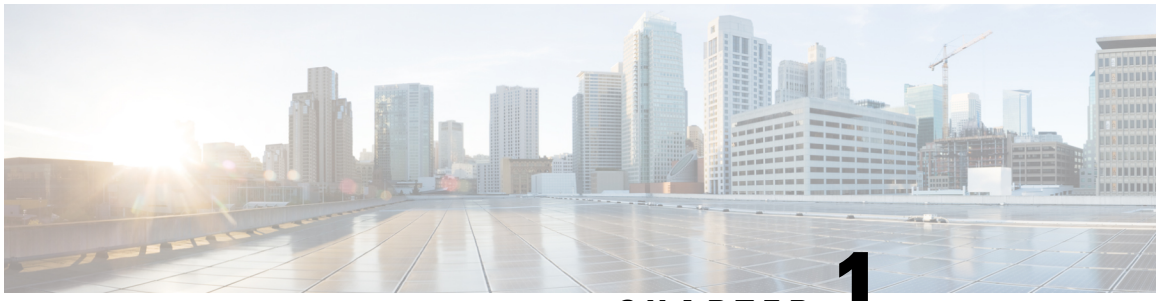
Cisco Identity Services Engine Installation Guide, Release 2.4

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

CONTENTS



CHAPTER 1

Network Deployments in Cisco ISE

Additional References

The following link contains additional resources that you can use when working with Cisco ISE: https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco ISE Network Architecture

Cisco ISE architecture includes the following components:

- Nodes and persona types
  - Cisco ISE node—A Cisco ISE node can assume any or all of the following personas: Administration, Policy Service, Monitoring, or pxGrid
- Network resources
- Endpoints

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

Cisco ISE Deployment Terminology

This guide uses the following terms when discussing Cisco ISE deployment scenarios:

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

Node Types and Personas in Distributed Deployments

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment can assume the Administration, Policy Service, pxGrid, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes on 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 Node

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 functionality such as authentication, authorization, and accounting. In a distributed deployment, you can have a maximum of two nodes running the Administration persona. The Administration persona can take on the standalone, primary, or secondary role.

Policy Service Node

A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this persona. Typically, there would be more than one Policy Service node in a distributed deployment. All Policy Service nodes that reside in the same high-speed Local Area Network (LAN) or behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any URL-redirected sessions.

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

Monitoring Node

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 in a network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage a network and resources. A node with this persona aggregates and correlates the data that it collects, and provides you with meaningful reports. Cisco ISE allows you to have a maximum of two nodes with this persona, and they can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring nodes collect log messages. 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 Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like 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 (EPS) to quarantine users/devices in response to a network or security event. The TrustSec information like tag definition, value, and description can be passed from Cisco ISE via TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through a endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

You can publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid. For more information about SXP bindings, see Security Group Tag Exchange Protocol section in *Cisco Identity Services Engine Administrator Guide*.

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

Standalone and Distributed ISE Deployments

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

A deployment that has more than one Cisco ISE node is called a *distributed deployment*. To support failover and to improve performance, you can set up a deployment with multiple Cisco ISE nodes in a distributed fashion. 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. A Cisco ISE node can assume any of the following personas: Administration, Policy Service, and Monitoring.

Distributed Deployment Scenarios

- Small Network Deployments
- Medium-Sized Network Deployments
- Large Network Deployments

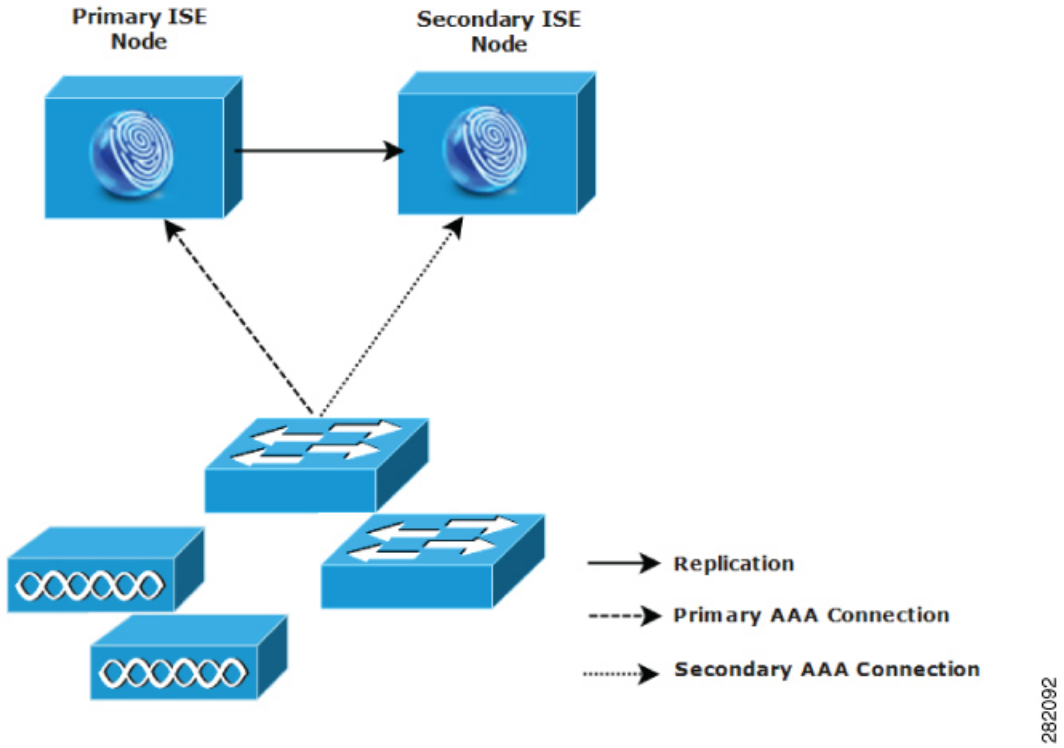
Small Network Deployments

The smallest Cisco ISE deployment consists of two Cisco ISE nodes with one Cisco ISE node functioning as the primary appliance in a small network.

The primary node provides all the configuration, authentication, and policy capabilities that are required for this network model, and the secondary Cisco ISE node functions in a backup role. The secondary node supports the primary node and maintains a functioning network whenever connectivity is lost between the primary node and network appliances, network resources, or RADIUS.

Centralized authentication, authorization, and accounting (AAA) operations between clients and the primary Cisco ISE node are performed using the RADIUS protocol. Cisco ISE synchronizes or replicates all of the content that resides on the primary Cisco ISE node with the secondary Cisco ISE node. Thus, your secondary node is current with the state of your primary node. In a small network deployment, this type of configuration model allows you to configure both your primary and secondary nodes on all RADIUS clients by using this type of deployment or a similar approach.

Figure 1: A Small Network Deployment of Cisco ISE nodes



As the number of devices, network resources, users, and AAA clients increases in your network environment, you should change your deployment configuration from the basic small model and use more of a split or distributed deployment model.

Split Deployments

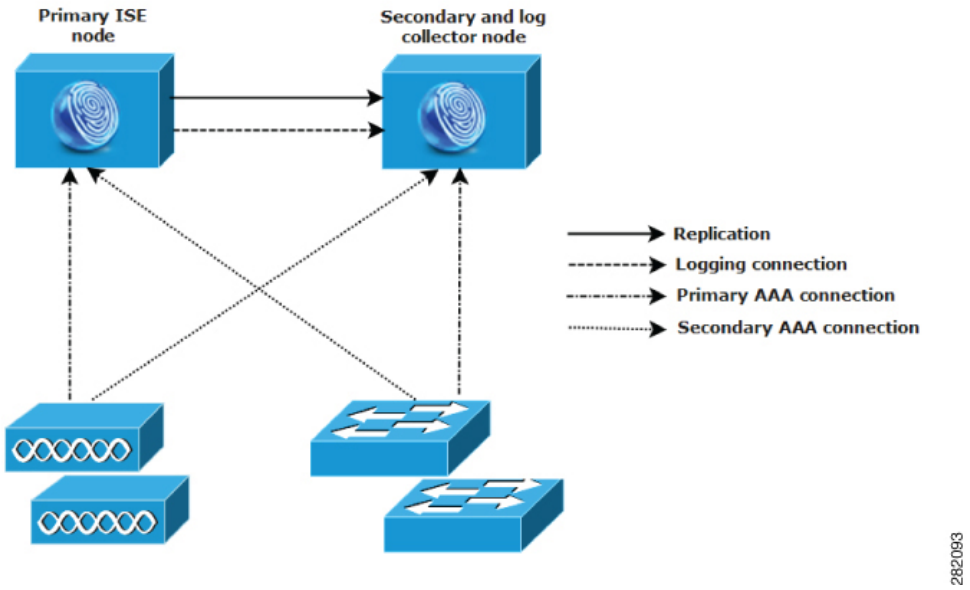
In split Cisco ISE deployments, you continue to maintain primary and secondary nodes as described in a small Cisco ISE deployment. However, the AAA load is split between the two Cisco ISE nodes to optimize the AAA workflow. Each Cisco ISE appliance (primary or secondary) needs to be able to handle the full workload if there are any problems with AAA connectivity. Neither the primary node nor the secondary nodes handles all AAA requests during normal network operations because this workload is distributed between the two nodes.

The ability to split the load in this way directly reduces the stress on each Cisco ISE node in the system. In addition, splitting the load provides better loading while the functional status of the secondary node is maintained during the course of normal network operations.

In split Cisco ISE deployments, each node can perform its own specific operations, such as network admission or device administration, and still perform all the AAA functions in the event of a failure. If you have two Cisco ISE nodes that process authentication requests and collect accounting data from AAA clients, we recommend that you set up one of the Cisco ISE nodes to act as a log collector.

In addition, the split Cisco ISE deployment design provides an advantage because it allows for growth.

Figure 2: Split Network Deployment in Cisco ISE



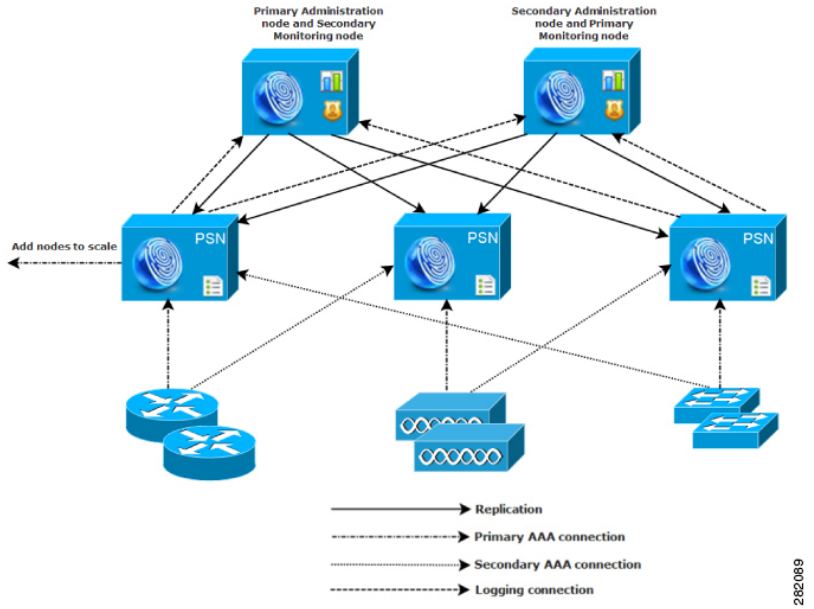
Medium-Sized Network Deployments

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

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

As the amount of log traffic increases in a network, you can choose to dedicate one or two of the secondary Cisco ISE nodes for log collection in your network.

Figure 3: A Medium-Sized Network Deployment in Cisco ISE



Large Network Deployments

Centralized Logging

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 serves as a Monitoring persona (for monitoring and logging) to handle the potentially high syslog traffic that a large, busy network can generate.

Because syslog messages are generated for outbound log traffic, any RFC 3164-compliant syslog appliance can serve as the collector for outbound logging traffic. A dedicated logging server enables you to use the reports and alert features that are available in Cisco ISE to support all the Cisco ISE nodes.

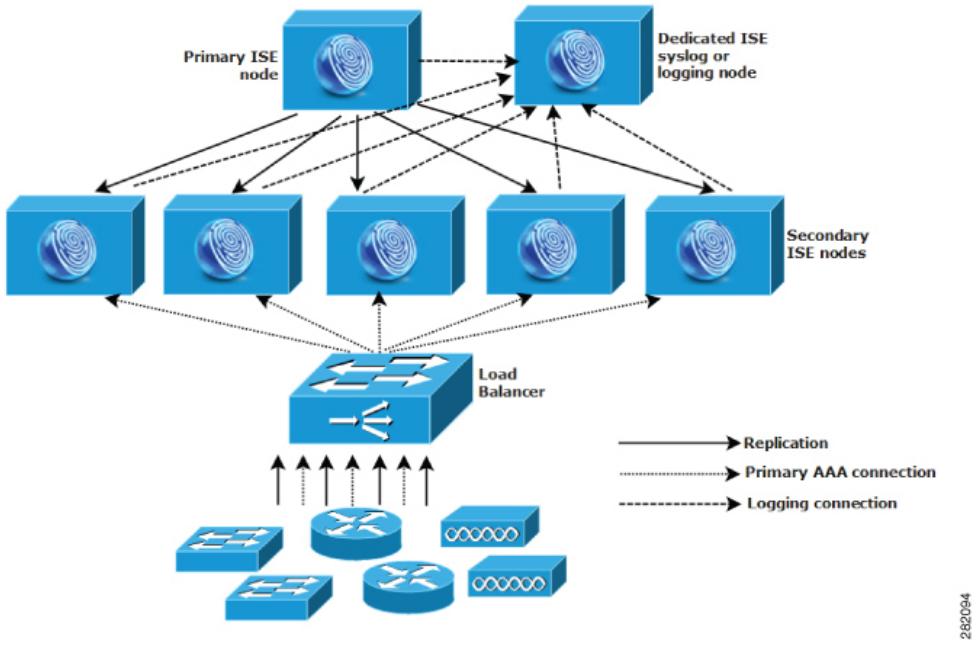
You can also consider having the appliances send logs to both a Monitoring persona on the Cisco ISE node and a generic syslog server. Adding a generic syslog server provides a redundant backup if the Monitoring persona on the Cisco ISE node goes down.

Using Load Balancers in Centralized Networks

In large centralized networks, you should use a load balancer, which simplifies the deployment of AAA clients. Using a load balancer requires only a single entry for the AAA servers, and the load balancer optimizes the routing of AAA requests to the available servers.

However, having only a single load balancer introduces the potential for having a single point of failure. To avoid this potential issue, deploy two load balancers to ensure a measure of redundancy and failover. This configuration requires you to set up two AAA server entries in each AAA client, and this configuration remains consistent throughout the network.

Figure 4: A Large Network Deployment in Cisco ISE using a Load Balancer

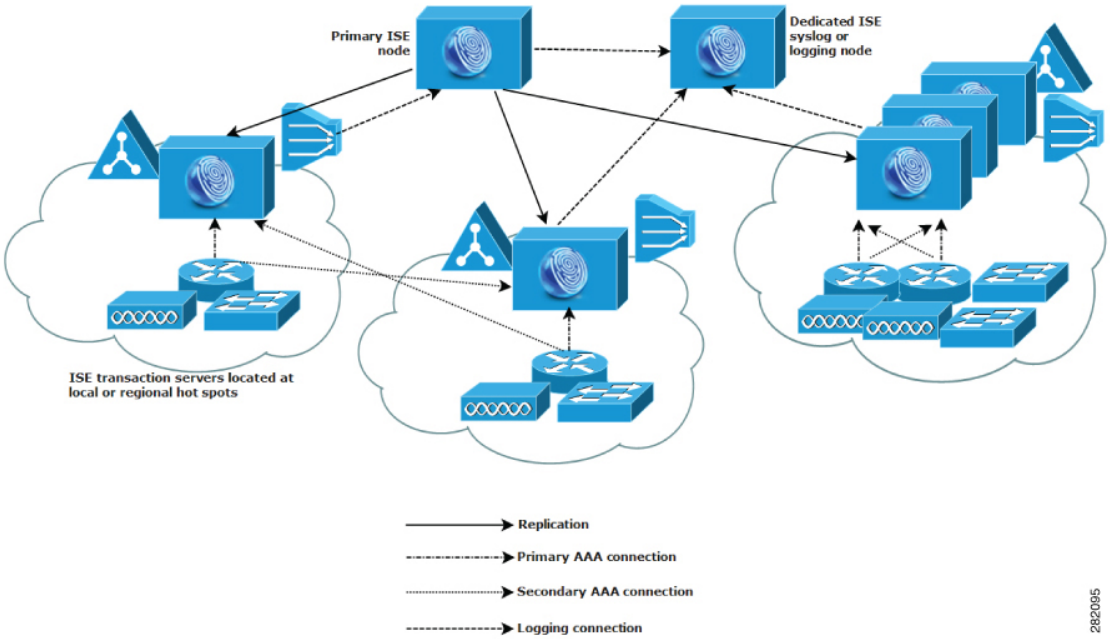


Dispersed Network Deployments in Cisco ISE

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, 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. A centralized management model helps maintain a consistent, synchronized AAA policy. A centralized configuration model uses a primary Cisco ISE node with secondary Cisco ISE nodes. We still recommend that you use a separate Monitoring persona on the Cisco ISE node, but each remote location should retain its own unique network requirements.

Figure 5: Dispersed Deployment in Cisco ISE



Considerations for Planning a Network with Several Remote Sites

- Verify if a central or external database is used, such as Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP). Each remote site should have a synchronized instance of the external database that is available for Cisco ISE to access for optimizing AAA performance.
- The location of AAA clients is important. You should locate the Cisco ISE nodes as close as possible to the AAA clients to reduce network latency effects and the potential for loss of access that is caused by WAN failures.
- Cisco ISE has console access for some functions such as backup. Consider using a terminal at each site, which allows for direct, secure console access that bypasses network access to each node.
- 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.
- Domain Name System (DNS) should be properly configured on all Cisco ISE nodes to ensure access to the 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.

Deployment Size and Scaling Recommendations for SNS 3500 Series Appliances

The following tables provide performance and scalability metrics for RADIUS sessions, Passive Identity, Easy Connect, pxGrid, and ISE services.

Table 1: Maximum RADIUS Scaling by Deployment with Maximum Passive Identity/Easy Connect Scaling by Deployment Size

Deployment Model	Platform	Max Number of Dedicated PSNs	Max RADIUS Sessions Per Deployment	Max Passive Identity Sessions Per Deployment	Max Merged and Easy Connect Sessions (Shared PSNs)	Max Merged and Easy Connect Sessions (Dedicated PSNs)
Standalone	3515	0	7500	100,000	1,000	N/A
	3595	0	20,000	300,000	2,000	N/A
PAN and MnT on same node and Dedicated PSNs	3515 as PAN and MnT	5	7,500	100,000	1,000	5,000
	3595 as PAN and MnT	5	20,000	300,000	2,000	10,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	3595 as PAN and MnT	50	500,000	300,000	N/A	50,000
Dedicated (PAN, MnT, PXG, and PSN Nodes)	Virtual Large SNS-3595 as PAN and MnT	50	500,000	300,000	N/A	50,000

Table 2: Scalability with pxGrid Services (pxGrid v1)

pxGrid Scaling Per Deployment	Platform	Max PSNs	Max PXGs	Max pxGrid Subscribers (Shared PSN+PXG)	Max pxGrid Subscribers (Dedicated PSN/PXG)
Standalone - All personas on same node (2 nodes redundant)	3515	0	0	2	N/A
	3595	0	0	2	N/A

pxGrid Scaling Per Deployment	Platform	Max PSNs	Max PXGs	Max pxGrid Subscribers (Shared PSN+PXG)	Max pxGrid Subscribers (Dedicated PSN/PXG)
• PAN, MnT, and PXG on same node and dedicated PSNs • PAN + MnT and dedicated PSN and PXG (Minimum 4 nodes redundant)	3515 as PAN + MnT/PXG	5*	2*	5	15
	3595 as PAN and MnT/PXG	5*	2*	5	15
Dedicated - All personas on dedicated nodes (Minimum 6 nodes redundant)	3595 as PAN and MnT	50	2	N/A	25
Scalability with pxGrid per PXG Node	**Platform**			**Max Subscribers per PXG Node**	
Dedicated pxGrid nodes (Max Publish Rate Gated by Total Deployment Size)	3515			15	
	3595			25	

Table 3: ISE Platform eXchange Grid (pxGrid v2) Scaling

Deployment Type	Platform	Max PSNs	Max PXGs	Max pxGrid Subscribers: Shared PAN+MNT+PXG	Max pxGrid Subscribers: Dedicated PSN/PXG
Standalone All personas on same node 2 nodes redundant	3515	0	0	20	N/A
	3595	0	0	30	N/A
Medium PAN+MnT+PXG on same node and dedicated PSNs -OR- PAN+MnT and dedicated PSN & PXG Minimum 4 nodes redundant	3515 as PAN+MNT/PXG	5*	2*	140	400
	3595 as PAN+MNT/PXG	5*	2*	160	400
	3595 as PAN+MNT/PXG	5*	3*	160	600
Dedicated All personas on dedicated nodes Minimum 6 nodes redundant	3595 as PAN and MNT	50	4	N/A	800
	3595 as PAN and MNT	50	4	N/A	800

* Maximum PSNs + PXG nodes = 5

Note Cisco ISE 2.3 and above releases support pxGrid v2, but require v2 Subscribers/Publishers. Each pxGrid v2 node can be Active.

Table 4: pxGrid v2 Scaling per Dedicated pxGrid Node

Platform	Max Subscribers per pxGrid node
3515	200
3595	200

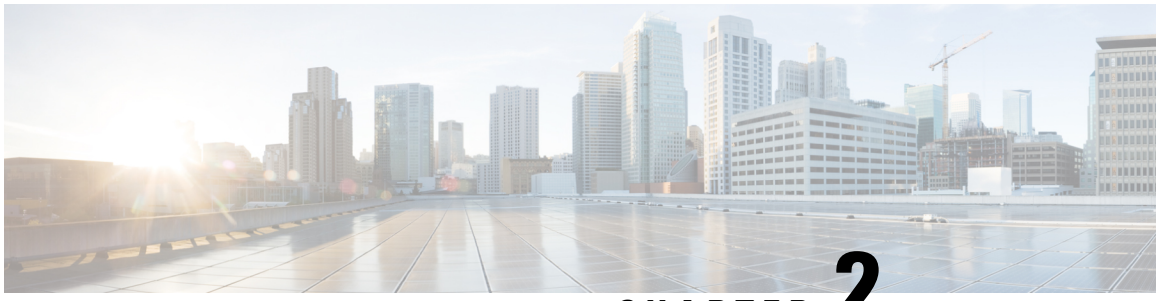
Maximum publish rate is gated by the total deployment size.

Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions

To ensure that Cisco ISE can interoperate with network switches and that functions from Cisco ISE are successful across the network segment, you must configure your network switches with certain required Network Time Protocol (NTP), RADIUS/AAA, IEEE 802.1X, MAC Authentication Bypass (MAB), and other settings.

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 3500/3600 Series Appliances and Virtual Machine Requirements

Hardware and Virtual Appliance Requirements for Cisco ISE

Cisco Identity Services Engine (Cisco ISE) can be installed on Cisco Secure Network Server (SNS) hardware or virtual appliances. To achieve performance and scalability comparable to the Cisco ISE hardware appliance, the virtual machine should be allocated system resources equivalent to the Cisco SNS hardware appliances. This section lists the hardware, software, and virtual machine requirements required to install Cisco ISE.

Note For Cisco SNS 3600 series appliance support (SNS-3615-K9, SNS-3655-K9, and SNS-3695-K9), you must use only the new ISO file (ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso). Cisco ISE 2.4 Patch 9 or above must be applied after installation. We recommend that you do not use this ISO file for SNS 3500 series appliance, VMware, KVM, or Hyper-V installation.

Note Harden your virtual environment and ensure that all the security updates are up-to-date. Cisco is not liable for any security issues found in hypervisors.

Note Cisco ISE does not support VM snapshots for backing up ISE data on any of the virtual environments (VMware, Linux KVM, Microsoft Hyper-V, and Nutanix AHV) because a VM snapshot saves the status of a VM at a given point in time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. We recommend that you use the backup functionality included in Cisco ISE for archival and restoration of data. Using snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

Caution If the Snapshot feature is enabled on the VM, it might corrupt the VM configuration. If this issue occurs, you might have to reimage the VM and disable VM snapshot.

Cisco Secured Network Server Hardware Appliances

For Cisco Secured Network Server (SNS) hardware appliance specifications, see "Table 1, Product Specifications" in the Cisco Secure Network Server Data Sheet.

For Cisco SNS 3500 series appliances, see Cisco SNS-3500 Series Appliance Hardware Installation Guide.

For Cisco SNS 3600 series appliances, see Cisco SNS-3600 Series Appliance Hardware Installation Guide.

VMware Virtual Machine Requirements for Cisco ISE

Cisco ISE supports the following VMware servers and clients:

- VMware Version 8 (default) for ESXi 5.*x* (5.1 U2 minimum)

Note If you are installing Cisco ISE on an ESXi 5.*x* server, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

- VMware version 11 (default) for ESXi 6.*x*
-

Cisco ISE supports the VMware cold migration feature that allows you to migrate virtual machine (VM) instances (running any persona) between hosts. For the cold migration feature to be functional, the following condition must be met:

- Cisco ISE must be shutdown and powered off: Cisco ISE does not allow to stop or pause the database operations during migration. This might lead to data corruption issues. Hence, ensure that Cisco ISE is not running and active during the migration.

Note

- You must use the application stop command before using the halt command or powering off the VM to prevent database corruption issues.
- Cisco ISE VM does not support hot migration (vMotion).

Refer to your VMware documentation for more information on vMotion requirements.

Cisco ISE offers the following OVA templates that you can use to install and deploy Cisco ISE on virtual machines (VMs):

- ISE-2.4.0.*xxx*-virtual-Eval.ova
- ISE-2.4.0.*xxx*-virtual-SNS3515-Small-200GBHD-16GBRAM-12CPU.ova

- ISE-2.4.0.*xxx*-virtual-SNS3515-Small-600GBHD-16GBRAM-12CPU.ova
- ISE-2.4.0.*xxx*-virtual-SNS3595-Medium-200GBHD-64GBRAM-16CPU.ova
- ISE-2.4.0.*xxx*-virtual-SNS3595-Medium-1200GBHD-64GBRAM-16CPU.ova
- ISE-2.4.0.*xxx*-virtual-SNS3595-Large-1200GBHD-256GBRAM-16CPU.ova

The 200 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 ISE 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.

The OVA template reservations for the base SNS platforms are provided in the table below.

Table 5: OVA Template Reservations

OVA Template	Memory	CPU
Virtual Eval OVA	16 GB RAM	2300 MHz (no reservation)
Virtual SNS-3515 OVA (Small)	16 GB RAM	12 GHz
Virtual SNS-3595 OVA (Medium)	64 GB RAM	16 GHz
Virtual SNS-3595 OVA (Large) The large node is only for use as a performance-enhanced MnT node. You cannot use the Large VM as a PAN, PSN, or pxGrid node.	256 GB RAM	16+ GHz

We strongly recommend that you reserve CPU and memory resources to match the resource allocation. Failure to do so may significantly impact ISE performance and stability.

For information about the product specifications for Cisco SNS appliance, see Cisco Secure Network Server Data Sheet.

The following table lists the VMware virtual machine requirements.

Table 6: VMware Virtual Machine Requirements

Requirement Type	Specifications
CPU	• **Evaluation** • Clock speed: 2.0 GHz or faster • Number of CPU cores: 2 CPU cores • **Production** • Clock speed: 2.0 GHz or faster • Number of cores: • **SNS 3500 Series Appliance:** • Small: 12 • Medium: 16 • Large: 16 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3500 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 3515, which has 8 CPU Cores or 16 Threads. See Table 5: OVA Template Reservations for CPU Reservations.
Memory	• **Evaluation**: 16 GB • **Production** • Small: 16 GB for SNS 3515 and 32 GB for SNS 3615 • Medium: 64 GB for SNS 3595 and 96 GB for SNS 3655 • Large: 256 GB for SNS 3695 The Large memory size is only for use as a performance-enhanced MnT node. You cannot use the Large VM as a PAN, PSN, or pxGrid node. See Table 5: OVA Template Reservations for Memory Reservations.

Requirement Type	Specifications
Hard Disks	• **Evaluation**: 200 GB • **Production** 200 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following link: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine 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.
Storage and File System	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. You can use the **show tech-support** command to view the read and write performance metrics. 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.
Disk Controller	Paravirtual (default for RHEL 7 64-bit) or LSI Logic Parallel For best performance and redundancy, a caching RAID controller is recommended. Controller options such as RAID 10 (also known as 1+0) can offer higher overall write performance and redundancy than RAID 5, for example. Additionally, battery-backed controller cache can significantly improve write operations. **Note** Updating the disk SCSI controller of an ISE VM from another type to VMware Paravirtual may render it not bootable.
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported). Cisco ISE supports E1000 and VMXNET3 adapters. **Note** We recommend that you select E1000 to ensure correct adapter order by default. If you choose VMXNET3, you might have to remap the ESXi adapter to synchronize it with the ISE adapter order.
VMware Virtual Hardware Version/Hypervisor	VMware Virtual Machine Hardware Version 8 or higher on ESXi 5.*x* (5.1 U2 minimum) and 6.x. **Note** If you are installing Cisco ISE on an ESXi 5.*x* server, to support RHEL 7 as the Guest OS, update the VMware hardware version to 9 or later. RHEL 7 is supported with VMware hardware version 9 and later.

Linux KVM Requirements for Cisco ISE

Table 7: Linux KVM Virtual Machine Requirements

Requirement Type	Minimum Requirements
CPU	• **Evaluation** • Clock Speed: 2.0 GHz or faster • Number of Cores: 2 CPU cores • **Production** • Clock Speed: 2.0 GHz or faster • **Number of Cores:** • **SNS 3500 Series Appliance:** • Small: 12 • Medium: 16 • Large: 16 **Note** The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3500 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 3515, which has 8 CPU Cores or 16 Threads. See Table 5: OVA Template Reservations for CPU Reservations.
Memory	• **Evaluation**: 16 GB • **Production** • Small: 16 GB for SNS 3515 and 32 GB for SNS 3615 • Medium: 64 GB for SNS 3595 and 96 GB for SNS 3655 • Large: 256 GB for SNS 3695 See Table 5: OVA Template Reservations for Memory Reservations.

Requirement Type	Minimum Requirements
Hard disks	• **Evaluation**: 200 GB • **Production** 200 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following link: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine 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.
KVM Disk Device	Disk bus - virtio, cache mode - none, I/O mode - native Use preallocated RAW storage format.
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported). Cisco ISE supports VirtIO drivers. We recommend VirtIO drivers for better performance.
Hypervisor	KVM on RHEL 7.0

Microsoft Hyper-V Requirements for Cisco ISE

Table 8: Microsoft Hyper-V Virtual Machine Requirements

Requirement Type	Minimum Requirements
CPU	• **Evaluation** • Clock speed: 2.0 GHz or faster • Number of cores: 2 CPU cores • **Production** • Clock speed: 2.0 GHz or faster • **Number of Cores:** • **SNS 3500 Series Appliance:** • Small: 12 • Medium: 16 • Large: 16 The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3500 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 3515, which has 8 CPU Cores or 16 Threads. See Table 5: OVA Template Reservations for CPU Reservations.
Memory	• **Evaluation**: 16 GB • **Production** • Small: 16 GB for SNS 3515 and 32 GB for SNS 3615 • Medium: 64 GB for SNS 3595 and 96 GB for SNS 3655 • Large: 256 GB for SNS 3695 See Table 5: OVA Template Reservations for Memory Reservations.

Requirement Type	Minimum Requirements
Hard disks	• **Evaluation**: 200 GB • **Production** 200 GB to 2.4 TB of disk storage (size depends on deployment and tasks). See the recommended disk space for VMs in the following link: Disk Space Requirements. We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM. **Note** When you create the Virtual Machine 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.
NIC	1 NIC interface required (two or more NICs are recommended; six NICs are supported).
Hypervisor	Hyper-V (Microsoft)

Virtual Machine Appliance Size Recommendations for Cisco ISE

Cisco ISE 2.4 introduces a large VM for Monitoring nodes. Deploying a Monitoring persona on a large VM offers the following advantages:

- Improves performance in terms of faster response to live log queries and report completion.
- Will be able to support the deployments that can handle more than 500, 000 sessions when the support is provided in future ISE releases.

Note This form factor is available only as a VM in Release 2.4 and later, and requires a large VM license.

The virtual machine (VM) appliance specifications should be comparable with physical appliances run in a production environment.

Keep the following guidelines in mind when allocating resources for the appliance:

- Failure to allocate the specified resources might result in performance degradation or service failure. We highly recommend that you deploy dedicated VM resources and not share or oversubscribe resources across multiple guest VMs. Deploying Cisco ISE virtual appliances using the OVF templates ensures that adequate resources are assigned to each VM. If you do not use OVF templates, then ensure that you assign the equivalent resource reservations when you manually install Cisco ISE using the ISO image.

Note If you choose to deploy Cisco ISE manually without the recommended reservations, you must assume the responsibility to closely monitor your appliance's resource utilization and 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 the following settings after the installation is complete:
  - Ensure that you assign the resource reservations that are specified in the VMware Virtual Machine Requirements for Cisco ISE, on page 16 section in the CPU/Memory **Reservation** field (under the **Virtual Hardware** tab in the **Edit Settings** window) to ensure proper health and functioning of the Cisco ISE deployment.
  - Ensure that the CPU usage in the **CPU Limit** field (under the **Virtual Hardware** tab in the **Edit Settings** window) is set to **Unlimited**. Setting a limit for CPU usage (for example, setting the CPU usage limit as 12000 MHz) will impact the system performance. If limit has been set, you must shutdown the VM client, remove the limit, and the restart the VM client.
  - Ensure that the memory usage in the **Memory Limit** field (under the **Virtual Hardware** tab in the **Edit Settings** window) is set to **Unlimited**. Setting a limit for memory usage (for example, setting the limit as 12000 MB) will impact the system performance.
  - Ensure that the **Shares** option is set as **High** in the **Hard Disk** area (under the **Virtual Hardware** tab in the **Edit Settings** window).

    Admin and MnT nodes rely heavily on disk usage. Using shared disk storage VMware environment might affect the disk performance. You must increase the number of disk shares allocated to a node to increase the performance of the node.
- Policy Service nodes on VMs can be deployed with less disk space than Administration or Monitoring nodes. The minimum disk space for any production Cisco ISE node is 200 GB.
- VMs can be configured with 1 to 6 NICs. The recommendation is to allow for 2 or more NICs. Additional interfaces can be used to support various services such as profiling, guest services, or RADIUS.

Note RAM and CPU adjustments on VM do not require re-image.

Disk Space Requirements for VMs in a Cisco ISE Deployment

The following table lists the Cisco ISE disk-space allocation recommended for running a virtual machine in a production deployment.

Note You must change the firmware from **BIOS** to **EFI** in the boot mode of VM settings to boot GPT partition with 2 TB or above.

Table 9: Recommended Disk Space for Virtual Machines

Cisco ISE Persona	Minimum Disk Space for Evaluation	Minimum Disk Space for Production	Recommended Disk Space for Production	Maximum Disk Space
Standalone Cisco ISE	200 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration only	200 GB	600 GB	600 GB	2.4 TB
Distributed Cisco ISE,Monitoring only	200 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE,Policy Service only	200 GB	200 GB	200 GB	2.4 TB
Distributed Cisco ISE, pxGrid only	200 GB	200 GB	200 GB	2.4 TB
Distributed Cisco ISE, Administration and Monitoring (and optionally, pxGrid)	200 GB	600 GB	600 GB to 2.4 TB	2.4 TB
Distributed Cisco ISE, Administration, Monitoring, and Policy Service (and optionally, pxGrid)	200 GB	600 GB	600 GB to 2.4 TB	2.4 TB

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

Disk Space Guidelines for Cisco ISE

Keep the following guidelines in mind when deciding the disk space for Cisco ISE:

- Cisco ISE must be installed on a single disk in virtual machine.
- 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. A fresh installation helps properly detect and utilize the full disk allocation.

The following table lists the number of days that RADIUS logs can be retained on your Monitoring node based on the allocated disk space and the number of endpoints that connect to your network. The numbers are based on the following 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

No. of Endpoints	200 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

The following table lists the number of days that TACACS+ logs can be retained on your Monitoring node based on the allocated disk space and the number of endpoints that connect to your network. The numbers are based on the following 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+

No. of Endpoints	200 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 you find that context and visibility functions are slow, or you are running out of room for logs, you must allocate more disk space.

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

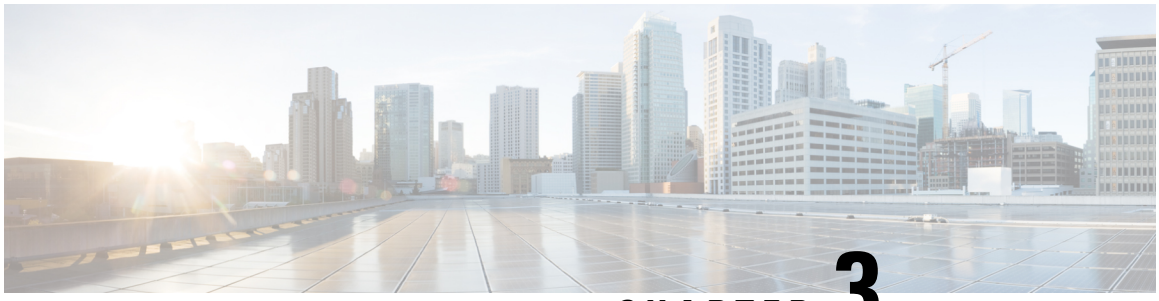
In order for ISE to detect and utilize the new disk allocation, you must deregister the node, update the VM settings, and reinstall ISE. One way to do this is to install ISE on a new larger node, and add that node to the deployment as high availability. After the nodes have synchronized, make the new VM the primary and deregister the original VM.

Decrease Disk Size

After you install Cisco ISE on a VM, you must not reduce the VM reservations. If you reduce the VM memory to less than what Cisco ISE services require, Cisco ISE services fail to come up due to insufficient resources.

After you install Cisco ISE, if you must reconfigure your VM, then carry out the following steps:

1. Perform backup of Cisco ISE.
2. Reimage Cisco ISE with the changed VM configuration as needed.
3. Restore Cisco ISE.



CHAPTER 3

Install Cisco ISE

Install Cisco ISE Using CIMC

This section lists the high-level installation steps to help you quickly install Cisco ISE:

Before you begin

- Ensure that you have met the System Requirements as specified in this guide.
- (Optional; required only if you are installing Cisco ISE on virtual machines) Ensure that you have created the virtual machine correctly.

  See the following topics for more information:

  - Configure a VMware Server, on page 42
  - Install Cisco ISE on KVM, on page 52
  - Create a Cisco ISE Virtual Machine on Hyper-V, on page 55

- (Optional; required only if you are installing Cisco ISE on SNS hardware appliances) Ensure that you set up the Cisco Integrated Management Interface (CIMC) configuration utility to manage the appliance and configure BIOS. See the following document for more information:

  - For SNS 3500 series appliances, see Cisco SNS-3500 Series Appliance Hardware Installation Guide.
  - For SNS-3600 series appliances, see Cisco SNS-3600 Series Appliance Hardware Installation Guide.

Step 1 If you are installing Cisco ISE on a:

- Cisco SNS appliance: Install the hardware appliance. Connect to CIMC for server management.
- Virtual Machine: Ensure that your VM is configured correct. Use the OVA template if you are installing Cisco ISE on VMware VM.

Step 2 Download the Cisco ISE ISO image. To install Cisco ISE on VMware VM, download the OVA template.

a) Go to http://www.cisco.com/go/ise. You must already have valid Cisco.com login credentials to access this link.

b) Click **Download Software for this Product**.

The Cisco ISE image comes with a 90-day evaluation license already installed, so you can begin testing all Cisco ISE services when the installation and initial configuration is complete.

Step 3 Boot the appliance or the virtual machine.

- Cisco SNS appliance:

  a. Connect to CIMC and log in using the CIMC credentials.

  b. Launch the KVM console.

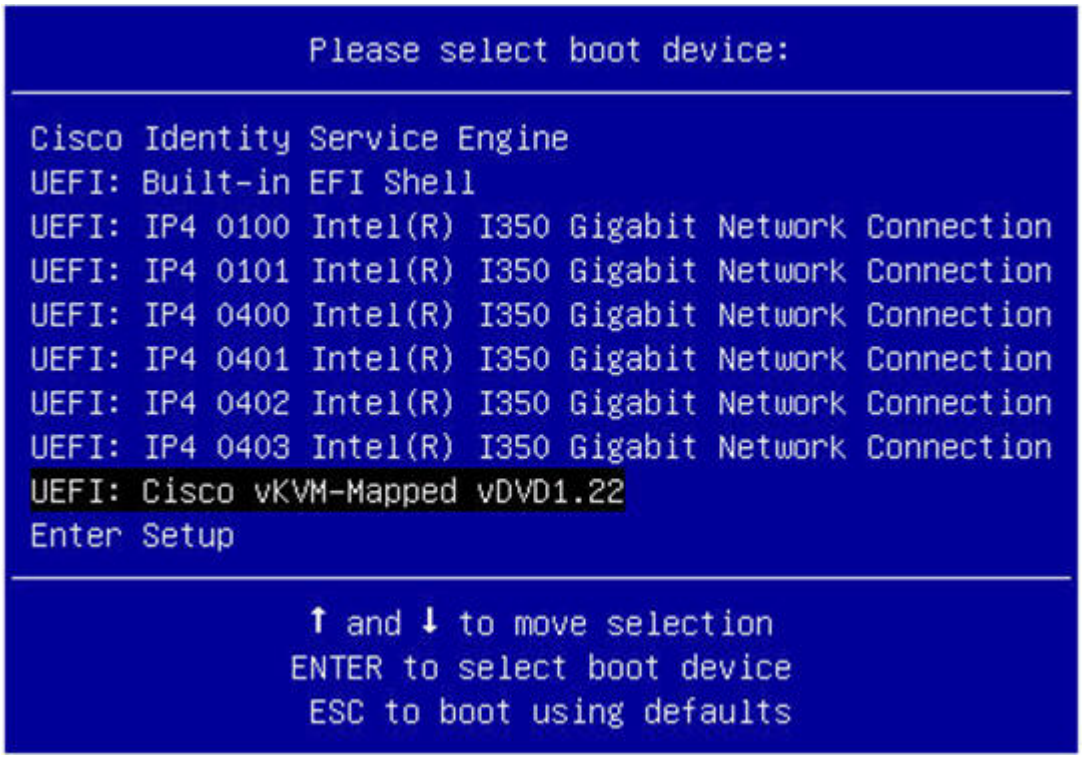
  c. Choose Virtual Media > Activate Virtual Devices.

  d. Choose Virtual Media > Map CD/DVD and select the ISE ISO image and click Map Device.

  e. Choose Macros > Static Macros > Ctrl-Alt-Del to boot the appliance with the ISE ISO image.

  f. Press F6 to bring up the boot menu. A screen similar to the following one appears:

Figure 6: Selection of Boot Device



Note If the SNS appliances are placed in a remote location (for example, data centers), to which you do not have any physical access and need to perform CIMC install from remote servers, it might take long hours for installation. We recommend that you copy the ISO file on a USB drive and use that in the remote location to speed up the installation process.

- Virtual Machine:

  a. Map the CD/DVD to an ISO image. A screen similar to the following one appears. The following message and installation menu are displayed.

```
Welcome to the Cisco Identity Services Engine Installer
Cisco ISE Version: 2.4.0.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 following message appears.

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

Step 5 At the prompt, type **setup** to start the Setup program. See Run the Setup Program of Cisco ISE, on page 31 for details about the Setup program parameters.

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 from the shell prompt mode. The appliance comes up.

Step 8 Continue with Verifying the Cisco ISE Installation Process, on page 34 .

Run the Setup Program of Cisco ISE

This section describes the setup process to configure the ISE server.

The setup program launches an interactive command-line interface (CLI) that prompts you for the required parameters. An administrator can use the console or a dumb terminal to configure the initial network settings and provide the initial administrator credentials for the ISE server using the setup program. This setup process is a one-time configuration task.

Note If you are integrating with Active Directory (AD), it is best to use the IP and subnet addresses from a dedicated Site created specifically for ISE. Consult with the staff in your organization responsible for AD and retrieve the relevant IP and subnet addresses for your ISE nodes prior to installation and configuration.

Note It is not recommended to attempt offline installation of Cisco ISE as this can lead to system instability. When you run the Cisco ISE installation script offline, the following error is shown:

Sync with NTP server failed' Incorrect time could render the system unusable until it is re-installed. Retry? Y/N [Y]:

Choose **Yes** to continue with the installation. Choose **No** to retry syncing with the NTP server.

It is recommended to establish network connectivity with both the NTP server and the DNS server while running the installation script.

To run the setup program:

Step 1 Turn on the appliance that is designated for the installation.

The setup prompt appears:

```
Please type 'setup' to configure the appliance
localhost login:
```

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

The console displays a set of parameters. You must enter the parameter values as described in the table that follows.

Table 12: Cisco ISE Setup Program Parameters

Prompt	Description	Example
Hostname	Must not exceed 19 characters. Valid characters include alphanumerical (A–Z, a–z, 0–9), and the hyphen (-). The first character must be a letter. **Note** We recommend that you use lowercase letters to ensure that certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verifications. You cannot use "localhost" as hostname for a node.	isebeta1
(eth0) Ethernet interface address	Must be a valid IPv4 address for the Gigabit Ethernet 0 (eth0) interface.	10.12.13.14
Netmask	Must be a valid IPv4netmask.	255.255.255.0
Default gateway	Must be a valid IPv4 address for the default gateway.	
DNS domain name	Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).	example.com
Primary name server	Must be a valid IPv4 address for the primary name server.	10.15.20.25

Prompt	Description	Example
Add/Edit another name server	Must be a valid IPv4 address for the primary name server.	(Optional) Allows you to configure multiple name servers. To do so, enter **y** to continue.
Primary NTP server	Must be a valid IPv4 address or hostname of a Network Time Protocol (NTP) server. **Note** Ensure that the primary NTP server is reachable.	**clock.nist.gov**
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 (or Coordinated Universal Time (UTC) minus 8 hours). **Note** Ensure that the system time and time zone match with the CIMC or Hypervisor Host OS time and time zone. System performance might be affected if there is any mismatch between the time zones. You can run the **show timezones** command from the Cisco ISE CLI for a complete list of supported time zones. **Note** We recommend that you set all the Cisco ISE nodes to the UTC 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.	UTC (default)
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 three to eight characters in length and comprise 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 When you create a password for the administrator during installation or after installation in the CLI, do not use the $ character in your password, unless it is the last character of the password. If it is the first or one of the subsequent characters, the password is accepted, but cannot be used to log in to the CLI.

If you inadvertently create such a password, reset your password by logging into the console and using the CLI command, or by getting an ISE CD or ISO file. Instructions for using an ISO file to reset the password are explained in the following document: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200568-ISE-Password-Recovery-Mechanisms.html

After the setup program is run, the system reboots automatically.

Now, you can log in to Cisco ISE using the username and password that was configured during the setup process.

Verifying the Cisco ISE Installation Process

To verify that you have correctly completed the installation process:

Step 1 When the system reboots, at the login prompt enter the username you configured during setup, and press **Enter**.

When you log in through the CLI for the first time after installation, the system prompts you to change the password.

Step 2 Enter a new password.

Step 3 Verify that the application has been installed properly by entering the **show application** command, and 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.

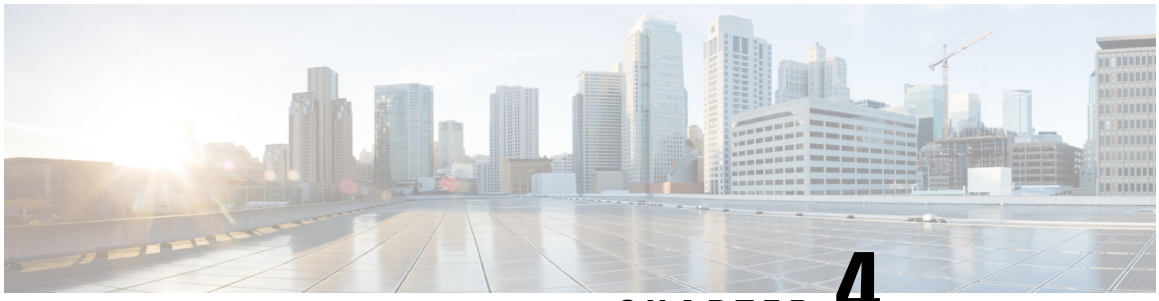
Step 4 Check the status of the ISE processes by entering the **show application status ise** command, and press **Enter**. The console displays:

```
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
Wifi Setup Helper Container            not running
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#
```



CHAPTER 4

Additional Installation Information

SNS Appliance Reference

Create a Bootable USB Device to Install Cisco ISE

Before you begin

- Use the Fedora Media Writer tool to create a bootable USB device from the Cisco ISE installation ISO file.

  Download Fedora Media Writerhttps://github.com/lmacken/liveusb-creator/releases/tag/3.12.0 to the local system.

Note Other USB tools might work, but we recommend that you use Fedora Media Writer 3.12.0 as it has been tested with Cisco ISE.

- Download the Cisco ISE installation ISO file to the local system.
- Use a 8-GB (or higher) USB device.

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 **Fedora Media Writer**.

Step 3 Click **Browse** from the **Use existing Live CD** area and choose the Cisco ISE ISO file.

Step 4 Choose the USB device from the **Target Device** drop-down list.

If there is only one USB device connected to the local system, it is selected automatically.

Step 5 Click **Create Live USB**.

The progress bar indicates the progress of the bootable USB creation. After this process is complete, the content of the USB drive is available in the local system that you used to run the USB tool. There are two text files that you must manually update before you can install Cisco ISE.

Step 6 From the USB drive, open the following text files in a text editor:

- isolinux/*isolinux.cfg* or syslinux/*syslinux.cfg*
- EFI/BOOT/*grub.cfg*

Step 7 Replace the term "**cdrom**" in both the files.

- If you have a SNS 3515, 3595, 3615, 3655, or 3695 appliance, replace the term "**cdrom**" with "**hd:sdb1**" in both the files.

Specifically, replace all instances of the "**cdrom**" string. For example, replace

ks=*cdrom*/ks.cfg

with

ks=*hd:sdb1:*/ks.cfg

Step 8 Save the files and exit.

Step 9 If you are using ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso to create Live USB, replace the BOOTX64.EFI and grub.efi files in the EFI/BOOT folder with the files available on the Cisco Software Download site and exit.

Step 10 Safely remove the USB device from the local system.

Step 11 Plug in the bootable USB device to the Cisco ISE appliance, restart the appliance, and 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 the following:

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.

The SNS 3515 and SNS 3595 appliances support only Cisco ISE 2.0.1 or later releases. You cannot install a release earlier than 2.0.1 on the SNS 3515 or SNS 3595 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 and plug in an USB external DVD drive and boot the appliance from the DVD drive.
- Create a bootable USB device using the installation .iso file and boot the appliance from the USB drive.

VMware Virtual Machine

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 VM resource check, the installer checks for the hard disk space, number of CPU cores allocated to the VM, CPU clock speed, and RAM allocated to the VM. If the VM resources do not meet the basic evaluation specifications, the installation terminates. This resource check is applicable only for ISO-based installations.

When you run the Setup program, a VM performance check is done, where the installer checks for disk I/O performance. If the disk I/O performance does not meet the recommended specifications, a warning appears on screen, but it allows you to continue with the installation.

The VM performance check is done periodically (every hour) and the results are averaged for a 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.

The VM resource and performance checks can be run independent of Cisco ISE installation. You can perform this test from the Cisco ISE boot menu.

Deploy Cisco ISE on Virtual Machines Using OVA Templates

You can use OVA templates to install and deploy Cisco ISE software on a virtual machine. Download the OVA template from Cisco.com.

Before you begin

Note When deploying Cisco ISE OVA files, we recommend that you remove or disconnect the unrequired network adapters after you complete the import, but before you run the setup for Cisco ISE. If you are using 4 or more network adapters, retain network adapter type E1000 to avoid interface reordering. If you are using up to 3 network adapters, you can delete all your E1000 network adapters and replace them with VMXNET3 ones.

Step 1 Open **VMware vSphere** client.

Step 2 Log in to VMware host.

Step 3 Choose **File** > **Deploy OVF Template** from the VMware vSphere Client.

Step 4 Click **Browse** to select the OVA template, and click **Next**.

Step 5 Confirm the details in the OVF Template Details page, and click **Next**.

Step 6 Enter a name for the virtual machine in the Name and Location page to uniquely identify it, and click **Next**.

Step 7 Choose a data store to host the OVA.

Step 8 Click the **Thick Provision** radio button in the Disk Format page, and click **Next**.

Cisco ISE supports both thick and thin provisioning. However, we recommend that you choose thick provisioning 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 9 Verify the information in the Ready to Complete page. Check the **Power on after deployment** check box.

Step 10 Click **Finish**.

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 your Guest Operating System is set to Red Hat Enterprise Linux (RHEL) 7 (64-bit) or Red Hat Enterprise Linux (RHEL) 6 (64-bit).
- For Red Hat Enterprise Linux 7, the default NIC type is VMXNET3 Adapter. You can add up to six NICs for your Cisco ISE virtual machine, but ensure that you choose the same Adapter for all the NICs. Cisco ISE supports the E1000 Adapter.

Note If you choose the default network driver (VMXNET3) as the Network Adapter, check the physical adapter mappings. Ensure that you map the Cisco ISE GigabitEthernet 0 interface to the 4th interface (NIC 4) in ESXi server as listed in the following table.

ADE-OS	Cisco ISE	E1000	VMXNET3
eth0	GE0	1	4
eth1	GE1	2	1
eth2	GE2	3	2
eth3	GE3	4	3
eth4	GE4	5	5
eth5	GE5	6	6

If you choose the E1000 Adapter, by default, the ESXi adapters and Cisco ISE adapters are mapped correctly.

- 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 have an ESXi server installed already, you can check if Virtualization Technology is enabled on it without rebooting the machine. To do this, use the **esxcfg-info** command. Here is an example:

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

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

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

Enable Virtualization Technology on an ESXi Server

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

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.

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**.

Repeat the same steps on the other VMware ESXi server interface used for profiler data collection of SPAN or mirrored traffic.

Connect to the VMware Server Using the Serial Console

Step 1 Power down the particular 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, click the **Use physical serial port on the host** or the **Connect via Network** radio button and 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 may choose one of the following two options:
  - **/dev/ttyS0** (In the DOS or Windows operating system, this will appear as COM1).
  - **/dev/ttyS1** (In the DOS or Windows operating system, this will appear as COM2).

Step 6 Click **Next**.

Step 7 In the Device Status area, check the appropriate check box. The default is Connected.

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 ESXi Server.

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 Configuration dialog box, choose **Custom** for the VMware configuration and click **Next**.

Step 4 Enter a name for the VMware system and click **Next**.

Tip Tip Use the hostname that you want to use for your VMware host.

Step 5 Choose a datastore that has the recommended amount of space available and click **Next**.

Step 6 (Optional) If your VM host or cluster supports more than one VMware virtual machine version, choose a Virtual Machine version such as Virtual Machine Version 7, and click **Next**.

Step 7 Choose **Linux** and select the supported Red Hat Enterprise Linux version from the **Version** drop-down list.

Step 8 Choose a value from the Number of virtual sockets and the Number of cores per virtual socket drop-down list. Total number of cores should be:

- Small—12
- Medium—16
- Large—16

The number of cores is twice of that present in equivalent of the Cisco Secure Network Server 3500 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 3515, which has 8 CPU Cores or 16 Threads.

Note We strongly recommend that you reserve CPU and memory resources to match the resource allocation. Failure to do so may significantly impact ISE performance and stability.

Step 9 Choose the amount of memory and click **Next**.

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

Step 11 Choose **Paravirtual** as the SCSI controller and click **Next**.

Step 12 Choose **Create a new virtual disk** and click **Next**.

Step 13 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 14 Uncheck the **Support clustering features such as Fault Tolerance** check box.

Step 15 Choose the advanced options, and click **Next**.

Step 16 Verify the configuration details, such as Name, Guest OS, CPUs, Memory, and Disk Size of the newly created VMware system. You must see the following values:

- Guest OS—Red Hat Enterprise Linux 7
- Logical CPUs—12
- Memory—16 GB or 16384 MB

For the Cisco ISE installation to be successful on a virtual machine, ensure that you adhere to the recommendations given in this document.

Step 17 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 by default is set to 0. You can change this boot delay to help you choose the boot options (while resetting the Administrator password, for example).

Step 1 From the VSphere client, right click the VM 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 Check 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

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.

Step 5 Click **OK**.

Step 6 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) 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/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.

e) Using the arrow keys, navigate to the Boot menu and press **Enter**.

f) Using the arrow keys, select 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**.

h) 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 displays:

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

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:
```

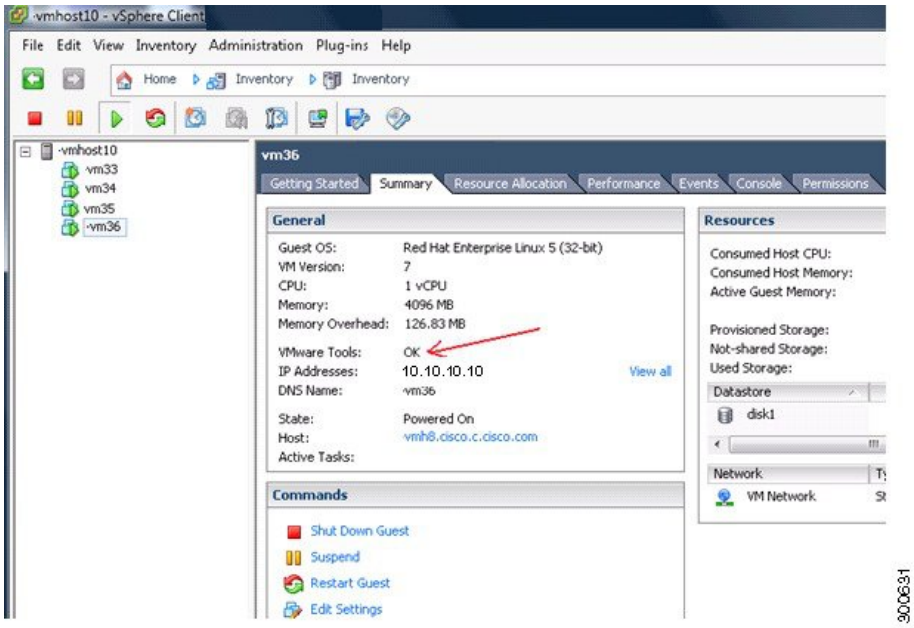
Step 9 At the system prompt, type **setup** and press **Enter**.
The Setup Wizard appears and guides you through the initial configuration.

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 vShpere Client. The value in the VMware Tools field should be OK.

Figure 7: Verifying VMware Tools in the vSphere Client



Verify VMWare Tools Installation Using the CLI

You can also verify if the VMware tools are installed using the **show inventory** command. This command lists the NIC driver information. On a virtual machine with VMware tools installed, VMware Virtual Ethernet driver will be listed in the Driver Descr 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 Cisco ISE ISO image contains the supported VMware tools. Upgrading VMware tools through the VMware client user interface is not supported with Cisco ISE. If you want to upgrade any VMware tools to a higher version, support is provided through a newer version of Cisco ISE.

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.

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**.
- Ensure that you change the IP Address and Hostname of the cloned machine before you power it on and connect it to the network.

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 Enter a name for the new machine that you are creating in the Name and Location dialog box 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 on which you want to run the new Cisco ISE VM and click **Next**.

Step 5 Select a datastore for the new Cisco ISE VM that you are creating and click **Next**.

This datastore could be the local datastore on the ESXi server or a remote storage. Ensure that the datastore has enough disk space.

Step 6 Click the **Same format as source** radio button in the Disk Format dialog box and click **Next**.

This option copies the same format that is used in the Cisco ISE VM that you are cloning this new machine from.

Step 7 Click the **Do not customize** radio button in the Guest Customization dialog box and 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 are using vCenter, then you can use a VMware template to clone a Cisco ISE virtual machine (VM). You can clone the Cisco ISE node to a template and use that template to create multiple new Cisco ISE nodes. Cloning a virtual machine using a template is a two-step process:

Before you begin

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

Step 1 Create a Virtual Machine Template, on page 47

Step 2 Deploy a Virtual Machine Template, on page 48

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.

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, you can deploy it on other virtual machines (VMs).

Step 1 Right-click the Cisco 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 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**.

Ensure that this datastore has the required amount of 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 appears.

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

The Virtual Machine Properties page appears.

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

Step 9 Click **Finish**.

You can now power on this Cisco ISE node, configure the IP address and hostname, and connect it to the network.

What to do next

- Change the IP Address and Hostname of a Cloned Virtual Machine
- Connect a Cloned Cisco Virtual Machine to the Network

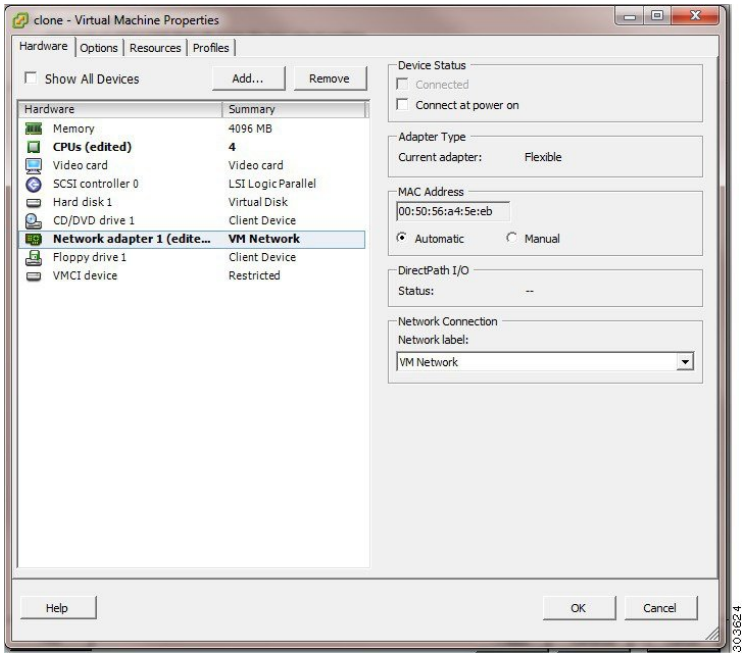
Change the IP Address and Hostname of a Cloned Virtual Machine

After you clone a Cisco ISE virtual machine (VM), you have to power it on and change the IP address and hostname.

Before you begin

- Ensure that the Cisco ISE node is in the standalone state.
- Ensure that the network adapter on the newly cloned Cisco ISE VM is not connected when you power on the machine. Uncheck the **Connected** and **Connect at power on** check boxes. Otherwise, if this node comes up, it will have the same IP address as the source machine from which it was cloned.

Figure 8: Disconnecting the Network Adapter



- Ensure that you have the IP address and hostname that you are going to configure for the newly cloned VM as soon as you power on the machine. This IP address and hostname entry should be in the DNS server. You cannot use "localhost" as the hostname for a node.
- Ensure that you have certificates for the Cisco ISE nodes based on 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
```

The hostname is the new hostname that you are going to configure. The Cisco ISE services are restarted.

Step 4 Enter the following commands:

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

The ip_address is the address that corresponds to the hostname that you entered in step 3 and netmask is the subnet mask of the ip_address. The system will prompt you to restart the Cisco ISE services. See the *Cisco Identity Services Engine CLI Reference Guide*, for the ip address and hostname commands.

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

Connect a Cloned Cisco Virtual Machine to the Network

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

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 from an evaluation system to a fully licensed production system.

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 not that you cannot migrate data to a production VM from a VM created with less than 200 GB of disk space. You can only migrate data from VMs created with 200 GB or more disk space to a production environment.

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 the VM performance at any point of time. The output of this command will be similar to the following:

```
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 for virtual machine resources independent of Cisco ISE installation from the boot menu.

The CLI transcript appears as follows:

```
  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 following 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 be similar to the following:

```
*****
***** 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

KVM virtualization requires virtualization support from the host processor; Intel VT-x for Intel processors and AMD-V for AMD processors. Open a terminal window on the host and enter the **cat /proc/cpuinfo** command. You must see either the vmx or the svm flag.

- 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
 aperfmperf 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 the following 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-2.4.0.x.SPA.x86_64.iso*
--disk=*/home/libvirt-images/kvm-ise1.img,size=100*
--network type=direct,model=virtio,source=*eth2***,source_mode=bridge**

where *ise-2.4.0.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.

Step 1 From the virt-manager, click **New**.

The Create a new virtual machine window appears.

Step 2 Click **Local install media (ISO media or CDROM)**, and then click **Forward**.

Step 3 Click the **Use ISO image** radio button, click **Browse**, and select the ISO image from your local system.

a) Uncheck the **Automatically detect operating system based on install media** check box, choose Linux as the OS type, choose supported Red Hat Enterprise Linux version, and click **Forward**.

Step 4 Choose the RAM and CPU settings and click **Forward**.

Step 5 Check the **Enable storage for this virtual machine** check box and choose the storage settings.

a) Click the **Select managed or other existing storage** radio button.
b) Click **Browse**.
c) From the Storage Pools navigation pane on the left, click **disk FileSystem Directory**.
d) Click **New Volume**.

A Create storage volume window appears.

e) Enter a name for the storage volume.
f) Choose **raw** from the **Format** drop-down list.
g) Enter the Maximum Capacity.
h) Click **Finish**.
i) Choose the volume that you created and click **Choose Volume**.
j) Click **Forward**.

The Ready to begin the installation screen appears.

Step 6 Check the **Customize configuration before install** check box.

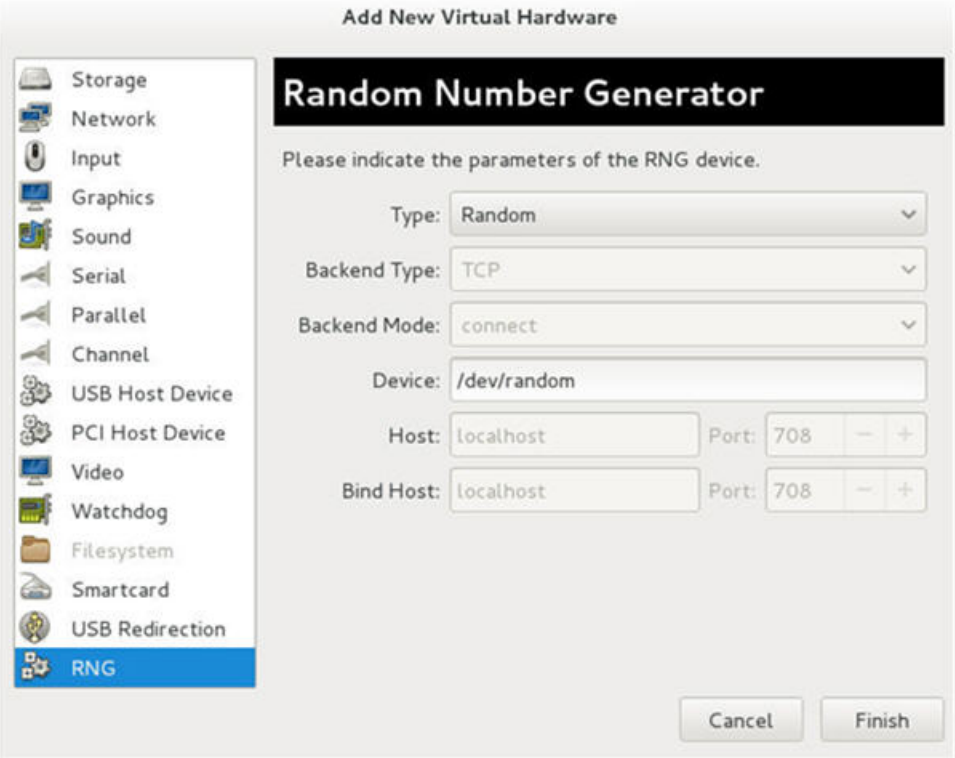
Step 7 Under Advanced options, choose the macvtap as the source for the interface, choose Bridge in the Source mode drop-down list, and click **Finish**.

a) (Optional) Click **Add Hardware** to add additional NICs.

Choose macvtap as the Network source and virtio as the Device model.

b) To support RHEL 7, the KVM virtual manager has to support Random Number Generator (RNG) hardware. See the following image for RNG configuration.

Figure 9: New Virtual Hardware



If you are using the CLI to create a new VM, be sure to include the following setting:

```
<rng model='virtio'
   <backend model='random'>/dev/random</backend>
   <address type='pci' domain='0x0000' bus='0x00' slot='0x08' function='0x0'/>
</rng>
```

c) Click **Finish**.

Step 8 In the Virtual Machine screen, choose the disk device and under **Advanced and Performance Options**, choose the following options, and click **Apply**.

Field	Value
Disk bus	VirtIO
Cache mode	none
IO mode	native

Step 9 Click **Begin Installation** to install Cisco ISE on KVM.
The Cisco ISE installation boot menu appears.

Step 10 At the system prompt, enter **1** to choose a monitor and keyboard port, or **2** to choose a console port, and press **Enter**.

The installer starts the installation of the Cisco ISE software on the VM. When the installation process finishes, the console displays:

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

Step 11 At the system prompt, type **setup** and press **Enter**.
The Setup Wizard appears and guides you through the initial configuration.

Microsoft Hyper-V

Create a Cisco ISE Virtual Machine on Hyper-V

This section describes how to create a new virtual machine, map the ISO image from the local disk to the virtual CD/DVD drive, edit the CPU settings, and install Cisco ISE on Hyper-V.

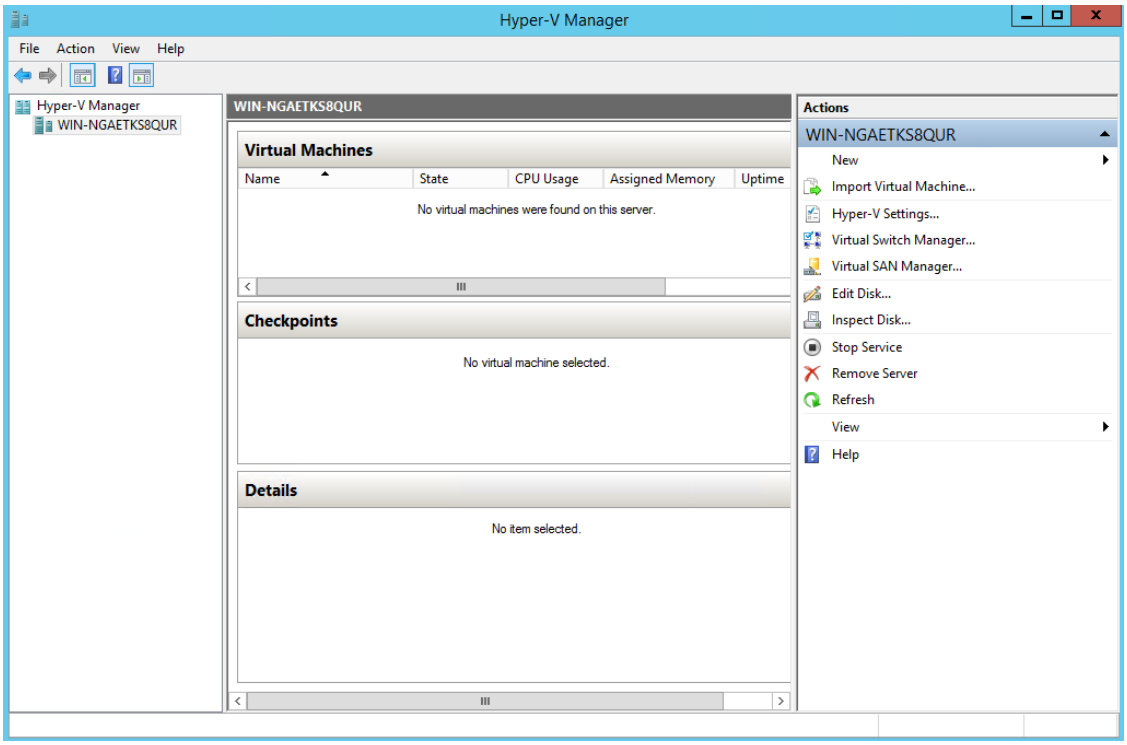
Note Cisco ISE does not support the use of Multipath I/O (MPIO). Hence, the installation will fail if you are using MPIO for the VM.

Before you begin

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

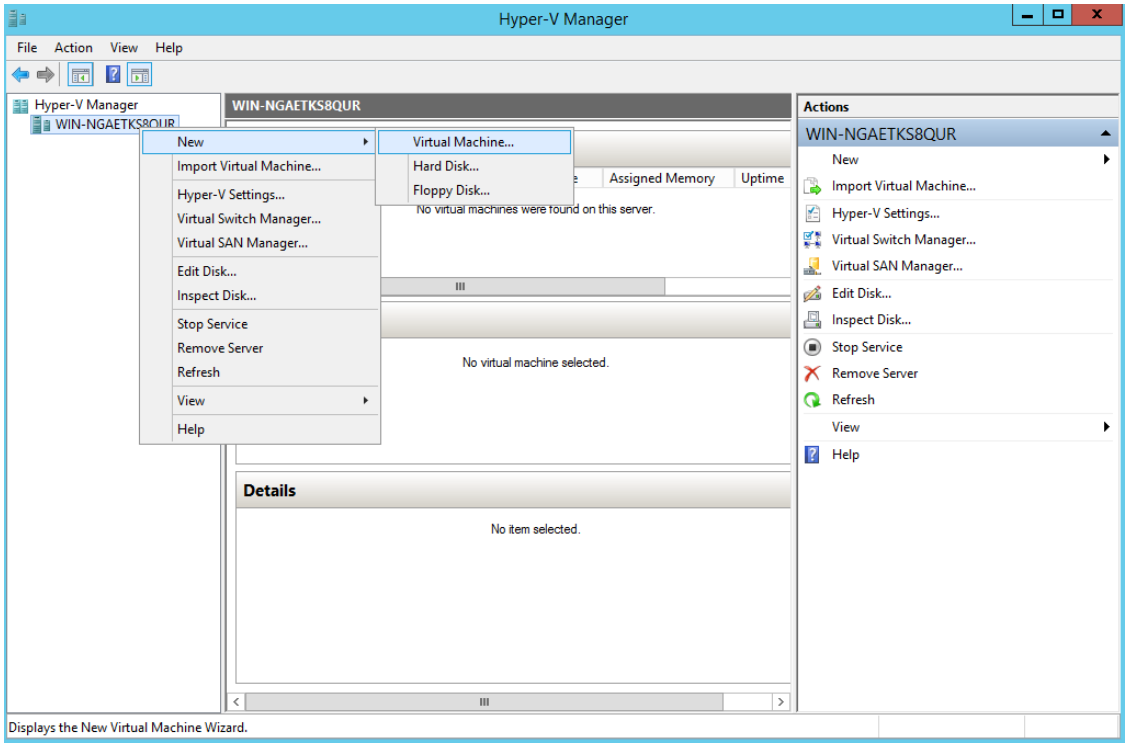
Step 1 Launch Hyper-V Manager on a supported Windows server.

Figure 10: Hyper-V Manager Console



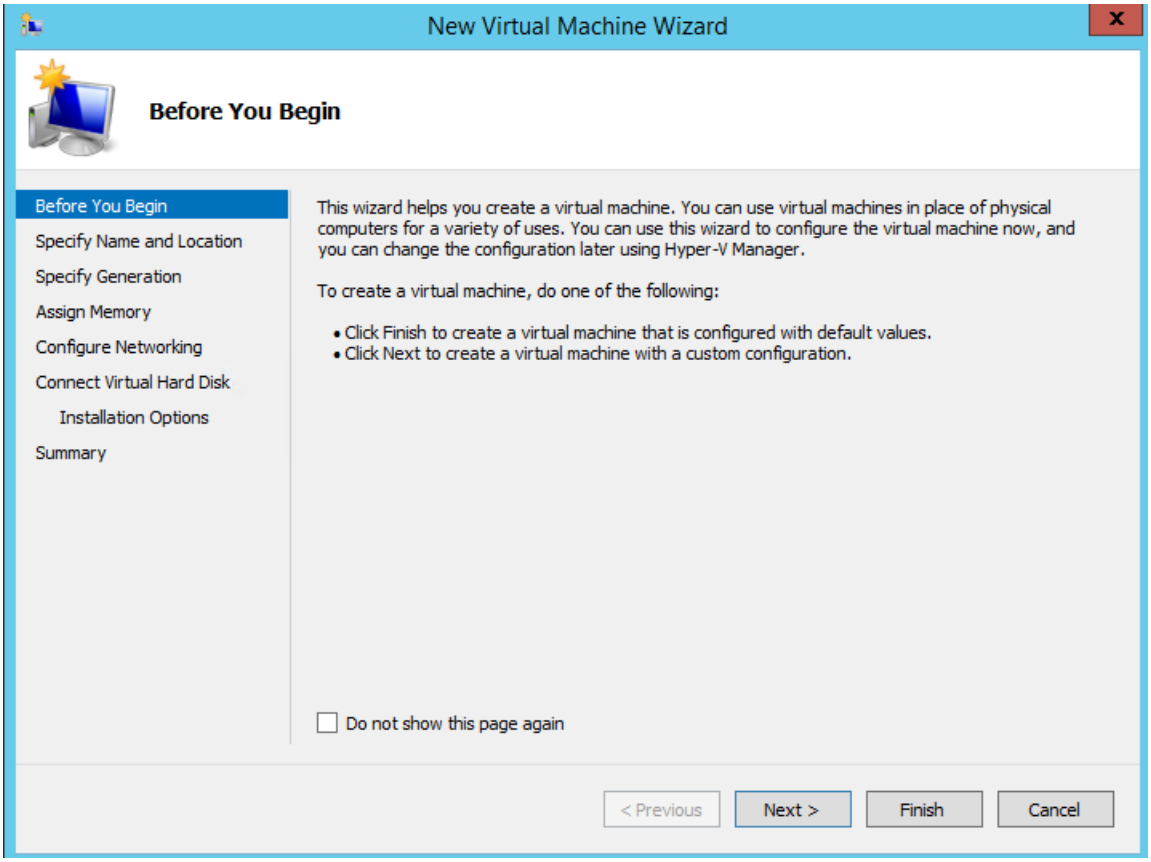
Step 2 Right-click the VM host and click **New** > **Virtual Machine**.

Figure 11: Create New Virtual Machine



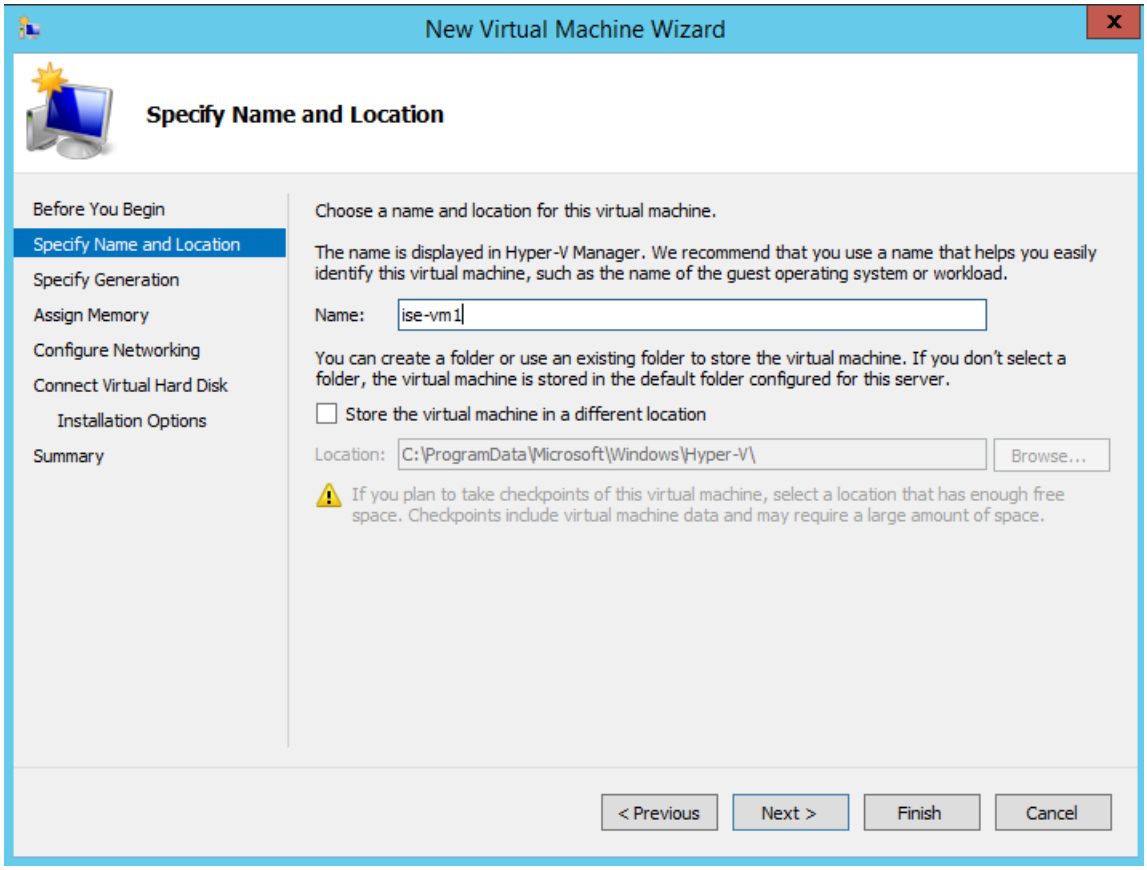
Step 3 Click **Next** to customize the VM configuration.

Figure 12: New Virtual Machine Wizard



Step 4 Enter a name for the VM and (optionally) choose a different path to store the VM, and click **Next**.

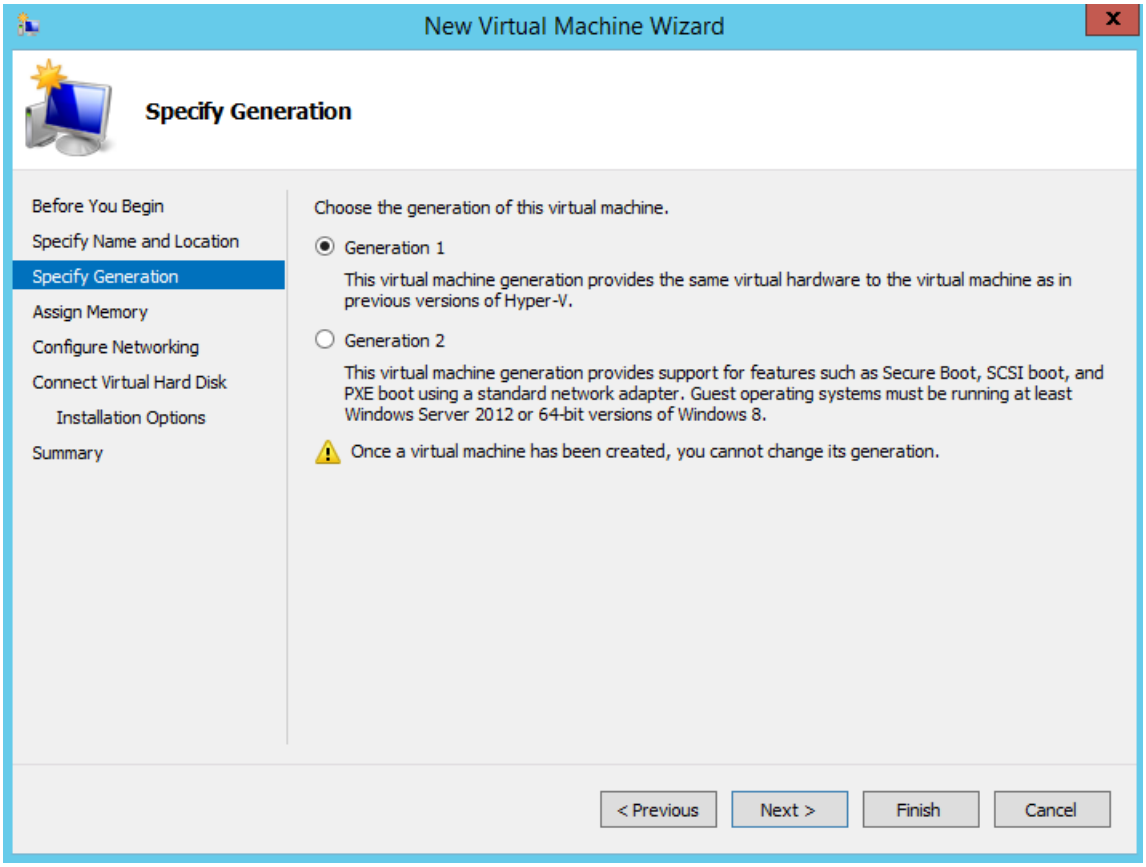
Figure 13: Specify Name and Location



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

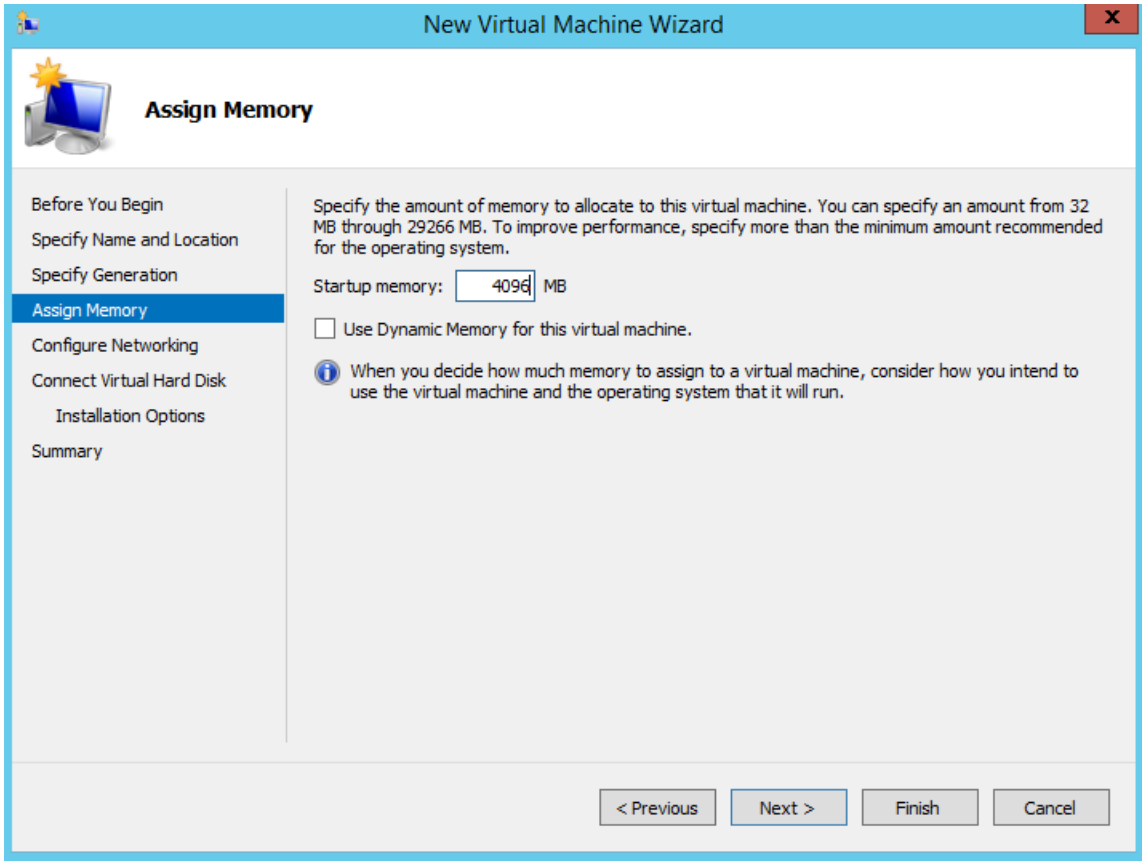
If you choose to create a Generation 2 ISE VM, ensure that you disable the **Secure Boot** option in the VM settings.

Figure 14: Specify Generation



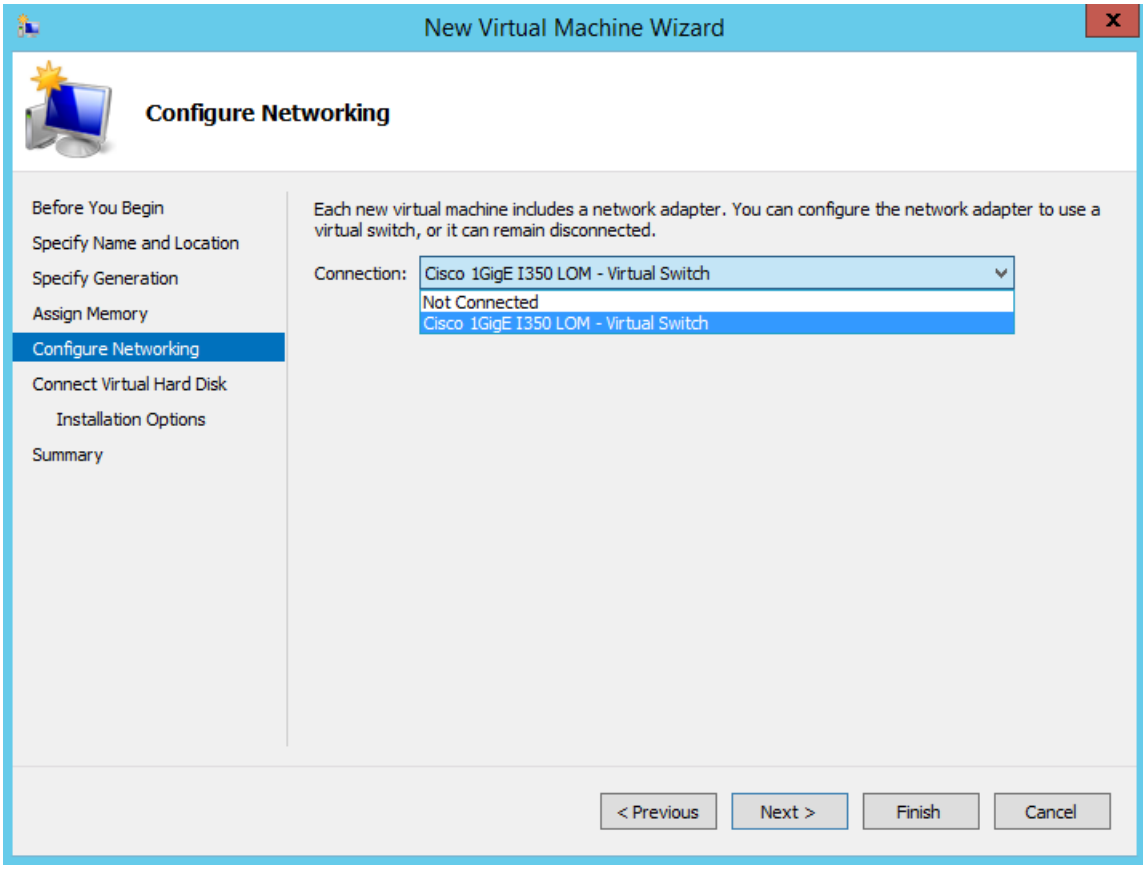
Step 6 Specify the amount of memory to allocate to this VM, for example, 16000 MB, and click **Next**.

Figure 15: Assign Memory



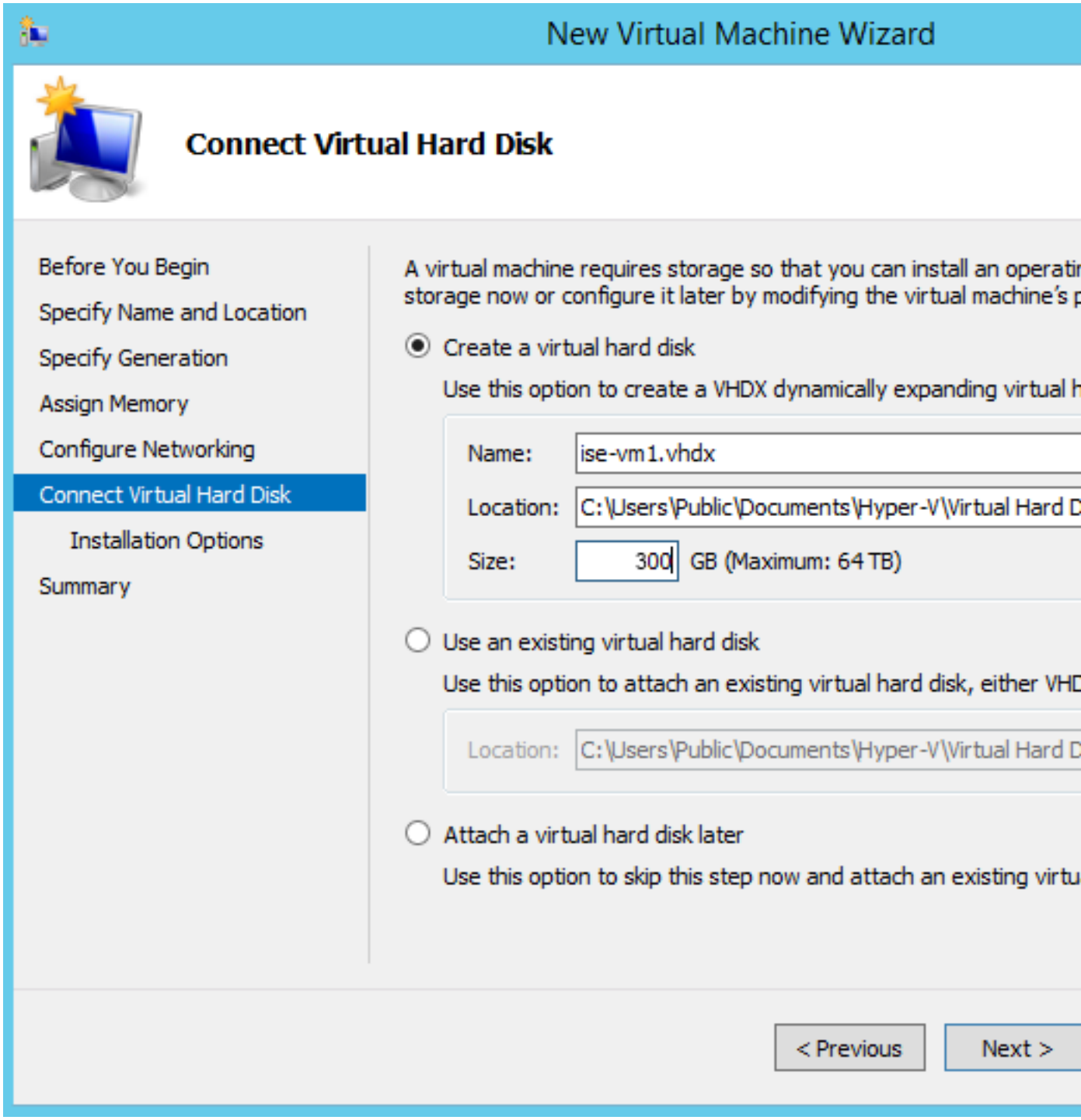
Step 7 Select the network adapter and click **Next**.

Figure 16: Configure Networking



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

Figure 17: Connect Virtual Hard Disk

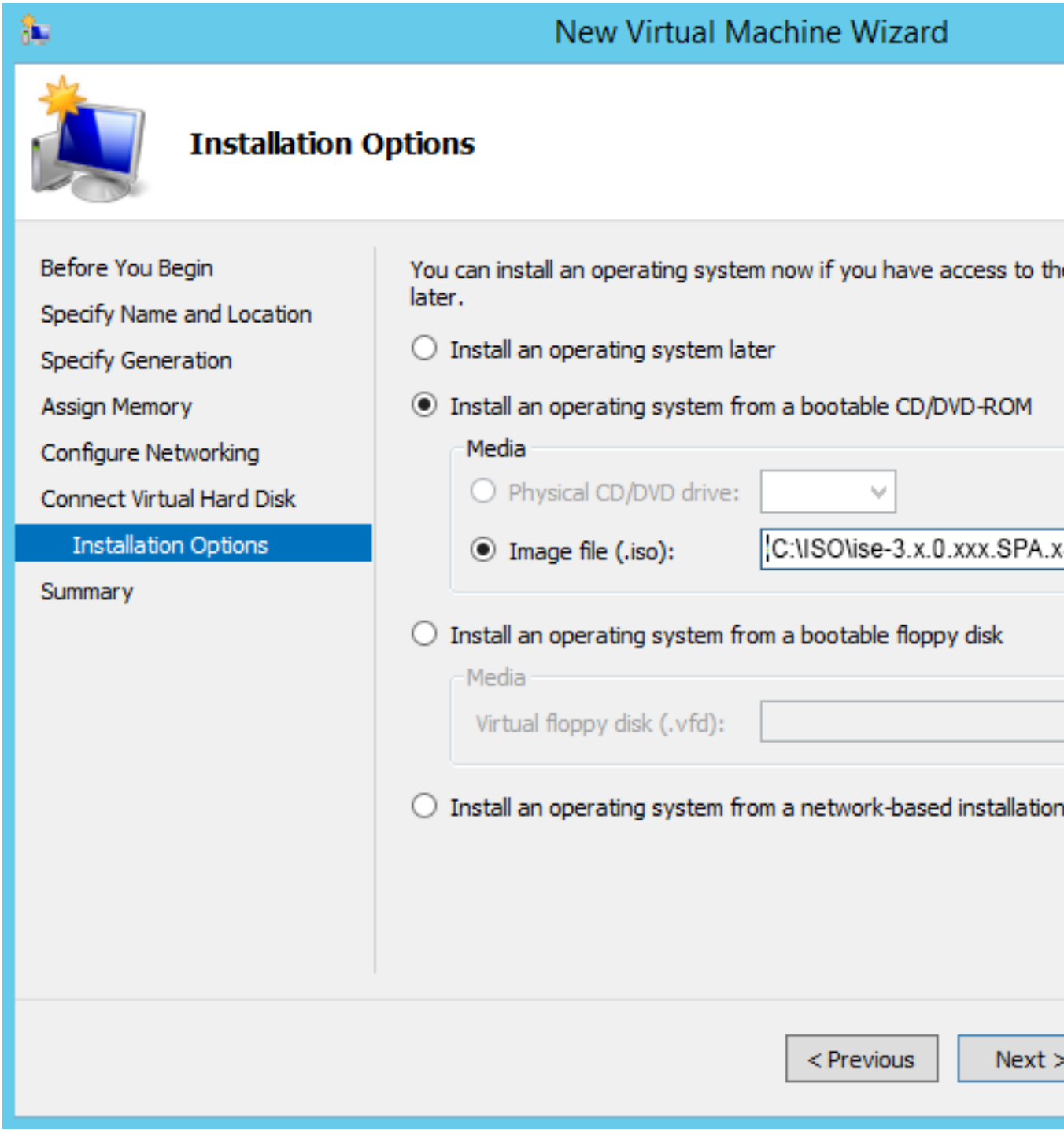


Step 9 Click the **Install an operating system from a bootable CD/DVD-ROM** radio button.

a) From the Media area, click the **Image file (.iso)** radio button.

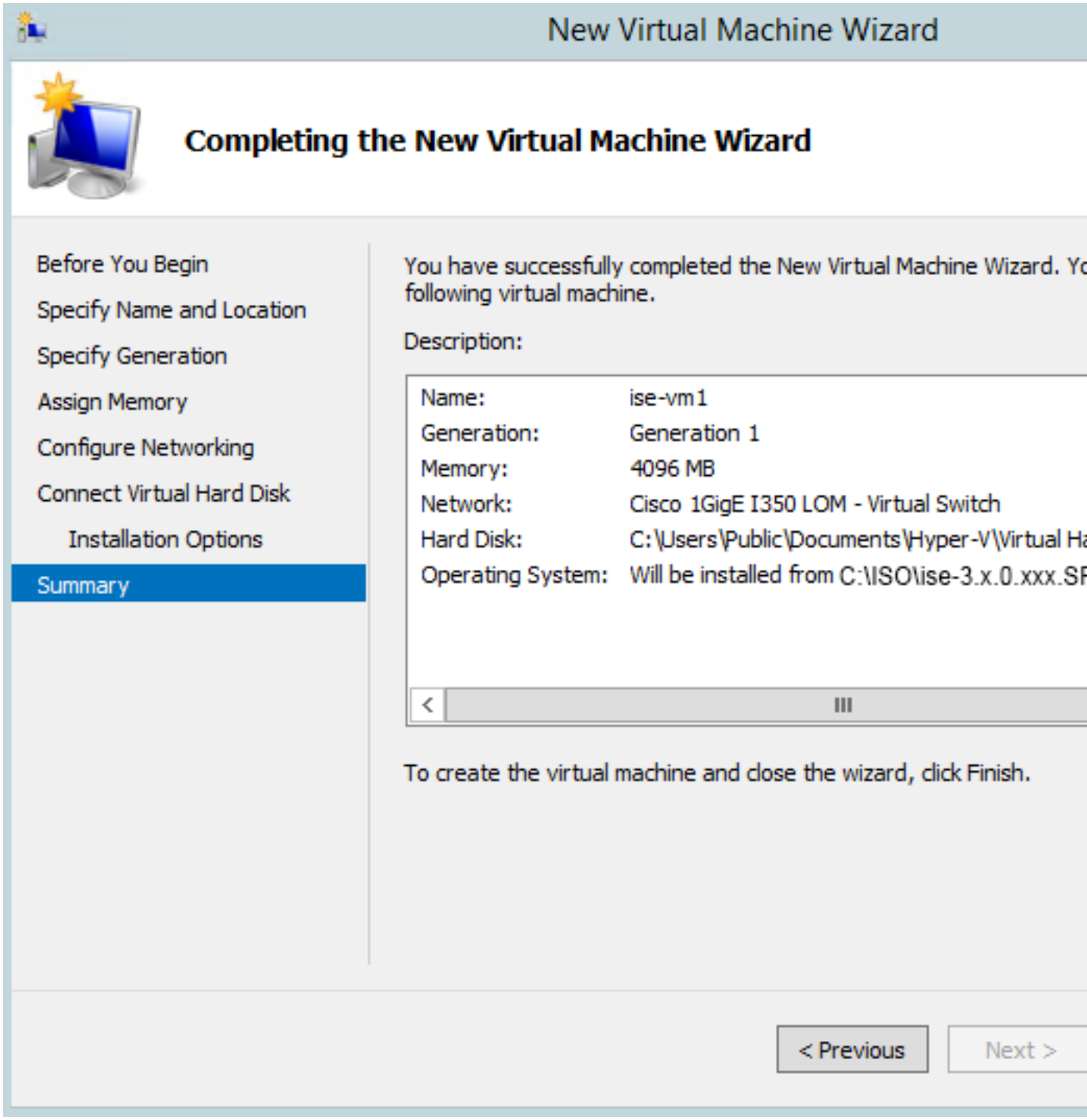
b) Click **Browse** to select the ISE ISO image from the local system and click **Next**.

Figure 18: Installation Options



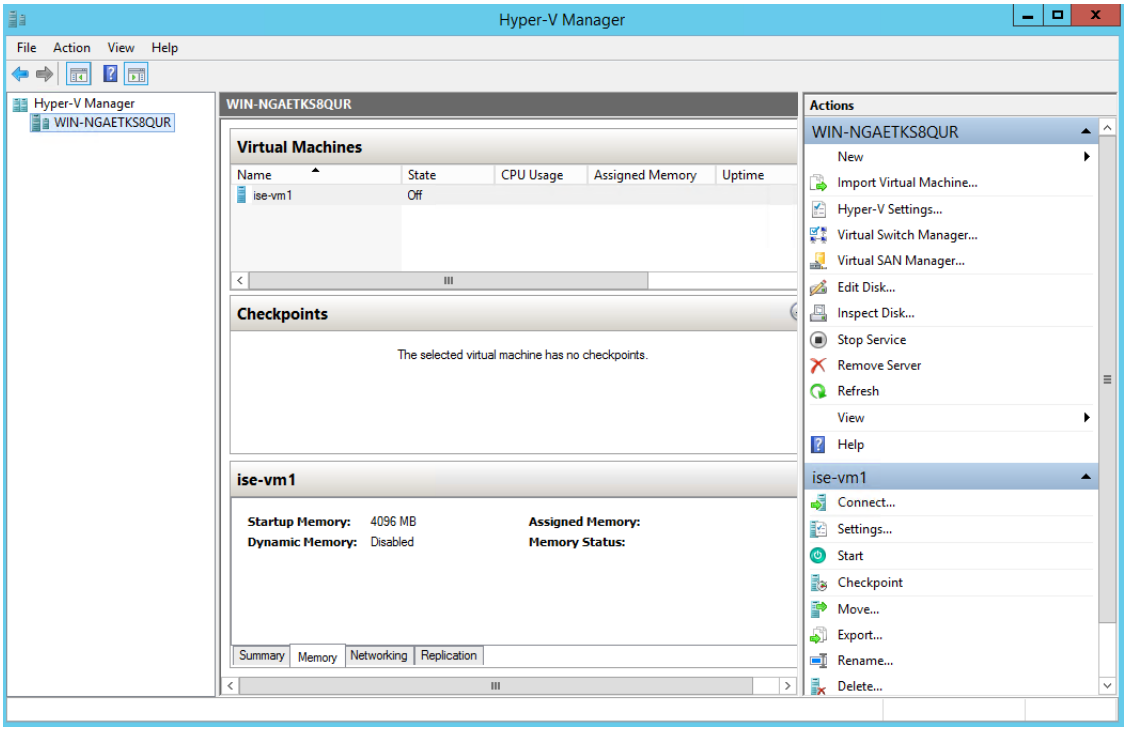
Step 10 Click **Finish**.

Figure 19: Complete the New Virtual Machine Wizard



The Cisco ISE VM is created on Hyper-V.

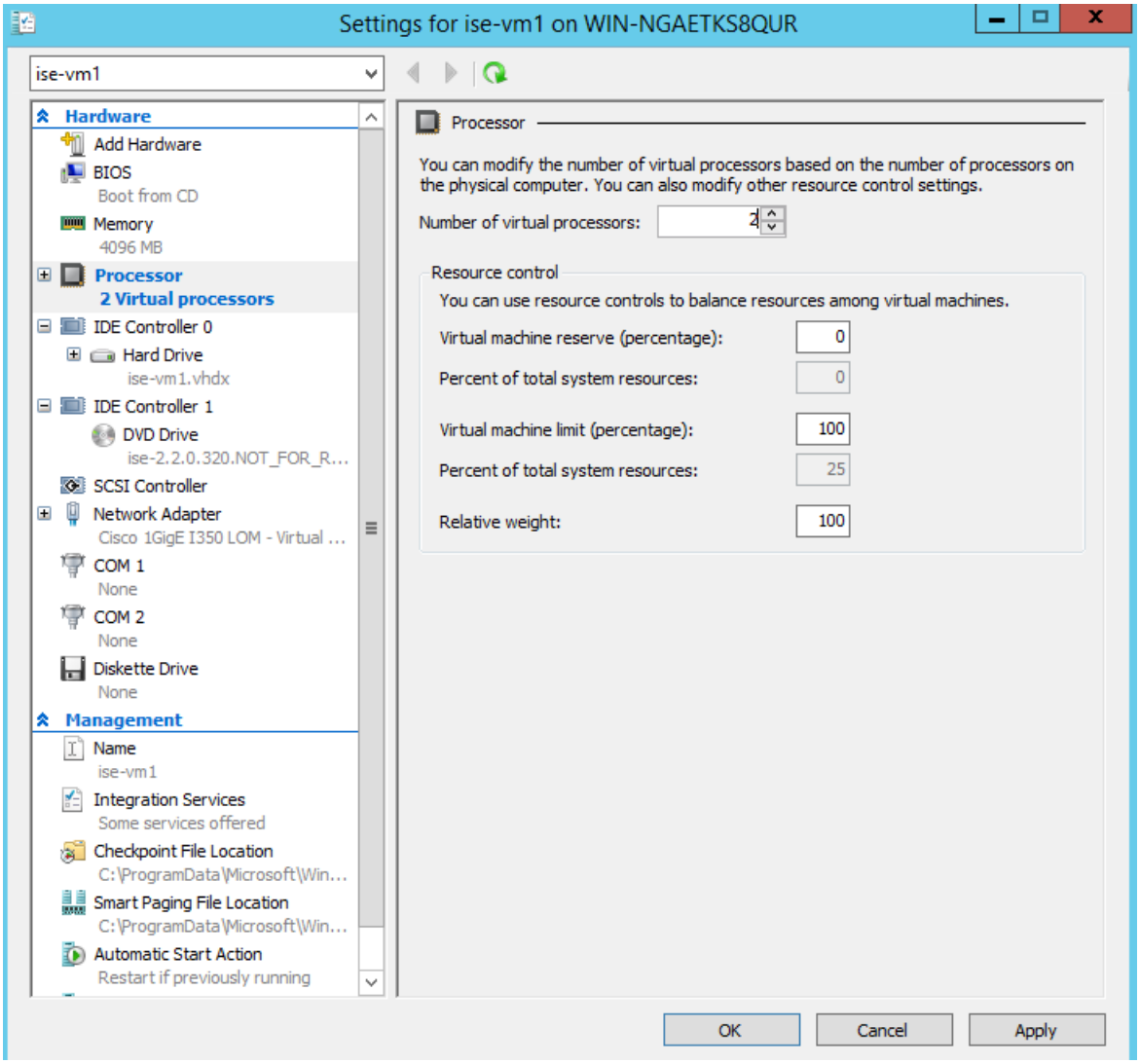
Figure 20: New Virtual Machine created



Step 11 Select the VM and edit the VM settings.

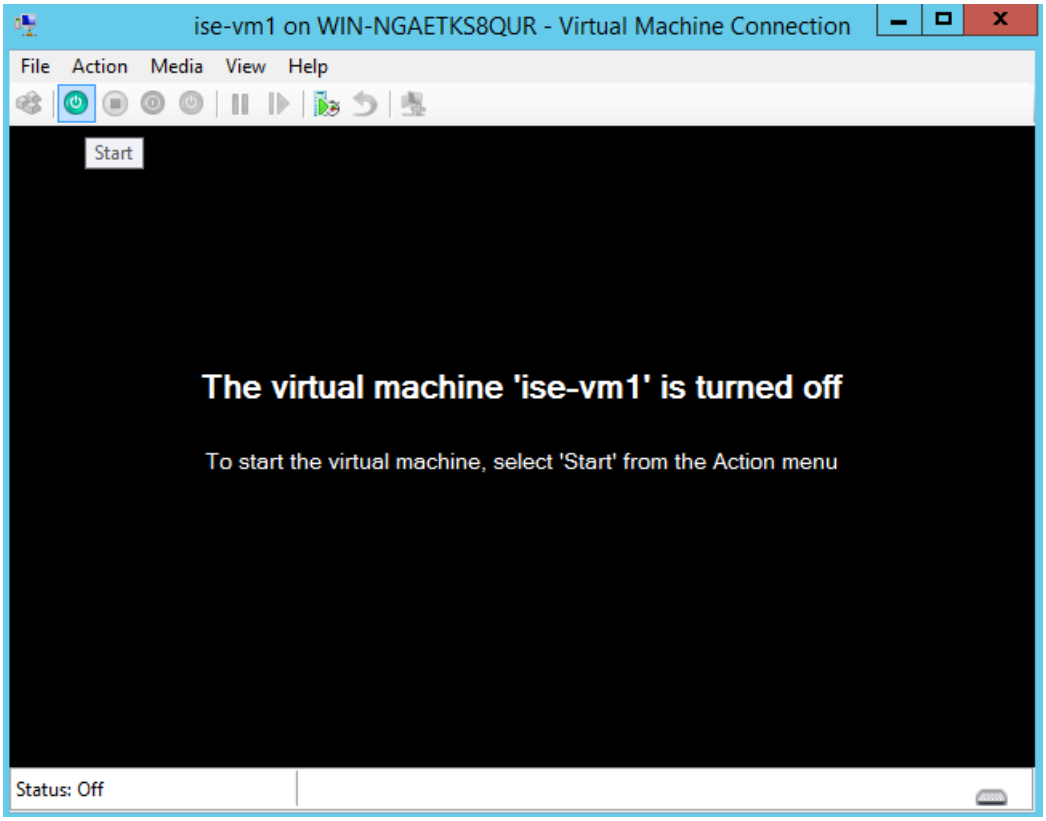
a) Select **Processor**. Enter the number of virtual processors, for example, 6, and click **OK**.

Figure 21: Edit VM Settings



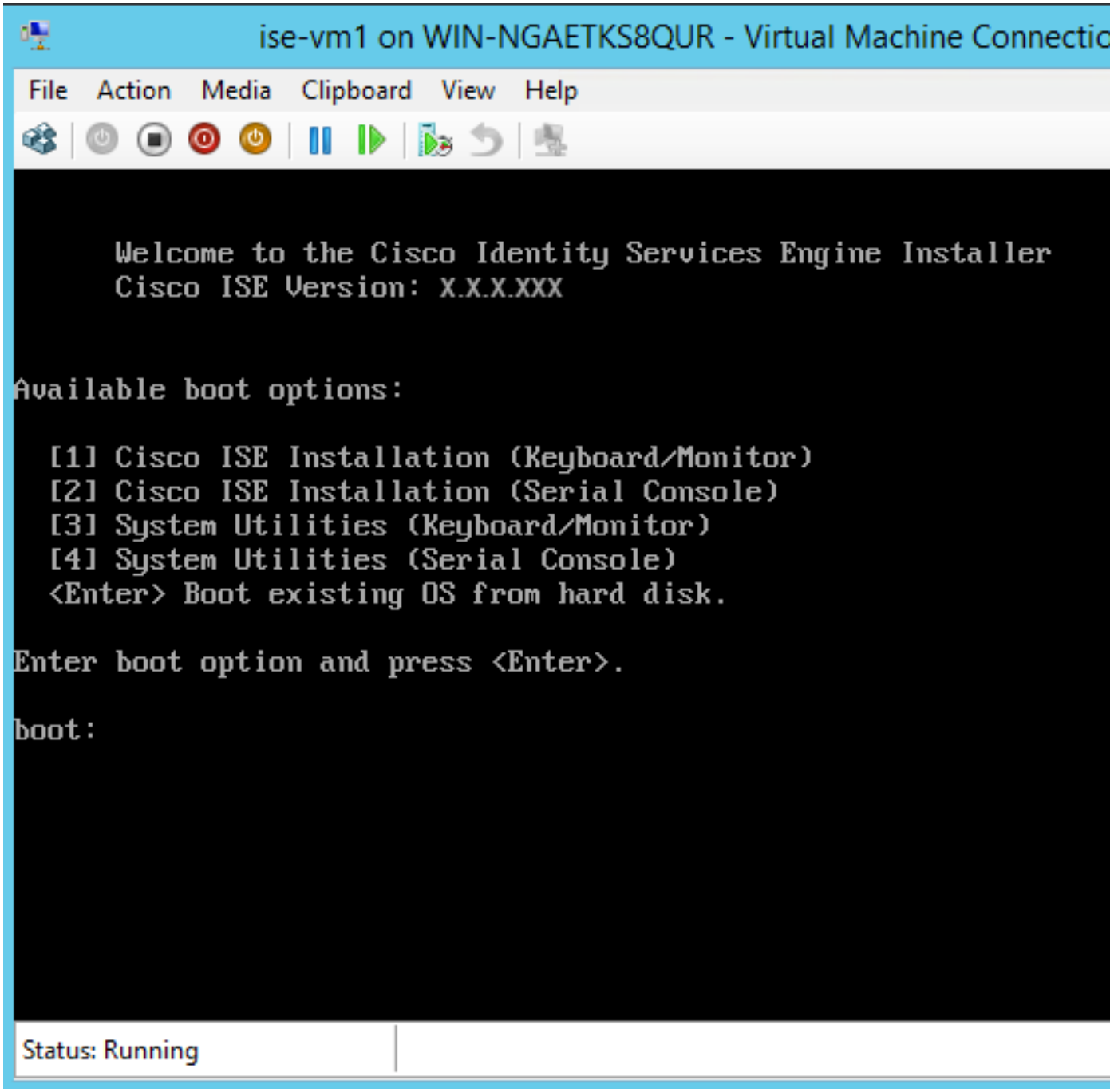
Step 12 Select the VM and click **Connect** to launch the VM console. Click the start button to turn on the Cisco ISE VM.

Figure 22: Start the Cisco ISE VM

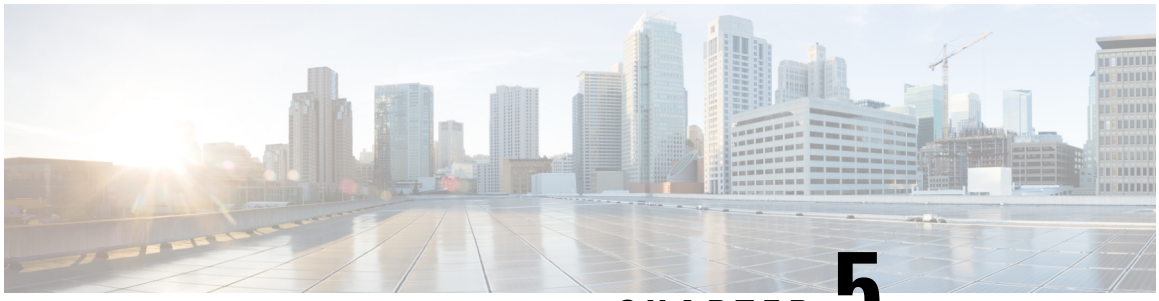


The Cisco ISE installation menu appears.

Figure 23: CIsco ISE installation menu



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



CHAPTER 5

Installation Verification and Post-Installation Tasks

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 will be using the preinstalled Evaluation license.

Note We recommend that you use the Cisco ISE user interface to periodically reset your administrator login password.

Caution For security reasons, we recommend that you log out when you complete your administrative session. If you do not log out, the Cisco ISE web-based web interface logs you out after 30 minutes of inactivity, and does not save any unsubmitted configuration data.

For information about the validated browsers, see "Validated Browsers" section in the Cisco ISE Release Notes.

Note 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.

Step 1 After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

Step 2 In the Address field, enter the IP address (or hostname) of the Cisco ISE appliance by using the following format and press **Enter**.

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

Step 3 Enter a username and password that you defined during setup.

Step 4 Click **Login**.

Differences Between CLI Admin and Web-Based Admin Users Tasks

The username and password that you configure when using the Cisco ISE setup program are intended to be used for administrative access to the Cisco ISE CLI and the Cisco ISE web interface. The administrator that has access to the Cisco ISE CLI is called the CLI-admin user. By default, the username for the CLI-admin user is admin and the password is user-defined during the setup process. There is no default password.

You can initially access the Cisco ISE web interface by using the CLI-admin user's username and password that you defined during the setup process. There is no default username and password for a web-based admin.

The CLI-admin user is *copied* to the Cisco ISE web-based admin user database. Only the first CLI-admin user is copied as the web-based admin user. You should keep the CLI- and web-based admin user stores synchronized, so that you can use the same username and password for both admin roles.

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

Table 13: Tasks Performed by CLI-Admin and Web-Based Admin Users

Admin User Type	Tasks
Both CLI-Admin and Web-Based Admin	• Back up the 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	• Start and stop the Cisco ISE application software. • Reload or shut down the Cisco ISE appliance. • Reset the web-based admin user in case of a lockout. • Access the ISE CLI.

Create a CLI Admin

Cisco ISE allows you to create additional CLI-admin user accounts other than the one you created during the setup process. To protect the CLI-admin user credentials, create the minimum number of CLI-admin users needed to access the Cisco ISE CLI.

You can add the CLI-admin user by using the following command in the configuration mode:

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

Create a Web-Based Admin

For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

To add an admin user:

1. Choose **Administration > System > Admin Access > Administrators > Admin Users**.
2. Choose **Add > Create an Admin User**.
3. Enter the name, password, admin group, and the other required details.
4. Click **Submit**.

Reset a Disabled Password Due to Administrator Lockout

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. The navigation path for this window is **Operations** > **Reports** > **Reports** > **Audit** > **Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

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 previous two passwords that were used for this administrator ID:

```
Enter new password:
Confirm new password:

Password reset successfully
```

Cisco ISE Configuration Verification

There are two methods that each use a different set of username and password credentials for verifying Cisco ISE configuration by using a web browser and CLI.

Note A CLI-admin user and a web-based admin user credentials are different in Cisco ISE.

Verify Configuration Using a Web Browser

Step 1 After the Cisco ISE appliance reboot has completed, launch one of the supported web browsers.

Step 2 In the **Address** field, enter the IP address (or host name) of the Cisco ISE appliance using the following format and press **Enter**.

Step 3 In the Cisco ISE Login page, enter the username and password that you have defined during setup and click **Login**.

For example, entering https://10.10.10.10/admin/ displays the Cisco ISE Login page.

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

Note For first-time web-based access to Cisco ISE system, the administrator username and password is the same as the CLI-based access that you configured during setup.

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

What to do next

By using the Cisco ISE web-based user interface menus and options, you can configure the Cisco ISE system to suit your needs. For details on configuring Cisco ISE, see *Cisco Identity Services Engine Administrator Guide*.

Verify Configuration Using the CLI

Before you begin

Download and install the latest Cisco ISE patch to keep Cisco ISE up-to-date.

Step 1 After the Cisco ISE appliance reboot has completed, launch a supported product, such as PuTTY, for establishing a Secure Shell (SSH) connection to a Cisco ISE appliance.

Step 2 In the Host Name (or IP Address) field, enter the hostname (or the IP address in dotted decimal format of the Cisco ISE appliance) and click **Open**.

Step 3 At the login prompt, enter the CLI-admin username (admin is the default) that you configured during setup and press **Enter**.

Step 4 At the password prompt, enter the CLI-admin password that you configured during setup (this is user-defined and there is no default) and press **Enter**.

Step 5 At the system prompt, enter **show application version ise** and press **Enter**.

Note The Version field lists the currently installed version of Cisco ISE software.

The console output appears as shown below:

```
ise/admin# show application version ise
```

```
Cisco Identity Services Engine
------------------------------------------
Version      : 2.4.0.226
Build Date   : Fri Nov 24 17:36:37 2017
Install Date : Thu Nov 30 21:40:54 2017
```

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 below:

```
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
```

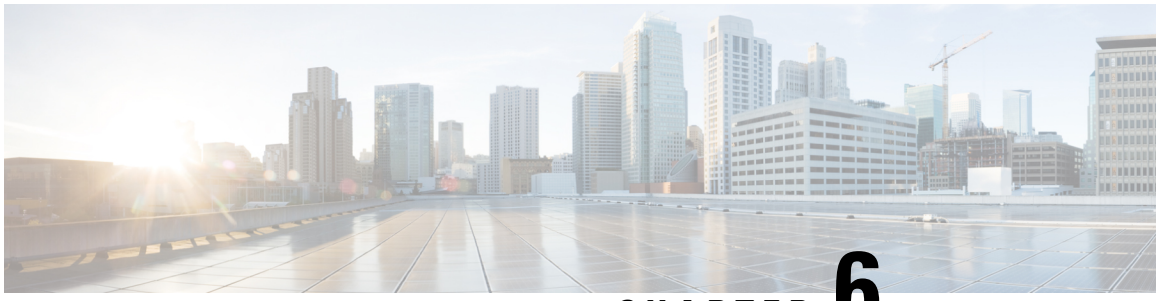
List of Post-Installation Tasks

After you install Cisco ISE, you must perform the following mandatory tasks:

Table 14: Mandatory Post-Installation Tasks

Task	Link in the Administration Guide
Apply the latest patches, if any	Install a Software Patch
Install Licenses	See the Cisco ISE Ordering Guide for more information. See the Administration Guide for information on how to Register Licenses.

Task	Link in the Administration Guide
Install Certificates	See the Manage Certificates chapter of the Cisco ISE Administration Guide for more details.
Create Repository for Backups	See the Create Repositories section of the Cisco ISE Administration Guide for more details.
Configure Backup Schedules	See the Schedule a Backup section of the Cisco ISE Administration Guide for more details.
Deploy Cisco ISE personas	See the Set Up Cisco ISE in a Distributed Environment chapter of the Cisco ISE Administration Guide.



CHAPTER 6

Common System Maintenance Tasks

Bond Ethernet Interfaces for High Availability

Cisco ISE supports bonding of two Ethernet interfaces into a single virtual interface to provide high availability for the physical interfaces. This feature is called Network Interface Card (NIC) bonding or NIC teaming. When two interfaces are bonded, the two NICs appear to be a single device with a single MAC address.

The NIC bonding feature in Cisco ISE does not support load balancing or link aggregation features. Cisco ISE supports only the high availability feature of NIC bonding.

The bonding of interfaces ensures that Cisco ISE services are not affected when there is:

- Physical interface failure
- Loss of switch port connectivity (shut or failure)
- Switch line card failure

When two interfaces are bonded, one of the interfaces becomes the primary interface and the other becomes the backup interface. When two interfaces are bonded, all traffic normally flows through the primary interface. If the primary interface fails for some reason, the backup interface takes over and handles all the traffic. The bond takes the IP address and MAC address of the primary interface.

When you configure the NIC bonding feature, Cisco ISE pairs fixed physical NICs to form bonded NICs. The following table outlines which NICs can be bonded together to form a bonded interface.

Table 15: 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	
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

The NIC bonding feature is supported on all supported platforms and node personas. The supported platforms include:

- SNS hardware appliances - Bond 0, 1, and 2
- VMware virtual machines - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)
- Linux KVM nodes - Bond 0, 1, and 2 (if six NICs are available to the virtual machine)

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. The following procedure explains how you can configure bond 0 between Eth0 and Eth1 interfaces.

Before you begin

If a physical interface that acts as a backup interface (for example, Eth1, Eth3, Eth5 interfaces), is configured with an IP address, you must remove the IP address from the backup interface. The backup interface should not be assigned an IP address.

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**.

Bond 0 is now configured. Cisco ISE restarts automatically. Wait for some time to ensure that all the services are up and running successfully. Enter the **show application status ise** command from the CLI to check if 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)# 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 the following:

```
!
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 above, "backup interface GigabitEthernet 1" indicates that NIC bonding is configured on Gigabit Ethernet 0, with Gigabit Ethernet 0 being the primary interface and Gigabit Ethernet 1 being the backup interface. Also, the ADE-OS configuration does not display an IP address on the backup interface in the running config, even though the primary and backup interfaces effectively have the same IP address.

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

```
ise/admin# show interface
bond0: flags=5187<UP,BROADCAST,RUNNING,MASTER,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,SLAVE,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,SLAVE,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

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 for some time to ensure that all the services are up and running successfully. Enter the **show application status ise** command from the CLI to check if 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

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a keyboard and video monitor connection and a serial console connection.
- You have a keyboard and video monitor connection to the Cisco ISE appliance (this can be either a remote keyboard and a video monitor connection or a VMware vSphere client console connection).
- You have a serial console connection to the Cisco ISE appliance.

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

Step 2 Insert the Cisco ISE Software DVD.

For example, the Cisco ISE 3515 console displays the following message:

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

Note You must use ise-2.6.0.156.SPA.x86_64.iso for Cisco SNS 3600 series appliance with Cisco ISE 2.4. You must not use ise-2.4.0.357.SPA.x86_64_SNS-36x5_APPLIANCE_ONLY.iso.

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 utilities menu as shown below.

```
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 abort 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 corresponding to 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

An administrator can enter an incorrect password enough times to disable the account. The minimum and default number of attempts is five.

Use these instructions to reset the administrator user interface password with the **application reset-passwd ise** command in the Cisco ISE CLI. It does not affect the CLI password of the administrator. After you successfully reset the administrator password, the credentials are immediately active and you can log in without having to reboot the system. .

Cisco ISE adds a log entry in the **Administrator Logins** window. The navigation path for this window is **Operations** > **Reports** > **Reports** > **Audit** > **Administrator Logins**. The credentials for that administrator ID is suspended until you reset the password associated with that administrator ID.

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 previous two passwords that were used for this administrator ID:

```
Enter new password:
Confirm new password:

Password reset successfully
```

Return Material Authorization

In case of a Return Material Authorization (RMA), if you are replacing individual components on an SNS server, be sure to reimage the appliance before you install Cisco ISE. Contact Cisco TAC for assistance.

Change the IP Address of a Cisco ISE Appliance

Before you begin

- Ensure that the Cisco ISE node is in a standalone state before you change the IP address. If the node is part of a distributed deployment, deregister the node from the deployment and make it a standalone node.
- Do not use the **no ip address** command when you change the Cisco ISE appliance IP address.

Step 1 Log in to the Cisco ISE CLI.

Step 2 Enter the following commands:

a) **configure terminal**

b) **interface GigabitEthernet 0**

c) **ip address new_ip_address new_subnet_mask**

The system prompts you for the IP address change. Enter **Y**. A screen similar to the following one 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.
```

Cisco ISE prompts you to restart the system.

Step 3 Enter **Y** to restart the system.

View Installation and Upgrade History

Cisco ISE provides a Command Line Interface (CLI) command to view the details of installation, upgrade, and uninstallation of Cisco ISE releases and patches. The **show version history** command provides the following details:

- Date—Date and time at which the installation or uninstallation was performed
- Application—Cisco ISE application
- Version—Version that was installed or removed.
- Action—Installation, Uninstallation, Patch Installation, or Patch Uninstallation
- Bundle Filename—Name of the bundle that was installed or removed
- Repository—Repository from which the Cisco ISE application bundle was installed. Not applicable for uninstallation.

Step 1 Log in to the Cisco ISE CLI.

Step 2 Enter the following command: **show version history**.

The following output appears:

```
ise/admin# show version history
-------------------------------------------
Install Date: Thu Nov 30 21:48:58 UTC 2017
Application: ise
Version: 2.4.0.226
Install type: Application Install
Bundle filename: ise.tar.gz
Repository: SystemDefaultPkgRepos

ise/admin#
```

Perform a System Erase

You can perform a system erase to securely erase all information from your Cisco ISE appliance or VM. This option to perform a system erase ensures that Cisco ISE is compliant with the NIST Special Publication 800-88 data destruction standards.

Before you begin

Make sure you understand the following connection-related conditions that can cause a problem when attempting to use the Cisco ISE Software DVD to start up a Cisco ISE appliance:

- You have a terminal server associated with the serial console connection to the Cisco ISE appliance that is set to exec. Setting it to *no exec* allows you to use a KVM connection and a serial console connection.

- You have a keyboard and video monitor (KVM) connection to the Cisco ISE appliance (this can be either a remote KVM or a VMware vSphere client console connection).
- You have a serial console connection to the Cisco ISE appliance.

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

Step 2 Insert the Cisco ISE Software DVD.

For example, the Cisco ISE 3515 console displays the following message:

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

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

The system displays the ISO utilities menu as shown below:

```
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 you with another warning:

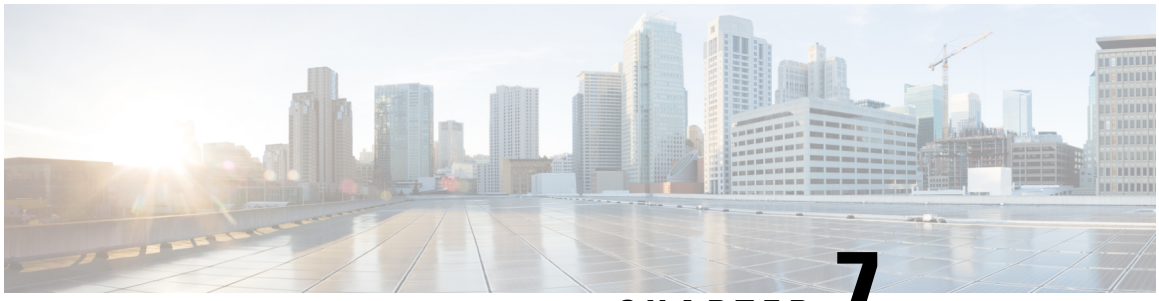
```
THIS IS YOUR LAST CHANGE TO ABORT. PROCEED WITH SYSTEM ERASE? [Y/N] Y
```

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.
```

After you perform a system erase, if you want to reuse the appliance, you must 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

Table 16: Ports Used by All Nodes

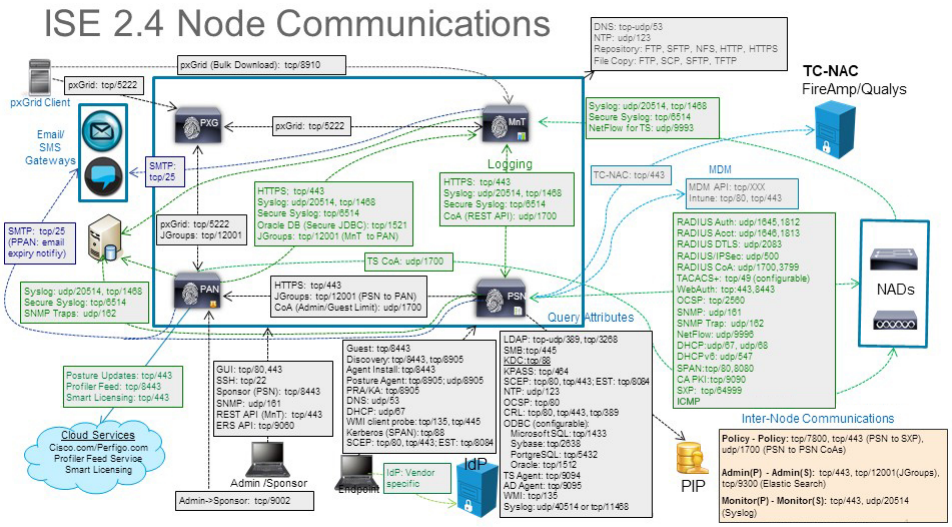
Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Replication and Synchronization	• HTTPS (SOAP): TCP/443 • Data Synchronization/ Replication (JGroups): TCP/12001 (Global) • ISE Messaging Service: SSL: TCP/8671	—

Cisco ISE Infrastructure

This appendix lists the TCP and User Datagram Protocol UDP ports that Cisco ISE uses for intranetwork communications with external applications and devices. The Cisco ISE ports listed in this appendix must be open on the corresponding firewall.

Keep in mind the following information when configuring services on a Cisco ISE network:

- The ports are enabled based on the services that are enabled in your deployment. Apart from the ports that are opened by the services running in ISE, Cisco ISE denies access to all other ports.
- Cisco ISE management is restricted to Gigabit Ethernet 0.
- RADIUS listens on all network interface cards (NICs).
- Cisco ISE server interfaces do not support VLAN tagging. If you are installing on a hardware appliance, ensure that you disable VLAN trunking on switch ports that are used to connect to Cisco ISE nodes and configure them as access layer ports.
- The ephemeral port range is from 10000 to 65500. This remains the same for Cisco ISE, Release 2.1 and later.
- All NICs can be configured with IP addresses.
- The policy information point represents the point at which external information is communicated to the Policy Service persona. For example, external information could be a Lightweight Directory Access Protocol (LDAP) attribute.



Related Concepts

Node Types and Personas in Distributed Deployments, on page 3

Note TCP keep alive time on ISE is 60 minutes. Adjust the TCP timeout values accordingly on the firewall if one exists between ISE nodes.

Operating System Ports

The following table lists the TCP ports that NMAP uses for OS scanning. In addition, NMAP uses ICMP and UDP port 51824.

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
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

The following table lists the ports used by the Administration nodes:

Table 17: Ports Used by the Administration Nodes

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)
Administration	• HTTP: TCP/80, HTTPS: TCP/443 (TCP/80 redirected to TCP/443; not configurable) • SSH Server: TCP/22 • CoA • External RESTful Services (ERS) REST API: TCP/9060 • • To manage guest accounts from Admin GUI: TCP/9002 • ElasticSearch (Context Visibility; to replicate data from primary to secondary Admin node): TCP/9300 **Note** Ports 80 and 443 support Admin web applications and are enabled by default. HTTPS and SSH access to Cisco ISE is restricted to Gigabit Ethernet 0. TCP/9300 must be open on both Primary and Secondary Administration Nodes for incoming traffic.	—
Monitoring	• SNMP Query: UDP/161 **Note** This port is route table dependent. • ICMP	
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces (Gigbit Ethernet 1 through 5, or Bond 1 and 2)

External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications:
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88
	  • KPASS: TCP/464
	• WMI : TCP/135
	• ODBC:
	Note The ODBC ports are configurable on the third-party database server.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	

Email	Guest account and user password expirations email notification: SMTP: TCP/25	
Smart Licensing	Connection to Cisco cloud over TCP/443	

Cisco ISE Monitoring Node Ports

The following table lists the ports used by the Monitoring nodes:

Table 18: Ports Used by the Monitoring 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)
Administration	• HTTP: TCP/80, HTTPS: TCP/443 • SSH Server: TCP/22	—
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 **Note** This port is route table dependent. • ICMP	
Logging	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SMTP: TCP/25 for email of alarms • SNMP Traps: UDP/162	

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)

External Identity Sources and Resources (Outbound)	• Admin User Interface and Endpoint Authentications:
	  • LDAP: TCP/389, 3268, UDP/389
	  • SMB: TCP/445
	  • KDC: TCP/88, UDP/88
	  • KPASS: TCP/464
	• WMI : TCP/135
	• ODBC:
	Note The ODBC ports are configurable on the third-party database server.
	  • Microsoft SQL: TCP/1433
	  • Sybase: TCP/2638
	  • PortgreSQL: TCP/5432
	  • Oracle: TCP/1521, 15723, 16820
	• NTP: UDP/123
	• DNS: UDP/53, TCP/53
	Note For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	

Bulk Download for pxGrid	SSL: TCP/8910	

Cisco ISE Policy Service Node Ports

Cisco ISE supports HTTP Strict Transport Security (HSTS) for increased security. Cisco ISE sends HTTPS responses indicating to browsers that ISE can only be accessed using HTTPS. If users then try to access ISE using HTTP instead of HTTPS, the browser changes the connection to HTTPS before generating any network traffic. This functionality prevents browsers from sending requests to Cisco ISE using unencrypted HTTP before the server can redirect them.

The following table lists the ports used by the Policy Service nodes:

Table 19: 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	• HTTP: TCP/80, HTTPS: TCP/443 • SSH Server: TCP/22 • OCSP: TCP/2560	Cisco ISE management is restricted to Gigabit Ethernet 0.
Clustering (Node Group)	Node Groups/JGroups: TCP/7800	—
SCEP	TCP/9090	—
IPSec/ISAKMP	UDP/500	—
Device Administration	TACACS+: TCP/49 **Note** This port is configurable in Release 2.1 and later releases.	
TrustSec	Use HTTP and Cisco ISE REST API to transfer TrustSec data to network devices over port 9063.	
SXP	• PSN (SXP node) to NADs: TCP/64999 • PSN to SXP (inter-node communication): TCP/9644	
TC-NAC	TCP/443	
Monitoring	Simple Network Management Protocol [SNMP]: UDP/161 **Note** This port is route table dependent.	
Logging (Outbound)	• Syslog: UDP/20514, TCP/1468 • Secure Syslog: TCP/6514 **Note** Default ports are configurable for external logging. • SNMP Traps: UDP/162	
Session	• RADIUS Authentication: UDP/1645, 1812 • RADIUS Accounting: UDP/1646, 1813 • RADIUS DTLS Authentication/Accounting: UDP/2083. • RADIUS Change of Authorization (CoA) Send: UDP/1700 • RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799 **Note** UDP port 3799 is not configurable.	

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)	• Admin User Interface and Endpoint Authentications: • LDAP: TCP/389, 3268 • SMB: TCP/445 • KDC: TCP/88 • KPASS: TCP/464 • WMI : TCP/135 • ODBC: **Note** The ODBC ports are configurable on the third-party database server. • Microsoft SQL: TCP/1433 • Sybase: TCP/2638 • PortgreSQL: TCP/5432 • Oracle: TCP/1521 • NTP: UDP/123 • DNS: UDP/53, TCP/53 **Note** For external identity sources and services reachable only through an interface other than Gigabit Ethernet 0, configure static routes accordingly.	
Passive ID (Inbound)	• TS Agent: tcp/9094 • AD Agent: tcp/9095 • Syslog: UDP/40514, TCP/11468	
Web Portal Services: - Guest/Web Authentication - Guest Sponsor Portal - My Devices Portal - Client Provisioning - Certificate Provisioning - BlackList Portal	HTTPS (Interface must be enabled for service in Cisco ISE): • Blacklist Portal: TCP/8000-8999 (default port is TCP/8444) • Guest Portal and Client Provisioning: TCP/8000-8999 (default port is TCP/8443) • Certificate Provisioning Portal: TCP/8000-8999 (default port is TCP/8443) • My Devices Portal: TCP/8000-8999 (default port is TCP/8443) • Sponsor Portal: TCP/8000-8999 (default port is TCP/8445) • SMTP guest notifications from guest and sponsor portals: TCP/25	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Posture - Discovery - Provisioning - Assessment/ Heartbeat	• Discovery (Client side): TCP/80 (HTTP), TCP/8905 (HTTPS) **Note** By default, TCP/80 is redirected to TCP/8443. See Web Portal Services: Guest Portal and Client Provisioning. Cisco ISE presents the Admin certificate for Posture and Client Provisioning on TCP port 8905. Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use). • Discovery (Policy Service Node side): TCP/8443, 8905 (HTTPS) From Cisco ISE, Release 2.2 or later with AnyConnect, Release 4.4 or later, this port is configurable. • Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning • Provisioning - Active-X and Java Applet Install including IP refresh, Web Agent Install, and launch NAC Agent Install: See Web Portal Services: Guest Portal and Client Provisioning. • Provisioning - NAC Agent Install: TCP/8443 • Provisioning - NAC Agent Update Notification: UDP/8905 • Provisioning - NAC Agent and Other Package/Module Updates: TCP/8905 (HTTPS)	
Bring Your Own Device (BYOD) / Network Service Protocol (NSP) - Redirection - Provisioning - SCEP	• Provisioning - URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning. • For Android devices with EST authentication: TCP/8084. Port 8084 must be added to the Redirect ACL for Android devices. • Provisioning - Active-X and Java Applet Install (includes the launch of Wizard Install): See Web Portal Services: Guest Portal and Client Provisioning • Provisioning - Wizard Install from Cisco ISE (Windows and Mac OS): TCP/8443 • Provisioning - Wizard Install from Google Play (Android): TCP/443 • Provisioning - Supplicant Provisioning Process: TCP/8905 • SCEP Proxy to CA: TCP/80 or TCP/443 (Based on SCEP RA URL configuration)	

Cisco ISE Service	Ports on Gigabit Ethernet 0 or Bond 0	Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2
Mobile Device Management (MDM) API Integration	• URL Redirection: See Web Portal Services: Guest Portal and Client Provisioning • API: Vendor specific • Agent Install and Device Registration: Vendor specific	
Profiling	• NetFlow: UDP/9996 **Note** This port is configurable. • DHCP: UDP/67 **Note** This port is configurable. • DHCP SPAN Probe: UDP/68 • HTTP: TCP/80, 8080 • DNS: UDP/53 (lookup) **Note** This port is route table dependent. • SNMP Query: UDP/161 **Note** This port is route table dependent. • SNMP TRAP: UDP/162 **Note** This port is configurable.	

Cisco ISE pxGrid Service Ports

The following table lists the ports used by the pxGrid Service nodes:

Table 20: Ports Used by the pxGrid Service Node

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)
Administration	• SSL: TCP/5222 (Inter-Node Communication) • SSL: TCP/7400 (Node Group Communication)	—
pxGrid Subscribers	TCP/8910	
Inter-node communication	TCP/8910	

OCSP and CRL Service Ports

For the Online Certificate Status Protocol services (OCSP) and the Certificate Revocation List (CRL), the ports are dependent on the CA Server or on service hosting OCSP/CRL although references to the Cisco ISE services and ports list basic ports that are used in Cisco ISE Administration Node, Policy Service Node, Monitoring Node separately.

For the OCSP, the default ports that can be used are TCP 80/ TCP 443. Cisco ISE Admin portal expects http-based URL for OCSP services, and so, TCP 80 is the default. You can also use non-default ports.

For the CRL, the default protocols include HTTP, HTTPS, and LDAP and the default ports are 80, 443, and 389 respectively. The actual port is contingent on the CRL server.

Cisco ISE Processes

The following table lists the Cisco ISE processes and their service impact:

Process Name	Description	Service Impact
Database Listener	Oracle Enterprise Database Listener	Must be in Running state for all services to work properly
Database Server	Oracle Enterprise Database Server. Stores both configuration and operational data.	Must be in Running state for all services to work properly
Application Server	Main Tomcat Server for ISE	Must be in Running state for all services to work properly
Profiler Database	Redis database for ISE Profiling service	Must be in Running state for ISE profiling service to work properly
AD Connector	Active Directory Runtime	Must be in Running state for ISE to perform Active Directory authentications
MnT Session Database	Oracle TimesTen Database for MnT service	Must be in Running state for all services to work properly
MnT Log Collector	Log collector for MnT service	Must be in Running state for MnT Operational Data
MnT Log Processor	Log processor for MnT service	Must be in Running state for MnT Operational Data
Certificate Authority Service	ISE Internal CA service	Must be in Running state if ISE internal CA is enabled

Required Internet URLs

The following table lists the features that use certain URLs. Configure either your network firewall or a proxy server so that IP traffic can travel between Cisco ISE and these resources. If access to any URL listed in the following table cannot be provided, the related feature may be impaired or inoperable.

Table 21: Required URLs Access

Feature	URLs
Posture updates	https://www.cisco.com/ https://iseservice.cisco.com
Profiling Feed Service	https://ise.cisco.com
Smart Licensing	https://tools.cisco.com
Social Login for Self-Registered Guests	facebook.co akamaihd.net akamai.co fbcdn.net

The Interactive Help feature needs Cisco ISE to connect to the following URLs using the administration portal browser:

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