

Cisco Identity Services Engine



Introduction

Traditional corporate network boundaries and siloed services are a thing of the past. Today's networks must accommodate an ever-growing array of consumer IT devices while providing user-centric policy and enabling global collaboration. The Cisco TrustSec® architecture addresses this shift by using identity-based access policies to tell you who and what is connecting to your network, allowing IT to enable appropriate services without sacrificing control.

The Cisco® Identity Services Engine (ISE) focuses on the pervasive service enablement of Cisco TrustSec for borderless networks. The Identity Services Engine delivers all the necessary services required by enterprise networks—AAA, profiling, posture, and guest management—on a common platform. As a core component of the SecureX framework, Cisco Identity Services Engine provides a unified policy platform that ties organizational security policies to business components such as security and network infrastructure, user identity, resources and IT operational processes. Cisco ISE allows customers to create and manage centralized policies, while Cisco TrustSec delivers policies and enforcement through the network.

Overview

Cisco ISE is a context aware identity-based platform that gathers real-time information from the network, users, and devices. ISE then uses this information to make proactive governance decisions by enforcing policy across the network infrastructure utilizing built in standard based controls. Cisco ISE offers:

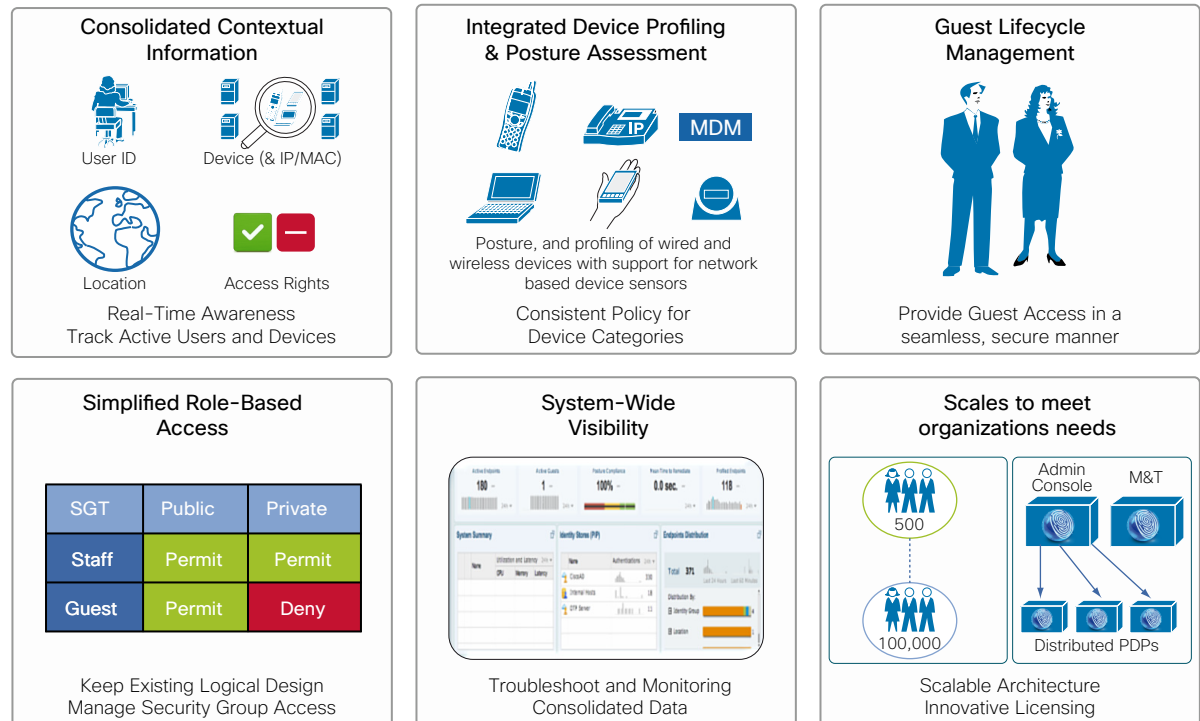
- **Security:** Secures your network by providing real-time visibility into and control over the users and devices on your network.

- **Compliance:** Enables effective corporate governance by creating consistent policy across an infrastructure.
- **Efficiency:** Helps increase IT and network staff productivity by automating traditionally labor-intensive tasks and streamlining service delivery.
- **Enablement:** Allows IT to support a range of new business initiatives, such as bring your own device (BYOD), through policy-enabled services.

Solution Highlights

- **Business-relevant policies:** Enables centralized, coordinated policy creation and consistent policy enforcement across the entire corporate infrastructure, from head office to branch office.
- **Systemwide operational visibility:** Discovers, assesses, and monitors users and endpoints and employs advanced troubleshooting capabilities to give IT teams complete visibility into who and what is on the corporate network.

Figure 1. Key Benefits of ISE





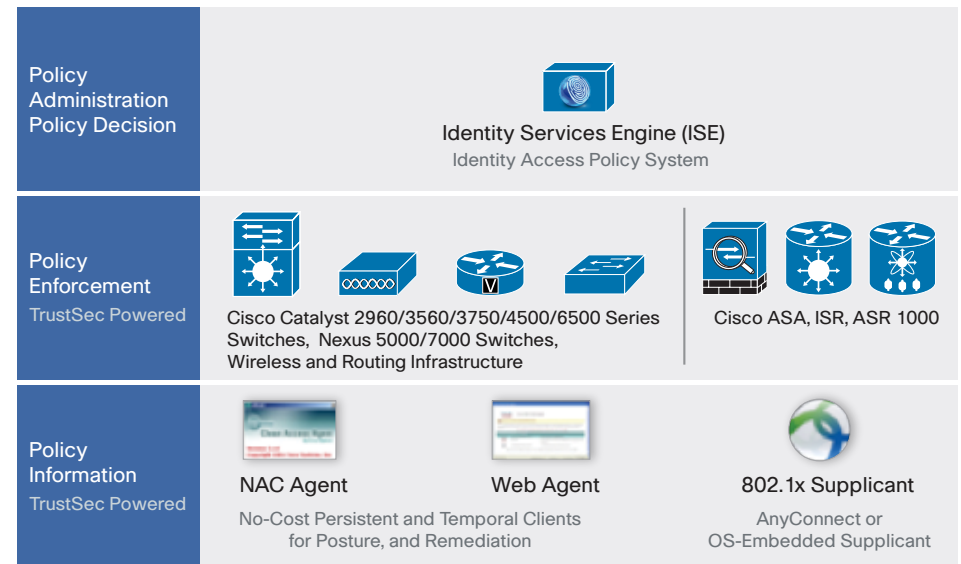
- **Context-aware enforcement:** Gathers information from users, devices, infrastructure, and network services to enable organizations to enforce contextual-based business policies across the network. The Cisco Identity Services Engine acts as the “single source of truth” for contextually rich identity attributes, including connection status, user and device identity, location, time, and endpoint health.
- **Highest Precision Device Profiling:** The combination of ISE based passive network probes and policy-driven active endpoint scanning working along side Cisco infrastructure based Device Sensor functionality gives IT the required endpoint fidelity and streamlined profiling capabilities needed for complete network awareness and automatic network enablement based on device type.
- **Flexible services architecture:** Combines AAA, posture, profiling, and guest management capabilities in a single appliance platform. The Cisco Identity Services Engine can be deployed across the enterprise infrastructure, applying the appropriate services supporting 802.1x wired, wireless, and VPN networks.
- **Operational Efficiencies Through IT Automation:** Empowers the user to be in charge of on-boarding their device through self registration and provisioning in line with IT defined policies. Delivers capabilities such as sponsor-driven guest access, automatic device classification, auto BYOD on-boarding, and portal-driven device registration, giving IT more time to spend on other tasks and giving users more flexibility in how they work.
- **MDM Integration:** Cisco will partner with leading MDM vendors to allow IT organizations to enable appropriate applications and services based on user and device, and to provide them with greater visibility and control over endpoint access based on company-defined policies. **Available in the second half of CY 2012.**

Deployment Components

The Identity Services Engine is part of an infrastructure-based Cisco TrustSec deployment that uses Cisco network devices to extend access enforcement throughout a network. Additional deployment components include Cisco NAC Agent and Cisco AnyConnect™ (or the native 802.1X supplicant) on the endpoint; Cisco Catalyst® switches and Cisco wireless LAN controllers acting as policy enforcement points for the LAN; and Cisco Adaptive Security Appliances for secure remote access.

The Cisco Identity Services Engine also integrates with directory services such as Microsoft Active Directory and Sun ONE Directory Server as policy information points. In the future, Cisco ISE will also integrate with the leading MDM vendors as external policy information points.

Figure 2. Components of the Cisco TrustSec Solution Architecture



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, which is why Cisco has minimized the ISE CAPEX migration costs accordingly.



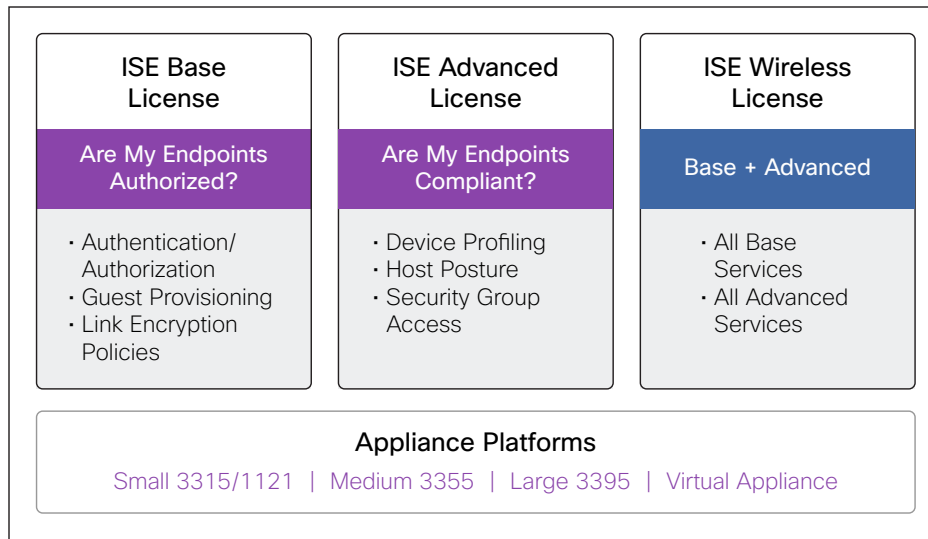
Licensing

Base licenses are intended for organizations that want to authenticate and authorize users and devices on their network (wired, wireless, and VPN). Base licenses include support for AAA services, guest lifecycle management, compliance reporting, and end-to-end monitoring and troubleshooting.

Advanced licenses expand upon Base license functionality, enabling organizations to make more advanced policy decisions based on richer contextual user and device information. Advanced license features include device profiling, posture services, and Security Group Access (SGA) enforcement capabilities.

Wireless licenses are intended for organizations that want to start their Identity Services Engine deployment for wireless endpoints only. Wireless licenses are simply predefined bundles of Base and Advanced licenses. Wireless Upgrade licenses allow customers who start with wireless only to expand their deployment to wired and VPN endpoints.

Figure 3. Cisco ISE licensing and packaging options



Why Cisco Identity Services Engine?

Market leadership:

- Largest market share in terms of customer deployments.
- Continually rated #1 by leading industry analysts including being positioned as a leader in the Gartner NAC Magic Quadrant report published on Dec 2011.
- Created by the company that pioneered the original network access control technologies and has developed numerous industry standards.
- The only comprehensive, single-vendor solution available today.

Technology and solution leadership:

- Uniquely combines AAA, posture, profiling, and guest management features in a single unified appliance, resulting in simplified deployments and integrated management.
- Dramatically reduces cost of ownership with world-class monitoring and troubleshooting features designed to streamline operations for your helpdesk and support teams.
- Delivers comprehensive security by integrating with embedded infrastructure features such as SGA.

For More Information

For more information on Cisco Identity Services Engine, visit <http://www.cisco.com/go/ise>. For more information about Cisco TrustSec and the full range of products that comprise the Cisco TrustSec solution, visit <http://www.cisco.com/go/trustsec>.