Network Deployments in Cisco ISE

- Cisco ISE network architecture, on page 1
- Cisco ISE deployment terminology, on page 1
- Node types and personas in distributed deployments, on page 2
- Cisco ISE deployment models, on page 4
- Small network deployments, on page 4
- Medium-sized network deployments, on page 5
- Large network deployments, on page 6
- Cisco ISE deployment sizing guidelines, on page 8
- Switch and Wireless LAN Controller configuration required to support Cisco ISE functions, on page 9

Cisco ISE network architecture

Cisco ISE architecture includes these components:

- Nodes and persona types

  A Cisco ISE node can assume any or all of these personas:

  - Administration
  - Policy Service
  - Monitoring
  - pxGrid

- Network resources
- Endpoints

The policy information point is where external information is communicated to the Policy Service persona. For example, external information might be a Lightweight Directory Access Protocol (LDAP) attribute.

Cisco ISE deployment terminology

This guide uses these terms to discuss Cisco ISE deployment scenarios:

Term	Definition
Service	A specific feature that a persona provides, such as network access, profiling, posture, security group access, monitoring, or troubleshooting.
Node	An individual physical or virtual Cisco ISE appliance.
Node type	The Cisco ISE node can assume any or all of these personas: • Administration • Policy Service • Monitoring • pxGrid
Persona	Determines the services provided by a node. The administrative user interface menu options depend on the roles and personas that a node assumes.
Role	This determines whether a node is standalone, primary, or secondary, and applies only to Administration and Monitoring nodes.

Node types and personas in distributed deployments

Each Cisco ISE node provides different services depending on its assigned persona. In a distributed deployment, you can have these combinations of nodes in your network:

- Primary and secondary Administration nodes for high availability
- A pair of Monitoring nodes for automatic failover
- One or more Policy Service nodes for session failover
- One or more pxGrid nodes for pxGrid services

Administration nodes

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all system-related configurations that are related to functionalities such as authentication, authorization, auditing, and so on.

In a distributed deployment, you can have a maximum of two nodes running the Administration persona. The Administration persona can take on of these roles—standalone, primary, or secondary.

Policy Service nodes

A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates policies and makes decisions.

You can have more than one node assume this persona. Typically, distributed deployments have more than one Policy Service node.

You can group all Policy Service nodes that reside in the same high-speed local area network (LAN) or are behind a load balancer as a node group. If one node in a group fails, the other nodes detect the failure and reset URL-redirected sessions.

At least one node in your distributed setup should assume the Policy Service persona.

Monitoring nodes

A Cisco ISE node with the Monitoring persona

- functions as the log collector and stores log messages from all the Administration and Policy Service nodes.
- provides advanced monitoring and troubleshooting tools to effectively manage a network and resources.
- aggregates and correlates the data that it collects and provides meaningful reports.

You can have a maximum of two nodes with this persona, and they can take on primary or secondary roles for high availability. In case the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node.

At least one node in your distributed setup should assume the Monitoring persona. We recommend that you do not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the Monitoring node be dedicated solely to monitoring for optimum performance.

pxGrid nodes

You can use Cisco pxGrid to share context-sensitive information from Cisco ISE session directory with other network systems such as ISE ecosystem partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes, such as sharing tags and policy objects between Cisco ISE and third-party vendors, and for other information exchanges. Cisco pxGrid also allows third-party systems to invoke adaptive network control actions to quarantine users or devices in response to a network or security event.

TrustSec information, such as tag definition, value, and description, can be passed from Cisco ISE to other networks through the TrustSec topic. You can publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid.

Endpoint profiles with fully qualified names (FQNs) can be passed from Cisco ISE to other networks through an endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

In a high-availability configuration, pxGrid servers replicate information between nodes through the PAN. When the PAN goes down, the pxGrid server stops handling client registration and subscription. You must manually promote the PAN to activate the pxGrid server.

Note Only the clients that are part of the groups included in the policy can subscribe to the service specified in that policy.

Cisco ISE deployment models

A deployment that has a single Cisco ISE node is called a standalone deployment. This node runs the Administration, Policy Service, and Monitoring personas.

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and improve performance, you can deploy multiple Cisco ISE nodes in a distributed way. In a Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across Policy Service nodes. Depending on your performance needs, you can scale your deployment.

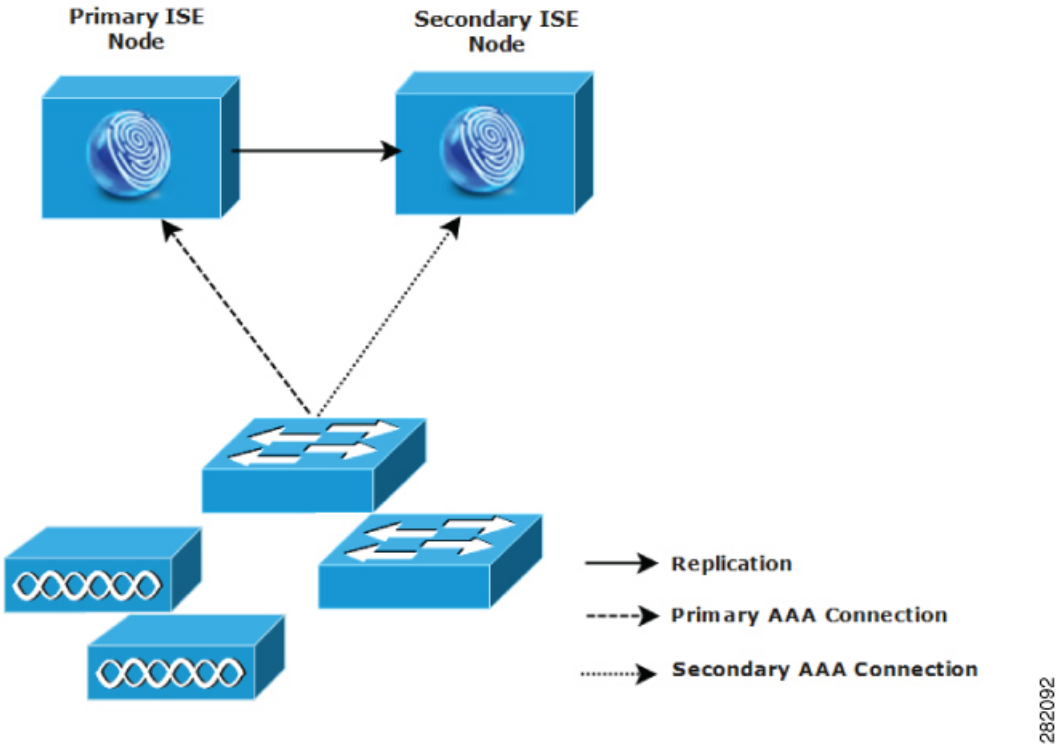
Small network deployments

The smallest Cisco ISE deployment consists of two Cisco ISE nodes with one Cisco ISE node functioning as the primary node.

The primary node manages all configuration, authentication, and policy tasks for your network. The secondary node acts as a backup. If connectivity is lost between the primary node and network appliances, network resources, or RADIUS, the secondary node supports the primary node and keeps the network running.

Centralized authentication, authorization, and accounting (AAA) operations between clients and the primary node are performed using the RADIUS protocol. Cisco ISE synchronizes all content from the primary node to the secondary node. In a small network deployment, you can configure both nodes on all RADIUS clients by using this model or a similar approach.

Figure 1: Small network deployment of Cisco ISE nodes



If you want to add more devices, network resources, users, or AAA clients, switch from the small deployment model to a split or distributed deployment model.

Split deployments

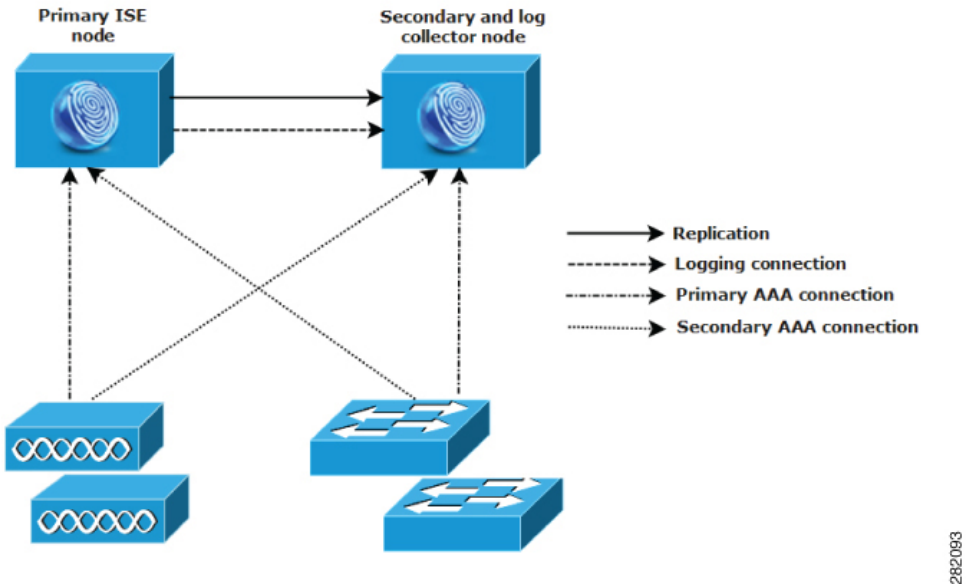
In split deployments, the AAA load is split between the primary and secondary nodes to optimize the AAA workflow.

Each node must be able to handle the full workload if there are any problems with AAA connectivity. During normal network operations, neither the primary node nor the secondary node handles all AAA requests, because the workload is distributed between the two nodes.

Split deployment provides better load distribution and ensures that the secondary node remains functional during normal network operations. This design also supports deployment expansion.

In split deployments, each node can perform its own specific operations, such as network admission or device administration, and still perform all the AAA functions if a failure occurs. If two nodes process authentication requests and collect accounting data from AAA clients, configure one node to act as a log collector.

Figure 2: Split network deployment in Cisco ISE



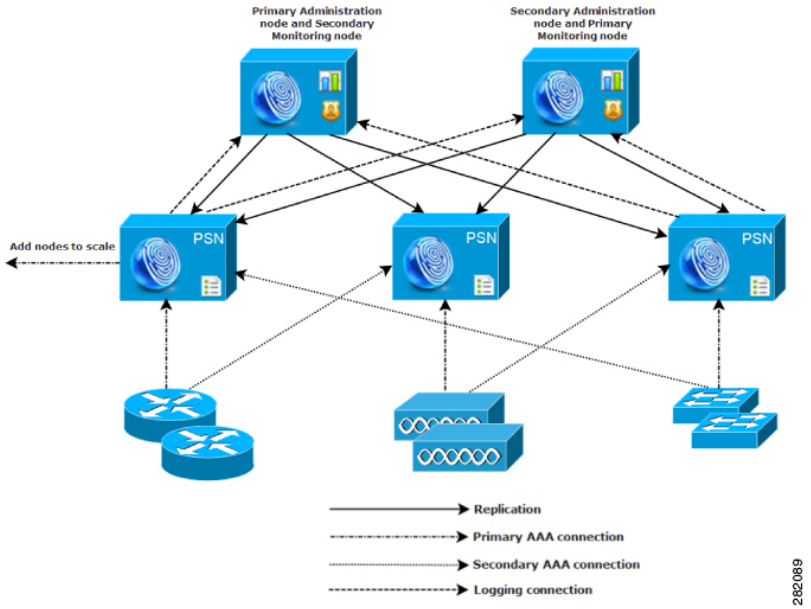
Medium-sized network deployments

As small networks grow, you can manage network growth by adding nodes to create a medium-sized network. In medium-sized network deployments, you can dedicate the new nodes for all AAA functions and use the original nodes for configuration and logging functions.

Note In a medium-sized network deployment, you cannot enable the Policy Service persona on a node that runs the Administration persona or the Monitoring persona. You need dedicated policy service nodes.

If the amount of log traffic increases in a network, you can dedicate one or two secondary nodes for log collection.

Figure 3: Medium-sized network deployment in Cisco ISE



Large network deployments

In a Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across the Policy Service nodes. Depending on your performance needs, you can scale your deployment.

Centralized log management

We recommend that you use centralized logging for large Cisco ISE networks. To use centralized logging, you must first set up a dedicated logging server that acts as a Monitoring node to handle the potentially high syslog traffic that a large, busy network can generate.

You can use an RFC 3164-compliant syslog appliance to collect the syslog messages generated for outbound log traffic.

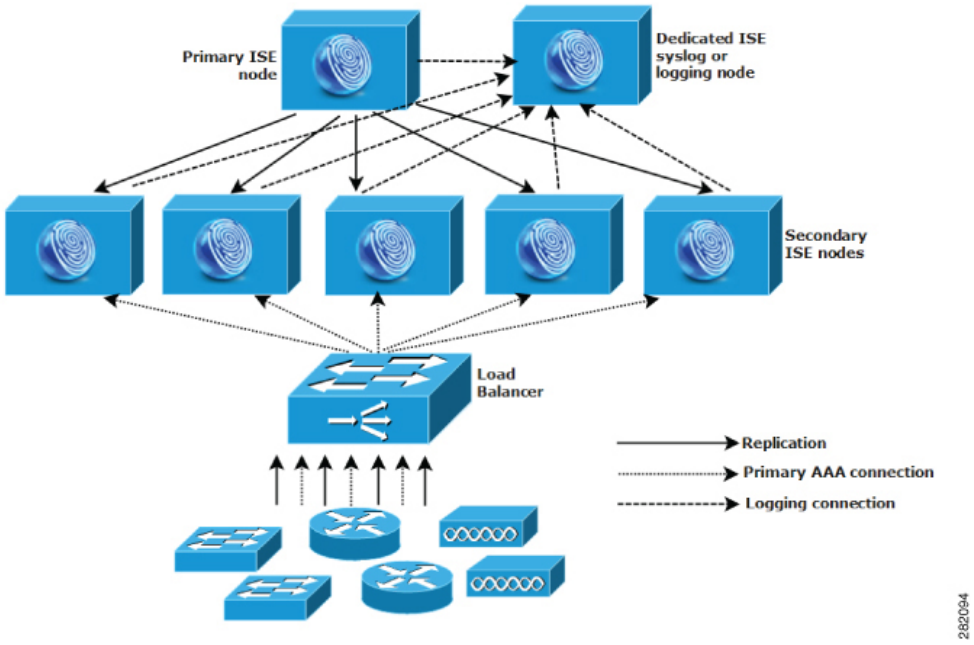
You can also consider having the appliances send logs to both a Monitoring node and a generic syslog server. A generic syslog server provides redundant backup if the Monitoring node goes down.

Load balancers for centralized networks

You can load balancers for large, centralized networks to optimize the routing of AAA requests to the available servers.

Having only a single load balancer creates a single point of failure in the system. To avoid this potential issue, deploy two load balancers to ensure redundancy and failover. This configuration requires you to set up two AAA server entries in each AAA client.

Figure 4: A large network deployment using a load balancer

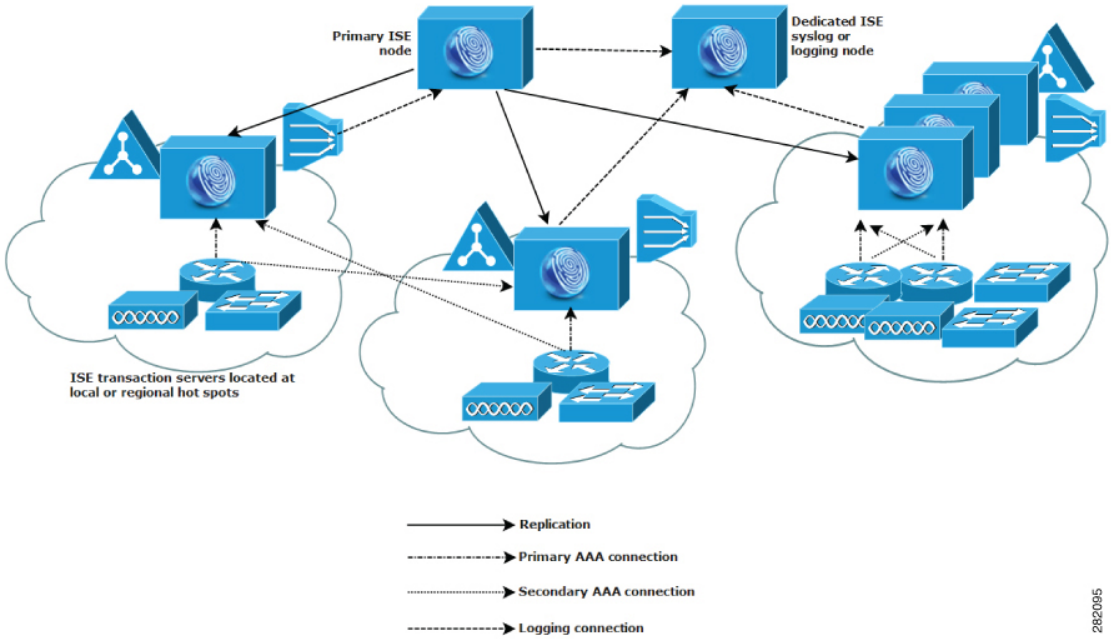


Dispersed network deployments

Dispersed Cisco ISE network deployments are most useful for organizations that have a main campus with regional, national, or satellite locations elsewhere. The main campus is where the primary network resides. It is connected to additional LANs, ranges in size from small to large, and supports appliances and users in different geographical regions and locations.

Large remote sites can have their own AAA infrastructure for optimal AAA performance. Use a centralized management model to maintain a consistent, synchronized AAA policy. A centralized configuration model uses a primary Cisco ISE node with secondary Cisco ISE nodes.

Figure 5: Dispersed deployment in Cisco ISE



Considerations for planning a network with several remote sites

Consider these factors when planning a network with several remote sites:

- Ensure that each remote site has a synchronized instance of the external database available for Cisco ISE access to optimize AAA performance.
- Locate Cisco ISE nodes as close as possible to AAA clients to reduce latency and prevent access loss during WAN failures.
- Use a terminal at each site for direct, secure console access. This is needed for certain functions, such as backup.
- If small, remote sites are in close proximity and have reliable WAN connectivity to other sites, consider using a Cisco ISE node as a backup for the local site to provide redundancy.
- Configure DNS correctly on all Cisco ISE nodes to ensure access to external databases.

Cisco ISE deployment sizing guidelines

For information about the deployment sizing guidelines and the scale limits for different types of Cisco ISE deployment, see Performance and Scalability Guide for Cisco Identity Services Engine.

Switch and Wireless LAN Controller configuration required to support Cisco ISE functions

To enable Cisco ISE to interoperate with network switches and to ensure successful function of Cisco ISE across the network segment, configure your network switches with required settings such as Network Time Protocol (NTP), RADIUS, AAA, IEEE 802.1X, MAC Authentication Bypass (MAB), and so on.

ISE Community Resource

For information about setting up Cisco ISE with WLC, see Cisco ISE with WLC Setup Video.