Cisco Identity Services Engine (ISE)

Product Overview

The Cisco® Identity Services Engine (ISE) helps IT professionals meet enterprise mobility challenges and secure the evolving network across the entire attack continuum. Cisco ISE is the market-leading security policy management platform that unifies and automates highly secure access control to enforce role-based access to networks and network resources. It delivers superior user and device visibility to enable simplified enterprise mobility experiences, and it shares vital contextual data with integrated ecosystem partner solutions using Cisco Platform Exchange Grid (pxGrid) technology to accelerate the identification, mitigation, and remediation of threats.

Security in a Mobile Enterprise

The enterprise network no longer sits within four secure walls. Employees today demand access to enterprise resources using more mediums than ever before, including personal laptops, tablets, and smartphones, and from home networks and mobile networks. Mobility, in particular, can expose networks to devastating attacks and data breaches, and the resulting economic costs to an organization can be huge. Yet today's mobile workforce needs to work anytime, anywhere, to stay competitive and be productive. With the increasing complexity of this expanded network and the advent of the "Internet of Things," and with network-enabled devices of all kinds connecting to private and public networks, the potential impact of failing to identify and remediate network security threats grows exponentially.

At the same time, IT professionals are being tasked with supporting enterprise mobility initiatives on tighter budgets while adhering to government, industry, and other compliance requirements. Among other things, these requirements demand clear visibility into network access and tight access controls. Security point solutions are often distributed and deployed in larger numbers across the entire enterprise network, focusing on identifying threats as they occur or assisting in forensic events after a breach or attack. Security solutions that focus on preventing compromised devices or users from accessing the network in the first place usually entail highly complex, time-consuming, expensive deployments. As your network evolves and expands, this disparate array of point solutions cannot scale quickly enough to keep up. A different approach is required for both the management and the security of this evolving, mobile enterprise. It's called the Cisco Identity Services Engine (ISE).

Features and Benefits

The Cisco ISE offers a more holistic approach to network access security and provides:

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

When operating in a network, customers gain the advantages from deploying Cisco ISE shown in Table 1.

Table 1. Key Customer Advantages

Cisco ISE Advantage	
Powerful device classification	Cisco ISE offers the industry's first integrated device profiler to identify each endpoint; match it to its user or function and other attributes, including time, location, and network; and create a contextual identity so IT can apply precise controls over who and what is allowed on the network. An automated device feed service updates Cisco ISE in real time to help ensure that new devices can be identified as soon as they are released to the market.
Extensive policy enforcement	Cisco ISE enables the organization to define access policy rules easily and with great flexibility to meet the ever-changing business requirement needs of the enterprise. For example, IT administrators can define policy in Cisco ISE that differentiates guest users and devices from registered users and devices. Guest users may receive limited access across the entire network, while registered users receive their policy-designated access. Further, policy in Cisco ISE can help ensure that only trusted or compliant devices from registered users access the network. Based on the user's or device's contextual identity, Cisco ISE sends rules for highly secure access to the network point of entry, so IT is assured of consistent policy enforcement from wherever the user or device is trying to access the network.
Streamlined guest experiences	Cisco ISE offers out-of-the-box simplicity for guest administration and onboarding. Administrators can customize guest portals in minutes through the use of dynamic visual tools that offer real-time previews of the portal screens and steps a guest will experience in order to demonstrate exactly how changes to settings will affect their users. Cisco ISE offers full customization of guest pages - including advertisements, banners, themes, and branding - full management of guest accounts and expirations, and complete auditing of guest accounts and activity across your network. Supporting every possible type of guest workflow - from hotspot to employee-sponsored guest access with SMS confirmation - Cisco ISE makes guest access easy.
Self-service device onboarding	Cisco ISE gives the IT staff flexibility in deciding how to implement an enterprise's bring-your-own-device (BYOD) or guest policies. Cisco ISE provides a self-service registration portal for users to register and provision new devices according to the business policies defined by IT. This permits IT to get the automated device provisioning, profiling, and posturing it needs to comply with security policies while keeping it extremely simple for employees to get their devices onto the network without requiring assistance from IT.
Security Compliance	A single management console simplifies policy creation, visibility, and reporting across all company networks, which makes it easy to validate compliance for audits, regulatory requirements, and mandated federal guidelines for IEEE 802.1X standards.
Automated device compliance checks	Cisco ISE provides device posture check and remediation options using the Cisco AnyConnect® 4.0 Unified Agent, which also provides advanced VPN services for desktop and laptop checks as well as integrations with market-leading enterprise mobility management (EMM) solutions for mobile devices. This capability helps to ensure that a user's device is both secure and policy compliant.
Dependable anywhere access	Cisco ISE provisions policy on the network access device in real time, so mobile or remote users can get the same consistent access to their services from wired and wireless connections.
Operational efficiency	Onboarding and security automation, central policy control, visibility, troubleshooting, and integration with Cisco Prime™ solutions helps ensure that IT and the help desk will spend far less time on user and network security fixes.
Embedded enforcement	Device-sensing capabilities are built into most Cisco switches and wireless controllers to extend profiling networkwide at the point of entry and without the costs and management of overlay appliances or infrastructure replacement.
Extension of policy from access into the data center with Cisco TrustSec® policy networking	Cisco ISE is the policy management point for the unique Cisco TrustSec network technology, which provides policy-defined network segmentation to take the complexity out of network security. Cisco TrustSec technology makes it simple for customers to logically and dynamically segment their network based on business rules using role-based access policy instead of managing multiple VLANs or changing network architecture, thereby simplifying highly secure access across an ever-changing expanded network.
Multivendor infrastructure support	Cisco ISE interoperates with multivendor infrastructure (for example, switches and wireless access points) that is compliant with RADIUS and IEEE 802.1X standards. Cisco and its partners offer best-practice guidelines as well as detailed, hands-on design guidance. Enterprise customers use Cisco ISE with network infrastructure designed by Cisco along with Cisco TrustSec technology to get even greater intelligence and enhanced visibility out of their networks.
Cisco pxGrid context sharing	Cisco ISE collects dynamic contextual data from throughout the network and uses Cisco 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 API, Cisco ISE network and security partners use this data in order to improve their own network access capabilities and accelerate their solutions' capabilities to identify, mitigate, and remediate network threats.

Cisco ISE Advantage	
Broad, integrated partner Ecosystem	Cisco ISE boasts one of the largest partner ecosystems. Partners use Cisco 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 (TD) all take advantage of the deep contextual identity awareness that Cisco ISE provides to address many more use cases than they could alone and subsequently undertake their functions even more effectively. With Cisco ISE, partner platforms can reach deep into the Cisco network infrastructure and implement network actions on users and devices (for example, quarantining smartphones or laptops and blocking network access).

The Cisco 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. Cisco ISE features and benefits are shown in Table 2.

Table 2. Features and Benefits

Feature	Benefit
Business policy enforcement	Provides a rules-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 Active Directory, LDAP, RADIUS, RSA 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's TrustSec technology-enabled network devices.
Guest lifecycle management	Provides an all-new, streamlined experience for enabling and customizing guest network access. With built-in support for hotspot, sponsored, self-service, and numerous other access workflows, ISE makes it easy to create corporate-branded guest experiences, with ads 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 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. By streamlining device onboarding, this creates fewer IT help desk cases along with more secure access and an easier, more transparent experience for users.
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), and EAP-Transport Layer Security (TLS). Cisco ISE is the only RADIUS server to support EAP-Chaining of machine and user credentials.
Internal certificate authority	Offers organizations an easy-to-deploy internal certificate authority within Cisco ISE to simplify certificate management for personal devices without adding the significant complexity of an external certificate authority application. Cisco ISE offers a single console to manage endpoints and their certificates with the ability 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 and subordinate (that is, with your existing enterprise PKI) deployments.
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 administrative-defined identities when endpoints connect to the network. Administrators can also associate endpoint-specific authorization policies based on device type. Cisco ISE 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 Cisco Catalyst switches is a subset of Cisco ISE's sensing technology. This capability allows the switch to quickly collect endpoint attribute information and then, using standard RADIUS, pass this information to Cisco ISE for endpoint classification and policy-based enforcement. This switch-based sensing promotes efficient and distributed collection of endpoint information for increased scalability, deployability, and time to classification.

Feature	Benefit
Device profile feed service	The industry-first device profile feed service available in Cisco ISE supports its out-of-the-box profiling technology by providing automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. The feed service 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 now have the capability 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 by the IT administrators.
Endpoint posture	Verifies endpoint posture assessment for PCs and mobile devices connecting to the network. Works through either a persistent client-based agent or a temporal web agent to validate that an endpoint is conforming 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.), and applications. Cisco ISE also supports the auto-remediation of PC clients as well as periodic reassessments to make sure the endpoint is not in violation of company policies.
Cisco pxGrid and ISE ecosystem	Cisco pxGrid is a robust context-sharing platform within Cisco ISE that delivers a deeper level of contextual data, collected by Cisco ISE, to external and internal ecosystem partner solutions in order to accelerate these solutions' capabilities across the network. From endpoint vulnerability assessment to web single sign-on, the list of Cisco ISE ecosystem partners who are taking advantage of the simple unified framework continues to expand.
ISE ecosystem: **EMM integration**	EMM integration enables Cisco ISE to connect with Cisco EMM technology partner solutions to help ensure that the mobile devices that are trying to connect to the network have previously registered with the EMM platform and are compliant with the enterprise policy. It can also help users remediate their devices. Compliance checks include, but are not limited to, checks for device encryption, pin-lock, and jail-broken status.
ISE ecosystem: **SIEM and TD**	Integration with Cisco ISE enables SIEM and TD partners to supplement their networkwide security event visibility with Cisco ISE's contextual information about user and device identities, network authorization levels, and security posture. This changes hunting down misbehaving devices on the network from a months-long forensic event to real-time visibility with security actions that can be taken directly from inside the administrator panel.
ISE ecosystem: **Control/SCADA operational and security policy integration**	Enables highly secure access and management of control and supervisory control and data acquisition (SCADA) network devices. Cisco ISE provides context and control for control and SCADA policy managers, leading to easier identification of rogue devices as well as faster remediation and isolation of the device in the event of compromise.
ISE ecosystem: **Simplified network troubleshooting and forensics**	Allows packet capture systems to use contextual data collected by Cisco ISE to associate users, devices, and user roles to the packet data captured. Because packet captures are often vital to threat and network issue investigations, linking the contextual data with packet capture simplifies network troubleshooting and accelerates forensic investigations.
ISE ecosystem: **Endpoint vulnerability remediation integration**	Knowing how and what to prioritize on a network vulnerability report is extremely difficult. Sharing contextual data from Cisco ISE with vulnerability reporting better identifies and prioritizes the endpoint vulnerabilities in need of investigation and helps users to take action in order to remediate quickly.
ISE ecosystem: **Risk-based, adaptive authentication and single sign-on**	Enables context-driven user authentication and web application authorization. Provides the capability to decrease and even eliminate authentication challenges entirely based on fine-grained policy created by a combination of federated identity, authentication risk factor, and contextual data provided by Cisco ISE. With the proliferation of mobile devices being used by employees to access business assets, user authentication - while vital for security - is cumbersome. This integration allows users to be transparently authenticated to business assets without repeated challenges while preventing access to cloud assets based on risk levels.
Extensive multiforest Active Directory support	Provides comprehensive authentication and authorization against multiforest Microsoft Active Directory (AD) domains. Can group multiple, disjointed domains into logical groups for simplified configuration of complex AD topologies to support ever-changing business environments. Also supports flexible identity rewriting rules to enable smooth transition and integration. Supports Microsoft AD 2003, 2008, 2008R2, 2012, 2012R2.
Endpoint protection service	Allows administrators to quickly take corrective action (quarantine, un-quarantine, or shut down) on risk-compromised endpoints within the network. This helps to reduce risk and increase security in the network.
Centralized management	Enables administrators to centrally configure and manage profiler, posture, guest, authentication, and authorization services in a single web-based GUI console, and greatly simplifies administration by providing integrated management services from a single pane of glass.

Feature	Benefit
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 ESX- or ESXi-based appliance. Both physical and virtual form factors can be used to create Cisco ISE clusters to serve larger organizations and provide the necessary scale, redundancy, and failover required of a critical enterprise business system.

Product Specifications

The two hardware options for Cisco ISE are outlined in Table 3.

Table 3. Cisco ISE Hardware Specifications

	Cisco Secure Network Server 3415 (Small)	Cisco Secure Network Server 3495 (Large)
Processor	1 x Intel® Xeon® Quad-Core 2.4-GHz E5-2609	2 x Intel Xeon Quad-Core 2.4-GHz E5-2609
Memory	16 GB	32 GB
Hard disk	1 x 600-GB 6-Gb SAS 10K RPM	2 x 600-GB 6-Gb SAS 10K RPM
RAID	No	Yes (RAID 1)
CD/DVD-ROM drive	No	No
Network Connectivity		
Ethernet NICs	4 x Integrated Gigabit NICs	4 x Integrated Gigabit NICs
10/100/1000BASE-TX cable support	Category 5 UTP up to 328 ft. (100 m)	Category 5 UTP up to 328 ft. (100 m)
Secure Sockets Layer (SSL) accelerator card	None	Cavium CN1620-400-NHB-G
Interfaces		
Front panel connector	1 x KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)	1 x KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)
Additional rear connectors	Additional interfaces including a VGA video port, 2 USB 2.0 ports, an RJ45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports	Additional interfaces including a VGA video port, 2 USB 2.0 ports, an RJ45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports
System Unit		
Form factor	Rack-mount 1 rack unit (1RU)	Rack-mount 1RU
Weight	35.6 lb. (16.2 kg) 26.8 lb. (12.1 kg)	35 lb. (15.87 kg) fully configured
Dimensions (H x W x L)	1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)	1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)
Power supply	650W	Dual 650W (redundant)
Cooling fans	5	5
Temperature: Operating	32 to 104°F (0 to 40°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)	32 to 104°F (0 to 40°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Temperature: Nonoperating	-40 to 158°F (-40 to 70°C)	-40 to 158°F (-40 to 70°C)

Platform Support and Compatibility

Cisco ISE virtual appliances are supported on VMware ESX/ESXi 4.x and 5.x and should be run on hardware that equals or exceeds the configurations of the physical platforms listed in Table 3. At minimum, Cisco ISE requires the virtual target to have at least 4 GB of memory and at least 200 GB of hard drive space available.

Posture Assessment System Requirements

System requirements for the Cisco AnyConnect 4.0 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

Ordering Information

To place an order, visit the Cisco Ordering Home Page. To download the Cisco 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.

For More Information

For more information about the Cisco ISE and the Cisco TrustSec 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 C78-656174-09 10/14