Cisco Identity Services Engine

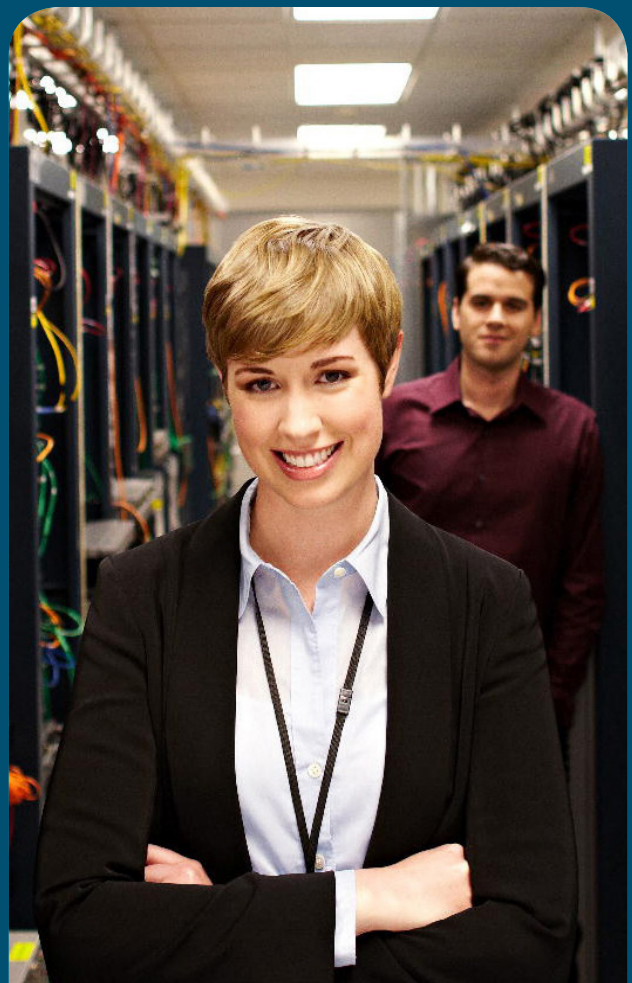
Secure and manage your evolving network

As mobility, digitization, and the Internet of Things (IoT) are changing the way we live and work, these trends are redefining the network by extending it to wherever employees and data travel.

Employees today demand access to work resources from more devices and through more outside networks than ever before. Businesses must support a proliferation of network-enabled devices even as a myriad of security threats and highly publicized data breaches demonstrate the importance of protecting access to the evolving enterprise network. And IoT devices are expanding exponentially and redefining industries such as manufacturing and healthcare.

Although this explosion of connected devices and the digitization of systems and services have produced significant value to customers, they are also leading to new challenges for constrained IT departments as they now must account for a larger attack surface and identify and remediate security threats or else risk allowing significant damage to the enterprise.

This increasing complexity requires a different approach to both manage and secure the evolving enterprise network. It's called the Cisco® Identity Services Engine (ISE).



Through its integrations with leading networking and threat defense solutions, its deep network visibility, and its secure access control capabilities, ISE safeguards your network, stops threats, and empowers your network security capabilities.

- **Accelerate Bring-Your-Own-Device (BYOD) and enterprise mobility**. ISE gives you an easy out-of-thebox setup. Use self-service device onboarding and management, internal device certificate management, and integrated Enterprise Mobility Management (EMM) partner software for device onboarding both on and off premises.
- **Construct a software-defined segmentation policy to contain network threats**. Use Cisco TrustSec technology to enforce role-based access control at the routing, switching, and firewall layer. Dynamically segment access without the complexity of multiple VLANs or the need to redesign the network.
- **Share user and device data with partner network and security solutions**. Improve their overall efficacy and accelerate the time to containment of network threats.
- **Automatically detect and contain threats** through integration with the Cisco Firepower® Management Center and 3rd party security partners. ISE can contain the infected endpoints for remediation, observation, or removal.

Narrow your exposure and reduce your risk

Getting ahead of threats requires thorough visibility and control. That means having deep visibility into the users, devices, and applications accessing your network. And it means gaining the dynamic control to make sure that only the right people with trusted devices get the right level of access to network services.

ISE simplifies the delivery of consistent, highly secure access control across wired, wireless, and VPN connections. With far-reaching, intelligent sensor and profiling capabilities, ISE can reach deep into the network to deliver superior visibility into who and what are accessing resources. Through the device profiler feed service, ISE delivers automatic updates of Cisco's validated device profiles for various IP-enabled devices from multiple vendors which simplifies the task of keeping an up-to-date library of the newest IP enabled devices.

ISE can implement Cisco TrustSec® policy for software-defined segmentation, which transforms the network from a simple conduit for data into a security enforcer that accelerates the time to detection and mitigates threats.

ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data with more than 50 integrated technology partner solutions. pxGrid is an Internet Engineering Task Force (IETF) standards-based way to accelerate your ability to identify, mitigate, and remediate security threats across your extended network. Access control is centralized and simplified to deliver vital business services more securely, enhance infrastructure security, enforce compliance, and streamline IT operations.

Next steps

To learn more about the Cisco ISE, visit https://www.cisco.com/go/ise or contact your local account representative.

C45-654884-17 04/18

Customer benefits

- **Enable Software-Defined Access (SDA)** by automating user access and highly secure end-to-end segmentation across a single network fabric. Cisco SDA is simpler to enable than other segmentation mechanisms such as VLANs, and policies stay consistent on the network regardless of the underlying infrastructure. The consistency in policy across the network simplifies segmentation, optimizes the use of resources, and fosters a more secure network.
- **Gain greater visibility and more accurate device** identification. Get additional user and endpoint visibility. Share this rich contextual information with other solutions on your network for a truly integrated experience.
- **Centralize and unify highly secure access control** based on business roles. Provide a consistent network access policy for end users whether they connect through a wired or wireless network or by VPN. Use multiple mechanisms to enforce policy, including Cisco TrustSec® software-defined segmentation. Cisco TrustSec security groups are based on business rules and not IP addresses or network hierarchy. These security groups give users access that is consistently maintained as resources move across domains. Managing switch, router, and firewall rules becomes easier.
- **Deploy robust guest experiences** that provide multiple levels of access to your network. Guests can use a coffee-shop hotspot, elf-service registered access, social login, or sponsored access to specific resources. Dynamic visual tools offer a real-time preview of the portal screen and the experience that a user would have when connecting.

Important ISE updates and enhancements allow:

- **Greater visibility of industrial IoT devices with IND integration:** Cisco's Industrial Network Director (IND) integrates with Cisco pxGrid (Platform Exchange Grid) technology to provide deep level of contextual visibility behind more than 300 industrial and 300 medical IoT device categories.
- **Improved pxGrid backward compatibility:** Simplify the integration with ISE in collecting context information and initiating ANC (Adaptive Network Control) actions.
- **Enhanced PCI Compliance:** Helps customers to meet the Payment Card Industry (PCI) Data Security compliance requirements by allowing them to disable TLS 1.0 and/or 1.1 and leave only TLS 1.2 version.
- **Efficent Cisco TrustSec Deployment:** ISE efficiently verifies Cisco TrustSec policies that are implemented throughout the network with improved troubleshooting for large scale IP-SGT deployments.