Revised: June 30, 2026

Cisco Identity Services Engine — Terminology

Cisco Identity Services Engine

Cisco Identity Services Engine (Cisco ISE) is an identity-based network access control and policy enforcement solution that allows you to control endpoint access and administer network devices through a common policy engine. Your deployment can start as a standalone node and scale to a distributed deployment with dedicated administration, policy service, monitoring, and pxGrid nodes.

Cisco Identity Services Engine terminology

Adaptive Network Control policy

An Adaptive Network Control (ANC) policy changes an endpoint's network access in response to a security event. For example, Cisco ISE can apply a quarantine policy and issue a Change of Authorization (CoA) so that the network access device reauthorizes the endpoint.

Administration persona

he Cisco ISE node persona that provides deployment configuration and administration services. In a distributed deployment, the primary Policy Administration Node (PAN) is active and the secondary PAN is on standby. Configuration changes made on the primary PAN are replicated to the secondary PAN.

Agentless Posture

A Cisco ISE posture method that collects compliance information from a supported endpoint without requiring a permanently installed posture agent.

ANC Policy

A Cisco ISE authorization condition that represents the Adaptive Network Control state assigned to an endpoint.

authorization profile

In Cisco ISE, a collection of authorization results that is returned when an authorization rule matches. It can specify access, network assignment, redirection, or other enforcement attributes.

Blocked List Portal

A Cisco ISE device portal that informs users that their personal devices are block listed and cannot access the network.

BYOD portal

A personal-device portal that employees use to register their devices through native supplicant provisioning. Cisco ISE uses the portal as part of a Bring Your Own Device (BYOD) flow that authenticates the user, registers the endpoint, and provisions supported devices for network access.

Certificate Provisioning Portal

A Cisco ISE portal that allows authorized users to request and download certificates for devices that cannot use the standard onboarding flow.

Cisco ISE API Gateway

The single entry point through which external API requests reach Cisco ISE service APIs.

Cisco ISE Data Connect

A Cisco ISE feature that provides read-only access to configuration and operational database views for reporting and analysis.

Cisco ISE internal Certificate Authority

The internal Certificate Authority (Cisco ISE CA) that issues and manages certificates for endpoints.

Cisco ISE Passive Identity Connector

A Cisco ISE virtual appliance, abbreviated as ISE-PIC, that collects authentication data and provides consolidated passive-identity information to subscribing systems.

client provisioning policy

A set of rules that determines which agent, compliance module, configuration, or other provisioning resource Cisco ISE supplies to an endpoint. Cisco ISE evaluates attributes such as identity group and operating system to select the provisioning result.

Client Provisioning Portal

A Cisco ISE portal from which endpoints obtain client-provisioning resources required for network access or posture assessment.

Cloud Multi-Factor Classification Profiler

A Cisco ISE profiling service that shares observed endpoint attributes with a cloud service and applies returned classification labels.

Conditions Studio

The Cisco ISE policy editor used to create, combine, save, and reuse policy conditions.

device administration policy set

A policy container that controls TACACS+ authentication and authorization for device administrators. A regular device administration policy set contains authentication and authorization rule tables. Its authorization rules can return TACACS+ command sets and shell profiles. A proxy-sequence policy set forwards requests to configured remote proxy servers.

Dynamic Reauthorization Scheduler

A Cisco ISE feature that terminates an authorized session at a learned expiration date and time.

Endpoint Debug Log Collector

A Cisco ISE troubleshooting facility that collects debug logs associated with a specified endpoint.

endpoint identity group

A logical group that Cisco ISE uses to classify endpoints for policy evaluation and management. Portal and registration flows can place devices in an endpoint identity group, and authorization rules can use the group as a condition.

endpoint purge policy

A Cisco ISE policy that defines which endpoint records to remove from the endpoint database.

guest type

In Cisco ISE, a reusable set of settings that defines a class of guest accounts, including account duration, access times, identity group, and the sponsor groups permitted to create the accounts.

health check node

In Cisco ISE, a non-Administration node that monitors the primary Policy Administration Node and initiates automatic promotion of the secondary node when the primary node is unavailable.

Hotspot Guest portal

A guest portal that provides network access without requiring a username and password. Cisco ISE works with the network access device and Device Registration Web Authentication to authorize the guest endpoint. The portal can require an access code or acceptance of an acceptable use policy.

identity source sequence

In Cisco ISE, an ordered set of identity sources that Cisco ISE searches during authentication. It can also include a certificate authentication profile.

Monitoring and Troubleshooting Node (MnT)

A Cisco ISE node that collects logs from Administration and Policy Service Nodes and provides monitoring, reporting, and troubleshooting functions.

Monitoring persona

The Cisco ISE node persona that collects operational and audit data and provides monitoring, reporting, and troubleshooting functions. In a distributed deployment, primary and secondary Monitoring and Troubleshooting (MnT) nodes form an active-standby pair, and Policy Service Nodes send operational data to both.

My Devices portal

A personal-device portal that employees use to add, register, and manage their devices. It supports devices that cannot use native supplicant provisioning. A device added through the portal is recorded as an endpoint and, unless another static assignment exists, is placed in the RegisteredDevices endpoint identity group.

native supplicant provisioning

A BYOD process that configures a supported endpoint's native network supplicant for secure access. Cisco ISE selects the applicable provisioning flow from a native supplicant profile based on the endpoint operating system.

network device group

In Cisco ISE, a hierarchical grouping of network devices, commonly organized by attributes such as location and device type, that can be used in policy conditions.

Policy Administration Node (PAN)

A Cisco ISE node that runs the Administration persona. The Policy Administration Node (PAN) is the central point for configuring the deployment and its policies. A high-availability deployment uses a primary PAN and a secondary PAN.

Policy Service Node (PSN)

A Cisco ISE node that handles endpoint sessions and evaluates network access policies. A Policy Service Node (PSN) can provide services such as RADIUS authentication and authorization, guest access, profiling, posture, and device administration. Distributed deployments can use PSN groups for session failover.

Policy Service Node group

A group of Cisco ISE Policy Service Nodes whose members detect node failures and reset affected URL-redirected sessions.

Policy Service persona

The Cisco ISE persona that evaluates access policies and provides network access, posture, guest, client-provisioning, and profiling services.

policy set

In Cisco ISE, a top-level policy container that groups authentication, authorization, and exception rules for a network-access use case.

posture condition

In Cisco ISE, a test for a specified endpoint state, such as the presence, status, or configuration of software, a file, a service, or another supported attribute.

posture lease

The period for which Cisco ISE can reuse a previously determined compliant posture state. When the lease expires, a subsequent applicable user session must undergo posture assessment again.

posture requirement

In Cisco ISE, a policy element that associates posture conditions with remediation actions and supported operating systems.

profiler service

In Cisco ISE, a service that collects endpoint attributes from probes and sensors and applies profiling policies to classify devices.

Protocols Engine

A dedicated service that validates certificates for specific authentication scenarios to optimize processing. The Protocols Engine communicates with the Cisco ISE application server through API calls.

pxGrid (Platform Exchange Grid)

A framework that enables secure, scalable, and bi-directional exchange of context and policy information between Cisco ISE and third-party security platforms. It facilitates real-time sharing of identity and security data across the network ecosystem.

pxGrid Cloud

A cloud-based framework that enables secure, bi-directional data exchange between Cisco ISE and cloud-based security platforms. It extends traditional pxGrid capabilities to facilitate context sharing and policy orchestration across hybrid environments.

pxGrid node

A Cisco ISE node that runs the pxGrid persona and provides context-sharing services to approved integration clients.

pxGrid persona

The Cisco ISE node persona that runs pxGrid services for approved clients and ecosystem integrations. It enables systems to publish, query, and subscribe to contextual information and to request supported control actions.

Remote Support Authorization

A Cisco ISE feature through which an administrator grants a specified Cisco specialist time-limited, audited access to selected Cisco ISE nodes.

Secure Network Server (SNS)

A dedicated hardware appliance platform engineered to host and run Cisco ISE software. These appliances provide the optimized compute, storage, and networking resources required for enterprise-grade policy management.

Self-Registered Guest Portal

In Cisco ISE, a credentialed guest portal through which visitors create their own guest accounts. The flow can require registration information, sponsor approval, or acceptance of an acceptable use policy.

Sponsor Portal

In Cisco ISE, a portal where authorized sponsors create, import, manage, and provide credentials for temporary guest accounts.

Sponsored-Guest Portal

A Cisco ISE credentialed guest portal through which guests use accounts created for them by authorized sponsors.

TACACS+ command set

In Cisco ISE, a device-administration authorization result that identifies the commands and arguments a device administrator is permitted or denied from running.

TACACS+ profile

In Cisco ISE, a device-administration authorization result that contains TACACS+ attributes, such as a shell privilege level or vendor-specific attributes.

TC-NAC node

A Policy Service Node (PSN) in a Cisco ISE deployment that is configured to run the Threat Centric Network Access Control (TC-NAC) service. This node processes incoming threat and vulnerability attributes to dynamically adjust authorization policies based on endpoint risk.

Temporal Agent

A temporary executable that Cisco ISE uses to assess endpoint posture without installing a persistent posture application.

Threat Centric Network Access Control service

A Cisco ISE service that receives threat and vulnerability attributes to dynamically adjust authorization policies based on endpoint risk. When enabled on a Policy Service Node (PSN), it allows for automated network access changes in response to identified security threats.