Cisco Identity Services Engine

Contents

Product overview

The Cisco® Identity Services Engine (ISE) is the industry's only complete Network Access Control (NAC) solution but it's more than that. Cisco ISE is the bedrock of a zero trust solution. Zero trust is a solution that helps enable secure access for users and devices and within apps, across networks, and clouds. Customers should embed zero trust across the fabric of their multi-environment IT for a user experience without compromise.

If a customer isn't running Cisco ISE, then that network is not getting the full zero trust experience. Cracks can form and bad actors can exploit those cracks, putting data and business in a compromising position.

Teams gain agility with zero trust provisioning and flexibility in automating their environment through the entire life cycle of managing Cisco ISE. With Cisco ISE as the centerpiece for zero trust access to the workplace (self managed infrastructure), organizations are lowering risk, protecting the integrity of their business, and accelerating secure network access across the distributed network.

Cisco ISE, provides customers with the ability to see users and devices, control access across wired, wireless VPN, and 5G connections to the corporate network.

Cisco ISE powers security resilience with the flexibility and choice required to host Cisco software as workloads in multiple clouds beyond on premises support and maintain business continuity through uncertainty. This allows customers to gain a more modernized approach to deploying NAC services from the cloud. When moving from managing infrastructure in a box to leveraging Infrastructure-as-Code (IaC) across hybrid deployments.

Customer Advantages

Cisco ISE offers a comprehensive solution to build, manage and integrate network access security to your ecosystem of security applications. You gain many advantages when ISE is deployed, including:

- Highly secure business and context-based access based on your company policies. Cisco ISE works with network devices to create an all-encompassing contextual identity with attributes such as user, time, device, device posture, location, threat, vulnerability, and access type. This identity can be used to enforce a highly secure access policy 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. Cisco ISE uses multiple mechanisms to enforce policy, including Cisco Security Group software-defined segmentation.
- Streamlined network visibility through a simple, flexible, and highly consumable interface. Cisco 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. All of these insights go into all network endpoints and devices that are connecting; providing visibility with context needed to assure device compliance.
- Threat Containment turns the network into the defender, and we are closing down access, removing the endpoint form the network completely. However, Cisco ISE does not block or prevent a threat from gaining access. And this level of protection can be automated with integration through pxGrid to give passive security the intelligence and analytics solutions it needs to become an active arm of defense.
- Network Segmentation is important within balancing business objectives and maintaining protection to limit organization risks. With Cisco ISE building security directly into the network, it dramatically reduces the attack surface, the scope of compliance and limits the lateral movement of malware to contain threats.

- Extensive and Flexible policy enforcement that defines easy, flexible access rules that meet ever-changing business requirements. This is 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 context to define intent based policies that are easy to understand. Cisco Scalable (or Security) Group Tags (SGT) allow organizations to base access control on business rules and not IP addresses or network hierarchy. This reduces operational complexity and helps to efficiently manage policies across your enterprise. These SGTs are building blocks for policies that can be defined in Cisco ISE and easily be shared to a non-Cisco infrastructure for creating their own security policies. These SGTs give users and endpoints access, on a least privilege policy, that is constantly maintained as assets and resources move across domains. Managing switch, router, and firewall rules becomes easier and has shown to help reduce IT Operations by 80% and increase time to implement changes by 98%.
- 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. Cisco 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.
- Security Eco-system Integrations: Cisco ISE offers over 100+ integrations with Cisco and non-Cisco eco-system products to enable security products to share data and work together to find threats faster by automatically removing infected endpoints and protecting critical data.
- 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.

Cisco DNA Center Integration

Cisco DNA Center is the foundational controller and analytics platform at the heart of Cisco's Intent based Network. Cisco DNA Center simplifies network management and allows one to quickly set up various Cisco ISE services such as Guest and BYOD quickly and easily throughout the network, Cisco 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. Cisco 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. Security Group Policy (based on groups) 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 Cisco Secure Client (formerly Anyconnect agent), Temporal and Agentless options with custom scripts support. Cisco Secure Client Temporal and Agentless are two different ways to gather posture from endpoints beyond a full agent. Agentless option is supported from ISE 3.0 onwards Io Cisco Secure client also provide 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 context and to contain threats 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
Common Policy	• Cisco ISE is the hub of Common Policy. • A multi-domained, multi-siloed network can be difficult for each part of the network to speak and understand the same language. For example in the Application Centric Infrastructure (ACI) world, they're not using SGT, they're using EPGs and ESGs. Thanks to Common Policy, Cisco ISE is the universal translator that allows for each part of the network to understand each other. • A network powered by Common Policy automation will handle the data center, cloud and campus all in one, bringing the next gen architecture together with legacy architecture allowing the ability to share Security Group Tags (SGTs), consume End Point Groups (EPG) and ESGs from an ACI. • Common Policy extends zero trust-based access to Cisco and other network domains by gathering context, then storing and sharing it with other controllers. • With 70% of the devices on the network being IoT, Common Policy is the best way to reach those devices to make sure that they are all consistently complying with the policies instituted by Cisco ISE. There is more visibility provided to these IoT devices through secure communication from the device to the network, allowing for an organization to streamline policy and operations.
Reboot Reduction Time	• The rebooting of ISE will now take a shorter time, in many cases, about five minutes. • Typically a reboot of Cisco ISE is usually called for when upgrading software or adding new services or reauthorizing new certifications and can take upwards of 20 minutes. • Thanks to improvements made in reboot reduction time, customers will see a reboot reduction savings of 40%.
Active Directory Site Awareness	• Customers have more control over Domain Controllers (DC) and in which priority the Policy Service Node (PSN) is selected. • There are situations when a domain controller is unavailable, and Cisco ISE will automatically choose the next DC available. When the original domain controller comes back online, the current protocol is for Cisco ISE to stick with the current DC and not return to the original one selected. • In these cases we are allowing the flexibility for our customers to override the Cisco ISE selection algorithm. This provides peace of mind for customers who will be safe in the knowledge that the domain controller that they chose originally is the one that will be connected once the DC is restored.

Feature	Benefit
Dynamic Reauthentication Times	• A time-saving feature that allows the administrator to set up a temporary policy where a group of devices are placed in a particular bucket. • This bucket is “dumped” or removed from the network at a particular time that is set by the administrator. This allows the administrator to set up a designated time period prior for the end devices to join the network and expel them concurrently once that designated period is completed. • This provides a sort of temporary segmentation that continues the Cisco ISE tradition of least privilege where users are allowed to access only the information that they need and no more.
pxGrid Direct enhancements	• There are two new enhancements that will strengthen the synergy between Cisco ISE and pxGrid. • Firstly, customers can immediately synchronize data from pxGrid Direct Connectors. Prior to this release Cisco ISE can synchronize a full data base update once a week or less (minimum once every 12 hours), with incremental updates every day (incremental updates minimum once every hour). With immediate synchronization, there is no longer a need to wait until once a week or the end of the day. Any and all updates can be made immediately without waiting. • Secondly, the server has been granted the ability to push updates immediately to Cisco ISE. This new feature is called pxGrid Direct Push and will allow a continuous synchronization of Cisco ISE without any lag. In other words, whenever a single record is adjusted, the server will send the change immediately to Cisco ISE.
Protected Access Credentials (PAC) less communication	• A PAC is a credential generated by Cisco that can be sent to Cisco ISE that allows for TrustSec devices to be authenticated. When the device needs to be identified later, the PAC file can be sent again. • Support of a PAC-less communication was developed and supported by Cisco ISE in efforts to make the network run smoother. • When a device that supports PAC-less communication connects to a network, newer switches and network devices will now understand whether this device supports PAC. The determination will then be sent to Cisco ISE. • If PAC is not supported, Cisco ISE will recognize this and results in a PAC-less double check. Older devices that still use PAC will still be covered and behave the way that it always has.
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	• Provides a rule-based, attribute-driven policy model for flexible and business-relevant access control policies. • Includes attributes such as user and endpoint identity, posture validation, authentication protocols, device 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 (On-Prem or Azure AD), Lightweight Directory Access Protocol (LDAP), RADIUS, RSA One-Time Password (OTP), certificate authorities for both authentication and authorization, Open Database Connectivity (ODBC) and SAML providers.
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 Group ACLs (SGACLs) with Cisco Security Group technology.

Feature	Benefit
Split Upgrades	• Upgrading to the newest version of Cisco ISE is now less complex as files are downloaded before upgrades and prechecks are done. • Split Upgrades shortens the upgrade process and becomes more predictable and runs without network interruption • Since the upgrade nodes are split into two distinct groups—allowing for the updates to be split—customers will no longer have to worry about a lack of network functionality when they see a Cisco ISE update request.
Cisco ISE Ciphers Control	• Provides the ability to edit a list of ciphers that can be disabled so that customers can be compliant with the latest security standards. • Customers that need to be compliant with the latest security standards now have an option to select which ciphers should be ignored using the authentication.
Controlled Application Restart	• Saves customers time by streamlining network security. • This feature allows for the ability to control the replacement of the ISE administrative certificate allowing them the ability to plan for maintenance once their current certificate expires. • Maintenance needed to update the certification—which can take upwards of 30 minutes per certificate—can be scheduled for the middle of the night, when network use is low, saving both time and resources.
New TPM Chip (for supported hardware)	• Found on the new SNS-3700 models and in some virtual environments, the TPM chip is a dedicated chip where sensitive information can be stored. • Thanks to chip improvements, data stored here can be more difficult to access thus providing a more secure location for information storage.
AI/ML Profiling and multifactor classification (MFC)	• Customers are able to quickly identify clusters of identical unknown endpoints via a cloud-based ML engine • Devices can be reviewed by proposed profiling policies via the ML engine and put into four distinct buckets • Grouping of unknown endpoints becomes much easier as a networking admin can create a profile and rules for that particular group of unknown devices.
Wi-Fi Edge Analytics	• Cisco-only feature that allows network admins to mine data from Apple, Intel and Samsung devices. • This allows for an improvement in device profiling. • This additional data allows the creation of a more precise profile which enables a safer network.
Secure supplicant-less network access with Easy Connect	• Provides the ability to swiftly roll out highly secure network access By deriving authentication and authorization from login information across application layers, allowing user access without requiring an 802.1X supplicant to exist on the endpoint.
Cisco Security Group Policy	• Cisco Security Group Policy software-defined segmentation provides simpler segmentation through the use of Security Group Tags (SGT). It is an open technology in IETF, available within OpenDaylight, and supported on third-party and Cisco platforms. • ISE is the Segmentation controller which simplifies the management of switch, router, wireless, and firewall rules. • Group information propagates SGTs across network devices in the data path (inline tagging) or via Security group tag exchange protocol (SXP) IP-to-SGT binding information where devices do not have the capability to tag packets with SGTs.

Feature	Benefit
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 and TEAP. • 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.

Feature	Benefit
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 PINlock, 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 and later ◦ Mac OS X 10.13 and later ◦ Linux (RedHat Enterprise Linux, SUSE Linux Enterprise Service and Ubuntu)
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, 2016, and 2019.
Monitoring and troubleshooting	• Offers a built-in help 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.
Upgrade Readiness Tool (URT)	• Runs pre-upgrade checks • Simulates an actual upgrade • Provides guidance on upgrade success/failure • Provide guidance on upgrade time per node • Constantly Updated and Learning
IPv6 Support	• IPv6 for RADIUS and TACACS+ based network devices. • ISE can be managed via IPv6 management network. This includes: Connecting to ISE management interface (Web or CLI), Connecting to Active Directory, Sending syslog messages, Sending SNMP traps, REST API over IPv6, DNS resolution and NTP time synchronization.

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 introduced 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. Additionally, pxGrid is used to share IP-to-SGT information about endpoints allowing security products to apply Security Group access control using SGTs. With ISE 3.1, pxGrid 1.0 connections are no longer supported.

As an extension to the prior Cisco ISE 3.2 release, with the Cisco ISE 3.3 release pxGrid Direct Visibility has improved visibility of attributes gathered from external databases such as ServiceNow. This allows network administrators to easily view the content gathered by any endpoints across all of the different sources. This provides a lot of information on the endpoints, users and devices, including which apps are running over the network and the different attributes– such as the device owner and type and whether the device is operational.

Customers can then take this data and use it to more efficiently run their network, such as creating an ISE authorization policy.

Cisco Rapid Threat Containment (RTC) 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 network.

ISE Virtual appliances are supported on the following on-premise and cloud platforms:

- VMware ESXi 6.5, 6.7 and 7.x
- KVM on Red Hat 7.x
- Microsoft Hyper-V on Microsoft Windows Server 2012R2 and later
- Nutanix AHV
- VMware Cloud
- Amazon Web Services
- Azure Web Services

For ISE physical appliance details please refer to the Cisco Secure Network Server datasheet.

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.

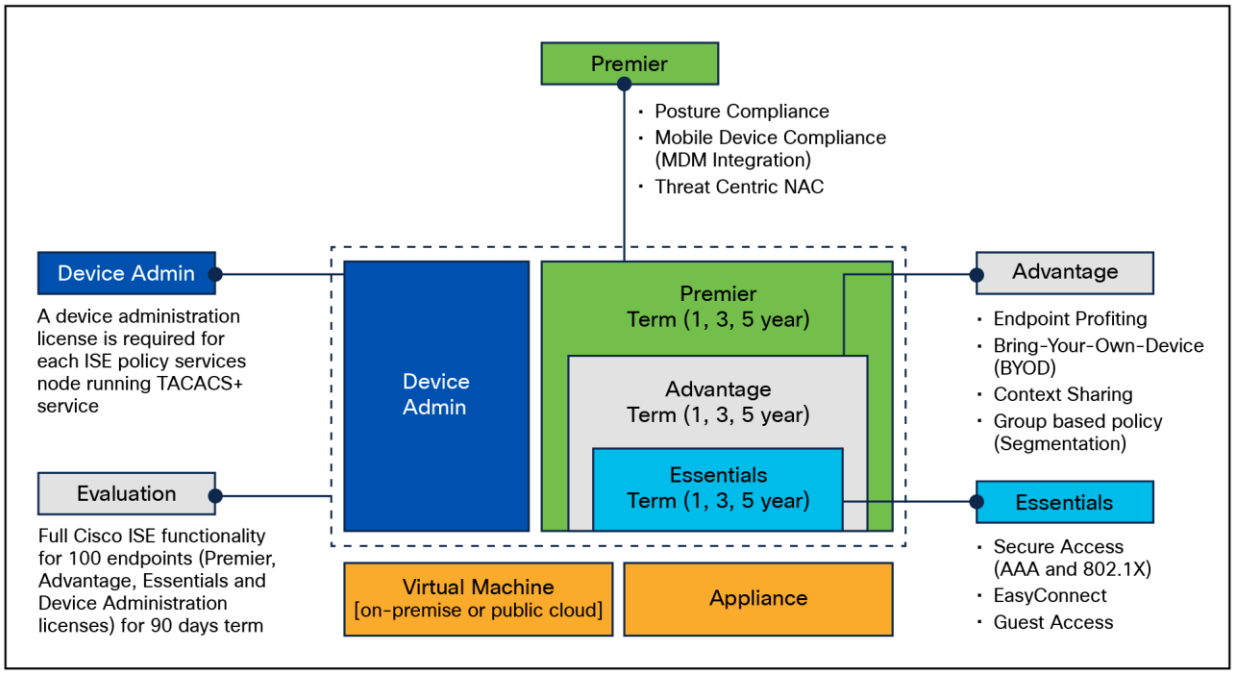

Figure 1.
Cisco ISE license packages

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

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation, and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services, and complementary third-party equipment in easy, predictable payments. Learn more.

How to buy

To view buying options and speak with a Cisco sales representative, visit https://www.cisco.com/c/en/us/buy.html.

For more information

For more information about the Cisco ISE solution, visit https://www.cisco.com/site/us/en/products/security/identityservices-engine/index.html or contact your local account representative.

Document history

New or revised topic	Described in	Date
Identity Service Engine	Page 3 Customer Advantages Page 5 Features and Benefits (Table 1)	May, 2024

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 C78-3740517-01 06/24