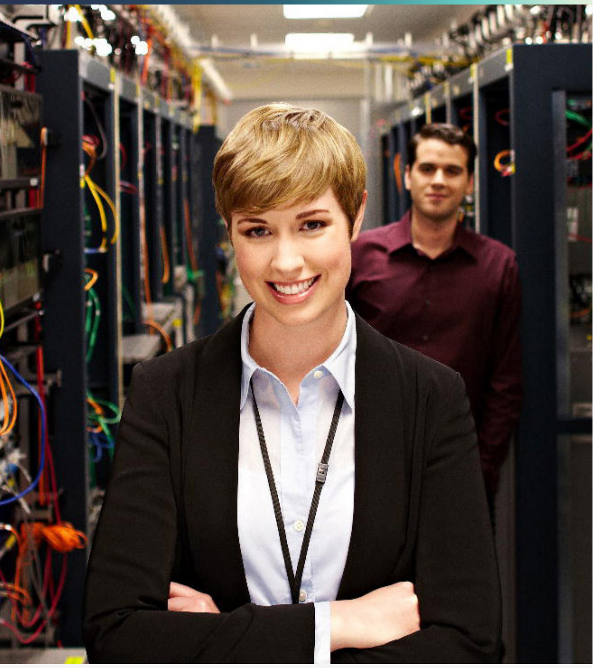
At-a-Glance



Benefits

- **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.
- **Gain greater visibility and more accurate device identification.** Device profiling and the device-profile feed service reduce the number of unknown endpoints.
- **Simplify guest experiences** for easier onboarding and administration. You can create fully customizable, branded mobile and desktop guest portals in minutes. Dynamic visual workflows let you easily manage the guest experience.

Cisco Identity Services Engine

Secure and Manage Your Evolving Network

The enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel. Employees today demand access to work resources from more devices and through more outside networks than ever before. Mobility, digitization, and the Internet of Things (IoT) are changing the way we live and work. 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.

As the modern network expands, so does the complexity of managing resources and disparate security solutions. Then factor in the ubiquitous connectivity of personal devices. The possibility that an already constrained IT staff may fail to identify and remediate security threats becomes serious.

A different approach is required to both manage and secure the evolving enterprise network. It's called the Cisco® Identity Services Engine (ISE).

Narrow Your Exposure and Reduce Your Risk

Get ahead of threats through 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. It can share vital contextual data using technology partner integrations. And it can implement Cisco TrustSec® policy for software-defined segmentation. Cisco ISE transforms the network from a simple conduit for data into a security enforcer that accelerates the time to detection and mitigates threats.

- **Accelerate bring-your-own-device (BYOD) and enterprise mobility.** ISE gives you an easy out-of-the-box 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.

Next Steps

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

- **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 contain threats** through integration with the Cisco Firepower® Management Center and technology partners. ISE can contain the infected endpoints for remediation, observation, or removal.

Important ISE updates and enhancements allow:

- **Visibility of rich user and device details.** Get additional user and endpoint visibility. Share this rich contextual information with other solutions on your network for a truly integrated experience.
- **Software-Defined Access (SDA).** User access policy is automated across a single network fabric with highly secure end-to-end segmentation. 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.
- **Deploy robust guest experiences** that provide multiple levels of access to your network. Guests can use a coffee-shop hotspot, self-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.

ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data with 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.

Through its integrations with leading networking and threat defense solutions, its deep network visibility, and its secure access control capabilities, ISE plays an integral role in the Rapid Threat Containment, network-as-a-sensor, and network-as-an-enforcer solutions that enable the Cisco Digital Network Architecture.