Cisco Identity Services Engine Installation Guide, Release 2.6

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
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1 Network Deployments in Cisco ISE

Cisco ISE Network Architecture 1
Cisco ISE Deployment Terminology 1
Node Types and Personas in Distributed Deployments 2
  Administration Node 2
  Policy Service Node 2
  Monitoring Node 3
  pxGrid Node 3
Standalone and Distributed ISE Deployments 3
Distributed Deployment Scenarios 4
Small Network Deployments 4
  Split Deployments 5
Medium-Sized Network Deployments 6
Large Network Deployments 7
  Centralized Logging 7
  Load Balancers 7
  Dispersed Network Deployments 8
Considerations for Planning a Network with Several Remote Sites 9
Maximum Supported Sessions for Each Deployment Model 9
Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions 11

CHAPTER 2 SNS 3500/3600 Series Appliances and Virtual Machine Requirements

Hardware and Virtual Appliance Requirements 13
  Cisco SNS-3500 and SNS-3600 Series Appliances 13
  VMware Virtual Machine Requirements 13
  Linux KVM Requirements 17
### Microsoft Hyper-V Requirements 19

### Virtual Machine Appliance Size Recommendations 21

### Disk Space Requirements 22

### Disk Space Guidelines 23

#### CHAPTER 3

**Install Cisco ISE** 27

- Install Cisco ISE Using CIMC 27
- Run the Setup Program 29
- Verify the Installation Process 31

#### CHAPTER 4

**Additional Installation Information** 33

- SNS Appliance Reference 33
- Create a Bootable USB Device to Install Cisco ISE 33
- Reimage the Cisco SNS 3500/3600 Series Appliance 34
- VMware Virtual Machine 35
- Virtual Machine Resource and Performance Checks 35
- Install Cisco ISE on VMware Virtual Machine Using the ISO File 35
- Prerequisites for Configuring a VMware ESXi Server 35
- Connect to the VMware Server Using the Serial Console 37
- Configure a VMware Server 38
- Increase Virtual Machine Power-On Boot Delay Configuration 39
- Install Cisco ISE Software on a VMware System 39
- VMware Tools Installation Verification 40
- Clone a Cisco ISE Virtual Machine 42
- Clone a Cisco ISE Virtual Machine Using a Template 43
- Change the IP Address and Hostname of a Cloned Virtual Machine 44
- Connect a Cloned Cisco Virtual Machine to the Network 46
- Migrate Cisco ISE VM from Evaluation to Production 46
- On-Demand Virtual Machine Performance Check Using the show tech-support Command 46
- Virtual Machine Resource Check from the Cisco ISE Boot Menu 47
- Linux KVM 48
- KVM Virtualization Check 48
- Install Cisco ISE on KVM 48
- Microsoft Hyper-V 51
CHAPTER 5

Installation Verification and Post-Installation Tasks

Log In to the Cisco ISE Web-Based Interface

Differences Between CLI Admin and Web-Based Admin Users Tasks

Create a CLI Admin

Create a Web-Based Admin

Reset a Disabled Password Due to Administrator Lockout

Cisco ISE Configuration Verification

Verify Configuration Using a Web Browser

Verify Configuration Using the CLI

List of Post-Installation Tasks

CHAPTER 6

Common System Maintenance Tasks

Bond Ethernet Interfaces for High Availability

Supported Platforms

Guidelines for Bonding Ethernet Interfaces

Configure NIC Bonding

Verify NIC Bonding Configuration

Remove NIC Bonding

Reset a Lost, Forgotten, or Compromised Password Using the DVD

Reset a Disabled Password Due to Administrator Lockout

Return Material Authorization

Change the IP Address of a Cisco ISE Appliance

View Installation and Upgrade History

Perform a System Erase

CHAPTER 7

Cisco ISE Ports Reference

Cisco ISE Infrastructure

Cisco ISE Administration Node Ports

Cisco ISE Monitoring Node Ports

Cisco ISE Policy Service Node Ports

Cisco ISE pxGrid Service Ports

OCSP and CRL Service Ports
CHAPTER 1

Network Deployments in Cisco ISE

- Cisco ISE Network Architecture, on page 1
- Cisco ISE Deployment Terminology, on page 1
- Node Types and Personas in Distributed Deployments, on page 2
- Standalone and Distributed ISE Deployments, on page 3
- Distributed Deployment Scenarios, on page 4
- Small Network Deployments, on page 4
- Medium-Sized Network Deployments, on page 6
- Large Network Deployments, on page 7
- Maximum Supported Sessions for Each Deployment Model, on page 9
- Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions, on page 11

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:
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>A specific feature that a persona provides such as network access, profiling, posture, security group access, monitoring, and troubleshooting.</td>
</tr>
<tr>
<td>Node</td>
<td>An individual physical or virtual ISE-PIC appliance.</td>
</tr>
<tr>
<td>Node Type</td>
<td>The Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring</td>
</tr>
<tr>
<td>Persona</td>
<td>Determines the services provided by a node. A Cisco ISE node can assume any or all of the following personas:</td>
</tr>
<tr>
<td>Role</td>
<td>Determines if a node is a standalone, primary, or secondary node and applies only to Administration and Monitoring nodes.</td>
</tr>
</tbody>
</table>

### 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 Source Group Tag 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.
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.
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.
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.

Load Balancers

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.
Dispersed Network Deployments

Dispersed Cisco ISE network deployments are most useful for organizations that have a main campus with regional, national, or satellite locations elsewhere. The main campus is where the primary network resides, 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.
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.

Maximum Supported Sessions for Each Deployment Model

The following tables list the maximum supported sessions for each deployment model.
Table 1: Maximum Supported Sessions per Deployment Model

<table>
<thead>
<tr>
<th>Deployment Model</th>
<th>Platform</th>
<th>Maximum Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone (All personas on a single node)</td>
<td>3615</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>3655</td>
<td>25,000</td>
</tr>
<tr>
<td></td>
<td>3695</td>
<td>50,000</td>
</tr>
<tr>
<td></td>
<td>3515</td>
<td>7,500</td>
</tr>
<tr>
<td></td>
<td>3595</td>
<td>20,000</td>
</tr>
<tr>
<td>Basic 2-node deployment (redundant)</td>
<td>3615</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>3655</td>
<td>25,000</td>
</tr>
<tr>
<td></td>
<td>3695</td>
<td>50,000</td>
</tr>
<tr>
<td></td>
<td>3515</td>
<td>7,500</td>
</tr>
<tr>
<td></td>
<td>3595</td>
<td>20,000</td>
</tr>
<tr>
<td>Hybrid-Distributed deployment (Admin and MnT on same appliance; Policy Service on dedicated appliance)</td>
<td>3615 as PAN and MnT</td>
<td>10,000</td>
</tr>
<tr>
<td></td>
<td>3655 as PAN and MnT</td>
<td>25,000</td>
</tr>
<tr>
<td></td>
<td>3695 as PAN and MnT</td>
<td>50,000</td>
</tr>
<tr>
<td></td>
<td>3515 as PAN and MnT</td>
<td>7,500</td>
</tr>
<tr>
<td></td>
<td>3595 as PAN and MnT</td>
<td>20,000</td>
</tr>
<tr>
<td>Dedicated (PAN, MnT, PXG, and PSN Nodes)</td>
<td>3595 as PAN and MnT</td>
<td>500,000</td>
</tr>
<tr>
<td></td>
<td>3655 as PAN and MnT</td>
<td>500,000</td>
</tr>
<tr>
<td></td>
<td>3695 as PAN/MnT</td>
<td>2,000,000</td>
</tr>
</tbody>
</table>

Table 2: Maximum Active Sessions per PSN

<table>
<thead>
<tr>
<th>Scaling per PSN1</th>
<th>Max Active Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNS 3615</td>
<td>10,000</td>
</tr>
<tr>
<td>SNS 3655</td>
<td>50,000</td>
</tr>
<tr>
<td>SNS 3695</td>
<td>100,000</td>
</tr>
<tr>
<td>SNS 3515</td>
<td>7,500</td>
</tr>
<tr>
<td>SNS 3595</td>
<td>40,000</td>
</tr>
</tbody>
</table>

1 Dedicated Policy nodes (Max sessions gated by 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.
SNS 3500/3600 Series Appliances and Virtual Machine Requirements

- Hardware and Virtual Appliance Requirements, on page 13
- Virtual Machine Appliance Size Recommendations, on page 21
- Disk Space Requirements, on page 22
- Disk Space Guidelines, on page 23

Hardware and Virtual Appliance Requirements

Cisco Identity Services Engine (ISE) can be installed on Cisco 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 3500 or 3600 series appliances. This section lists the hardware, software, and virtual machine requirements required to install Cisco ISE.

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.

Cisco SNS-3500 and SNS-3600 Series Appliances

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

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.

VMware Virtual Machine Requirements

Cisco ISE supports the following VMware servers and clients:

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

Note

The ISE OVA templates are not compatible with VMware web client for vCenter 6.5. As a workaround, use the VMware OVF tool to import the OVA templates.

You must reimage Cisco ISE from ISO if the virtual hard disk is resized after importing the OVA, as Cisco ISE does not support resizing hard disk and file systems after installation.

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

- Cisco ISE should be logged off—Cisco ISE does not allow to stop/pause the db operations during vMotion and so this may lead to data corruption issues. Hence, ensure that ISE is not running and active during the migration.

Note

Cisco ISE VM does not support Hot vMotion.

- Shared storage—The storage for the VM must reside on a storage area network (SAN), and the SAN must be accessible by all the VMware hosts that can host the VM being moved.

- VMFS volume sharing—The VMware host must use shared virtual machine file system (VMFS) volumes.

- Gigabit Ethernet interconnectivity—The SAN and the VMware hosts must be interconnected with Gigabit or faster Ethernet links.

- Processor compatibility—A compatible set of processors must be used. Processors must be from the same vendor and processor family for vMotion compatibility.

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 ISE does not support VMware snapshots for backing up ISE data because a VMware 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 VMware snapshots to back up ISE data results in stopping Cisco ISE services. A reboot is required to bring up the ISE node.

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

Note

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. For additional information about disk space requirements, see Disk Space Requirements, on page 22.

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.

* ISE-2.6.0.156-virtual-SNS3615-SNS3655-200.ova
* ISE-2.6.0.156-virtual-SNS3615-SNS3655-600.ova
* ISE-2.6.0.156-virtual-SNS3655-SNS3695-1200.ova
* ISE-2.6.0.156-virtual-SNS3695-2400.ova

The following table lists the VMware virtual machine requirements.
## VMware Virtual Machine Requirements

### CPU
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Specifications</th>
</tr>
</thead>
</table>
| **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 processors (6 cores with hyperthreading enabled)  
                   • Medium—16 processors (8 cores with hyperthreading enabled)  
                   • Large—16 processors (8 cores with hyperthreading enabled)  
                   SNS 3600 Series Appliance:  
                   • Small—16 processors (8 cores with hyperthreading enabled)  
                   • Medium—24 processors (12 cores with hyperthreading enabled)  
                   • Large—24 processors (12 cores with hyperthreading enabled) |

**Note** Even though Hyperthreading might improve overall VM performance, it does not change the supported scaling limits per VM appliance. Additionally, you must still allocate CPU resources based on the required number of physical cores, not the number of logical processors.

### Memory
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation</strong></td>
<td>• 16 GB</td>
</tr>
</tbody>
</table>
| **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 |

### Hard Disks
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation</strong></td>
<td>• 200 GB</td>
</tr>
</tbody>
</table>

See the recommended disk space for VMs in the following link: Disk Space Requirements.
Specifications

**Requirement Type** | **Specifications**
---|---
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.
Cisco ISE provides a number of methods to verify if your storage system meets these minimum requirements before, during, and after Cisco ISE installation. See Virtual Machine Resource and Performance Checks, on page 35 for more information.
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 GB 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**

The following table lists the Linux KVM virtual machine requirements.
## SNS 3500/3600 Series Appliances and Virtual Machine Requirements

<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td></td>
</tr>
</tbody>
</table>
| **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 processors (6 cores with hyperthreading enabled)  
|                  | • Medium—16 processors (8 cores with hyperthreading enabled)  
|                  | • Large—16 processors (8 cores with hyperthreading enabled)  |
| **SNS 3600 Series Appliance:** |  
|                  | • Small—16 processors (8 cores with hyperthreading enabled)  
|                  | • Medium—24 processors (12 cores with hyperthreading enabled)  
|                  | • Large—24 processors (12 cores with hyperthreading enabled)  |

**Note**  
Even though Hyperthreading might improve overall performance, it does not change the supported scaling limits per virtual machine appliance. Additionally, you must still allocate CPU resources based on the required number of physical cores, not the number of logical processors.

See [OVA Template Reservations](#) for CPU Reservations.
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Minimum Requirements</th>
</tr>
</thead>
</table>
| 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  
|                  | See [OVA Template Reservations](#) for Memory Reservations.  
| Hard disks       | • **Evaluation**—200 GB  
|                  | • **Production**  
|                  | 200 GB to 2.4 TB of disk storage (size depends on deployment and tasks).  
|                  | We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM.  
|                  | **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.  
|                  | See the recommended disk space for VMs in the following link: [Disk Space Requirements](#).  
| KVM Disk Device  | Disk bus - virtio, cache mode - none, I/O mode - native  
|                  | Use preallocated RAW storage format.  
| NIC              | 1 GB 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**

The following table lists Microsoft Hyper-V virtual machine requirements.
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td><strong>Evaluation</strong></td>
</tr>
<tr>
<td></td>
<td>• Clock speed—2.0 GHz or faster</td>
</tr>
<tr>
<td></td>
<td>• Number of cores—2 CPU cores</td>
</tr>
<tr>
<td></td>
<td><strong>Production</strong></td>
</tr>
<tr>
<td></td>
<td>• Clock speed—2.0 GHz or faster</td>
</tr>
<tr>
<td></td>
<td><strong>Number of Cores</strong></td>
</tr>
<tr>
<td><strong>SNS 3500 Series Appliance:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Small—12 processors (6 cores with hyperthreading enabled)</td>
</tr>
<tr>
<td></td>
<td>• Medium—16 processors (8 cores with hyperthreading enabled)</td>
</tr>
<tr>
<td></td>
<td>• Large—16 processors (8 cores with hyperthreading enabled)</td>
</tr>
<tr>
<td><strong>SNS 3600 Series Appliance:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Small—16 processors (8 cores with hyperthreading enabled)</td>
</tr>
<tr>
<td></td>
<td>• Medium—24 processors (12 cores with hyperthreading enabled)</td>
</tr>
<tr>
<td></td>
<td>• Large—24 processors (12 cores with hyperthreading enabled)</td>
</tr>
</tbody>
</table>

See OVA Template Reservations for CPU Reservations.

<table>
<thead>
<tr>
<th>Memory</th>
<th><strong>Evaluation</strong>—16 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Production</strong></td>
</tr>
<tr>
<td></td>
<td>• Small—16 GB for SNS 3515 and 32 GB for SNS 3615</td>
</tr>
<tr>
<td></td>
<td>• Medium—64 GB for SNS 3595 and 96 GB for SNS 3655</td>
</tr>
<tr>
<td></td>
<td>• Large—256 GB</td>
</tr>
</tbody>
</table>

See OVA Template Reservations for Memory Reservations.
<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Minimum Requirements</th>
</tr>
</thead>
</table>
| Hard disks       | • **Evaluation**—200 GB  
|                  | • **Production**  
|                  | 200 GB to 2.4 TB of disk storage (size depends on deployment and tasks).  
|                  | We recommend that your VM host server use hard disks with a minimum speed of 10,000 RPM.  
|                  | **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.  
|                  | See the recommended disk space for VMs in the following link: [Disk Space Requirements](#). |
| NIC              | 1 GB NIC interface required (two or more NICs are recommended; six NICs are supported). |
| Hypervisor       | Hyper-V (Microsoft) |

**Virtual Machine Appliance Size Recommendations**

Large VM for Monitoring nodes was introduced in Cisco ISE 2.4. 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. The following tables provide the minimum resources required to size your virtual appliance comparable to that of an SNS 3500 or SNS 3600 series physical appliance.

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.

Note

OVF templates are not applicable for Linux KVM. OVF templates are available only for VMware virtual machines.

• 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. See Disk Space Requirements, on page 22 for details on the disk space required for various Cisco ISE nodes and personas.

• 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.

Table 3: VM Appliance Specifications for a Production Environment for SNS 3600 Series Appliance

<table>
<thead>
<tr>
<th>Platform</th>
<th>Small VM Appliance (based on SNS-3615)</th>
<th>Medium VM Appliance (based on SNS-3655)</th>
<th>Large VM Appliance (based on SNS-3695)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>8 total cores—You must enable hyperthreading and assign the resulting number of logical processors (16) to each server.</td>
<td>12 total cores—You must enable hyperthreading and assign the resulting number of logical processors (24) to each server.</td>
<td>12 total cores—You must enable hyperthreading and assign the resulting number of logical processors (24) to each server.</td>
</tr>
<tr>
<td>Memory</td>
<td>32 GB</td>
<td>96 GB</td>
<td>256 GB</td>
</tr>
<tr>
<td>Total Disk Space</td>
<td>200 GB—2.4 TB.</td>
<td>200 GB—2.4 TB.</td>
<td>200 GB—2.4 TB.</td>
</tr>
<tr>
<td>Ethernet NICs</td>
<td>Up to 6 Gigabit Ethernet NICs</td>
<td>Up to 6 Gigabit Ethernet NICs</td>
<td>Up to 6 Gigabit Ethernet NICs</td>
</tr>
</tbody>
</table>

Disk Space Requirements

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 4: Recommended Disk Space for Virtual Machines

<table>
<thead>
<tr>
<th>ISE Persona</th>
<th>Minimum Disk Space for Evaluation</th>
<th>Minimum Disk Space for Production</th>
<th>Recommended Disk Space for Production</th>
<th>Maximum Disk Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone ISE</td>
<td>200 GB</td>
<td>600 GB</td>
<td>600 GB to 2.4 TB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—Administration only</td>
<td>200 GB</td>
<td>250 GB</td>
<td>250 to 300 GB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—Monitoring only</td>
<td>200 GB</td>
<td>600 GB</td>
<td>600 GB to 2.4 TB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—Policy Service only</td>
<td>200 GB</td>
<td>200 GB</td>
<td>200 GB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—pxGrid only</td>
<td>200 GB</td>
<td>200 GB</td>
<td>200 GB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—Administration and Monitoring (and optionally pxGrid)</td>
<td>200 GB</td>
<td>600 GB</td>
<td>600 GB to 2.4 TB</td>
<td>2.4 TB</td>
</tr>
<tr>
<td>Distributed ISE—Administration, Monitoring, and Policy Service (and optionally pxGrid)</td>
<td>200 GB</td>
<td>600 GB</td>
<td>600 GB to 2.4 TB</td>
<td>2.4 TB</td>
</tr>
</tbody>
</table>

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**

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

- You can allocate only up to 1.999 TB of disk space for a Cisco ISE VM.
- 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. Depending on your requirements, you can increase the VM disk size up to a maximum of 1.999 TB.

If you increase the disk size of your virtual machine after initial installation, then you must perform a fresh installation of Cisco ISE on your virtual machine to 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 5: Monitoring Node Log Storage—Retention Period in Days for RADIUS**

<table>
<thead>
<tr>
<th>No. of Endpoints</th>
<th>200 GB</th>
<th>600 GB</th>
<th>1024 GB</th>
<th>2048 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>5,000</td>
<td>504</td>
<td>1510</td>
<td>2577</td>
<td>5154</td>
</tr>
<tr>
<td>10,000</td>
<td>252</td>
<td>755</td>
<td>1289</td>
<td>2577</td>
</tr>
<tr>
<td>25,000</td>
<td>101</td>
<td>302</td>
<td>516</td>
<td>1031</td>
</tr>
<tr>
<td>50,000</td>
<td>51</td>
<td>151</td>
<td>258</td>
<td>516</td>
</tr>
<tr>
<td>100,000</td>
<td>26</td>
<td>76</td>
<td>129</td>
<td>258</td>
</tr>
<tr>
<td>150,000</td>
<td>17</td>
<td>51</td>
<td>86</td>
<td>172</td>
</tr>
<tr>
<td>200,000</td>
<td>13</td>
<td>38</td>
<td>65</td>
<td>129</td>
</tr>
<tr>
<td>250,000</td>
<td>11</td>
<td>31</td>
<td>52</td>
<td>104</td>
</tr>
<tr>
<td>500,000</td>
<td>6</td>
<td>16</td>
<td>26</td>
<td>52</td>
</tr>
</tbody>
</table>

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 6: Monitoring Node Log Storage—Retention Period in Days for TACACS+**

<table>
<thead>
<tr>
<th>No. of Endpoints</th>
<th>200 GB</th>
<th>600 GB</th>
<th>1024 GB</th>
<th>2048 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>12,583</td>
<td>37,749</td>
<td>64,425</td>
<td>12,8850</td>
</tr>
<tr>
<td>500</td>
<td>2,517</td>
<td>7,550</td>
<td>12,885</td>
<td>25,770</td>
</tr>
</tbody>
</table>
If you find that context and visibility is slow, or you are running out of room for logs, you need to allocate more disk space.

To plan for additional log storage, for every 100 GB of disk space that you add, 60 GB is available for log storage. The maximum VM disk size is 1.999 TB.

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.
Install Cisco ISE

• Install Cisco ISE Using CIMC, on page 27
• Run the Setup Program, on page 29
• Verify the Installation Process, on page 31

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 Hardware and Virtual Appliance Requirements as specified in this book.

• (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 38
  • Install Cisco ISE on KVM, on page 48
  • Create a Cisco ISE Virtual Machine on Hyper-V, on page 51

• (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.

Step 2

Download the Cisco ISE ISO image.

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:
  1. Connect to CIMC and log in using the CIMC credentials.
  2. Launch the KVM console.
  3. Choose Virtual Media > Activate Virtual Devices.
  4. Choose Virtual Media > Map CD/DVD and select the ISE ISO image and click Map Device.
  5. Choose Macros > Static Macros > Ctrl-Alt-Del to boot the appliance with the ISE ISO image.
  6. Press F6 to bring up the boot menu. A screen similar to the following one appears:

    
    ![Figure 6: Boot Device Selection](image)

    **Figure 6: Boot Device Selection**

- Virtual Machine:

  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.
1. 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: 2.6.0.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, on page 29 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 Verify the Installation Process, on page 31.

---

Run the Setup Program

This section describes the setup process to configure the ISE-PIC 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-PIC 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.

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.

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

**Table 7: Cisco ISE-PIC Setup Program Parameters**

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>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.</td>
<td>isebeta1</td>
</tr>
<tr>
<td>(eth0) Ethernet interface address</td>
<td>Must be a valid IPv4 or Global IPv6 address for the Gigabit Ethernet 0 (eth0) interface.</td>
<td>10.12.13.14/2001:420:54ff:4::458:121:119</td>
</tr>
<tr>
<td>Netmask</td>
<td>Must be a valid IPv4 or IPv6 netmask.</td>
<td>255.255.255.0/2001:420:54ff:4::458:121:119/122</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Must be a valid IPv4 or Global IPv6 address for the default gateway.</td>
<td>10.12.13.1/2001:420:54ff:4::458:1</td>
</tr>
<tr>
<td>DNS domain name</td>
<td>Cannot be an IP address. Valid characters include ASCII characters, any numerals, the hyphen (-), and the period (.).</td>
<td>example.com</td>
</tr>
<tr>
<td>Primary name server</td>
<td>Must be a valid IPv4 or Global IPv6 address for the primary name server.</td>
<td>10.15.20.25 / 2001:420:54ff:4::458:118</td>
</tr>
<tr>
<td>Add/Edit another name server</td>
<td>Must be a valid IPv4 or Global IPv6 address for the primary name server.</td>
<td>(Optional) Allows you to configure multiple name servers. To do so, enter y to continue.</td>
</tr>
<tr>
<td>Primary NTP server</td>
<td>Must be a valid IPv4 or Global IPv6 address or hostname of a Network Time Protocol (NTP) server.</td>
<td>clock.nist.gov / 10.15.20.25 / 2001:420:54ff:4::458:117</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Ensure that the primary NTP server is reachable.</td>
<td></td>
</tr>
<tr>
<td>Add/Edit another NTP server</td>
<td>Must be a valid NTP domain.</td>
<td>(Optional) Allows you to configure multiple NTP servers. To do so, enter y to continue.</td>
</tr>
</tbody>
</table>
ExampleDescriptionPrompt
UTC (default)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).
You can run the show timezones command from the Cisco ISE-PIC CLI for a complete list of supported time zones.

System Time Zone

Username
Identifies the administrative username used for CLI access to the Cisco ISE-PIC 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-PIC 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-PIC using the username and password that was configured during the setup process.

Verify the 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 (dhcpcd)    disabled   
DNS Server (named)      disabled   
```

ise/admin#
Additional Installation Information

• SNS Appliance Reference, on page 33
• VMware Virtual Machine, on page 35
• Linux KVM, on page 48
• Microsoft Hyper-V, on page 51

SNS Appliance Reference

Create a Bootable USB Device to Install Cisco ISE

Use the Fedora Media Writer (formerly Fedora Live USB Creator) tool to create a bootable USB device from the Cisco ISE installation ISO file.

Before you begin

- Download Fedora Media Writer to the local system from the following location: https://github.com/lmacken/liveusb-creator/releases/tag/3.12.0

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 an 8-GB (or higher) USB device.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Reformat the USB device using FAT16 or FAT32 to free up all the space.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Plug in the USB device to the local system and launch Fedora Media Writer.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Browse from the Use existing Live CD area and select the Cisco ISE ISO file.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(If there is only one USB device connected to the local system, it is selected automatically) Select the USB device from the Target Device drop down.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Create Live USB.</td>
</tr>
</tbody>
</table>
The progress bar indicates the progress of the bootable USB creation. After this process is complete, the contents 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:

- syslinux/sylinux.cfg
- EFI/BOOT/grub.cfg

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

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

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

\[ \text{ks=cdrom:/ks.cfg} \]

with

\[ \text{ks=hd:sdb1:/ks.cfg} \]

**Step 8**
Save the files and exit.

**Step 9**
Safely remove the USB device from the local system.

**Step 10**
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 3500/3600 Series Appliance

The Cisco SNS 3500/3600 series 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
The SNS 3500 and 3600 series 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 3500 and 3600 series 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.

The SNS 3600 series appliances support only Cisco ISE 2.5 or later releases.

- Use the Cisco Integrated Management Controller (CIMC) interface to map the installation .iso file to the virtual DVD device. See Install Cisco ISE Using CIMC, on page 27 for more information.

- 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. See Create a Bootable USB Device to Install Cisco ISE, on page 33 and Install Cisco ISE Using CIMC, on page 27 for more information.
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 aborts. 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.

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. You must also ensure that your guest operating system type is set to Red Hat Enterprise Linux 7 (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.
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.

<table>
<thead>
<tr>
<th>ADE-OS</th>
<th>Cisco ISE</th>
<th>E1000</th>
<th>VMXNET3</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth0</td>
<td>GE0</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>eth1</td>
<td>GE1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>eth2</td>
<td>GE2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>eth3</td>
<td>GE3</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>eth4</td>
<td>GE4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>eth5</td>
<td>GE5</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

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

Note

- Ensure that you allocate the recommended amount of disk space on the VMware virtual machine. See the Disk Space Requirements, on page 22 section for more information.

- 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 VT 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.
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 details in the Prerequisites for Configuring a VMware ESXi Server, on page 35 section.

---

**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**
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 **Red Hat Enterprise Linux 7** 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:

**SNS 3500 Series Appliance:**
- Small—12 processors (6 cores with hyperthreading enabled)
- Medium—16 processors (8 cores with hyperthreading enabled)
- Large—16 processors (8 cores with hyperthreading enabled)

**SNS 3600 Series Appliance:**
- Small—16 processors (8 cores with hyperthreading enabled)
- Medium—24 processors (12 cores with hyperthreading enabled)
- Large—24 processors (12 cores with hyperthreading enabled)

**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 **E1000** NIC driver from the Adapter drop-down list and click **Next**.

**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.

**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 Provision** radio button, and click **Next** to continue.
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 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.

**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

**Before you begin**
- After installation, if you do not install a permanent license, Cisco ISE automatically installs a 90-day evaluation license that supports a maximum of 100 endpoints.

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

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

**Step 3**
Click the **Options** tab.
Step 4  Select **Boot Options** and configure the following option:

a)  In the **Force BIOS Setup** area, check the check box to enter the BIOS setup screen when the virtual machine boots.

*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.

Step 5  Click **OK**.

Step 6  Ensure that the Coordinated Universal Time (UTC) and the correct boot order is set in BIOS:

a) If the virtual machine is turned on, turn the system off.

b) Turn on the virtual machine.

   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](https://www.vmware.com/support/pubs/vsphere_6.7_pubs.html) 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.
Verify VMWare Tools Installation Using the CLI

You can also verify if the VMware tools are installed using the `showinventory` 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: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 2: Device Name: eth2:
NIC 2: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 3: Device Name: eth3:
NIC 3: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 4: Device Name: eth4:
NIC 4: Driver Descr: Intel(R) Gigabit Ethernet Network Driver
NIC 5: Device Name: eth5:
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 (regular, upgrade, or patch) 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 (regular, upgrade, or patch release).

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**  
- Change the IP Address and Hostname of a Cloned Virtual Machine  
- Connect 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 43

**Step 2**  
Deploy a Virtual Machine Template, on page 44

---

#### 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**.
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 1.999 TB).

- Please note 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.

---

**On-Demand Virtual Machine Performance Check Using the show tech-support Command**

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
[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:
  ```bash
  # cat /proc/cpuinfo
  flags: fpu vme de pse 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:
  ```bash
  # cat /proc/cpuinfo
  flags: fpu tsc mcr pse 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:

```bash
# 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-2.6.0.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-2.6.0.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, Red Hat Enterprise Linux 7.0 as the 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 File System 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.
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk bus</td>
<td>VirtIO</td>
</tr>
<tr>
<td>Cache mode</td>
<td>none</td>
</tr>
<tr>
<td>IO mode</td>
<td>native</td>
</tr>
</tbody>
</table>

**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.

**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.

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

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

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

**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.

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

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

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

**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**.

**Step 10**  Click **Finish**.

The Cisco ISE VM is created on Hyper-V.

**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**.

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

The Cisco ISE installation menu appears.

**Step 13**  Enter 1 to install Cisco ISE using a keyboard and monitor.
Create a Cisco ISE Virtual Machine on Hyper-V
Installation Verification and Post-Installation Tasks

- Log In to the Cisco ISE Web-Based Interface, on page 53
- Cisco ISE Configuration Verification, on page 55
- List of Post-Installation Tasks, on page 57

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.

---

Before you begin

The Cisco ISE Admin portal supports the following browsers for the Admin Portal:

- Mozilla Firefox 62 and earlier versions
- Google Chrome 69 and earlier versions
- Microsoft Internet Explorer 10.x and 11.x

If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

---

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 hostname>/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 8: Tasks Performed by CLI-Admin and Web-Based Admin Users

<table>
<thead>
<tr>
<th>Admin User Type</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both CLI-Admin and Web-Based Admin</td>
<td>• Back up the Cisco ISE application data.</td>
</tr>
<tr>
<td></td>
<td>• Display any system, application, or diagnostic logs on the Cisco ISE appliance.</td>
</tr>
<tr>
<td></td>
<td>• Apply Cisco ISE software patches, maintenance releases, and upgrades.</td>
</tr>
<tr>
<td></td>
<td>• Set the NTP server configuration.</td>
</tr>
<tr>
<td>CLI-Admin only</td>
<td>• Start and stop the Cisco ISE application software.</td>
</tr>
<tr>
<td></td>
<td>• Reload or shut down the Cisco ISE appliance.</td>
</tr>
<tr>
<td></td>
<td>• Reset the web-based admin user in case of a lockout.</td>
</tr>
<tr>
<td></td>
<td>• Access the ISE CLI.</td>
</tr>
</tbody>
</table>
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 entering into the configuration mode in the CLI and using the `username` command.

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.

You can add web-based admin users through the user interface itself.

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 Monitor > Reports > Catalog > Server Instance > Server Instance > Server Administrator Logins report, and suspends the credentials for that administrator ID 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.
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**

To get the latest Cisco ISE patches and keep Cisco ISE up-to-date, visit the following web site:


**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.

**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

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

List of Post-Installation Tasks

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

Table 9: Mandatory Post-Installation Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Link in the Administration Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the latest patches, if any</td>
<td>Install a Software Patch</td>
</tr>
<tr>
<td>Install Licenses</td>
<td>See the Cisco ISE Ordering Guide for more information. See the Administration Guide for information on how to Register Licenses.</td>
</tr>
<tr>
<td>Install Certificates</td>
<td>See the Manage Certificates chapter of the Cisco ISE Administration Guide for more details.</td>
</tr>
<tr>
<td>Create Repository for Backups</td>
<td>See the Create Repositories section of the Cisco ISE Administration Guide for more details.</td>
</tr>
<tr>
<td>Configure Backup Schedules</td>
<td>See the Schedule a Backup section of the Cisco ISE Administration Guide for more details.</td>
</tr>
</tbody>
</table>
## List of Post-Installation Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Link in the Administration Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploy Cisco ISE personas</td>
<td>See the Set Up Cisco ISE in a Distributed Environment chapter of the Cisco ISE Administration Guide.</td>
</tr>
</tbody>
</table>
Common System Maintenance Tasks

- Bond Ethernet Interfaces for High Availability, on page 59
- Reset a Lost, Forgotten, or Compromised Password Using the DVD, on page 64
- Reset a Disabled Password Due to Administrator Lockout, on page 65
- Return Material Authorization, on page 66
- Change the IP Address of a Cisco ISE Appliance, on page 66
- View Installation and Upgrade History, on page 67
- Perform a System Erase, on page 67

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 10: Physical NICs Bonded Together to Form an Interface

<table>
<thead>
<tr>
<th>Cisco ISE Physical NIC Name</th>
<th>Linux Physical NIC Name</th>
<th>Role in Bonded NIC</th>
<th>Bonded NIC Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet 0</td>
<td>Eth0</td>
<td>Primary</td>
<td>Bond 0</td>
</tr>
<tr>
<td>Gigabit Ethernet 1</td>
<td>Eth1</td>
<td>Backup</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet 2</td>
<td>Eth2</td>
<td>Primary</td>
<td>Bond 1</td>
</tr>
<tr>
<td>Gigabit Ethernet 3</td>
<td>Eth3</td>
<td>Backup</td>
<td></td>
</tr>
<tr>
<td>Gigabit Ethernet 4</td>
<td>Eth4</td>
<td>Primary</td>
<td>Bond 2</td>
</tr>
<tr>
<td>Gigabit Ethernet 5</td>
<td>Eth5</td>
<td>Backup</td>
<td></td>
</tr>
</tbody>
</table>

Supported Platforms

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

- SNS 3500 and 3600 series 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.
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:

```plaintext
!  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.

```plaintext
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=6147<UP,BROADCAST,SLAVE,MULTICAST> mtu 1500
```
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.
Reset a Lost, Forgotten, or Compromised Password Using the 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)
```

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
[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:
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 Monitor > Reports > Catalog > Server Instance > Server Instance > Server Administrator Logins report, and suspends the credentials for that administrator ID 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 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: Fri Nov 30 21:48:58 UTC 2018
Application: ise
Version: 2.6.0.xxx
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
[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.
Perform a System Erase
Cisco ISE Ports Reference

- Cisco ISE Infrastructure, on page 71
- Cisco ISE Administration Node Ports, on page 71
- Cisco ISE Monitoring Node Ports, on page 73
- Cisco ISE Policy Service Node Ports, on page 75
- Cisco ISE pxGrid Service Ports, on page 79
- OCSP and CRL Service Ports, on page 80

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:

- 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.
- All NICs can be configured with IP addresses.

Cisco ISE Administration Node Ports

The following table lists the ports used by the Administration nodes:
### Table 11: Ports Used by the Administration Nodes

<table>
<thead>
<tr>
<th>Cisco ISE Service</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>• HTTP: TCP/80, HTTPS: TCP/443 (TCP/80 redirected to TCP/443; not configurable)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• SSH Server: TCP/22</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• External RESTful Services (ERS) REST API: TCP/9060</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• To display Sponsor portal from the Admin GUI: TCP/9002</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ElasticSearch (Context Visibility; to replicate data from primary to secondary Admin node): TCP/9300</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ports 80 and 443 support Admin web applications and are enabled by default.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>HTTPS and SSH access to Cisco ISE is restricted to Gigabit Ethernet 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP/9300 must be open on both Primary and Secondary Administration Nodes for incoming traffic.</td>
<td></td>
</tr>
<tr>
<td>Replication and Synchronization</td>
<td>• HTTPS (SOAP): TCP/443</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• Data synchronization/Replication (JGroups): TCP/12001 (Global)</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>SNMP Query: UDP/161</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>This port is route table dependent.</td>
<td></td>
</tr>
<tr>
<td>Cisco ISE Service</td>
<td>Ports on Gigabit Ethernet 0 or Bond 0</td>
<td>Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and 2)</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logging (Outbound)</td>
<td>• Syslog: UDP/20514, TCP/1468</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Secure Syslog: TCP/6514</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Default ports are configurable for external logging.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SNMP Traps: UDP/162</td>
<td></td>
</tr>
</tbody>
</table>

| 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                                                                                       |
|                                                   | • PostgreSQL: TCP/5432                                                                                  |
|                                                   | • Oracle: TCP/1512                                                                                       |
|                                                   | • 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 12: Ports Used by the Monitoring Nodes

<table>
<thead>
<tr>
<th>Cisco ISE Service</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>• HTTP: TCP/80, HTTPS: TCP/443</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• SSH Server: TCP/22</td>
<td></td>
</tr>
<tr>
<td>Replication and Synchronization</td>
<td>• HTTPS (SOAP): TCP/443</td>
<td>Oracle DB Listener: TCP/1521</td>
</tr>
<tr>
<td></td>
<td>• Oracle DB Listener: TCP/1521</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Data Synchronization/Replication (JGroups): TCP/12001 (Global)</td>
<td></td>
</tr>
<tr>
<td>Monitoring</td>
<td>Simple Network Management Protocol [SNMP]: UDP/161</td>
<td>This port is route table dependent.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>• Syslog: UDP/20514, TCP/1468</td>
<td>Default ports are configurable for external logging.</td>
</tr>
<tr>
<td></td>
<td>• Secure Syslog: TCP/6514</td>
<td></td>
</tr>
<tr>
<td>Note</td>
<td></td>
<td>SMTP: TCP/25 for email of alarms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP Traps: UDP/162</td>
</tr>
<tr>
<td>Cisco ISE Service</td>
<td>Ports on Gigabit Ethernet 0 or Bond 0</td>
<td>Ports on Other Ethernet Interfaces (Gigabit Ethernet 1 through 5, or Bond 1 and Bond 2)</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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  
  • PostgreSQL: TCP/5432  
  • Oracle: TCP/1512  
  • 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

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

*Table 13: Ports Used by the Policy Service Nodes*

<table>
<thead>
<tr>
<th>Cisco ISE Service</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2</th>
</tr>
</thead>
</table>
| Administration    | • HTTP: TCP/80, HTTPS: TCP/443  
  • SSH Server: TCP/22  
  • OCSP: TCP/2560 | Cisco ISE management is restricted to Gigabit Ethernet 0. |
<table>
<thead>
<tr>
<th>Cisco ISE Service</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication and Synchronization</td>
<td>• HTTPS (SOAP): TCP/443</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• Data Synchronization / Replication (JGroups): TCP/12001 (Global)</td>
<td>—</td>
</tr>
<tr>
<td>Clustering (Node Group)</td>
<td>Node Groups/JGroups: TCP/7800</td>
<td>—</td>
</tr>
<tr>
<td>CA PKI</td>
<td>TCP/9090</td>
<td>—</td>
</tr>
<tr>
<td>IPSec/ISAKMP</td>
<td>UDP/500</td>
<td>—</td>
</tr>
<tr>
<td>Device Administration</td>
<td>TACACS+: TCP/49</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This port is configurable in Release 2.1 and later releases.</td>
<td>—</td>
</tr>
<tr>
<td>SXP</td>
<td>• PSN (SXP node) to NADs: TCP/64999</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• PSN to SXP (inter-node communication): TCP/443</td>
<td>—</td>
</tr>
<tr>
<td>TC-NAC</td>
<td>TCP/443</td>
<td>—</td>
</tr>
<tr>
<td>Monitoring</td>
<td>Simple Network Management Protocol [SNMP]: UDP/161</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This port is route table dependent.</td>
<td>—</td>
</tr>
<tr>
<td>Logging (Outbound)</td>
<td>• Syslog: UDP/20514, TCP/1468</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• Secure Syslog: TCP/6514</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Default ports are configurable for external logging.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• SNMP Traps: UDP/162</td>
<td>—</td>
</tr>
<tr>
<td>Session</td>
<td>• RADIUS Authentication: UDP/1645, 1812</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• RADIUS Accounting: UDP/1646, 1813</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• RADIUS DTLS Authentication/Accounting: UDP/2083.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• RADIUS Change of Authorization (CoA) Send: UDP/1700</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• RADIUS Change of Authorization (CoA) Listen/Relay: UDP/1700, 3799</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> UDP port 3799 is not configurable.</td>
<td>—</td>
</tr>
<tr>
<td>Cisco ISE Service</td>
<td>Ports on Gigabit Ethernet 0 or Bond 0</td>
<td>Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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  
  • PostgreSQL: TCP/5432  
  • Oracle: TCP/1512  
  • 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  
  - BlackListing 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/8443.)  
  • SMTP guest notifications from guest and sponsor portals: TCP/25 |
## Cisco ISE Ports Reference

### Cisco ISE Service

<table>
<thead>
<tr>
<th>Posture</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Discovery</td>
<td>• Discovery (Client side): TCP/80 (HTTP), TCP/8905 (HTTPS)</td>
<td></td>
</tr>
<tr>
<td>- Provisioning</td>
<td>• Discovery (Policy Service Node side): TCP/8443, 8905 (HTTPS)</td>
<td></td>
</tr>
<tr>
<td>- Assessment/ Heartbeat</td>
<td>• Note: By default, TCP/80 is redirected to TCP/8443. See Web Portal Services: Guest Portal and Client Provisioning.</td>
<td>Cisco ISE presents the Admin certificate for Posture and Client Provisioning on TCP port 8905.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).</td>
</tr>
</tbody>
</table>

### Note

- **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
- **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.
- **NAC Agent Install:** TCP/8443
- **NAC Agent Update Notification:** UDP/8905
- **NAC Agent and Other Package/Module Updates:** TCP/8905 (HTTPS)
- **Assessment - Posture Negotiation and Agent Reports:** TCP/8905 (HTTPS)
- **Assessment - PRA/Keep-alive:** UDP/8905

### Bring Your Own Device (BYOD) / Network Service Protocol (NSP)

| - Provisioning                        | • For Android devices with EST authentication: TCP/8084. Port 8084 must be added to the Redirect ACL for Android devices. |
| - SCEP                                 | • 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 pxGrid Service Ports

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

Table 14: Ports Used by the pxGrid Service Node

<table>
<thead>
<tr>
<th>Cisco ISE Service</th>
<th>Ports on Gigabit Ethernet 0 or Bond 0</th>
<th>Ports on Other Ethernet Interfaces, or Bond 1 and Bond 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>• SSL: TCP/5222 (Inter-Node Communication)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>• SSL: TCP/7400 (Node Group Communication)</td>
<td>—</td>
</tr>
</tbody>
</table>
OCSP and CRL Service Ports

Port 8671 is used for inter-node secure AMQPS communication and must be open on all the nodes.

Port 8672 is exposed by the ISE RabbitMQ Service for AMQP communication. However, none of the ISE services connect to the RabbitMQ service.

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.