is for a single-site deployment (non-distributed, no high availability).
Evaluation	Limited use of product for presales customer evaluation	Temporary (90 days)	Full functionality is provided for 100 endpoints.

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® 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.

Printed in USA C78-656174-11 10/15