Cisco ISE Performance, Scalability, and Best Practices

Contents

Cisco ISE Deployment and Sizing 4
- Cisco ISE personas 4
- Cisco ISE profiles 6
- Cisco ISE deployment types 8
- Latency guidelines 9
- Cisco ISE session management and sizing 10

Cisco ISE Installation on Cisco Secure Network Server (SNS) 11
- Decision guide for installing Cisco ISE on SNS 12
- General pre-installation checklist 12
- Detailed installation methods 13
- Common post-installation steps 15

Scaling Cisco ISE Services 15
- The impact of mobile and IoT proliferation 15
- Managing authentication load 16
- Certificate management 16
- Domain name service (DNS) 18

Network Device and Load Balancer Best Practices 20
- RADIUS/TACACS+ server configuration 21
- Wired device best practices 21
- Catalyst 9800 series wireless controllers best practices 22
- Load balancer implementation 23

Security: Mitigating Blast RADIUS (CVE-2024-3596) 25
- Mitigation strategies 25

Profiling and Endpoint Management 25
- Choosing the right probes 25
- Understanding probe attributes 26
- Detailed probe attributes 27
- Optimizing global profiler settings 30
- Endpoint management 30
- Cisco ISE Profiler Feed Service 30
- Comprehensive best practices summary 31

External Databases and Active Directory 32
- Policy set organization 32
- Authorization rule optimization 32
- Active Directory integration 33

© 2026 Cisco and/or its affiliates. All rights reserved.

Logging and Monitoring 34
Hardware and storage considerations 34
Remote logging targets 34
Log suppression and filtering 34
Performance monitoring and troubleshooting 35
Operational data management and retention 35
Posture Compliance 35
Redirection and posture flow 35
Timers and session management 36
Posture configuration: agentless vs. agent-based 36
Client provisioning and remediation 36
Administrative practices 36
Mobile Device Management (MDM) 36
Integration and trust establishment 36
MDM server configuration in Cisco ISE 36
Device identification and compliance 37
Multiple MDM environments 37
Policy and access control 37

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco ISE Deployment and Sizing

Before you size a Cisco ISE deployment, identify each node persona and its role. Each persona performs a distinct function, which lets you distribute workloads across the network.

Cisco ISE personas

A Cisco ISE node can run one or more personas. Identify the required roles when planning capacity and high availability.

Table 1. Cisco ISE personas and deployment considerations

Persona	Primary Function	Key Responsibilities	Deployment Considerations
Policy Administration Node (PAN)	Management & Configuration	• Central configuration repository • Policy management interface • Administrative access point • Node-to-node replication control	• Deploy as primary or secondary pair • Limited to 2 nodes per deployment
Monitoring & Troubleshooting (MnT)	Logging & Analytics	• Central session directory • Log collection and reporting • Alerting and troubleshooting tools • Historical data analysis	• High storage requirements • Memory-intensive operations • Sized based on log retention needs • Maximum 2 nodes per deployment
Policy Service Node (PSN)	Authentication & Authorization	• RADIUS/TACACS+ request processing • Real-time policy decisions • Profiling and posture assessment • Guest and BYOD services	• Most performance-critical persona • Scales horizontally for capacity • Deploy in strategic network locations • Requires proper load balancing • Maximum 50 nodes per deployment
pxGrid node	Integration & Context Sharing	• Security ecosystem integration • Context sharing framework	• Dedicated nodes for large integrations • Scales with third-party connections

© 2026 Cisco and/or its affiliates. All rights reserved.

Persona	Primary Function	Key Responsibilities	Deployment Considerations
		• Threat containment • Publisher/subscriber services	• Optimized for API interactions • Supports cloud and on-premises services • Maximum 4 nodes per deployment

Personas can be combined on a single node for smaller deployments or distributed across dedicated nodes for larger environments. The optimal distribution depends on network size, authentication volume, and performance requirements.

For most deployments, start with combined PAN and MnT nodes and dedicated PSNs. As scale increases, dedicate nodes to each persona to improve performance and stability.

PSN node variations

Policy Service Nodes can be specialized for specific network functions to optimize performance and resource utilization:

Table 2. Policy Service Node specializations

PSN Specialization	Primary Function	Key Considerations
TACACS+ PSN (T+PSN)	Device administration	• Dedicated for TACACS+ services only • Optimized for high volumes of network device admin sessions • Ideal for environments with heavy usage of scripts or NMS
TC-NAC PSN (TCNPSN)	Threat-Centric NAC	• Supports higher numbers of TC-NAC adapters • Optimized for Incident Response Framework (IRF) TPS • Specialized for Vulnerability Assessment Framework (VAF) TPM
Guest PSN (GPSN)	Guest access services	• Dedicated to guest portal operations • Optimized for large-scale guest deployments • Positioned at network edge or DMZ for external access
TrustSec PSN (CTSPSN)	Security Group policy	• RADIUS authentication focused on TrustSec functions • Prevents TrustSec policy pushes from impacting general authentication • Dedicated to Security Group Tag (SGT) distribution
SXP PSN (SXPSN)	Security Group eXchange	• Maximum four pairs in a deployment • Supports up to 200 peers per pair • Dedicated nodes required for large SXP deployments

© 2026 Cisco and/or its affiliates. All rights reserved.

PSN Specialization	Primary Function	Key Considerations
PassiveID PSN (PIDPSN)	Identity Firewall services	• Supports Identity Firewall (IDFW) operations • Maximum 2 nodes for redundancy • Optimized for user-to-IP mapping functions

Deploy specialized PSNs when you have high volumes of specific traffic types. This prevents resource contention between different authentication protocols and improves overall system stability.

Cisco ISE profiles

Cisco ISE profiles allocate CPU, memory, and thread-pool resources according to the hardware or VM specifications. Choose a profile that matches your deployment size and use case.

Resource allocation

Each profile configures several system parameters, including:

Each profile sets Java heap size and garbage collection, Oracle database memory allocation and cache sizes, authentication thread-pool sizes, and the maximum number of concurrent endpoint sessions.

Profile types and sizing

Cisco ISE automatically selects a profile at boot time based on available hardware resources. The profile selected determines system resource allocation and performance capabilities. Use sizing guidelines to maintain stable operation and authentication throughput.

For detailed specifications, refer to the Performance and Scalability Guide for Cisco Identity Services Engine.

The relevant tables in that guide are Table 24, “Specifications for Cisco SNS 3700 series hardware appliances”; Table 25, “Specifications for Cisco SNS 3800 series hardware appliances”; Table 26, “Specifications for Cisco ISE VM and cloud instances”; and Table 27, “Extra small form factor for Cisco ISE VM and cloud instances”.

Validation and verification

To verify the profile applied to a Cisco ISE node, use one of these methods:

CLI Method:

```
show tech-support | begin "Displaying ISE Profile"
```

GUI Method:

Navigate to Operations > Reports > Diagnostics > ISE Counters > Select Node

Virtual machine best practices

Cisco ISE virtual deployments require specific resource configurations to maintain performance parity with physical appliances.

Table 3. Virtual machine resource recommendations

Resource	Recommendation	Rationale
CPU Reservation	100% reservation	Prevents resource contention during authentication spikes

© 2026 Cisco and/or its affiliates. All rights reserved.

Resource	Recommendation	Rationale
Memory Reservation	100% reservation	Ensures consistent Java heap and database performance
Disk Provisioning	Thick provision eager zeroed	Provides consistent I/O performance
Resource Limits	No limits	Prevents artificial throttling during peak loads
OVA Templates	Use official Cisco OVAs	Includes proper resource reservations by default
VM Snapshots	Not supported	Can severely impact performance. Use Cisco ISE backup instead.
vMotion	Cold vMotion preferred	Run application stop ise before migration

Important: VM resource overcommitment at the hypervisor level is not supported and can lead to unpredictable authentication performance.

Limitations of SNS 3615/3715 nodes (32 GB) and equivalent virtual machines

Proper sizing based on workload is critical, especially for memory-constrained 32 GB platforms.

Table 4. Limitations of 32 GB nodes and equivalent virtual machines

Feature/Function	Support Status	Impact
Multiple Personas	Limited	Avoid PAN and MnT+PSN combinations
Protocol Support	Choose One	Run either RADIUS or TACACS+, not both
pxGrid	Limited	Dedicated nodes recommended for integrations
Advanced Features	Not Recommended	Log Analytics, AI/ML Profiling, ACI, Workload Connectors require more memory

Deployment recommendations

Small deployments

For small deployments, dedicate each node to one authentication protocol, RADIUS or TACACS+. Disable unused features and probes to conserve memory, monitor memory utilization during peak periods, and apply memory optimization patches as Cisco releases them.

Medium deployments

Medium deployments have the same constraints as small deployments when 32 GB appliances run combined PAN and MnT roles.

Upgrade planning

For advanced features, plan a phased migration from 32 GB nodes to SNS 3655/3695 appliances with 96 GB or more of memory, or equivalent VM resources. In larger deployments, consider 32 GB nodes for specialized roles with limited functions.

Memory pressure issues often manifest as slow authentication response, policy service restarts, or database synchronization failures. Regular monitoring of system resources is essential when operating 32 GB platforms.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco ISE deployment types

Choose a deployment type based on network size, redundancy requirements, and authentication volume. The deployment type determines node count, persona distribution, and system capacity.

Deployment type overview

Table 5. Cisco ISE deployment types and node allocations

Deployment Type	Node Count	Personas Distribution	Best for	Max PSNs
Standalone	1	All on single node	Labs, PoC, Small Sites	1
Small	2-3	Multi-persona nodes	SMB, Branch Offices	3
Medium	4-8	Mixed dedicated/combined	Mid-Enterprise	6
Large	6-58	Dedicated persona nodes	Large Enterprise, Service Provider	50

Standalone deployment

A standalone deployment uses one node for the PAN, MnT, PSN, and pxGrid personas. It suits labs, proof-of-concept deployments, and small networks with fewer than 1000 endpoints. It has no high availability or redundancy, scales only to the capacity of the single node, and requires a complete service outage for maintenance.

Small deployment

A small deployment uses two nodes with the PAN, MnT, and PSN personas. Typically, both nodes run all personas, including pxGrid. An optional third node can serve as a dedicated PSN, pxGrid node, or health-check node for automatic PAN failover; pxGrid can be enabled on up to two nodes when needed. This design provides basic redundancy and can suit distributed branches, although combined personas and a limited node count can constrain performance under heavy load.

Medium deployment

A medium deployment uses 4–8 nodes with mixed persona assignments. Two nodes typically run combined Primary or Secondary PAN and MnT roles; 64 GB of RAM is recommended for optimal performance, and 32 GB PAN and MnT nodes may degrade with 5 or more PSNs. Deploy 2–6 dedicated PSNs according to geography and authentication volume.

Enable pxGrid on at most two existing nodes or deploy up to two dedicated pxGrid/SXP nodes, reducing the number of dedicated PSNs accordingly. This design balances performance and operational complexity, provides redundancy for critical services, suits regional offices or mid-size enterprises, and can grow into a large deployment by adding dedicated nodes.

Large deployment

A large deployment supports up to 58 nodes with dedicated personas: two PANs, two MnT nodes, up to 50 PSNs, and up to four pxGrid nodes. The PAN and MnT pairs each have primary and secondary roles. The design offers the highest performance and scalability, supports high authentication rates, complex segmentation, and global deployments, and requires more operational oversight and maintenance planning.

© 2026 Cisco and/or its affiliates. All rights reserved.

Latency guidelines

Network latency affects Cisco ISE performance, especially in distributed deployments. Use the latency requirements to plan authentication and replication between nodes.

Network latency requirements

Table 6. Network latency requirements

Connection Endpoints	Maximum Allowed Latency	Recommended	Impact of Exceeding
Primary PAN – other Cisco ISE nodes	300 ms*	<30 ms	Replication delays, configuration inconsistency
PSN – NADs	100 ms	<100 ms	Authentication timeouts, poor user experience
Cisco ISE – Duo	-	<5 s	Authentication delays or timeouts
Cisco ISE – CMDB	-	<50 ms	Download failures
Cisco ISE – External ID source	50 ms	<5 ms	Authentication delays or timeouts
Cisco ISE – Cisco Catalyst Center	300 ms	<200 ms	Longer execution time with >200 ms and not supported beyond 300 ms

Primary PAN to other Cisco ISE nodes: latency targets by replication publish rate

The higher the replication publish rate, measured in transactions per second (TPS), the lower the maximum allowed latency between the Primary PAN and the other Cisco ISE nodes.

Table 7. Maximum latency by replication publish rate

Replication Publish Rate	Maximum Allowed Latency
TPS ≤ 30	300 ms
30 < TPS ≤ 50	100 ms
50 < TPS ≤ 80	50 ms
TPS > 80	30 ms

To measure the Primary PAN publish rate:

1. Get tracking.log from the Primary PAN:

In the Cisco ISE Admin GUI, select Operations > Troubleshoot > Download Logs > [Primary PAN] > Debug Logs > tracking.log. Alternatively, run show logging application tracking.log | save trackingLog, then download the file from Administration > System > Local Disk Management > [Primary PAN].

2. Calculate publish rate per second:

```
awk '$0~/Publishing message for event/ {print substr($0,1,19)}' tracking.log | sort
| uniq -c
```

3. Review output for average/peak TPS to determine the correct replication latency target.

© 2026 Cisco and/or its affiliates. All rights reserved.

Deployment considerations

For geographic distribution, co-locate PSNs with the network access devices they serve and deploy regional PSN pairs for local authentication. Place monitoring nodes centrally with enough bandwidth to collect logs.

For WAN optimization, prioritize Cisco ISE traffic through QoS, avoid congested links for Cisco ISE replication, and monitor jitter and packet loss as well as latency.

High authentication rates require lower latency thresholds. Rates above 80 TPS typically require latency below 30 ms; consider dedicated network segments for Cisco ISE traffic in high-volume deployments.

While RADIUS traffic can tolerate higher latency than node replication, authentication performance significantly degrades as latency increases. Test under peak load conditions to validate performance.

Measuring Cisco ISE latency

Use ping and traceroute for basic connectivity checks, and use network monitoring tools to track latency over time. Enable Cisco ISE latency monitoring through Operations > Reports > System Summary. During peak periods, validate actual authentication latency in Live Logs, the RADIUS Authentication and Authentication Summary reports, and Log Analytics.

Cisco ISE session management and sizing

Understanding Cisco ISE session management is critical for proper deployment capacity and license planning. Each unique MAC address consumes one session license and contributes to the total session count, regardless of authentication method or network access type.

Session limits by platform

Size the deployment against the maximum session counts for the appliances assigned as PAN and MnT nodes and as PSNs.

For detailed sizing information, refer to the Performance and Scalability Guide for Cisco Identity Services Engine:

The relevant tables in that guide are Table 3, “Maximum concurrent active sessions for deployments with different SNS appliances acting as PAN, MnT, or PAN/MnT” and Table 4, “Maximum concurrent active sessions for different Cisco ISE appliances acting as PSNs”.

Session lifecycle management

Cisco ISE tracks sessions through RADIUS authentication/authorization and accounting. Understanding this lifecycle helps predict system behavior.

Table 8. Session lifecycle events

Event	Action	Impact
Authentication/Authorization	Session identified	License consumed, endpoint marked as authenticated/authorized
Accounting Start	Session fully established	Endpoint marked as started
Accounting Updates	Session refreshed	Keeps session active, updates attributes
Accounting Stop	Session terminated	Endpoint marked as terminated

© 2026 Cisco and/or its affiliates. All rights reserved.

Event	Action	Impact
Session Timeout	Session expired	Endpoint removed

Session count considerations

Each unique endpoint MAC address consumes one session, regardless of connection method. Reauthentication by the same MAC address does not create another session. A session remains active until it is terminated or times out. Missing accounting stop messages can leave orphaned sessions until timeout.

Steady state vs. peak demand

Plan for both steady-state and peak authentication demand. Sizing only for average load can cause authentication failures, policy timeouts, and user disruption during high-volume events.

Understanding load patterns

Table 9. Steady state and peak demand

Load Type	Characteristics	Examples	Planning Considerations
Steady State	Predictable, consistent baseline load	Regular business-hour usage, static endpoints	Forms your minimum capacity requirement
Peak Demand	Short-duration authentication spikes	Building access periods, shift changes, device roaming	Must drive your actual deployment sizing

Common peak demand scenarios

Peak demand can follow global business hours, synchronized shift or class changes and meetings, power outages or maintenance, and device behavior such as sleep, wake, roaming, or VPN reconnection.

Scale of peak events

Wireless roaming can generate 3–10× the normal authentication load, and mass reconnection during power recovery can generate 10–100× the baseline. Misconfigured clients can generate 100–1000× more attempts, while software updates can trigger simultaneous posture checks.

Best practices

Calculate peak transactions per second (TPS) from worst-case scenarios and size PSN capacity for peak load with N+1 redundancy. Monitor historical authentication patterns to identify peak periods, schedule maintenance outside those periods, and test PSN capacity under simulated peak conditions before production deployment.

Key principle: Always size your Cisco ISE deployment for peak demand capacity, as authentication failures during high-volume periods have the greatest user impact.

Cisco ISE Installation on Cisco Secure Network Server (SNS)

Before selecting an installation method for your Cisco SNS, consider your environment constraints, access capabilities, and time requirements. This matrix compares the four primary installation methods to help you quickly identify the most suitable approach.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 10. Cisco ISE installation methods on SNS

Installation Method	Time Required	Physical Access	Complexity	Reliability	Best Use Case
Localized (CLI)	<1 hour	No*	Low	Very High	Quickly re-image or upgrade existing operational nodes
USB Drive	~1 hour	Yes	Low	High	Single appliance installation with direct physical access
CIMC-Mapped vDVD	4-5 hours	No	High	High	Multiple remote installations with file server available
vKVM-Mapped vDVD	5-7+ hours	No	Medium	Medium**	Remote installations without file server

*Requires regular Cisco ISE CLI access to an operational node

**Most vulnerable to network interruptions during lengthy installation

For remote installations, prioritize the Localized method when available. For a fresh installation, CIMC-mapped vDVD with NFS is faster than vKVM-mapped vDVD, especially when deploying multiple nodes.

Each method requires specific prerequisites:

The Localized method requires an operational Cisco ISE node with CLI access. A USB installation requires bootable USB creation tools and physical access. CIMC-mapped vDVD requires an NFS, CIFS, or HTTP server and CIMC access; vKVM-mapped vDVD requires CIMC access and a stable network connection.

Decision guide for installing Cisco ISE on SNS

- If an operational Cisco ISE node needs reimaging or upgrading and CLI access is available, use **Method 1**, Re-Image from Localized. This takes less than one hour.
- For a new bare-metal or corrupted appliance with physical access, use **Method 2**, a bootable USB drive, which takes about one hour.
- For a remote appliance, use **Method 3**, CIMC-mapped vDVD, when an NFS, CIFS, or HTTP file server is available in the data center; the source estimates about four hours.
- Without such a file server, use **Method 4**, vKVM-mapped vDVD, which takes four to seven hours or longer.

General pre-installation checklist

Before beginning any installation, ensure these prerequisites are met:

Before installation, confirm that the SNS model or VM resources (vCPU, RAM, and disk) support the target Cisco ISE version. Download the official ISO from software.cisco.com and verify its MD5 or SHA512 hash.

Gather the static IP address and subnet mask, default gateway, primary and secondary DNS servers, NTP servers, hostname (FQDN recommended), and an initial administrator password that meets complexity requirements. Check the CIMC, SSH, and NFS firewall paths between the management station, repositories, and appliance. Schedule a maintenance window and, if upgrading an existing node, back up its configuration.

© 2026 Cisco and/or its affiliates. All rights reserved.

Detailed installation methods

Method 1: re-image from localized (CLI option 38)

The Localized method reinstalls or upgrades an operational Cisco ISE node. Copy the ISO to the appliance local disk, then start the installation from the CLI.

Table 11 (Localized re-image method advantages and disadvantages) compares the advantages and disadvantages of the Localized method.

Table 11. Localized re-image method advantages and disadvantages

Advantages	Disadvantages
Unmatched speed reduces downtime	Cannot be used on new, bare-metal appliances
High reliability and not prone to network drops	Does not support downgrading to a previous version
Minimal dependencies (CLI and repository only)	Requires sufficient free disk space for the ISO

Choose this method to reimage or upgrade an operational remote node when CLI access is available.

Before starting the copy, make sure MD5/SHA hash matches.

To reimage an operational Cisco ISE node with the Localized method:

1. Copy the Cisco ISE ISO file to the appliance's disk:/ repository using the copy command.
2. Run application configure ise and select option [25] Localised Cisco ISE Install.
3. Confirm the ISO and verify its checksum.

The appliance will automatically reboot and begin the installation.

Method 2: installation from a bootable USB drive

Use a bootable USB drive for a fresh installation on one appliance that you can access physically.

Choose this method for a fresh installation on a bare-metal appliance when you have physical access.

Table 12 (Cisco ISE releases and bootable USB tools) identifies the appropriate USB creation tool by Cisco ISE release and appliance.

Table 12. Cisco ISE releases and bootable USB tools

Cisco ISE Release	Tool
Cisco ISE Release 3.2 and later	Rufus
Cisco ISE Release 3.1	• Fedora LiveUSB-creator for SNS 3500/3600 series appliance • Rufus for SNS 3700 series appliance
Cisco ISE Release 3.0	Fedora LiveUSB-creator

When installing Cisco ISE from USB, set end-of-line (EOL) characters to **LF**, not **CR LF**.

Use a text editor, such as Notepad, that preserves **LF** end-of-line characters in configuration files. The USB installation does not work when the files use **CR LF**.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 13 (Bootable USB installation advantages and disadvantages) compares the advantages and disadvantages of USB installation.

Table 13. Bootable USB installation advantages and disadvantages

Advantages	Disadvantages
Simple and reliable process	Physical access is mandatory
No network dependency during installation	Not scalable for multiple installs
Fast installation once booted	Requires tools to create the bootable media

To install Cisco ISE from a bootable USB drive:

1. Create a bootable USB drive from the Cisco ISE ISO using a tool like Rufus/LiveUSBCreator.

If the USB creation tool shows a Use existing Live CD area, click Browse and select the Cisco ISE ISO file.

2. Plug the USB into the appliance and connect a monitor and keyboard.
3. Enter the BIOS/Boot Menu (for example, F6) and select the USB drive as the boot device.

Method 3: installation via CIMC-mapped vDVD

This remote method mounts the Cisco ISE ISO from an NFS, CIFS, or HTTP file server in the appliance data center. It combines remote access with local network speed.

Table 14 (CIMC-mapped vDVD installation advantages and disadvantages) compares the advantages and disadvantages of CIMC-mapped vDVD installation.

Table 14. CIMC-mapped vDVD installation advantages and disadvantages

Advantages	Disadvantages
Fast and reliable remote installation	Requires setting up and managing an NFS/CIFS/HTTP file server
Highly scalable for multiple installs	Complex setup with permissions and firewalls
Frees up the administrator's machine	Security requires careful NFS/CIFS/HTTP file server configuration

Choose this method for fast remote installations when an NFS, CIFS, or HTTP file server is available in the data center.

To install Cisco ISE through CIMC-mapped vDVD:

1. Place the Cisco ISE ISO on an NFS, CIFS, or HTTP file server in the data center.
2. In the CIMC vKVM client, map the NFS/CIFS/HTTP share by providing the server IP and the full path to the ISO.
3. Reboot the server, enter the boot menu (F6), and select the **Cisco Virtual CD/DVD**.

The installation will run over the fast local network.

Method 4: installation via vKVM-mapped vDVD

This method maps the Cisco ISE ISO on an administrator computer as a virtual CD/DVD drive through the CIMC vKVM client.

© 2026 Cisco and/or its affiliates. All rights reserved.

Table 15 (vKVM-mapped vDVD installation advantages and disadvantages) compares the advantages and disadvantages of vKVM-mapped vDVD installation.

Table 15. vKVM-mapped vDVD installation advantages and disadvantages

Advantages	Disadvantages
Fully remote installation from anywhere	Extremely slow (5-7+ hours)
No extra infrastructure needed	Prone to failure from network disconnects
Standard data center procedure	Can be hampered by browser/Java issues

Choose this method for a fresh remote installation when the other methods are unavailable.

The device from which the ISO is mounted should be as close as possible to the Cisco ISE SNS appliance.

The network speed between the admin workstation and the Cisco ISE appliance should be at least 1 Gbps with latency below 10 ms to ensure reliable and timely installation.

To install Cisco ISE through vKVM-mapped vDVD:

1. Log into the CIMC and launch the vKVM client (HTML5 is preferred).
2. Use the **Virtual Media** menu to map the local Cisco ISE ISO file.
3. Reboot the server, enter the boot menu (F6), and select the **Cisco Virtual CD/DVD**.

The server will boot from the mapped ISO.

Common post-installation steps

After the base OS installation is complete via any method, these steps are required:

1. Run the **setup** wizard: On the first boot, you will be prompted to run the "setup" command to configure the node's hostname, IP address, DNS, NTP, and initial administrator credentials.
2. Install patches: The base ISO is rarely the latest version. The first step after network configuration should be to download and install the latest cumulative patch for your Cisco ISE release.
3. Join to deployment: If this is a secondary node, register it to your Primary Administration Node (PAN).
4. Apply system certificates: Replace the default self-signed certificates with certificates from a trusted Certificate Authority (CA) for Admin, EAP, and Portal functions.

Scaling Cisco ISE Services

Mobile and IoT growth can increase authentication load. This section describes ways to manage that load and maintain stability during peak demand.

The impact of mobile and IoT proliferation

The explosion of mobile devices and IoT endpoints has fundamentally changed network authentication patterns, creating significant scaling challenges for Cisco ISE deployments:

Authentication volume challenges

Mobile devices, IoT sensors, and BYOD increase endpoint counts. Mobility, sleep and wake cycles, and roaming cause frequent reconnections; short-lived connections can create authentication storms at peak times. Usage patterns also vary across locations and time zones.

© 2026 Cisco and/or its affiliates. All rights reserved.

Configuration issues

Client supplicants can have incorrect certificates or outdated operating systems. Aggressive NAD timeouts, inadequate throttling, excessive load-balancer health probes, improper persistence, and insufficient logging controls can add load and overwhelm monitoring nodes.

System impact

These conditions can cause authentication spikes above designed capacity, increase database replication load between distributed nodes, and create resource contention. Delays or timeouts then degrade the user experience.

Managing authentication load

Control authentication volume by addressing both traffic sources and Cisco ISE configuration:

Network device configuration

Wired NAD settings

Set wired NAD timers to limit repeated authentication attempts: held-period, quiet-period, and ratelimit-period to 300+ seconds; tx-period to 10 seconds; inactivity to 1+ hour or disabled; and session timeout and reauthentication to 2+ hours or disabled.

Wireless controller configuration

For wireless controllers, enable Fast BSS Transition (802.11r) for compatible clients, configure client exclusion to block misbehaving endpoints temporarily, and tune EAP timers so exclusion takes effect before client retry storms. Send interim accounting updates only when new information is available or a client roams.

Cisco ISE optimization strategies

Authentication processing

To reduce authentication processing load, suppress redundant authentication logs, use authentication caching where appropriate, prune inactive endpoints, and distribute requests across PSNs with load balancing.

System monitoring

Establish a baseline for authentication patterns and alert on anomalies. Monitor authentication latency, use Log Analytics to find problematic endpoints or NADs, and apply targeted log filters during troubleshooting.

Certificate management

Proper certificate management is critical for Cisco ISE deployments to ensure secure client communications, especially for mobile devices. During EAP-TLS, endpoints authenticate the Cisco ISE EAP server certificates and the Cisco ISE EAP server on each PSN authenticates endpoint certificates. Poor certificate practices can lead to authentication failures, security vulnerabilities, and service disruptions during renewals.

Mobile device certificate challenges

When mobile devices roam between Policy Service Nodes (PSNs), they may encounter certificate trust prompts for each new PSN they connect to. This creates several issues:

If users do not respond to certificate trust prompts, authentication can fail with “5440 Endpoint abandoned EAP session and started new.” Repeated prompts can frustrate users and generate support calls.

© 2026 Cisco and/or its affiliates. All rights reserved.

Hundreds of devices across multiple PSNs compound the disruption, while certificate validation during roaming can degrade Wi-Fi performance.

Wildcard vs. Multi-SAN certificates

To prevent certificate trust prompts during roaming, consolidate PSN identity with unified server certificates. Organizations typically choose between wildcard certificates that cover all subdomains or multi-SAN certificates that specify each PSN explicitly. Each approach offers distinct advantages and trade-offs:

Table 16. Wildcard and multi-SAN certificate comparison

Feature	Wildcard Certificates	Multi-SAN Certificates
Format	*.example.com	ise1.example.com, ise2.example.com, ...
Coverage	All subdomains automatically	Only explicitly listed hostnames
Scalability	Excellent - new PSNs automatically covered	Limited - requires certificate reissuance
Security	Higher risk if compromised	Limited exposure to listed hostnames
Cost	Generally lower (single certificate)	Higher (more complex certificate)
Renewal	Must modify at least one field (such as OU)	Can add/remove SANs during renewal
Best Use	Growing deployments with frequent changes	Static environments with fixed node count

Certificate best practices

Use public CAs for guest and BYOD portals to avoid trust prompts on unmanaged devices, and use a dedicated subdomain such as ise.example.com to limit wildcard certificate scope. For production, prefer a public CA or private enterprise PKI over self-signed certificates or the Cisco ISE internal CA.

Ensure CRLs come from the same CAs, verify that OCSP and CRL Distribution Point (CDP) endpoints are reachable from every Cisco ISE node, and test CRL and OCSP validation during maintenance windows. Set each trusted certificate's usage flags as appropriate:

- **Trust for authentication within Cisco ISE** for server certificates
- **Trust for client authentication and Syslog** for EAP clients, syslog servers, and SAML IdP
- **Trust for certificate-based admin authentication** for admin access
- **Trust for authentication of Cisco Services** for Cisco ISE feed services

For Cisco ISE Messaging Service (IMS), use either an internal CA or external PKI consistently across the deployment. Verify certificate chains after upgrades, patches, restores, and PAN promotions.

Recommended renewal process

1. Verify node synchronization.

Ensure all nodes are synchronized before renewal. Check replication status in Administration > System > Deployment.

2. Update the trust chain.

© 2026 Cisco and/or its affiliates. All rights reserved.

If you are using a new CA, upload and trust its certificates first. Verify the certificate chain before continuing.

3. Modify the certificate subject.

Change at least one certificate-subject field when generating a new CSR. Typically, change the Organizational Unit (OU) for tracking; for example, add a renewal date such as OU=Renewed-MMYYYY.

4. Generate and process the CSR.

Create a CSR with the modified subject and have the CA sign it. Upload and bind the new certificate without assigning roles yet.

5. Verify replication.

Confirm that the new certificate appears on every node by logging in to each one. Manually synchronize any node that does not show it.

6. Assign roles after replication.

After successful replication, assign the appropriate system roles and verify that the certificate appears in the correct services.

7. Schedule a controlled restart.

To minimize impact, use scheduled restart in Cisco ISE Release 3.3 or later. If possible, schedule the restart outside business hours.

8. Validate the new certificate and clean up.

Test authentication flows. After successful validation, remove the old certificates.

Renewal planning

Monitor certificate expiration alarms and plan renewals 30–60 days ahead. Document the subject-field changes used in each renewal and create a new private key and CSR when using external certificate tools. For larger deployments, consider wildcard certificates. Test the renewal process in a lab before using it in production.

Domain name service (DNS)

Configure DNS and caching to support Cisco ISE reliability and performance, especially in large deployments.

DNS server types

Understanding the roles of different DNS servers helps design reliable name resolution infrastructures. The three core types are:

Authoritative DNS servers

Authoritative servers host the official DNS zone data for one or more domains and deliver final, trusted answers directly to requesting clients.

A primary or master authoritative DNS server holds a writable copy of zone data; a secondary or slave server replicates that data. Authoritative servers return final answers without further lookups.

Recursive DNS servers

Recursive servers (resolvers) handle client requests by performing the full resolution process on behalf of the client.

© 2026 Cisco and/or its affiliates. All rights reserved.

They query root, TLD, and authoritative servers in sequence until they find the answer.

Recursive DNS servers cache responses to speed later queries. ISPs and enterprise networks commonly use them to provide a single lookup service for end devices.

Recursive DNS is relevant for Cisco ISE because it can introduce significant latency and potential points of failure, impacting authentication performance and reliability if DNS lookups are slow or misconfigured.

Non-recursive DNS servers

Non-recursive servers only answer queries from their own zone data or cache without performing additional queries. When they lack data, they either refer to the query to another DNS server or return an error.

Nonrecursive DNS servers can forward unresolved queries to a specified resolver, restrict lookup paths, or enforce resolution policies. They do not perform iterative or recursive lookups themselves.

In Cisco ISE environments, non-recursive DNS servers are useful when you want to tightly control which DNS queries are resolved locally and which are forwarded, such as for compliance, security, or to ensure that Cisco ISE only queries trusted DNS sources for identity-related lookups.

Table 17. DNS server types

Server Type	Key Behavior	Typical Use Case
Authoritative	Direct answers from zone data	Hosting company DNS, domain owners
Recursive	Full lookup chain + local caching	ISP resolvers, internal DNS caches
Non-Recursive	Answers from local data or cache, with no recursion	Forwarders, policy-controlled resolvers

Cisco ISE and Active Directory integration

Cisco ISE integration with Active Directory depends on precise and fast DNS resolution of critical records such as:

Cisco ISE relies on DNS records for domain controllers (DCs), global catalogs (GCs), and Kerberos key distribution centers (KDCs).

Missing or misconfigured DNS entries can result in:

Missing or incorrect DNS records can delay or time out authentication, cause LDAP or Kerberos failures, and prevent Cisco ISE from joining AD domains or querying group memberships.

To prevent such issues, authoritative resolution of AD-related queries is essential.

DNS server configuration in Cisco ISE

Cisco ISE supports configuration of up to three DNS servers per node. This allows for:

Up to three DNS servers per Cisco ISE node provide redundant resolution paths, distribute queries, and support failover during DNS outages.

DNS caching in Cisco ISE

Prior to Cisco ISE Release 3.1, Cisco ISE did not support DNS caching. In Cisco ISE Releases 3.1 and 3.2, DNS caching is available but must be manually enabled; in Cisco ISE Release 3.3 and later, it is enabled by

© 2026 Cisco and/or its affiliates. All rights reserved.

default. Without DNS caching, every authentication request or syslog event referencing a fully qualified domain name (FQDN) generates a DNS query, which in high-volume environments can flood upstream DNS servers, introduce latency, and degrade performance. The DNS caching feature stores resolved IP addresses locally for a configurable duration, reducing repetitive queries and improving performance.

Benefits of DNS caching

DNS caching reduces authentication latency by serving repeated lookups locally. It also lowers traffic to external DNS servers and supports higher throughput under load. For syslog and RADIUS traffic that uses FQDNs, caching avoids repeated resolution for each event. Cached entries can also provide resolution when DNS servers are temporarily unreachable.

How to enable DNS caching via Cisco ISE CLI

1. Log in to Cisco ISE CLI with administrative privileges.
2. Enter configuration mode:

```
configure terminal
```

3. Enable DNS caching and set the TTL (Time-To-Live):

```
service cache enable hosts ttl <ttl_in_seconds>
```

Example: `service cache enable hosts ttl 3600`

This sets the cache validity period to 1 hour (3600 seconds).

DNS infrastructure practices

Configure authoritative DNS servers for AD zones, use separate forwarders for other domains, and define domain-based mappings to send queries to the appropriate resolvers. Validate resolution regularly with nslookup and the AD diagnostic tool in Cisco ISE.

Performance considerations

Recursive lookups may add hundreds of milliseconds to response time. Under load, this latency compounds and affects policy decision delays.

Prefer authoritative servers for core identity services, especially in federated or multi-domain environments.

Deploy DNS caching in tandem with authoritative resolution for optimal throughput and resiliency.

By thoughtfully configuring DNS parameters and enabling caching, administrators can greatly enhance the reliability and responsiveness of Cisco ISE, especially in large-scale, security-critical deployments.

Network Device and Load Balancer Best Practices

Configure network devices and load balancers to support authentication performance, reduce authentication storms, and maintain service availability in large Cisco ISE deployments.

© 2026 Cisco and/or its affiliates. All rights reserved.

RADIUS/TACACS+ server configuration

Core network device settings

Table 18. Core network device settings

Setting	Recommendation	Purpose
Server Count	Maximum 3 RADIUS/TACACS+ servers per device	Prevents excessive authentication attempts
Dead Timer	10+ minutes	Prevents authentication storms after Cisco ISE node recovery
Retransmit Value	2-3 retries	Balances reliability with unnecessary load
Timeout Value	5-10 seconds	Allows sufficient time for authentication processing

If you need more than three servers, use load balancers rather than configuring additional direct server entries.

Wired device best practices

These best practices focus on accounting configuration and 802.1X timer optimization to prevent authentication storms and unnecessary load on Cisco ISE.

Accounting configuration

Enable both start and stop accounting messages for accurate session tracking and license utilization. Reduce interim-update traffic by using longer intervals:

```
aaa accounting update newinfo periodic 2880
```

Configure session timeouts to balance security and performance. As accounting traffic grows, monitor MnT performance because accounting can add significant database load.

802.1X timer optimization

Improper timer settings are a common cause of authentication storms. Configure these critical timers on all wired devices:

Table 19. 802.1X timer recommendations

Timer Parameter	Recommended Value	Impact if Set Too Low
held-period	300+ seconds	Authentication storms after failures
quiet-period	300+ seconds	Excessive retries from failing devices
ratelimit-period	300+ seconds	High TPS during connection events
tx-period	10 seconds	Unnecessary EAPOL traffic
inactivity	3600+ seconds or disable	Frequent disconnects of idle devices
session timeout	7200+ seconds or disable	Regular reauthentication load

© 2026 Cisco and/or its affiliates. All rights reserved.

Timer Parameter	Recommended Value	Impact if Set Too Low
reauthenticate	7200+ seconds or disable	Unnecessary authentication refreshes

Sample Catalyst switch configuration

```
interface GigabitEthernet1/0/1
description 802.1X-Optimized-Configuration
authentication periodic
authentication timer reauthenticate 7200
authentication timer restart 300
authentication timer inactivity 3600
dot1x pae authenticator
dot1x timeout quiet-period 300
dot1x timeout tx-period 10
dot1x timeout supp-timeout 30
dot1x timeout ratelimit-period 300
dot1x max-reauth-req 3
dot1x max-req 3
```

These timer values should be adjusted based on your specific network requirements and device types. Higher values reduce authentication load but may increase the time to detect disconnected devices.

Catalyst 9800 series wireless controllers best practices

Calling-Station-ID and Called-Station-ID format

Configure the Calling-Station-ID and Called-Station-ID attributes to ensure consistent MAC address formatting and improve client tracking. Using uppercase hexadecimal format with hyphen delimiters for Calling-Station-ID enables reliable endpoint identification and profiling across authentication and accounting sessions.

```
9800(config)#radius-server attribute wireless accounting call-station-id-case upper
9800(config)#radius-server attribute wireless authentication call-station-id-case
upper
9800(config)#radius-server attribute wireless accounting call-station-id-delimiter
hyphen
9800(config)#radius-server attribute wireless authentication call-station-id-
delimiter hyphen
```

Interim accounting management

By default, interim accounting is enabled with the `aaa accounting Identity default start-stop group radius` command. This setting is recommended for most deployments.

From IOS XE Cupertino 17.9.1, the no accounting-interim command is introduced under the policy profile to disable interim accounting.

```
9800(config)#wireless profile policy <POLICY-PROFILE-NAME>
9800(config-wireless-policy)#no accounting-interim
```

Consider disabling interim accounting updates for these reasons:

Interim accounting updates can generate unnecessary traffic, increase error rates, and affect alarm thresholds and other venue authentication metrics.

© 2026 Cisco and/or its affiliates. All rights reserved.

Fast Transition (802.11r) implementation

Enable standard Fast Transition (FT) to reduce authentication load during roaming. Configure SSIDs that use WPA2-Enterprise (802.1X-SHA1) for standard, rather than adaptive, FT (802.11r) over the air rather than over the distribution system.

Only Apple and Samsung clients understand adaptive FT. Standard FT also allows Windows, other Android, and ChromeOS clients to fast-roam. Adaptive FT can cause connectivity problems for some older Android clients; refer to CSCvu24770: Android clients fail to connect when Adaptive 802.11r is enabled.

```
9800(config-wlan)#security ft
9800(config-wlan)#no security ft over-the-ds
9800(config-wlan)#security wpa akm ft dot1x
9800(config-wlan)#security wpa akm dot1x
```

Client exclusion and EAP timers

To neutralize RADIUS load caused by misconfigured/misbehaving clients, and to impose admission control after a widespread RADIUS failure/restart (for example, after a 9800 reboot or network outage), 802.1X Client Exclusion should be configured. With the default EAP retransmission timers, Client Exclusion may have a harder time coming into play (as clients may “abandon the EAP session”), and so shorter EAP timers may be beneficial (and provide for a better user experience in the case of packet loss during roams.) The default EAP retransmission timeouts are 30 seconds; instead, use 5-second timeouts.

Increasing the exclusion list timeout to 90 seconds, from its default value of 60 seconds, will provide better protection to the authentication infrastructure, at the cost of potential frustration for end users who may be attempting manually to connect to the network.

```
9800(config)#wireless wps client-exclusion dot1x-timeout
9800(config)#wireless wps client-exclusion dot1x-auth
9800(config)#wireless security dot1x identity-request timeout 5
9800(config)#wireless security dot1x identity-request retries 5
9800(config)#wireless security dot1x request timeout 5
9800(config)#wireless security dot1x request retries 5

9800(config)#wireless profile policy <POLICY-PROFILE-NAME>
9800(config-wireless-policy)#exclusionlist timeout 90
```

Session timeout optimization

The 802.1X Session Timeout is set to 1800 seconds (30 minutes). Load on the RADIUS server can be reduced by increasing the Session Timeout (maximum is 86400, one day). We recommend a Session Timeout of 12 hours, 43200 seconds.

```
9800(config)#wireless profile policy default-policy-profile
9800(config-wireless-policy)#session-timeout 43200
```

Load balancer implementation

Load balancers distribute authentication traffic across multiple PSNs, providing high availability, fault tolerance, and optimal performance. They prevent authentication timeouts during peak loads and enable seamless maintenance without service interruption. When properly configured, load balancers improve authentication reliability while simplifying PSN scaling as environments grow.

© 2026 Cisco and/or its affiliates. All rights reserved.

Design principles

Size each PSN cluster for N+1 redundancy so it can carry the full load after one node fails. Configure health probes to detect PSN failures before RADIUS timeouts, retain client-to-PSN affinity through each authentication session, and use consistent hashing based on Calling-Station-ID (MAC address).

Protocol-specific configuration

RADIUS load balancing

Table 20 (Load balancer persistence settings) lists the settings for RADIUS persistence.

Table 20. Load balancer persistence settings

Persistence Setting	Recommendation	Impact if Misconfigured
Method	Calling-Station-ID hash	Without persistence, authentication state breaks and CoA fails
Sticky Timer	Match NAD session timeout	• Too short: breaks CoA functionality • Too long: prevents proper failover
Distribution	Round-robin with persistence	Ensures even PSN utilization while maintaining session state
Health Checks	Every 15-30 seconds	Frequent enough to detect failures before user impact

Use source IP persistence with a Calling-Station-ID (MAC address) hash as the primary method. Fall back to NAS-IP-Address when Calling-Station-ID is unavailable. Round-robin distribution with sticky sessions can preserve both load distribution and session state.

Important: Without proper persistence configuration, round-robin distribution will send different authentication requests for the same session to different PSNs, breaking authentication state and preventing CoA functionality.

Avoid Cisco IOS XE RADIUS load balancing for Cisco ISE deployments, as currently it does not have mac stickiness to guarantee all authentication and accounting requests for the same endpoint session reach the same PSN.

Advanced persistence strategies

For hardware load balancers such as F5 or Citrix ADC, extract and hash Calling-Station-ID (RADIUS attribute 31). For redundant load balancers, synchronize persistence tables between the primary and backup devices.

TACACS+ load balancing

TACACS+ load balancing does not require session persistence because of the protocol design. Configure appropriate health checks using TACACS authentication probes.

Health check configuration

Table 21. Load balancer health checks

Load Balancer	Health Check Type	Interval	Success Threshold	Failure Threshold
F5 BIG-IP	RADIUS Auth	30 seconds	3	3
Citrix ADC	RADIUS	5 seconds	2	3

© 2026 Cisco and/or its affiliates. All rights reserved.

For detailed load balancing configuration examples, refer to the Cisco ISE Load Balancing Guides.

Security: Mitigating Blast RADIUS (CVE-2024-3596)

Blast RADIUS (CVE-2024-3596) allows attackers to exploit MD5 prefix collisions to modify RADIUS responses and potentially bypass authentication. The mitigation options help secure Cisco ISE deployments.

Mitigation strategies

Table 22. Blast RADIUS mitigation approaches

Approach	Implementation	Considerations
RADIUS over DTLS/TLS	Preferred method, DTLS supported natively by Cisco ISE	• Expect ~15% performance impact • Requires compatible NAD firmware
Message-Authenticator	Enable attribute for all RADIUS requests/responses	• Compatible with most devices • Minimal impact
IPsec Tunnels	Create encrypted tunnels between NADs and PSNs	• Limited to 50 tunnels per PSN • Complex configuration

DTLS implementation guidelines

Configure DTLS on both Cisco ISE PSNs and network devices, and deploy trusted certificates. Monitor performance after implementation; if authentication volume is high, consider additional PSNs.

Message-Authenticator configuration

Message-Authenticator verifies message integrity without encryption. It is required in all RADIUS requests and responses, included automatically in EAP-based authentication, and must be configured explicitly for non-EAP traffic.

For Cisco ISE acting as a RADIUS server, select **Require Message-Authenticator for all RADIUS Requests** in the allowed protocols

For Cisco ISE acting as a RADIUS client, apply Cisco ISE Releases 3.1 Patch 10, 3.2 Patch 8, 3.3 Patch 5, or 3.4 Patch 2.

For detailed implementation steps, refer to the Cisco Security Advisory and Mitigation Guide.

Profiling and Endpoint Management

Use endpoint profiling to identify devices and apply policies. Balance data collection with resource use.

Choosing the right probes

Each probe collects specific endpoint attributes that help identify devices on your network. This section will help you select the most appropriate probes for your environment.

© 2026 Cisco and/or its affiliates. All rights reserved.

Understanding probe attributes

Table 23 (Profiling probes, attributes, and use cases) summarizes the attributes collected by each probe and their common uses.

Table 23. Profiling probes, attributes, and use cases

Probe	Key Profiling Attributes	Common Endpoint Profiling Use Cases
RADIUS	• MAC Address (OUI) • IP Address • NDG values	Identify device vendors through MAC address OUI. Especially useful for IP phones, mobile devices, and gaming consoles. Provides MAC-to-IP bindings and location information.
RADIUS w/Device Sensor	• CDP/LLDP • DHCP • User-Agent • mDNS • H323/SIP	Collects rich endpoint data without additional infrastructure. Captures CDP/LLDP, DHCP, HTTP, and voice/video protocol information.
RADIUS w/ACIDex	• MAC Address • UDID • Operating System • Platform/Device Type	Excellent for profiling remote access VPN clients with detailed OS and device information. Provides unique device identifiers for MDM correlation.
SNMP	• MAC Address/OUI • CDP/LLDP • ARP tables	Identifies Cisco devices (phones, cameras, APs). Collects CDP/LLDP data and populates MAC-to-IP bindings from device ARP tables.
DHCP	• DHCP	Captures vendor IDs, OS fingerprints, hostnames, and custom identifiers. Provides critical MAC-to-IP bindings to support other probes.
DNS	• FQDN	Useful when standardized naming conventions are used for hostnames.
HTTP	• User-Agent	Detects operating systems (though some browsers may mask the actual OS).
NetFlow	• Protocol • Source/Dest IP • Source/Dest/Ports	Identifies endpoints with unique traffic patterns or anomalous behavior.
NMAP	• Operating System • Port information • Service Version Info • SMB data • Endpoint SNMP data	Detects OS, open ports, running services, and domain information. Useful for endpoints running SNMP agents like printers and cameras.

© 2026 Cisco and/or its affiliates. All rights reserved.

Probe	Key Profiling Attributes	Common Endpoint Profiling Use Cases
AD	• AD presence • Operating System and Version • AD Domain	Verifies managed domain assets and collects OS details from Active Directory.
pxGrid	• IoT Asset • Custom Attributes	Gathers IoT asset information from integrated solutions and supports custom attributes.
Custom Attributes	• Customer defined	Enables flexible classifications based on your organization's specific needs.

Detailed probe attributes

This list provides more detail about the key attributes collected by each probe.

Table 24. Profiling probe attributes

Probe	Key Profiling Attributes
RADIUS	• Calling-Station-ID (OUI) • Framed-IP-Address • Location • Device Type (NAD)
RADIUS w/Device Sensor	• cdpCacheAddress • cdpCacheCapabilities • cdpCacheDeviceId • cdpCachePlatform • cdpCacheVersion • lldpCacheCapabilities • lldpSystemDescription • lldpSystemName • dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • dhcp-user-class-id • host-name • client-fqdn • mud-url

© 2026 Cisco and/or its affiliates. All rights reserved.

Probe	Key Profiling Attributes
	• User-Agent • H323DeviceName • H323DeviceVendor • H323DeviceVersion • mdnsVSMclassidentifier • mdnsVSMsrvidentifier • mdnsVSMtxt_identifier • sipDeviceName • sipDeviceVendor • sipDeviceVersion
RADIUS w/ACIDex	• device-platform • device-platform-version • device-type
SNMP Query	• MACAddress(OUI) • MAC-IP (ARP) • cdpCacheAddress • cdpCacheCapabilities • cdpCacheDeviceId • cdpCachePlatform • cdpCacheVersion • lldpCacheCapabilities • lldpSystemDescription • lldpSystemName • mud-url
SNMP Trap	• MACAddress(OUI) (MAC Notification)
DHCP	• dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • dhcp-user-class-id • host-name • client-fqdn

© 2026 Cisco and/or its affiliates. All rights reserved.

Probe	Key Profiling Attributes
	• mud-url
DNS	• FQDN
HTTP	• User-Agent
NetFlow	• IPV4DSTADDR • IPV4SRCADDR • PROTOCOL • L4SRCPORT • L4DESTPORT • MINTTL • MAXTTL
NMAP	• operating-system • tcp-x • udp-x • tcp/udp Service Version • ePO agent • SMB attributes • SMB.domain • SMB.fqdn • SMB.operating-system • Endpoint SNMP Attributes • hrDeviceDescr • sysDescr • sysLocation • sysName
AD	• AD-Host-Exists • AD-Join-Point • AD-Operating-System • AD-OS-Version
pxGrid	• assetDeviceType • assetIpAddress • assetMacAddress • assetName

© 2026 Cisco and/or its affiliates. All rights reserved.

Probe	Key Profiling Attributes
	• assetProductId • assetProtocol • assetVendor • Custom Attributes
Other	• Custom Attributes • PortalUser • DeviceRegistrationStatus

Optimizing global profiler settings

Enable **Endpoint Attribute Filter** in production to store and replicate only relevant attributes; add an attribute to the allowed list by creating a profiler condition and policy that use it. During a lab deployment, initial discovery, or troubleshooting, disable the filter to collect all potential attributes and identify attributes that may improve visibility or profiler policies.

Keep **Custom Attribute for Profiling Enforcement** disabled unless specifically needed

Enable **profiler forwarder persistence queue** setting to optimize endpoint update event processing

Endpoint management

Endpoint purge recommendations

Monitor your endpoint database regularly and implement purge policies to maintain optimal performance:

Keep the endpoint database below 2 million entries. Purge stale or inactive devices using default rules for guest and registered endpoints, and create custom purge rules for the environment.

Sample use case

Cisco SNS 3795 appliances support different endpoint capacities based on deployment sizes:

Table 25. Endpoint purge recommendations

Deployment Size	Active Endpoints	Inactive Endpoints	Total Endpoints
Large	2,000,000	2,000,000	4,000,000
Medium	150,000	3,850,000	4,000,000
Small	50,000	3,950,000	4,000,000

For optimal performance, monitor your active-to-inactive endpoint ratio and implement appropriate purge policies based on your deployment size.

Cisco ISE Profiler Feed Service

Cisco ISE Profiler Feed Service automates the delivery of new or updated profiler policies and conditions provided by Cisco as well as OUI updates. It is important to keep your profiling database (policies, conditions, and OUIs) current by regular Profiler Feed updates.

© 2026 Cisco and/or its affiliates. All rights reserved.

Update options

Cisco ISE Profiler Feed Service offers two update options:

The online subscription option retrieves scheduled or on-demand updates directly from Cisco and requires internet access. The offline option lets you download updates separately and import them manually in environments without internet access.

Comprehensive best practices summary

General recommendations

Use Device Sensors when possible and enable Endpoint Attribute Filter in production. Avoid collecting the same data from multiple sources, and direct each endpoint's profiling data to the same PSN when possible.

Probe-specific recommendations

RADIUS probe

For the RADIUS probe, set the authentication session and reauthentication timer to at least two hours (eight or more recommended), the idle or inactivity timer to at least one hour, and the accounting update timer to at least one day. Suppress unnecessary authentication and accounting requests.

HTTP probe

For the HTTP probe, prefer Device Sensor or URL redirection over SPAN or RSPAN. If HTTP SPAN is required, focus on network chokepoints such as the internet edge or wireless controllers, and use intelligent SPAN or tap options to limit traffic volume.

DHCP probe

For the DHCP probe, use Device Sensor when available. Otherwise, prefer DHCP relays (IP Helpers) over SPAN. Set DHCP leases between one day and one week, and avoid leases shorter than four hours.

SNMP probe

For the SNMP probe, use Device Sensor when available, set polling intervals to at least eight hours, and disable polling for intermittently connected devices.

NetFlow probe

Use selectively for specific use cases to avoid excessive load.

pxGrid probe

Limit to 1–2 PSNs to avoid duplicate data collection and replication.

Custom attributes

Disable when not needed for profiling.

Leverage external data sources when available (asset management systems, etc.).

Custom profiles

Use **Get All Endpoints** or Endpoint Analysis Tool to identify profile gaps.

Leverage organizational naming standards for custom profile creation.

Authorization policy

Ensure sufficient network access during the profiling process.

© 2026 Cisco and/or its affiliates. All rights reserved.

Use Logical Profiles for policy conditions whenever possible.

External Databases and Active Directory

Effective integration with external identity sources is crucial for Cisco ISE performance and reliability. This section covers best practices for policy set organization, authorization rule optimization, and Active Directory integration to ensure efficient authentication processing and minimize external lookups.

Policy set organization

Policy sets provide logical grouping of authentication and authorization rules, improving both performance and manageability. Properly structured policy sets reduce processing overhead and simplify troubleshooting.

Best practices for policy sets

Table 26. Policy set practices

Practice	Benefit	Implementation
Logical Grouping	Improves readability and maintenance	Group by use case (e.g., Guest, Corporate, IoT)
Rule Efficiency	Reduces processing time	Place most-used policy sets first in evaluation order
Condition Specificity	Minimizes rule evaluation	Use specific conditions based on initial RADIUS attributes
Modular Design	Simplifies updates and testing	Isolate complex or frequently changing policies

Use network device groups or location attributes as initial conditions for policy sets to create a hierarchical policy structure that scales with network growth.

Authorization rule optimization

Authorization rules should be designed to minimize external database lookups while ensuring effective policy enforcement. Properly structured rules reduce authentication latency and improve overall system performance.

Rule processing strategies

Table 27. Authorization rule processing strategies

Strategy	Implementation	Benefit
Process Order	Place most frequently matched rules first	Reduces average processing time
Attribute Source Prioritization	Check internal attributes before external ones	Minimizes expensive lookups
Authentication Store Leverage	Use Network Access:AuthenticationIdentityStore to determine if lookup is necessary	Prevents extra external queries
Avoid MAC-to-AD Lookups	Never authorize MAC addresses against Active Directory	Eliminates unnecessary domain queries
Condition Complexity	Use simpler conditions for high-volume rules	Decreases processing overhead

© 2026 Cisco and/or its affiliates. All rights reserved.

Regularly analyze LiveLogs to identify your most frequently triggered rules and optimize their position and conditions. During performance troubleshooting, focus on rules that trigger external lookups.

The most efficient authorization policies follow this evaluation sequence:

1. First check internal endpoint attributes (profiling data).
2. Then verify certificate or internal user properties when available.
3. Only perform external lookups (AD, LDAP) when necessary.

Active Directory integration

Active Directory integration requires careful planning to ensure reliable, high-performance authentication. Proper configuration of DNS, site services, and domain controllers significantly impacts authentication speed and reliability.

Performance considerations

Table 28. Active Directory configuration considerations

Configuration Area	Recommendation	Impact
DC Selection	• Configure AD Sites and Services properly • Ensure Cisco ISE servers are in the correct AD sites	Ensures Cisco ISE communicates with local/optimal domain controllers, reducing authentication latency by 50-200 ms
Allowed Domains	• Restrict to only domains containing user accounts needed for authentication	Eliminates unnecessary domain queries, reducing lookup overhead and potential timeouts
AD Scopes	• Create specific scopes targeting only required join points and domains	Prevents Cisco ISE from querying all domains for every authentication, significantly improving performance in multi-domain environments
DNS Configuration	• Enable DNS caching with 180-300 second TTL values	Reduces repeated DNS lookups by 90%, dramatically improving authentication response times
Dedicated Resources	• Deploy dedicated domain controllers for authentication services in environments with high TPS	Prevents authentication delays during peak periods and isolates Cisco ISE traffic from general AD operations
Connection Monitoring	• Implement regular latency checks between Cisco ISE and DCs • Alert when latency exceeds the baseline (for example, 10 ms)	Provides early warning of network issues affecting authentication performance before user impact occurs

Implementation best practices

Enable DNS Caching: Configure with appropriate TTL values to reduce repeated lookups:

```
service cache enable hosts ttl 180
```

Create dedicated test accounts to validate authentication and attribute retrieval. Use the Active Directory Diagnostics Tool regularly to check health and connectivity, and monitor AD request latency. In multi-domain environments, create a join point for each domain and use it in the relevant authorization rules.

© 2026 Cisco and/or its affiliates. All rights reserved.

For high-volume deployments, consider implementing dedicated Active Directory infrastructure for authentication services to isolate from general-purpose directory operations.

When properly configured, external database integration should add minimal latency to authentication processing while providing the rich identity context needed for effective policy decisions.

Logging and Monitoring

Use logging and monitoring to support Cisco ISE operations, troubleshooting, and security auditing. Configure log collection to meet hardware requirements without degrading system performance.

Hardware and storage considerations

Table 29. Logging hardware and storage recommendations

Environment	Recommendation	Rationale
Physical Appliances	SSD drives	Higher IOPS for better logging performance
Virtual Machines	High-throughput storage	Ensures consistent log processing
Large Deployments	Dedicated MnT nodes	Separates logging from authentication workloads

For virtual environments, disable VM snapshots on Cisco ISE nodes. Snapshots can severely impact performance and are not supported for backup/recovery.

Remote logging targets

Mnts as syslog targets optimization

Table 30. Monitoring and Troubleshooting nodes as syslog targets

Targets	Recommendation
Enable LogCollector, LogCollector2	Enable to use **ISE Messaging Service** for UDP Syslogs delivery to MnT.
Disable SecureSyslogCollector, TCPLogCollector, SecureSyslogCollector2, TCPLogCollector2	Must be disabled to reduces redundant data

External syslog configuration

Use IP addresses for external syslog targets to avoid DNS dependency, and limit the number of targets to reduce processing overhead. If targets must use FQDNs, consider enabling DNS caching.

Log suppression and filtering

RADIUS suppression settings

In production, suppress repeated failed authentications and successful reauthentications. For troubleshooting, disable suppression selectively through collection filters for specific clients. Exclude load-balancer probes and monitoring scripts from event collection through health-check filters.

© 2026 Cisco and/or its affiliates. All rights reserved.

Logging category management

Table 31. Logging category management

Category	Recommendation	Rationale
RADIUS Diagnostics	Disable MnT targets	Extremely verbose, impacts MnT performance
TACACS Diagnostics	Disable MnT targets	Extremely verbose, impacts MnT performance

Performance monitoring and troubleshooting

Investigating performance issues

When Live Logs or the Cisco ISE GUI is slow, inspect collector-stats.log for categories with more than one million entries. Use Cisco ISE Log Analytics or external tools to find noisy NADs, misconfigured endpoints, or users generating automated traffic. Check database performance with show-tech, including slow queries and tablespace issues.

RADIUS authentication monitoring

Review RADIUS authentication summaries for success and failure rates by identity store, response times by PSN, authentication-method distribution, and failure-reason patterns.

Operational data management and retention

Operational data purging

Monitor database utilization daily and adjust retention periods as needed. If storage is constrained, shorten retention or reinstall MnT nodes with larger disks; the filesystem cannot be resized without a reinstall.

Backup strategy

Schedule Cisco ISE configuration backups weekly and operational backups monthly to preserve historical data.

Advanced analysis

In Cisco ISE Release 3.1 or later, use **Log Analytics** to identify RADIUS authentication trends and top talkers. In Cisco ISE Release 3.3 or later, use detailed authentication reports with millisecond timestamps to locate bottlenecks. For advanced correlation and long-term storage, consider Splunk or a similar SIEM platform.

Regular log analysis helps identify authentication pattern changes that may indicate misconfiguration, security issues, or capacity constraints before they impact users.

Posture Compliance

Cisco ISE assesses endpoint posture before granting network access. This section describes practices for a secure, scalable posture deployment.

Redirection and posture flow

How Cisco ISE posture flow works

1. Initial Connection: Endpoint connects to the network and receives limited access through a restricted VLAN or DACL.

© 2026 Cisco and/or its affiliates. All rights reserved.

2. Web Redirection: HTTP/HTTPS traffic is intercepted and redirected to a Cisco ISE client provisioning portal.
3. Client Provisioning: Users download and install the necessary posture agent if not present.
4. Posture Assessment: The agent performs compliance checks against defined policies.
5. Access Adjustment: Upon successful verification, Cisco ISE triggers a CoA to update access privileges.

Best practices for redirection

Prefer redirection-based posture flows for the user experience. Use VLANs, DACLs, or ACLs to segment authorization rules, and dedicate PSNs to different connection media when possible.

Timers and session management

Configure NAD accounting to maintain accurate session state. With load balancing, evaluate the load-balancer persistence timer, Cisco ISE posture lease timer, Cisco ISE posture periodic reassessment (PRA) timer, and RADIUS session timeout together. Set the session timeout below the persistence timer, and set the PRA continuous monitoring interval to at least 60 minutes.

Posture configuration: agentless vs. agent-based

Agentless posture

Agentless posture supports simpler endpoint assessments using native operating-system tools. It requires port 5985 for PowerShell and port 22 for SSH, regular posture feed updates, local administrator credentials, and distinct posture requirements and policies.

Agent-based posture

Agent-based posture supports more comprehensive assessments and controls. Deploy Cisco Secure Client with the Cisco ISE posture module, configure client provisioning policies for each operating system, and use dACLs to restrict access until the endpoint is compliant and remediation is complete.

Client provisioning and remediation

Maintain a current repository of posture agents, compliance modules, and remediation options. Automate remediation where possible, such as antimalware updates, and give users clear guidance through custom portal messages.

Administrative practices

Apply role-based administrator access controls, document and review policy changes, and test posture changes in a lab before deployment. Monitor posture compliance through dashboards and reports.

Mobile Device Management (MDM)

Integration and trust establishment

Cisco ISE integrates MDM or Unified Endpoint Management (UEM) servers using supported APIs.

Exchange trusted certificates between Cisco ISE and the MDM server to secure API communication. For Microsoft Intune, ensure the PSN certificates are trusted by the Intune instance. With Cisco ISE Release 3.1 or later, use a device GUID rather than a MAC address for more reliable identification when mobile operating systems randomize MAC addresses.

MDM server configuration in Cisco ISE

Add the MDM/UEM server as an external MDM resource in Cisco ISE:

© 2026 Cisco and/or its affiliates. All rights reserved.

1. Navigate to **Administration > Network Resources > External MDM.**
2. Configure server details including hostname, port, and credentials.

Device identification and compliance

Use certificate-based authentication and device GUIDs for compliance queries, especially for modern iOS and Android endpoints; avoid MAC-based identification when possible. On the MDM platform, check registration, enrollment, and compliance status. Configure network policies so only compliant devices receive permitted access.

Multiple MDM environments

Enable **Query Multiple MDM / UEM Integrations** in **Administration > System > General MDM / UEM Settings**. With multiple MDM platforms, use MDM server-name conditions in Cisco ISE authorization rules and logical profiles to direct devices to the appropriate platform by device type or ownership.

Policy and access control

Segment Cisco ISE authorization by MDM compliance state. Give compliant devices normal or full access; limit noncompliant devices to a remediation VLAN or restricted ACL, or redirect them for remediation; and direct unknown or unenrolled devices to the MDM or BYOD onboarding portal.

Always refer official Cisco documentation for version-specific implementation details.

© 2026 Cisco and/or its affiliates. All rights reserved.