Data Sheet

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:

Secure business and context-based access per on your company policies. ISE can match users and endpoints and other attributes such as time, location, and access type or method, creating an all-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 use multiple mechanisms to enforce policy, including the Cisco TrustSec® solution' for software-defined segmentation.

Streamlined network visibility through a simple, flexible, and highly consumable interface. ISE now stores a history of all endpoints that have been on the network with the associated visibility. The Streamlined Visibility Wizard can quickly stand up a proof of value to demonstrate visibility into all the endpoints on a given network.

Extensive policy enforcement to define access rules easily and with great flexibility that meets your ever-changing business needs. All this can be done from a centralized location that distributes enforcement across the entire network and security infrastructure. 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 that provide multiple levels of access to your networks. Guests can use a coffee-shop hotspot, self-service registered access, or sponsored access to get to specific resources. Dynamic visual tools offer real-time previews of the portal screens and the steps that a user experiences. You can see how changes affect the settings in sponsored guest accounts, self-registrations, and SMS and email confirmations of access. Deployment is quick and easy with the ISE Wireless Guest Setup Guide.

Self-service device onboarding to implement 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 can get the automated device provisioning, profiling, and posturing it needs to comply with security policies. At the same time, employees can get their devices onto the network without requiring IT assistance.

A single management console for simpler 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 for device-posture checks and remediation options using the Cisco AnyConnect® Unified Agent. The AnyConnect® agent also provides advanced VPN services for desktop and laptop checks. ISE can also be integrated 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 user and device details that make up the dynamic contextual data from 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 technology partner solutions. 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.

Access to the Technology Partner Community, which includes technology partners for MDM/EMM vendors, security information and event management (SIEM), and threat defense.

Features and Benefits

Cisco ISE empowers organizations in a number of ways (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.
Business-policy enforcement	• Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. Also provides the ability to create fine-grained policies by pulling attributes from predefined dictionaries. • Includes attributes such as user and endpoint identity, posture validation, authentication protocols, profiling identity, and other external attribute sources. These 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 supports Open Database Connectivity (ODBC).
Access control	• Provides a range of access control options, including downloadable access control lists (dACLs), VLAN assignments, URL redirections, named ACLs, and security group tag (SGT) using the advanced capabilities of network devices enabled with Cisco TrustSec technology.
Secure supplicant-less network access with Easy Connect	• Provides the ability to swiftly roll out highly secure network access without configuring endpoints for authentication and authorization. • Derives authentication and authorization from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
Source-Group Tag Exchange Protocol (SXP) support	• Acts 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. • Bridges over the segments that are not compliant with Cisco TrustSec policies to 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. • 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 your network for security and compliance demands and full guest auditing. Time limits, account expirations, and SMS verification offer additional security controls.

Feature	Benefit
Streamlined device onboarding	• Offers automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. This reduces IT help desk cases along with providing more secure access and 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 to enroll mobile devices and help ensure that they are compliant with access policy.
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 TACACS+ protocol to authenticate, authorize, and audit users when they access devices that support the TACACS+ protocol, such as network devices and servers. • Grants users 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. • 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 to simplify certificate management for devices. There is no need to add the significant complexity of an external certificate authority application. • Provides a single console to manage endpoints and their certificates. Certificate status is checked through the standards-based Online Certificate Status Protocol (OCSP). Certificate revocation is automatic. • Supports standalone deployments 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 these devices 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. • Creates custom device templates to automatically detect, classify, and associate administration-defined identities when endpoints connect to the network. • Helps to associate endpoint-specific authorization policies based on device type. • Collects endpoint attribute data with passive network monitoring and telemetry. It queries the actual endpoints or, alternatively, the Cisco infrastructure using device sensors on Cisco Catalyst® switches.
Device-profile feed service	• Delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors. It detects all the newest devices and simplifies the task of keeping up with them. • Offers a mechanism where partners and customers can share their customized profile information to be vetted by Cisco and redistributed.
Endpoint posture service	• Performs endpoint posture assessment on PCs and mobile devices connecting to the network. • Works through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM vendors system to validate that an endpoint conforms to appropriate compliance policies. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patches, 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, USB attached media and so on. • 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. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: Microsoft Windows 7, 8, or 10 (32-bit or 64-bit) and Mac OS X 10.7, 10.8, 10.9, or 10.11.
Extensive multi-forest Active Directory support	• Provides comprehensive authentication and authorization against multi-forest Microsoft Active Directory domains. • Groups multiple disjointed domains into logical groups. Configurations of complex Active Directory topologies are simplified to support ever-changing business environments. • Includes flexible identity rewriting rules to smooth the solution's transition and integration. • Supports Microsoft Active Directory 2003, 2008, 2008R2, 2012, and 2012R2.
Cisco Rapid Threat Containment	• Takes network mitigation and investigation actions in response to security events. • Integrates Cisco ISE and Cisco security technology partner solutions in a broad variety of technology areas. • Uses Cisco pxGrid as a highly scalable IT clearinghouse for multiple security tools to communicate with each other in real time, automatically.

Feature	Benefit
Monitoring and troubleshooting	• Offers a built-in web console for monitoring, reporting, and troubleshooting to assist help desk and network operators in quickly identifying and resolving issues. • Provides robust historical and real-time reporting for all services. Logs all activities 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. 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 is available as a physical or virtual appliance. Both physical and virtual form factors can be used to create ISE clusters to serve larger organizations and provide the scale, redundancy, and failover required 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.

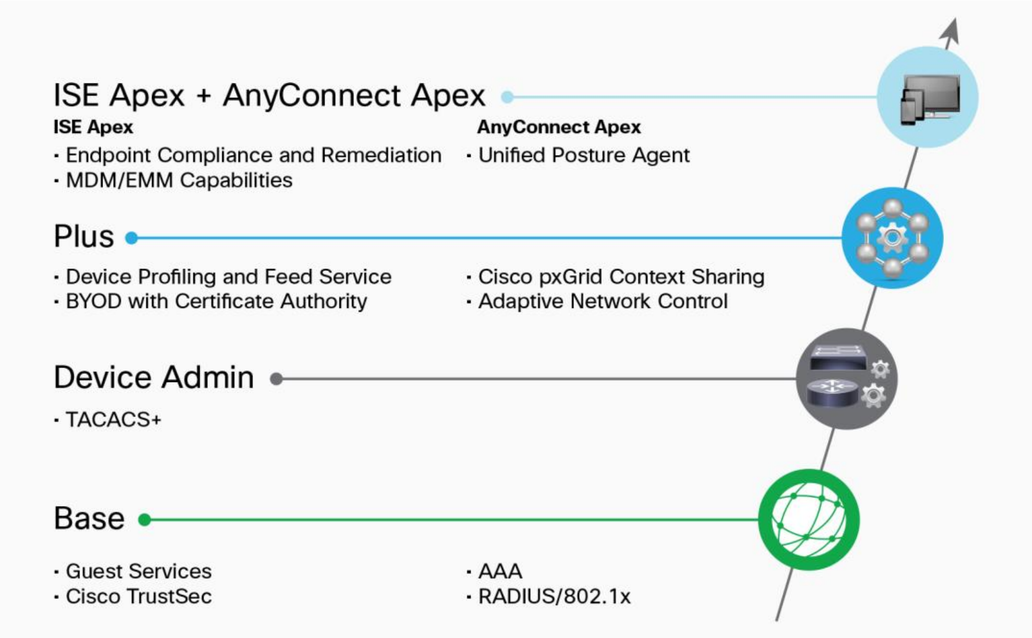
For physical platform support of ISE, please refer to the Cisco Secure Network Server Data Sheet.

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 on 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


ISE Apex + AnyConnect Apex
ISE Apex
· Endpoint Compliance and Remediation
· MDM/EMM Capabilities
AnyConnect Apex
· Unified Posture Agent
Plus
· Device Profiling and Feed Service
· BYOD with Certificate Authority
· Cisco pxGrid Context Sharing
· Adaptive Network Control
Device Admin
· TACACS+
Base
· Guest Services
· Cisco TrustSec
· AAA
· RADIUS/802.1x

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.

Printed in USA

C78-656174-13 08/16