



Cisco Identity Services Engine Installation Guide, Release 3.4

First Published: 2024-07-05

Last Modified: 2026-04-15

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Network Deployments in Cisco ISE

- [Cisco ISE network architecture, on page 1](#)
- [Cisco ISE deployment terminology, on page 2](#)
- [Node types and personas in distributed deployments, on page 3](#)
- [Cisco ISE deployment models, on page 4](#)
- [Small network deployments, on page 4](#)
- [Medium-sized network deployments, on page 6](#)
- [Large network deployments, on page 7](#)
- [Cisco ISE deployment sizing guidelines, on page 9](#)
- [Switch and Wireless LAN Controller configuration required to support Cisco ISE functions, on page 10](#)

Cisco ISE network architecture

Cisco ISE network architecture integrates specialized nodes and deployment models to deliver comprehensive, scalable network access control and security policy enforcement.

The core components include nodes with specific personas that work together to manage network access and security. It supports various deployment models, including standalone and distributed setups, suited for small to large networks. This architecture ensures scalable, secure, and efficient policy enforcement across wired, wireless, and VPN connections.

Cisco ISE network architecture components

Cisco ISE architecture includes these components:

Table 1: Components of Cisco ISE network architecture

Cisco ISE network components	Description
Nodes (personas or roles)	Cisco ISE servers that run one or more roles. A node can run multiple personas.
Network resources	Infrastructure that controls or provides network access, such as switches, WLCs, VPN devices and so on.
Endpoints	Users or devices trying to connect to the network, such as laptops, phones, printers, IoT and so on.

Cisco ISE nodes and personas

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

Table 2: Cisco ISE nodes and personas

Persona	Role	Use cases
Administration persona	Manages configuration and system settings	Primary or secondary admin nodes
Policy Service persona (PSN)	Makes access-control decisions and enforces policy The policy information point (PIP) is where external information is communicated to the Policy Service persona. For example, external information might be a Lightweight Directory Access Protocol (LDAP) attribute.	RADIUS and TACACS+ processing
Monitoring persona	Collects logs and reporting data	Troubleshooting, audits, reports
pxGrid persona	Shares context with other systems	Integrations with security tools

Cisco ISE deployment terminology

This book 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: <ul style="list-style-type: none"> • 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-redirection 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.



Restriction 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

Cisco ISE deployment models illustrate how Cisco ISE nodes and personas are arranged to meet specific size, performance, and availability requirements.

Standalone deployment

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

Distributed deployment

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.

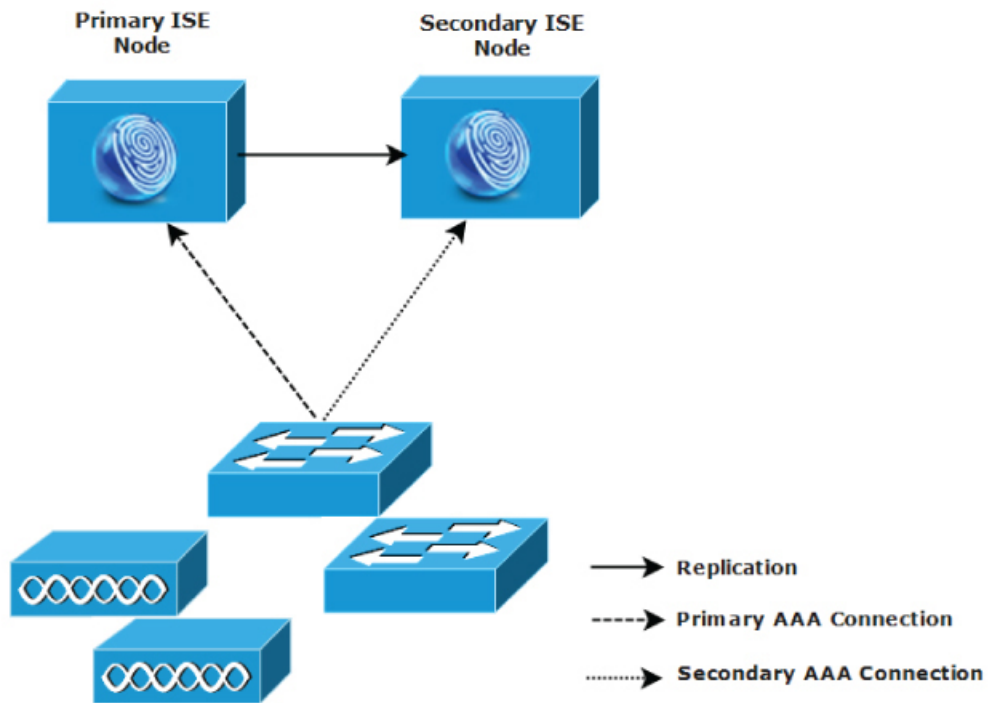
Small network deployments

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



282092

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

A split deployment in Cisco ISE separates key personas across different nodes, for example, running the Administration and Monitoring personas on one node and the Policy Service persona on separate nodes. This deployment model improves performance and scalability by isolating policy processing from management and reporting functions.

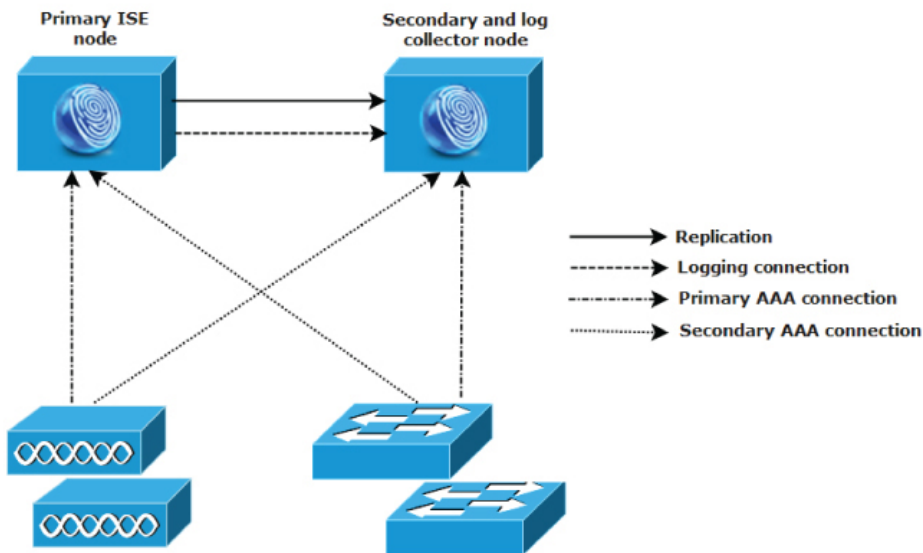
Split deployment provides better load distribution and ensures that the secondary node remains functional during normal network operations. This design also supports deployment expansion.

In split deployments, 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.

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



282093

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.

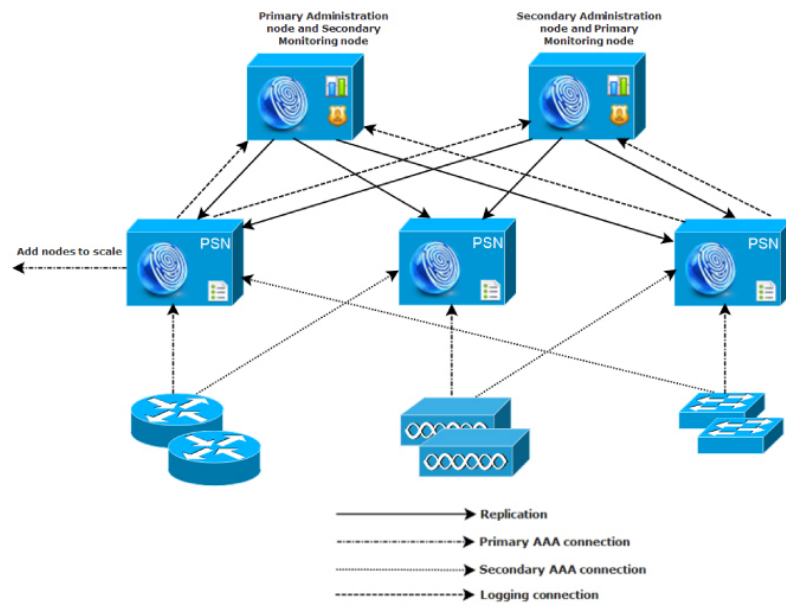
If the amount of log traffic increases in a network, you can dedicate one or two secondary nodes for log collection.



Restriction

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.

Figure 3: Medium-sized network deployment in Cisco ISE



Large network deployments

Large network deployments in Cisco ISE use distributed nodes for optimal load sharing, high authentication volume support, operational resilience, and scalable policy enforcement.

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.

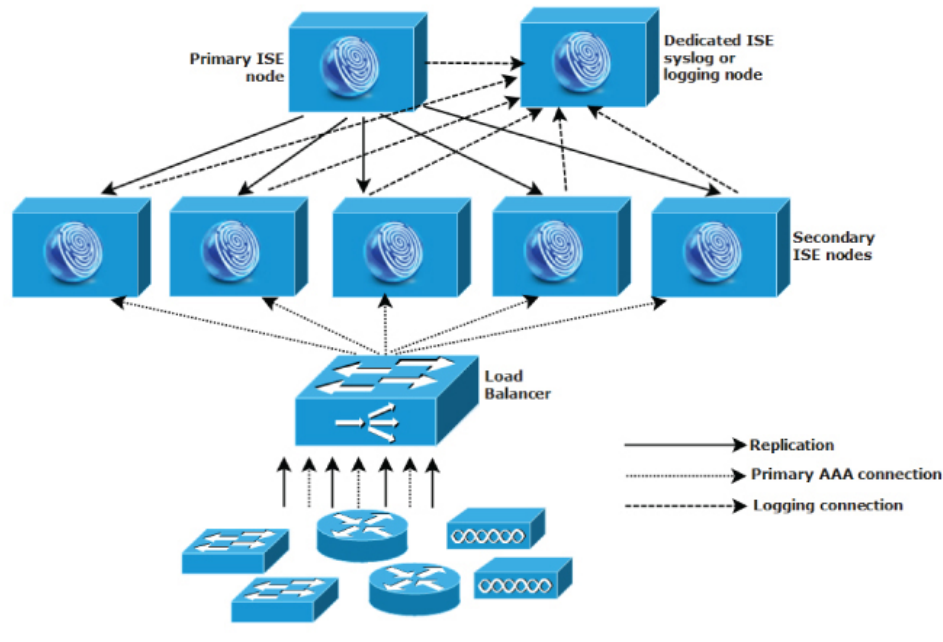
You can also consider having the appliances send logs to both a Monitoring node and a generic syslog server. A generic syslog server provides redundant backup if the Monitoring node goes down.

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

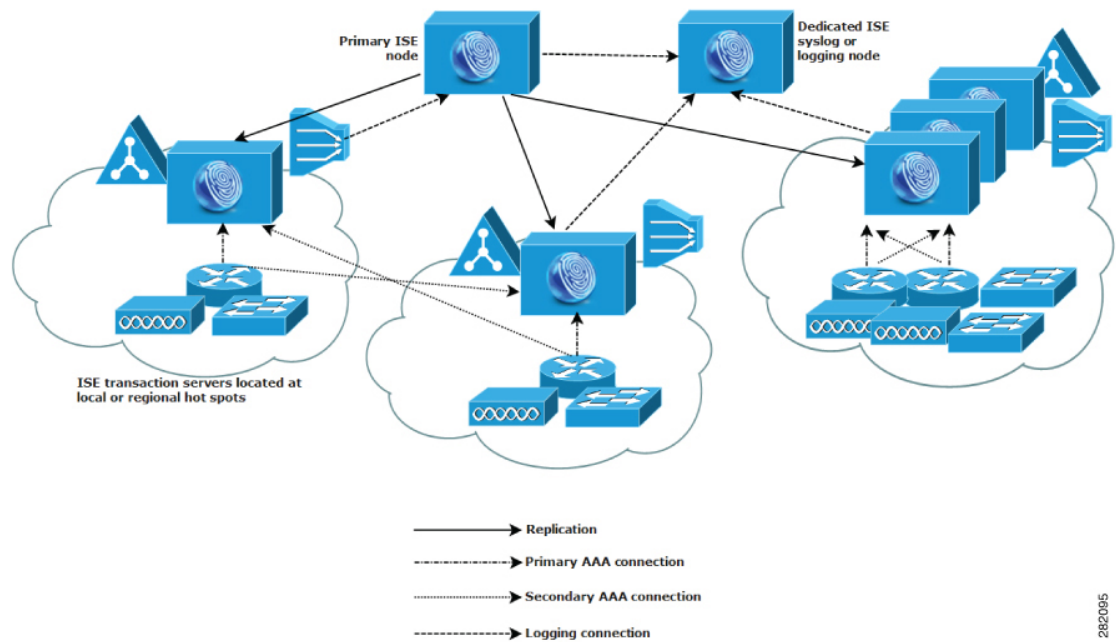


Dispersed network deployments

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



282095

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](#).



CHAPTER 2

Cisco Secured Network Server Series Appliances and Virtual Machine Requirements

- [Cisco ISE hardware and virtual appliance requirements, on page 11](#)
- [VMware cloud solutions for Cisco ISE, on page 29](#)
- [Virtual machine size recommendations, on page 29](#)
- [Disk space requirements for VMs in a Cisco ISE deployment, on page 30](#)
- [Disk space guidelines for Cisco ISE, on page 31](#)
- [CPU requirements for hypervisors, on page 33](#)

Cisco ISE hardware and virtual appliance requirements

Cisco ISE can be installed on Cisco Secure Network Server (SNS) hardware or virtual appliances. The virtual machine should have the same system resources as the Cisco SNS hardware appliances to achieve similar performance and scalability as the Cisco ISE hardware appliance. This section lists the hardware, software, and virtual machine requirements for installing Cisco ISE.

Cisco ISE pxGrid Direct Service and Cisco ISE pxGrid Direct Pusher require a CPU that supports the x86-64-v2 architecture or higher. If the CPU does not support x86-64-v2 or if a hypervisor masks the required CPU features for a virtual machine, Cisco ISE pxGrid Direct Service and Cisco ISE pxGrid Direct Pusher do not start.



Note Harden your virtual environment and ensure that all security updates are current. Cisco is not liable for any security issues found in hypervisors.

For all VMs, you must use the **application stop** command before using the **halt** command or powering off the VM to prevent database corruption issues.



Caution Cisco ISE does not support VM snapshots to back up data on any virtual environment. Enabling the Snapshot feature on the VM might corrupt the configuration. If this happens, you may need to reimagine the VM.

Cisco SNS hardware appliances

For Cisco SNS 3600 series appliances, see [Cisco SNS-3600 Series Appliance Hardware Installation Guide](#).

For Cisco SNS 3700 series appliances, see [Cisco SNS-3700 Series Appliance Hardware Installation Guide](#).

For Cisco SNS 3800 series appliances, see [Cisco SNS-3800 Series Appliance Hardware Installation Guide](#).

For information about the supported hardware platforms for your version of Cisco ISE, see the [Release Notes for Cisco Identity Services Engine](#).

Support for Cisco SNS 3800 series appliance

The Cisco SNS 3800 series appliances are based on the Cisco Unified Computing System (Cisco UCS) C225 M8 Rack Server and are configured specifically to support Cisco ISE. Cisco SNS 3800 series appliances are designed to deliver high performance and efficiency for a wide range of workloads.

The Cisco SNS 3800 series appliances are available in these models:

- Cisco SNS 3815 (SNS-3815-K9)
- Cisco SNS 3855 (SNS-3855-K9)
- Cisco SNS 3895 (SNS-3895-K9)

Cisco SNS 3815 appliance is ideal for small deployments. Cisco SNS 3855 and Cisco SNS 3895 appliances have several redundant components such as hard disks and power supplies and are suitable for larger deployments that require highly reliable system configurations. Cisco SNS 3895 is recommended for PAN and MnT personas.



Note

- You must use only these OVA, ISO, and upgrade bundle files for Cisco SNS 3800 appliances:
 - Cisco-vISE-300-3.4.0.608b.ova
 - Cisco-vISE-600-3.4.0.608b.ova
 - Cisco-vISE-1200-3.4.0.608b.ova
 - Cisco-vISE-2400-3.4.0.608b.ova
 - ise-3.4.0.608b.SPA.x86_64.iso
 - ise-upgradebundle-3.1.x-3.3.x-to-3.4.0.608b.SPA.x86_64.tar.gz
 - ise-urtbundle-3.4.0.608b-1.0.0.SPA.x86_64.tar.gz
- Cisco SNS 3800 appliances are supported from Cisco ISE release 3.4 patch 4 onwards.
- Cisco SNS 3855 appliance can be configured with one hard disk or four hard disks. It is recommended to enable only the PSN or pxGrid persona if your Cisco SNS 3855 appliance is configured with only one hard disk.

This table describes the hardware specifications of Cisco SNS 3800 series appliances.

Table 3: Cisco SNS 3800 series appliance hardware specifications

Cisco SNS 3800 series appliance	RAM	CPU cores	Number of hard disks	Total hard disk capacity	RAID
Cisco SNS-3815-K9	64 GB	16 cores, 32 threads	NVME-1	960 GB	NA
	64 GB	16 cores, 32 threads	SED-1	960 GB	RAID-0
	64 GB	16 cores, 32 threads	SED-FIPS-1	1.6 TB	RAID-0
Cisco SNS-3855-K9	128 GB	24 cores, 48 threads	NVME-1	960 GB	NA
	128 GB	24 cores, 48 threads	NVME-4	1.9 TB	RAID-10
	128 GB	24 cores, 48 threads	SED-1	960 GB	RAID-0
	128 GB	24 cores, 48 threads	SED-4	1.9 TB	RAID-10
	128 GB	24 cores, 48 threads	SED-FIPS-1	1.6 TB	RAID-0
	128 GB	24 cores, 48 threads	SED-FIPS-4	3.2 TB	RAID-10
Cisco SNS-3895-K9	256 GB	24 cores, 48 threads	NVME-8	3.8 TB	RAID-10
	256 GB	24 cores, 48 threads	SED-8	3.8 TB	RAID-10
	256 GB	24 cores, 48 threads	SED-FIPS-8	6.4 TB	RAID-10

For more information, see the [Cisco SNS 3800 Series Appliance Hardware Installation Guide](#).

VMware virtual machine requirements

You can use the VMware migration feature to migrate VM instances (running any persona) between hosts. Cisco ISE supports both hot and cold migration.

- Hot migration is also called live migration or vMotion. You do not need to shut down or power off Cisco ISE during hot migration. You can migrate the Cisco ISE VM without any interruption in its availability.
- Cisco ISE must be shutdown and powered off for cold migration. Cisco ISE does not allow to stop or pause the database operations during cold migration. Hence, ensure that Cisco ISE is not running and active during the cold migration.

The 300 GB OVA templates are sufficient for Cisco ISE nodes that serve as dedicated Policy Service or pxGrid nodes.

The 600 GB and 1.2 TB OVA templates are recommended to meet the minimum requirements for nodes that run the Administration or Monitoring persona.

If you need to customize the disk size, CPU, or memory allocation, you can manually deploy Cisco ISE using the standard .iso image. However, it is important that you ensure the minimum requirements and resource reservations specified in this document are met. The OVA templates simplify ISE virtual appliance deployment by automatically applying the minimum resources required for each platform.

Table 4: OVA template reservations

OVA template type	Number of CPUs	CPU reservation (in GHz)	Memory (in GB)	Memory reservation (in GB)
Evaluation	4	No reservation.	16	No reservation.
Extra Small	8	8	32	32
Small (SNS 3615)	16	16	32	32
Medium (SNS 3655)	24	24	96	96
Large (SNS 3695)	24	24	256	256
Small (SNS 3715)	24	24	32	32
Medium (SNS 3755)	40	40	96	96
Large (SNS 3795)	40	40	256	256
Small (SNS 3815)	32	32	64	64
Medium (SNS 3855)	48	48	128	128
Large (SNS 3895)	48	48	256	256



Note You can enable only the PSN persona on Extra Small VM. PAN and MnT personas are not supported for this node.

Reserve CPU and memory resources to match the required allocation. Not reserving enough resources can significantly affect ISE performance and stability.

This table lists the VMware virtual machine requirements.

Table 5: VMware virtual machine requirements

Requirement type	Specifications
CPU	

Requirement type	Specifications
	<ul style="list-style-type: none"> • Evaluation <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of CPU cores: 4 CPU cores • Production <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: <ul style="list-style-type: none"> • SNS 3600 series appliance: <ul style="list-style-type: none"> • Extra Small: 8 • Small: 16 • Medium: 24 • Large: 24 <p>Note The number of cores is twice that found in the equivalent Cisco SNS 3600 series because of hyperthreading. For example, in a small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU cores or 16 threads.</p> <ul style="list-style-type: none"> • SNS 3700 series appliance: <ul style="list-style-type: none"> • Small: 24 • Medium: 40 • Large: 40 <p>Note The number of cores is twice that found in the equivalent Cisco SNS 3700 series because of hyperthreading. For example, in a small network deployment, you must allocate 24 vCPU cores to meet the CPU specification of SNS 3715, which has 12 CPU cores or 24 threads.</p> <ul style="list-style-type: none"> • SNS 3800 series appliance: <ul style="list-style-type: none"> • Small: 32 • Medium: 48 • Large: 48

Requirement type	Specifications
	<p>Note The number of cores is twice that found in the equivalent Cisco SNS 3800 series because of hyperthreading. For example, in a small network deployment, you must allocate 32 vCPU cores to meet the CPU specification of SNS 3815, which has 16 CPU cores or 32 threads.</p>
Memory	<ul style="list-style-type: none"> • Evaluation: 16 GB • Production <ul style="list-style-type: none"> • Extra Small: 32 GB • Small: <ul style="list-style-type: none"> • 32 GB for SNS 3615 and SNS 3715 • 64 GB for SNS 3815 • Medium: <ul style="list-style-type: none"> • 96 GB for SNS 3655 and SNS 3755 • 128 GB for SNS 3855 • Large: 256 GB for SNS 3695, SNS 3795, and SNS 3895
Hard disks	<ul style="list-style-type: none"> • Evaluation: 300 GB • Production <p>300 GB to 2.4 TB of disk storage (size depends on deployment and tasks).</p> <p>We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM.</p> <p>Note When you create the VM for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use more than one virtual disk to meet the disk space requirement, the installer may not recognize all the disk space.</p>

Requirement type	Specifications
Storage and file system	<p>The storage system for the Cisco ISE virtual appliance requires a minimum write performance of 50 MB per second and a read performance of 300 MB per second. Deploy a storage system that meets these performance criteria and is supported by VMware server.</p> <p>You can use the show tech-support command to view the read and write performance metrics.</p> <p>We recommend the VMFS file system because it is most extensively tested, but other file systems, transports, and media can also be deployed provided they meet the above requirements.</p>
Disk controller	<p>Paravirtual or LSI Logic Parallel</p> <p>For best performance and redundancy, a caching RAID controller is recommended. Additionally, battery-backed controller cache can significantly improve write operations.</p> <p>Note Updating the disk SCSI controller of a Cisco ISE VM from another type to VMware Paravirtual may render it not bootable.</p>
NIC	<p>1 NIC interface required (two or more NICs are recommended; six NICs are supported).</p> <p>Cisco ISE supports E1000E and VMXNET3 adapters.</p> <p>Note You have to remap the ESXi adapter to synchronize it with the Cisco ISE adapter order.</p>
VMware virtual hardware version/Hypervisor	<ul style="list-style-type: none"> • OVA templates: VMware version 14 or higher on ESXi 6.7, ESXi 7.0, and ESXi 8.0. • ISO file supports ESXi 6.7, ESXi 7.0, and ESXi 8.0.

Incorrect configuration of VMware High Availability (HA) or Distributed Resource Scheduler (DRS) policies may trigger false host failure events, which can cause ESXi to restart your Cisco ISE virtual machines unexpectedly. To maintain deployment stability and prevent Cisco ISE service disruption, ensure that your VMware virtual machines are configured according to VMware recommendations.

Linux KVM requirements

Table 6: Linux KVM requirements

Requirement type	Minimum requirements
CPU	

Requirement type	Minimum requirements
	<ul style="list-style-type: none"> • Evaluation <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: 4 CPU cores • Production <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: <ul style="list-style-type: none"> • SNS 3600 series appliance: <ul style="list-style-type: none"> • Extra Small: 8 • Small: 16 • Medium: 24 • Large: 24 <p>Note The number of cores is twice that of an equivalent Cisco SNS 3600 series appliance, due to hyperthreading. For example, for a small network deployment, you must allocate 16 vCPU cores to match the CPU specification of SNS 3615, which has 8 CPU cores or 16 threads.</p> • SNS 3700 series appliance: <ul style="list-style-type: none"> • Small: 24 • Medium: 40 • Large: 40 <p>Note The number of cores is twice that of an equivalent Cisco SNS 3700 series appliance, due to hyperthreading. For example, for a small network deployment, you must allocate 24 vCPU cores to meet the CPU specification of SNS 3715, which has 12 CPU cores or 24 threads.</p> • SNS 3800 series appliance: <ul style="list-style-type: none"> • Small: 32 • Medium: 48 • Large: 48

Requirement type	Minimum requirements
	<p>Note The number of cores is twice that of an equivalent Cisco SNS 3800 series appliance, due to hyperthreading. For example, for a small network deployment, you must allocate 32 vCPU cores to match the CPU specification of SNS 3815, which has 16 CPU cores or 32 threads.</p>
Memory	<ul style="list-style-type: none"> • Evaluation: 16 GB • Production <ul style="list-style-type: none"> • Extra Small: 32 GB • Small: <ul style="list-style-type: none"> • 32 GB for SNS 3615 and SNS 3715 • 64 GB for SNS 3815 • Medium: <ul style="list-style-type: none"> • 96 GB for SNS 3655 and SNS 3755 • 128 GB for SNS 3855 • Large: 256 GB for SNS 3695, SNS 3795, and SNS 3895
Hard disks	<ul style="list-style-type: none"> • Evaluation: 300 GB • Production <p>300 GB to 2.4 TB of disk storage (size depends on deployment and tasks).</p> <p>We recommend using hard disks with a minimum speed of 10,000 RPM on your VM host server.</p> <p>Note When you create the VM for Cisco ISE, use a single virtual disk that meets the storage requirement. If you use multiple virtual disks to meet disk space requirements, the installer might fail to detect the total disk space.</p>
KVM Disk Device	<p>Disk bus - virtio, cache mode - none, I/O mode - native</p> <p>Use preallocated RAW storage format.</p>

Requirement type	Minimum requirements
NIC	1 NIC interface required (two or more NIC interfaces are recommended; six NIC interfaces are supported). Cisco ISE supports VirtIO drivers. We recommend VirtIO drivers for better performance.
Hypervisor	KVM on QEMU 2.12.0-99 or above

Microsoft Hyper-V requirements

Table 7: Microsoft Hyper-V requirements

Requirement type	Minimum requirements
CPU	

Requirement type	Minimum requirements
	<ul style="list-style-type: none"> • Evaluation <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: 4 CPU cores • Production <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: <ul style="list-style-type: none"> • SNS 3600 series appliance: <ul style="list-style-type: none"> • Extra Small: 8 • Small: 16 • Medium: 24 • Large: 24 <p>Note The number of cores is twice that of the equivalent Cisco SNS 3600 series, due to hyperthreading. For example, for a small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU cores or 16 threads.</p> • SNS 3700 series appliance: <ul style="list-style-type: none"> • Small: 24 • Medium: 40 • Large: 40 <p>Note The number of cores is twice that of the equivalent Cisco SNS 3700 series, due to hyperthreading. For example, for a small network deployment, you must allocate 24 vCPU cores to meet the CPU specification of SNS 3715, which has 12 CPU cores or 24 threads.</p> • SNS 3800 series appliance: <ul style="list-style-type: none"> • Small: 32 • Medium: 48 • Large: 48 <p>Note The number of cores is twice that of the equivalent Cisco SNS 3800 series, due to hyperthreading. For example, for a small network deployment, you must allocate 32 vCPU cores to meet the CPU specification of SNS 3815, which has 16 CPU cores or 32 threads.</p>

Requirement type	Minimum requirements
Memory	<ul style="list-style-type: none"> • Evaluation: 16 GB • Production <ul style="list-style-type: none"> • Extra Small: 32 GB • Small: <ul style="list-style-type: none"> • 32 GB for SNS 3615 and SNS 3715 • 64 GB for SNS 3815 • Medium: <ul style="list-style-type: none"> • 96 GB for SNS 3655 and SNS 3755 • 128 GB for SNS 3855 • Large: 256 GB for SNS 3695, SNS 3795, and SNS 3895
Hard disks	<ul style="list-style-type: none"> • Evaluation: 300 GB • Production <p>300 GB to 2.4 TB of disk storage (size depends on deployment and tasks).</p> <p>We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM.</p> <p>Note Create the VM for Cisco ISE with a single virtual disk that meets the storage requirement. If you use multiple virtual disks, the installer may not detect the total disk space.</p>
NIC	1 NIC interface required (two or more NICs are recommended, and six NICs are supported).
Hypervisor	Hyper-V (Microsoft)



Note Cisco ISE supports Azure Stack HCI 23H2 and later versions. The virtual machine requirements and the installation procedure for the Cisco ISE VMs in the Azure Stack HCI are the same as that of Microsoft Hyper-V.

Nutanix AHV requirements



Caution You must deploy Cisco ISE on Nutanix AHV using the standard .iso image. Do not attempt to deploy or import Cisco ISE OVA templates into Nutanix AHV. Doing so breaks the system's SMBIOS generation, resulting in an unsupported UDI and permanently preventing the node from being licensed.

This table specifies the recommended resource reservations for different types of deployment on Nutanix AHV:

Type	Number of CPUs	CPU reservation	Memory (in GB)	Memory reservation (in GB)	Hard disks
Evaluation	4	No reservation	16	No reservation	300 GB
Extra Small	8	8	32	32	300 GB
Small	16	16	32	32	600 GB
Medium	24	24	96	96	1.2 TB
Large	24	24	256	256	2.4 TB (4*600 GB)

Note these points when deploying Cisco ISE on Nutanix AHV:

- Memory is automatically reserved by default. Assign the amount specified in the Cisco ISE sizing table. No additional configuration is required.
- Nutanix AHV does not support CPU reservation features. There is no MHz or GHz guarantee, and no options for `cpu_reservation` or `cpu_shares` in the GUI or CLI across all AOS versions.
- Nutanix AHV uses fair-share scheduling. CPU time is allocated proportionally based on the number of vCPUs assigned to each VM. For example, a VM with 24 vCPUs receives approximately three times the CPU time of a VM with 8 vCPUs.

Follow these guidelines to ensure optimal performance:

- Keep the total number of vCPUs on a host at or below the number of physical cores to avoid CPU oversubscription
- Avoid placing CPU-intensive or unpredictable workloads on the same host as Cisco ISE to protect ISE performance.

You must do these configurations on Nutanix AHV before you install Cisco ISE:

- Create a VM on Nutanix AHV and keep the VM powered off.
- If you are using AOS 6.8 or earlier versions, access the Nutanix CVM using ssh login and run these commands:
 - `<acropolis> vm.serial_port_create <Cisco ISE VM Name> type=kServer index=0`
 - `<acropolis> vm.update <Cisco ISE VM Name> disable_branding=true`
 - `<acropolis> vm.update <Cisco ISE VM Name> disable_hyperv=true`

If you are using AOS 7.0, access the Nutanix CVM using ssh login and run these commands:

- `<acropolis> vm.serial_port_create <Cisco ISE VM Name> type=kServer index=0`
- `<acropolis> vm.update <Cisco ISE VM Name> disable_branding=true`
- Exit Acropolis CLI, power on the VM, and install Cisco ISE using the standard .iso image.

Table 8: Nutanix AHV requirements

Requirement type	Minimum requirements
CPU	<ul style="list-style-type: none"> • Evaluation: <ul style="list-style-type: none"> • Clock speed: 2.0 GHz or faster • Number of cores: 2 CPU cores • Production: <ul style="list-style-type: none"> • Clock Speed: 2.0 GHz or faster • Number of Cores <ul style="list-style-type: none"> • Extra Small: 8 processors (4 cores with hyperthreading enabled) • Small: 16 processors (8 cores with hyperthreading enabled) • Medium: 24 processors (12 cores with hyperthreading enabled) • Large: 24 processors (12 cores with hyperthreading enabled) <p>Cisco ISE supports hyperthreading. We recommend that you enable hyperthreading, if it is available.</p> <p>Note Hyperthreading can improve overall performance, but supported scaling limits for each virtual machine appliance remain unchanged. Allocate CPU resources based on the required number of physical cores instead of logical processors.</p>
Memory	<ul style="list-style-type: none"> • Evaluation: <ul style="list-style-type: none"> • Basic: 4 GB (for evaluating guest access and basic access policy flows) • Advanced: 16 GB (for evaluating advanced features such as pxGrid, Internal CA, SXP, Device Administration, and Passive Identity Services) • Production: <ul style="list-style-type: none"> • Extra Small: 32 GB • Small: 32 GB • Small: 96 GB • Large: 256 GB

Requirement type	Minimum requirements
Hard disks	<ul style="list-style-type: none"> • Evaluation: 300 GB • Production: 300 GB to 2 TB of disk storage (size depends on deployment and tasks). We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. <p>Note You must use four 600 GB hard disks for 2.4 TB hard disk support.</p>
KVM disk device	Disk bus - SCSI
NIC	<p>1 GB NIC interface required (two or more NICs are recommended; six NICs are supported).</p> <p>Cisco ISE supports VirtIO drivers. We recommend VirtIO drivers for better performance.</p>
Hypervisor	AOS - 6.8 and 7.0, Nutanix AHV - 10.0

Red Hat OpenShift requirements

You can deploy Cisco ISE release 3.4 patch 4 and later VMs on Red Hat OpenShift Virtualization platform. This enables you to manage both VM and container workloads on a single platform.

Review these requirements before you deploy a Cisco ISE VM on Red Hat OpenShift platform.

- Cisco ISE must be deployed on OpenShift platform using the standard Cisco ISE ISO image. Deploying Cisco ISE using OVA templates is not supported.
- Cisco ISE supports Red Hat OpenShift container platform 4.19 and later versions.
- You must install the OpenShift Virtualization plug-in to deploy Cisco ISE.
- You must install the OpenShift Container Network Interface (CNI) for network configuration.

Ensure you meet these prerequisites before installing Cisco ISE on OpenShift platform:

- Create the storage infrastructure for Cisco ISE on OpenShift platform. Configure persistent volumes, storage classes, and persistent volume claims to meet CPU, memory, and other resource requirements for Cisco ISE VMs.
- Create a bootable volume for the Cisco ISE ISO file. Choose **Bootable Volume > Add Volume > ISO image** and upload the Cisco ISE ISO file. Enter the required details in the **Volume Mode**, **Access Mode**, **Volume Name**, and **Preferences** fields and then click **Save**.
- Configure a secondary-VLAN interface. Choose **Networking > Network Attachment Definitions** and create a secondary network.

Do not use the pod network for Cisco ISE configuration.

- Create YAML files to configure a VM. In the YAML file, specify the VM settings such as CPU cores, disks, and boot order.
- Choose **Virtualization > Overview > Create Virtual Command Line Tools** and use the **oc** and **virtctl** OpenShift Command Line Interface utilities to create partitions based on Cisco ISE VM resource requirements.

You can also create a pod to upload the ISO file.

- Ensure that the persistent volume claims and VM are on the same node.

Choose **Virtual Machine > Create > YAML file** to create a VM. You can monitor the installation progress from the **Console > VNC** page.

The installation process for Cisco ISE on OpenShift platform is the same as on other VM platforms. For information on how to install Cisco ISE using the ISO image, see [Install Cisco ISE using Cisco Integrated Management Interface, on page 35](#).



Note You must use only this ISO file for Cisco ISE release 3.4 to support the Red Hat OpenShift platform: `ise-3.4.0.608b.SPA.x86_64.iso`

VMware cloud solutions for Cisco ISE

On any public cloud platform, configure your VPN to allow the VMware engine to connect to on-premises deployments and to other required devices and services. You can deploy Cisco ISE on VMware cloud solutions using these public cloud platforms:

- VMware Cloud on Amazon Web Services (AWS): Host Cisco ISE on a software-defined data center provided by VMware Cloud on AWS. Configure the appropriate security group policies on VMware Cloud (in the **Networking and Security > Security > Gateway Firewall Settings** page) to allow access to on-premises deployments and other required devices and services.
- Azure VMware Solution: Azure VMware Solution runs VMware workloads natively on Microsoft Azure. You can host Cisco ISE as a VMware virtual machine.
- Google Cloud VMware Engine: The Google Cloud VMware Engine runs software-defined data centers by VMware. You can host Cisco ISE as a VMware virtual machine using the VMware Engine.

For more information on deploying Cisco ISE on cloud platforms, see [Deploy Cisco Identity Services Engine Natively on Cloud Platforms](#).

Virtual machine size recommendations

The VM appliance specifications should match those of physical appliances used in a production environment.

Follow these guidelines when allocating resources for the appliance:

- Do not share or oversubscribe resources across multiple guest VMs. Use OVF templates to assign adequate resources. If you install Cisco ISE manually using the ISO image, ensure you assign equivalent reservations.

If you do not allocate the specified resources, performance degradation or service failure might occur. To avoid these issues, deploy dedicated VM resources.

If you deploy Cisco ISE manually without the recommended reservations, you must closely monitor your appliance's resource utilization. Increase resources as needed to ensure proper health and functioning of the Cisco ISE deployment.

- If you are using the OVA templates for installation, check these settings in the **Edit Settings** page (under the **Virtual Hardware** tab), after the installation is complete:
 - Ensure that you assign the resource reservations that are specified in the [VMware virtual machine requirements, on page 13](#) section in the **CPU/Memory Reservation** field to ensure proper health and functioning of the Cisco ISE deployment.
 - Ensure that the CPU usage in the **CPU Limit** field is set to **Unlimited**. Setting a limit for CPU usage impacts system performance. If a limit is set, shut down the VM client, remove the limit, and restart the client.
 - Ensure that the memory usage in the **Memory Limit** field is set to **Unlimited**. Setting a limit for memory usage will impact the system performance.
 - Ensure that the **Shares** option is set as **High** in the **Hard Disk** area.

Admin and MnT nodes rely heavily on disk usage. Using shared disk storage VMware environment might degrade disk performance. You must increase the number of disk shares allocated to a node to improve performance.

- You can deploy Policy Service nodes on VMs with less disk space than Administration or Monitoring nodes. The minimum disk space for any production Cisco ISE node is 300 GB.
- VMs can be configured with one to six NICs. Configure VMs with at least two NICs when possible. Additional interfaces support services such as profiling, guest services, or RADIUS.



Note If you decrease the RAM or CPU allocation for a VM, you must reimage Cisco ISE with the new VM configuration. However, increasing the RAM or CPU capacity does not require reimaging.

Disk space requirements for VMs in a Cisco ISE deployment

This table provides the recommended Cisco ISE disk-space allocation for running a VM in a production deployment.



Note To boot a GPT partition with 2 TB or more, change the firmware from **BIOS** to **EFI** in the VM settings boot mode.

Table 9: Recommended disk space for VMs

Cisco ISE persona	Minimum disk space for evaluation	Minimum disk space for production	Recommended disk space for production	Maximum disk space
Standalone Cisco ISE	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration only	300 GB	600 GB	600 GB	2.4 TB
Distributed Cisco ISE, Monitoring only	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Policy Service only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, pxGrid only	300 GB	300 GB	300 GB	2.4 TB
Distributed Cisco ISE, Administration and Monitoring (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration, Monitoring, and Policy Service (and optionally, pxGrid)	300 GB	600 GB	600 GB to 2.4 TB	2.4 TB



Note Additional disk space is required to store local debug logs and staging files. Extra space is also needed to handle log data during an upgrade, when the Primary Administration node temporarily becomes a Monitoring node.

Disk space guidelines for Cisco ISE

Consider these guidelines when determining the disk space for Cisco ISE:

- Cisco ISE must be installed on a single disk in a VM.
- Disk allocation varies based on logging retention requirements. On any node that has the Monitoring persona enabled, 60 percent of the VM disk space is allocated for log storage. A deployment with 25,000 endpoints generates approximately 1 GB of logs per day.

For example, if you have a Monitoring node with 600 GB VM disk space, 360 GB is allocated for log storage. If 100,000 endpoints connect to this network every day, it generates approximately 4 GB of logs per day. In this case, you can store 76 days of logs in the Monitoring node, after which you must transfer the old data to a repository and purge it from the Monitoring database.

For extra log storage, you can increase the VM disk space. For every 100 GB of disk space that you add, you get 60 GB more for log storage.

If you increase the disk size of your virtual machine after initial installation, perform a fresh installation of Cisco ISE. This ensures that Cisco ISE properly detects and uses the full disk allocation.

This table shows the retention period for RADIUS logs on your Monitoring node based on disk space and endpoint count. These values are based on these assumptions: Ten or more authentications per day per endpoint with logging suppression enabled.

Table 10: Monitoring node log storage (retention period in days for RADIUS)

Number of endpoints	300 GB	600 GB	1024 GB	2048 GB
5,000	504	1510	2577	5154
10,000	252	755	1289	2577
25,000	101	302	516	1031
50,000	51	151	258	516
100,000	26	76	129	258
150,000	17	51	86	172
200,000	13	38	65	129
250,000	11	31	52	104
500,000	6	16	26	52

This table shows the TACACS+ log retention period on your Monitoring node based on disk space and endpoint count. These values are based on these assumptions: The script runs against all NADs, 4 sessions per day, and 5 commands per session.

Table 11: Monitoring node log storage (retention period in days for TACACS+)

Number of endpoints	300 GB	600 GB	1024 GB	2048 GB
100	12,583	37,749	64,425	128,850
500	2,517	7,550	12,885	25,770
1,000	1,259	3,775	6,443	12,885
5,000	252	755	1,289	2,577
10,000	126	378	645	1,289
25,000	51	151	258	516
50,000	26	76	129	258
75,000	17	51	86	172
100,000	13	38	65	129

Increase disk size

If the context and visibility functions are slow or storage space for logs is not sufficient, you must allocate more disk space.

For every 100 GB of disk space that you add, 60 GB is available for log storage.

To enable Cisco ISE to detect and use the new disk allocation, you must deregister the node, update the VM settings, and reinstall Cisco ISE. You can install Cisco ISE on a new, larger node and add that node to the deployment for high availability. After synchronizing the nodes, configure the new VM as the primary node and deregister the original VM.

Decrease disk size

If you reduce the VM reservations after installing Cisco ISE, you must perform these steps:

1. Perform a backup of Cisco ISE.
2. Re-image Cisco ISE with the updated VM configuration.
3. Restore Cisco ISE.

CPU requirements for hypervisors

From Cisco ISE release 3.4, several Cisco ISE services run inside containers based on RHEL 9.3. RHEL 9.3 requires a minimum CPU architecture of x86-64-v2.

If your hypervisor presents a CPU baseline below x86-64-v2 to the guest VM, the affected containers fail to start. The Cisco ISE GUI and CLI show the processes that require x86-64-v2 (Cisco ISE release 3.4 and later) as not running or initializing :

- ISE pxGrid Direct Service
- ISE pxGrid Direct Pusher
- Hermes (pxGrid Cloud Agent)
- McTrust (Meraki Sync Service)
- ACI Connector
- MFC Profiler

To verify whether your hypervisor exposes the required CPU flags, run this command from the Cisco ISE CLI admin or root shell:

To verify x86-64-v2 support (including SSE4.2 and POPCNT), use this command:

```
show tech-support | include sse4_2
```

If the output is empty, the hypervisor is masking the required CPU features, which prevents affected services from starting.

If the output includes these flags, your VM detects the modern CPU instruction sets exposed by the hypervisor. For example, if `sse4_2` and `popcnt` are present, the guest VM receives the x86-64-v2 instruction set from the hypervisor. This instruction set is required for RHEL 9-based ISE containers.

If these strings are missing, your hypervisor masks the CPU features required by Cisco ISE.

If the physical CPU supports these instruction sets, you can enable or expose them to the VM using these hypervisor-specific settings:

- ESXi: Enable **Expose hardware-assisted virtualization to the guest OS**.
- Hyper-V: Disable **Migrate to a physical computer with a different processor version**. Migration to another physical host remains supported if the CPU vendor and processor generation are the same.
- KVM, Proxmox, or Nutanix: Change the CPU type from default to **host**.



CHAPTER 3

Install Cisco ISE

- [Install Cisco ISE using Cisco Integrated Management Interface, on page 35](#)
- [Run the setup program of Cisco ISE, on page 38](#)
- [Verify the Cisco ISE installation process, on page 40](#)
- [Install Cisco ISE from an ISO on OpenStack, on page 41](#)
- [Install Cisco ISE on a Cisco SNS appliance using NFS, on page 44](#)
- [Localized ISE installation, on page 44](#)

Install Cisco ISE using Cisco Integrated Management Interface

Use these high-level steps to install Cisco ISE.

Before you begin

- Verify that your system meets the [System Requirements](#).
- For virtual machine installations, create the VM according to the specified configuration. Refer to these topics for more information.
- For SNS hardware appliances, set up Cisco Integrated Management Interface (Cisco IMC) to manage the appliance and configure BIOS. Refer to the respective hardware installation guides:
 - SNS-3600 Series: [Cisco SNS-3600 Series Appliance Hardware Installation Guide](#)
 - SNS-3700 Series: [Cisco SNS-3700 Series Appliance Hardware Installation Guide](#)
 - SNS-3800 Series: [Cisco SNS-3800 Series Appliance Hardware Installation Guide](#)

Procedure

Step 1 Installation Overview

- For Cisco SNS Appliances
 - a. Install the hardware appliance.
 - b. Connect to Cisco IMC for server management.

- For Virtual Machines
 - a. Confirm your VM configuration matches the requirements.

Step 2 Download Software: Download the Cisco ISE ISO image.

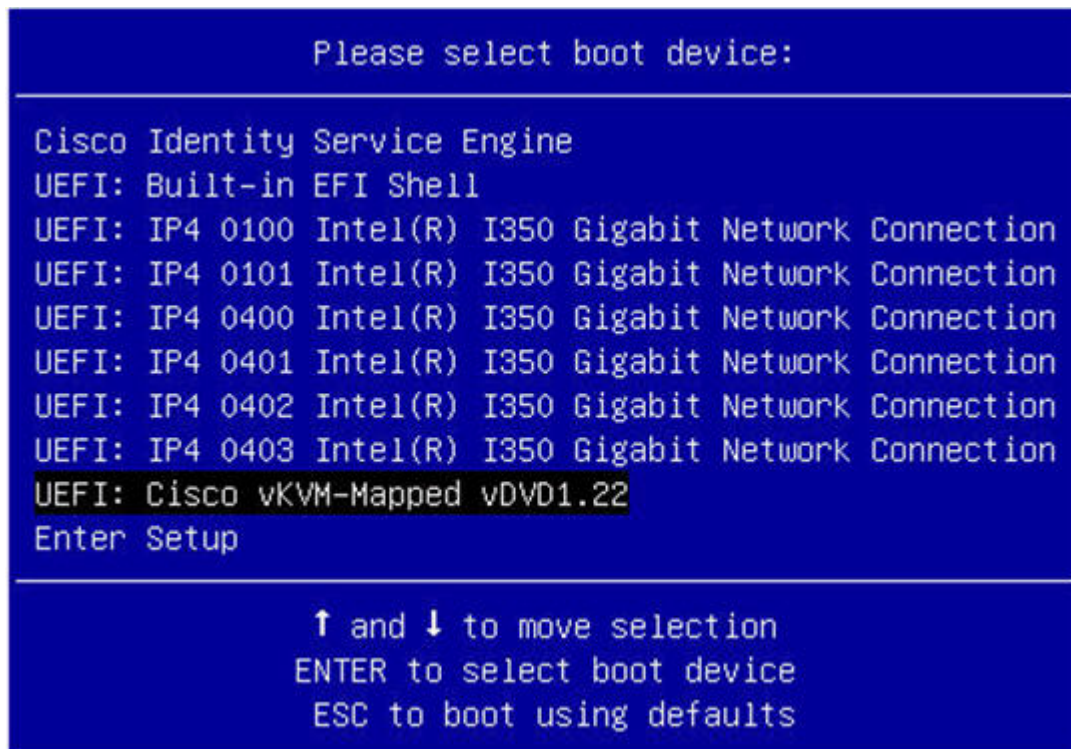
- a) Go to <http://www.cisco.com/go/ise>. You need valid Cisco.com login credentials to access the site.
- b) Click **Download Software for this Product**.

The Cisco ISE image includes a pre-installed 90-day evaluation license, which enables you to test all Cisco ISE services after completing installation and initial configuration.

Step 3 Booting the appliance or VM

- Cisco SNS appliance:
 - a. Connect to Cisco IMC and log in using the Cisco IMC credentials.
 - b. Launch the KVM console.
 - c. Select **Virtual Media > Activate Virtual Devices**.
 - d. Select **Virtual Media > Map CD/DVD**, select the Cisco ISE ISO image, and click **Map Device**.
 - e. Select **Macros > Static Macros > Ctrl-Alt-Del** to boot the appliance with the Cisco ISE ISO image.
 - f. Press **F6** to open the boot menu. A similar screen appears:

Figure 6: Selection of boot device



Note

For remote SNS appliances without physical access, installation through Cisco IMC may take several hours. To speed up installation, copy the ISO file to a USB drive and use it during installation.

Installation time may vary (approximately 30 minutes) depending on network speed, stability, TCP segmentation, and operating system factors.

If the system enters an emergency shell during initial boot due to incomplete hardware initialization, reboot to allow initialization to complete and continue installation.

- Virtual Machine:

- a. Map the CD/DVD to an ISO image. A similar screen appears. The installation menu appears with the message.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 3.x.x.xxx
```

```
Available boot options:
```

```
Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)
```

Step 4 At the boot prompt, press **1** and **Enter** to install Cisco ISE using a serial console.

If you want to use a keyboard and monitor, use the arrow key to select the **Cisco ISE Installation (Keyboard/Monitor)** option. The message appears.

```
*****
Please type 'setup' to configure the appliance
*****
```

Step 5 **Setup program:** At the prompt, type **setup** to start the setup program. See [Run the setup program of Cisco ISE, on page 38](#) for details about the parameters that the setup program uses.

Step 6 After you enter the network configuration parameters in the setup mode, the appliance automatically reboots, and returns to the shell prompt mode.

Step 7 Exit shell prompt mode. The appliance starts.

Step 8 Proceed to [Verify the Cisco ISE installation process, on page 40](#).

Installation metrics for Cisco ISE

The table outlines the installation duration and network latency metrics for various mount types for Cisco ISE.

Table 12: Latency and installation metrics for Cisco ISE

Mount type	Time taken for installation	Approximate latency
NFS-CIMC Mount	7 hours	Average round-trip time is less than 1 millisecond

CD or DVD - KVM Mount	4 hours	-
USB	1 hour	-

Run the setup program of Cisco ISE

This section explains how to configure the Cisco ISE server. The interactive command-line interface (CLI) helps you configure network settings, administrator credentials, and management interfaces. It supports IPv4, IPv6, and dual-stack configurations and covers integration with Active Directory (AD) and essential parameters such as hostname, IP addresses, DNS, NTP servers, and system time zone.

The setup program launches an interactive CLI that prompts you for required parameters. Use the console or a dumb terminal to configure the initial network settings and administrator credentials for the Cisco ISE server. You only need to perform this setup process once. For AD integration, use IP and subnet addresses from a dedicated site created for Cisco ISE. Contact your organization's AD staff to obtain the IP and subnet addresses for your Cisco ISE nodes before installation and configuration.

Follow these steps to run the setup program.

Procedure

Step 1 Power on the appliance designated for the installation.

The setup prompt appears:

```
Type 'setup' to configure the appliance
localhost login:
```

Step 2 At the setup prompt, enter **setup** and press **Enter**.

The console displays a set of parameters. Enter the parameter values for each prompt in the table.

Note

The eth0 interface of Cisco ISE must be statically configured with an IPv6 address if you want to add a Domain Name Server or an NTP Server with an IPv6 address.

Table 13: Cisco ISE setup program parameters

Prompt	Description	Example
Hostname	Up to 19 characters; alphanumeric and hyphen only; first character must be a letter. Note Use lowercase to avoid certificate issues. Do not use "localhost" as hostname for a node.	isebeta1
(eth0) Ethernet interface address	Valid IPv4 or global IPv6 for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14/ 2001:420:54ff:4:458:121:119

Prompt	Description	Example
Netmask	Valid IPv4 or IPv6 netmask.	255.255.255.0/ 2001:420:54ff:4:458:121:119:122
Default gateway	Valid IPv4 or global IPv6 address for the default gateway.	10.12.13.1/ 2001:420:54ff:4:458:1
DNS domain name	Must not be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.). Note The top-level domain name must not exceed 6 characters in length. If the TLD length exceeds six characters, Cisco ISE will become unusable.	example.com
Primary name server	Valid IPv4 or global IPv6 address for the primary name server.	10.15.20.25 / 2001:420:54ff:4:458:118
Add/Edit another name server	Valid IPv4 or global IPv6 address for the primary name server.	(Optional) Allows you to configure multiple name servers. To configure multiple name servers, enter y to continue.
Primary NTP server	Valid IPv4 or global IPv6 address or hostname of a Network Time Protocol (NTP) server. Note Ensure that the primary NTP server is reachable.	clock.nist.gov / 10.15.20.25 / 2001:420:54ff:4:458:117
Add/Edit another NTP server	Must be a valid NTP domain.	(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.
System Time Zone	Must be a valid time zone. For example, for Pacific Standard Time (PST), the System Time Zone is PST8PDT, which is Coordinated Universal Time (UTC) minus 8 hours (UTC-08:00 or 16:00). Note Ensure that the system time and time zone match the CIMC or Hypervisor Host OS time and time zone. If there is any mismatch between the time zones, system performance might be affected. Note Set all Cisco ISE nodes to the UTC time zone. This setting ensures that reports, logs, and posture agent log files from the nodes in your deployment are always synchronized by timestamp.	UTC (default)

Prompt	Description	Example
Username	Identifies the administrative username used for CLI access to the Cisco ISE system. If you choose not to use the default (admin), you must create a new username. The Username must be 3 to 8 characters in length and consist of valid alphanumeric characters (A–Z, a–z, or 0–9).	admin (default)
Password	Identifies the administrative password that is used for CLI access to the Cisco ISE system. You must create this password in order to continue because there is no default password. The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).	MyIseYPass2

Note

- If you create a password that includes the `§` character anywhere except as the last character, the system accepts the password, but you cannot log in to the CLI with it.
- To reset such a password, log into the console and use CLI commands or reset using an ISE CD or ISO file. Refer to the [Cisco ISE password reset documentation](#) for instructions.

After the setup

- The system reboots automatically after completing the setup.
- Log in to Cisco ISE using the configured username and password.

Verify the Cisco ISE installation process

Use this procedure to confirm successful installation.

Procedure

- Step 1** When the system reboots and the login prompt appears, enter the username you configured during setup. Then press **Enter**.
- Step 2** Enter a new password.
- Step 3** To verify that the application has been installed properly, enter the **show application** command. Then press **Enter**. The console displays:

```
ise/admin# show application
<name>           <Description>
ise              Cisco Identity Services Engine
```

Note

The version and date might change for different versions of this release.

Step 4 To check the status of the ISE processes, enter the **show application status ise** command, and press **Enter**. The console displays:

```
ise/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	14890
Database Server	running	70 PROCESSES
Application Server	running	19158
Profiler Database	running	16293
ISE Indexing Engine	running	20773
AD Connector	running	22466
M&T Session Database	running	16195
M&T Log Collector	running	19294
M&T Log Processor	running	19207
Certificate Authority Service	running	22237
EST Service	running	29847
SXP Engine Service	disabled	
Docker Daemon	running	21197
TC-NAC Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID WMI Service	disabled	
PassiveID Syslog Service	disabled	
PassiveID API Service	disabled	
PassiveID Agent Service	disabled	
PassiveID Endpoint Service	disabled	
PassiveID SPAN Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	

```
ise/admin#
```

Install Cisco ISE from an ISO on OpenStack

You can install Cisco ISE release 3.4 patch 4 and later releases in an OpenStack environment using these methods:

- OpenStack Dashboard (for example, Horizon): A web-based interface that allows administrators to manage OpenStack resources and services, including the deployment of Cisco ISE instances.
- OpenStack Orchestration Tools (for example, HEAT): Templates that define the network, compute, and storage topology for automated deployment and management of Cisco ISE virtual machines.
- OpenStack Command Line Interfaces (CLI): Command-line tools that provide granular control over deploying and managing Cisco ISE instances within OpenStack.

This section provides a sample CLI-based Cisco ISE installation procedure in an OpenStack environment.

Follow these steps to install Cisco ISE using OpenStack CLI.

Procedure

Step 1 Create a custom flavor in OpenStack that matches the Cisco ISE appliance size requirements.

Here is a sample command for Cisco SNS 3715 to create a flavor named "sns3715-openstack" with 32 GB RAM, 300 GB disk, and 24 virtual CPUs, with an automatically assigned ID.

```
openstack flavor create sns3715-openstack --id auto --ram 32768 --disk 300 --vcpus 24
```

For information about the Cisco SNS appliance size requirements, refer to [Cisco SNS Appliance Hardware Installation Guide](#).

This process takes about 5 to 10 minutes.

You need this flavor name when creating the bootable VM instance.

Step 2 Create the Glance image for Cisco ISE installation.

- Follow these steps to create the Glance image using the ISO file:

- a. Create a blank Cinder volume for the VM's main hard drive using this command:

```
openstack volume create --size <volume_size_in_GB> <volume_name>
```

Ensure that the volume size meets Cisco ISE specifications.

- b. Create a temporary VM to copy the Cisco ISE filesystem onto the blank volume using this command:

```
openstack server create --image <iso-image-name-or-id> --volume <volume_name> --flavor <custom-flavor-name> --network <network-name> <temp-ise-install-vm-name>
```

Attach both the blank Cinder volume and the installation ISO to the VM.

This process takes about 5 minutes.

- c. Install the operating system through the VM console.

1. Access the VM console using this command:

```
openstack console url show <temp-ise-install-vm-name>
```

2. When the boot menu appears, select **[1] Cisco ISE Installation (Keyboard/Monitor)** to begin the installation.

The installer writes the operating system to the blank volume. Wait 20 to 30 minutes for installation to complete.

After installation completes, the console returns to the boot prompt. The volume now contains a bootable operating system.

- d. Set the volume as bootable.

1. Delete the temporary VM to release the volume using this command:

```
openstack server delete <temp-ise-install-vm-name>
```

2. Verify that the volume status is "available" using this command:

```
watch openstack volume show <volume_name>
```

3. Mark the volume as bootable using this command:

```
openstack volume set --bootable <volume_name>
```

- Follow these steps to create a QCOW2 image, install Cisco ISE using the ISO, and upload the image to OpenStack.

- a. Create the QCOW2 image using this command:

```
qemu-img create -f qcow2 <image_name>.qcow2 <size>
```

- b. Install the Cisco ISE ISO on the QCOW2 image. Run this command to boot the ISO and begin the installation on the disk image.

```
/usr/libexec/qemu-kvm -enable-kvm -m <memory_size> -smp <cpu_cores> -cpu host \ -drive  
file=<image_name>.qcow2,format=qcow2 \ -cdrom <iso_file_path> \ -boot d -net nic,model=virtio  
-net user \ -nographic -serial mon:stdio
```

- c. Perform the installation via the serial console. When the installation menu appears, select **2** to proceed with the installation using the serial console. Follow the on-screen prompts to complete the setup.

- d. Upload the QCOW2 image to OpenStack. After the installation is complete and the image is prepared, use the OpenStack CLI to create a new image in your environment.

```
openstack image create --disk-format qcow2 --container-format bare --file <image_file_name>  
--private <image_name>
```

Note

You must use this ISO file for OpenStack support:

```
ise-3.4.0.608b.SPA.x86_64.iso
```

- Step 3** Create and launch the Cisco ISE server VM with the prepared bootable volume by using this command:

```
openstack server create --volume <volume_name> --flavor <custom-flavor-name> --network <network-name>  
<vm-name>
```

This process takes approximately 5 minutes.

- Step 4** Configure the network settings for the VM.

- a. Access the VM console and enter this command at the setup prompt:

```
setup
```

- b. Follow the prompts to configure the hostname, IP address, and network details.

After you complete the configuration, access the VM using the assigned IP address.

Run these commands to verify the Cisco ISE VM configuration.

- To check inventory, use this command:

```
show inventory
```

- To check the profiles, use this command:

```
show tech | inc profile
```

Install Cisco ISE on a Cisco SNS appliance using NFS

This section explains how to install Cisco ISE on a Cisco SNS appliance by using a Network File System (NFS) server.

Before you begin

- Ensure that you meet the requirements specified in the guide.
- Set up the Cisco Integrated Management Interface (CIMC) configuration utility to manage the appliance and configure the BIOS. For more information, see these documents:
 - For SNS-3600 series appliances, refer to [Cisco SNS-3600 Series Appliance Hardware Installation Guide](#) for details.
 - For SNS-3700 series appliances, refer to [Cisco SNS-3700 Series Appliance Hardware Installation Guide](#) for details.
 - For SNS-3800 series appliances, refer to [Cisco SNS-3800 Series Appliance Hardware Installation Guide](#) for details.

Procedure

- Step 1** Download the Cisco ISE ISO image from <http://www.cisco.com/go/ise>.
- Step 2** Connect to CIMC and log in using the CIMC credentials.
- Step 3** Choose **Compute > Remote Management > Virtual Media > Add New Mapping**, enter the NFS server details in the **Add New Mapping** window, and then click **Save**.
- Step 4** Verify that the mapping status shows **OK** in the **Current Mappings** window.
- Step 5** Launch the KVM console.
- Step 6** Choose **Power > Power Cycle System** and click **Confirm** to reboot the appliance.
- Step 7** Press **F6** to enter the boot menu.
- Step 8** In the **Select Boot Device** window, choose **UEFI: Cisco CIMC-Mapped vDVD2.00**, and press **Enter**.
The Cisco ISE installation menu appears after the server completes the booting process.
- Step 9** Choose **Cisco ISE Installation (Keyboard/Monitor)** to continue with the installation.
-

Localized ISE installation

While reinstalling Cisco ISE, you can use the **Localized ISE Install** option in the **application configure ise** command to reduce the installation time. This option reduces the reinstallation time from an average of 5 to 7 hours to approximately 1 to 2 hours. This option can be used for both Secure Network Servers (SNS) and virtual appliances. However, it significantly reduces the reinstallation time only for SNS.

**Note**

- **Localized ISE Install** option is supported for Cisco ISE release 3.1 patch 9 and later, Cisco ISE release 3.2 patch 5 and later, Cisco ISE release 3.3 patch 2 and later, and Cisco ISE release 3.4 and later releases.
- You can use this option to reinstall the current version and higher versions. You cannot install a version that is older than the current version.

For more information, see "Localized ISE Installation" in the Chapter "Cisco ISE CLI Commands in EXEC Mode" in the [Cisco Identity Services Engine CLI Reference Guide](#).



CHAPTER 4

Additional Installation Information

- [Tools used to create a bootable USB device from Installation ISO File, on page 47](#)
- [SNS Appliance Reference, on page 48](#)
- [VMware Virtual Machine, on page 50](#)
- [Linux KVM, on page 64](#)
- [Microsoft Hyper-V, on page 67](#)
- [Create a Cisco ISE virtual machine on Hyper-V, on page 67](#)
- [Zero Touch Provisioning, on page 82](#)

Tools used to create a bootable USB device from Installation ISO File

The following table shows the tools to be used to create a bootable USB device from the installation ISO file in different Cisco ISE versions.

Table 14: Tools Used to Create Bootable USB Device

Cisco ISE release	Tool
Cisco ISE 3.4	<ul style="list-style-type: none">• Rufus for ise-3.4.0.608.SPA.x86_64.iso file• Rufus, Fedora Media Writer, and balenaEtcher for ise-3.4.0.608a.SPA.x86_64.iso
Cisco ISE 3.3	Rufus
Cisco ISE 3.2	Rufus
Cisco ISE 3.1	Fedora LiveUSB-creator for SNS 3500 and SNS 3600 series appliances. Rufus for SNS 3700 series appliances



Note Cisco ISE 3.1 patch 6 and later and Cisco ISE 3.2 patch 2 and later versions support Cisco SNS 3700 series appliances.

You can download Rufus from this location:

<https://rufus.ie/downloads/>

You can download Fedora Media Writer from this location:

<https://github.com/FedoraQt/MediaWriter/releases/tag/5.0.6>

You can download balenaEtcher from this location:

<https://github.com/balena-io/etcher/releases/tag/v1.19.21>

SNS Appliance Reference

Create a Bootable USB Device Using Rufus

Before you begin

- Download the Cisco ISE installation ISO file to the local system.
- Use a 16 GB or 32 GB USB device.

Procedure

Step 1 Reformat the USB device using FAT16 or FAT32 to free up all the space.

Step 2 Plug in the USB device to the local system and launch **Rufus**.

Step 3 From the **Boot Selection** drop-down list, choose **Disk or ISO Image**.

Step 4 Click **Select** and choose the Cisco ISE ISO file.

Note

You must use the latest ISO file (ise-3.4.0.608b.SPA.x86_64.iso) for Cisco SNS 3800 appliance support.

Step 5 From the **Partition Scheme** drop-down list, choose **MBR**.

Step 6 From the **Target System** drop-down list, choose **BIOS or UEFI**.

Step 7 Click **Start**.

You can view the status of the bootable USB creation in the progress bar. After the process completes, you can access the contents of the USB drive on your local system.

Step 8 Remove the USB device from the local system safely.

Step 9 Plug in the bootable USB device to the Cisco ISE appliance, restart the appliance, and install Cisco ISE by booting from the USB drive.

Create a Bootable USB Device Using Fedora Media Writer

Before you begin

- Download the Cisco ISE installation ISO file to the local system.
You must use the ISO file for Cisco ISE Release 3.4:
`ise-3.4.0.608a.SPA.x86_64.iso`
- Download Fedora Media Writer from this location:
<https://github.com/FedoraQt/MediaWriter/releases/tag/5.0.6>
- Use a 16-GB or 32-GB USB device.
- Reformat the USB device using FAT16 or FAT32 to free up all the space.

Procedure

- Step 1** Open the Fedora Media Writer application.
- Step 2** In the **Select Image Source** tab, click **Select .iso file**, choose the ISO file, and click **Next**.
- Step 3** Plug in the USB device to the local system and launch **Fedora Media Writer**.
- Step 4** Choose the ISO file and click **Write**.
- Wait for the process to complete. This process may take several minutes, depending on the speed of your USB device. When the process finishes, the application displays a notification message.
- Step 5** Safely remove the USB device from the local system.
- Step 6** Plug the bootable USB device into the Cisco ISE appliance. Restart the appliance. Boot from the USB drive to install Cisco ISE.
-

Create a Bootable USB Device Using balenaEtcher

Before you begin

- Download the Cisco Identity Services Engine (ISE) installation ISO file to your local system.
You must use this ISO file for Cisco ISE Release 3.4:
`ise-3.4.0.608a.SPA.x86_64.iso`
- Download balenaEtcher from this location:
<https://github.com/balena-io/etcher/releases/tag/v1.19.21>
- Use a 16 GB or 32 GB USB device.
- Reformat your USB device using the FAT-16 or FAT-32 file system to ensure all space is available.

Procedure

- Step 1** Run the balenaEtcher application.
- Step 2** Click **Flash from file**. Choose the ISO file from your local system.
If a Missing Partition Table message appears, click **Continue**.
- Step 3** Click **Select Target**. Choose the USB device.
- Step 4** Click **Flash** to start the process.
You will see a notification message when the process is complete.
- Step 5** Plug in the bootable USB device into the Cisco ISE appliance. Restart the appliance. Boot from the USB drive to install Cisco ISE.
-

Reimage the Cisco SNS Hardware Appliance

The Cisco SNS hardware appliances do not have built-in DVD drives. Therefore, to reimage a Cisco ISE hardware appliance with Cisco ISE software, you can do one of these options:



Note Cisco SNS hardware appliances support the Unified Extensible Firmware Interface (UEFI) secure boot feature. This feature ensures that only a Cisco-signed ISE image can be installed on the SNS hardware appliances, and prevents installation of any unsigned operating system even with physical access to the device. For example, generic operating systems, such as Red Hat Enterprise Linux or Microsoft Windows cannot boot on this appliance.

- Use the Cisco Integrated Management Controller (Cisco IMC) interface to map the installation .iso file to the virtual DVD device.
- Create an install DVD with the installation .iso file. Plug in a USB external DVD drive, then boot the appliance from the DVD drive.
- Create a bootable USB device using the installation .iso file. Boot the appliance from the USB drive.

VMware Virtual Machine



Note The VMware form factor instructions provided in this document are also applicable for Cisco Identity Services Engine (ISE) installed on Hyperflex.

Virtual Machine Resource and Performance Checks

Before installing Cisco ISE on a virtual machine, the installer performs hardware integrity checks by comparing the available hardware resources on the virtual machine with the recommended specifications.

During a virtual machine (VM) resource check, the installer verifies the hard disk space, number of CPU cores, CPU clock speed, and RAM allocated to the VM. If the VM resources do not meet the basic evaluation specifications, installation terminates. This check applies only to ISO-based installations.

When you run the Setup program, the installer performs a VM performance check for disk I/O. If disk I/O performance does not meet the recommended specifications, the installer displays a warning, but you can continue with installation.

The VM performance check is done periodically (every hour), and the results are averaged over one day. If the disk I/O performance does not meet the recommended specification, an alarm is generated.

The VM performance check can also be done on demand from the Cisco ISE CLI using the **show tech-support** command.

You can run VM resource and performance checks outside Cisco ISE installation. Use the Cisco ISE boot menu to perform these tests.

Install Cisco ISE on VMware Virtual Machine Using the ISO File

This section describes how to install Cisco ISE on a VMware virtual machine using the ISO file.

Prerequisites for Configuring a VMware ESXi Server

Review the following configuration prerequisites listed in this section before you attempt to configure a VMWare ESXi server:

- Remember to log in to the ESXi server as a user with administrative privileges (root user).
- Cisco ISE is a 64-bit system. Before you install a 64-bit system, ensure that Virtualization Technology (VT) is enabled on the ESXi server.
- Ensure that you allocate the recommended amount of disk space on the VMware virtual machine.
- If you have not created a VMware virtual machine file system (VMFS), you must create one to support the Cisco ISE virtual appliance. The VMFS is set for each of the storage volumes configured on the VMware host. For VMFS5, the 1-MB block size supports up to 1.999 TB virtual disk size.

Virtualization Technology Check

If you already have an ESXi server installed, you can check whether Virtualization Technology (VT) is enabled without rebooting the machine. Use the **esxcfg-info** command to perform this check.

```
~ # esxcfg-info |grep "HV Support"
|----HV Support.....3
|----World Command Line.....grep HV Support
```

If HV Support has a value of 3, VT is enabled on the ESXi server. You can proceed with the installation.

If HV Support has a value of 2, VT is supported, but not enabled on the ESXi server. Edit the BIOS settings and enable VT on the server.

Enable Virtualization Technology on an ESXi Server

You can reuse the same hardware that hosted a previous version of the Cisco ISE virtual machine. However, you must enable Virtualization Technology (VT) on the ESXi server before installing the latest release.

Procedure

- Step 1** Reboot the appliance.
 - Step 2** Press **F2** to enter setup.
 - Step 3** Choose **Advanced** > **Processor Configuration**.
 - Step 4** Select **Intel(R) VT** and enable it.
 - Step 5** Press **F10** to save your changes and exit.
-

Configure VMware Server Interfaces for the Cisco ISE Profiler Service

Configure VMware server interfaces to support the collection of Switch Port Analyzer (SPAN) or mirrored traffic to a dedicated probe interface for the Cisco ISE Profiler Service.

Procedure

- Step 1** Choose **Configuration** > **Networking** > **Properties** > **VMNetwork** (the name of your VMware server instance) **VMswitch0** (one of your VMware ESXi server interfaces) **Properties** **Security**.
 - Step 2** In the Policy Exceptions pane on the **Security** tab, check the **Promiscuous Mode** check box.
 - Step 3** In the Promiscuous Mode drop-down list, choose **Accept** and click **OK**.
- Perform these steps on any other VMware ESXi server interface that collects SPAN or mirrored profiler traffic.
-

Connect to the VMware Server Using the Serial Console

Procedure

- Step 1** Power off the specific VMware server (for example, ISE-120).
- Step 2** Right-click the VMware server, and choose **Edit**.
- Step 3** Click **Add** on the Hardware tab.
- Step 4** Choose **Serial Port** and click **Next**.
- Step 5** In the Serial Port Output area, select the **Use physical serial port on the host** radio button or the **Connect via Network** radio button and then click **Next**.
 - If you choose the Connect via Network option, you must open the firewall ports over the ESXi server.
 - If you select the Use physical serial port on the host, choose the port. You must choose the port. There are two options available:

- **/dev/ttyS0** (In the DOS or Windows operating system, this appears as COM1).
- **/dev/ttyS1** (In the DOS or Windows operating system, this appears as COM2).

- Step 6** Click **Next**.
- Step 7** Check the appropriate check box in the Device Status area. By default, Connected is selected.
- Step 8** Click **OK** to connect to the VMware server.
-

Configure a VMware Server

Before you begin

Ensure that you have read the [Prerequisites for configuring a VMware Server](#).

Procedure

- Step 1** Log in to the ESXi server.
- Step 2** In the VMware vSphere Client, in the left pane, right-click your host container and choose **New Virtual Machine**.
- Step 3** In the **Select a Creation Type** area, click **Create a new virtual machine** and click **Next**.
- Step 4** In the **Select a Name and Folder** area, enter a name for the VMware system, select a location from the displayed list, and click **Next**.
- Tip**
Use the hostname that you want to use for your VMware host.
- Step 5** In the **Select a compute resource** area, choose a destination compute resource and click **Next**.
- Step 6** In the **Select storage** area, choose a datastore that has the recommended amount of space available and click **Next**.
- Step 7** In the **Select compatibility** area, from the **Compatible with** drop-down list, choose an ESXi version that is compatible with your Cisco ISE version and click **Next**.
- For information about the ESXi versions compatible with your Cisco ISE release, see "Supported Virtual Environments" in the [Release Notes for Cisco Identity Services Engine](#) for your release.
- Step 8** In the **Select a guest OS** area, complete these steps and then click **Next**:
- From the **Guest OS Family** drop-down list, choose **Linux**.
 - From the **Guest OS Version** drop-down list, choose the supported Red Hat Enterprise Linux (RHEL) version. Cisco ISE Release 3.1 and later use RHEL 8.
- Step 9** In the **Customize hardware** area, in the **Virtual Hardware** tab, carry out the following configurations and then click **Next**.
- Choose the required values from the **CPU** and **Memory** drop-down lists based on the SNS series appliance you use:
SNS 3600 Series Appliance:
 - Small: 16 vCPU cores, 32 GB

- Medium: 24 vCPU cores, 96 GB
- Large: 24 vCPU cores, 256 GB

The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3600 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 16 vCPU cores to meet the CPU specification of SNS 3615, which has 8 CPU Cores or 16 Threads.

SNS 3700 Series Appliance:

- Small: 24 vCPU cores, 32 GB
- Medium: 40 vCPU cores, 96 GB
- Large: 40 vCPU cores, 256 GB

The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3700 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 24 vCPU cores to meet the CPU specification of SNS 3715, which has 12 CPU Cores or 24 Threads.

SNS 3800 Series Appliance:

- Small: 32 vCPU cores, 64 GB
- Medium: 48 vCPU cores, 128 GB
- Large: 48 vCPU cores, 256 GB

The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3800 series, due to hyperthreading. For example, in case of Small network deployment, you must allocate 32 vCPU cores to meet the CPU specification of SNS 3815, which has 16 CPU Cores or 32 Threads.

Note

Reserve vCPU and memory resources equal to the configured vCPU cores and memory allocations. If you do not do this, Cisco ISE performance and stability can be significantly impacted. Click the **CPU** and **Memory** collapsible areas and update the reservation fields for each setting.

- From the **New SCSI Controller** drop-down list, choose **Paravirtual**.
- From the **New Network** and **New CD/DVD Drive** drop-down lists, choose the required network and ISO files.

Step 10 Choose the NIC driver from the **Adapter** drop-down list and click **Next**.

Step 11 Choose **Create a new virtual disk** and click **Next**.

Step 12 In the Disk Provisioning dialog box, click **Thick provisioned, eagerly zeroed** radio button, and click **Next** to continue.

Cisco ISE supports both thick and thin provisioning. However, we recommend that you choose thick provisioned, eagerly zeroed for better performance, especially for Monitoring nodes. If you choose thin provisioning, operations such as upgrade, backup and restore, and debug logging that require more disk space might be impacted during initial disk expansion.

Step 13 Clear the check box for **Support clustering features such as Fault Tolerance** check box.

Step 14 In the **Ready to complete** area, verify the configuration details, such as name, guest OS, CPUs, memory, and disk size of the newly created VMware system.

Step 15 Click **Finish**.

The VMware system is now installed.

What to do next

To activate the newly created VMware system, right-click VM in the left pane of your VMware client user interface and choose **Power > Power On**.

Increase Virtual Machine Power-On Boot Delay Configuration

On a VMware virtual machine, the boot delay is set to 0 by default. You can change the boot delay to make it easier to choose boot options, such as when resetting the Administrator password.

Procedure

- Step 1** From the VSphere client, right click the virtual machine and choose **Edit Settings**.
 - Step 2** Click the **Options** tab.
 - Step 3** Choose **Advanced > Boot Options**.
 - Step 4** From the **Power on Boot Delay** area, select the time in milliseconds to delay the boot operation.
 - Step 5** Select the check box in the **Force BIOS Setup** area to enter into the BIOS setup screen when the VM boots the next time.
 - Step 6** Click **OK** to save your changes.
-

Install Cisco ISE Software on a VMware System

Before you begin

- After installation, if you do not install a permanent license, Cisco ISE automatically installs a 90-day evaluation license that supports a maximum of 100 endpoints.
- Download the Cisco ISE software from the Cisco Software Download Site at <http://www.cisco.com/en/US/products/ps11640/index.html> . Then, burn the software on a DVD. You must provide your Cisco.com site credentials.
- (Optional; applicable only if you are installing Cisco ISE on VMware Cloud) The process of installing Cisco ISE on VMware Cloud is identical to the process for installing Cisco ISE on a VMware virtual machine.
 - Cisco ISE virtual machine deployed on VMware cloud in Amazon Web Services (AWS): Cisco ISE can be hosted on software-defined data center (SDDC) provided by VMware Cloud on AWS. Ensure that appropriate security group policies are configured on VMware Cloud (under **Networking and Security > Security > Gateway Firewall Settings**) to enable access to the on-premises deployment, required devices, and services.
 - Cisco ISE virtual machine deployed on Azure VMware Solution (AVS): AVS runs VMware workloads natively on Microsoft Azure, where Cisco ISE can be hosted as a VMware virtual machine.

Procedure

- Step 1** Log in to the VMware client.
- Step 2** For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.
- Step 3** Click the **Options** tab.
- Step 4** Click **Boot Options**, and in the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note

You must change the firmware from **BIOS** to **EFI** in the boot mode of VM settings to boot GPT partitions with 2 TB or more capacity.

If you have selected **Guest OS RHEL 8** and **EFI** boot mode, disable the **Enable UEFI Secure Boot** option. This option is enabled by default for Guest operating system RHEL 8 VM.

- Step 5** Click **OK**.
- Step 6** Set the Coordinated Universal Time (UTC) and the correct boot order in BIOS.
- If the VM is turned on, turn the system off.
 - Turn on the VM.
The system enters BIOS setup mode.
 - In the Main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.
 - Enter the UTC/Greenwich Mean Time (GMT) time zone.
This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.
 - Using the arrow keys, navigate to the Boot menu and press **Enter**.
 - Using the arrow keys, select CD-ROM drive and press + to move the CD-ROM drive up the order.
 - Using the arrow keys, navigate to the Exit menu and choose **Exit Saving Changes**.
 - Choose **Yes** to save the changes and exit.

- Step 7** Insert the Cisco ISE software DVD into the VMware ESXi host CD/DVD drive and turn on the virtual machine.
When the DVD boots, the console shows:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

- Step 8** Use the arrow keys to select **Cisco ISE Installation (Serial Console)** or **Cisco ISE Installation (Keyboard/Monitor)** and press **Enter**. If you choose the serial console option, you should have a serial console set up on your virtual machine. See the [VMware vSphere Documentation](#) for information on how to create a console.

The installer starts the installation of the Cisco ISE software on the VMware system. Allow 20 minutes for the installation process to complete. When the installation process finishes, the virtual machine reboots automatically. When the VM reboots, the console displays:

```
Type 'setup' to configure your appliance
localhost:
```

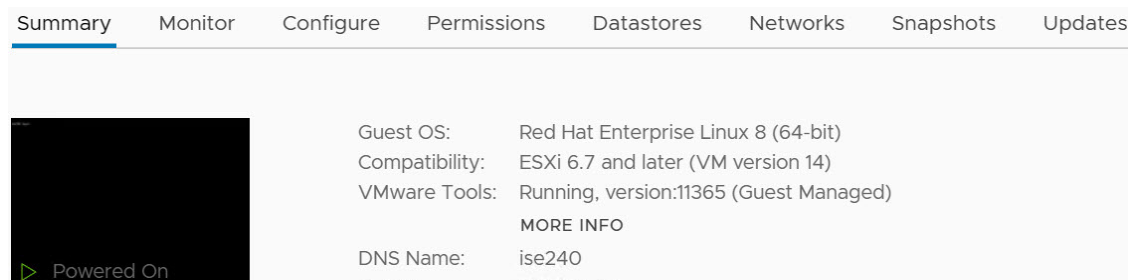
- Step 9** At the system prompt, type **setup** and press **Enter**.
The Setup Wizard appears and guides you through the initial configuration.

VMware Tools Installation Verification

Verify VMWare Tools Installation Using the Summary Tab in the vSphere Client

Go to the Summary tab of the specified VMware host in the vSphere Client. Verify that the value in the VMware Tools field displays "OK".

Figure 7: Verifying VMware Tools in the vSphere Client



Verify VMware Tools Installation Using the CLI

To check if VMware Tools are installed, run the **show inventory** command. The output displays NIC driver information. If VMware Tools are installed, you see "VMware Virtual Ethernet driver" in the Driver Description field.

```
NAME: "ISE-VM-K9 chassis", DESCR: "ISE-VM-K9 chassis"
PID: ISE-VM-K9      , VID: A0  , SN: FCH184X9XXX
Total RAM Memory: 65700380 kB
CPU Core Count: 16
CPU 0: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 1: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 2: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 3: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 4: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 5: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 6: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 7: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 8: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 9: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 10: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 11: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 12: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 13: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 14: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
CPU 15: Model Info: Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz
Hard Disk Count(*): 1
Disk 0: Device Name: /xxx/abc
Disk 0: Capacity: 1198.00 GB
```

```

NIC Count: 6
NIC 0: Device Name: eth0:
NIC 0: HW Address: xx:xx:xx:xx:xx:xx
NIC 0: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 1: Device Name: eth1:
NIC 1: HW Address: xx:xx:xx:xx:xx:xx
NIC 1: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: HW Address: xx:xx:xx:xx:xx:xx
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: HW Address: xx:xx:xx:xx:xx:xx
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: HW Address: xx:xx:xx:xx:xx:xx
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
NIC 5: HW Address: xx:xx:xx:xx:xx:xx
NIC 5: Driver Descr: Intel(R) Gigabit Ethernet Network Driver

(*) Hard Disk Count may be Logical.

```

Support for Upgrading VMware Tools

The ISE ISO image contains the supported VMware tools. You cannot upgrade VMware tools using the VMware client user interface. To use a newer version of VMware tools, upgrade ISE to a newer version.

Clone a Cisco ISE Virtual Machine

You can clone a Cisco ISE VMware virtual machine (VM) to create an exact replica of a Cisco ISE node. For example, in a distributed deployment with multiple Policy Service nodes (PSNs), VM cloning helps you deploy the PSNs quickly and effectively. You do not have to install and configure the PSNs individually.

You can also clone a Cisco ISE VM using a template.



Note For cloning, you need VMware vCenter. Cloning must be done before you run the Setup program. When you power on the cloned VM for the first time, if VMware prompts you to choose between **I Copied It** and **I Moved It**, you must choose **I Copied It**. This ensures the VM is assigned a new MAC address and UUID, resulting in a unique UDI. Choosing **I Moved It** causes duplicate UDI and registration or licensing issues in Cisco ISE deployments.

Before you begin

- Shut down the Cisco ISE VM that you plan to clone. In the vSphere client, right-click the Cisco ISE VM and choose **Power > Shut Down Guest**.
- Do not change the IP address or hostname before powering on the cloned VM. Complete the cloning process. Power on the VM and choose **I Copied It** when prompted. Configure the IP address and hostname during the initial setup.

Procedure

- Step 1** Log in to the ESXi server as a user with administrative privileges (root user).
VMware vCenter is required to perform this step.
- Step 2** Right-click the Cisco ISE VM you want to clone, and click **Clone**.
- Step 3** In the Name and Location dialog box, enter a name for the new machine and click **Next**.
This is not the hostname of the new Cisco ISE VM that you are creating, but a descriptive name for your reference.
- Step 4** Select a host or cluster to run the new Cisco ISE VM, and click **Next**.
- Step 5** Select a datastore for the new Cisco ISE VM and click **Next**.
The datastore may be the local option on the ESXi server, or remote storage. Ensure the datastore has sufficient disk space.
- Step 6** In the Disk Format dialog box, select the **Same format as source** radio button, and click **Next**.
This option copies the format used in the Cisco ISE VM that you are cloning.
- Step 7** In the Guest Customization dialog box, select the **Do not customize** radio button, then click **Next**.
- Step 8** Click **Finish**.
-

What to do next

- [Changing the IP Address and Hostname of a Cloned Virtual Machine](#)
- [Connecting a Cloned Cisco Virtual Machine to the Network](#)

Clone a Cisco ISE Virtual Machine Using a Template

If you use vCenter, you can use a VMware template to clone a Cisco ISE virtual machine (VM). You can create a template by cloning a Cisco ISE node, then use the template to create multiple Cisco ISE nodes. Cloning a virtual machine using a template involves two steps.

Before you begin



Note For cloning, you need VMware vCenter. Cloning must be done before you run the Setup program.

Procedure

- Step 1** [Create a Virtual Machine Template, on page 60](#)
- Step 2** [Deploy a Virtual Machine Template, on page 60](#)
-

Create a Virtual Machine Template

Before you begin

- Ensure that you shut down the Cisco ISE VM that you are going to clone. In the vSphere client, right-click the Cisco ISE VM that you are about to clone and choose **Power > Shut Down Guest**.
- We recommend that you create a template from a Cisco ISE VM that you have just installed and not run the setup program on. You can then run the setup program on each of the individual Cisco ISE nodes that you have created and configure IP address and hostnames individually.

Procedure

- Step 1** Log in to the ESXi server as a user with administrative privileges (root user).
VMware vCenter is required to perform this step.
- Step 2** Right-click the Cisco ISE VM that you want to clone and choose **Clone > Clone to Template**.
- Step 3** Enter a name for the template, choose a location to save the template in the Name and Location dialog box, and click **Next**.
- Step 4** Choose the ESXi host that you want to store the template on and click **Next**.
- Step 5** Choose the datastore that you want to use to store the template and click **Next**.
Ensure that this datastore has the required amount of disk space.
- Step 6** Click the **Same format as source** radio button in the Disk Format dialog box and click **Next**.
The Ready to Complete dialog box appears.
- Step 7** Click **Finish**.
-

Deploy a Virtual Machine Template

After you create a virtual machine template, deploy it on other virtual machines (VMs)

Procedure

- Step 1** Right-click the ISE VM template that you have created and choose **Deploy Virtual Machine from this template**.
- Step 2** Enter a name for the new Cisco ISE node. Choose a location for the node in the Name and Location dialog box, and click **Next**.
- Step 3** Choose either the ESXi host where you want to store the new Cisco ISE node and click **Next**.
- Step 4** Choose the datastore that you want to use for the new Cisco ISE node and click **Next**.
Verify that the datastore has enough disk space.
- Step 5** Click the **Same format as source** radio button in the Disk Format dialog box and click **Next**.
- Step 6** Click the **Do not customize** radio button in the Guest Customization dialog box.

The Ready to Complete dialog box is displayed.

Step 7 Check the **Edit Virtual Hardware** check box and click **Continue**.

The Virtual Machine Properties page is displayed.

Step 8 Choose **Network adapter**, uncheck the **Connected** and **Connect at power on** check boxes, and click **OK**.

Step 9 Click **Finish**.

Power on the Cisco ISE node, configure its IP address and hostname, and connect it to the network.

What to do next

- [Changing the IP Address and Hostname of a Cloned Virtual Machine](#)
- [Connecting a Cloned Cisco Virtual Machine to the Network](#)

Change the IP address and hostname of a cloned virtual machine

After cloning a Cisco ISE virtual machine (VM), power it on and change its IP address and hostname.

Before you begin

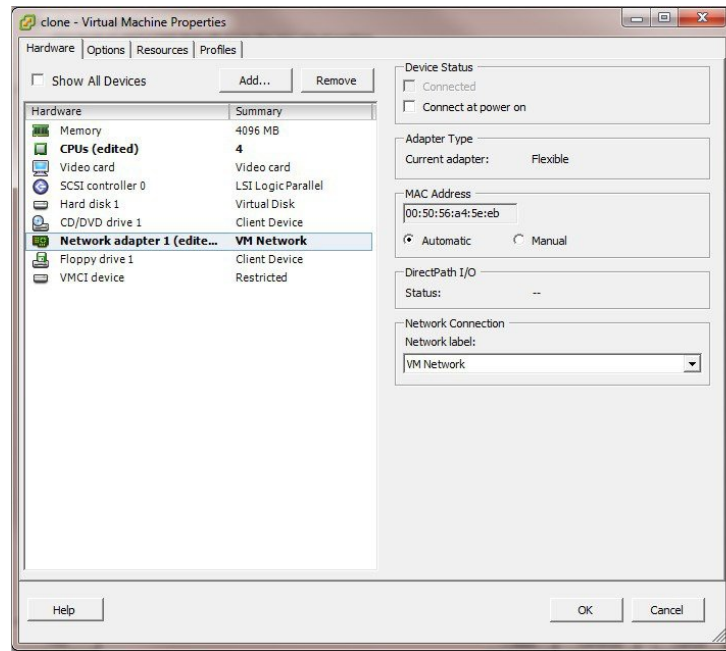
- Make sure your Cisco ISE node is in the standalone state.
- Before you power on the newly cloned Cisco ISE VM, make sure its network adapter is not connected. Uncheck the **Connected** and **Connect at power on** check boxes. This prevents the node from using the same IP address as the original source machine.



Caution

Cloning a Cisco ISE virtual machine will result in the hypervisor assigning a new MAC address to the primary network interface (eth0). Because Cisco ISE licenses are tied to the Unique Device Identifier (UDI) generated from this MAC address, cloning an already-registered node will invalidate its licenses. You must re-host your licenses in the Cisco Smart Software Manager for the new UDI.

Figure 8: Disconnecting the Network Adapter



- Before powering on the newly cloned VM, prepare the IP address and hostname you want to assign. Add this IP address and hostname in the DNS server. Do not use “localhost” as a hostname.
- Obtain certificates for the Cisco ISE nodes using the new IP address or hostname.

Procedure

Step 1 Right-click the newly cloned Cisco ISE VM and choose **Power > Power On**.

Step 2 Select the newly cloned Cisco ISE VM and click the **Console** tab.

Step 3 Enter the following commands on the Cisco ISE CLI:

```
configure terminal
hostname hostname
```

Enter the new hostname you want to configure. Cisco ISE services restart after this step.

Step 4 Enter the following commands:

```
interface gigabit 0
ip address ip_address netmask
```

Assign an IP address that matches the hostname you entered. Enter the appropriate netmask for this IP address. After you finish, Cisco ISE prompts you to restart services. For details on the ip address and hostname commands, refer to the *Cisco Identity Services Engine CLI Reference Guide*.

Step 5 Enter **Y** to restart Cisco ISE services.

Connect a Cloned Cisco VM to the Network

After you power on the system and change the IP address and hostname, connect the Cisco ISE node to the network.

Procedure

- Step 1** Right-click the newly cloned Cisco ISE virtual machine (VM) and click **Edit Settings**.
 - Step 2** Click **Network adapter** in the Virtual Machine Properties dialog box.
 - Step 3** In the Device Status area, check the **Connected** and **Connect at power on** check boxes.
 - Step 4** Click **OK**.
-

Migrate Cisco ISE VM from Evaluation to Production

After evaluating the Cisco ISE release, you can migrate the system from an evaluation environment to a fully licensed production environment.

Before you begin

- When you move the VMware server to a production environment that supports a larger number of users, be sure to reconfigure the Cisco ISE installation to the recommended minimum disk size or higher (up to the allowed maximum of 2.4 TB).
- Please note that you cannot migrate data to a production VM from a VM created with less than 300 GB of disk space. Data can only be migrated from VMs created with 300 GB or more disk space to a production environment.

Procedure

- Step 1** Back up the configuration of the evaluation version.
 - Step 2** Ensure that your production VM has the required amount of disk space.
 - Step 3** Install a production deployment license.
 - Step 4** Restore the configuration to the production system.
-

Check Virtual Machine Performance On-Demand

You can run the **show tech-support** command from the CLI to check VM performance at any time. The output of this command is similar to this example:

```
ise-vm123/admin# show tech | begin "disk IO perf"
Measuring disk IO performance
*****
Average I/O bandwidth writing to disk device: 48 MB/second
Average I/O bandwidth reading from disk device: 193 MB/second
```

```

WARNING: VM I/O PERFORMANCE TESTS FAILED!
WARNING: The bandwidth writing to disk must be at least 50 MB/second,
WARNING: and bandwidth reading from disk must be at least 300 MB/second.
WARNING: This VM should not be used for production use until disk
WARNING: performance issue is addressed.
Disk I/O bandwidth filesystem test, writing 300 MB to /opt:
314572800 bytes (315 MB) copied, 7.81502 s, 40.3 MB/s
Disk I/O bandwidth filesystem read test, reading 300 MB from /opt:
314572800 bytes (315 MB) copied, 0.416897 s, 755 MB/s

```

Virtual Machine Resource Check from the Cisco ISE Boot Menu

You can check virtual machine resources from the boot menu without installing Cisco ISE.

The CLI transcript appears in this example:

```

Cisco ISE Installation (Serial Console)
Cisco ISE Installation (Keyboard/Monitor)
System Utilities (Serial Console)
System Utilities (Keyboard/Monitor)

```

Use the arrow keys to select **System Utilities (Serial Console)** or **System Utilities (Keyboard/Monitor)** and press **Enter**. The screen appears:

Available System Utilities:

```

[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload

```

Enter option [1 - 3] q to Quit

Enter **2** to check for VM resources. The output will resemble this example:

```

*****
***** Virtual Machine host detected..
***** Hard disk(s) total size detected: 600 Gigabyte
***** Physical RAM size detected: 16267516 Kbytes
***** Number of network interfaces detected: 6
***** Number of CPU cores: 12
***** CPU Mhz: 2300.00
***** Verifying CPU requirement...
***** Verifying RAM requirement...
***** Writing disk partition table...

```

Linux KVM

KVM Virtualization Check

Your host processor must support KVM virtualization. For Intel, check for VT-x. For AMD, check for AMD-V. Open a terminal window on your host and run the **cat /proc/cpuinfo** command. You should see either the "vmx" flag or the "svm" flag displayed in the command output.

- For Intel VT-x:

```
# cat /proc/cpuinfo
flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush
dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx
pdpe1gb rdtscp lm constant_tsc arch_perfmon pebs bts rep_good nopl xtopology nonstop_tsc
aperfmpperf eagerfpu pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 cx16 xtpr pdcm pcid dca sse4_1 sse4_2 x2apic popcnt
tsc_deadline_timer aes xsave avx lahf_lm arat epb xsaveopt
pln pts dtherm tpr_shadow vnmi flexpriority ept vpid
```

- For AMD-V:

```
# cat /proc/cpuinfo
flags: fpu tsc msr pae mce cx8 apic mtrr mca cmov pat pse36 clflush mmx fxsr sse sse2
ht syscall nx mmxext fxsr_opt rdtscp lm 3dnowext 3dnow
pni cx16 lahf_lm cmp_legacy svm cr8_legacy
```

Install Cisco ISE on KVM

This procedure explains how to create a KVM on RHEL and install Cisco ISE on it using the Virtual Machine Manager (virt-manager).

If you choose to install Cisco ISE through the CLI, enter a command similar to this one:

```
#virt-install --name=kvm-ise1 --arch=x86_64 --cpu=host --vcpus=2 --ram=4096
--os-type=linux --os-variant=rhel6 --hvm --virt-type=kvm
--cdrom=/home/admin/Desktop/ise-3.x.0.x.SPA.x86_64.iso
--disk=/home/libvirt-images/kvm-ise1.img,size=300
--network type=direct,model=virtio,source=eth2,source_mode=bridge
```

where *ise-3.4.0.x.SPA.x86_64.iso* is the name of the Cisco ISE ISO image.

Before you begin

Download the Cisco ISE ISO image to your local system.

Procedure

Step 1

From the Virtual Machine Manager window, click **File** and navigate to **New Virtual Machine**. In the **Create a new virtual machine** dialog box, complete these actions:

- Click **Local install media (ISO media or CDROM)** and click **Forward**.
- Uncheck the **Automatically detect from the installation media/source** check box.
- Choose **Red Hat Enterprise Linux 8.2** from the OS drop-down list.
- Click **Browse** and choose the disk file system directory from the storage pools navigation pane.
- Click **Browse Local** and select the ISO image from your local system and click **Open**.
- Click **Forward**.
- Choose the Memory and CPU settings and click **Forward**.
- Check the **Enable storage for the virtual machine** check box.

- i. Click **Select or create custom storage**.
- j. Click **Manage**. In the **Choose Storage Volume** dialog box, complete these actions:
 1. Click + icon next to **Volumes**.
 2. Choose **RAW** from the **Format** drop-down list.
 3. Enter the **Max Capacity** as 300 GB.
Note
Use at least 300 GB for production PSN or pxGrid, and at least 600 GB for PAN or MnT personas. For detailed recommendations, see the table titled **Recommended disk space for VMs** in this guide.
 4. Click **Finish**.
- k. Choose the volume that you created and click **Choose Volume**.
- l. Click **Forward**.
- m. Check the **Customize configuration before install** check box and click **Finish**.

The installation screen appears.

Step 2 Click **NIC:61:25:78** from the left navigation menu. Under **Details** tab, perform these actions:

- a. Choose **Host device eno1:macvtap** as the Network source.
- b. Choose **Bridge** as the Source mode.
- c. Choose **virtio** as the Device model.
- d. Click **Apply**.

Step 3 Click **Overview** from the left navigation menu. Under **Details** tab, perform these actions:

- a. Choose the required firmware from the **Firmware** drop-down list.
- b. Click **Apply**.

Step 4 Click **Begin Installation** to install Cisco ISE on KVM.
The Cisco ISE installation boot menu appears.

Step 5 At the system prompt, enter **1** to continue with the installation.

Step 6 At the system prompt, type **setup** and press **Enter**.
The Setup Wizard appears and guides you through the initial configuration.



Note You must add the following text to the VM settings XML file (under vcpu information) while installing Cisco ISE on Ubuntu Linux KVM. Otherwise, serial number will not be properly displayed in the **About ISE and Server** window:

```
<sysinfo type="smbios">
  <system>
    <entry name="product">KVM</entry>
  </system>
  <baseBoard>
    <entry name="product">KVM</entry>
  </baseBoard>
</sysinfo>
<OS>
  <type arch="x86_64" machine="pc-q35-6.2">hvm</type>
  <boot dev="hd"/>
  <smbios mode="sysinfo"/>
</os>
```

Microsoft Hyper-V

Create a Cisco ISE virtual machine on Hyper-V

This section explains how to create a new virtual machine, map the ISO image, edit CPU settings, and install Cisco ISE on Hyper-V.



Note Cisco ISE does not support Multipath I/O (MPIO). If you use MPIO for the VM, installation will fail.

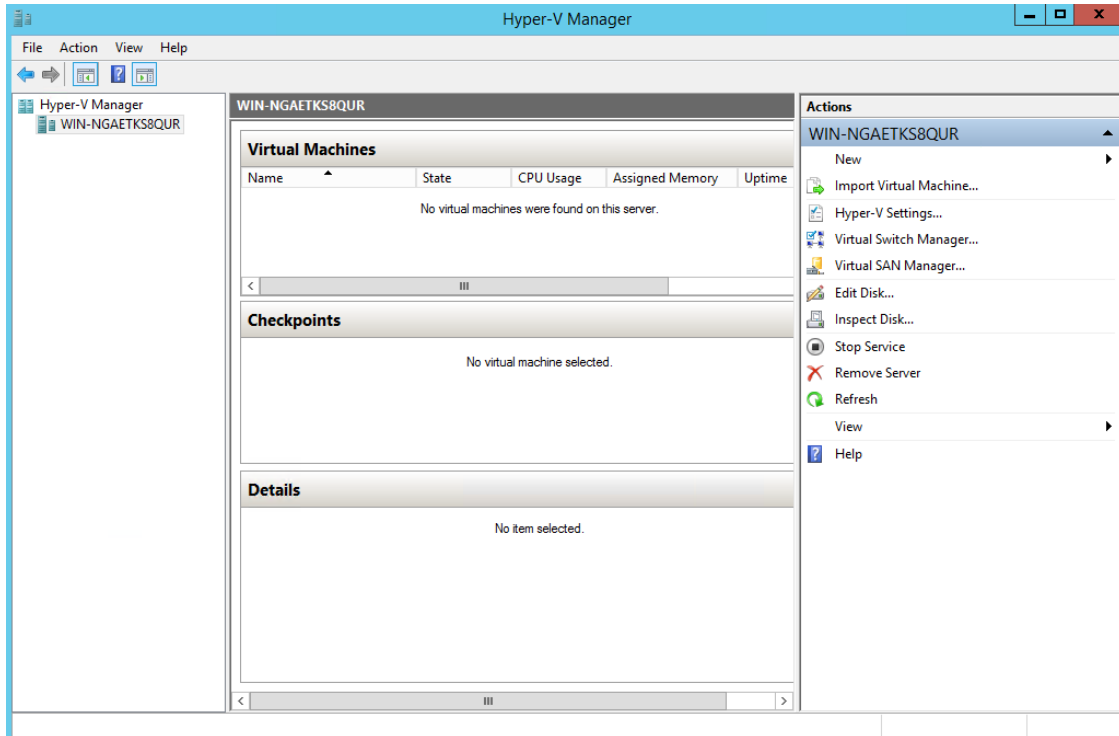
Before you begin

Download the Cisco ISE ISO image from cisco.com to your computer.

Procedure

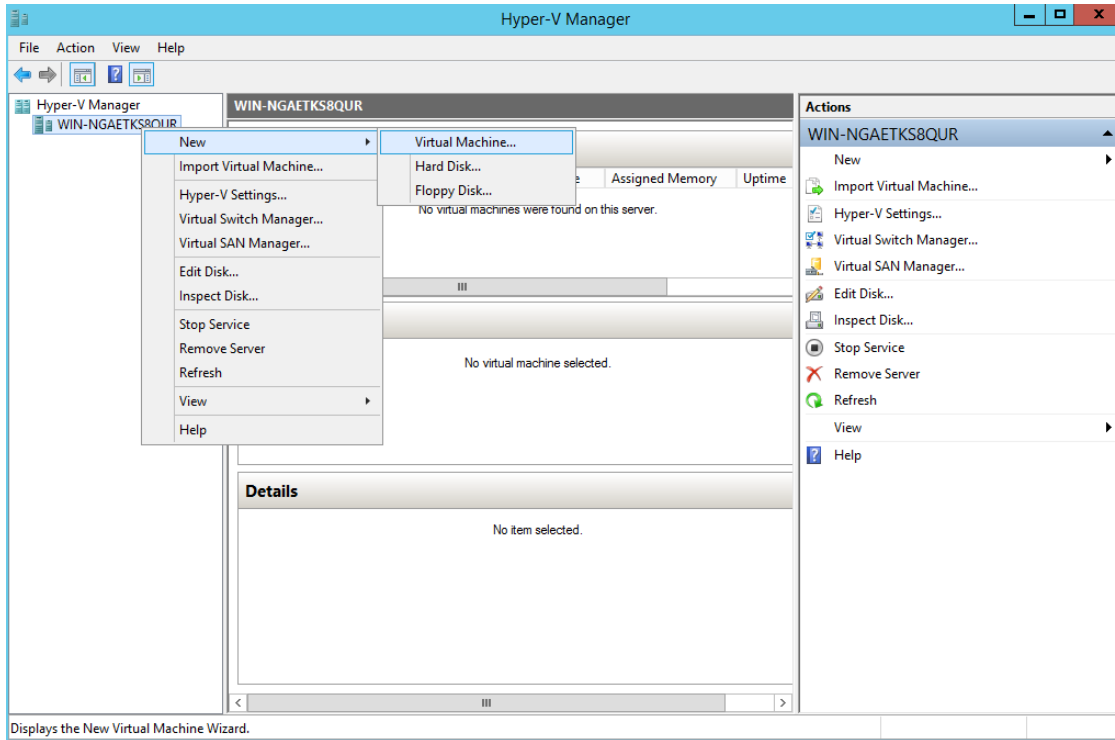
Step 1 Launch Hyper-V Manager on a supported Windows server.

Figure 9: Hyper-V Manager Console



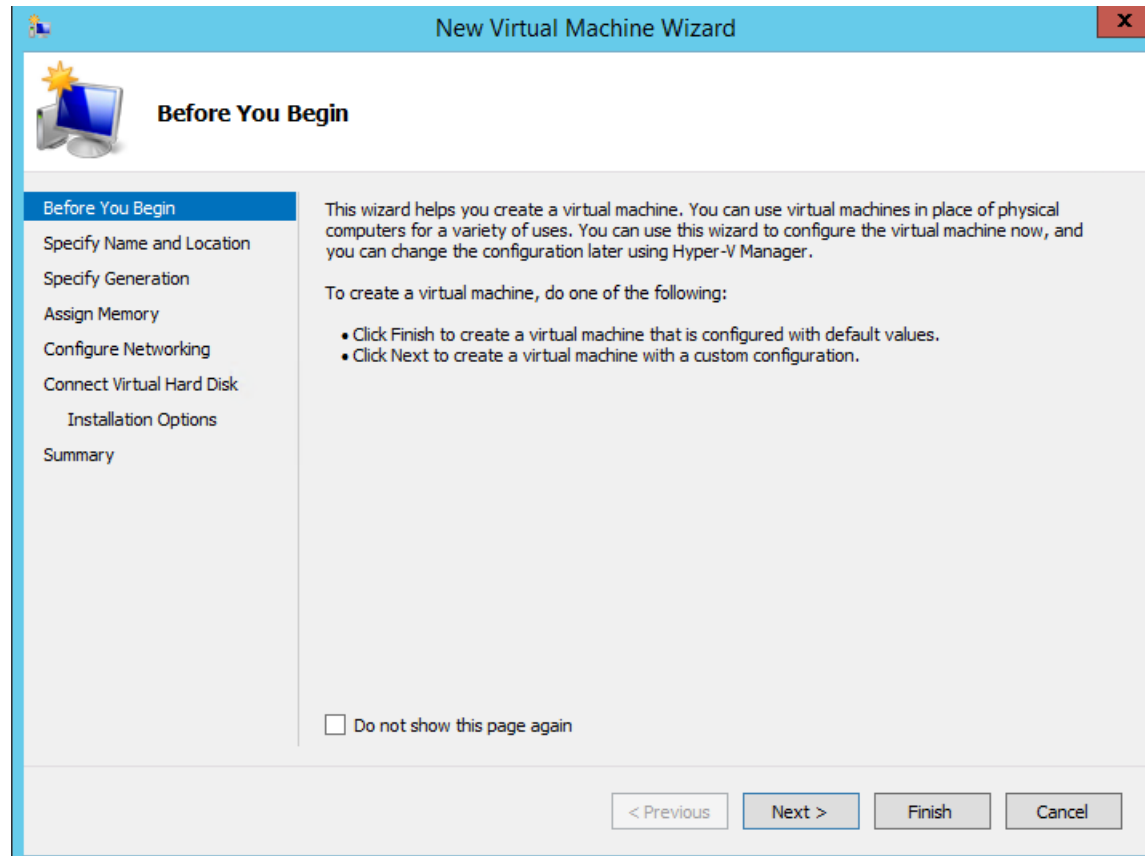
Step 2 Right-click the VM host and click **New > Virtual Machine**.

Figure 10: Create New Virtual Machine



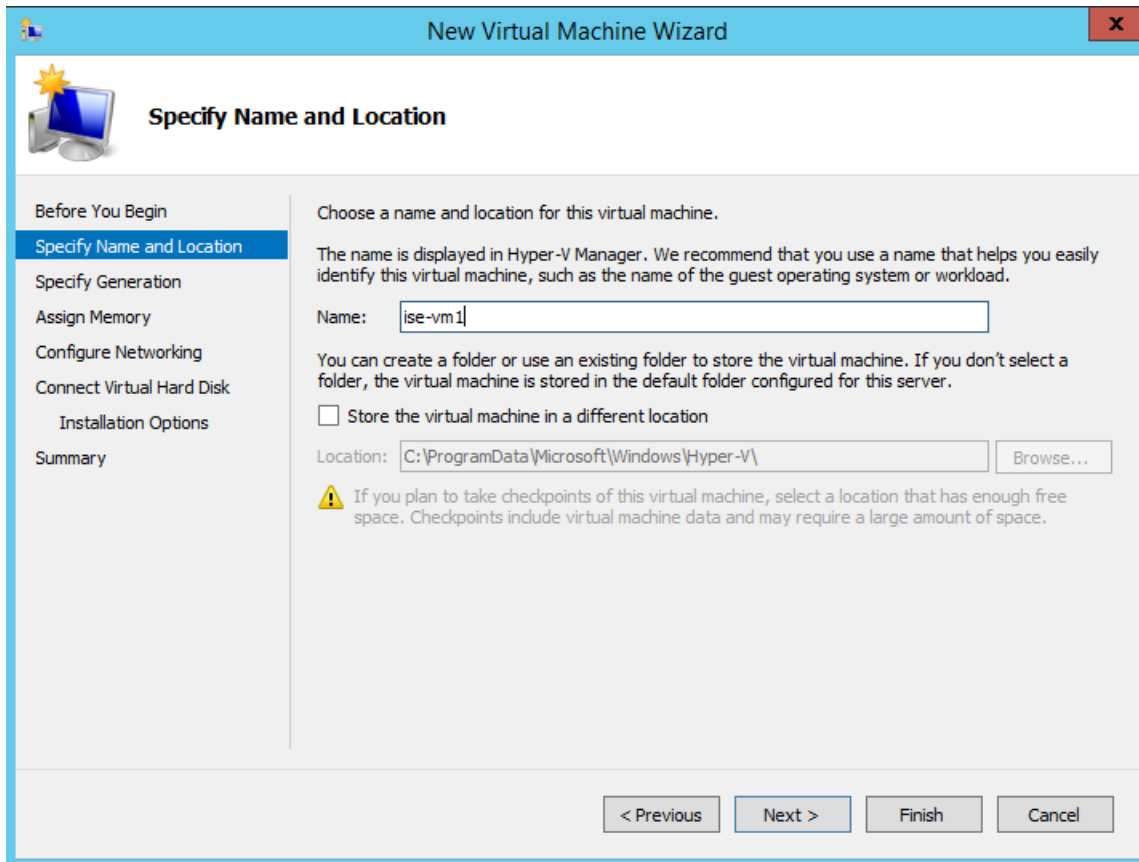
Step 3 Click **Next** to customize the VM configuration.

Figure 11: New Virtual Machine Wizard



Step 4 Enter a name for the VM. Choose a different path to store the VM. Click **Next**.

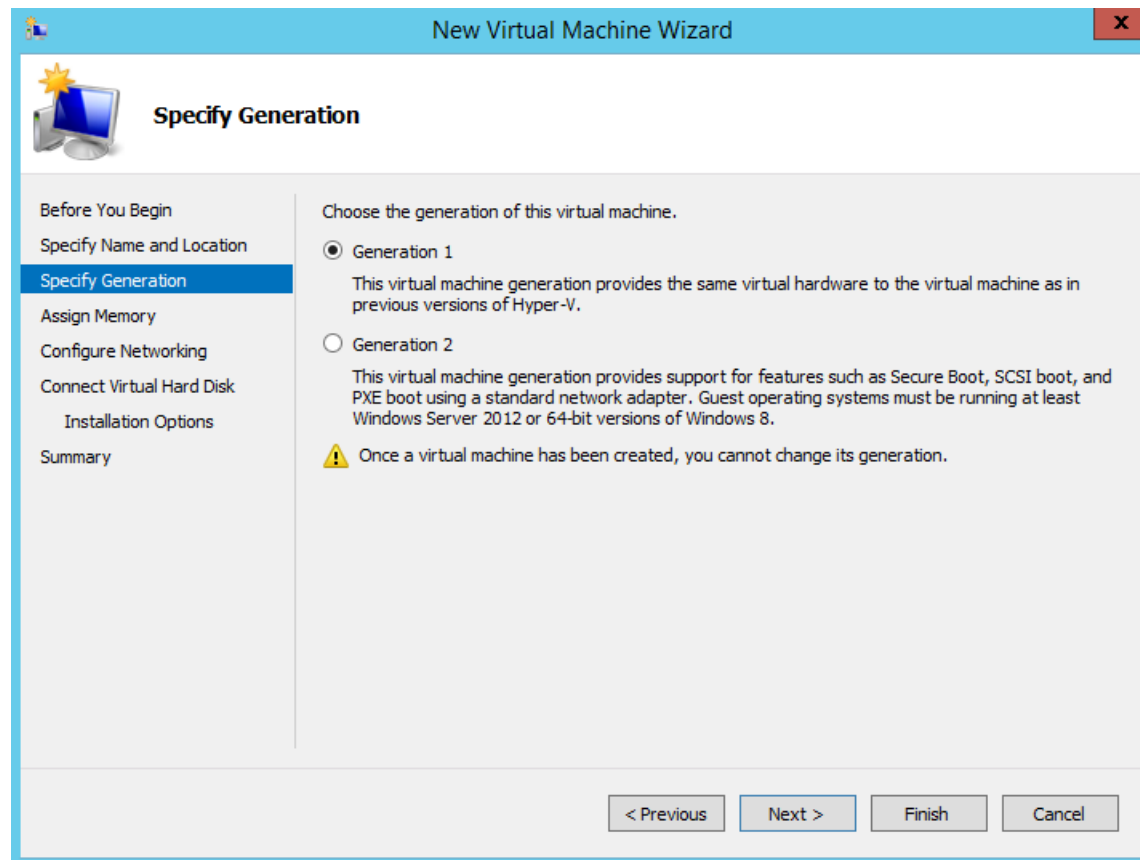
Figure 12: Specify Name and Location



Step 5 Click the **Generation 1** radio button and click **Next**.

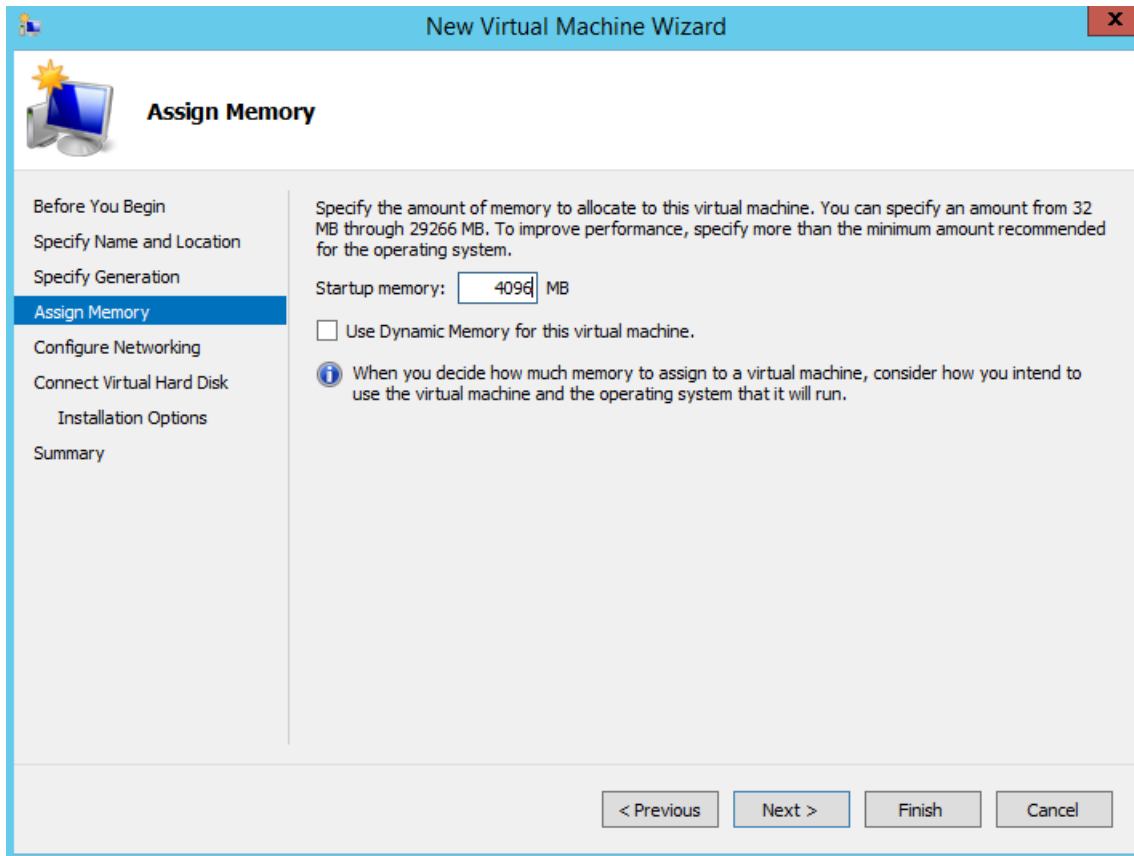
If you create a Generation 2 Cisco ISE VM, disable the **Secure Boot** option in the VM settings.

Figure 13: Specify Generation



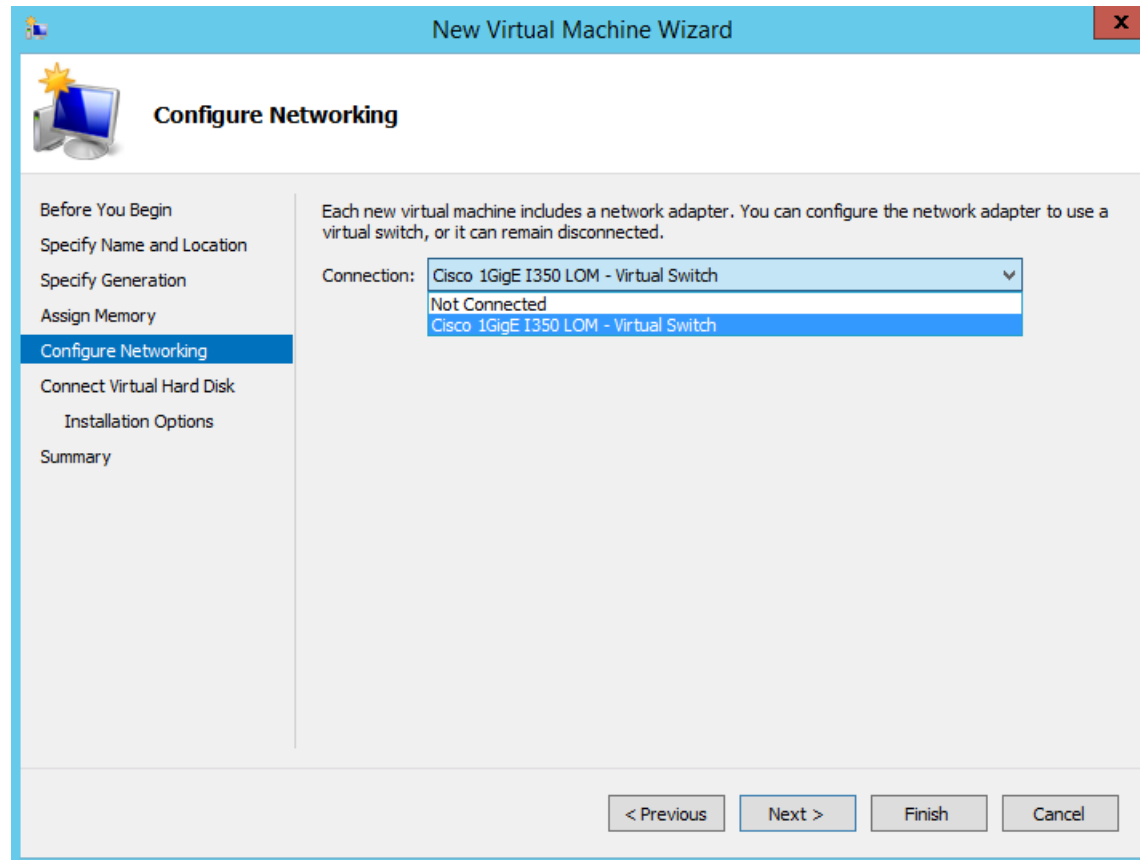
Step 6 Allocate memory to the VM, for example, 16,000 MB. Click **Next**.

Figure 14: Assign Memory



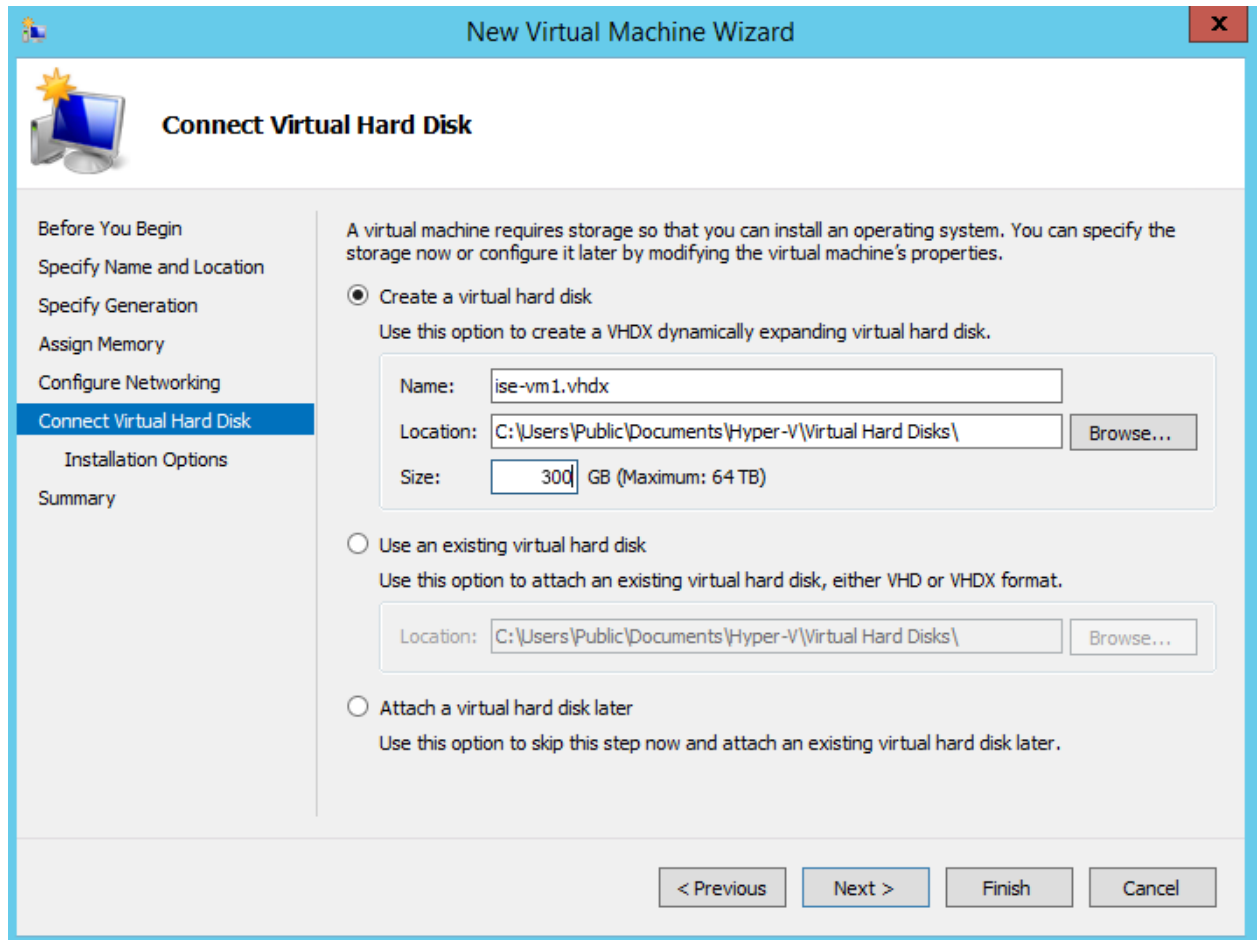
Step 7 Select your network adapter and click **Next**.

Figure 15: Configure Networking



Step 8 Click the **Create a virtual hard disk** radio button and click **Next**.

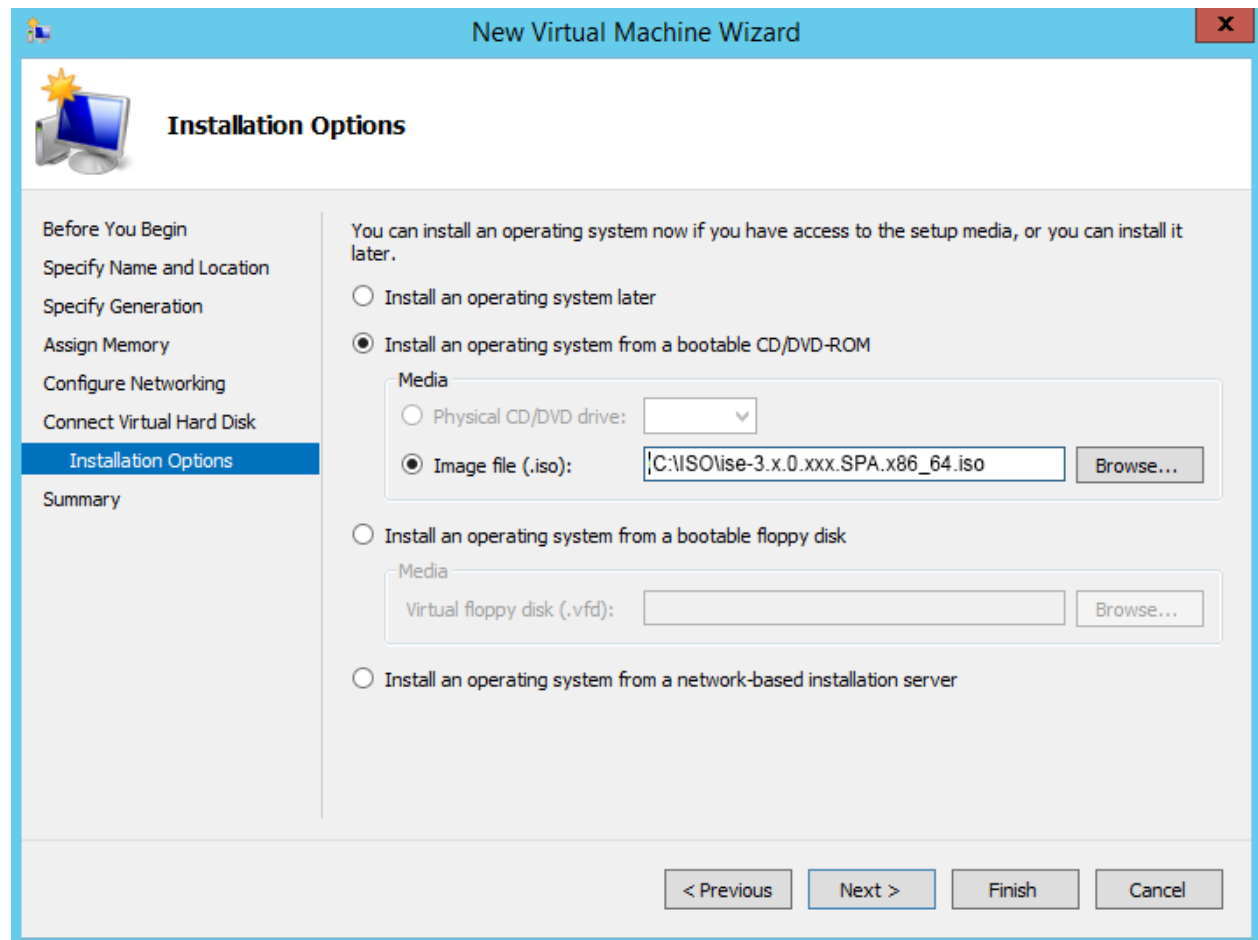
Figure 16: Connect Virtual Hard Disk

**Step 9**

Click the **Install an operating system from a bootable CD/DVD-ROM** radio button.

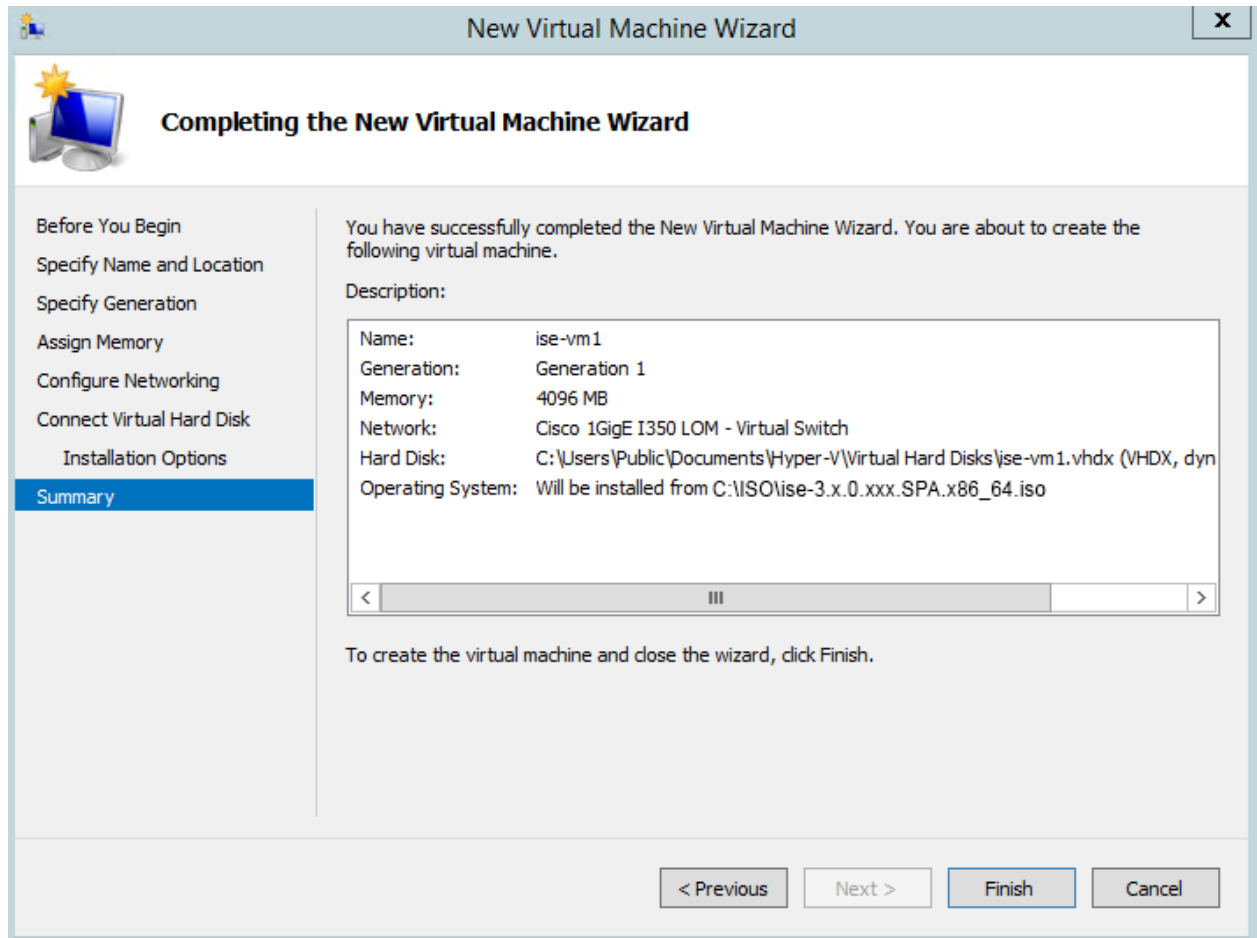
- a) In the Media area, click the **Image file (.iso)** radio button.
- b) Click **Browse** to select the ISE ISO image from the local system and click **Next**.

Figure 17: Installation Options



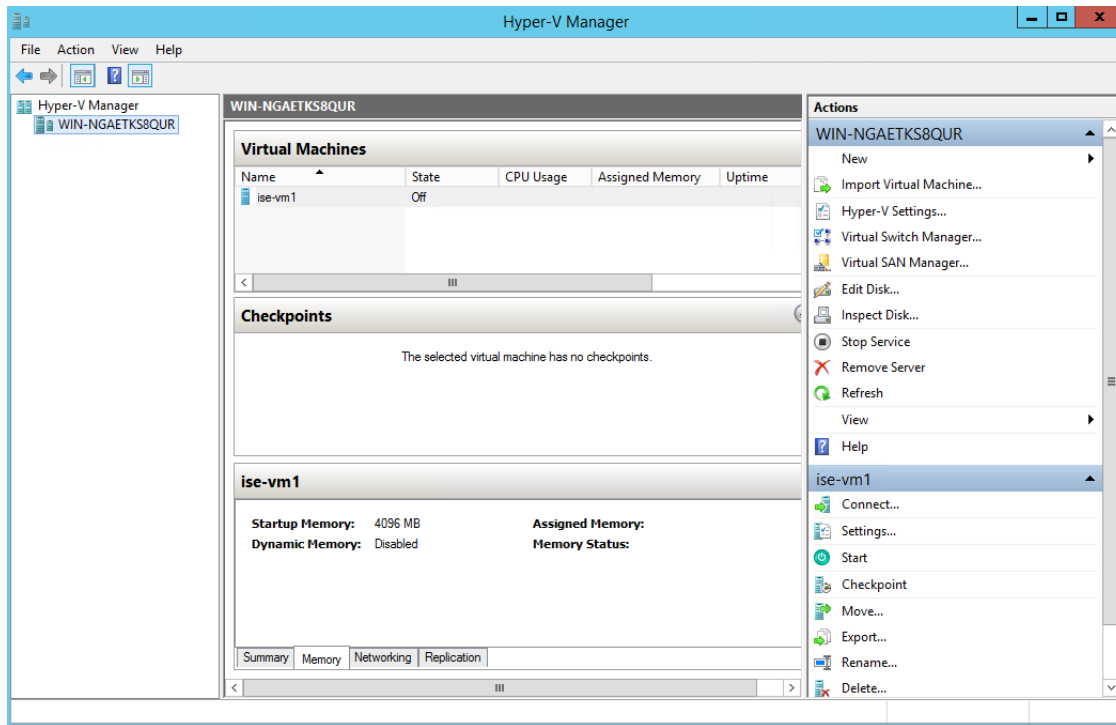
Step 10 Click **Finish**.

Figure 18: Complete the New Virtual Machine Wizard



You have created the Cisco ISE VM on Hyper-V.

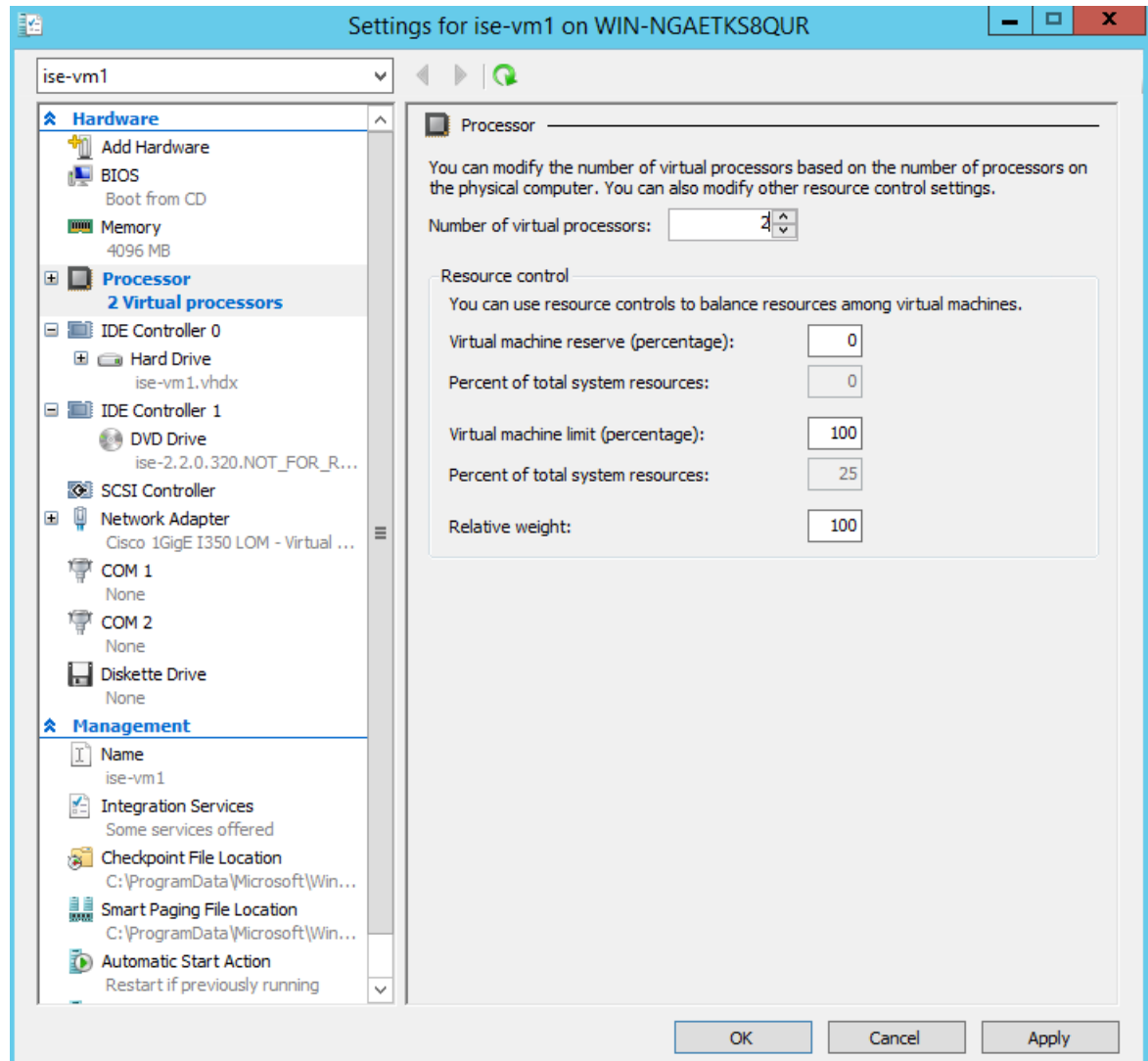
Figure 19: New Virtual Machine created

**Step 11**

Select the VM and edit the VM settings.

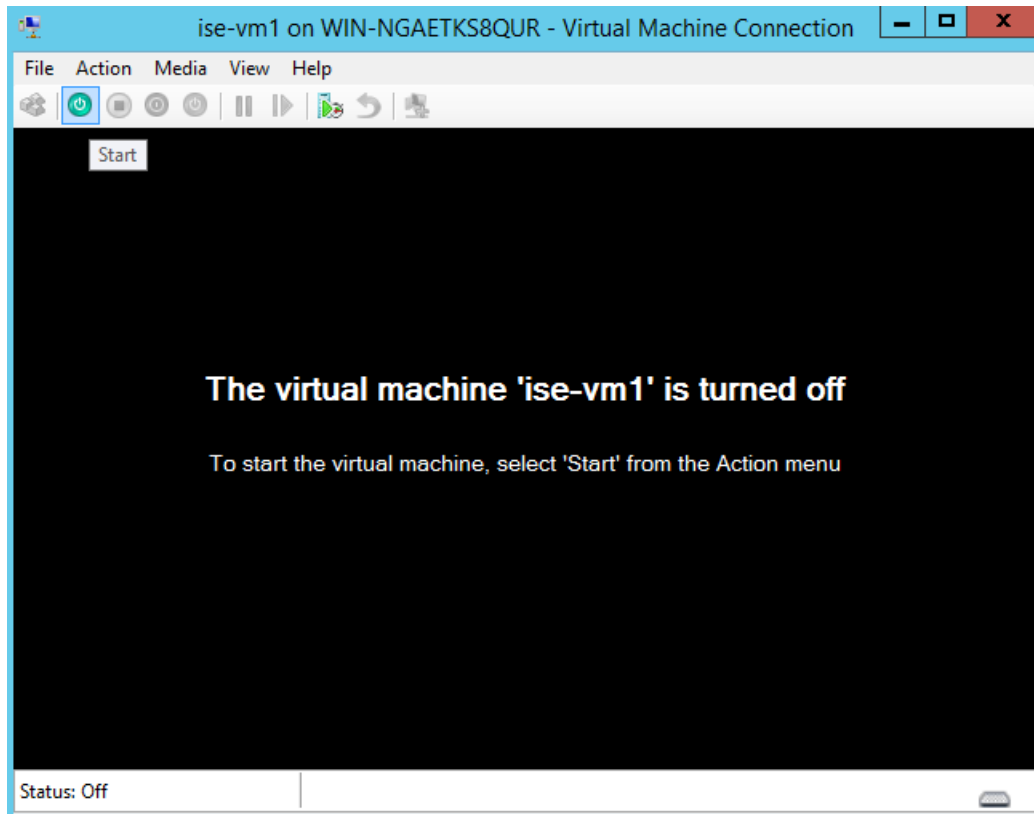
- a) Select **Processor**. Enter the number of virtual processors (such as 6). Click **OK**.

Figure 20: Edit VM Settings



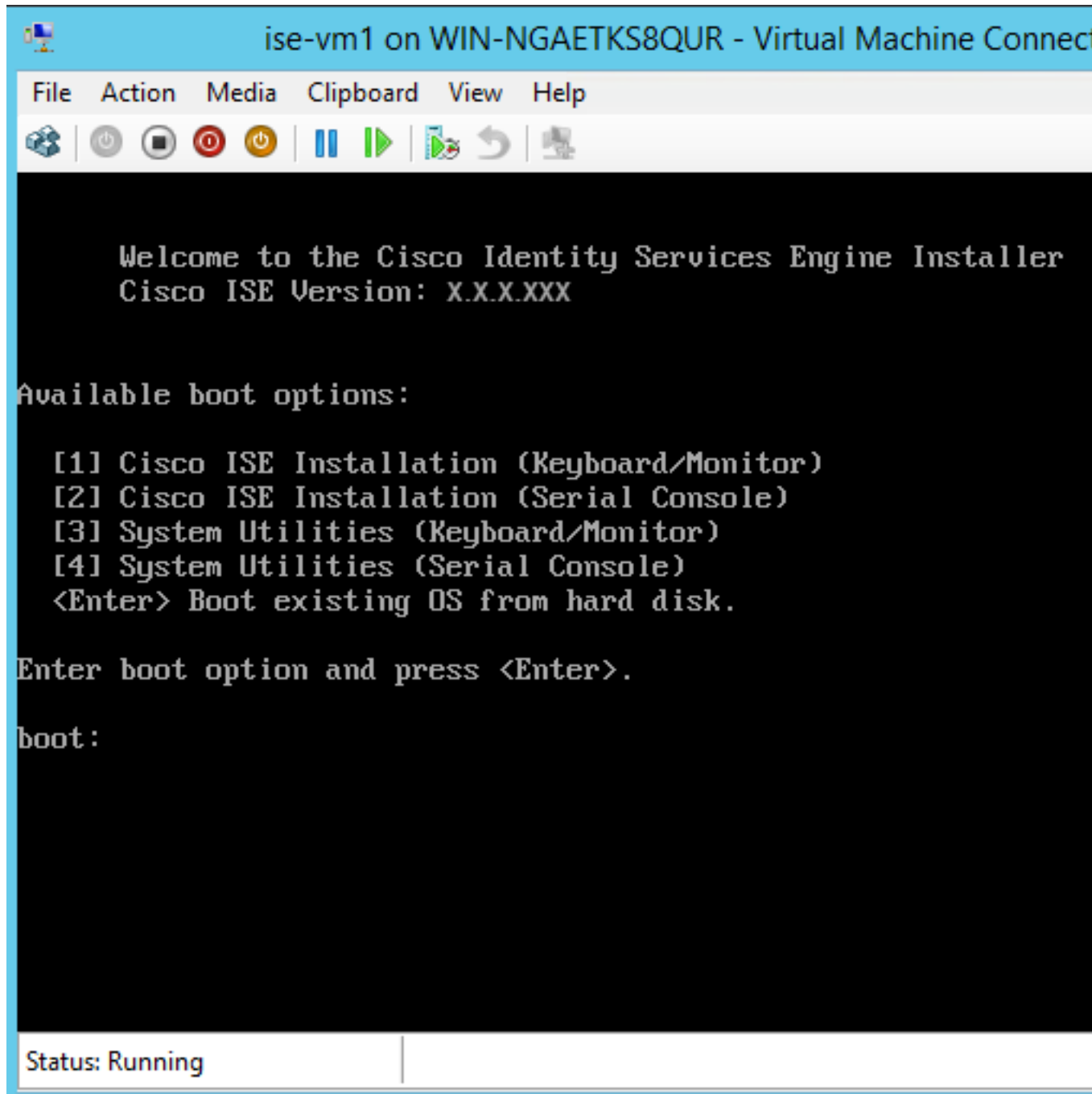
Step 12 Select the VM and click **Connect** to launch the VM console. Click Start to power on the Cisco ISE VM.

Figure 21: Start the Cisco ISE VM



The Cisco ISE installation menu appears.

Figure 22: Cisco ISE installation menu



Step 13 Enter 1 to install Cisco ISE using a keyboard and monitor.

Zero Touch Provisioning

Use Zero Touch Provisioning (ZTP) to automate Cisco ISE installation, patches, hot patches, and infrastructure service enablement without manual steps.

ZTP is available starting with Cisco ISE Release 3.1. There are two options available in ZTP:

- **Mapping .img file:** Use this method for virtual-machine (VM) automatic installations, appliances, and OVA installations. Configure the required parameters: hostname, IP address, netmask, default gateway, DNS domain, primary name server, NTP server, system timezone, SSH, username, and password. Optionally, configure IPv6, patch, hot patch, services, and repository details. See the [ZTP Configuration Image File](#) for more information.



Note For ZTP on Microsoft Hyper-V, use an .iso file and create a Generation 2 VM. Do not use an .img file.

- **VM User Data:** Set mandatory parameters: hostname, IP address, IP netmask, IP default gateway, DNS domain, primary name server, NTP server, system timezone, SSH, username, and password when using this method. For more information, see [VM User Data](#).



Note

- Enable the serial console for both the VM and appliance to track installation progress during ZTP.
- Ensure you have a [ZTP Configuration Image File](#).

Provisioning Cisco ISE with ZTP makes these security features available:

- [Public Key Authentication](#)
- [First Login Password Change](#)



Note Use TFTP, HTTP, HTTPS, or NFS repositories to install hot patches and patches on Cisco ISE with ZTP. Repositories created during ZTP are not visible or accessible from the Cisco ISE GUI. You can use only repositories with anonymous access (no username or password) during ZTP.

Configure Public Key Authentication

Users can be authenticated using public key authentication when you add the public key to the ZTP configuration file. Enabling public key authentication disables password-based user authentication. You can disable public key authentication at any time.

To switch back to password-based authentication, use this command in the Cisco ISE CLI:

```
conf t
no service sshd PubkeyAuthentication
```

For more details about this command, refer to the 'Service' section in the chapter 'Cisco ISE CLI Commands in Configuration Mode' of the *Cisco Identity Services Engine CLI Reference Guide* for your Cisco ISE release.



Note Do not execute the command **service sshd PubkeyAuthentication** unless you have included the public key in the ZTP configuration image file before installation. This disables password-based authentication, requiring you to log in using a private key. If you encounter this issue, use the console port to log in to Cisco ISE and revert the configuration.

Procedure

- Step 1** Generate a public and private RSA key pair using a third-party application.
- Step 2** Include the public key that is generated in the [ZTP configuration image file](#).
- Step 3** Install Cisco ISE using ZTP.
- Step 4** Log in to the CLI of Cisco ISE using the private key that is generated, using the following command:

```
ssh -i <path to private key> <username>@<ise-ip>
```

You can now successfully log in to the CLI of Cisco ISE using your private key.

First Login Password Change

After successfully installing Cisco ISE using ZTP, you are prompted to reset the password the first time you log in to the Cisco ISE GUI. The password must be changed because it is specified in plain text in the ZTP configuration image file. By default, this feature is enabled when you install Cisco ISE using ZTP.

Automatic Installation in Virtual Machine

These subsections provide information about automatic installation in the VM.

These settings are applicable for all on-prem hypervisors:

- VMware
- Linux KVM
- Microsoft Hyper-V
- Nutanix AHV

Automatic Installation in Virtual Machine Using the ZTP Configuration Image File

Procedure

- Step 1** Log in to the VMware client.

Note

If you already have an existing VM setup, proceed to Step 2 and continue to Step 6. For a new VM setup, go directly to Step 8.

Step 2 To enter BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**.

Step 5 In the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note

You must change the firmware from **BIOS** to **EFI** in the VM boot mode settings. This allows you to boot GPT partitions with 2 TB or greater capacity.

Step 6 Click **OK**.

Step 7 Ensure that the time zone and the correct boot order are set in BIOS or EFI:

- a) If the VM is turned on, turn the system off.
- b) Turn on the VM.

The system enters the BIOS setup mode.

- c) In the main **BIOS** menu, use the arrow keys to go to the **Date and Time** field and press **Enter**.
- d) Enter the time zone.

This time zone setting ensures your reports, logs, and posture-agent log files from all nodes stay synchronized by timestamp.

- e) Using the arrow keys, navigate to the boot menu and press **Enter**.
- f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.
- g) Using the arrow keys, navigate to the **Exit** menu and choose **Exit Saving Changes**. (Press the Enter or Return key to select your choice).
- h) Choose **Yes** to save the changes and exit.

Step 8 Insert the Cisco ISE software DVD into the primary CD or DVD drive on the VMware ESXi host.

Step 9 Insert the ZTP configuration image file into a secondary CD or DVD drive.

Step 10 Power on the VM.

When the DVD starts, the console displays this message:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

Note

From Cisco ISE 3.1 onwards, pressing **Enter** choosing a boot option triggers ZTP instead of starting installation with the hard disk.

Step 11 After 150 seconds, the boot process automatically starts if your system meets the prerequisites.

Note

- Monitor installation logs through the serial console while ZTP is running. When the setup prompt appears, you can monitor logs from the VM console.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD or DVD.

Perform this procedure using ZTP from the setup prompt with the keyboard until the setup prompt appears.

1. Install Cisco ISE manually until setup (using boot option 1 or 2) and use the procedure steps to create the ZTP configuration image file.
2. Power off the VM and map the ZTP configuration image file to the CD or DVD drive.
3. Power on the VM.

The installation process uses the setup details from the ZTP configuration file you mapped to the CD or DVD drive.

Troubleshooting

Issue: If the automatic installation in the VM is triggered without mapping the .img file, after 150 seconds, the installation fails with this message.

```
***** The ZTP configuration image is missing or improper. Automatic installation flow
        exited.
***** Power off and attach the proper ZTP configuration image or choose manual boot to
        proceed.
```

Solution: This error message is displayed only on the serial console and not on the VM console. If this happens in an existing VM where Cisco ISE is already installed, the hard disk will not be formatted in this state. The existing VM can be recovered by performing these steps:

1. Turning off the VM.
2. Powering on the VM.
3. Press option five to boot from the hard disk within 150 seconds to load the existing VM.

Issue: If the setup details are invalid in the configuration file, ZTP installation is stopped and the following message is displayed on the VM Console:

```
=====
Cisco ISE Installation Failed
=====

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
=====
```

Solution:

1. Create a new configuration .img file with valid details.
2. Power off the VM.

3. Map the new valid image to the CD or DVD drive.
 4. Power on the VM.
- Installation begins from the setup.

Automatic Installation in Virtual Machine using VM User Data

Procedure

Step 1 Log in to the VMware client.

Note

If you already have an existing VM setup, proceed to Step 2 and continue till Step 6. For a new VM setup, go directly to Step 8.

Step 2 For the VM to enter the BIOS setup mode, right-click the VM and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**.

Step 5 In the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note

You must change the firmware from **BIOS** to **EFI** in the the boot mode of VM settings in order to boot GPT partitions with 2 TB or more capacity.

Step 6 Click **OK**.

Step 7 Ensure that the time zone and the correct boot order are set in BIOS/EFI:

- a) If the VM is turned on, turn the system off.
- b) Turn on the VM.

The system enters the BIOS setup mode.

- c) In the main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.
- d) Enter the time zone.

This time zone setting ensures that the reports, logs, and posture-agent log files from the various nodes in your deployment are always synchronized with regard to the time stamps.

- e) Using the arrow keys, navigate to the boot menu and press **Enter**.
- f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.
- g) Using the arrow keys, navigate to the **Exit** menu and choose **Exit Saving Changes** (Press the Enter or Return key to select your choice).
- h) Choose **Yes** to save the changes and exit.

Step 8 Insert the Cisco ISE software DVD into the VMware ESXi host's primary CD/DVD drive.

Step 9 Configure the [VM user data](#) options.

Note

If both the .img file and VM user data options are configured in the VM, the user data option is considered.

Step 10 Turn on the VM.

When the DVD boots, the console displays the following message:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

Note

From Cisco ISE 3.1 onwards, pressing **Enter** without entering a boot option does not trigger the installation using the hard disk option. Instead it triggers ZTP.

Step 11

After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note

- Installation logs can be monitored only through the serial console because ZTP works only through the serial console. It can be monitored from the VM console after the setup prompt is displayed.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD/DVD.

To leverage ZTP from the setup prompt (ZTP is carried out using the keyboard until the setup prompt appears) perform this procedure:

1. Power off the VM.
2. Configure user-data option mentioned above.
3. Power on the VM .

The setup details are picked from the VM options.

Troubleshooting

Issue: If invalid setup details are entered in the user data option, the ZTP installation stops and the following message is displayed on the VM console:

```
=====
Cisco ISE Installation Failed
=====
```

```
Error: Sync with NTP server failed.
```

```
Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
=====
```

Solution:

1. Power off the VM.

2. Update user data details with valid data.
3. Power on the VM.

Installation begins from the setup.

Automatic Installation in Appliance

The following subsections provide information about automatic installation in an appliance.

Automatic Installation in Appliance Using the ZTP Configuration Image File

Procedure

- Step 1** Log in to the SNS Appliance.
- Step 2** Shut down the host system.
- Step 3** Choose **Compute > Remote Management > Virtual media**.
- Step 4** Map the Cisco ISE software ISO and the ZTP configuration image file to the primary CD or DVD drive and the secondary CD or DVD drive.
- Step 5** Start the host system.

When the appliance boots, the console displays this message:

```
Please select boot device:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Cisco ISE Installation Through ZTP Configuration (Serial Console)
```

- Step 6** After 2 minutes and 30 seconds, the process starts automatically if the prerequisites are met.

Note

- ZTP works on the SNS appliance through virtual media only.
- Before mapping the ISO file, ensure the .img file is mapped in virtual media.
 - Installation logs can be monitored only through the serial console because ZTP works through the serial console. The logs can be monitored through the KVM console after the setup prompt appears
- Only the .img file supports automatic installation in the appliance.

To use ZTP from the setup prompt (ZTP uses the keyboard until the setup prompt appears), complete these steps:

1. Install Cisco ISE manually till setup (using boot option 1 or 2) and create the ZTP configuration image file using the steps described in the previous.
2. Shut down the host system and map the ZTP configuration image file that is created, to the CD or DVD drive.
3. Start the host system.

The setup details are picked from the ZTP configuration file that is mapped to the CD or DVD drive.

Troubleshooting

Issue: If the automatic installation in the appliance is triggered without mapping the image file, after 150 seconds, the installation fails with the this message:

```
***** The ZTP configuration image is missing or improper. Automatic installation flow
exited.
***** Power off and attach the proper ZTP configuration image or choose manual boot to
proceed.
```

Solution:

1. Turn off the VM.
2. Turn on the VM.
3. To load the existing VM, press option 5 to boot from the hard disk, within 150 seconds.

Issue: If the setup details are invalid in the config file, ZTP installation is stopped and the following message is displayed on the Keyboard, video, and mouse (KVM) console:

```
=====
Cisco ISE Installation Failed
=====
Error: Sync with NTP server failed.
Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
=====
```

Solution:

1. Create a new configuration .img file with valid details.
2. Power off the VM.
3. Map the new valid image to the CD or DVD drive.
4. Power on the VM.

Installation begins from the setup prompt.

Trigger Automatic Installation using UCS XML APIs

To trigger automatic installation:



Note The API URL and the request header are the same for all the methods:

API URL

`https://<ucs_server_ip>/nuova`

Header

```
headers["Accept"] = "application/xml"
headers["Content-Type"] = "application/xml"
```

Procedure

Step 1 Obtain the login session cookie to authenticate the session.

The aaaLogin method initiates the login process and is required to begin a session. This method establishes the HTTP or HTTPS session between the client and Cisco IMC. The session cookie is then used in subsequent requests to maintain authentication.

Request

```
<aaaLogin inName='admin' inPassword='password'/>
```

Response

```
<aaaLogin cookie="" response="yes" outCookie="<real_cookie>" outRefreshPeriod="600" outPriv="admin"
  outSessionId="17" outVersion="3.0(0.149)"> </aaaLogin>
```

Step 2 Configure the Cisco ISE ISO file as virtual media.

This configures a Cisco ISE ISO file as a virtual media volume.

Request

```
<configConfMo cookie='<real_cookie>' dn='sys/svc-ext/vmedia-svc/vmmmap-ISE_ISO' inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmmap-ISE_ISO'
  map='nfs'
  remoteFile='<ise_iso_file>'
  remoteShare='<nfs_server_path>'
  status='created' volumeName='ISE_ISO' />
</inConfig>
</configConfMo>
```

Response

```
<configConfMo dn="sys/svc-ext/vmedia-svc/vmmmap-ISE_ISO"
  cookie="<real_cookie>" response="yes">
<outConfig>
  <commVMediaMap volumeName="ISE_ISO" map="nfs"
    remoteShare='<nfs_server_path>'
    remoteFile="<ise_iso_file>"
    mappingStatus="In Progress"
    dn="sys/svc-ext/vmedia-svc/vmmmap-ISE_ISO" status="created"/>
</outConfig>
</configConfMo>
```

Step 3 Configure the configuration image file as a virtual media volume.

This configures a configuration image as a vMedia volume.

Request

```
<configConfMo cookie='<real_cookie>'
dn='sys/svc-ext/vmedia-svc/vmmmap-CONFIG-IMG' inHierarchical='false'>
<inConfig>
<commVMediaMap dn='sys/svc-ext/vmedia-svc/vmmmap-CONFIG-IMG'
  map='nfs'
  remoteFile='<config_img_file>'
```

```

    remoteShare='<nfs_server_path>'
    status='created' volumeName='CONFIG-IMG' />
</inConfig>
</configConfMo>

```

Response

```

<configConfMo dn="sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG"
  cookie="<real_cookie>" response="yes">
<outConfig>
  <commVMediaMap volumeName="CONFIG-IMG" map="nfs"
    remoteShare='<nfs_server_path>'
    remoteFile="<config_img_file>"
    mappingStatus="In Progress"
    dn="sys/svc-ext/vmedia-svc/vmmap-CONFIG-IMG" status="created"/>
  </outConfig>
</configConfMo>

```

Step 4 Set the CD-ROM as the first device in the boot order.

This maps the Cisco ISE ISO file that is picked for installation during the power restart.

Request

```

<configConfMo cookie="<real_cookie>"
inHierarchical="true" dn="sys/rack-unit-1/boot-policy">
  <inConfig>
    <lsbootDef dn="sys/rack-unit-1/boot-policy" rebootOnUpdate="yes">
      <lsbootVirtualMedia access="read-only" order="1" dn="sys/rack-unit-1/boot-policy/vm-read-only"/>
    </lsbootDef>
  </inConfig>
</configConfMo>

```

Response

```

<configConfMo dn="sys/rack-unit-1/boot-policy" cookie="<real_cookie>" response="yes">
<outConfig>
  <lsbootDef dn="sys/rack-unit-1/boot-policy" name="boot-policy" purpose="operational"
rebootOnUpdate="no" status="modified" >
  </lsbootDef>
</outConfig>
</configConfMo>

```

Step 5 Enable the SoL (Serial over LAN).

This enables the SoL to view installation logs through Telnet.

Request

```

<configConfMo cookie='<real_cookie>'
dn='sys/rack-unit-1/sol-if'>
<inConfig>
  <solIf dn='sys/rack-unit-1/sol-if' adminState='enable'/>
</inConfig>
</configConfMo>

```

Response

```

<configConfMo dn="sys/rack-unit-1/sol-if" cookie="<real_cookie>" response="yes">
<outConfig>
<solIf dn="sys/rack-unit-1/sol-if" adminState="enable" name="SoLInterface" speed="115200" comport="com0"
  sshPort="2400" status="modified" ></solIf></outConfig>
</configConfMo>

```

Step 6 Power restart.

This triggers Cisco ISE installation in automatic mode.

Request

```
<configConfMo cookie='<real_cookie>' dn='sys/rack-unit-1'>
<inConfig><computeRackUnit
dn='sys/rack-unit-1'
adminPower='cycle-immediate' />
</inConfig>
</configConfMo>
```

Response

```
<configConfMo dn="sys/rack-unit-1" cookie="<real_cookie>" response="yes">
<outConfig>
  <computeRackUnit dn="sys/rack-unit-1" adminPower="policy" availableMemory="262144"
model="SNS-3695-K9" memorySpeed="2400" name="SNS-3695-K9" numofAdaptors="0" numofCores="12"
numofCoresEnabled="12" numofCpus="1" numofEthHostIfs="0" numofFcHostIfs="0" numofThreads="24"
operPower="on" originalUuid="1935836B-B968-4031-8A98-7984F1D35449" presence="equipped" serverId="1"
serial="WZP2228085W" totalMemory="262144" usrLbl="" uuid="1935836B-B968-4031-8A98-7984F1D35449"
vendor="Cisco Systems Inc" cimcResetReason="graceful-reboot
" assetTag="Unknown" adaptorSecureUpdate="Enabled" resetComponents="components" storageResetStatus="NA"
vicResetStatus="NA" bmcResetStatus="NA" smartUsbAccess="disabled" smartUsbStatus="Disabled"
biosPostState="completed" status="modified" >
  </computeRackUnit>
</outConfig>
</configConfMo>
```

Step 7 Log out to end the session.

Request

```
<aaaLogout
  cookie="<real_cookie>"
  inCookie="<real_cookie>"
</aaaLogout>
```

Response:

```
<aaaLogout cookie="" response="yes" outStatus="success"> </aaaLogout>
```

For more information, see [UCS API methods](#).

OVA Automatic Installation

Use these sections to automatically install the OVA.

Automatic OVA Installation Using the ZTP Configuration Image File

Procedure

Step 1 Log in to the VMware client.

Note

If you already have an existing virtual machine setup, complete Steps 2 through 6. For a new virtual machine setup, start with Step 8.

Step 2 To enter BIOS setup mode, right-click the virtual machine and select **Edit Settings**.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**.

Step 5 In the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note

Change the firmware from **BIOS** to **EFI** in the VM's boot mode to enable GPT partitions of 2 TB or more.

Step 6 Click **OK**.

Step 7 Ensure that the Coordinated Universal Time (UTC) is set and the boot order is correct in BIOS.

- a) If the virtual machine is turned on, turn the system off.
- b) Turn on the VM.

The system enters the BIOS setup mode.

- c) In the main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.
- d) Enter the UTC or Greenwich Mean Time (GMT) time zone.

This time zone setting keeps reports, logs, and posture-agent log files from all nodes in your deployment synchronized for timestamps.

- e) Use the arrow keys to open the boot menu and press **Enter**.
- f) Using the arrow keys, select the CD-ROM drive and press + to move the CD-ROM drive up the order.
- g) Using the arrow keys, navigate to the **Exit** menu and choose **Exit Saving Changes** (Press the Enter or Return key to select your choice).
- h) Choose **Yes** to save the changes and exit.

Step 8 Import the Cisco ISE OVA file into your VMware ESXi host.

Step 9 Insert the ZTP configuration image file into the primary CD drive or DVD drive of your VMware ESXi host.

Step 10 Turn on your virtual machine.

When the DVD boots, the console displays a message:

```
Automatic installation starts in 150 seconds.  
Available boot options:  
[1] Cisco ISE Installation (Keyboard/Monitor)  
[2] Cisco ISE Installation (Serial Console)  
[3] System Utilities (Keyboard/Monitor)  
[4] System Utilities (Serial Console)  
[5] Hard Disk  
Enter boot option and press <Enter>.  
boot:
```

Note

If you press **Enter** without selecting a boot option in Cisco ISE 3.1 or later, the system initiates ZTP instead of installing using the hard disk option.

Step 11 After 150 seconds, the bootup process automatically starts if the prerequisites are met.

Note

- Monitor the installation logs through the serial console while ZTP runs. After the setup prompt appears, view the logs in your virtual machine console.
- After the Cisco ISE services are started, you must manually unmount the ZTP configuration image file from the CD or DVD.

Use the keyboard to perform ZTP until the setup prompt appears. Then, follow this procedure:

- a. Install Cisco ISE manually using boot option 1 or 2, and create the ZTP configuration image file using the steps in this procedure.
- b. Power off the virtual machine.
- c. Map the ZTP configuration image file to the CD or DVD drive.
- d. Power on the virtual machine.

The system uses the setup details from the ZTP configuration file that mapped to the CD or DVD drive.

Troubleshooting

Issue: If the setup details are invalid in the configuration file, ZTP installation stops and the following message is displayed on the VM console:

```
=====
Cisco ISE Installation Failed
=====

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
=====
```

Solution: This can be resolved by performing the following steps:

1. Create a new configuration .img file with valid details.
2. Power off the VM.
3. Map the new valid image to the CD or DVD drive.
4. Power on the VM.

OVA Automatic Installation Using the VM User Data

Procedure

Step 1 Log in to the VMware client.

Note

If you already set up a VM, start at Step 2 and continue to Step 6. If you are setting up a new VM, start at Step 8.

Step 2 Right-click the VM and select **Edit Settings** to enter the BIOS setup mode.

Step 3 Click the **Options** tab.

Step 4 Click **Boot Options**.

Step 5 In the **Force BIOS Setup** area, check the **BIOS** check box to enter the BIOS setup screen when the VM boots.

Note

Change the firmware from **BIOS** to **EFI** in the VM's boot mode settings so you can boot GPT partitions larger than 2 TB.

Step 6 Click **OK**.

Step 7 Ensure that the Coordinated Universal Time (UTC) and the correct boot order are set in BIOS:

- a) If the VM is turned on, turn the system off.
- b) Power off the VM.

You see the BIOS setup mode.

- c) In the main **BIOS** menu, using the arrow keys, navigate to the **Date and Time** field and press **Enter**.
- d) Enter the Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) zone.

With this time zone setting, the reports, logs, and posture-agent log files from the nodes in your deployment always have synchronized timestamps.

- e) Using the arrow keys, navigate to the boot menu and press **Enter**.
- f) Select the compact disc read-only memory (CD-ROM) drive using the arrow keys and press+ to move the CD-ROM drive up the order.
- g) Using the arrow keys, navigate to the **Exit** menu and choose **Exit Saving Changes** (Press the Enter or Return key to select your choice).
- h) Choose **Yes** to save the changes and exit.

Step 8 Import the Cisco ISE OVA file into the VMware ESXi.

Step 9 Configure the [VM user data](#) options.

Note

The VM uses the user data option if both the image file and the VM user data options are configured.

Step 10 Turn on the VM.

When the DVD boots, the console displays the following message:

```
Automatic installation starts in 150 seconds.
Available boot options:
[1] Cisco ISE Installation (Keyboard/Monitor)
[2] Cisco ISE Installation (Serial Console)
[3] System Utilities (Keyboard/Monitor)
[4] System Utilities (Serial Console)
[5] Hard Disk
Enter boot option and press <Enter>.
boot:
```

Note

From Cisco ISE 3.1 onwards, pressing **Enter** without entering a boot option does not trigger the installation using the hard disk option. Instead, it triggers ZTP.

Step 11 If the prerequisites are met, the bootup process starts automatically after 150 seconds.

Note

- To monitor installation logs, use the serial console. ZTP interacts only through the serial console. Monitoring from the VM console is possible after the setup prompt is displayed.

- After Cisco ISE services have started, manually unmount the ZTP configuration image file from the CD or DVD.

To use ZTP from the setup prompt, perform this procedure. ZTP is carried out using the keyboard until the setup prompt appears.

- Power off the VM.
- Configure user-data option mentioned above.
- Power on the VM .

The VM options provide the setup details.

Troubleshooting information

Issue: If invalid setup details are entered in the user data option, the ZTP installation stops and this message is displayed on the VM console:

```
=====
Cisco ISE Installation Failed
=====

Error: Sync with NTP server failed.

Check the setup details in your configuration image and reboot Cisco ISE
with proper ZTP configuration.
=====
```

Solution: To resolve this issue, complete the following steps.

1. Power off the VM.
2. Update user data details with valid data.
3. Power on the VM.

Installation begins from the setup.

Create a ZTP Configuration Image File

Create the ZTP configuration image file using the `./create_ztp_image.sh ise-ztp.conf ise-ztp.img` command. The script can be executed on Red Hat Enterprise Linux (RHEL), CentOS, or Ubuntu.

To skip the ICMP, DNS, and NTP checks, set the flags to True in the configuration image file:

- **ICMP:** SkipIcmpChecks=true
- **DNS:** SkipDnsChecks=true
- **NTP:** SkipNtpChecks=true



Note The default value for each flag is **false**. By default, during the ZTP installation performs these checks if the flags are not explicitly mentioned in the configuration file.

***create_ztp_image.sh* script creation**

```
#!/bin/bash
#####
# This script is used to generate ise ztp image with ztp
# configuration file.
#
# Need to pass ztp configuration file as input.
#
# Copyright (c) 2021 by Cisco Systems, Inc.
# All rights reserved.
# Note:
# To mount the image use below command
# mount ise_ztp_config.img /ztp
# To mount the image from cdrom
# mount -o ro /dev/sr1 /ztp
#####
if [ -z "$1" ];then
echo "Usage:$0 <ise-ztp.conf> [out-ztp.img]"
exit 1
elif [ ! -f $1 ];then
echo "file $1 not exist"
exit 1
else
conf_file=$1
fi
if [ -z "$2" ] ;then
image=ise_config.img
else
image=$2
fi
mountpath=/tmp/ise_ztp
ztplabel=ISE-ZTP
rm -fr $mountpath
mkdir -p $mountpath
dd if=/dev/zero of=$image bs=1k count=1440 > /dev/null 2>&1
if [ `echo $?` -ne 0 ];then
echo "Image creation failed\n"
exit 1
fi
mkfs.ext4 $image -L $ztplabel -F > /dev/null 2>&1
mount -o rw,loop $image $mountpath
cp $conf_file $mountpath/ise-ztp.conf
sync
umount $mountpath
sleep 1
# Check for automount and unmount
automountpath=$(mount | grep $ztplabel | awk '{print $3}')
if [ -n "$automountpath" ];then
umount $automountpath
fi
echo "Image created $image"
```

VM User Data

You can use VM user data with Cisco ISE installation on ESXi version 6.5 and later.

Paste the contents that are in the **ise-ztp.conf** file into the Base64 encode tool. Use the [base64encode tool](#) to obtain the encoded string.

Enter the encoded Base64 string in the VM with the VM user data. In VMware ESXi, go to **VM Options > Advanced > Configuration Parameters > Edit Configuration > guestinfo.ise.ztp = [Value] Base Encoded ZTP Configuration** with the Base Encoded ZTP Configuration string.



Note When configuring ZTP to deploy a patch or hot patch, you must use http (lowercase) instead of HTTP. Otherwise, the patch files cannot be downloaded from the repository.



CHAPTER 5

Installation Verification and Post-Installation Tasks

- [Log in to the Cisco ISE web-based interface, on page 99](#)
- [Cisco ISE configuration verification, on page 101](#)
- [List of post-installation tasks, on page 103](#)

Log in to the Cisco ISE web-based interface

When you log in to the Cisco ISE web-based interface for the first time, you use the preinstalled Evaluation license.

Procedure

- Step 1** After the Cisco ISE appliance finishes rebooting, launch one of the supported web browsers.
For information about validated browsers, refer to the “Validated Browsers” section in the [Cisco ISE Release Notes](#).
- Step 2** In the **Address** field, enter the IP address or hostname of the Cisco ISE appliance in this format, then press **Enter**.
`https://<IP address or host name>/admin/`
- Step 3** Enter your username and password.
- Step 4** Click **Login**.
-



Note

- For security, log out when you complete your administrative session. If you do not log out, Cisco ISE logs you out after 30 minutes of inactivity and does not save any unsubmitted configuration data.
 - If Cisco ISE is installed in the cloud or using the ZTP process, you will be prompted to change the web-based admin user password during the first login.
-

Differences between CLI admin and web-based admin user tasks

Use the username and password you set during Cisco ISE setup for administrative access to the CLI and the web interface.

The administrator with access to the Cisco ISE CLI is called the CLI-admin user. By default, the CLI-admin username is admin. The administrator must create the password during the setup process, as Cisco ISE does not provide a default password.

You can initially access the Cisco ISE web interface by using the CLI-admin username and password that you defined during setup. A web-based admin user does not have a default username or password.

Cisco ISE copies the CLI-admin user to the web-based admin user database. Only the first CLI-admin user is copied as the web-based admin user. Ensure that the CLI and web-based administrator user stores remain synchronized. Using the same username and password for both roles simplifies administration.

The CLI-admin user has different rights and capabilities than the web-based admin user and can perform additional administrative tasks.

Table 15: Tasks performed by CLI-admin and web-based admin users

Admin user type	Tasks
Both CLI-admin and web-based admin	<ul style="list-style-type: none"> • Back up Cisco ISE application data • Display any system, application, or diagnostic logs on the Cisco ISE appliance • Apply Cisco ISE software patches, maintenance releases, and upgrades • Set the NTP server configuration
CLI-admin only	<ul style="list-style-type: none"> • Start and stop Cisco ISE application software • Reload or shut down the Cisco ISE appliance • Reset the web-based admin user in case of a lockout • Access Cisco ISE CLI

Create a CLI admin

You can create additional CLI-admin user accounts after you complete the setup process. To keep your account secure, create only the number of CLI-admin users you need for Cisco ISE CLI access. This method helps you protect your credentials.


You can add a CLI-admin user with this command in configuration mode:

```
username <username> password [plain/hash] <password> role admin
```

Create a web-based admin

To access Cisco ISE through the web interface initially, use the administrator username and password configured during CLI setup.


To add an administrator user, perform these steps:

1. In the Cisco ISE GUI, click the **Menu** icon () and choose **Administration > System > Admin Access > Administrators > Admin Users**.
2. Choose **Add > Create an Admin User**.
3. Add web-based administrator users using the user interface.
4. Click **Submit**.

Reset a disabled password due to administrator logout

If you enter an incorrect password five times, your account becomes disabled.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. Resetting the administrator password activates new credentials immediately and allows you to log in without rebooting the system. This process does not affect the administrator's CLI password.

Cisco ISE adds a log entry in the **Administrator Logins** window. To view this window, click the **Menu** icon () and choose **Operations > Reports > Reports > Audit > Administrator Logins**. Reset your administrator ID password to regain access to your credentials.

Procedure

Step 1 Access the direct-console CLI and enter:

```
application reset-passwd ise administrator_ID
```

Step 2 Specify and confirm a new password that is different from the passwords that were used most recently for this administrator ID.

```
Enter new password:  
Confirm new password:  
  
Password reset successfully
```

Cisco ISE configuration verification

You can verify the Cisco ISE configuration using a web browser or the CLI. Each method requires a different set of username and password credentials.



Note The CLI administrator user credentials and the web-based administrator user credentials are different in Cisco ISE.

Verify configuration using a web browser

Follow these steps to verify the configuration using a web browser:

Procedure

-
- Step 1** After the Cisco ISE appliance reboots, open a supported web browser.
 - Step 2** In the **Address** field, enter the IP address or host name of the Cisco ISE appliance using this format, and press **Enter**.
 - Step 3** On the Cisco ISE Login page, enter the username and password you created during setup. Click **Login**.

For example, enter `https://192.0.2.10/admin/`. The Cisco ISE Login page appears.

```
https://<IP address or host name>/admin/
```

Note

For first-time access to the Cisco ISE system using a web browser, the administrator username and password are the same as the credentials you configured for command-line interface access during setup.

- Step 4** Use the Cisco ISE dashboard to verify that the appliance is working correctly.
-

What to do next

Use the Cisco ISE web-based interface menus and options to configure the system to suit your needs. For details on configuring Cisco ISE, refer to [Cisco Identity Services Engine Administrator Guide](#).

Verify configuration using the CLI

Follow these steps to verify the configuration using the CLI:

Before you begin

Download and install the latest [Cisco ISE patch](#) to keep Cisco ISE appliance up to date.

Procedure

-
- Step 1** After your Cisco ISE appliance reboots, open a supported application, such as PuTTY, to connect to your Cisco ISE appliance using Secure Shell (SSH).
 - Step 2** In the **Host Name or IP Address** field, enter the hostname or IP address (in dotted decimal format) for your Cisco ISE appliance, and click **Open**.
 - Step 3** At the login prompt, enter the CLI-admin username you created during setup. The default user name is admin. Press **Enter**.
 - Step 4** At the password prompt, enter the CLI-admin password you created during setup. Press **Enter**.
 - Step 5** At the system prompt, enter **show application version ise** and press **Enter**.
 - Step 6** To check the status of the Cisco ISE processes, enter **show application status ise** and press **Enter**.

The console output appears as shown:

```
ise-server/admin# show application status ise
```

```

ISE PROCESS NAME                STATE                PROCESS ID
-----
Database Listener                running             4930
Database Server                  running             66 PROCESSES
Application Server                running             8231
Profiler Database                running             6022
ISE Indexing Engine              running             8634
AD Connector                      running             9485
M&T Session Database             running             3059
M&T Log Collector                running             9271
M&T Log Processor                running             9129
Certificate Authority Service     running             8968
EST Service                       running             18887
SXP Engine Service                disabled
TC-NAC Docker Service            disabled
TC-NAC MongoDB Container         disabled
TC-NAC RabbitMQ Container        disabled
TC-NAC Core Engine Container     disabled
VA Database                       disabled
VA Service                       disabled
pxGrid Infrastructure Service     disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager        disabled
pxGrid Controller                disabled
PassiveID Service                disabled
DHCP Server (dhcpd)              disabled
DNS Server (named)               disabled

```

List of post-installation tasks

After you install Cisco ISE, you must perform these mandatory tasks:

Table 16: Mandatory post-installation tasks

Task	Link in the Administration Guide
Apply the latest patches, if any	Refer to the "Software Patch Installation Guidelines" in the "Maintain and Monitor" chapter of the <i>Cisco ISE Administrator Guide</i> for your release.
Install licenses	Refer to the Cisco ISE Licensing Guide for more information. See the chapter "Licensing" in the <i>Cisco ISE Administrator Guide</i> for your release.
Install certificates	Refer to the section "Certificate Management in Cisco ISE" in the chapter "Basic Setup" in the <i>Cisco ISE Administrator Guide</i> for your release.
Create repository for backups	Refer to "Create Repositories" in the "Maintain and Monitor" chapter of the <i>Cisco ISE Administrator Guide</i> for your release

List of post-installation tasks

Task	Link in the Administration Guide
Configure backup schedules	Refer to "Schedule a Backup" in the "Maintain and Monitor" chapter of the <i>Cisco ISE Administrator Guide</i> for your release.
Deploy Cisco ISE personas	Refer to the section "Cisco ISE Distributed Deployment" in the chapter "Deployment" in the <i>Cisco ISE Administrator Guide</i> for your release.



CHAPTER 6

Common System Maintenance Tasks

- [Bond ethernet interfaces for high availability, on page 105](#)
- [Reset a lost, forgotten, or compromised password using a DVD, on page 110](#)
- [Reset a disabled password due to administrator lockout, on page 111](#)
- [Change the IP address of a Cisco ISE appliance, on page 111](#)
- [View installation and upgrade history, on page 112](#)
- [Perform a system erase, on page 113](#)

Bond ethernet interfaces for high availability

Cisco ISE supports bonding two ethernet interfaces into a single virtual interface, providing high availability for the physical interfaces. This feature is called Network Interface Card (NIC) bonding or NIC teaming. When two interfaces are bonded, they appear as a single device with one MAC address.

You can use NIC bonding in Cisco ISE only for high availability. It does not support load balancing or link aggregation.

Bonding interfaces ensures that the Cisco ISE services are not affected by:

- Physical interface failure
- Loss of switch port connectivity due to shutdown or failure
- Switch line card failure

When two interfaces are bonded, one becomes the primary interface and the other becomes the backup interface. All traffic flows through the primary interface. If the primary interface fails, the backup interface then routes all traffic. The bond uses the IP address and MAC address of the primary interface.

When you configure the NIC bonding feature, Cisco ISE pairs fixed physical NICs into bonded NICs. The table lists the NIC pairs that can form a bonded interface.

Table 17: Physical NICs bonded together to form an interface

Cisco ISE physical NIC name	Linux physical NIC name	Role in bonded NIC	Bonded NIC name
Gigabit Ethernet 0	Eth0	Primary	bond 0
Gigabit Ethernet 1	Eth1	Backup	

Cisco ISE physical NIC name	Linux physical NIC name	Role in bonded NIC	Bonded NIC name
Gigabit Ethernet 2	Eth2	Primary	bond 1
Gigabit Ethernet 3	Eth3	Backup	
Gigabit Ethernet 4	Eth4	Primary	bond 2
Gigabit Ethernet 5	Eth5	Backup	

Supported platforms

You can use the NIC bonding feature on all supported platforms and node personas. The supported platforms are:

- SNS hardware appliances—bond 0, 1, and 2.
- You can configure bond 0, 1, and 2 on virtual machines if six NICs are available.

Guidelines for bonding ethernet interfaces

- As Cisco ISE supports up to six Ethernet interfaces, it can have only three bonds, bond 0, bond 1, and bond 2.
- You cannot change the interfaces that are part of a bond or change the role of the interface in a bond. See the above table for information on which NICs can be bonded together and their role in the bond.
- The Eth0 interface acts as both the management interface as well as the runtime interface. The other interfaces act as runtime interfaces.
- Before you create a bond, the primary interface (primary NIC) must be assigned an IP address. The Eth0 interface must be assigned an IPv4 address before you create bond 0. Similarly, before you create bond 1 and 2, Eth2 and Eth4 interfaces must be assigned an IPv4 or IPv6 address, respectively.
- Before you create a bond, if the backup interface (Eth1, Eth3, and Eth5) has an IP address assigned, remove the IP address from the backup interface. The backup interface should not be assigned an IP address.
- You can choose to create only one bond (bond 0) and allow the rest of the interfaces to remain as is. In this case, bond 0 acts as the management interface and runtime interface, and the rest of the interfaces act as runtime interfaces.
- You can change the IP address of the primary interface in a bond. The new IP address is assigned to the bonded interface because it assumes the IP address of the primary interface.
- When you remove the bond between two interfaces, the IP address assigned to the bonded interface is assigned back to the primary interface.
- If you want to configure the NIC bonding feature on a Cisco ISE node that is part of a deployment, you must deregister the node from the deployment, configure NIC bonding, and then register the node back to the deployment.

- If a physical interface that acts as a primary interface in a bond (Eth0, Eth2, or Eth4 interface) has static route configured, the static routes are automatically updated to operate on the bonded interface instead of the physical interface.

Configure NIC bonding

You can configure NIC bonding from the Cisco ISE CLI for bond 0 between Eth0 and Eth1 interfaces.

Before you begin

If a physical interface, such as Eth1, Eth3, or Eth5, serves as a backup and is configured with an IP address, remove the IP address from that interface. Leave the backup interface without an IP address.

Procedure

- Step 1** Log in to Cisco ISE CLI with your administrator account.
- Step 2** Enter **configure terminal** to enter the configuration mode.
- Step 3** Enter the **interface GigabitEthernet 0** command.
- Step 4** Enter the **backup interface GigabitEthernet 1** command.
The console displays:

```
% Warning: IP address of interface eth1 will be removed once NIC bonding is enabled. Are you sure you want to proceed? Y/N [N]:
```

- Step 5** Enter **Y** and press **Enter**.

After you configure bond 0, Cisco ISE restarts automatically. Wait until all services are running. Enter the **show application status ise** command from the CLI to check whether all services are running.

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# backup interface gigabitEthernet 1
Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
```

```

Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin(config-GigabitEthernet)#

```

Verify NIC bonding configuration

To verify if NIC bonding feature is configured, run the **show running-config** command from the Cisco ISE CLI. You will see an output similar to this example:

```

!
interface GigabitEthernet 0
  ipv6 address autoconfig
  ipv6 enable
  backup interface GigabitEthernet 1
  ip address 192.168.118.214 255.255.255.0
!

```

In the output, the entry "backup interface GigabitEthernet 1" indicates that NIC bonding is configured on Gigabit Ethernet 0. Gigabit Ethernet 0 is the primary interface, and Gigabit Ethernet 1 is the backup interface. The ADE-OS configuration does not display an IP address for the backup interface in the running configuration. The same IP address is used for both the primary and backup interfaces.

You can also run the **show interface** command to see the bonded interfaces.

```

ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,PRIMARY,MULTICAST> mtu 1500
  inet 10.126.107.60 netmask 255.255.255.0 broadcast 10.126.107.255
  inet6 fe80::8a5a:92ff:fe88:4aea prefixlen 64 scopeid 0x20<link>
  ether 88:5a:92:88:4a:ea txqueuelen 0 (Ethernet)
  RX packets 1726027 bytes 307336369 (293.0 MiB)
  RX errors 0 dropped 844 overruns 0 frame 0
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

GigabitEthernet 0
  flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST> mtu 1500
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)
  RX packets 1726027 bytes 307336369 (293.0 MiB)
  RX errors 0 dropped 844 overruns 0 frame 0
  TX packets 1295620 bytes 1073397536 (1023.6 MiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  device memory 0xfab00000-fabfffff

GigabitEthernet 1
  flags=6211<UP,BROADCAST,RUNNING,SUBORDINATE,MULTICAST> mtu 1500
  ether 88:5a:92:88:4a:ea txqueuelen 1000 (Ethernet)
  RX packets 0 bytes 0 (0.0 B)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 0 bytes 0 (0.0 B)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

```
device memory 0xfaa00000-faafffff
```

Remove NIC bonding

Use the **no** form of the **backup interface** command to remove a NIC bond.

Before you begin

Procedure

- Step 1** Log in to Cisco ISE CLI with your administrator account.
- Step 2** Enter **configure terminal** to enter the configuration mode.
- Step 3** Enter the **interface GigabitEthernet 0** command.
- Step 4** Enter the **no backup interface GigabitEthernet 1** command.

```
% Notice: Bonded Interface bond 0 has been removed.
```

- Step 5** Enter **Y** and press Enter.

Bond 0 is now removed. Cisco ISE restarts automatically. Wait until all services are running successfully. Enter the **show application status ise** command from the CLI to verify that all the services are running.

```
ise/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ise/admin(config)# interface gigabitEthernet 0
ise/admin(config-GigabitEthernet)# no backup interface gigabitEthernet 1

Changing backup interface configuration may cause ISE services to restart.
Are you sure you want to proceed? Y/N [N]: Y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
ISE PassiveID Service is disabled
ISE pxGrid processes are disabled
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE EST Service...
ISE Sxp Engine Service is disabled
Stopping ISE Profiler Database...
Stopping ISE Indexing Engine...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE Application Server...
Starting ISE Indexing Engine...
Starting ISE Certificate Authority Service...
Starting ISE EST Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
```

```
ise/admin(config-GigabitEthernet)#
```

Reset a lost, forgotten, or compromised password using a DVD

Before you begin

Understand these connection-related conditions that can cause problems when you use the Cisco ISE software DVD to start device.

- If your terminal server associated with the serial console connection to the Cisco ISE appliance is set to `exec`, only one connection method is available. After you set it to `no exec`, you can use both a keyboard and video monitor connection and a serial console connection.
- If you have a keyboard and video monitor connection to the Cisco ISE appliance, you can use a remote keyboard and video monitor connection or a VMware vSphere client console connection.
- Ensure you have a serial console connection to the Cisco ISE appliance.

Procedure

Step 1 Ensure that the Cisco ISE device is powered up.

Step 2 Insert the Cisco ISE software DVD.

Step 3 Use the arrow keys to select **System Utilities (Serial Console)** if you use a local serial console port connection or select **System Utilities (Keyboard/Monitor)** if you use a keyboard and video monitor connection to the appliance, and press **Enter**.

The system displays the ISO uses menu as shown here.

```
Available System Utilities:
[1] Recover Administrator Password
[2] Virtual Machine Resource Check
[3] Perform System Erase
[q] Quit and reload
Enter option [1 - 3] q to Quit:
```

Step 4 Enter **1** to recover the administrator password.

The console displays:

```
Admin Password Recovery
This utility will reset the password for the specified ADE-OS administrator.
At most the first five administrators will be listed. To cancel without
saving changes, enter [q] to Quit and return to the utilities menu.

[1]:admin
[2]:admin2
[3]:admin3
[4]:admin4

Enter choice between [1 - 4] or q to Quit: 2
```

```
Password:
Verify password:


Save change and reboot? [Y/N]:
```

- Step 5** Enter the number for the admin user whose password you want to reset.
- Step 6** Enter the new password and verify it.
- Step 7** Enter **Y** to save the changes.
-

Reset a disabled password due to administrator lockout

If you enter an incorrect password five times, your account becomes disabled.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. Resetting the administrator password activates new credentials immediately and allows you to log in without rebooting the system. This process does not affect the administrator's CLI password.

Cisco ISE adds a log entry in the **Administrator Logins** window. To view this window, click the **Menu** icon () and choose **Operations > Reports > Reports > Audit > Administrator Logins**. Reset your administrator ID password to regain access to your credentials.

Procedure

- Step 1** Access the direct-console CLI and enter:
- ```
application reset-passwd ise administrator_ID
```
- Step 2** Specify and confirm a new password that is different from the passwords that were used most recently for this administrator ID.

```
Enter new password:
Confirm new password:

Password reset successfully
```

---

## Change the IP address of a Cisco ISE appliance

### Before you begin

- Deregister your Cisco ISE node from the distributed deployment. Then, convert it to a standalone node before you change the IP address
- Do not use the **no ip address** command when changing the Cisco ISE device's IP address.

## Procedure

---

**Step 1** Log in to the Cisco ISE CLI.

**Step 2** Enter these commands:

- a) **configure terminal**
- b) **interface GigabitEthernet 0**
- c) **ip address new\_ip\_address new\_subnet\_mask**

When prompted for the IP address change, enter **Y**. A similar screen appears.

```
ise-13-infra-2/admin(config-GigabitEthernet)# ip address a.b.c.d 255.255.255.0
```

```
% Changing the IP address might cause ISE services to restart
Continue with IP address change? Y/N [N]: y
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Identity Mapping Service...
Stopping ISE pxGrid processes...
Stopping ISE Application Server...
Stopping ISE Certificate Authority Service...
Stopping ISE Profiler Database...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE AD Connector...
Stopping ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Profiler Database...
Starting ISE pxGrid processes...
Starting ISE Application Server...
Starting ISE Certificate Authority Service...
Starting ISE Monitoring & Troubleshooting Log Processor...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Identity Mapping Service...
Starting ISE AD Connector...
Note: ISE Processes are initializing. Use 'show application status ise'
CLI to verify all processes are in running state.
```

When the process is complete, restart the system when prompted.

**Step 3** To restart the system, enter **Y**.

---

## View installation and upgrade history

You can use a CLI command in Cisco ISE to view the details of installing, upgrading, and uninstalling releases and patches. To view these details, enter the **show version history** command.

- **Date:** Indicates date and time at which the installation or uninstallation was performed.
- **Application:** The Cisco ISE application used for installation or upgrade.
- **Version:** Version that was installed or removed.
- **Action:** Installation, uninstallation, patch installation, or patch uninstallation.

- **Bundle Filename:** Specifies the name of the bundle that was installed or removed.
- **Repository:** The repository you used to install the Cisco ISE application bundle. This does not apply if you uninstall the application..

### Procedure

---

**Step 1** Log in to the Cisco ISE CLI.

**Step 2** Enter this command: **show version history**.

This output appears:

```
ise/admin# show version history

Install Date: Fri Nov 30 21:48:58 UTC 2022
Application: ise
Version: 3.x.0.xxx
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

---

## Perform a system erase

You can securely erase all information from your Cisco ISE appliance or VM by performing a system erase. This method helps you comply with NIST Special Publication 800-88 data destruction standards.

This method ensures Cisco ISE compliance with NIST Special Publication 800-88 data destruction standards.

### Before you begin

Understand these connection-related conditions that may cause problems when you use the Cisco ISE software DVD to start a Cisco ISE appliance:

- If your terminal server is associated with the serial console connection to the Cisco ISE appliance and is set to `exec`, change the setting to `no exec`. This change allows you to use both a KVM connection and a serial console connection.
- Set up a keyboard and video monitor (KVM) connection to the Cisco ISE appliance. Use either a remote KVM connection or a VMware vSphere client console connection.
- Set up a serial console connection to the Cisco ISE appliance.

### Procedure

---

**Step 1** Ensure that the Cisco ISE device is powered up.

**Perform a system erase**

**Step 2** Insert the Cisco ISE software DVD.

**Step 3** Use the arrow keys to select **System Utilities (Serial Console)**, and press Enter.

The system displays the ISO utilities menu as shown here:

```
Available System Utilities:
```

```
[1] Recover administrator password
[2] Virtual Machine Resource Check
[3] System Erase
[q] Quit and reload
```

```
Enter option [1 - 3] q to Quit:
```

**Step 4** Enter **3** to perform a system erase.

The console displays:

```
***** W A R N I N G *****
THIS UTILITY WILL PERFORM A SYSTEM ERASE ON THE DISK DEVICE(S). THIS PROCESS CAN TAKE UP TO 5 HOURS
TO COMPLETE. THE RESULT WILL BE COMPLETE
DATA LOSS OF THE HARD DISK. THE SYSTEM WILL NO LONGER BOOT AND WILL REQUIRE A RE-IMAGE FROM INSTALL
MEDIA TO RESTORE TO FACTORY DEFAULT STATE.
```

```
ARE YOU SURE YOU WANT TO CONTINUE? [Y/N] Y
```

**Step 5** Enter **Y**.

The console prompts with another warning:

```
THIS IS YOUR LAST CHANGE TO CANCEL. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

**Step 6** Enter **Y** to perform a system erase.

The console displays:

```
Deleting system disk, please wait...
Writing random data to all sectors of disk device (/dev/sda)...
Writing zeros to all sectors of disk device (/dev/sda)...
Completed! System is now erased.
Press <Enter> to reboot.
```

To reuse the appliance after performing a system erase, boot the system using the Cisco ISE DVD and choose the install option from the boot menu.

---



# CHAPTER 7

## Cisco ISE Ports Reference

- Cisco ISE all persona nodes ports, on page 115
- Cisco ISE infrastructure requirements, on page 116
- Operating system ports, on page 117
- Cisco ISE administration node ports, on page 120
- Cisco ISE monitoring node ports, on page 122
- Cisco ISE policy service node ports, on page 124
- Cisco pxGrid service ports, on page 128
- OCSP and CRL service ports, on page 128
- Cisco ISE processes, on page 129
- Required internet URLs, on page 129

### Cisco ISE all persona nodes ports

This table shows the ports used by all Cisco ISE nodes.

**Table 18: Ports used by all Cisco ISE nodes**

| Cisco ISE service               | Ports on Gigabit Ethernet 0 or on Bond 0                                                                                                                                                                                                                                                                                                                                                              | Ports on other Ethernet interfaces (Gigabit Ethernet 1–5 or Bond 1 and Bond 2) |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Replication and synchronization | <ul style="list-style-type: none"> <li>• HTTPS (SOAP) protocol: TCP port 443</li> <li>• Data synchronization and replication (JGroups) protocol uses TCP port 12001 (Global)</li> <li>• Cisco ISE messaging service - SSL: TCP port 8671</li> <li>• Cisco ISE internal communication: TCP port 15672</li> <li>• Profiler endpoint ownership synchronization and replication: TCP port 6379</li> </ul> | Not applicable                                                                 |

The TCP keepalive interval on Cisco ISE is 60 minutes. If a firewall is deployed between Cisco ISE nodes, configure firewall TCP timeout values accordingly.

## Cisco ISE infrastructure requirements

This section describes the infrastructure requirements and design considerations for deploying Cisco ISE. It outlines management access restrictions, network interface limitations, port and firewall requirements, and supported deployment models to help ensure proper connectivity, policy enforcement, and Cisco ISE operation.

### Management interface requirements

Management access to Cisco ISE is restricted to the management interface.

- Management access is allowed only through Gigabit Ethernet 0.
- Administrative access includes the web-based GUI, CLI, and APIs.
- Other network interfaces are not used for management access.

### Network interface and VLAN requirements

- Cisco ISE interfaces do not support VLAN tagging.
- Switch ports connected to Cisco ISE nodes must be configured as access ports.
- VLAN trunking must be disabled.
- Each network interface card (NIC) can be assigned a unique IP address.

### Ports and firewall requirements

Cisco ISE uses a restricted port model and opens only the ports required by enabled services.

- Ports not explicitly required by active services are denied by default.
- The ephemeral port range used by Cisco ISE is 10000–65500.
- Firewalls must allow required service ports and the ephemeral port range.

### RADIUS traffic handling

- RADIUS authentication and accounting traffic is accepted on all available NICs.
- RADIUS traffic is not limited to the management interface.

### Cloud and virtual deployment requirements

- VMware on Cloud deployments are supported.
- Connectivity must be provided using a site-to-site VPN.
- Network address translation (NAT) and port filtering are not supported between Cisco ISE nodes and network access devices.

# Operating system ports

This table lists the TCP ports that NMAP uses for OS scanning. NMAP also uses ICMP and UDP port 51824.

**Table 19: Operating system ports**

|      |      |      |      |      |      |      |      |           |
|------|------|------|------|------|------|------|------|-----------|
| 1    | 3    | 4    | 6    | 7    | 9    | 13   | 17   | 19        |
| 20   | 21   | 22   | 23   | 24   | 25   | 26   | 30   | 32        |
| 33   | 37   | 42   | 43   | 49   | 53   | 70   | 79   | 80        |
| 81   | 82   | 83   | 84   | 85   | 88   | 89   | 90   | 99        |
| 100  | 106  | 109  | 110  | 111  | 113  | 119  | 125  | 135       |
| 139  | 143  | 144  | 146  | 161  | 163  | 179  | 199  | 211       |
| 212  | 222  | 254  | 255  | 256  | 259  | 264  | 280  | 301       |
| 306  | 311  | 340  | 366  | 389  | 406  | 407  | 416  | 417       |
| 425  | 427  | 443  | 444  | 445  | 458  | 464  | 465  | 481       |
| 497  | 500  | 512  | 513  | 514  | 515  | 524  | 541  | 543       |
| 544  | 545  | 548  | 554  | 555  | 563  | 587  | 593  | 616       |
| 617  | 625  | 631  | 636  | 646  | 648  | 666  | 667  | 668       |
| 683  | 687  | 691  | 700  | 705  | 711  | 714  | 720  | 722       |
| 726  | 749  | 765  | 777  | 783  | 787  | 800  | 801  | 808       |
| 843  | 873  | 880  | 888  | 898  | 900  | 901  | 902  | 903       |
| 911  | 912  | 981  | 987  | 990  | 992  | 993  | 995  | 999       |
| 1000 | 1001 | 1002 | 1007 | 1009 | 1010 | 1011 | 1021 | 1022      |
| 1023 | 1024 | 1025 | 1026 | 1027 | 1028 | 1029 | 1030 | 1031      |
| 1032 | 1033 | 1034 | 1035 | 1036 | 1037 | 1038 | 1039 | 1040-1100 |
| 1102 | 1104 | 1105 | 1106 | 1107 | 1108 | 1110 | 1111 | 1112      |
| 1113 | 1114 | 1117 | 1119 | 1121 | 1122 | 1123 | 1124 | 1126      |
| 1130 | 1131 | 1132 | 1137 | 1138 | 1141 | 1145 | 1147 | 1148      |
| 1149 | 1151 | 1152 | 1154 | 1163 | 1164 | 1165 | 1166 | 1169      |
| 1174 | 1175 | 1183 | 1185 | 1186 | 1187 | 1192 | 1198 | 1199      |
| 1201 | 1213 | 1216 | 1217 | 1218 | 1233 | 1234 | 1236 | 1244      |

## Operating system ports

|      |           |      |      |           |           |           |           |           |
|------|-----------|------|------|-----------|-----------|-----------|-----------|-----------|
| 1247 | 1248      | 1259 | 1271 | 1272      | 1277      | 1287      | 1296      | 1300      |
| 1301 | 1309      | 1310 | 1311 | 1322      | 1328      | 1334      | 1352      | 1417      |
| 1433 | 1434      | 1443 | 1455 | 1461      | 1494      | 1500      | 1501      | 1503      |
| 1521 | 1524      | 1533 | 1556 | 1580      | 1583      | 1594      | 1600      | 1641      |
| 1658 | 1666      | 1687 | 1688 | 1700      | 1717      | 1718      | 1719      | 1720      |
| 1721 | 1723      | 1755 | 1761 | 1782      | 1783      | 1801      | 1805      | 1812      |
| 1839 | 1840      | 1862 | 1863 | 1864      | 1875      | 1900      | 1914      | 1935      |
| 1947 | 1971      | 1972 | 1974 | 1984      | 1998-2010 | 2013      | 2020      | 2021      |
| 2022 | 2030      | 2033 | 2034 | 2035      | 2038      | 2040-2043 | 2045-2049 | 2065      |
| 2068 | 2099      | 2100 | 2103 | 2105-2107 | 2111      | 2119      | 2121      | 2126      |
| 2135 | 2144      | 2160 | 2161 | 2170      | 2179      | 2190      | 2191      | 2196      |
| 2200 | 2222      | 2251 | 2260 | 2288      | 2301      | 2323      | 2366      | 2381-2383 |
| 2393 | 2394      | 2399 | 2401 | 2492      | 2500      | 2522      | 2525      | 2557      |
| 2601 | 2602      | 2604 | 2605 | 2607      | 2608      | 2638      | 2701      | 2702      |
| 2710 | 2717      | 2718 | 2725 | 2800      | 2809      | 2811      | 2869      | 2875      |
| 2909 | 2910      | 2920 | 2967 | 2968      | 2998      | 3000      | 3001      | 3003      |
| 3005 | 3006      | 3007 | 3011 | 3013      | 3017      | 3030      | 3031      | 3052      |
| 3071 | 3077      | 3128 | 3168 | 3211      | 3221      | 3260      | 3261      | 3268      |
| 3269 | 3283      | 3300 | 3301 | 3306      | 3322      | 3323      | 3324      | 3325      |
| 3333 | 3351      | 3367 | 3369 | 3370      | 3371      | 3372      | 3389      | 3390      |
| 3404 | 3476      | 3493 | 3517 | 3527      | 3546      | 3551      | 3580      | 3659      |
| 3689 | 3690      | 3703 | 3737 | 3766      | 3784      | 3800      | 3801      | 3809      |
| 3814 | 3826      | 3827 | 3828 | 3851      | 3869      | 3871      | 3878      | 3880      |
| 3889 | 3905      | 3914 | 3918 | 3920      | 3945      | 3971      | 3986      | 3995      |
| 3998 | 4000-4006 | 4045 | 4111 | 4125      | 4126      | 4129      | 4224      | 4242      |
| 4279 | 4321      | 4343 | 4443 | 4444      | 4445      | 4446      | 4449      | 4550      |
| 4567 | 4662      | 4848 | 4899 | 4900      | 4998      | 5000-5004 | 5009      | 5030      |
| 5033 | 5050      | 5051 | 5054 | 5060      | 5061      | 5080      | 5087      | 5100      |
| 5101 | 5102      | 5120 | 5190 | 5200      | 5214      | 5221      | 5222      | 5225      |

|           |           |           |       |       |       |       |       |       |
|-----------|-----------|-----------|-------|-------|-------|-------|-------|-------|
| 5226      | 5269      | 5280      | 5298  | 5357  | 5405  | 5414  | 5431  | 5432  |
| 5440      | 5500      | 5510      | 5544  | 5550  | 5555  | 5560  | 5566  | 5631  |
| 5633      | 5666      | 5678      | 5679  | 5718  | 5730  | 5800  | 5801  | 5802  |
| 5810      | 5811      | 5815      | 5822  | 5825  | 5850  | 5859  | 5862  | 5877  |
| 5900-5907 | 5910      | 5911      | 5915  | 5922  | 5925  | 5950  | 5952  | 5959  |
| 5960-5963 | 5987-5989 | 5998-6007 | 6009  | 6025  | 6059  | 6100  | 6101  | 6106  |
| 6112      | 6123      | 6129      | 6156  | 6346  | 6389  | 6502  | 6510  | 6543  |
| 6547      | 6565-6567 | 6580      | 6646  | 6666  | 6667  | 6668  | 6669  | 6689  |
| 6692      | 6699      | 6779      | 6788  | 6789  | 6792  | 6839  | 6881  | 6901  |
| 6969      | 7000      | 7001      | 7002  | 7004  | 7007  | 7019  | 7025  | 7070  |
| 7100      | 7103      | 7106      | 7200  | 7201  | 7402  | 7435  | 7443  | 7496  |
| 7512      | 7625      | 7627      | 7676  | 7741  | 7777  | 7778  | 7800  | 7911  |
| 7920      | 7921      | 7937      | 7938  | 7999  | 8000  | 8001  | 8002  | 8007  |
| 8008      | 8009      | 8010      | 8011  | 8021  | 8022  | 8031  | 8042  | 8045  |
| 8080-8090 | 8093      | 8099      | 8100  | 8180  | 8181  | 8192  | 8193  | 8194  |
| 8200      | 8222      | 8254      | 8290  | 8291  | 8292  | 8300  | 8333  | 8383  |
| 8400      | 8402      | 8443      | 8500  | 8600  | 8649  | 8651  | 8652  | 8654  |
| 8701      | 8800      | 8873      | 8888  | 8899  | 8994  | 9000  | 9001  | 9002  |
| 9003      | 9009      | 9010      | 9011  | 9040  | 9050  | 9071  | 9080  | 9081  |
| 9090      | 9091      | 9099      | 9100  | 9101  | 9102  | 9103  | 9110  | 9111  |
| 9200      | 9207      | 9220      | 9290  | 9415  | 9418  | 9485  | 9500  | 9502  |
| 9503      | 9535      | 9575      | 9593  | 9594  | 9595  | 9618  | 9666  | 9876  |
| 9877      | 9878      | 9898      | 9900  | 9917  | 9929  | 9943  | 9944  | 9968  |
| 9998      | 9999      | 10000     | 10001 | 10002 | 10003 | 10004 | 10009 | 10010 |
| 10012     | 10024     | 10025     | 10082 | 10180 | 10215 | 10243 | 10566 | 10616 |
| 10617     | 10621     | 10626     | 10628 | 10629 | 10778 | 11110 | 11111 | 11967 |
| 12000     | 12174     | 12265     | 12345 | 13456 | 13722 | 13782 | 13783 | 14000 |
| 14238     | 14441     | 14442     | 15000 | 15002 | 15003 | 15004 | 15660 | 15742 |
| 16000     | 16001     | 16012     | 16016 | 16018 | 16080 | 16113 | 16992 | 16993 |

|       |       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 17877 | 17988 | 18040 | 18101 | 18988 | 19101 | 19283 | 19315 | 19350 |
| 19780 | 19801 | 19842 | 20000 | 20005 | 20031 | 20221 | 20222 | 20828 |
| 21571 | 22939 | 23502 | 24444 | 24800 | 25734 | 25735 | 26214 | 27000 |
| 27352 | 27353 | 27355 | 27356 | 27715 | 28201 | 30000 | 30718 | 30951 |
| 31038 | 31337 | 32768 | 32769 | 32770 | 32771 | 32772 | 32773 | 32774 |
| 32775 | 32776 | 32777 | 32778 | 32779 | 32780 | 32781 | 32782 | 32783 |
| 32784 | 32785 | 33354 | 33899 | 34571 | 34572 | 34573 | 34601 | 35500 |
| 36869 | 38292 | 40193 | 40911 | 41511 | 42510 | 44176 | 44442 | 44443 |
| 44501 | 45100 | 48080 | 49152 | 49153 | 49154 | 49155 | 49156 | 49157 |
| 49158 | 49159 | 49160 | 49161 | 49163 | 49165 | 49167 | 49175 | 49176 |
| 49400 | 49999 | 50000 | 50001 | 50002 | 50003 | 50006 | 50300 | 50389 |
| 50500 | 50636 | 50800 | 51103 | 51493 | 52673 | 52822 | 52848 | 52869 |
| 54045 | 54328 | 55055 | 55056 | 55555 | 55600 | 56737 | 56738 | 57294 |
| 57797 | 58080 | 60020 | 60443 | 61532 | 61900 | 62078 | 63331 | 64623 |
| 64680 | 65000 | 65129 | 65389 |       |       |       |       |       |

## Cisco ISE administration node ports

This table shows the ports used by Cisco ISE administration nodes.

Table 20: Ports used by the administration nodes

| Cisco ISE service | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Ports on other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2) |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administration    | <ul style="list-style-type: none"> <li>• HTTPS: TCP/443</li> <li>• SSH Server: TCP/22</li> <li>• CoA</li> <li>• External RESTful Services (ERS)<br/>REST API: TCP/9060</li> </ul> <p>The ERS and OpenAPI services are HTTPS-only REST APIs and operate over port 443. Currently, ERS APIs also operate over port 9060. This port might not be supported for ERS APIs in later Cisco ISE releases. We recommend that you only use port 443 for ERS APIs. The default conn-limit value for port 9060 is 30. If consecutive ERS API calls are returning a HTTP 502 error, we recommend that you increase the conn-limit value of port 9060 to 60 using the command <b>conn-limit cl1 60 port 9060</b>.</p> <ul style="list-style-type: none"> <li>• External RESTful Services (ERS)<br/>REST API Certificate-based authentication for DNAC integration mode: TCP/9062</li> <li>• To manage guest accounts from Admin GUI: TCP/9002</li> <li>• Port 443 supports Admin web applications and is enabled by default.</li> </ul> <p>Access to Cisco ISE via HTTPS and SSH is restricted to Gigabit Ethernet 0.</p> <ul style="list-style-type: none"> <li>• For SAML admin login, Port 8443 of PSN should be reachable from the device where the admin is trying to do the SAML login.</li> </ul> | Not applicable                                                                     |
| Monitoring        | <ul style="list-style-type: none"> <li>• SNMP Query: UDP/161</li> </ul> <p>This port is route table dependent.</p> <ul style="list-style-type: none"> <li>• ICMP</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                    |

| Cisco ISE service                                  | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Ports on other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2) |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Logging (Outbound)                                 | <ul style="list-style-type: none"> <li>• Syslog: UDP/20514, TCP/1468</li> <li>• Secure Syslog: TCP/6514</li> </ul> <p style="margin-left: 20px;">Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> <li>• SNMP Traps: UDP/162</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |
| External identity sources and resources (Outbound) | <ul style="list-style-type: none"> <li>• Admin user interface and endpoint authentications:               <ul style="list-style-type: none"> <li>• LDAP: TCP/389, 3268, UDP/389</li> <li>• SMB: TCP/445</li> <li>• KDC: TCP/88</li> <li>• KPASS: TCP/464</li> </ul> </li> <li>• WMI : TCP/135</li> <li>• ODBC:               <p style="margin-left: 20px;">The ODBC ports are configurable on the third-party database server.</p> <ul style="list-style-type: none"> <li>• Microsoft SQL: TCP/1433</li> <li>• Sybase: TCP/2638</li> <li>• PostgreSQL: TCP/5432</li> <li>• Oracle: TCP/1521, TCPS/2484</li> </ul> </li> <li>• NTP: UDP/123 (localhost interfaces only)</li> <li>• DNS: UDP/53, TCP/53</li> <li>• For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.</li> <li>• Cisco ISE sends an ICMP ping to the configured DNS server when diagnosing connectivity for an Active Directory connection.</li> </ul> |                                                                                    |
| Email                                              | Guest account and user password expiration email notification: SMTP: TCP/25                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                    |
| Smart licensing                                    | <ul style="list-style-type: none"> <li>• Connection to Cisco cloud over TCP/443</li> <li>• Connection to SSM on-premises server over TCP/443 and ICMP</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                    |

## Cisco ISE monitoring node ports

Use this table to find the ports used by Cisco ISE nodes with the monitoring persona.

Table 21: Ports used by monitoring nodes

| Cisco ISE service                                  | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Ports on other Ethernet interfaces (Gigabit Ethernet 1 to 5, or Bond 1 and Bond 2) |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Administration                                     | <ul style="list-style-type: none"> <li>• HTTPS uses TCP port 443</li> <li>• SSH Server uses TCP port 22</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Not applicable                                                                     |
| Monitoring                                         | <ul style="list-style-type: none"> <li>• Simple Network Management Protocol (SNMP): SNMP uses UDP port 161. This port is route-table-dependent.</li> <li>• ICMP</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                    |
| Logging                                            | <ul style="list-style-type: none"> <li>• Syslog uses UDP port 20514 and TCP port 1468</li> <li>• Secure Syslog uses TCP port 6514</li> </ul> <p>Default ports are configurable for external logging.</p> <ul style="list-style-type: none"> <li>• SMTP uses TCP port 25 for email of alarms</li> <li>• SNMP traps use UDP port 162</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                    |
| External identity sources and resources (Outbound) | <ul style="list-style-type: none"> <li>• Admin user interface and endpoint authentications: <ul style="list-style-type: none"> <li>• LDAP uses TCP ports 389 and 3268, and UDP port 389</li> <li>• SMB uses TCP port 445</li> <li>• KDC uses TCP port 88 and UDP port 88</li> <li>• KPASS uses TCP port 464</li> </ul> </li> <li>• WMI uses TCP port 135</li> <li>• ODBC: <p>The ODBC ports are configurable on the third-party database server.</p> <ul style="list-style-type: none"> <li>• Microsoft SQL uses TCP port 1433</li> <li>• Sybase uses TCP port 2638</li> <li>• PostgreSQL uses TCP port 5432</li> <li>• Oracle uses TCP ports 1521, 15723, and 16820</li> </ul> </li> <li>• NTP uses UDP port 123 (localhost interfaces only)</li> <li>• DNS uses UDP port 53 and TCP port 53</li> </ul> <p>For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.</p> |                                                                                    |

| Cisco ISE service                    | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Ports on other Ethernet interfaces (Gigabit Ethernet 1 to 5, or Bond 1 and Bond 2) |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Ports used for inbound communication | <p>These ports are required in all types of deployments regardless of being on-premises or in the cloud.</p> <ul style="list-style-type: none"> <li>• MnT node REST APIs: TCP 9443. This allows inbound API requests for monitoring and troubleshooting.</li> <li>• Policy Administration Node (PAN) to MnT: TCP 1521. This enables communication from the PAN to MnT nodes.</li> <li>• OpenAPIs: TCP 443, TCP 9070. These provide access to OpenAPI interfaces for integration.</li> <li>• ERS APIs: TCP 443, TCP 9060. These ports facilitate inbound API requests through ERS interfaces.</li> </ul> |                                                                                    |
| Bulk download for pxGrid             | TCP ports 9993, 2000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                    |

## Cisco ISE policy service node ports

Cisco ISE supports HTTP Strict Transport Security (HSTS) to enhance communication security. When enabled, Cisco ISE includes an HSTS header in its HTTPS responses, instructing browsers to interact with the server exclusively over HTTPS. If a user attempts to access Cisco ISE via HTTP, the browser automatically upgrades the connection to HTTPS before transmitting any data. This process prevents unencrypted communication and eliminates the need for server-side redirects.

This table provides a list of ports used by the PSNs.

**Table 22: Ports used by the policy service nodes**

| Cisco ISE service       | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                     | Ports on other Ethernet interfaces, or Bond 1, and Bond 2  |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| Administration          | <ul style="list-style-type: none"> <li>• HTTPS: TCP port 443</li> <li>• SSH server: TCP port 22</li> <li>• OCSP: TCP port 2560</li> </ul> | You can manage the device only through Gigabit Ethernet 0. |
| Clustering (Node group) | Node groups or JGroups: TCP port 7800                                                                                                     | Not applicable                                             |
| SCEP                    | TCP port 9090                                                                                                                             | Not applicable                                             |
| IPsec or ISAKMP         | UDP port 500                                                                                                                              | Not applicable                                             |
| Device Administration   | TACACS+: TCP port 49                                                                                                                      |                                                            |
| TrustSec                | Use HTTP and Cisco ISE REST API to transfer TrustSec data to network devices over port 9063.                                              |                                                            |

| Cisco ISE service  | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                         | Ports on other Ethernet interfaces, or Bond 1, and Bond 2 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| SXP                | <ul style="list-style-type: none"> <li>• PSN (SXP node) to NADs: TCP port 64999</li> <li>• PSN to SXP (internal communication on the same Cisco ISE): TCP port 9644</li> </ul>                                                                                                                                                                                                                                                |                                                           |
| TC-NAC             | TCP port 443                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                           |
| Monitoring         | Simple Network Management Protocol (SNMP): UDP port 161. This port is route table dependent.                                                                                                                                                                                                                                                                                                                                  |                                                           |
| Logging (Outbound) | <ul style="list-style-type: none"> <li>• Syslog: UDP port 20514, TCP port 1468</li> <li>• Secure Syslog: TCP port 6514</li> </ul> <p>You can configure the default ports for external logging.</p> <ul style="list-style-type: none"> <li>• SNMP traps: UDP port 162</li> </ul>                                                                                                                                               |                                                           |
| Session            | <ul style="list-style-type: none"> <li>• RADIUS authentication: UDP ports 1645, 1812</li> <li>• RADIUS accounting: UDP ports 1646, 1813</li> <li>• RADIUS DTLS authentication and accounting: UDP ports 2083.</li> <li>• RADIUS Change of Authorization (CoA) send: UDP port 1700</li> <li>• RADIUS Change of Authorization (CoA) listen or relay: UDP ports 1700, 3799</li> </ul> <p>You cannot configure UDP port 3799.</p> |                                                           |

| Cisco ISE service                                                                                                                                                                                                                                                    | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Ports on other Ethernet interfaces, or Bond 1, and Bond 2 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| External identity sources and resources (Outbound)                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• Admin user interface and endpoint authentications:               <ul style="list-style-type: none"> <li>• LDAP: TCP ports 389, 3268</li> <li>• SMB: TCP port 445</li> <li>• KDC: TCP port 88</li> <li>• KPASS: TCP port 464</li> </ul> </li> <li>• WMI : TCP port 135</li> <li>• ODBC: The ODBC ports are configurable on the third-party database server.               <ul style="list-style-type: none"> <li>• Microsoft SQL: TCP port 1433</li> <li>• Sybase: TCP port 2638</li> <li>• PostgreSQL: TCP port 5432</li> <li>• Oracle: TCP port 1521</li> </ul> </li> <li>• NTP: UDP port 123 (localhost interfaces only)</li> <li>• DNS: UDP port 53, TCP port 53</li> </ul> <p>If an external identity source or service is accessible only through an interface other than Gigabit Ethernet 0, configure static routes for that interface.</p> |                                                           |
| Passive ID (Inbound)                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>• TS agent: TCP port 9094</li> <li>• AD agent: TCP port 9095</li> <li>• Syslog: UDP port 40514, TCP port 11468</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                           |
| Web portal services: <ul style="list-style-type: none"> <li>• Guest and web authentication</li> <li>• Guest sponsor portal</li> <li>• My devices portal</li> <li>• Client provisioning</li> <li>• Certificate provisioning</li> <li>• Blocked list portal</li> </ul> | HTTPS (Interface must be enabled for service in Cisco ISE): <ul style="list-style-type: none"> <li>• Blocked list portal: TCP port 8000-8999 (default port is TCP port 8444)</li> <li>• Guest portal and client provisioning: TCP port 8000-8999 (default port is TCP port 8443)</li> <li>• Certificate provisioning portal: TCP port 8000-8999 (default port is TCP port 8443)</li> <li>• My devices portal: TCP port 8000-8999 (default port is TCP port 8443)</li> <li>• Sponsor portal: TCP portal 8000-8999 (default port is TCP portal 8445)</li> <li>• SMTP guest notifications from guest and sponsor portals: TCP portal 25</li> </ul>                                                                                                                                                                                                                                             |                                                           |

| Cisco ISE service                                                                                                                                                      | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Ports on other Ethernet interfaces, or Bond 1, and Bond 2 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Posture <ul style="list-style-type: none"> <li>• Discovery</li> <li>• Provisioning</li> <li>• Assessment or heartbeat</li> </ul>                                       | <ul style="list-style-type: none"> <li>• Discovery (Client side): TCP port 8905 (HTTPS)</li> </ul> <p>Cisco ISE presents the admin certificate for Posture and client provisioning on TCP port 8905.</p> <p>Cisco ISE presents the portal certificate on TCP port 8443 (or the port that you have configured for portal use).</p> <p>From Cisco ISE release 3.1, port 8905 is disabled by default on non-PSNs. To enable this port, check the <b>Enable Port 8905 on non-Policy Service Nodes for Posture Services</b> check box in the <b>General Settings</b> window (<b>Administration &gt; System &gt; Settings &gt; Posture &gt; General Settings</b>).</p> <ul style="list-style-type: none"> <li>• Discovery (Policy Service Node side): TCP port 8443, 8905 (HTTPS) . This is configurable in the latest Cisco ISE release with Cisco Secure Client release 4.4 and later.</li> <li>• Assessment - Posture negotiation and agent reports: TCP port 8905 (HTTPS)</li> <li>• Bidirectional posture flow - TCP port 8000-8999 (default port is TCP port 8449)</li> </ul> |                                                           |
| Bring Your Own Device (BYOD) or Network Service Protocol (NSP) <ul style="list-style-type: none"> <li>• Redirection</li> <li>• Provisioning</li> <li>• SCEP</li> </ul> | <ul style="list-style-type: none"> <li>• Provisioning - URL redirection: See web portal services: Guest portal and client provisioning</li> <li>• For android devices with EST authentication: TCP port 8084. Port 8084 must be added to the redirect ACL for android devices.</li> <li>• Provisioning - Active-X and Java applet install (includes the launch of wizard install): See web portal services: Guest portal and client provisioning</li> <li>• Provisioning - Wizard install from Cisco ISE (Windows and Mac OS): TCP port 8443</li> <li>• Provisioning - Wizard install from Google Play (Android): TCP port 443</li> <li>• Provisioning - Supplicant provisioning process: TCP port 8905</li> <li>• SCEP proxy to CA: TCP port 443 (Based on SCEP RA URL configuration)</li> </ul>                                                                                                                                                                                                                                                                             |                                                           |
| Mobile Device Management (MDM) API integration                                                                                                                         | <ul style="list-style-type: none"> <li>• Provisioning - URL redirection: See web portal services: Guest portal and client provisioning</li> <li>• API: Vendor specific</li> <li>• Agent install and device registration: Vendor specific</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                           |

| Cisco ISE service | Ports on Gigabit Ethernet 0 or Bond 0                                                                                                                                                                                                                                                                                                                                                                         | Ports on other Ethernet interfaces, or Bond 1, and Bond 2 |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| Profiling         | <ul style="list-style-type: none"> <li>• NetFlow: UDP port 9996 can be configured</li> <li>• DHCP: UDP port 67 can be configured</li> <li>• DHCP SPAN Probe: UDP/68</li> <li>• HTTP: 8080</li> <li>• DNS: UDP port 53 (lookup). This port is route table dependent.</li> <li>• SNMP query: UDP port 161. This port is route table dependent.</li> <li>• SNMP trap: UDP port 162 can be configured.</li> </ul> |                                                           |

## Cisco pxGrid service ports

From Cisco ISE release 3.1, all pxGrid connections must use version 2.0. Integrations that rely on pxGrid version 1.0 (XMPP-based) are no longer operational. We recommend upgrading your other systems to Cisco pxGrid 2.0-compliant versions to avoid potential disruptions to integrations.

This table lists the ports used by Cisco pxGrid service nodes.

*Table 23: Ports used by Cisco pxGrid service nodes*

| Cisco ISE service        | Ports on Gigabit Ethernet 0 or Bond 0 | Ports on other Ethernet interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2) |
|--------------------------|---------------------------------------|-----------------------------------------------------------------------------------------|
| pxGrid subscribers       | TCP port 8910                         |                                                                                         |
| Inter-node communication | TCP port 8910                         |                                                                                         |

## OCSP and CRL service ports

The ports required for Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) services depend on the CA server or the service hosting OCSP or CRL. Cisco ISE services and ports documentation lists the basic ports used by the Cisco ISE administration node, monitoring node, and policy service node separately.

For OCSP, the default port is TCP 443. The Cisco ISE Admin portal accepts HTTP-based URLs for OCSP services. Non-default ports can also be used.

For CRL, the default protocols are HTTP, HTTPS, and LDAP. The default ports are 443 (HTTPS) and 389 (LDAP), respectively. The actual port depends on the CRL server.

## Cisco ISE processes

This table lists the Cisco ISE processes and their service impact.

| Process name                  | Description                                                                             | Service impact                                                                                        |
|-------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Database listener             | Oracle Enterprise Database listener                                                     | The process must be in the running state for all services to work properly.                           |
| Database server               | Oracle Enterprise Database server, which stores both configuration and operational data | The process must be in the running state for all services to work properly.                           |
| Application server            | Main Tomcat server for Cisco ISE                                                        | Must be in running state for all services to work properly                                            |
| Profiler database             | Redis database for Cisco ISE profiling service                                          | The process must be in the running state for Cisco ISE profiling service to work properly.            |
| AD connector                  | Active Directory runtime                                                                | The process must be in the running state for Cisco ISE to perform Active Directory authentications.   |
| MnT session database          | Oracle TimesTen Database for monitoring and troubleshooting (MnT) service               | Must be in Running state for all services to work properly.                                           |
| MnT log collector             | Log collector for MnT service                                                           | The process must be in the running state to support MnT operational data.                             |
| MnT log processor             | Log processor for MnT service                                                           | Must be in Running state for MnT operational data.                                                    |
| Certificate authority service | Cisco ISE Internal Certificate Authority (CA) service                                   | The process must be in the running state if Cisco ISE internal Certificate Authority (CA) is enabled. |

## Required internet URLs

This table lists the features that use certain URLs. You must configure either your network firewall or a proxy server so that IP traffic can travel between Cisco ISE and these resources. If you cannot provide access to a required URL, the related feature may not work as intended.

Configure your network firewall or proxy server to allow IP traffic between Cisco ISE and these resources. If access to any required URL is not possible, the feature may not function as intended.

**Table 24: Required URLs access**

| Feature                | URLs                                                                                                                                   |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Posture updates        | <a href="https://www.cisco.com/">https://www.cisco.com/</a><br><a href="https://iseservice.cisco.com">https://iseservice.cisco.com</a> |
| Profiling feed service | <a href="https://ise.cisco.com">https://ise.cisco.com</a>                                                                              |
| Smart licensing        | <a href="https://smartreceiver.cisco.com">https://smartreceiver.cisco.com</a>                                                          |
| Telemetry              | <a href="https://connectdna.cisco.com/">https://connectdna.cisco.com/</a>                                                              |

## Required internet URLs

| Feature                                                | URLs                                                                                                                                                                                                             |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connection from Cisco ISE to Cisco pxGrid Cloud Portal | https://dna.cisco.com<br>https://dnaservices.cisco.com<br>https://ciscodnacloud.com                                                                                                                              |
| Cisco AI analytics                                     | http://api.use1.prd.kairos.ciscolabs.com for the US East region<br>http://api.euc1.prd.kairos.ciscolabs.com for EU central region<br>Network connectivity to these required URLs is through HTTPS, TCP port 443. |
| Microsoft Entra ID                                     | graph.microsoft.com<br>login.microsoftonline.com:443<br>*.login.microsoftonline.com:443<br>*.login.microsoft.com:443                                                                                             |
| Workload connector                                     | public.ecr.aws                                                                                                                                                                                                   |
| Social login for self-registered guests                | facebook.co<br>akamaihd.net<br>akamai.co<br>fbedn.net                                                                                                                                                            |
| Cisco DUO integration for multifactor authentication   | *.duosecurity.com:443                                                                                                                                                                                            |

The **Interactive Help** feature requires Cisco ISE to connect to these URLs through the administration portal browser:

- \*.walkme.com
- \*.walkmeusercontent.com