# Cisco Identity Services Engine (ISE)

## Introduction

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.

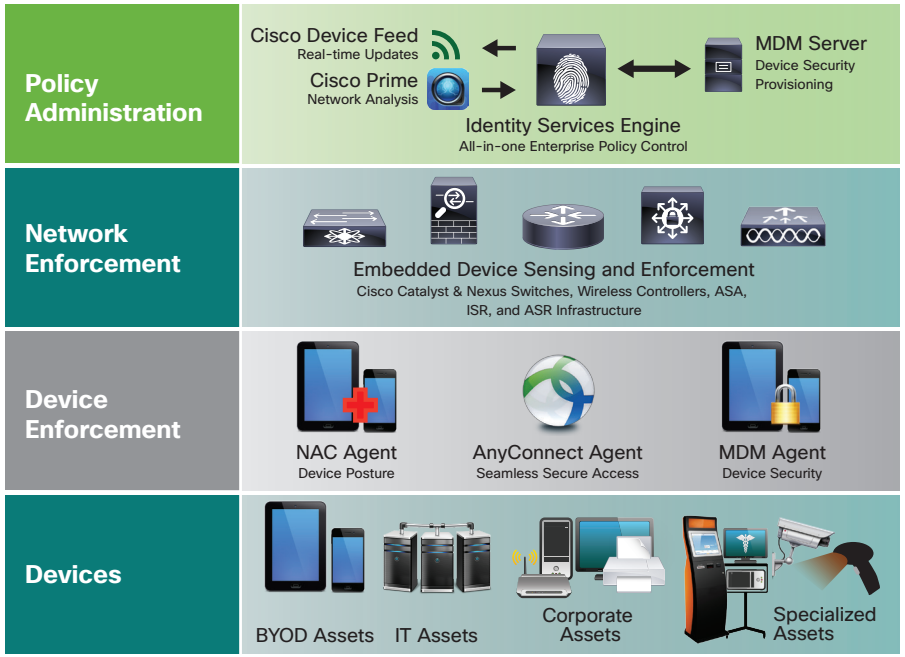
At the same time, IT professionals are being tasked with supporting these enterprise mobility initiatives on tighter budgets and under the watchful eye of government and other compliance requirements. These requirements demand visibility into network access and tighter controls. Security point solutions 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 new 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, or ISE, helps IT professionals conquer enterprise mobility challenges and secure the evolving network – now and in the future.

**Figure 1.** Components of a Cisco Identity Services Engine (ISE) Deployment




## Product Overview

Cisco ISE offers a centralized control point for comprehensive policy management and enforcement in a single RADIUS-based product from Cisco – the world leader in network security. It starts with rigorous identity enforcement that includes the industry-first automatic device feed service to keep the profiling engine up-to-date with the latest smartphones, tablets, laptops, and even specialized network-enabled devices used in retail, healthcare, and manufacturing industries.

ISE offers an easy onboarding experience for BYOD (bring your own device) and guest workers, so that personal devices can be secured and granted access via a simple self-service portal and meet security policy. For comprehensive device security, ISE offers a seamless integration with market-leading Mobile Device Management (MDM) platforms for policy compliance. Even better, ISE can be provisioned to give workers the option to provision MDM on their device for full company access or refuse MDM and receive only Internet access.

Cisco ISE is designed to be a strategic, enterprise-class product in the network. To that end, Cisco ISE is designed to support up to 250,000 active, concurrent endpoints – more than any other product in the marketplace – to ensure seamless onboarding, roaming, and network access control throughout a distributed enterprise network. ISE interoperates with multivendor infrastructure that is 802.1X-compliant. Finally, to make deployment even easier than before, Cisco ISE now includes bootstrap wizards to deploy across the enterprise in a "cookie-cutter" fashion. Cisco partners and support are highly trained and experienced, with some of the broadest and deepest knowledge in the industry. They have helpful guidelines and design guidance to leverage and are ready to work with you to ensure every deployment is of the utmost quality and efficacy.

Cisco ISE represents the future of context-aware access policy management across the new enterprise network – the borderless, distributed, mobile network. It's no wonder that Cisco ISE is the product of choice for well over 4,000 customers – including a number of Fortune 500, educational institutions, and government agencies. That number increases every day as more and more enterprises recognize that their network needs are evolving, and that ISE is the clear answer for unified policy management and enforcement in this era of enterprise mobility.

## Benefits

- 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 security compliance requirements and guidelines.
- 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.

## 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.
- **Industry-first device profile feed service:** Have a new smartphone? New network-enabled surveillance camera, printer, or heart monitor? Recognizing and profiling these devices was once a tedious task. Not anymore. ISE provides a device feed service that automatically receives updated profiles of the latest devices. ISE will know about the latest smartphone before the IT staff will. Community-sourced, vetted-by-Cisco, the device feed ensures that there will be no devices that escape network visibility.
- **Extensive policy enforcement:** ISE enables the organization to define access policy rules easily and dynamically to meet the ever-changing business requirement needs of the enterprise. For example, IT administrators can easily define policy in ISE that differentiates guest users/devices versus registered users/devices on the same network. Guest users receive limited access across the entire network, while registered users receive their policy-designated access.
- **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 and 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."
- **Broad solution ecosystem:** Companies use Mobile Data/Application Management (MDM/MAM) and Security Information and Event Management (SIEM) software platforms to ensure device security and monitor network behavior. Cisco has partnered with the best-of-breed vendors in MDM/MAM and SIEM and integrated their platforms into Cisco ISE. With ISE as the policy control point, partners gain added network identity and context. As a result, MDM/SIEM is more effective and is able to address ***far more security use cases than they could alone***. Customers gain enhanced visibility, stronger control, and greater certainty over the devices connecting to their networks.
- **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 easy 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.

## Deployment Components

The Identity Services Engine can use most Cisco network devices as device profiling sensors and access enforcement points. It is also capable of extending authentication services on most 802.1X-compliant devices, although profiling may require a specialized architectural design. Additional deployment components include Cisco NAC Agent, Cisco AnyConnect™, or the native 802.1X supplicant on the endpoint; Cisco partner MDM solutions, Cisco Catalyst® switches and Cisco wireless LAN controllers acting as policy enforcement points for the LAN; and Cisco Adaptive Security Appliances (ASA) for secure remote access. Cisco Identity Services Engine also integrates with directory services such as Microsoft Active Directory and Sun ONE Directory Server as policy information points.

## Packaging and Licensing

The Cisco Identity Services Engine is available as either a physical or virtual appliance. Licensing options allow customers to choose the functionality they need, based on the number of active endpoints on the network. Depending on environment and policies, existing ACS and NAC customers can consider migrating to ISE. ISE is the natural evolution of the endpoint access services currently provided by ACS and the NAC portfolio.


C45-654884-10 09/13