Cisco ISE Features

• Cisco ISE Overview, page 2
• Key Functions, page 2
• Identity-Based Network Access, page 3
• Support for Multiple Deployment Scenarios, page 3
• Support for UCS Hardware, page 3
• Basic User Authentication and Authorization, page 4
• Policy Sets, page 5
• FIPS 140-2 Implementation, page 5
• Support for Common Access Card Functions, page 5
• Client Posture Assessment, page 6
• Network Access for Guests, page 6
• Support for Personal Devices, page 7
• Mobile Device Manager Interoperability with Cisco ISE, page 7
• Profiled Endpoints on the Network, page 7
• pxGrid Persona, page 7
• TrustSec Work Center, page 8
• TACACS+ Device Administration, page 8
• Support for SXP, page 8
• Third Party Device Support, page 8
• Telemetry, page 9
• IPv6 Support, page 9
• Location Based Authorization, page 10
• Cisco ISE Certificate Authority, page 10
• Support for Active Directory Multidomain Forests, page 11
Cisco ISE Overview

Cisco ISE is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make governance decisions by tying identity to various network elements, including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

ISE Community Resource

Join the ISE Community to view resources, ask questions, and participate in discussions. See ISE Product Documentation, Introduction to ISE, YouTube Videos, DrmosFeatures and Integration Demos, and Training Resources.

Note

The examples and screenshots provided in the ISE Community resources may be from earlier releases of Cisco ISE. Check the GUI for newer or extra features and updates.

Key Functions

Cisco ISE is a consolidated policy-based access control system that incorporates a superset of features available in existing Cisco policy platforms. Cisco ISE performs the following functions:

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance
- Provides for comprehensive guest access management for Cisco ISE administrators, sanctioned sponsor administrators, or both
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing the device posture for all endpoints that access the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed
- Employs advanced enforcement capabilities including Trustsec through the use of Security Group Tags (SGTs) and Security Group Access Control Lists (SGACLs)
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments
Facilitates TACACS-enabled device administration through its Work Center. The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators. However, pages such as Users, User Identity Groups, Network Devices, Default Network Devices, Network Device Groups, Authentication and Authorization Conditions, are shared with other menu options.

Identity-Based Network Access

The Cisco ISE solution provides context-aware identity management in the following areas:

- Cisco ISE determines whether users are accessing the network on an authorized, policy-compliant device.
- Cisco ISE establishes user identity, location, and access history, which can be used for compliance and reporting.
- Cisco ISE assigns services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).
- Cisco ISE grants authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.

Support for Multiple Deployment Scenarios

Cisco ISE can be deployed across an enterprise infrastructure, supporting 802.1X wired, wireless, and Virtual Private Networks (VPNs).

The Cisco ISE architecture supports both standalone and distributed (also known as "high-availability" or "redundant") deployments where one machine assumes the primary role and another "backup" machine assumes the secondary role. Cisco ISE features distinct configurable personas, services, and roles, which allow you to create and apply Cisco ISE services where they are needed in the network. The result is a comprehensive Cisco ISE deployment that operates as a fully functional and integrated system.

Cisco ISE nodes can be deployed with one or more of the Administration, Monitoring, and Policy Service personas—each one performing a different vital part in your overall network policy management topology. Installing Cisco ISE with an Administration persona allows you to configure and manage your network from a centralized portal to promote efficiency and ease of use.

Support for UCS Hardware

Cisco ISE 2.0 supports the following hardware platforms:

- SNS-3415 (small)
- SNS-3495 (large)

Refer to Table 3 in the Cisco Identity Services Engine Data Sheet for the hardware specifications.
Basic User Authentication and Authorization

User authentication policies in Cisco ISE enable you to provide authentication for a number of user login session types using a variety of standard authentication protocols including, but not limited to, Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol (EAP). Cisco ISE specifies the allowable protocol(s) that are available to the network devices on which the user tries to authenticate and specifies the identity sources from which user authentication is validated.

Cisco ISE allows for a wide range of variables within authorization policies to ensure that only authorized users can access the appropriate resources when they access the network. The initial release of Cisco ISE supports only RADIUS-governed access to the internal network and its resources.

At the most fundamental level, Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and browser-based Web authentication login for basic user authentication and access via both wired and wireless networks. Upon receiving an authentication request, the “outer part” of the authentication policy is used to select the set of protocols that are allowed when processing the request. Then, the “inner part” of the authentication policy is used to select the identity source that is used to authenticate the request. The identity source may consist of a specific identity store or an identity store sequence that lists a set of accessible identities until the user received a definitive authorization response.

Once authentication succeeds, the session flow proceeds to the authorization policy. (There are also options available that allow Cisco ISE to process the authorization policy even when the authentication did not succeed.) Cisco ISE enables you to configure behavior for “authentication failed,” “user not found,” and “process failed” cases, and also to decide whether to reject the request, drop the request (no response is issued), or continue to the authorization policy. In cases where Cisco ISE continues to perform authorization, you can use the “AuthenticationStatus” attribute in the “NetworkAccess” dictionary to incorporate the authentication result as part of the authorization policy.

The authorization policy result is Cisco ISE assigning an authorization profile that might also involve a downloadable ACL specifying traffic management on the network policy enforcement device. The downloadable ACL specifies the RADIUS attributes that are returned during authentication and that define the user access privileges granted once authenticated by Cisco ISE.

---

**Note**

Cisco ISE processes the attributes in the following order while identifying the Authentication session for the incoming accounting packet:

- For Cisco devices:
  1. Class/State
  2. audit-session-id

- For third party devices:
  1. Class/State
  2. Calling-Station-ID
  3. If the authentication session cannot be identified, Cisco ISE creates a new session ID based on the Calling-Station-ID, NAS-Port, and NAS-IP-Address.
Policy Sets

Network access policies are consolidated together under Policy Sets, which can be accessed from Policy > Policy Sets. Each policy set is a container defined on the top level of the policy hierarchy, under which all relevant Authentication and Authorization policy and policy exception rules for that set are configured. Multiple rules can be defined for both authentication and authorization, all based on conditions. Conditions and additional related configurations can also be easily accessed and reused directly from the Policy Set interface.

FIPS 140-2 Implementation

Cisco ISE, supports Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

In addition, the FIPS standard places limitations on the use of certain algorithms, and in order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS Shared Secret and Key Management measures and provides SHA-256 encryption and decryption capabilities for certificates. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled.

The certificates installed in ISE may need to be re-issued if the encryption method used in the certificates is not supported by FIPS. When you turn on FIPS mode in Cisco ISE, the following functions are affected:

- IEEE 802.1X environment
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - PEAP
  - RADIUS

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other protocols like EAP-Message Digest 5 (EAP-MD5), Lightweight Extensible Authentication Protocol (LEAP), and PAP are not compatible with a FIPS 140-2 compliant system and are disabled while Cisco ISE is in FIPS mode. Local Web Authentication (LWA), a legacy method of guest access uses PAP and will not work when Cisco ISE is in FIPS mode; However, Cisco ISE deployment with FIPS mode enabled might use &quot;host lookup&quot; in Allowed Protocols for MAC Authentication Bypass (MAB), and hence guess access with Central Web Authentication (CWA) will work.</td>
</tr>
</tbody>
</table>

- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)

Support for Common Access Card Functions

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509
client certificates that identify a particular employee of, for example, the U.S. Department of Defense (DoD).
Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates
from the card are then transferred into the Windows certificate store, where they are available to applications
such as the local browser running Cisco ISE.

Benefits of using a CAC card to authenticate include these:

- Common Access Card X.509 certificates are the identity source for 802.1X EAP-TLS authentication.
- Common Access Card X.509 certificates are also the identity source for authentication and authorization
to Cisco ISE administration.

Cisco ISE only supports login to the Admin portal. It does not support CAC authentication for the following
access methods:

- You cannot use CAC authentication login to manage the Cisco ISE Command Line Interface.
- External REST API (Monitoring and Troubleshooting) and Endpoint Protection Services Adaptive
  Network Control APIs are outside the scope of the CAC authentication.
- Guest Services and Guest Sponsor Administration access does not support the CAC authentication
  method in Cisco ISE.

## Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you
to validate and maintain security capabilities on any client machine that accesses the protected network. By
employing posture policies that are designed to ensure that the most up-to-date security settings or applications
are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses
the network meets, and continues to meet, the defined security standards for enterprise network access. Posture
compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the
time of user login, as well as any time a periodic reassessment occurs.

Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE:

- Cisco NAC Web Agent—A temporal agent that the users install on their system at the time of login and
  that is no longer visible on the client machine once the login session terminates.
- Cisco NAC Agent—A persistent agent that, once installed, remains on a Windows or Mac OS X client
  machine to perform all security compliance functions.
- AnyConnect ISE Agent—A persistent agent that can be installed on Windows or Mac OS X client to
  perform posture compliance functions.
- Cisco Temporal Agent—A temporary executable file that is run on the client to check the compliance
  status. The agent is removed from the client machine after the login session is terminated. By default,
  the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.

## Network Access for Guests

Cisco ISE administrators and employees who are granted appropriate access to the Cisco ISE guest registration
portal as guest sponsors can create temporary guest login accounts and specify available network resources
to allow guests, visitors, contractors, consultants, and customers to get restricted access to the specified network
resources and Internet. Guest access sessions have expiration timers associated with them, so they are effective in controlling guest access to a specific day, time period, and so forth.

All aspects of a guest user session (including account creation and termination) are tracked and recorded in Cisco ISE so that you can provide audit information and troubleshoot session access, as necessary.

Guests can select a social login provider as a way to provide credentials as a self-registered guest, instead of entering username and password in the guest portal. To enable this, you can configure a social media site as an external identity source, and configure a portal that allows users to use that external identity source (social login provider). Facebook is the social login provider supported by this release.

Support for Personal Devices

Cisco ISE allows employees to connect their personal devices, such as laptop computers, mobile phones, tablets, printers, and other network devices on the enterprise network.

Supporting these devices presents difficulties in protecting network services and enterprise data, so you must ensure that both the employees and their devices are authenticated and authorized for network access. With a Plus license, Cisco ISE provides you with the tools you need to allow employees to securely use their personal devices on your corporate network.

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM enforces policy on endpoints, but it cannot force users to register their device or force remediation. ISE retrieves policies from the MDM server, and enforces those policies when users register their devices. If the ISE device policy requires MDM, and the device is not compliant with MDM, then ISE redirects the user to the MDM on-boarding portal, and prompts the user to update the device for network access. ISE can also allow internet-only access to users who decline MDM compliance.

Profiled Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their device types, to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer, where the known endpoints are classified according to their associated policies and identity groups.

The Profiler Feed service allows administrators to retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE.

pxGrid Persona

Cisco pxGrid is used to enable the sharing of contextual-based information from Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework
can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between ISE and third party vendors, and for non-ISE related information exchanges such as threat information.

**TrustSec Work Center**

All TrustSec-related options are consolidated under the TrustSec Work Center menu (Work Centers > TrustSec), so that the administrator can easily access all the TrustSec options at one location.

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network. The Metrics dashlet displays statistics about the behavior of the TrustSec network. The Active SGT Sessions dashlet displays the SGT sessions that are currently active in the network. The Alarms dashlet displays the alarms related to the TrustSec sessions. The Quick View dashlet displays TrustSec-related information for NADs and SGTs.

You can click the TrustSec Sessions link in the Live Log dashlet to view the active TrustSec sessions. You can also view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

**TACACS+ Device Administration**

Cisco ISE supports device administration using the Terminal Access Controller Access-Control System (TACACS+) security protocol to control and audit the configuration of network devices. The network devices are configured to query ISE for authentication and authorization of device administrator actions, and send accounting messages for ISE to log the actions. It facilitates granular control of who can access which network device and change the associated network settings. An ISE administrator can create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service. The ISE Monitoring node provides enhanced reports related to device administration. The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators.

ISE requires a Device Administration license to use TACACS+.

**Support for SXP**

Source Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint’s SGT along with the IP address from one SGT-aware network device to another.

To enable SXP service on a node, check the Enable SXP Service check box in the General Node Settings page. You must also specify the interface to be used for SXP service.

Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.

**Third Party Device Support**

Cisco ISE supports some third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.
Cisco ISE includes predefined profiles for network devices from the following vendors:

- Cisco—Wired and Wireless
- Aruba—Wireless
- HP—Wired and Wireless
- Motorola—Wireless
- Brocade—Wired
- Alcatel—Wired
- Ruckus—Wireless

You can also create profiles for additional third-party network device that does not have a predefined profile. AnyConnect client provisioning and posture discovery do not mandate CoA and URL redirection.

If you have deployed non-Cisco NADs prior to Release 2.0 and created policy rules/RADIUS dictionaries to use them, after upgrade these will continue to work as usual.

**Telemetry**

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner appears on screen. Using this feature, Cisco ISE securely collects non-sensitive information about your deployment, network access devices, profiler, and other services that you are using. The data that is collected will be used to provide better services and additional features in forthcoming releases. By default, the telemetry feature is enabled. You can choose to disable it from the Admin portal.

**IPv6 Support**

Cisco ISE, Release 2.0 supports the following IPv6 capabilities:

- Support for IPv6-Enabled Endpoints: Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints. You can configure authorization profiles and policies in Cisco ISE using IPv6 attributes to process requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.
- IPv6 Support in Reports: Reports in Release 2.0 support IPv6 values. The Live Session and Live Authentication pages also support IPv6 values.
- IPv6 Support in CLI: Release 2.0 supports IPv6 in the following CLI commands:
  - ipv6 address-To allow for static IPv6 address configuration per network interface
  - ipv6 enable-To enable or disable IPv6 on all network interfaces
  - ipv6 route-To configure IPv6 static routes
  - ip host-To allow for adding IPv6 addresses in host local table
  - show IPv6 route-To display IPv6 routes

Refer to the Cisco Identity Services Engine CLI Reference Guide for more information on these commands.
Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

`MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone`

You can define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers.

The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.

Cisco ISE Certificate Authority

Cisco ISE provides a native Certificate Authority (CA) that issues and manages digital certificates for endpoints from a centralized console to allow employees to connect to the company’s network using their personal devices. Cisco ISE CA supports standalone and subordinate deployments.

Certificate Provisioning Portal

Cisco ISE offers a Certificate Provisioning portal that allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate. Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

Certificate Template Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate. You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.
Cisco ISE Internal CA Issues Certificates to ASA VPN Users

The internal ISE CA can issue certificates to client machines that connect over ASA VPN. ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates from Cisco ISE to the client machines.

Support for Active Directory Multidomain Forests

Cisco ISE supports Active Directory with multidomain forests. Cisco ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which Cisco ISE is connected and the other domains.

Support for SAnet Devices

Cisco ISE provides limited support for Session Aware Networking (SAnet), a session management framework on the switches that provides more consistent and flexible management of access-sessions, including visibility, authentication, and authorization. SAnet defines the notion of a service template which is an authorization object accepted both by ISE as well as by the device. This is in contradistinction to Cisco ISE authorization profiles which are containers of RADIUS authorization attributes that are merged and flattened into a list of attributes before they are sent to the device. Similarly, SAnet service templates are also containers of RADIUS authorization attributes but they are not flattened into a list before sending to the device. Instead, Cisco ISE sends the name of the service template and the device downloads the content (RADIUS attributes) if it does not already have a cached or statically defined version of it. In addition, Cisco ISE sends CoA notifications to the device if the definition of a service template has changed, that is, if a RADIUS attribute was added, removed or changed.

Cisco ISE implements service templates as authorization profiles that contain a special flag that marks them as "Service Template" compatible. This way the service template, which is also an authorization profile, can be used in a single policy statement that will support sessions connecting from SAnet capable devices as well as legacy devices.

Support for Installation on Multiple Hardware and VMware Platforms

Cisco ISE comes preinstalled on a range of physical appliances with various performance characteristics. The Cisco Application Deployment Engine (ADE) and Cisco ISE software run either on a dedicated SNS-3400 Series appliance or on a virtual machine (Cisco ISE VM). The Cisco ISE software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed.

Identity Provider as an External Identity Source

Cisco ISE supports SAML Single Sign On (SSO) for the following portals:
Support for Automatic Failover for the Administration Node

Cisco ISE supports automatic failover for the Administration persona. To enable the auto-failover feature, at least two nodes in your distributed setup should assume the Administration persona and one node should assume the non-Administration persona. If the Primary Administration Node (PAN) goes down, an automatic promotion of the Secondary Administration Node is initiated. For this, a non-administration secondary node is designated as the health check node for each of the administration nodes. The health check node checks the health of PAN at configured intervals. If the health check response received for the PAN health is not good due to being down or not reachable, the health check node initiates the promotion of the Secondary Administration Node to take over the primary role after waiting for the configured threshold value. There are some features that are unavailable after auto-failover of the Secondary Administrative Node. Cisco ISE does not support fallback to the original PAN. Refer to the High Availability in Administration Nodes section in the Deploy Cisco ISE Nodes chapter for more information.

GUI-Based Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified and the progress of the upgrade and the status of the nodes are displayed on screen.

The GUI-based upgrade is applicable only if you are upgrading from Release 2.0 to a higher release or if you are upgrading a Limited Availability Release of Cisco ISE 2.0 to the General Availability Release.

Technical Support Tunnel for Advanced Troubleshooting

Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server in your deployment and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel. As an administrator, you can control the tunnel access; you can choose when and how long to grant access to the support engineer. Cisco Customer Support cannot establish the tunnel without your intervention. You will receive notification about the service logins. You can disable the tunnel connection at any point of time.