Cisco Identity Services Engine (ISE)

The enterprise network today no longer sits within four secure walls. Employees today demand access to enterprise resources and their work via more mediums than ever before - by personal laptop from home networks, by tablets, and by smartphones. Mobility is a real game-changer, and enterprise networks need to grant access to this mobile workforce to keep workers productive. However, the shadow of security threats, data breaches, and the subsequent effects on the company still looms large.

At the same time, IT professionals are being tasked with supporting these enterprise mobility initiatives on tighter budgets and under the watchful eye of government, regulatory, and other compliance requirements. These requirements demand visibility into network access and tighter controls. Security point solutions are often distributed and deployed in larger numbers across the entire enterprise network - from wired to wireless to remote access. This is unsustainable.

Maintaining network security and operational efficiency in today's distributed enterprise networks demands technology that takes a more holistic approach to network access security:

- Accurate identification of every user and device
- Easy onboarding, provisioning, and securing of all devices
- Centralized, context-aware policy management to control user access - whoever, wherever, and from whatever device

The enterprise is evolving. The network must too. The Cisco Identity Services Engine helps IT professionals address these challenges… and succeed.

Product Overview

The Cisco Identity Services Engine (ISE) is an all-in-one enterprise policy control product that enables comprehensive secure wired, wireless, and VPN access. When operating in a network, ISE provides the following key features:

- **Rigorous identity verification:** ISE offers the industry's first device profiler to identify each device; match it to its user or function and other attributes, including time, location, and network; and create a contextual identity so IT can apply granular control over who and what is allowed on the network. An automated device feed service updates ISE in real time to ensure that new devices can be identified as soon as they are released to the market.

- **Extensive policy enforcement:** 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 ISE that differentiates guest users/devices versus registered users/devices. Guest users receive limited access across the entire network, while registered users receive their policy-designated access. Further, policy in ISE can ensure that only trusted or compliant devices from registered users access the network. Based on the user's or device's contextual identity, ISE sends secure access rules to the network point of access, so IT is assured of consistent policy enforcement from wherever the user or device is trying to access the network.
- **Security compliance:** A single dashboard simplifies policy creation, visibility, and reporting across all company networks, which makes it easy to validate compliance for audits, regulatory requirements, and mandated federal 802.1X guidelines.
- **Self-service device onboarding:** ISE gives IT flexibility in deciding how to implement an enterprise's BYOD or Guest policies. ISE provides a self-service registration portal for users to register and provision new devices - according to the business policies defined by IT - automatically. 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 IT's help.
- **Automated device compliance checks:** Provides device posture check and remediation options, including integrations with many market-leading mobile device management (MDM) solutions as well as the lightweight Cisco NAC Client for desktop/laptop checks. Users can easily keep their devices secure and policy-compliant.
- **Dependable anywhere access:** 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 as they would from wired and wireless, from wherever they enter the network.
- **Operational efficiency:** Onboarding and security automation, central policy control, visibility, troubleshooting and integration with Cisco Prime™ ensures that IT and the helpdesk 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 network-wide, without the costs and management of overlay appliances or infrastructure "rip and replace."
- **Extend policy from access into the datacenter with TrustSec policy networking:** ISE is the policy control point for Cisco TrustSec, unique network technology that provides policy-defined network segmentation to take the complexity out of network security. Cisco TrustSec makes it simple for customers to migrate their network infrastructure, thereby increasing the value of their ISE investment while ending the pain of excessive VLAN, ACL, and firewall rule administration.
- **Multivendor infrastructure support:** Cisco ISE interoperates with multivendor infrastructure (e.g., routers, switches, access points) that is 802.1X-compliant. Cisco partners and support offer best-practice guidelines as well as detailed, hands-on design guidance. Enterprise customers leverage ISE with Cisco-designed network infrastructure and TrustSec to get even greater intelligence and enhanced visibility out of their networks.

- **Broad solution ecosystem:** Integrated technology partners for Mobile Device Management (MDM), Security Information and Event Management (SIEM), and Threat Defense (TD) all leverage the deep, contextual identity awareness ISE provides to address far many more use cases than they could alone and subsequently undertake their functions even more effectively. With ISE, partner platforms can reach deep into the Cisco network infrastructure and execute network actions on users and devices - e.g., quarantining smartphones or laptops and blocking network access. The newly announced Cisco Platform Exchange Grid (pxGrid) is a unified, customizable method for two-way context sharing between ISE and other IT platforms to formulate more sophisticated network access policy.

Benefits

The Cisco Identity Services Engine provides comprehensive policy management, device onboarding, and enforcement for ensuring secure wired, wireless, and VPN access.

- Unsurpassed visibility into the network with extensive profiling capabilities to accurately identify and assess all users and devices connecting to the network.
- Exceptionally robust control to grant, limit, and quarantine network access in alignment with the company's appropriate business policy or the most pressing security needs, regulatory guidelines, and compliance requirements.
- Extensive, consistent policy enforcement via network access controls, MDM device security, and SIEM/TD threat mitigation in order to identify security threats and mitigate the spread of attacks on the network.
- Reduced operational costs through efficiency by leveraging the embedded sensing and enforcement in the existing network in conjunction with centralized policy control and network visibility to streamline efforts to secure access.

Table 1. Features and Benefits

Feature	Benefit
AAA protocols	Uses standard RADIUS protocol for authentication, authorization, and accounting (AAA).
Authentication protocols	Supports a wide range of authentication protocols, including PAP, MS-CHAP, Extensible Authentication Protocol (EAP)-MD5, Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (FAST), and EAP-Transport Layer Security (TLS).
Policy model	Offers 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.
Access control	Provides a range of access control options, including downloadable access control lists (dACLs), VLAN assignments, URL redirect, and Security Group Access (SGA) tagging using the advanced capabilities of Cisco's TrustSec-enabled network devices.
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. ISE collects endpoint attribute data via passive network telemetry, querying the actual endpoints, or alternatively from the Cisco infrastructure via device sensors on Cisco Catalyst® switches. The infrastructure-driven endpoint-sensing capability on Cisco 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 efficient distribution of endpoint information for increased scalability, deployability, and time to classification. The industry-first device feed service available in ISE provides regular, validated device profile updates for various IP-enabled devices from multiple vendors as well as a mechanism where partners can share their own customized profile information. Now, with all of this seamlessly delivered to administrators through this service, enterprises now have the capability to detect the latest devices when their users try to connect them to the network. This simplifies the task of keeping up with the hundreds of new devices coming out every week and reduces a significant amount of support by the IT administrators.

Feature	Benefit
Device onboarding	Allows users to interact with a self-service portal to onboard and register all types of devices, as well as make use of automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. This means fewer cases for IT staff and helpdesk personnel, more secure access, and a seamless user experience.
Guest lifecycle management	Enables full guest lifecycle management, whereby guest users can access the network for a limited time, either through administrator sponsorship or by self-signing via a guest portal. Allows administrators to customize portals and policies based on specific needs of the enterprise as well as track guest access across the network for security and compliance demands.
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. ISE also supports auto-remediation of PC clients as well as periodic reassessment to make sure the endpoint is not in violation of company policies.
Mobile device management (MDM) integration	MDM integration enables ISE to connect with Cisco MDM technology partner solutions to ensure that the mobile devices that are trying to connect to the network have previously registered with the MDM platform, are compliant with the enterprise policy, and can help users remediate their devices.
Security Information and Event Management (SIEM) and Threat Defense (TD) integration	Integration with Cisco ISE enables SIEM/TD partners to supplement their network wide security event visibility with 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.
Endpoint protection service	Allows administrators to quickly take corrective action (Quarantine, Un-Quarantine, or Shutdown) 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.
Monitoring and troubleshooting	Includes a built-in web console for monitoring, reporting, and troubleshooting to assist helpdesk 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 form 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 ISE are outlined in Table 2.

Table 2. ISE Hardware Specifications

	Cisco Secure Network Server 3415 (Small)	Cisco Secure Network Server 3495 (Large)
Processor	1 x Intel Xenon Quad-Core 2.4 GHz E5-2609	2 x Intel Xenon Quad-Core 2.4 GHz E5-2609
Memory	16 GB	32 GB
Hard disk	1 x 600GB 6Gb SAS 10K RPM	2 x 600GB 6Gb SAS 10K RPM
RAID	No	Yes (RAID 0+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	Cat 5 UTP up to 328 ft (100 m)	Cat 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

	Cisco Secure Network Server 3415 (Small)	Cisco Secure Network Server 3495 (Large)
System Unit		
Form factor	Rack-mount 1 RU	Rack-mount 1 RU
Weight	35.6 lbs (16.2 kg) 26.8 lbs (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℉ (0 to 40℃) (operating, sea level, no fan fail, no CPU throttling, turbo mode)	32 to 104℉ (0 to 40℃) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Temperature: Nonoperating	-40 to 158℉ (-40 to 70℃)	-40 to 158℉ (-40 to 70℃)
Compliance		
FIPS	Uses FIPS 140-2 Level 1 validated cryptographic modules	Uses FIPS 140-2 Level 1 validated cryptographic modules

Platform Support/Compatibility

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 2 below. At minimum, ISE requires the virtual target to have at least 4 GB of memory and at least 200 GB of hard drive space available. The virtual appliance is also FIPS 140-2 Level 1 compliant.

System Requirements

System requirements for the Cisco NAC Agent, used for posture assessment, are shown in Table 3.

Table 3. Cisco NAC Agent System Requirements

Feature	Minimum Requirement
Supported OS	Windows 8 Basic, Windows 8 Professional, Windows 8 Enterprise, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise, Windows Vista Home, Windows 7, Windows XP Professional, Windows XP Home, Windows XP Media Center Edition, Windows XP Tablet PC; Mac OS X (v10.5.x, v10.6.x, v10.7.x and v10.8.x)
Hard drive space	Minimum of 10 MB free hard drive space
Hardware	No minimum hardware requirements (works on various client machines)

Ordering Information

To place an order, visit the Cisco Ordering Home Page. To download the ISE software, visit the Cisco Software Center.

Service and Support

Cisco offers a wide range of service programs to accelerate your success. 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 to 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 Advanced Services.

Warranty information is found on at http://www.cisco.com/go/warranty. Licensing information is available at http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html.

For More Information

For more information about the Cisco Identity Services Engine (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 C78-656174-08 09/13