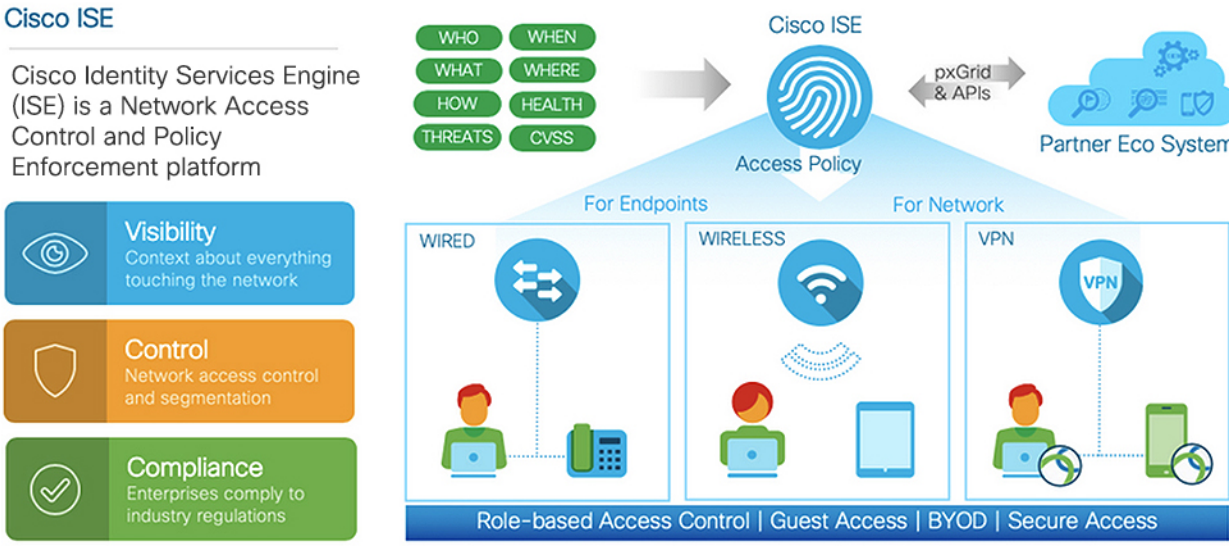
Introduction to Cisco ISE



Cisco Identity Services Engine (ISE) is an identity-based network access control and policy enforcement system. It functions as a common policy engine that enables endpoint access control and network device administration for enterprises.

You can leverage Cisco ISE to ensure compliance, enhance infrastructure security, and streamline service operations.

A Cisco ISE administrator can gather real-time contextual data for a network, including users and user groups (who?), device type (what?), access time (when?), access location (where?), access type (wired, wireless, or VPN) (how?), and network threats and vulnerabilities.

As a Cisco ISE administrator, you can use this information to make network governance decisions. You can also tie identity data to various network elements to create policies that govern network access and usage.

- Cisco ISE Features, on page 2

Cisco ISE Features

Cisco ISE software must be installed as is. You cannot install any other third-party applications at the underlying operating system level.

Cisco ISE empowers you with the following capabilities:

- **Device Administration**: Cisco ISE uses the TACACS+ security protocol to control and audit the configuration of network devices. It facilitates granular control of who can access which network device and change the associated network settings. Network devices can be configured to query Cisco ISE for authentication and authorization of device administrator actions. These devices also send accounting messages to Cisco ISE to log such actions.
- **Guest and Secure Wireless**: Cisco ISE enables you to provide secure network access to visitors, contractors, consultants, and customers. You can use web-based and mobile portals to on-board guests to your company's network and internal resources. You can define access privileges for different types of guests, and assign sponsors to create and manage guest accounts.
- **Bring Your Own Device (BYOD)**: Cisco ISE allows your employees and guests to securely use their personal devices on your enterprise network. BYOD feature end users can use configured pathways to add their devices, and provision predefined authentications and levels of network access.
- **Asset Visibility**: Cisco ISE gives you visibility and control over who and what is on your network consistently, across wireless, wired, and VPN connections. Cisco ISE uses probes and device sensors to listen to the way devices connect to the network. The Cisco ISE profile database, which is extensive, then classifies the device. This gives the visibility and context you need to grant the right level of network access.
- **Secure Access**: Cisco ISE uses a wide range of authentication protocols to provide network devices and endpoints with a secure network access. These include, but are not limited to, 802.1X, RADIUS, MAB, web-based, EasyConnect, and external agent-enabled authentication methods.
- **Segmentation**: Cisco ISE uses contextual data about network devices and endpoints to facilitate network segmentation. Security group tags, access control lists, network access protocols, and policy sets that define authorization, access, and authentication, are some ways in which Cisco ISE enables secure network segmentation.
- **Posture or Compliance**: Cisco ISE allows you to check for compliance, also known as posture, of endpoints, before allowing them to connect to your network. You can ensure that endpoints receive the appropriate posture agents for posturing services.
- **Threat Containment**: If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change the access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy.
- **Security Ecosystem Integrations**: The pxGrid feature allows Cisco ISE to securely share context-sensitive information, policy and configuration data, and so on, with connected network devices, third-party vendors, or Cisco partner systems.